



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

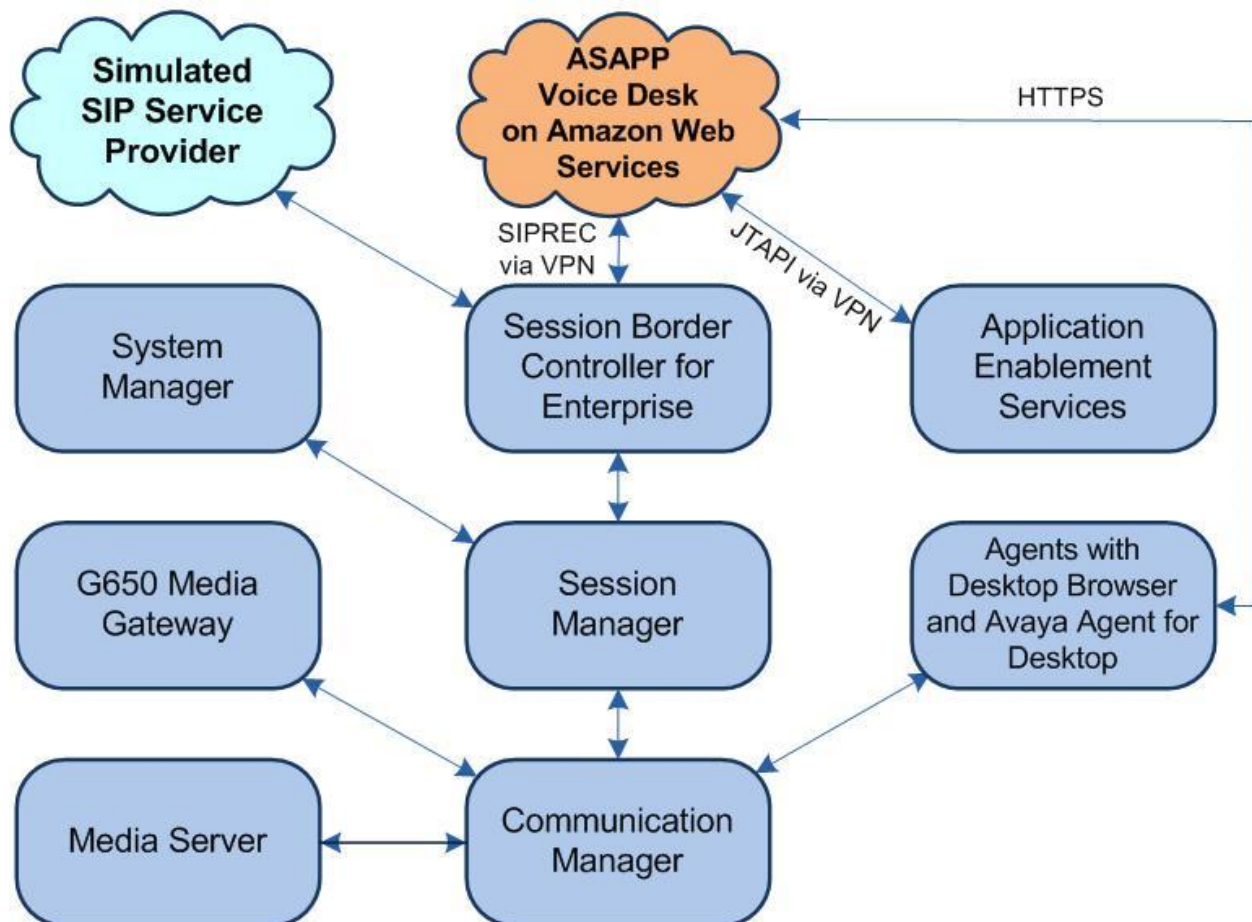


Figure 1: Compliance Testing Configuration

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 <ul style="list-style-type: none">• 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		
Name: AES CTI Link		
Unicode Name? n		
	COR: 1	

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 UII 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.

- **UI 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		
UI Treatment: shared		
Maximum Size of UII 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 screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page, there is a light gray rectangular box containing the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. A second red horizontal bar is located at the bottom of the page.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". On the right, a welcome message for the user is displayed, including login details and system information. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, explaining the purpose of the OAM Web and listing the administrative domains it manages: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also notes that these domains can be managed by a single administrator or separate administrators.

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Home | Help | Logout

Home

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

Welcome to OAM

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

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

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

6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" page, which provides instructions on how to set up and maintain the WebLM, import and set up the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. The left sidebar shows the navigation menu with "Licensing" selected, and sub-options like WebLM Server Address, WebLM Server Access, and Reserved Licenses are visible under the "Licensing" section.

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking

Licensing

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

- WebLM Server Address

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

- WebLM Server Access

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

- Reserved Licenses

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.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home User Management Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
- ▼ Application_Enablement
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
- ASBCE
 - Session_Border_Controller_E_AE
- CCTR
 - ContactCenter
- COMMUNICATION_MANAGER
 - Call_Center
 - Communication_Manager
- MESSAGING
 - Messaging
- MSR
 - Media_Server
- SYSTEM_MANAGER
 - System_Manager
- SessionManager

Application Enablement (CTI) - Release: 8 - SID: 10503000(Enterprise)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: August 8, 2019 4:43:51 PM -05:00

License File Host IDs:	VE-83-02-2D-26-52-01
Active License Mode	Standard
License State	NA
Pay Per Use License Available	No
Standard License Available	Yes

Feature (License Keyword)	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
DLG (VALUE_AES_DLG)	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	1000

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 screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays user information: Welcome: User, Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes7/10.64.101.239, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 8.1.3.0.0.25-0, Server Date and Time: Tue Sep 14 10:42:19 EDT 2021, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected and 'TSAPI Links' highlighted. The main content area is titled 'TSAPI Links' and contains a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete 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.

The screenshot shows the AVAYA Application Enablement Services Management Console, specifically the 'Edit TSAPI Links' screen. The top right corner displays the same user information as the previous screenshot. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected and 'TSAPI Links' highlighted. The main content area is titled 'Edit TSAPI Links' and contains a form with the following fields: Link (text input), Switch Connection (drop-down menu with 'cm7' selected), Switch CTI Link Number (drop-down menu with '1' selected), ASAI Link Version (drop-down menu with '12' selected), and Security (drop-down menu with 'Both' selected). Below the form are buttons for 'Apply Changes', 'Cancel Changes', and 'Advanced Settings'.

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:46:36 EDT 2021
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Idasapp

* Common Nameasapp

* Surnameasapp

* User Password*****

* Confirm Password*****

Admin Note

Avaya RoleNone

Business Category

Car License

CM Home

Css Home

CT UserYes

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.3.0.0.25-0", "Server Date and Time: Tue Sep 14 10:42:19 EDT 2021", and "HA Status: Not Configured".

The main navigation bar is red and contains the text "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar is a dark grey menu with the following items: "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security" (expanded), "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database" (expanded), and "Control" (selected).

The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services". It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.201
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP/TLS Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

Enabled Disabled

DLG Port

TCP Port

5678

TSAPI Ports

TSAPI Service Port450

Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

Enabled Disabled

TR/87 Port4723

Enabled Disabled

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows a tree structure with "Maintenance" expanded, and "Service Controller" selected. The main content area, titled "Service Controller", contains a table of services and their statuses. The "TSAPI Service" is checked, and the "Restart Service" button is highlighted. Below the table, there is a link to "Status and Control" and a row of action buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, and Restart Web Server.

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Maintenance | Service Controller Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Date Time/NTP Server
Security Database
Service Controller
Server Data
Networking
Security
Status

Service Controller

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

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

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". A welcome message and system information are shown in the top right corner. The main navigation bar is red and contains links for "Security", "Security Database", and "Tlinks". The left sidebar shows a tree view of the application's structure, with "Security" expanded and "Tlinks" selected under "Security Database". The main content area shows the "Tlinks" screen with a list of Tlink names. Two Tlink names are listed: "AVAYA#CM7#CSTA#AES7" and "AVAYA#CM7#CSTA-S#AES7". The second Tlink name is selected with a radio button. A "Delete Tlink" button is visible below the list.

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:49:38 EDT 2021
HA Status: Not Configured

AVAYA Application Enablement Services
Management Console

Security | Security Database | Tlinks Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
Devices
Device Groups
Tlinks

Tlinks

Tlink Name

☐ AVAYA#CM7#CSTA#AES7
☒ AVAYA#CM7#CSTA-S#AES7

Delete Tlink

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**.

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates

Home | Help | Logout

CA Trusted Certificates

View Import Export Delete

Alias	Status	Issued To	Issued By	Expiration Date
<input type="radio"/> serverCertDefault	expired	aes7-081738682-labUseOnly	aes7-081738682-labUseOnly	Aug 5, 2020
<input type="radio"/> avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
<input type="radio"/> avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
<input checked="" type="radio"/> SystemManagerCA	valid	System Manager CA	System Manager CA	Oct 8, 2028

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

Welcome: User
Last login: Tue Sep 14 09:55:06 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 10:42:19 EDT 2021
HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates

Home | Help | Logout

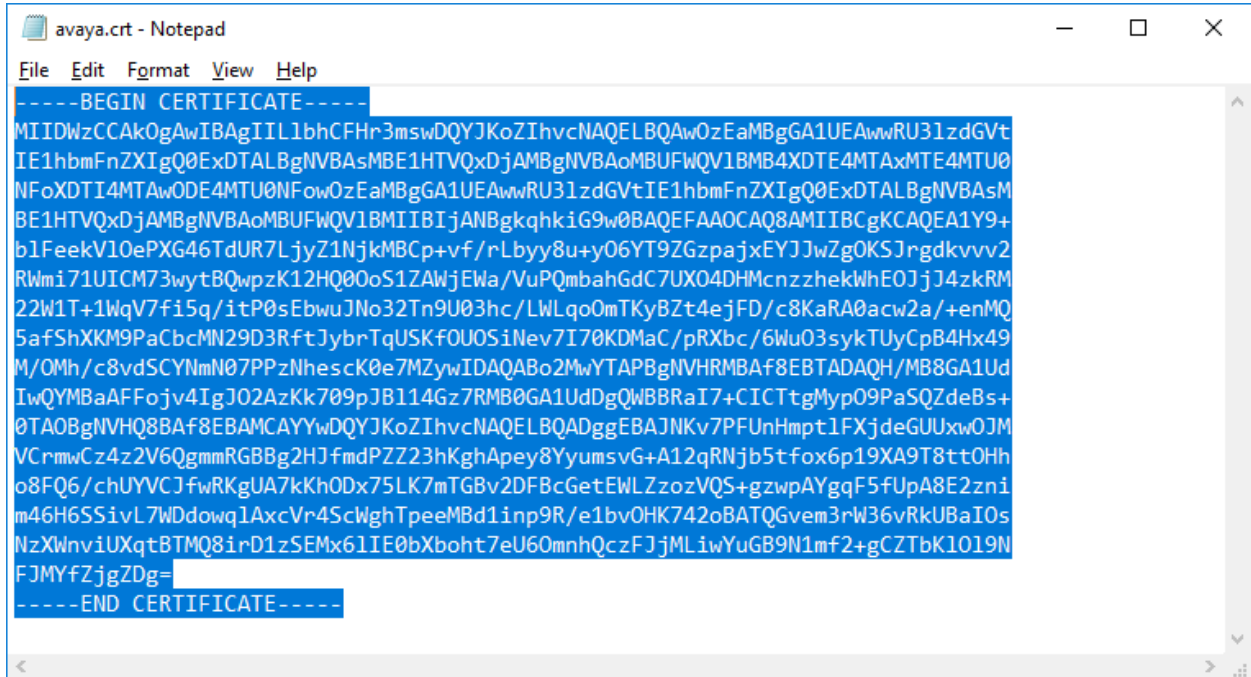
Trusted Certificate Export

Issued To: System Manager CA
Issued By: System Manager CA
Expiration Date: Oct 8, 2028

Certificate PEM:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILbHCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwRU3lzdG
IE1hbmFnZXIqQ0ExDTALBgNVBAsMBE1HTVQxZjAMBGMBAQMBUFQVIBMB4XDTE4MTA4MTE4
NfFoXDTI4MTA0ODE4MTU0NfowOzEaMBGGA1UEAwRU3lzdGVtIE1hbmFnZXIqQ0ExDTALBgNV
BE1HTVQxZjAMBGMBAQMBUFQVIBMB4XDTE4MTA4MTE4NfFoXDTI4MTA0ODE4MTU0NfowOzEa
blFeekVLOePXG46TdUR7LjyZ1NjkMBGp+vf/rLbyy8u+yO6YT9ZGzpjxYJwZgOKSjrgdkvvv2
RWmi71UICM73wyTBQwpzK12HQ00oS1ZAWjEwa/VuPQmbahGdC7UXO4DHMcnczhekWhEOJj4
22W1T+1WqV7R5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBzt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PpZnHesck0e7MZYwIDAQABo2MwYTABBgNVHRMBAF8EBTADAQH/MB8G
IwQYMBaAFFojv41gJO2AZKk709pJBl14Gz7RMB0GA1UdDgQWBBrA17+CICtTgMyp09PaSQZdeBs
DTA0BgNVHQ8BAf8EBAMCAAYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwC
VCrmwCz4z2V6qgmmRGBBg2HJfmdPZZ23hKghApey8YyumsVG+A12qRnjb5tfox6p19XA9T8ttO
```

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-----
MIIDWzCCAkOgAwIBAgIILlhbCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwRU31zdGVt
IE1hbmFnZXIqQ0ExDTALBgNVBAsMIBE1HTVQxDjAMBGA1UEAOMBUFWQV1BMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBGGA1UEAwRU31zdGVtIE1hbmFnZXIqQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBGA1UEAOMBUFWQV1BMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
b1FeekV10ePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+y06YT9ZGzpaJxYJjWZgOKSJrgdkvvv2
RWmi71UICM73wyTBQwpzK12HQ0o5S1ZAWjEwa/VuPQmbahGdC7UX04DHMczzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOU0SiNev7I70KDMaC/pRXbc/6Wu03sykTuyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJB114Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMyp09PaSQZdeBs+
0TA0BgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmpt1FXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOHh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzoZVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowq1AxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIOs
NzXWnvIUxqtBTMQ8irD1zSEMx61IE0bXboht7eU60mnhQczFJjMLiWYuGB9N1mf2+gCZTbK1019N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

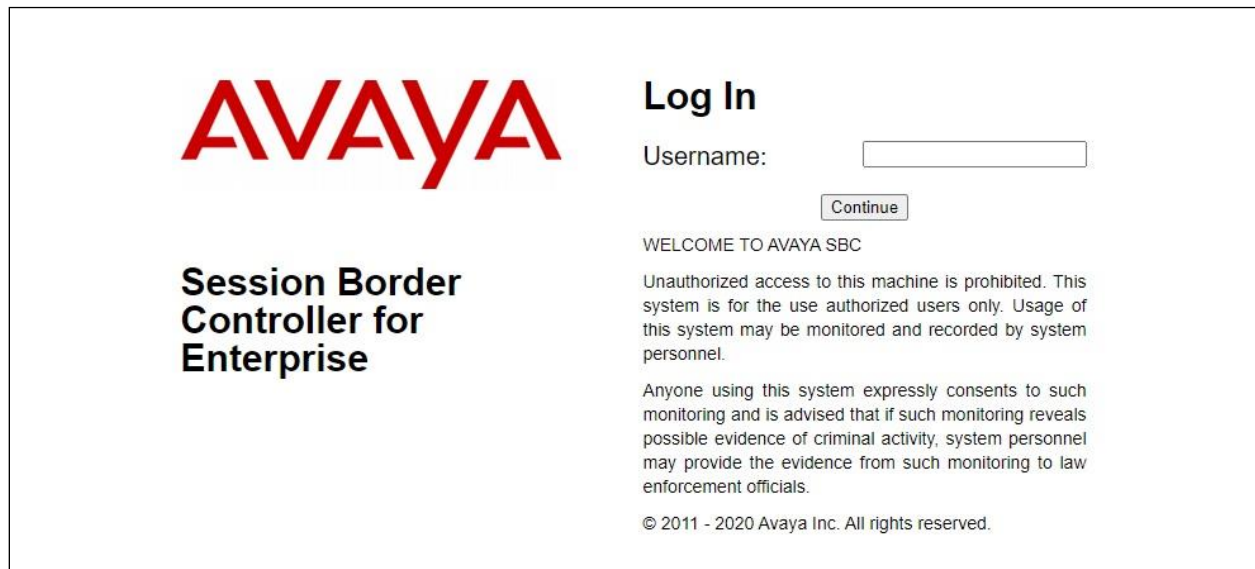

7. Configure Avaya Session Border Controller for Enterprise

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.



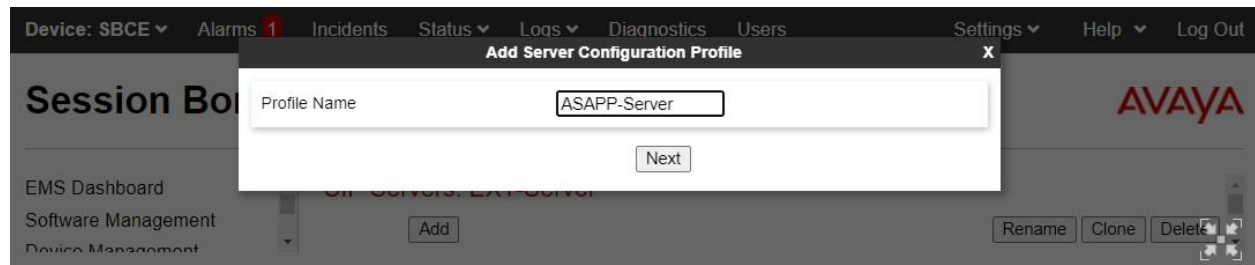
The image shows the login page of the Avaya Session Border Controller for Enterprise (SBCE) web interface. On the left, the Avaya logo is displayed in red, with the text "Session Border Controller for Enterprise" below it. On the right, under the heading "Log In", there is a "Username:" label followed by a text input field. Below the input field is a "Continue" button. Further down, a "WELCOME TO AVAYA SBC" message is shown, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." Below this is a consent statement: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2020 Avaya Inc. All rights reserved." is displayed.

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”

Edit SIP Server Profile - General

Server Type: Recording Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
	5060	TCP

Delete

Back Next

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

Add SIP Server Profile - Advanced

Enable Grooming: ☒

Interworking Profile: None

Signaling Manipulation Script: None

Securable: ☐

Enable FGDN: ☐

TCP Failover Port: 5060

TLS Failover Port: 5061

Tolerant: ☐

URI Group: None

Back Finish

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 screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration options, with "Routing" highlighted under the "Configuration Profiles" section. The main content area is titled "Routing Profiles: default" and features an "Add" button (highlighted with a red box) and a "Clone" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new profile instead." Below this, a "Routing Profile" pop-up window is displayed, containing a table with columns: Priority, URI Group, Time of Day, Load Balancing, Next Hop Address, and Transport. The table has one row with the following values: Priority 1, URI Group *, Time of Day default, Load Balancing DNS/SRV, Next Hop Address Auto-Detect, and Transport Auto-Detect. The "Add" button is also visible in the top right of the pop-up window.

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	*	default	DNS/SRV	Auto-Detect	Auto-Detect

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

The screenshot shows the "Routing Profile" pop-up screen. It features a text input field for "Profile Name" with the value "ASAPP-Route" entered. Below the input field is a "Next" button. The background shows the same SBCE web interface as the previous screenshot, with the "Routing Profiles: default" section visible.

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).

Routing Profile

URI Group

*

▼

Time of Day

default

▼

Load Balancing

Priority

▼

NAPTR

☐

Transport

None

▼

LDAP Routing

☐

LDAP Server Profile

None

▼

LDAP Base DN (Search)

None

▼

Matched Attribute Priority

☒

Alternate Routing

☒

Next Hop Priority

☒

Next Hop In-Dialog

☐

Ignore Route Header

☐

ENUM

☐

ENUM Suffix

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				ASAPP-Server		None	Delete

Back

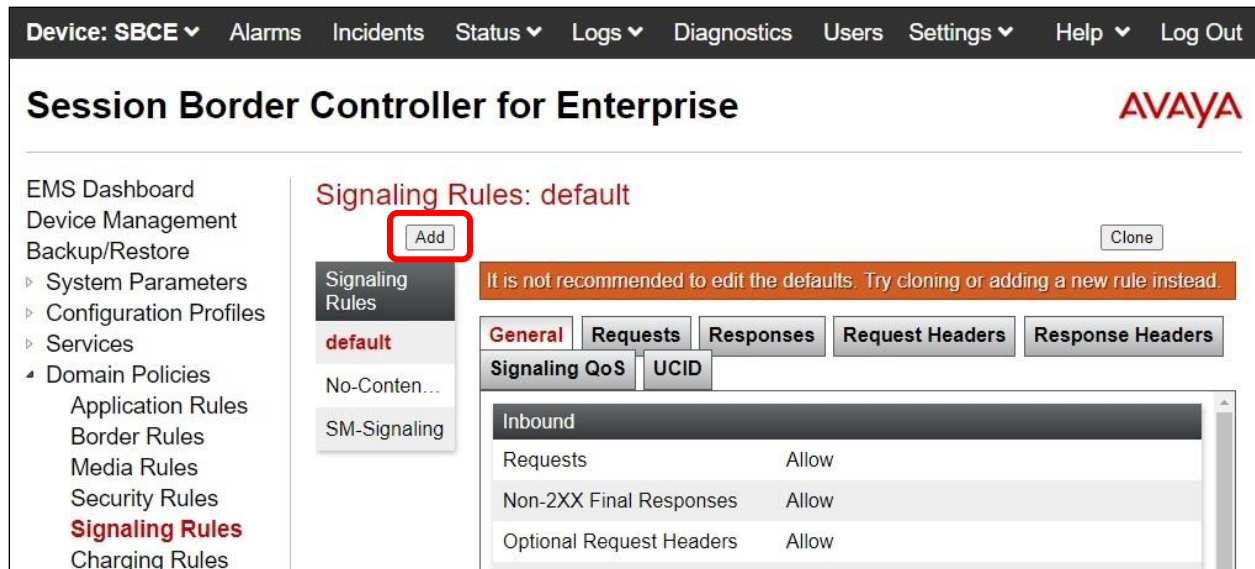
Finish

7.4. Administer Signaling Rules

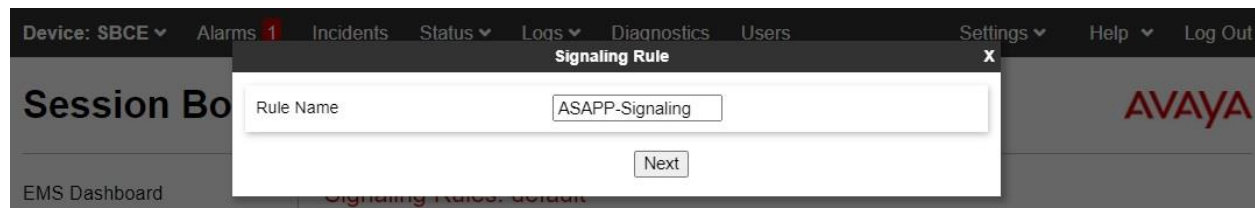
Select **Backup/Restore** → **Domain Policies** → **Signaling Rules** from the left pane to display existing signaling rules.

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.

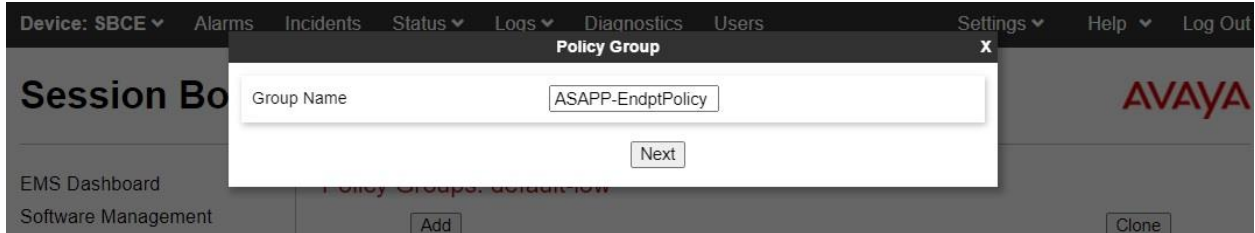
The screenshot shows the 'Controller for Enterprise' interface. The top navigation bar includes 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main title is 'Controller for Enterprise' with the AVAYA logo. Below the title, the section is 'Signaling Rules: SM-Signaling'. There are buttons for 'Add', 'Rename', 'Clone', and 'Delete'. A left sidebar lists 'Signaling Rules' with options: 'default', 'No-Content-Typ...', 'SM-Signaling' (highlighted), and 'Uniphore-signali...'. The main area has a blue bar with 'Click here to add a description.' Below this are tabs: 'General', 'Requests', 'Responses', 'Request Headers', 'Response Headers', 'Signaling QoS', and 'UCID' (selected). The 'UCID' tab shows a table with columns 'UCID', 'Node ID', and 'Protocol Discriminator'. The 'UCID' column has a checked checkbox. The 'Node ID' is '11' and the 'Protocol Discriminator' is '0x00'. There is an 'Edit' button at the bottom right of the table.

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 screenshot shows the 'Session Border Controller for Enterprise' interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main title is 'Session Border Controller for Enterprise' with the AVAYA logo. On the left, a sidebar lists various management options, with 'End Point Policy Groups' highlighted under 'Domain Policies'. The main area is titled 'Policy Groups: default-low'. There is an 'Add' button (highlighted with a red box) and a 'Clone' button. Below this is a blue bar with 'Hover over a row to see its description.' A table titled 'Policy Group' is shown with a 'Summary' button. The table has columns: 'Order', 'Application', 'Border', 'Media', 'Security', 'Signaling', 'Charging', and 'RTCP Mon Gen'. The first row shows '1', 'default', 'default', 'default-low-med', 'default-low', 'default', 'None', and 'Off'.

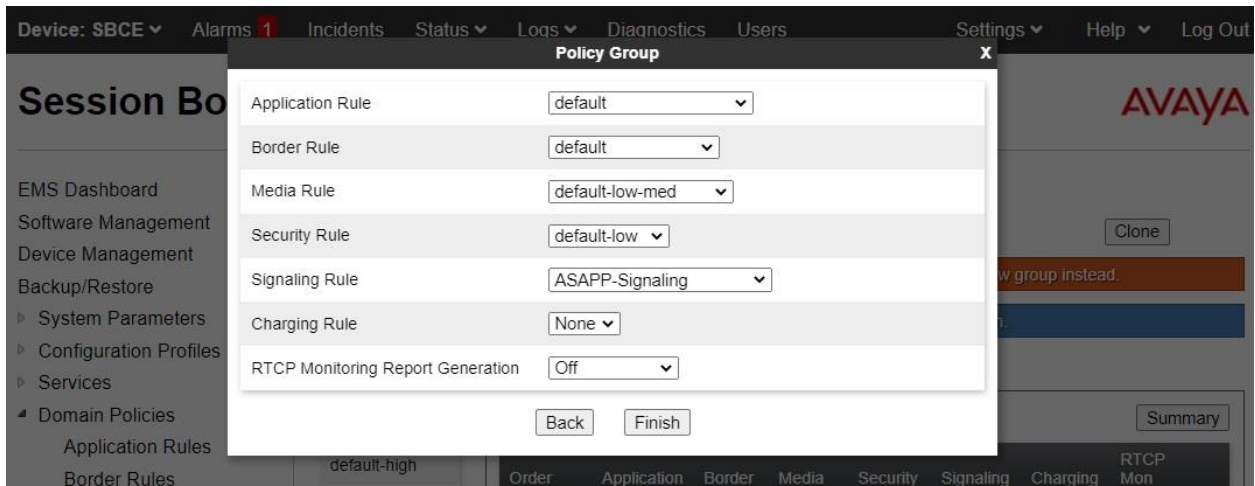
The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name** as shown below.



The screenshot shows the 'Policy Group' pop-up window. The 'Group Name' field is populated with 'ASAPP-EndptPolicy'. A 'Next' button is visible at the bottom right of the pop-up. The background shows the main interface with a sidebar menu and a top navigation bar.

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.



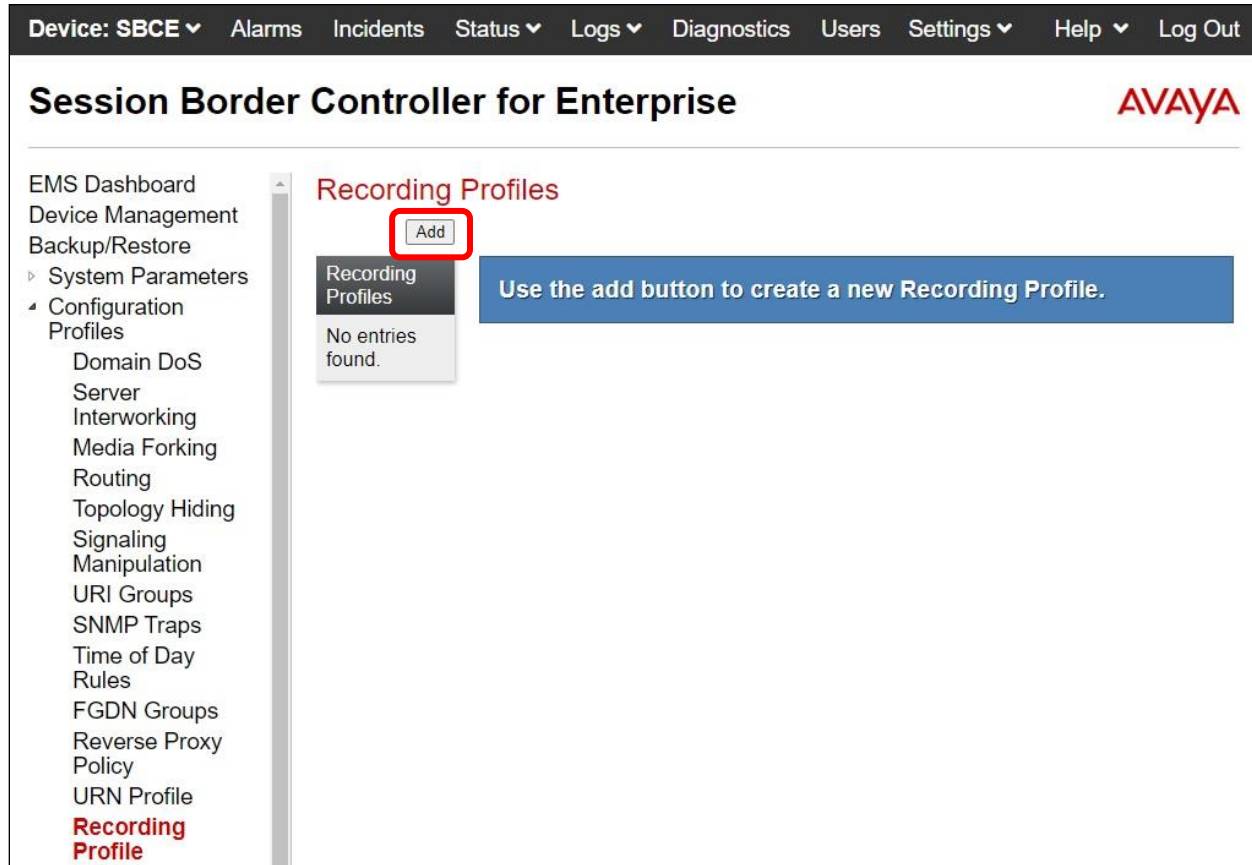
The screenshot shows the 'Policy Group' pop-up window with the following settings:

Field	Value
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	ASAPP-Signaling
Charging Rule	None
RTCP Monitoring Report Generation	Off

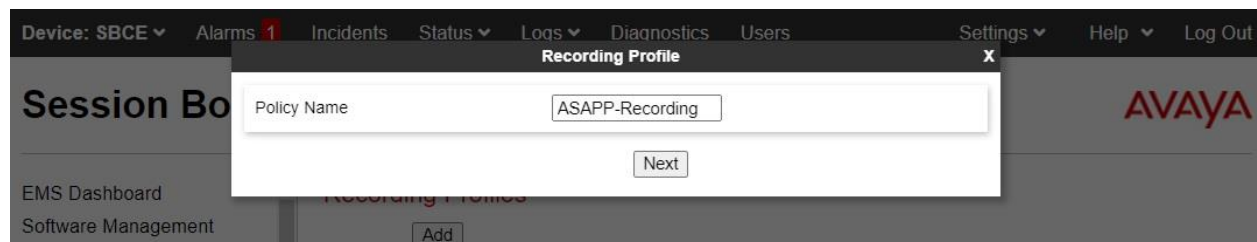
Buttons: Back, Finish, Summary

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”

The screenshot shows the 'Recording Profile' pop-up window. It has a title bar with 'Device: SBCE', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The window contains the following fields and controls:

- Call Termination on Recording Failure:** ☐
- Play Recording Tone:** ☐
- Add:** Button
- Routing Profile:** Dropdown menu with 'ASAPP-Route' selected.
- Recording Type:** Dropdown menu with 'Full Time' selected.
- Video Recording:** ☐
- Delete:** Button
- Back:** Button
- Finish:** Button

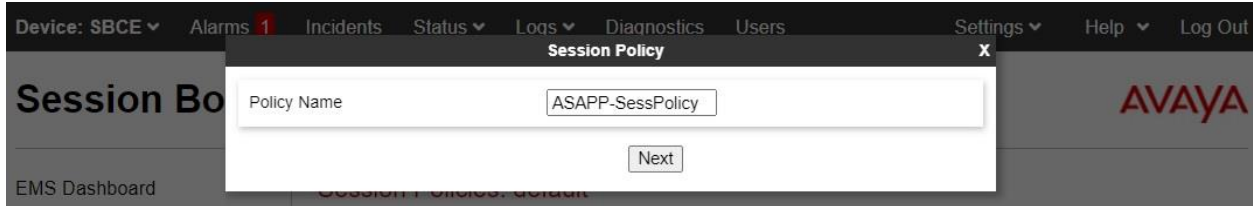
7.7. Administer Session Policies

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 screenshot shows the 'Session Policies: default' configuration page. The left pane shows the navigation menu with 'Session Policies' selected. The main area displays the 'default' policy with the following settings:

- Session Policies:** default
- Add:** Button (highlighted with a red box)
- Clone:** Button
- Warning:** It is not recommended to edit the defaults. Try cloning or adding a new policy instead.
- Media:** Tab selected
- URN Profile:** Tab
- Media Anchoring:** ☒
- Media Forking Profile:** None
- Converged Conferencing:** ☐
- Recording Server:** ☐
- Media Server:** ☐
- Edit:** Button

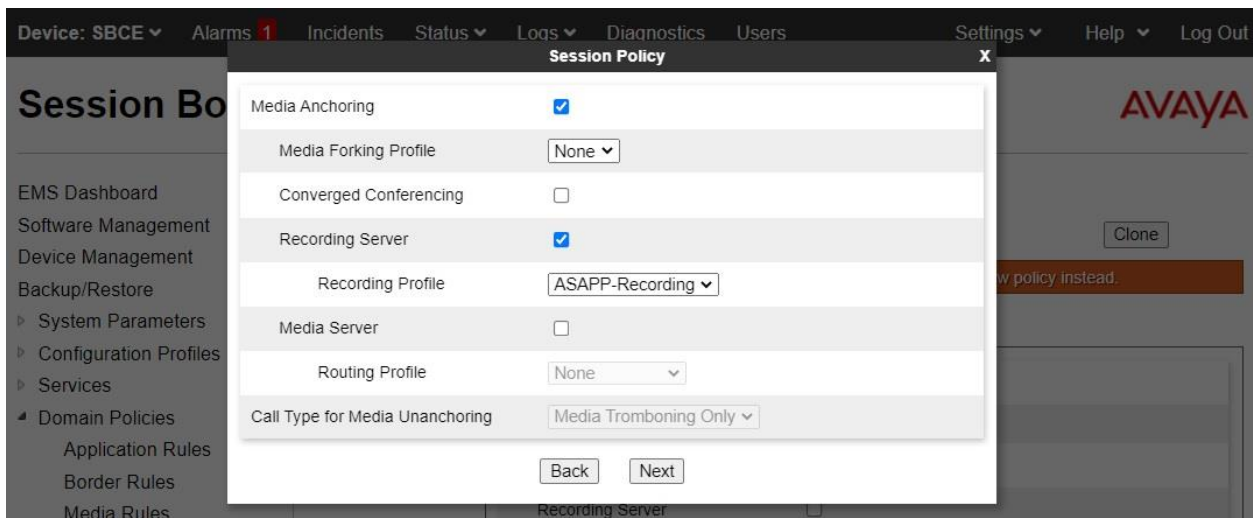
The **Session Policy** pop-up screen is displayed. Enter a desired **Policy Name** as shown below.



The screenshot shows the 'Session Policy' pop-up window. The 'Policy Name' field is populated with 'ASAPP-SessPolicy'. A 'Next' button is visible at the bottom right of the form. The background shows the Avaya EMS Dashboard with a navigation menu on the left and a top bar with 'Device: SBCE', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'.

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.

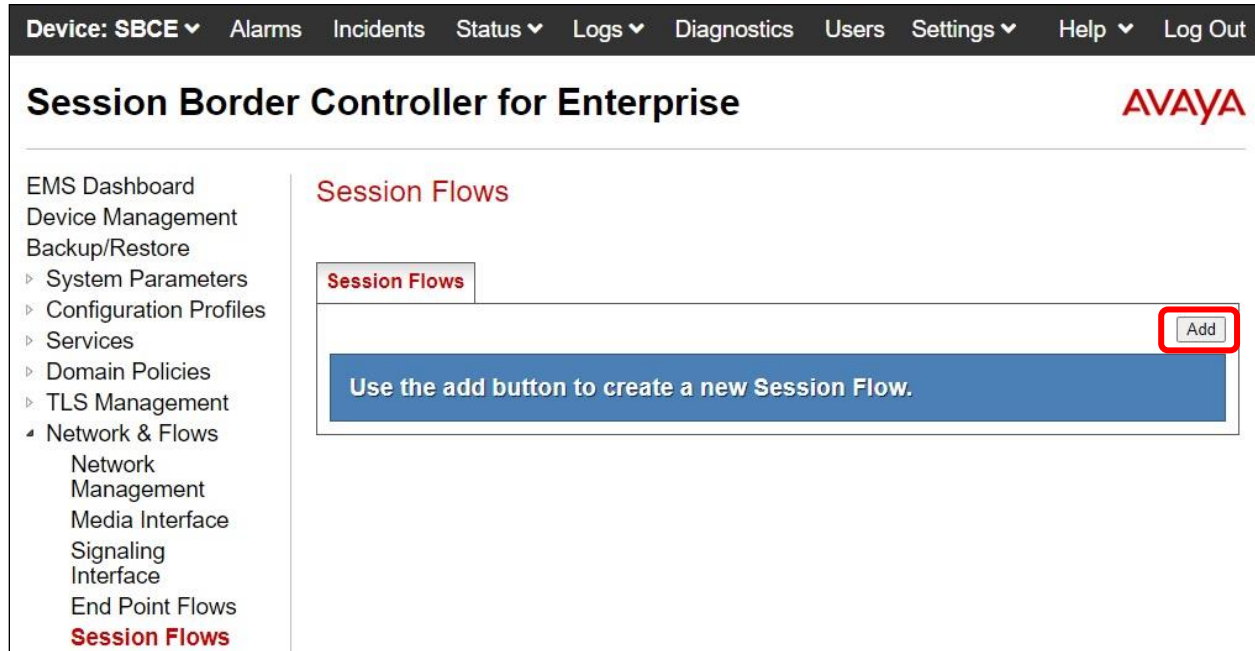
- **Media Anchoring:** Check this field.
- **Recording Server:** Check this field.
- **Recording Profile:** Select the ASAPP recording profile from **Section 7.6**.



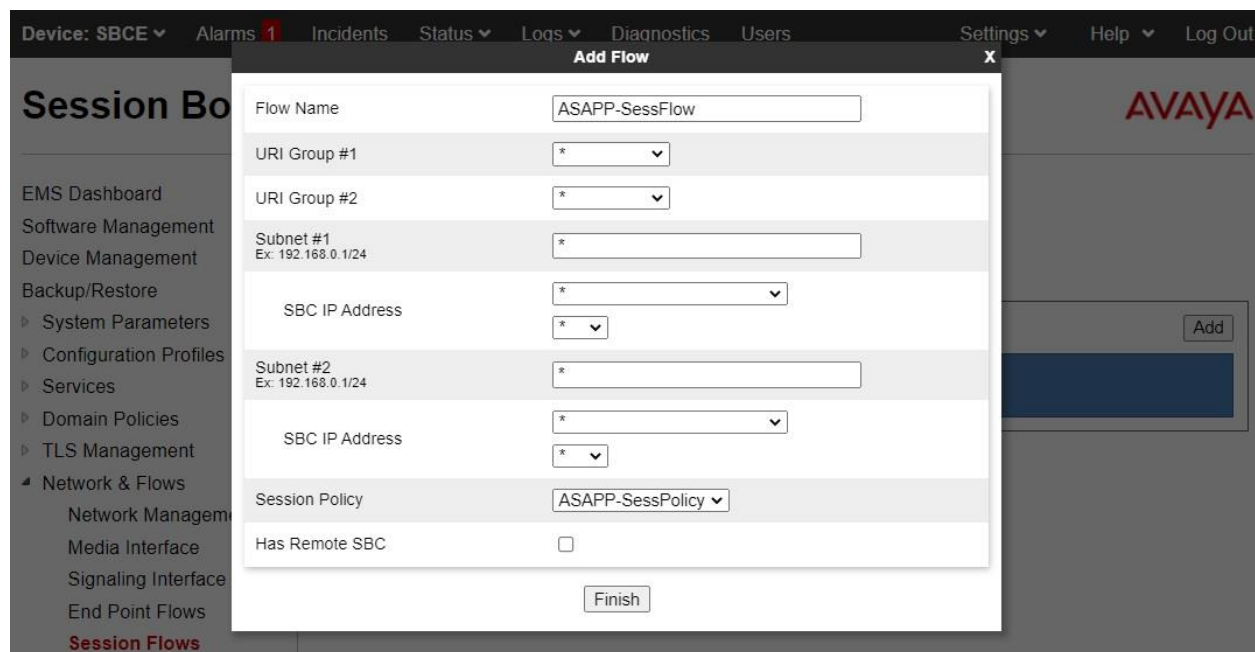
The screenshot shows the 'Session Policy' pop-up window with the following fields updated: 'Media Anchoring' is checked, 'Media Forking Profile' is set to 'None', 'Converged Conferencing' is unchecked, 'Recording Server' is checked, 'Recording Profile' is set to 'ASAPP-Recording', 'Media Server' is unchecked, 'Routing Profile' is set to 'None', and 'Call Type for Media Unanchoring' is set to 'Media Tromboning Only'. 'Back' and 'Next' buttons are at the bottom. The background shows the Avaya EMS Dashboard with a navigation menu on the left and a top bar with 'Device: SBCE', 'Alarms 1', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'.

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 screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. The left sidebar contains a navigation menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. Under Network & Flows, the End Point Flows option is highlighted. The main content area is titled 'End Point Flows' and features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, and an 'Add' button is highlighted with a red box. Below the tabs, a message states: 'Modifications made to a Server Flow will only take effect on new sessions.' A blue bar indicates 'Hover over a row to see its description.' The interface shows two sections for SIP Servers: 'EXT-server' and 'SM-server'. Each section contains a table with columns for Priority, Flow Name, URI Group, Received Interface, Signaling Interface, End Point Policy Group, and Routing Profile. The 'EXT-server' table has one row with Priority 1, Flow Name EXT-Flow, URI Group *, Received Interface Private-Signaling, Signaling Interface Public-Signaling, End Point Policy Group default-low, and Routing Profile SM-Route. The 'SM-server' table has one row with Priority 1, Flow Name SM-Flow, URI Group *, Received Interface Public-Signaling, Signaling Interface Private-Signaling, End Point Policy Group default-low, and Routing Profile EXT-Route. Each row has links for View, Clone, Edit, and Delete.

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

Session Border Controller for Enterprise

AVAYA

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

End Point Flows

Subscriber Flows **Server Flows**

Add

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

Hover over a row to see its description.

SIP Server: EXT-server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	EXT-Flow	*	Private-Signaling	Public-Signaling	default-low	SM-Route	View Clone Edit Delete

SIP Server: SM-server

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	SM-Flow	*	Public-Signaling	Private-Signaling	default-low	EXT-Route	View Clone Edit Delete

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**.

The screenshot displays the Avaya Session Border Controller (SBCE) configuration interface. The top navigation bar includes tabs for Device: SBCE, Alarms (1), Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar shows a tree view of configuration options, with 'End Point Flows' highlighted under 'Network & Flows'. The main area shows the 'Add Flow' pop-up screen with the following fields and values:

Field	Value
Flow Name	ASAPP-Flow
SIP Server Profile	ASAPP-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public-Signaling
Signaling Interface	Private-Signaling
Media Interface	Private-Media
Secondary Media Interface	None
End Point Policy Group	ASAPP-EndptPolicy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>

The 'Finish' button is located at the bottom right of the pop-up screen.

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**”.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Sep 14 13:53:20 2021 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.0.0.25-0
Server Date and Time: Tue Sep 14 14:32:01 EDT 2021
HA Status: Not Configured

Status | Status and Control | TSAPI Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ Switch Conn Summary

▪ **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	cm7	1	Talking	Mon Aug 30 16:16:46 2021	Online	18	4	64	107	30

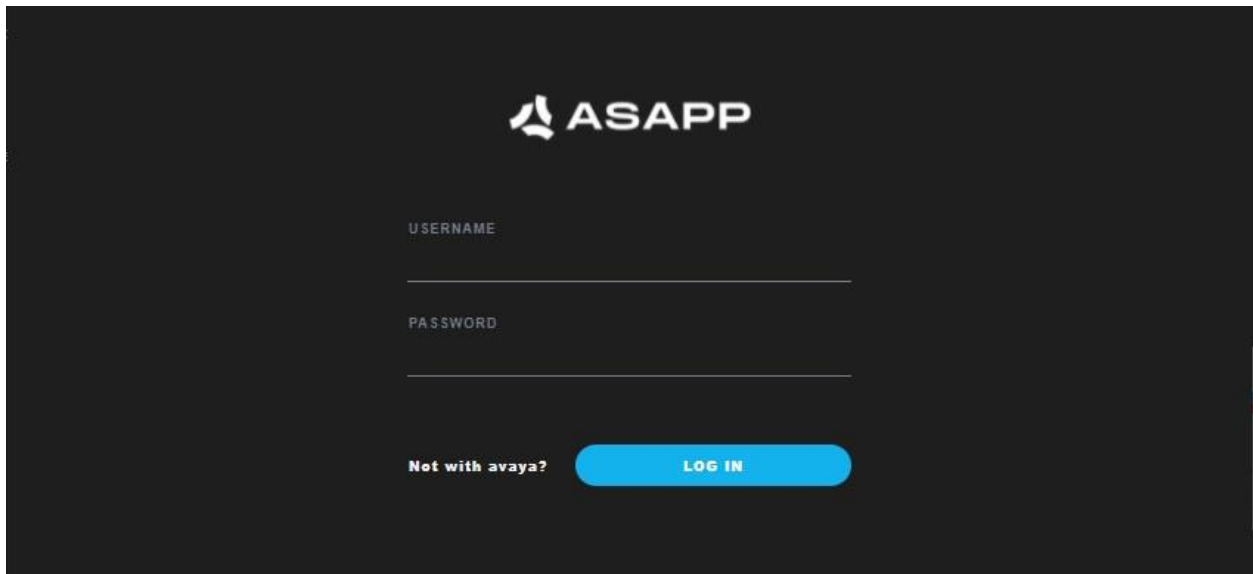
OnlineOffline

For service-wide information, choose one of the following:

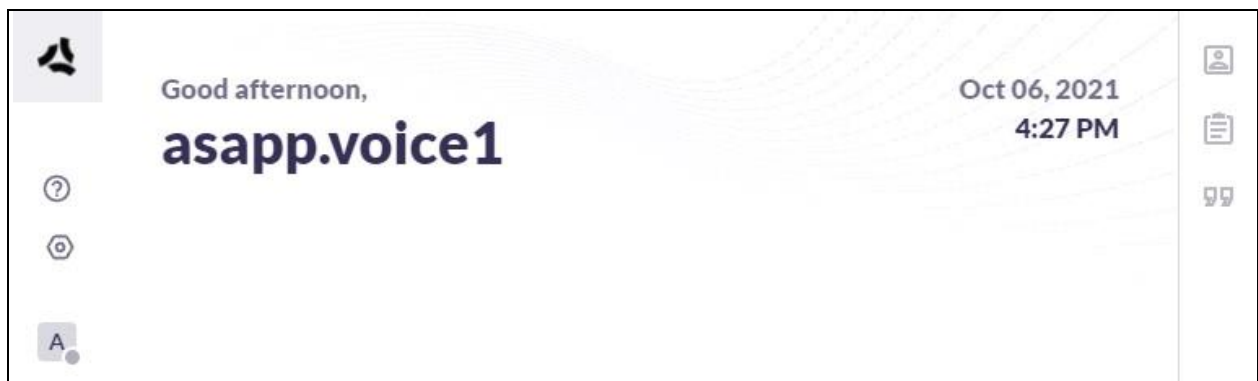
TSAPI Service StatusTLink StatusUser Status

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 image shows the ASAPP login interface. At the top center is the ASAPP logo, which consists of a stylized 'A' icon followed by the text 'ASAPP'. Below the logo are two input fields: the first is labeled 'USERNAME' and the second is labeled 'PASSWORD'. Both fields are empty. At the bottom left, there is a link that says 'Not with avaya?'. To the right of this link is a blue button with the text 'LOG IN' in white capital letters.

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.

The screenshot displays a customer service interface. At the top, a header bar shows a customer icon, the name "Customer", a red status indicator, and the ID "2500001". Below this, a secondary bar indicates the "Issue: 13035360001" and a duration of "00:52". The main chat area contains a series of messages:

- A** asapp.voice1 01:17:26 PM: Hello, this is agent, Alice? How may I help you today?
- C** Customer 01:17:32 PM: Hi, Alice, this is the customer, I'd like to check on my account balance?
- C** Customer 01:17:40 PM: What is
- A** asapp.voice1 01:17:41 PM: Hi, Mr customer, I'd be happy to happy to help you with your account balance? What is your 5 digit account number?
- C** Customer 01:17:47 PM: 36925.
- A** asapp.voice1 01:17:55 PM: The current balance is \$41.78. Is there anything else I can help you with?
- C** Customer 01:17:58 PM: Nope, that was it. Thanks.
- A** asapp.voice1 01:18:00 PM: Bye.

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.

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.