Application Notes for Uniphore Real Intent 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 Uniphore Real Intent 2.2 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Application Enablement Services 8.1.

Uniphore Real Intent is an audio capture application that uses the Telephony Services 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 can be made available to agents as transcriptions and are used by Uniphore Real Intent to automate call summary and disposition.

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 Uniphore Real Intent 2.2 with Avaya Session Border Controller for Enterprise 8.1 and Avaya Aura® Application Enablement Services 8.1.

Real Intent is an audio capture application that uses the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor skill groups and agent stations, and the SIP-based Media Recording (SIPREC) interface from Session Border Controller for Enterprise (SBCE) to capture media for calls between agents and the PSTN. The captured media can be made available to agents as transcriptions and are used by Uniphore Real Intent to automate call summary and disposition.

The Real Intent solution consists of multiple components distributed across multiple servers, including the Logger component as the audio capture engine. In the compliance testing, the Logger component consisted of two servers– one Linux server running the OrkWeb and OrkAudio components, and a Windows server running the OrkAvayaTSAPI component along with the Avaya TSAPI Windows Client. The OrkAudio component is responsible for SIPREC connection with SBCE, and the OrkAvayaTSAPI component is responsible for TSAPI connection with Application Enablement Services.

When there is an active ACD call at the agent station, Real Intent is informed of the call via TSAPI events and starts the transcription with captured media from the SIPREC interface. The TSAPI events are also used to determine when to stop the transcription, and the captured media are analyzed by Real Intent. At the end of the ACD call, Real Intent stops the transcription and presents an auto generated summary and disposition to the agent based on the call conversation.

The compliance testing covered inbound ACD calls that are delivered to agents and a couple of outbound calls manually dialed by agent to the PSTN. The compliance testing scope did not include outbound calls as part of any outbound application.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Real Intent application, the application automatically established TSAPI 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 Ethernet connection to Real Intent.

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 Real Intent and Avaya products did not include use of any specific encryption features as requested by Uniphore.

2.1. Interoperability Compliance Testing

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

- Use of TSAPI in areas of event notification and value queries.
- Use of SIPREC to capture media from SBCE.
- Proper transcription and disposition handling 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 Real Intent to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to Real Intent.

2.2. Test Results

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

- The tested Real Intent release 2.2.1.1 assumes fixed station extension association for each agent user and did not allow for changes. Support for variable station extensions is available in subsequent Real Intent release 2.3 but was not verified as part of this compliance test.

- The application requires agents to use the manual-in work mode, so that there is time to process the auto generated call summary and disposition prior to delivery of next ACD call.

- In the compliance testing, transcription for each call started appearing ~15 seconds into the call with varied accuracy on the transcriptions. Uniphore shared that the transcription delay can vary depending on customer environments, and that the accuracy experienced in the compliance testing represents baseline accuracy for out of the box. The accuracy can be enhanced in customer deployments by training models with domain specific data.

- The current release does not support non-monitored stations as transferred-to and conference-to destinations.

- By design, after the conference-from agent completes the conference action to add in the conference-to agent with three-way conversation, the transcription ceased at the conference-from agent and continued at the conference-to agent. At this point, should the conference-to agent drop from the three-way conversation first, then the transcription still continued at the conference-to agent screen until the call is dropped by the remaining parties or until the next ACD call is delivered to the conference-to agent.

- After recovery from a 60 seconds disruption to the Real Intent server, the time indication on the agent screens started incrementing at twice the speed. The workaround to fix the clock increment speed is for agents to log out of Real Intent and then log back in.

- After recovery from a 60 seconds disruption to the agent desktop, transcription for subsequent ACD calls were no longer reflected. Similarly, the workaround is for the agent to log out of Real Intent and then log back in.

- In the tested Real Intent release 2.2.1.1, after a server outage, the NLP service required a manual start. Support for auto start of the NLP service is available in subsequent Real Intent release 2.3 but was not verified as part of this compliance test.

2.3. Support

Technical support on Real Intent can be obtained through the following:

- **Email :** support@uniphore.com
- **Web :** https://www.uniphore.com/contact

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, Uniphore monitored the skill groups and agent stations shown in the table below.

Device Type	Extension
Skill Group	61001, 61002
Agent Station	65001 (H.323), 66002 (SIP)

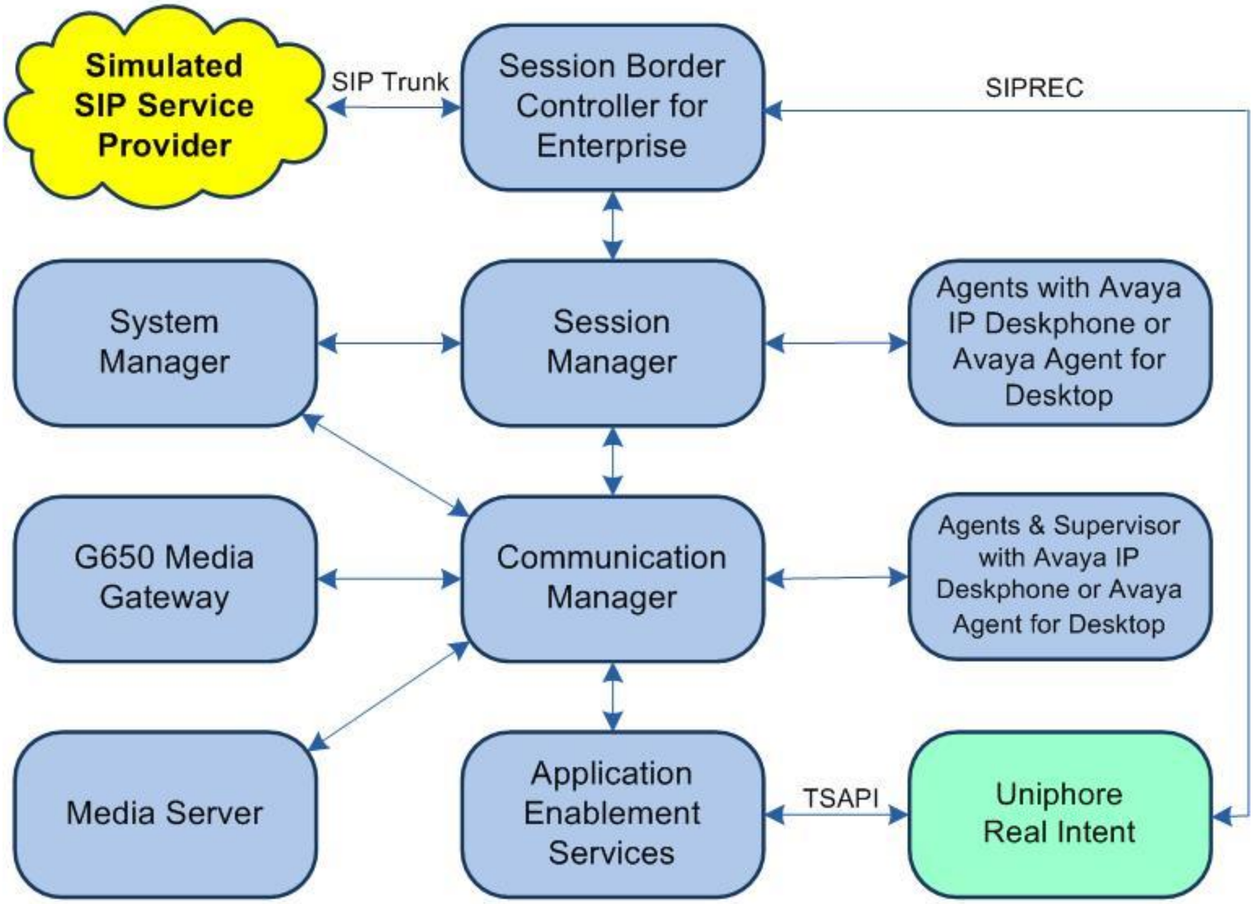

Simulated SIP Service Provider
SIP Trunk
Session Border Controller for Enterprise
SIPREC
System Manager
Session Manager
Agents with Avaya IP Deskphone or Avaya Agent for Desktop
G650 Media Gateway
Communication Manager
Agents & Supervisor with Avaya IP Deskphone or Avaya Agent for Desktop
Media Server
Application Enablement Services
TSAPI
Uniphore Real Intent

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	8.0.2.138
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 & SIP)	2.0.6.0.10
Avaya 9611G & J179 IP Deskphone (H.323)	6.8502
Avaya J169 IP Deskphone (SIP)	4.0.7.1.5
Uniphore Real Intent on CentOS Linux • UI • User Management Service • Audio Receiver • PostgreSQL • Apache Kafka • Nuance Transcription Service • Mongo Database	2.2.1.1 7.9.2009 2.2.1.1 2.2.1.1 2.2.1.1 11.1 2.4.1 4.7 4.2.1.1
Uniphore Logger with components on CentOS Linux & Microsoft Windows Server • OrkWeb • OrkAudio • OrkAvayaTSAPI • Avaya TSAPI Windows Client (csta32.dll)	NA 7.9.2009 & 2016 Standard 2.70 2.85 x8553 6.3.3.103

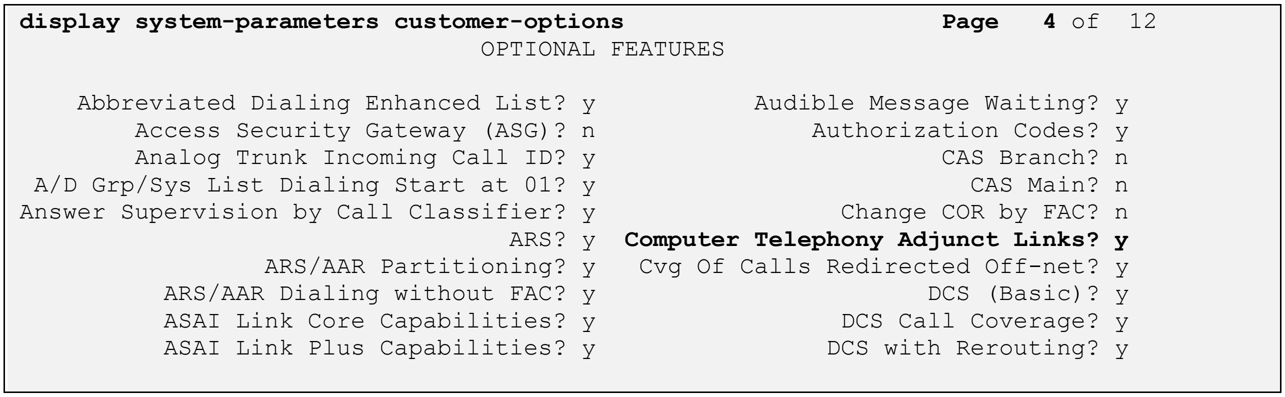
5. Configure Avaya Aura® Communication Manager

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

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

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.

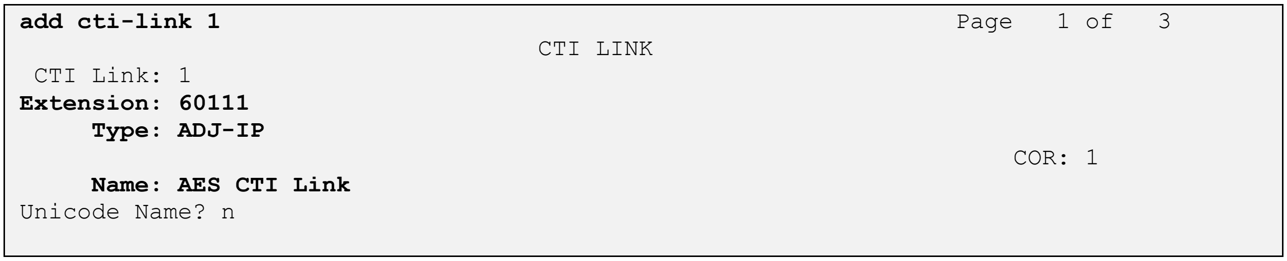


```
display system-parameters customer-options                      Page   4 of  12
                                OPTIONAL FEATURES

    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.

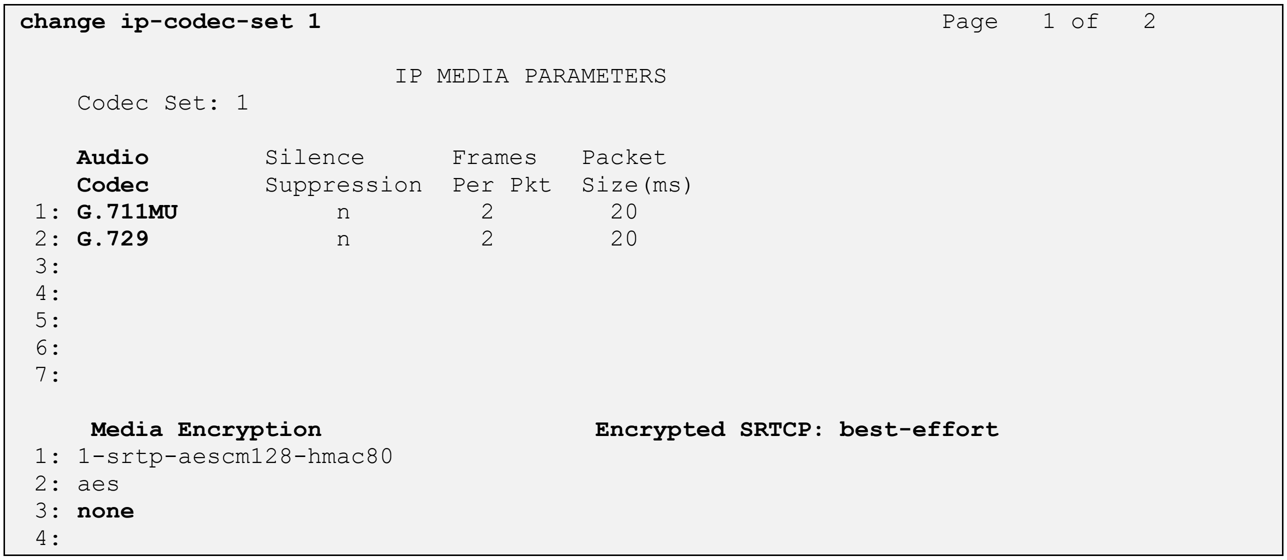
Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
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 Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used by the agent stations. For **Audio Codec**, make certain only variants of G711 and/or G729 codec are configured, as shown below. Note that Uniphore supports the G711 and G729 codec variants.



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

                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.729             n         2        20
 3:
 4:
 5:
 6:
 7:

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

5.4. 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 Uniphore.

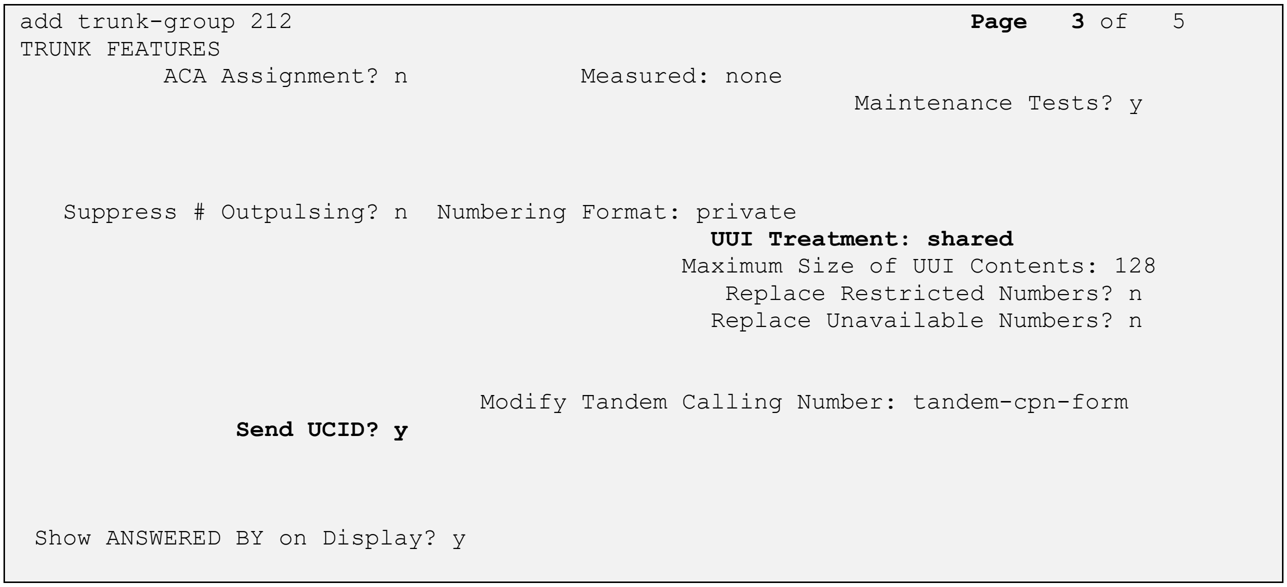
```
change system-parameters features                               Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
            Callr-info Display Timer (sec): 10
                          Clear Callr-info: next-call
         Allow Ringer-off with 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
```

5.5. 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 outbound calls to 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


                                Modify Tandem Calling Number: tandem-cpn-form
               Send UCID? y



 Show ANSWERED BY on Display? y
```

6. Configure Avaya Aura® Application Enablement Services

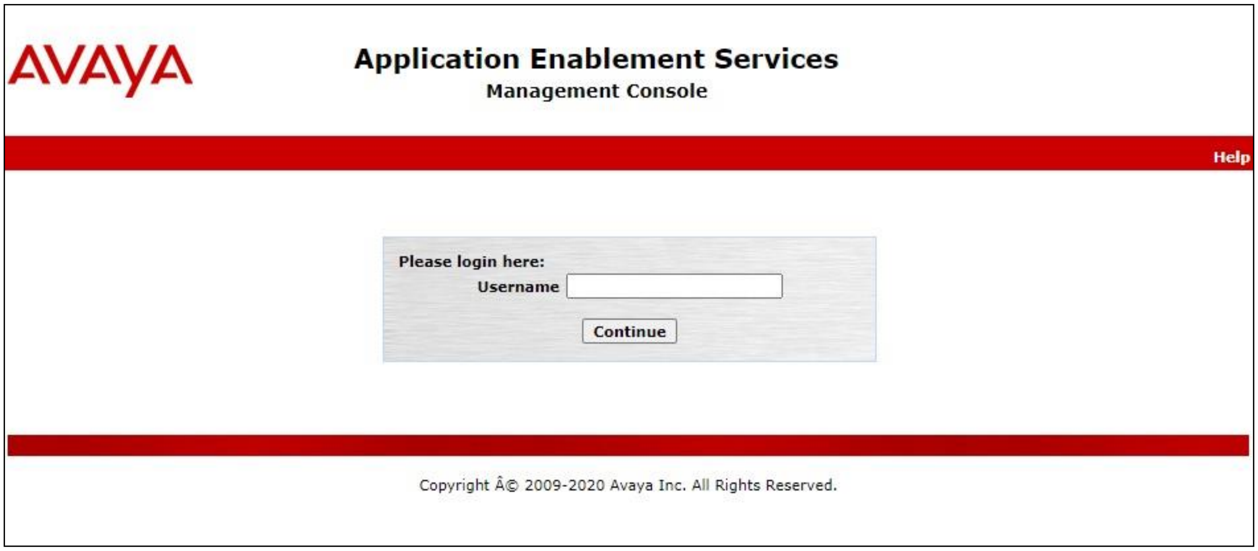
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer Uniphore user
- Administer security database
- Restart service
- Obtain Tlink name

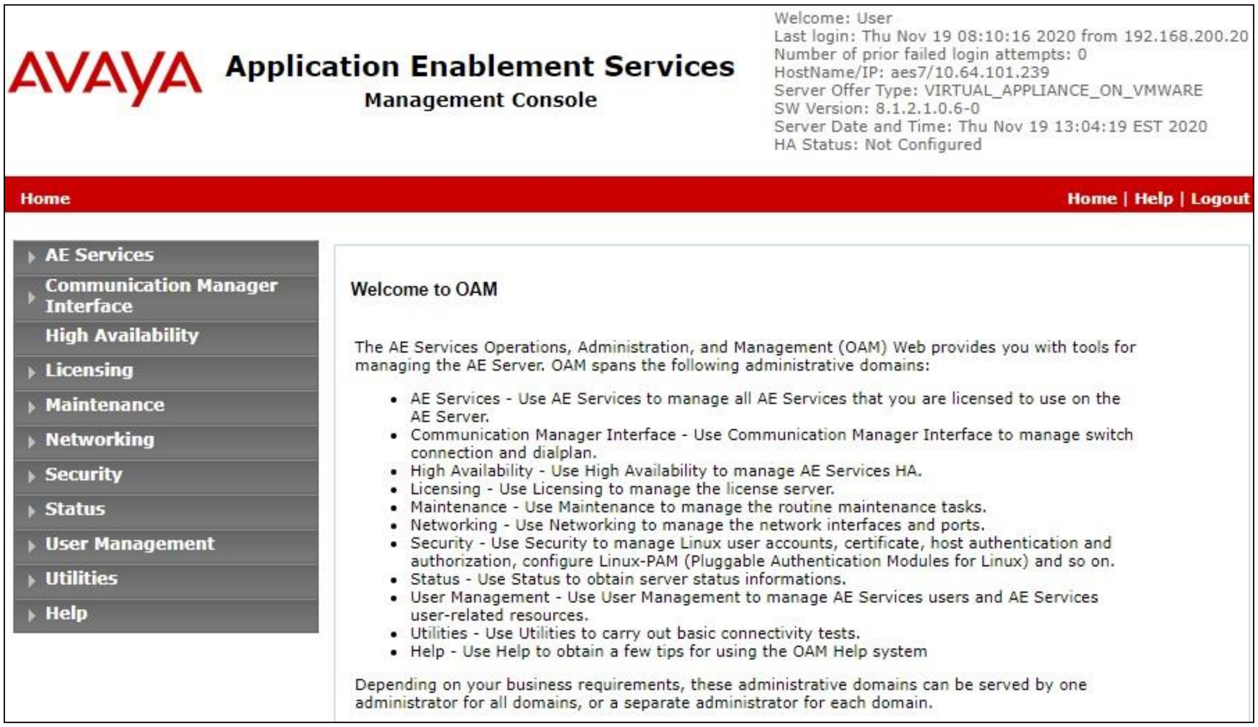
6.1. Launch OAM Interface

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.


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Continue
Copyright Â© 2009-2020 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:04:19 EST 2020
HA Status: Not Configured

Welcome to OAM

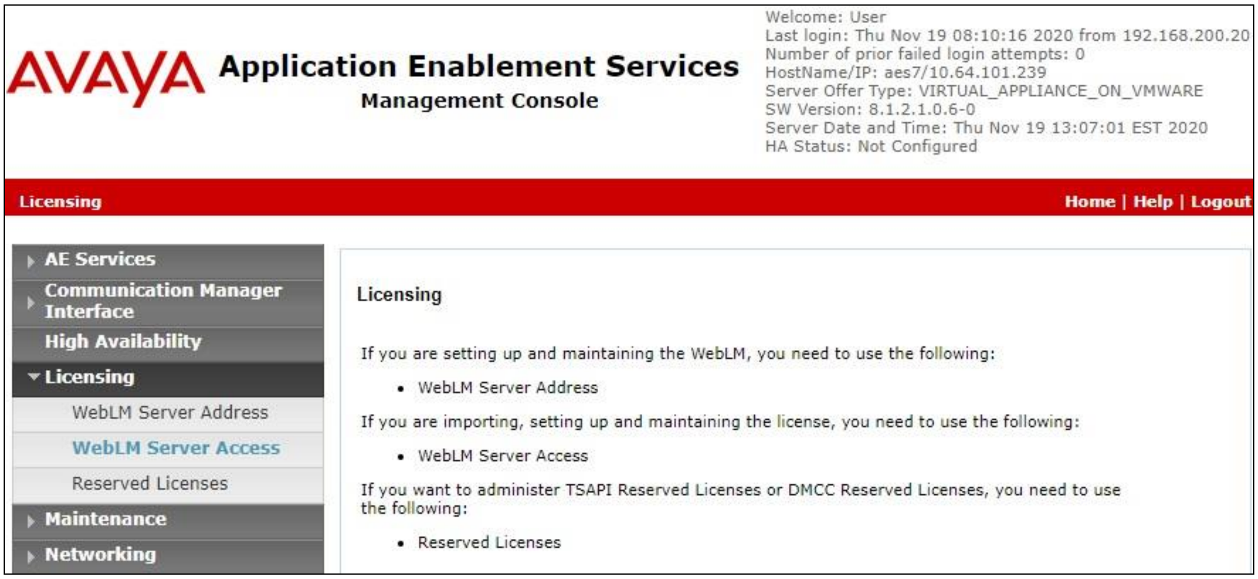
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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).



Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:07:01 EST 2020
HA Status: Not Configured

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:

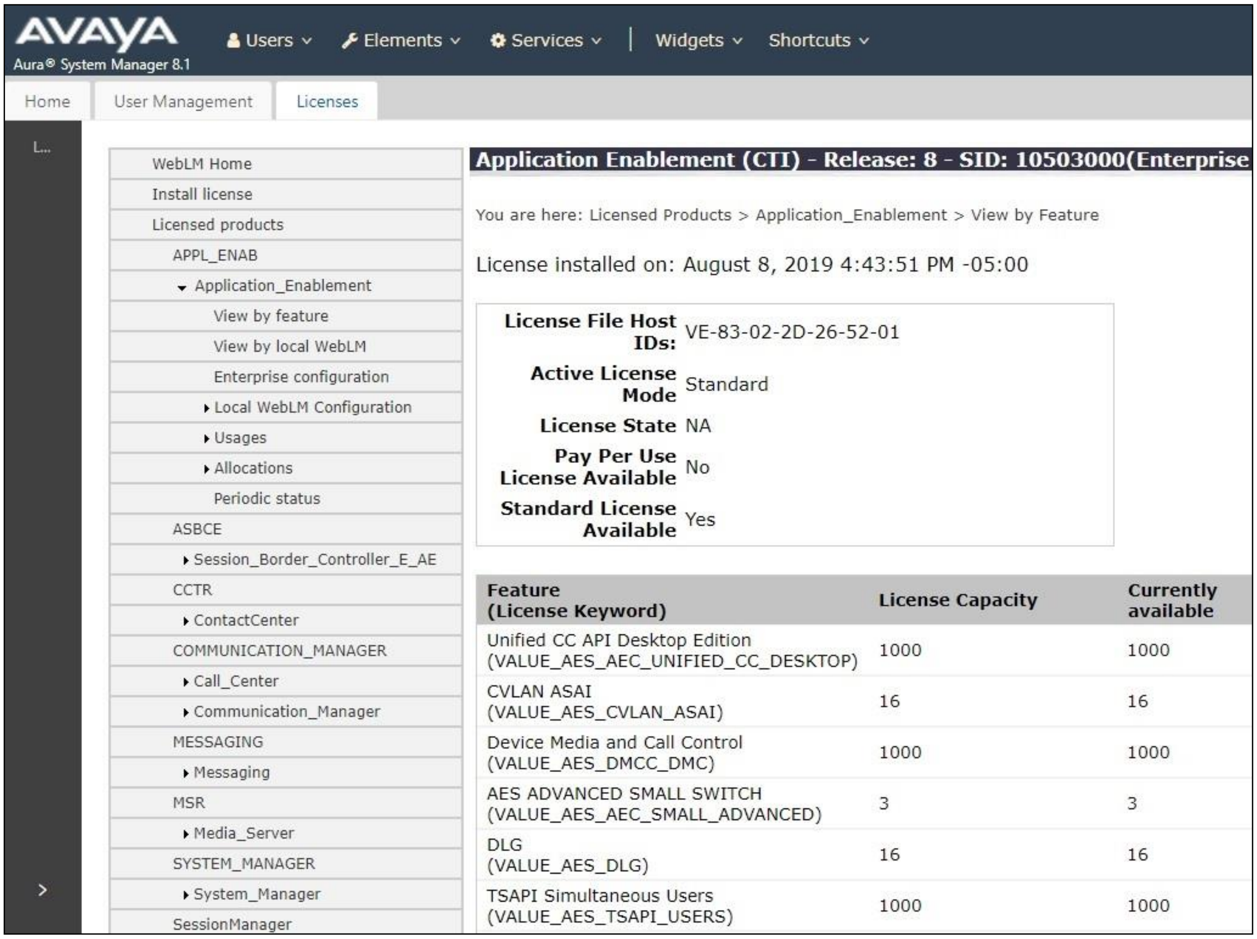
- WebLM Server Access

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.



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

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

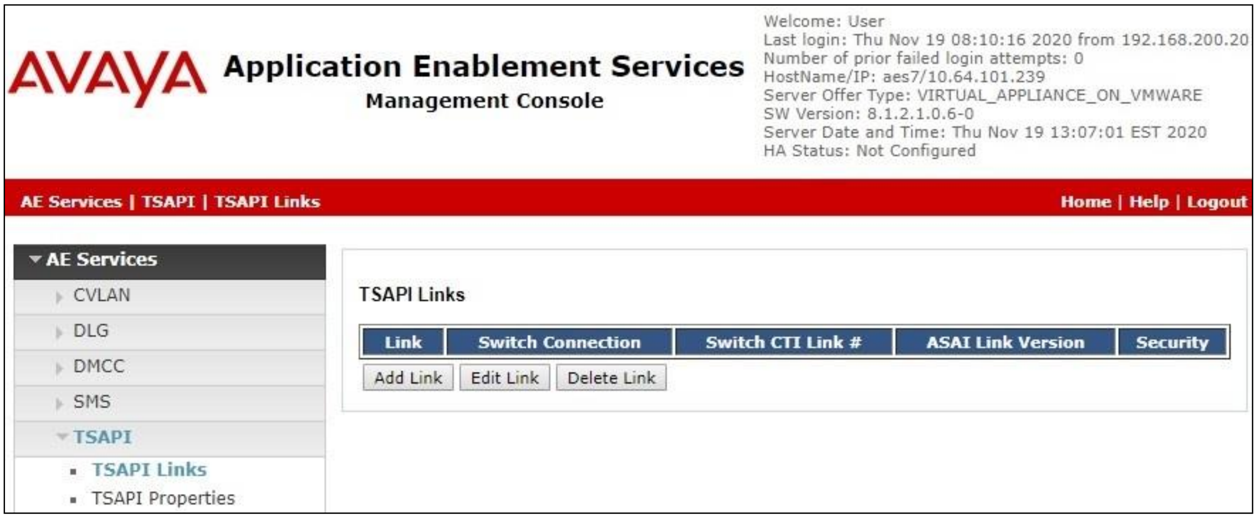
License installed on: August 8, 2019 4:43:51 PM -05:00

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**.



Application Enablement Services
Management Console

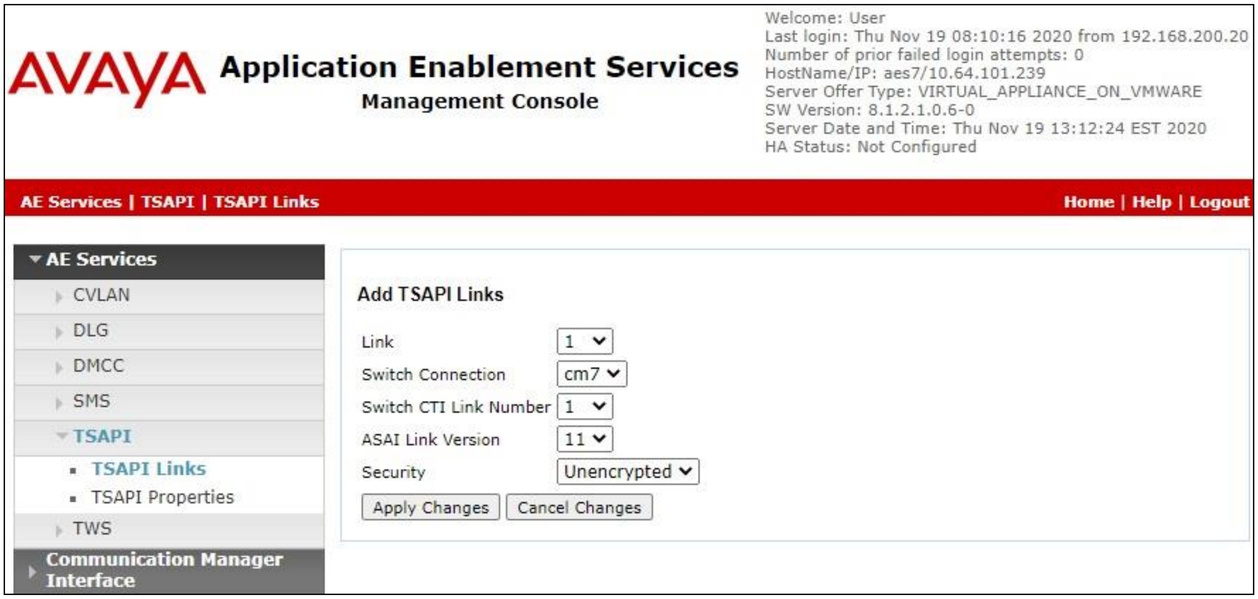
Welcome: User
Last login: Thu Nov 19 08:10:16 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:07:01 EST 2020
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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, the existing switch connection "cm7" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



Application Enablement Services
Management Console

Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:12:24 EST 2020
HA Status: Not Configured

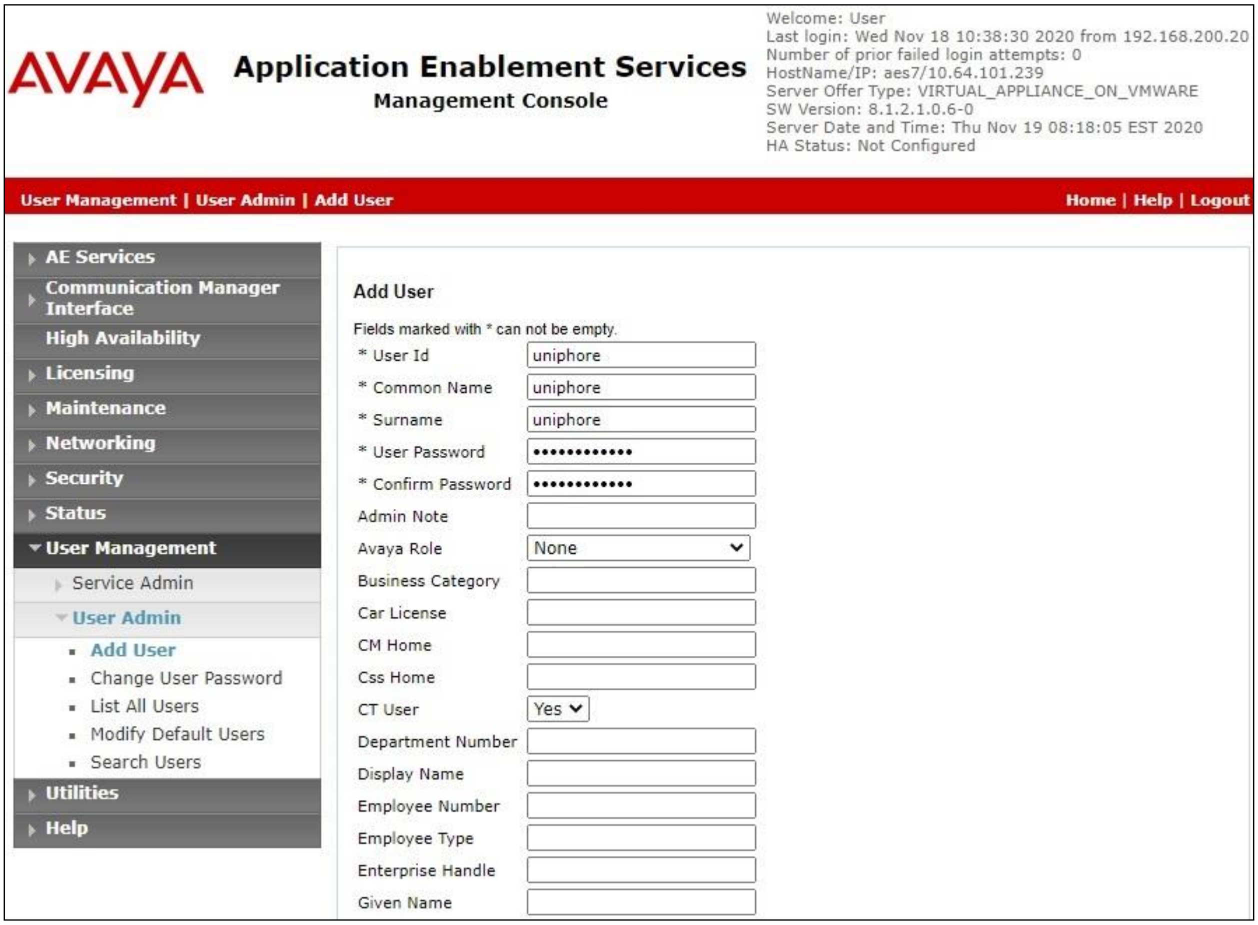
Add TSAPI Links

Link: 1
Switch Connection: cm7
Switch CTI Link Number: 1
ASAI Link Version: 11
Security: Unencrypted

6.4. Administer Uniphore 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.



Welcome: User
Last login: Wed Nov 18 10:38:30 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 08:18:05 EST 2020
HA Status: Not Configured

Add User

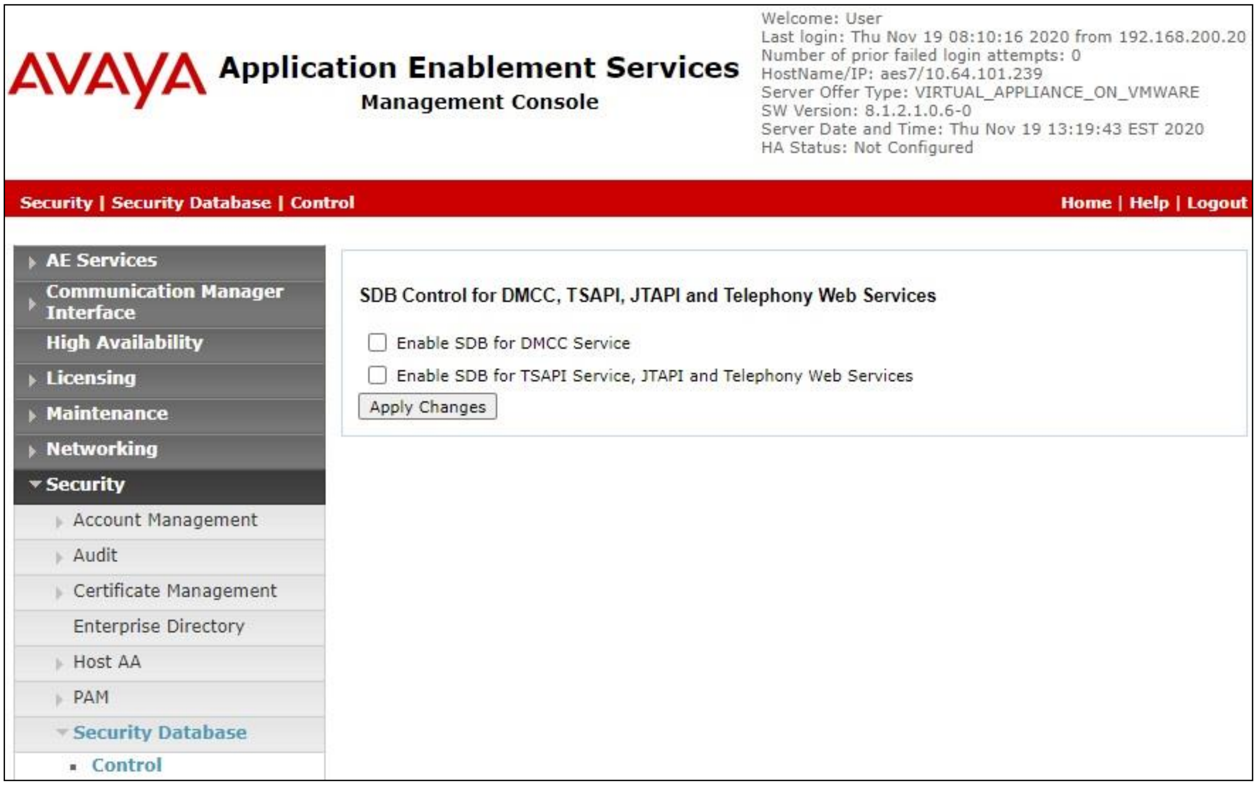
Fields marked with * can not be empty.

* User Id	uniphore
* Common Name	uniphore
* Surname	uniphore
* User Password	••••••••••••
* Confirm Password	••••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	

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 Uniphore user from **Section 6.4**.



Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:19:43 EST 2020
HA Status: Not Configured

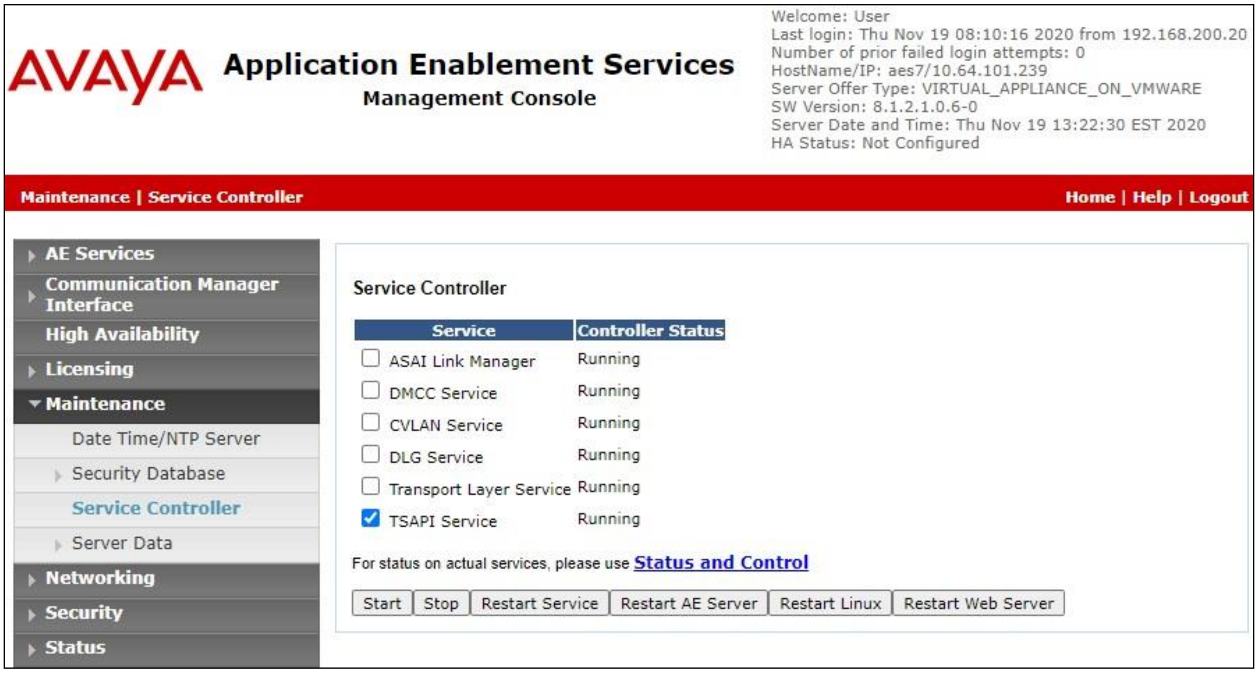
SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. 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**.



Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:22:30 EST 2020
HA Status: Not Configured

Service Controller

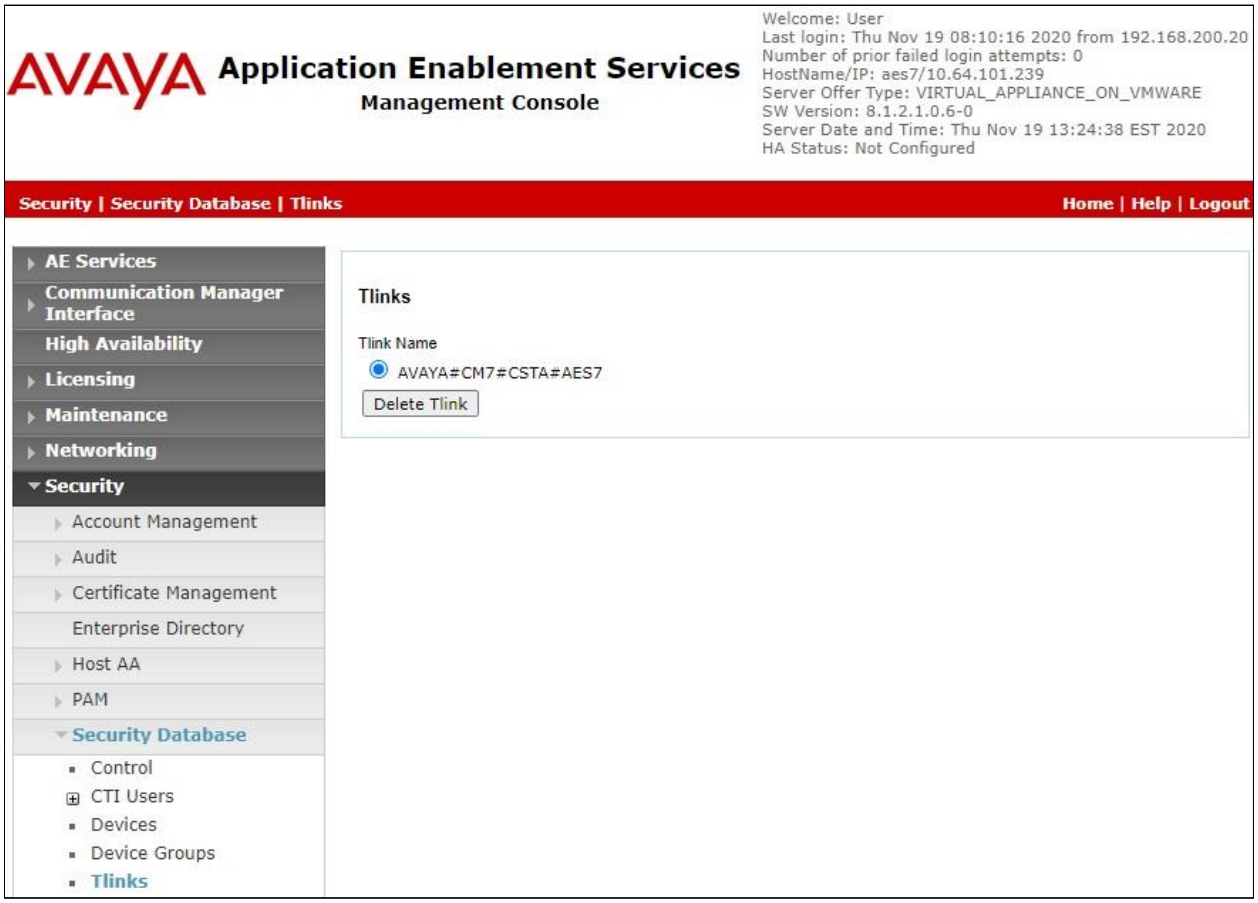
Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.7. 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 associated Tlink name, to be used later for configuring Uniphore.

In this case, the associated Tlink name is “AVAYA#CM7#CSTA#AES7”. Note the use of the switch connection “CM7” from **Section 6.3** as part of the Tlink name.



Welcome: User
Last login: Thu Nov 19 08:10:16 2020 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: 8.1.2.1.0.6-0
Server Date and Time: Thu Nov 19 13:24:38 EST 2020
HA Status: Not Configured

Tlinks

Tlink Name

● AVAYA#CM7#CSTA#AES7

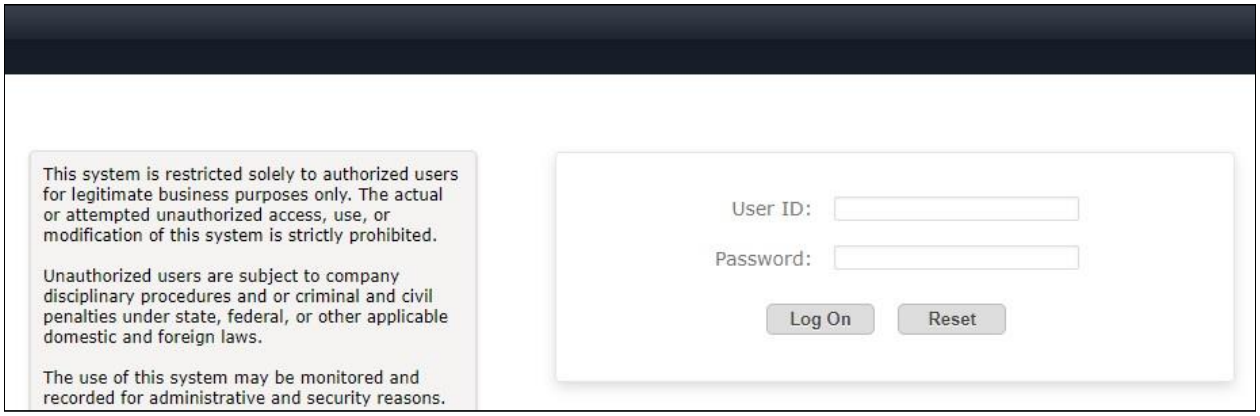
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

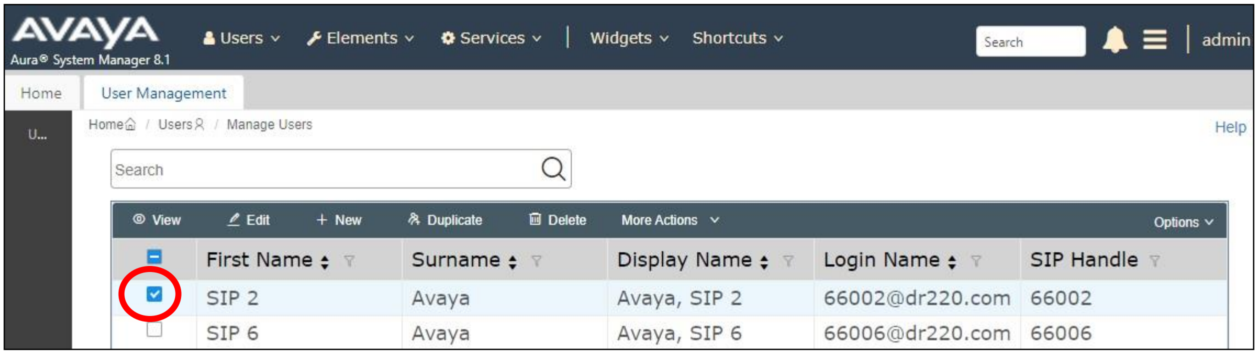
User ID:

Password:

7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

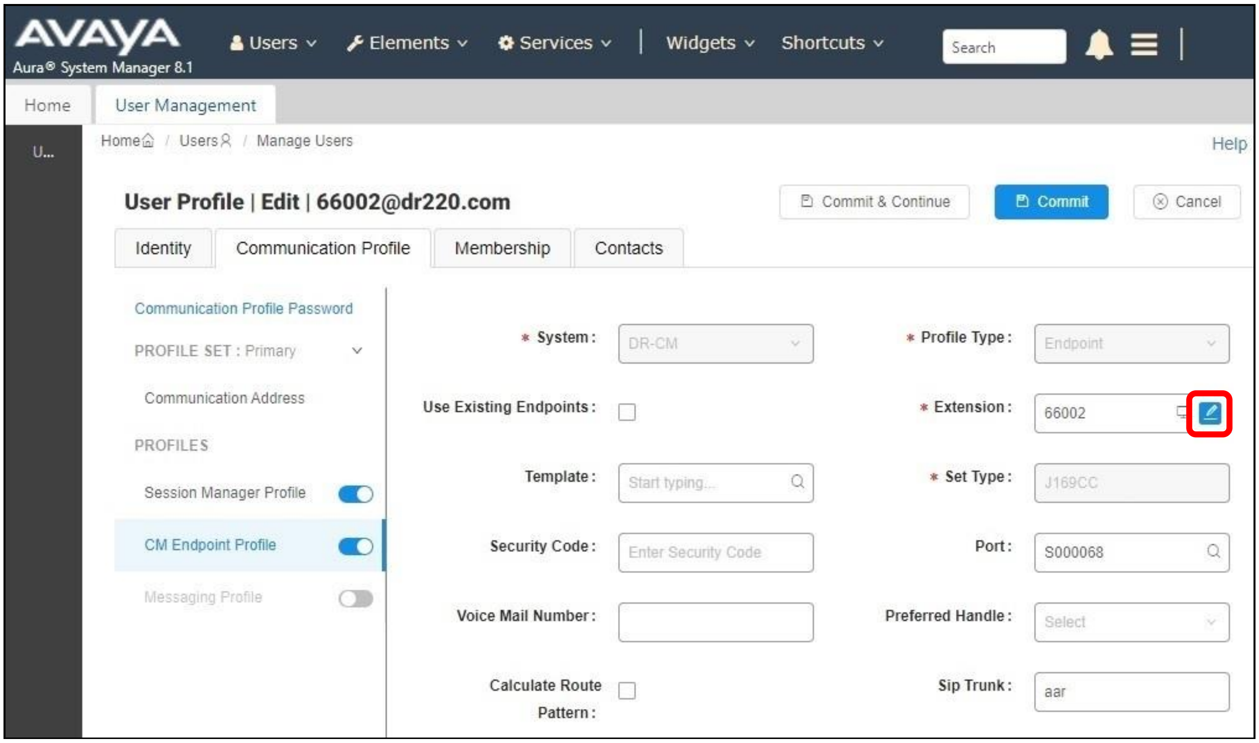
Select the entry associated with the first SIP agent station from **Section 3**, in this case "66002", and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
☑	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
□	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

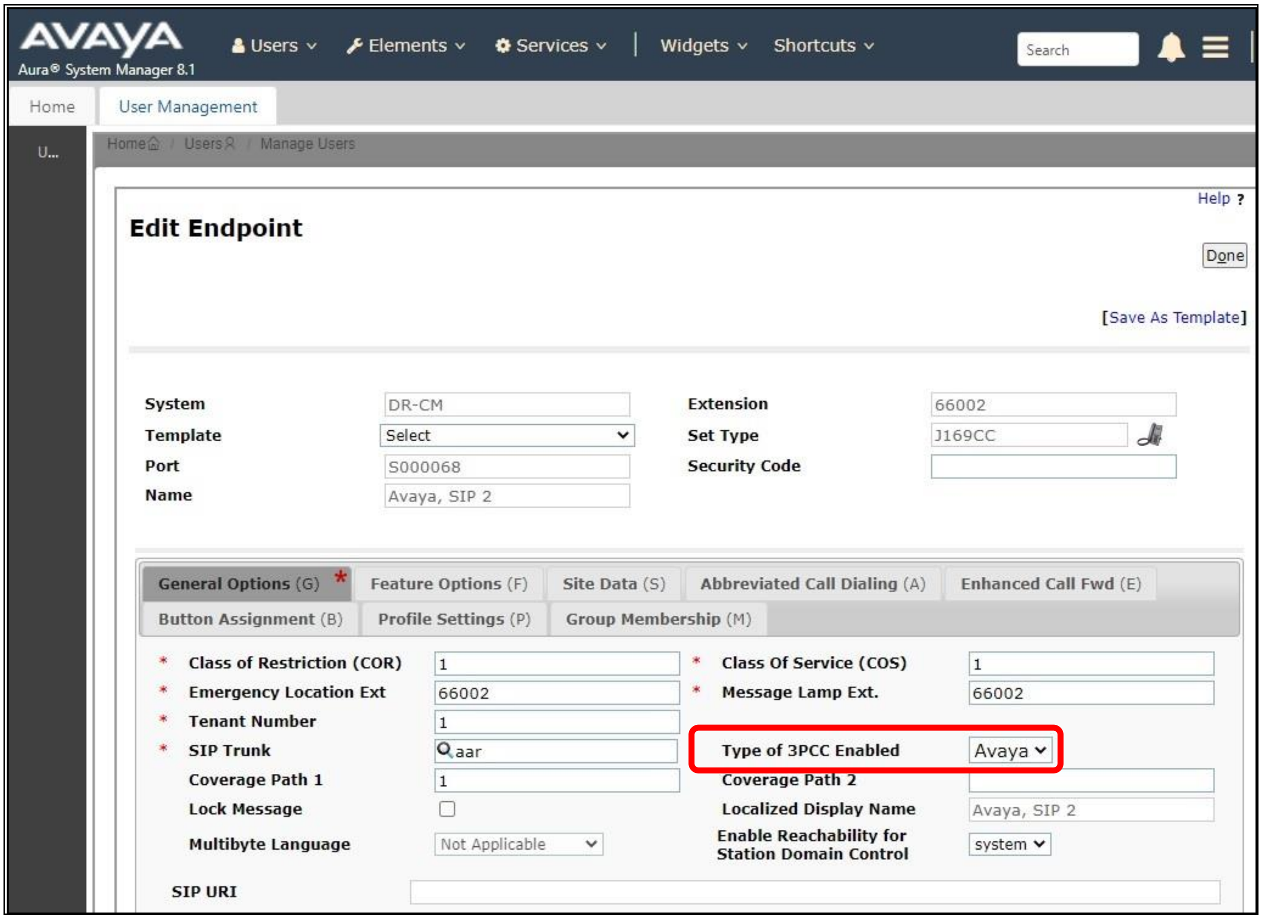


User Profile | Edit | 66002@dr220.com

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66002
Template :	Start typing...	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000068
Voice Mail Number :		Preferred Handle :	Select
Calculate Route Pattern :	□	Sip Trunk :	aar

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select “Avaya” as shown below.

Repeat this section for all SIP agent users from **Section 3**. In the compliance testing, one SIP agent extension 66002 was configured.



Edit Endpoint

System	DR-CM	Extension	66002
Template	Select	Set Type	J169CC
Port	S000068	Security Code	
Name	Avaya, SIP 2		

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	66002	* Message Lamp Ext.	66002
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1	1	Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 2
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

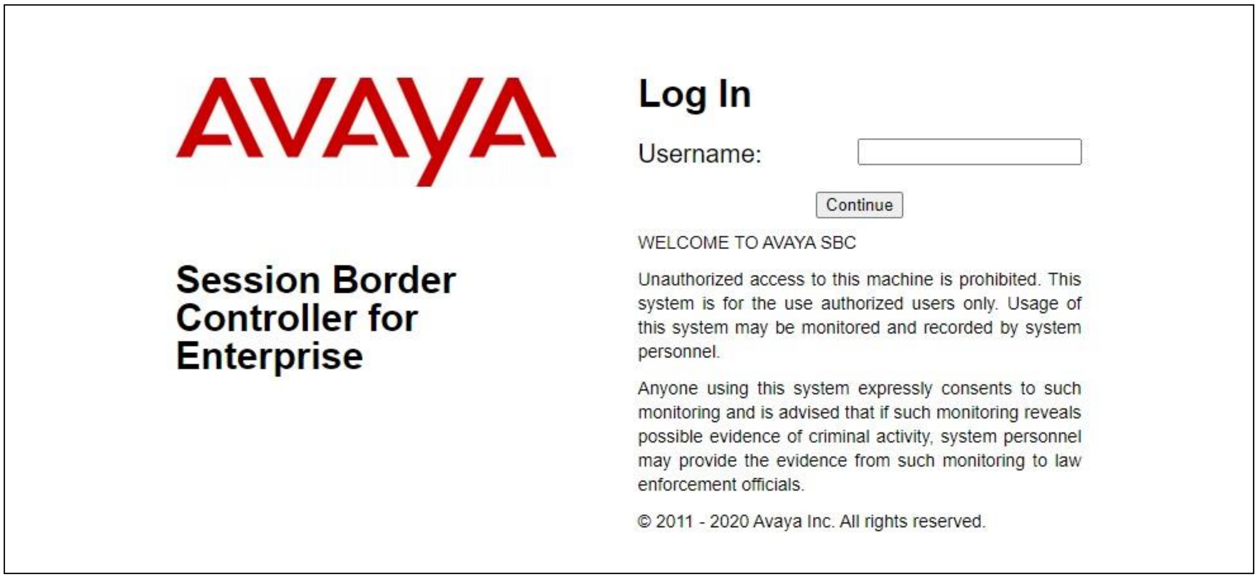
8. Configure Avaya Session Border Controller for Enterprise

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

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

8.1. 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.



WELCOME TO AVAYA SBC

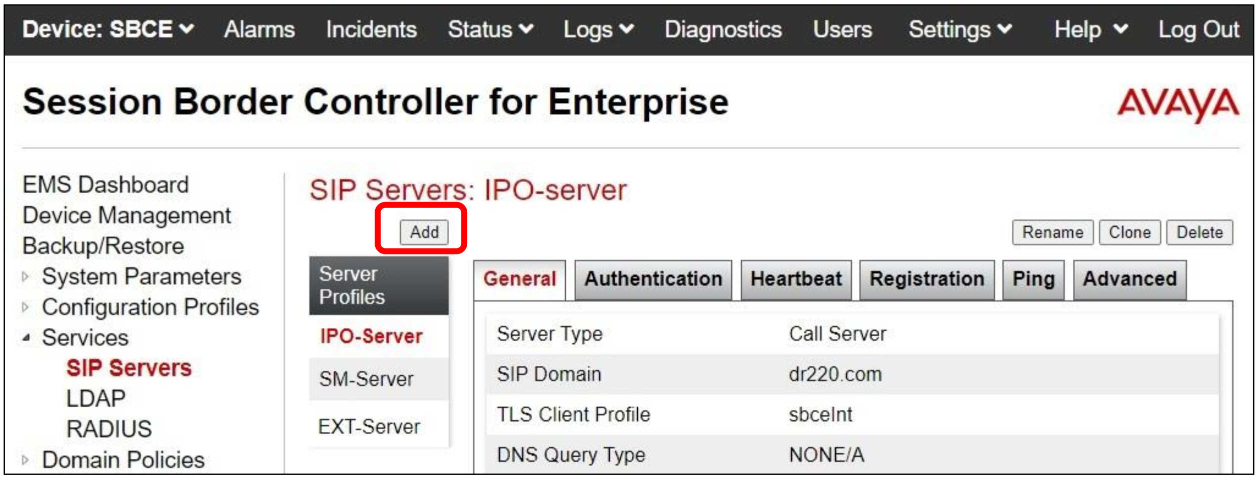
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

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.

© 2011 - 2020 Avaya Inc. All rights reserved.

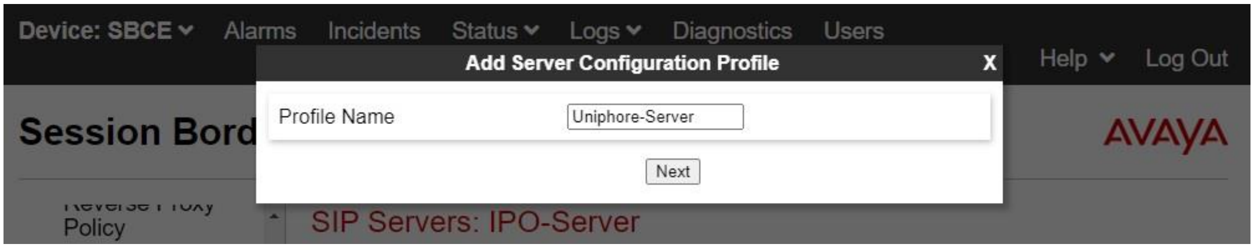
8.2. Administer SIP Servers

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



Server Type	Call Server
SIP Domain	dr220.com
TLS Client Profile	sbceInt
DNS Query Type	NONE/A

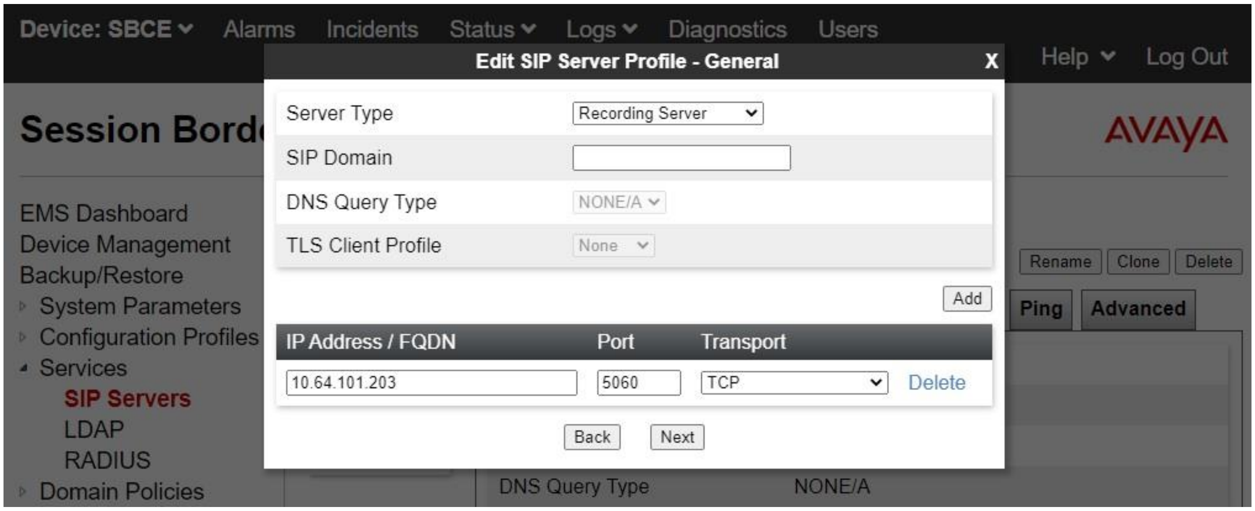
The **Add Server Configuration Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



Profile Name: Uniphore-Server

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 Uniphore server with the OrkAudio component.
- **Port:** "5060"
- **Transport:** "TCP"

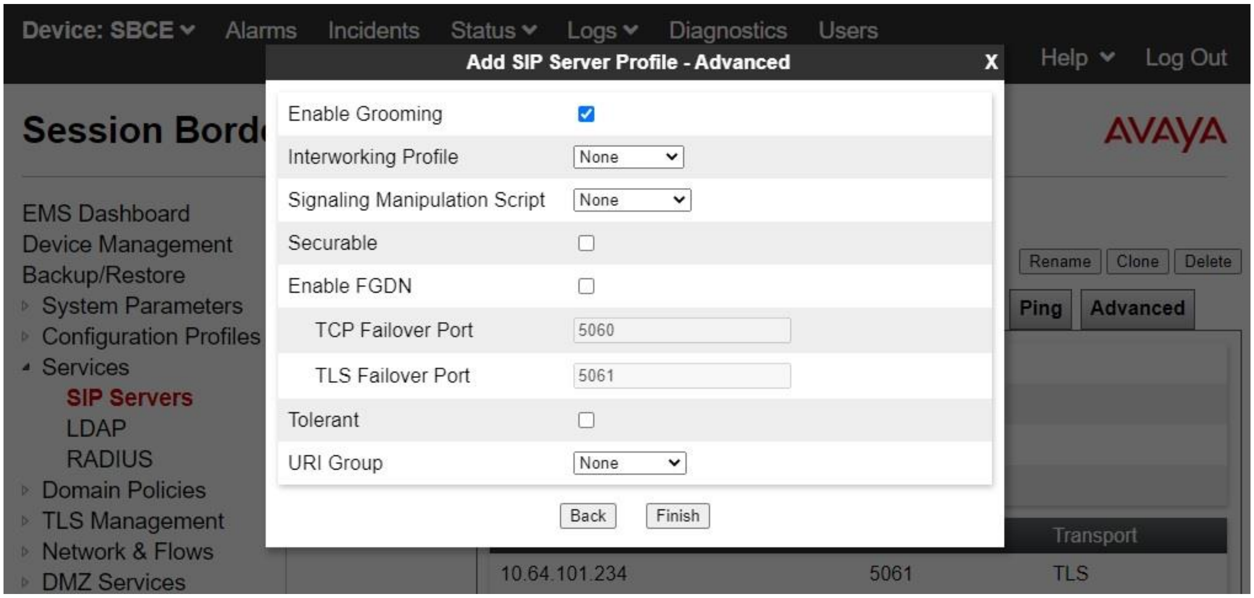


Edit SIP Server Profile - General

Server Type: Recording Server
SIP Domain:
DNS Query Type: NONE/A
TLS Client Profile: None

IP Address / FQDN	Port	Transport	
10.64.101.203	5060	TCP	Delete

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

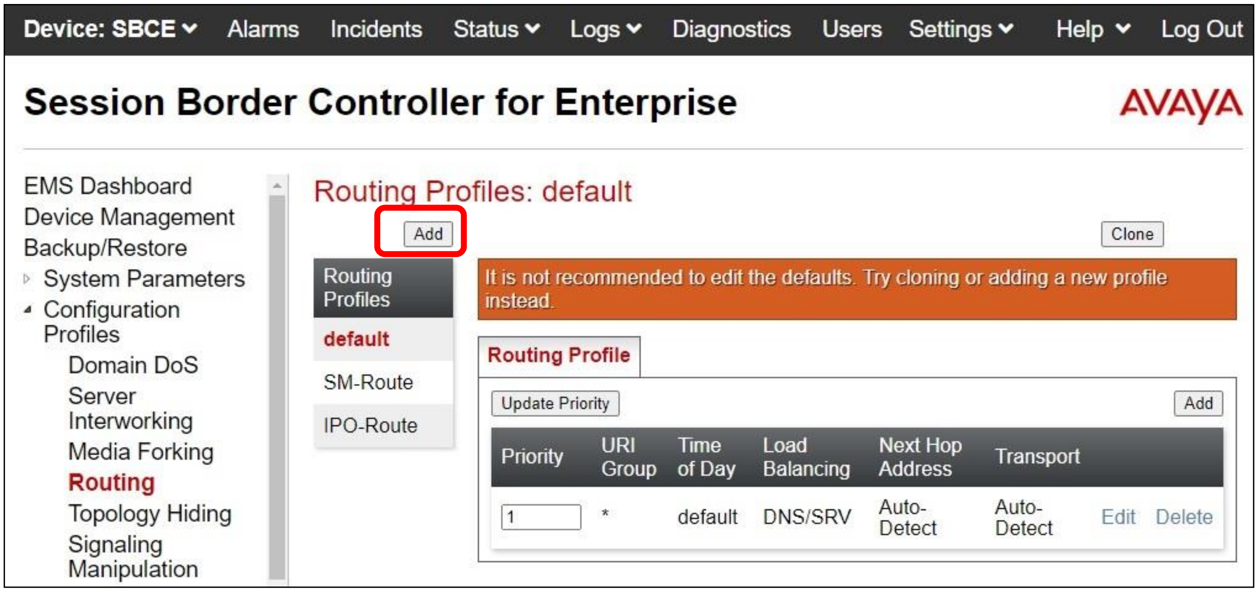


Add SIP Server Profile - Advanced

Enable Grooming: ☑
Interworking Profile: None
Signaling Manipulation Script: None
Securable: ☐
Enable FGDN: ☐
TCP Failover Port: 5060
TLS Failover Port: 5061
Tolerant: ☐
URI Group: None

8.3. Administer Routing

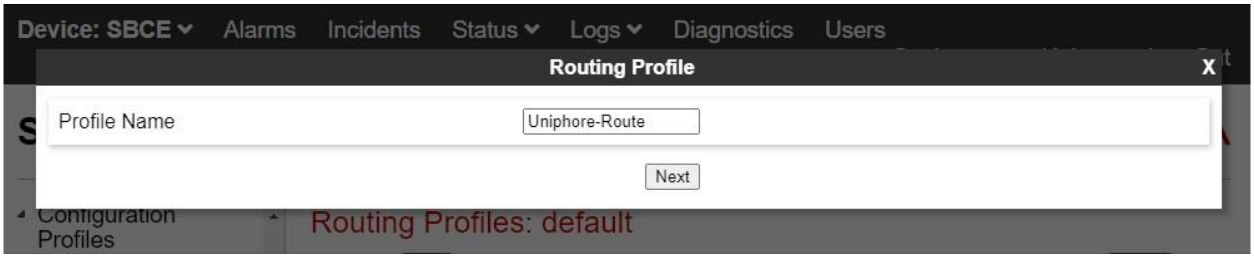
Select **Backup/Restore → Configuration Profiles → Routing** from the left pane to display the existing routing profiles. Click **Add** to add a routing profile for Uniphore.



It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

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

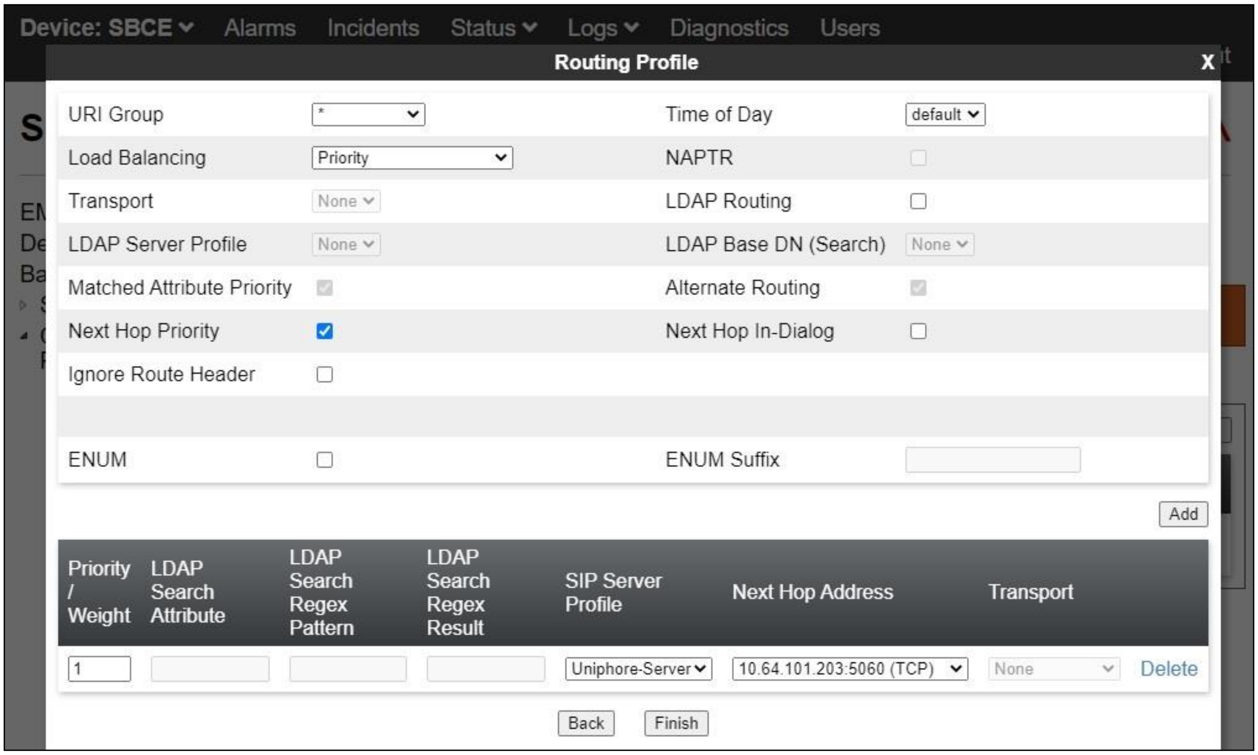
The **Routing Profile** pop-up screen is displayed. Enter a desired **Profile Name** as shown below.



Profile Name: Uniphore-Route

The **Routing Profile** pop-up screen is updated. 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 Uniphore SIP server profile from **Section 8.2**.
- **Next Hop Address:** Retain the auto populated value.



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	

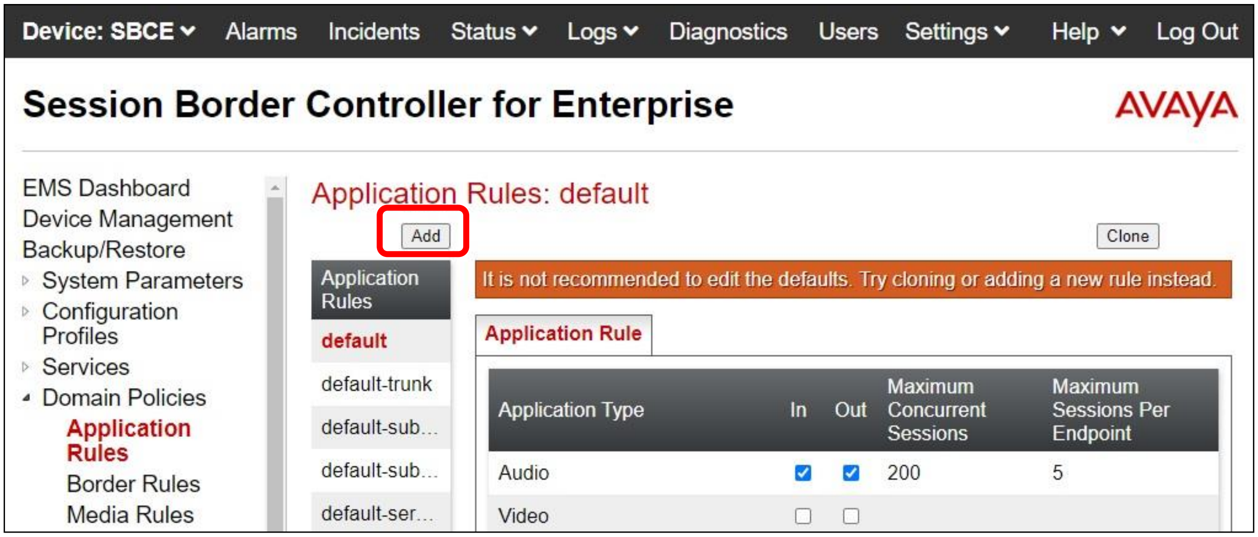
Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				Uniphore-Server	10.64.101.203:5060 (TCP)	None	Delete

Back Finish

8.4. Administer Application Rules

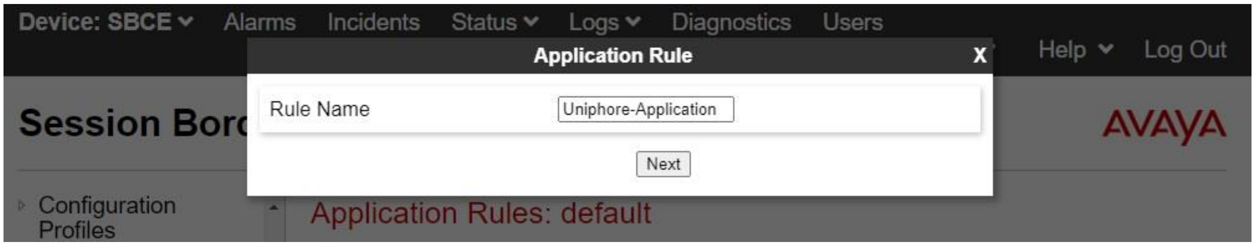
Select **Backup/Restore → Domain Policies → Application Rules** from the left pane to display the existing application rules. Click **Add** to add an application rule for Uniphore.



It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

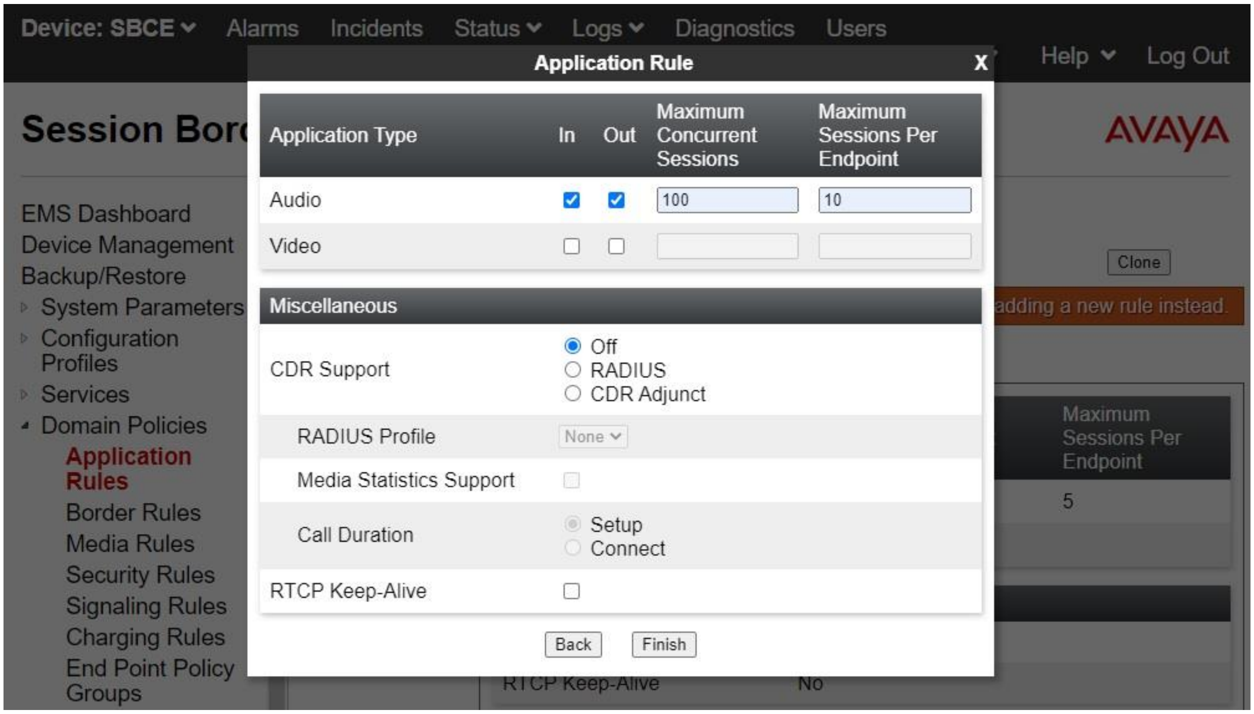
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	200	5
Video	□	□		

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



Rule Name: Uniphore-Application

The **Application Rule** pop-up screen is updated. Check **Audio In** and **Audio Out**, and enter desired values for **Maximum Concurrent Sessions** and **Maximum Sessions Per Endpoint**, as shown below. Retain the default values in the remaining fields.



Application Rule

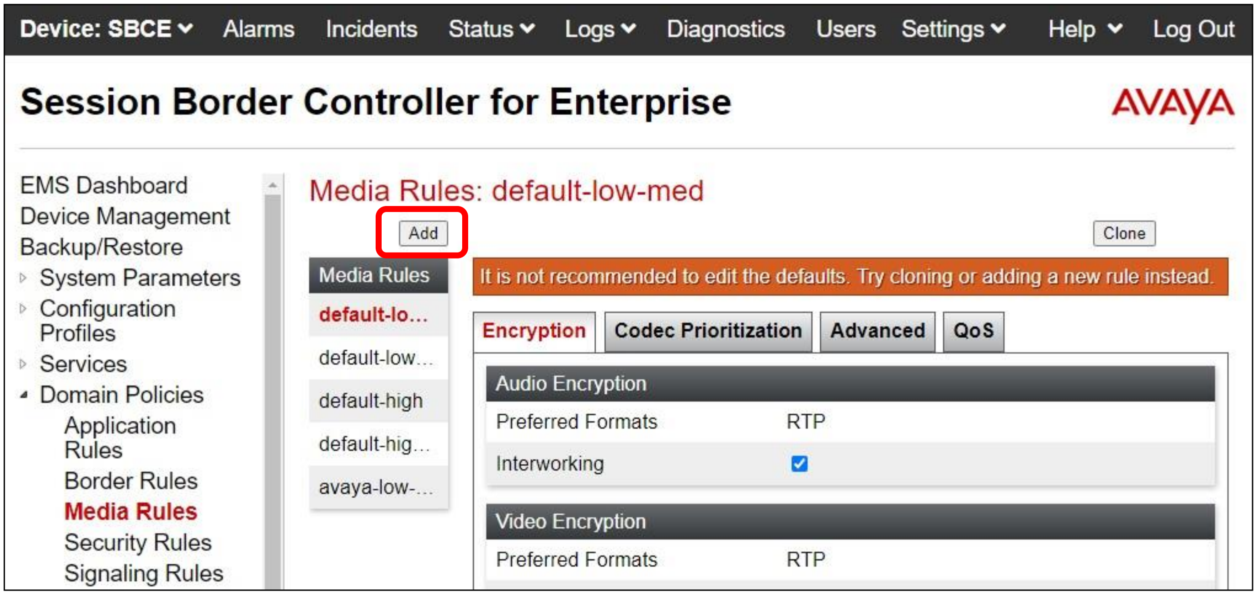
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	100	10
Video	□	□		

Miscellaneous

CDR Support	● Off ○ RADIUS ○ CDR Adjunct
RADIUS Profile	None
Media Statistics Support	□
Call Duration	○ Setup ○ Connect
RTCP Keep-Alive	□

8.5. Administer Media Rules

Select **Backup/Restore → Domain Policies → Media Rules** from the left pane to display the existing media rules. Click **Add** to add a media rule for Uniphore.



Media Rules: default-low-med

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

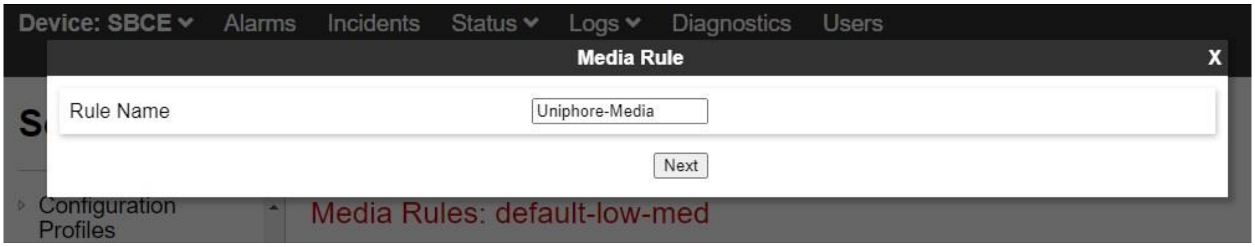
Audio Encryption

Preferred Formats	RTP
Interworking	☑

Video Encryption

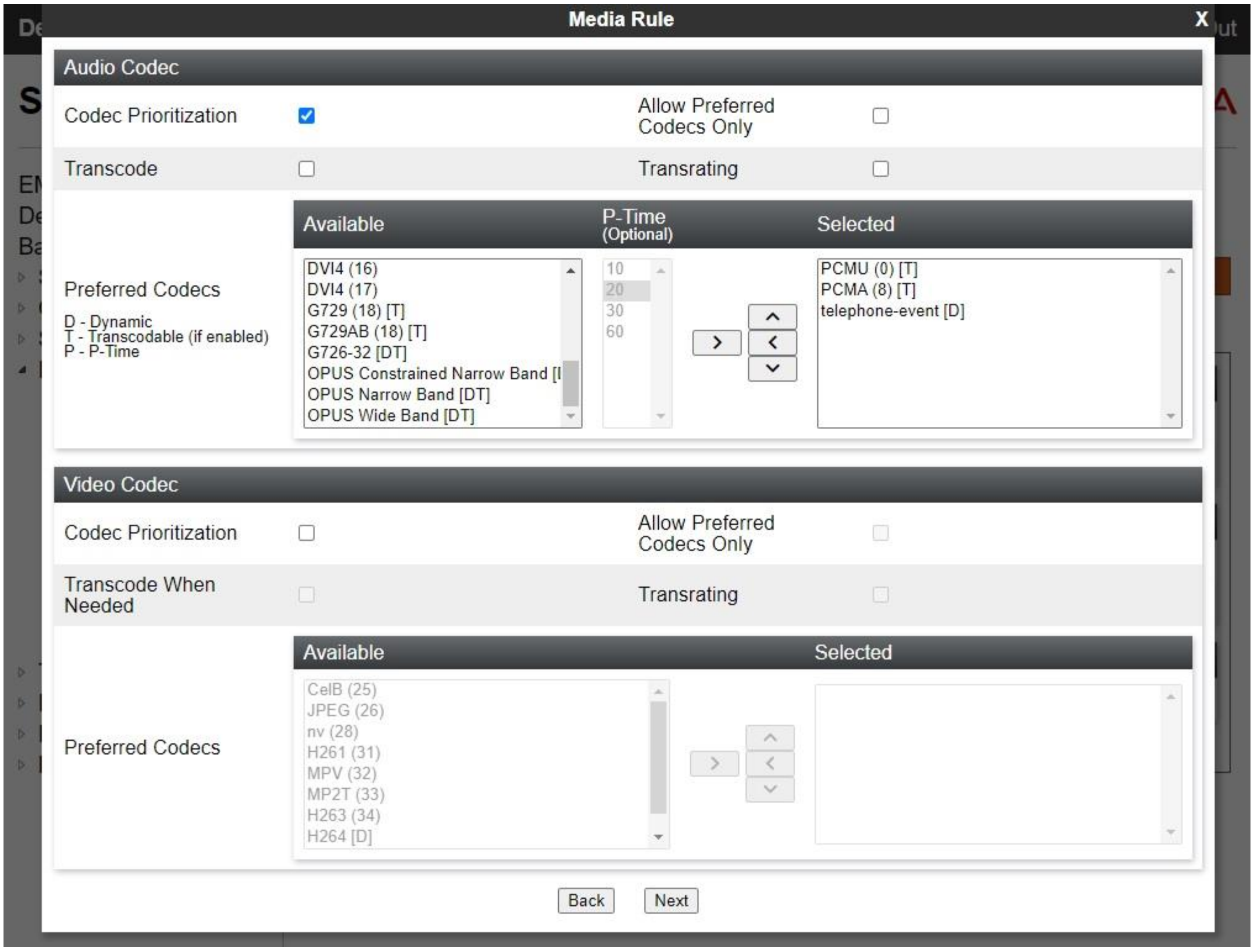
Preferred Formats	RTP

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



Rule Name: Uniphore-Media

The **Media Rule** pop-up screen is updated. Navigate to the **Audio Codec** page. Select the relevant codecs from the **Available** column to the **Selected** column, as shown below. Retain the default values in all remaining fields and pages.



Audio Codec

Codec Prioritization ☑ Allow Preferred Codecs Only □

Transcode □ Transrating □

Preferred Codecs
D - Dynamic
T - Transcodable (if enabled)
P - P-Time

Available: DVI4 (16), DVI4 (17), G729 (18) [T], G729AB (18) [T], G726-32 [DT], OPUS Constrained Narrow Band [I, OPUS Narrow Band [DT], OPUS Wide Band [DT]

P-Time (Optional): 10, 20, 30, 60

Selected: PCMU (0) [T], PCMA (8) [T], telephone-event [D]

Video Codec

Codec Prioritization □ Allow Preferred Codecs Only □

Transcode When Needed □ Transrating □

Preferred Codecs

Available: CelB (25), JPEG (26), nv (28), H261 (31), MPV (32), MP2T (33), H263 (34), H264 [D]

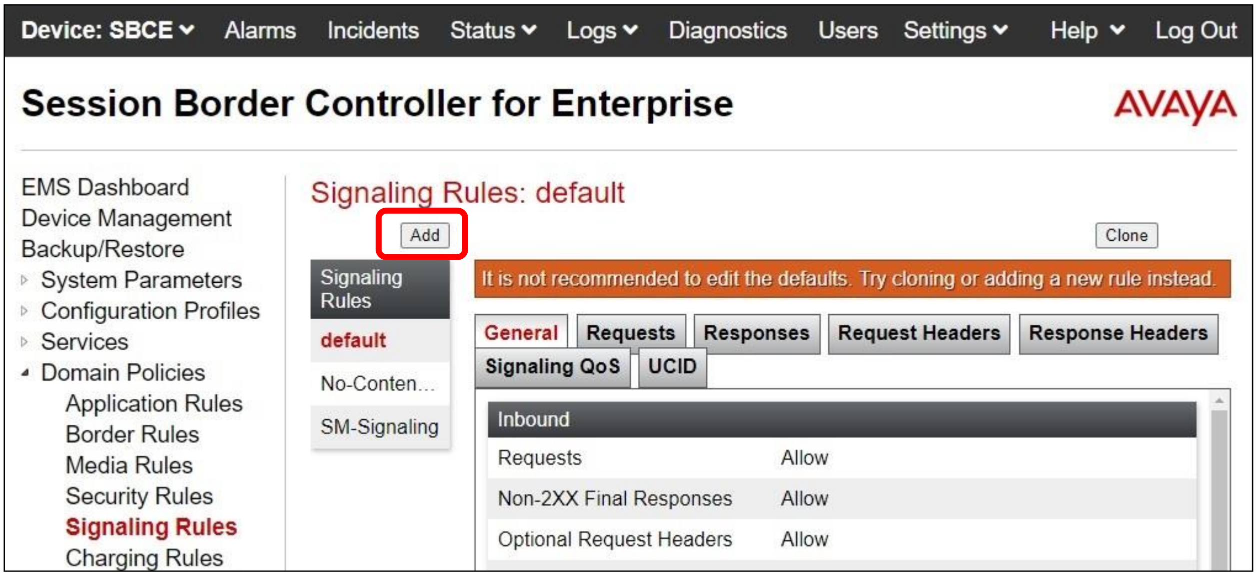
Selected:

8.6. Administer Signaling Rules

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

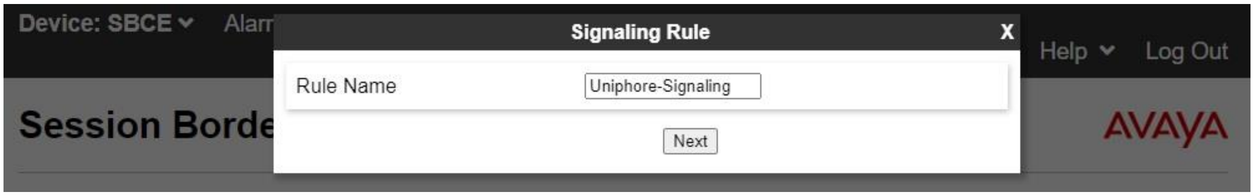
8.6.1. Uniphore Signaling Rule

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



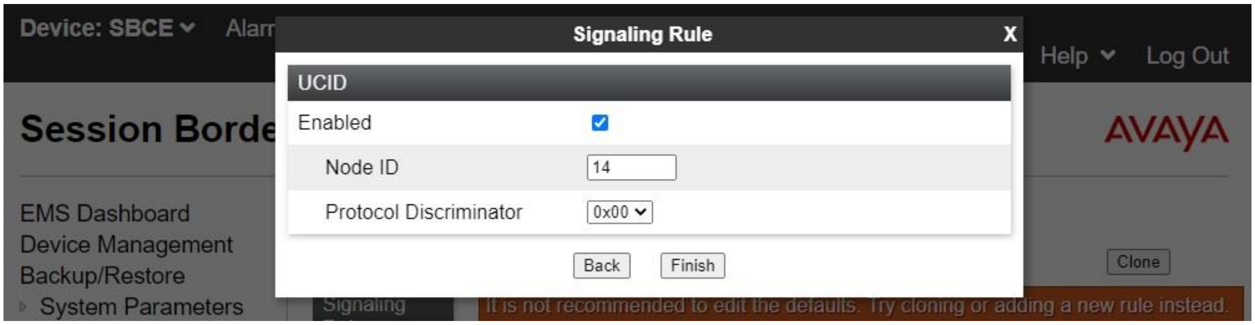
Inbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow

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



Rule Name	Uniphore-Signaling

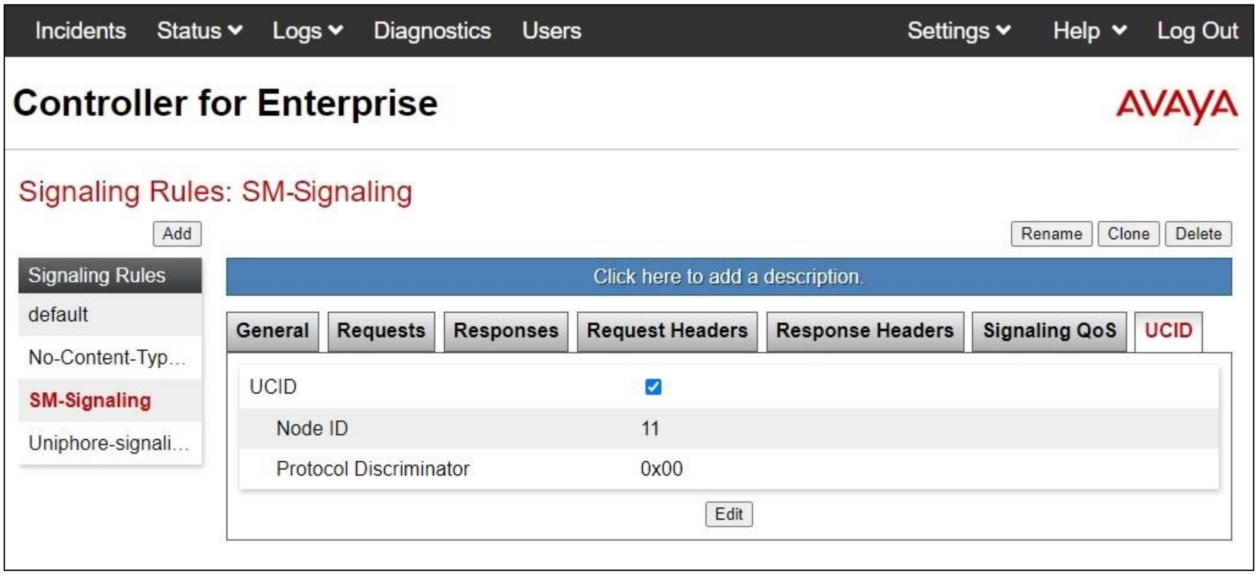
The **Signaling Rule** pop-up screen is updated. Navigate to the **UCID** page. Check **Enabled**. For **Node ID**, enter a unique number across the customer system, in this case "14". Retain the default value in the remaining field.



UCID	
Enabled	☑
Node ID	14
Protocol Discriminator	0x00

8.6.2. 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.

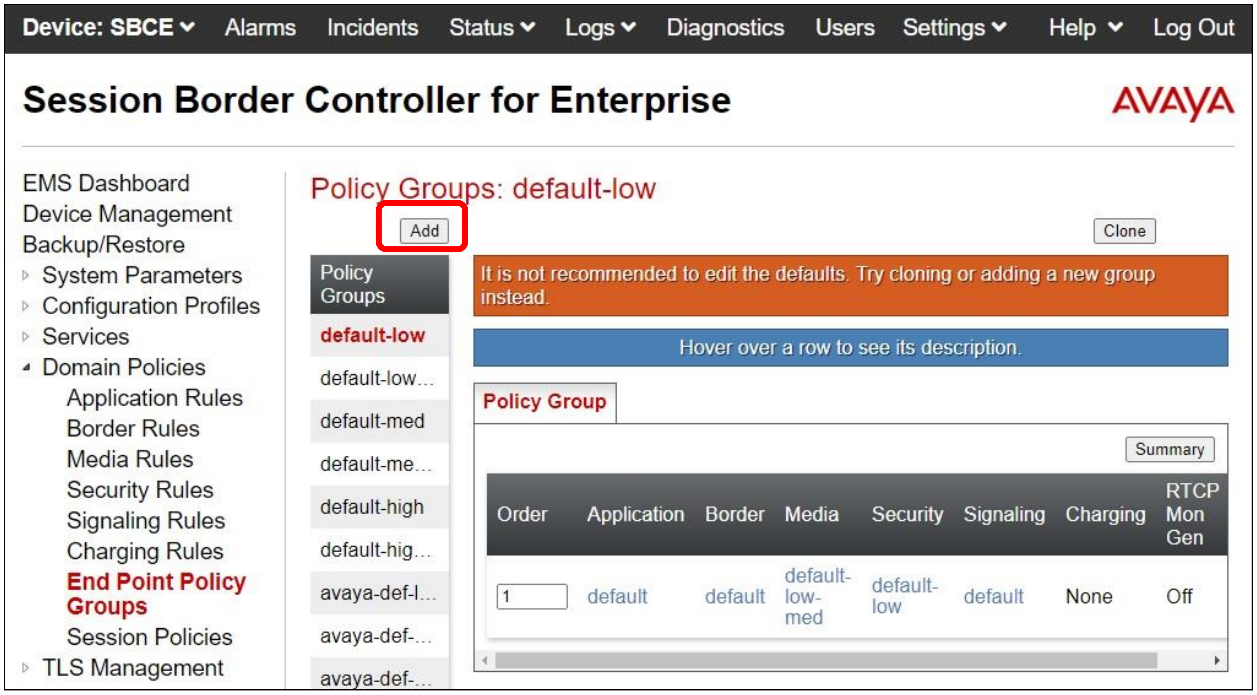


Signaling Rules: SM-Signaling

UCID	☑
Node ID	11
Protocol Discriminator	0x00

8.7. Administer End Point Policy Groups

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

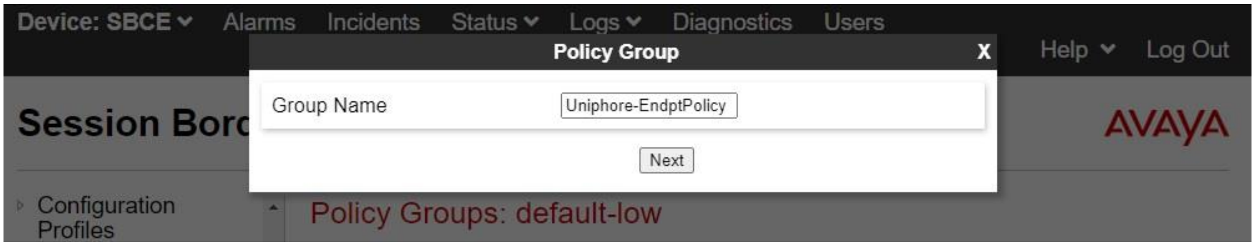


Policy Groups: default-low

It is not recommended to edit the defaults. Try cloning or adding a new group instead.

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

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

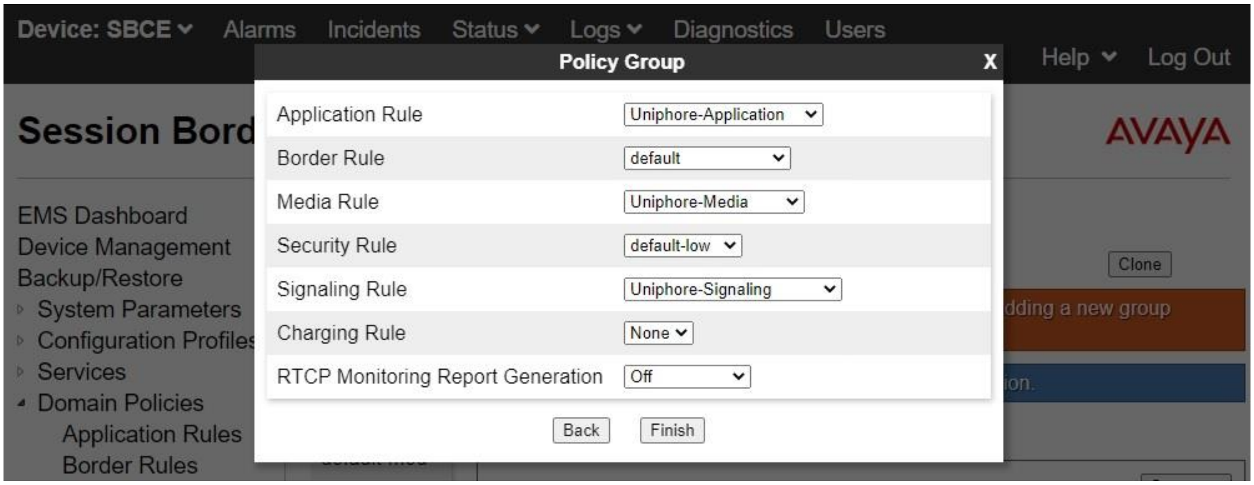


Policy Group

Group Name: Uniphore-EndptPolicy

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

- **Application Rule:** Select the Uniphore application rule from **Section 8.4**.
- **Media Rule:** Select the Uniphore media rule from **Section 8.5**.
- **Signaling Rule:** Select the Uniphore signaling rule from **Section 8.6.1**.

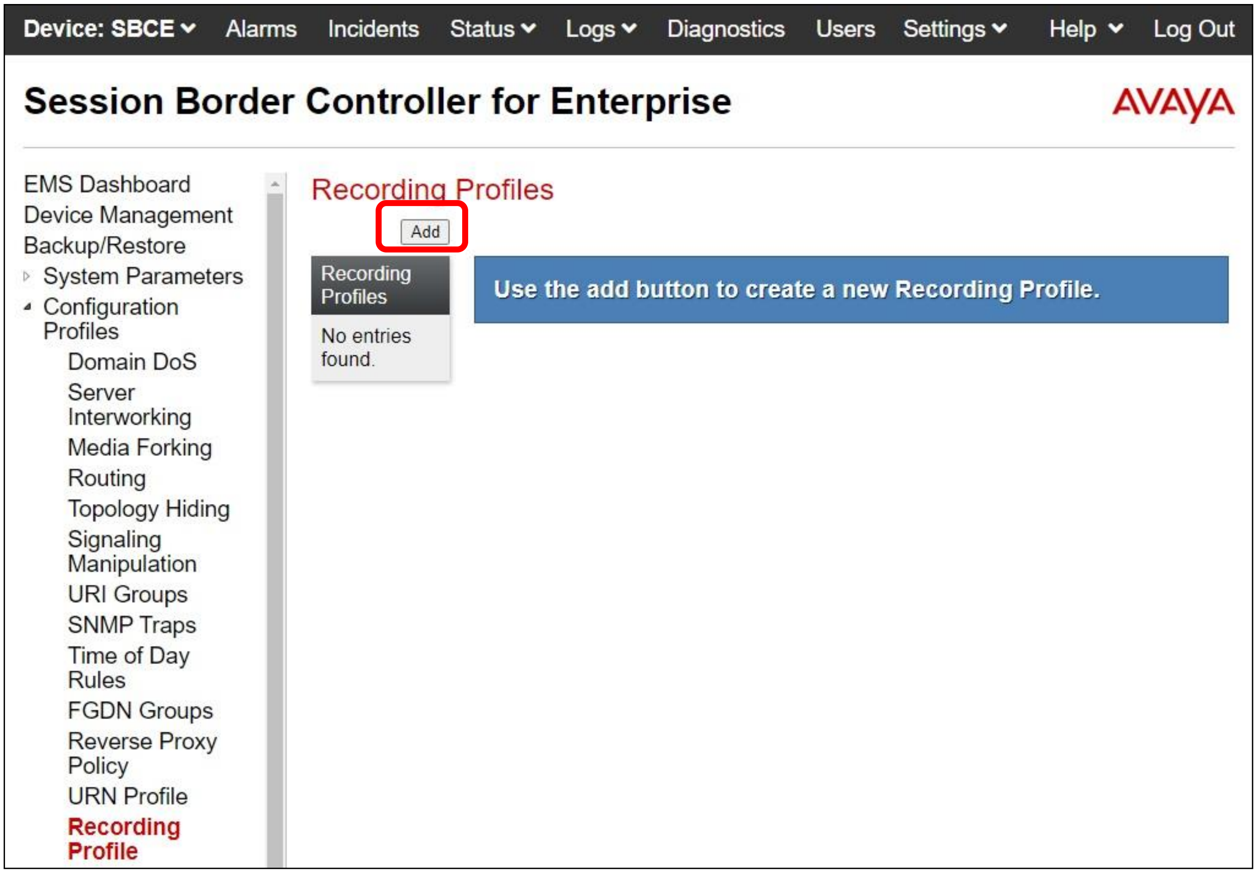


Policy Group

Application Rule	Uniphore-Application
Border Rule	default
Media Rule	Uniphore-Media
Security Rule	default-low
Signaling Rule	Uniphore-Signaling
Charging Rule	None
RTCP Monitoring Report Generation	Off

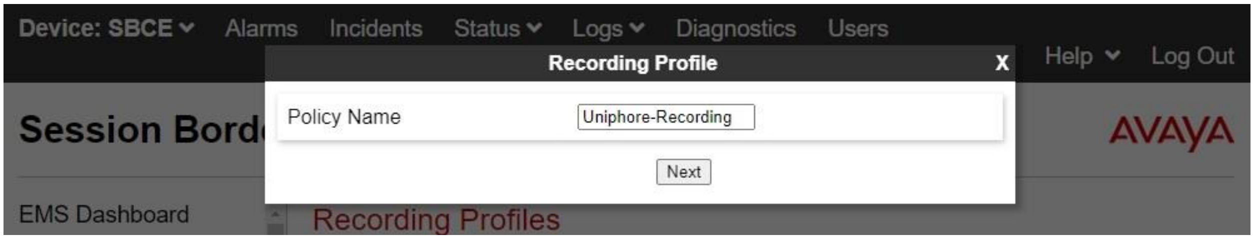
8.8. Administer Recording Profile

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



Use the add button to create a new Recording Profile.

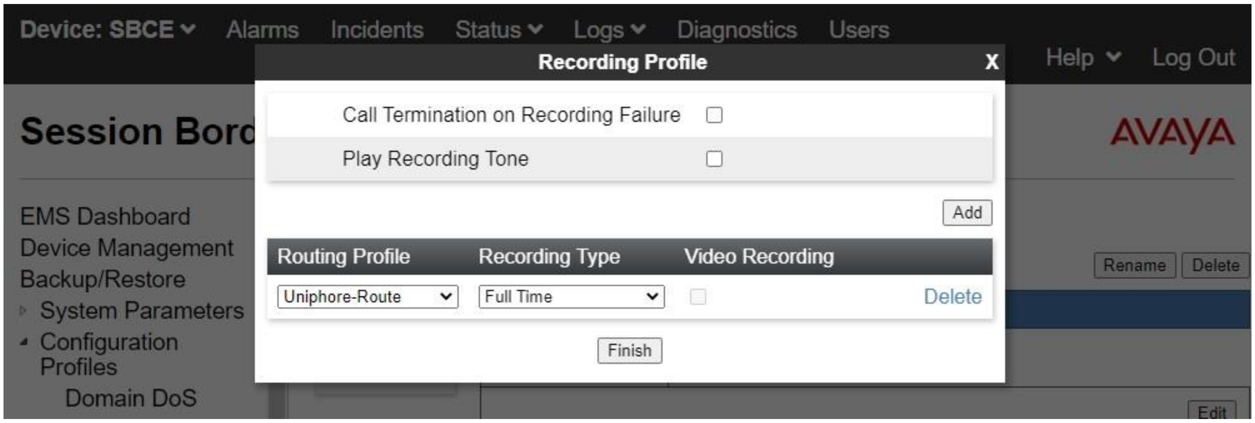
The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name** as shown below.



Policy Name: Uniphore-Recording

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

- **Play Recording Tone:** Check this field is customer desires recording tone to be played.
- **Routing Profile:** Select the Uniphore routing profile from **Section 8.3**.
- **Recording Type:** "Full Time"



Recording Profile

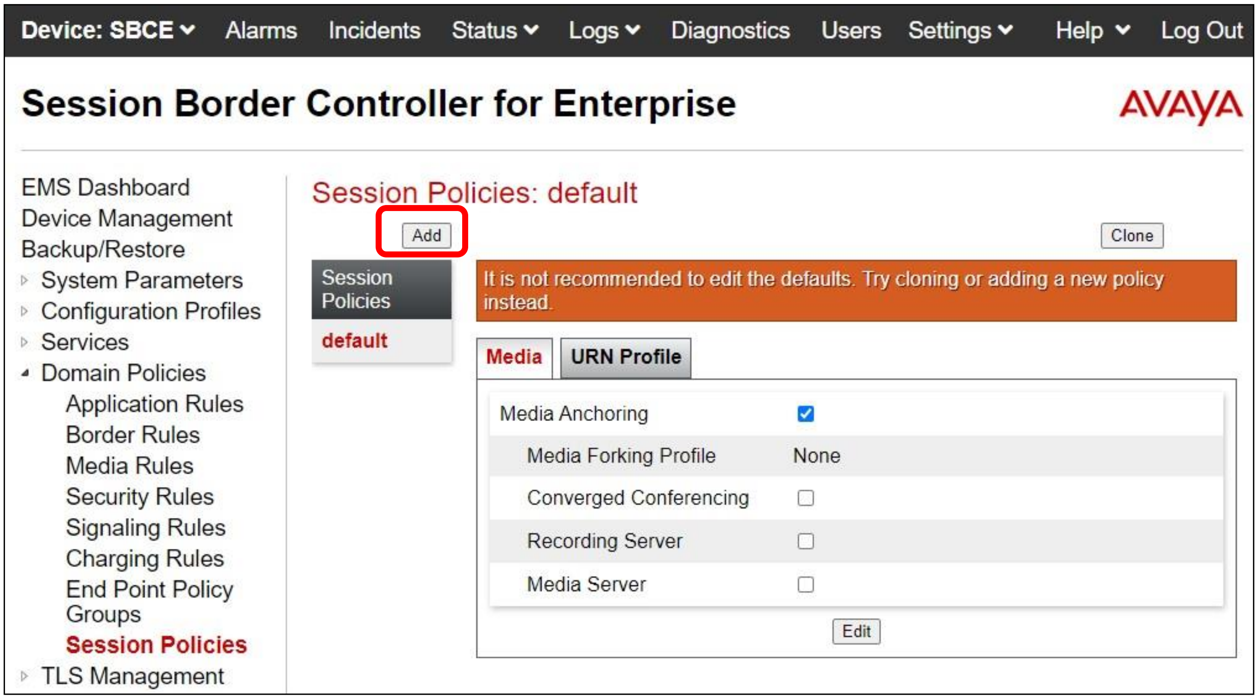
Call Termination on Recording Failure □

Play Recording Tone □

Routing Profile	Recording Type	Video Recording	
Uniphore-Route	Full Time	□	Delete

8.9. Administer Session Policies

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

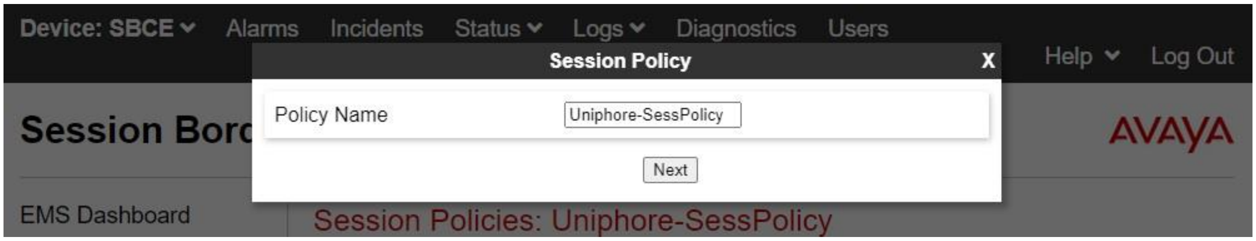


Session Policies: default

It is not recommended to edit the defaults. Try cloning or adding a new policy instead.

Media Anchoring	☑
Media Forking Profile	None
Converged Conferencing	□
Recording Server	□
Media Server	□

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

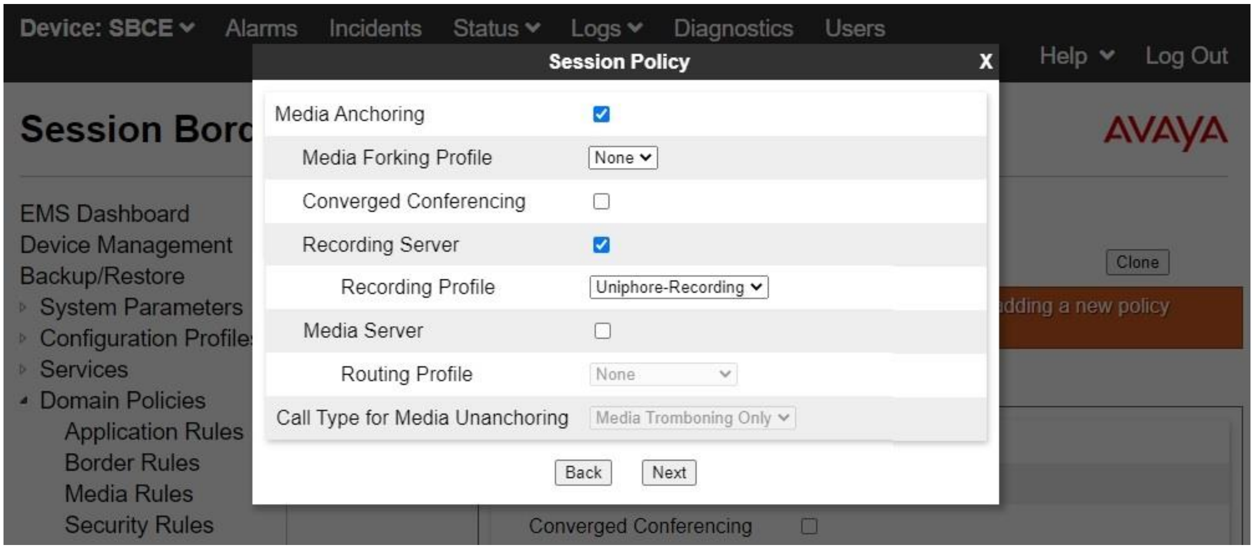


Session Policy

Policy Name: Uniphore-SessPolicy

The **Session Policy** pop-up screen is updated. 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 Uniphore recording profile from **Section 8.8**.

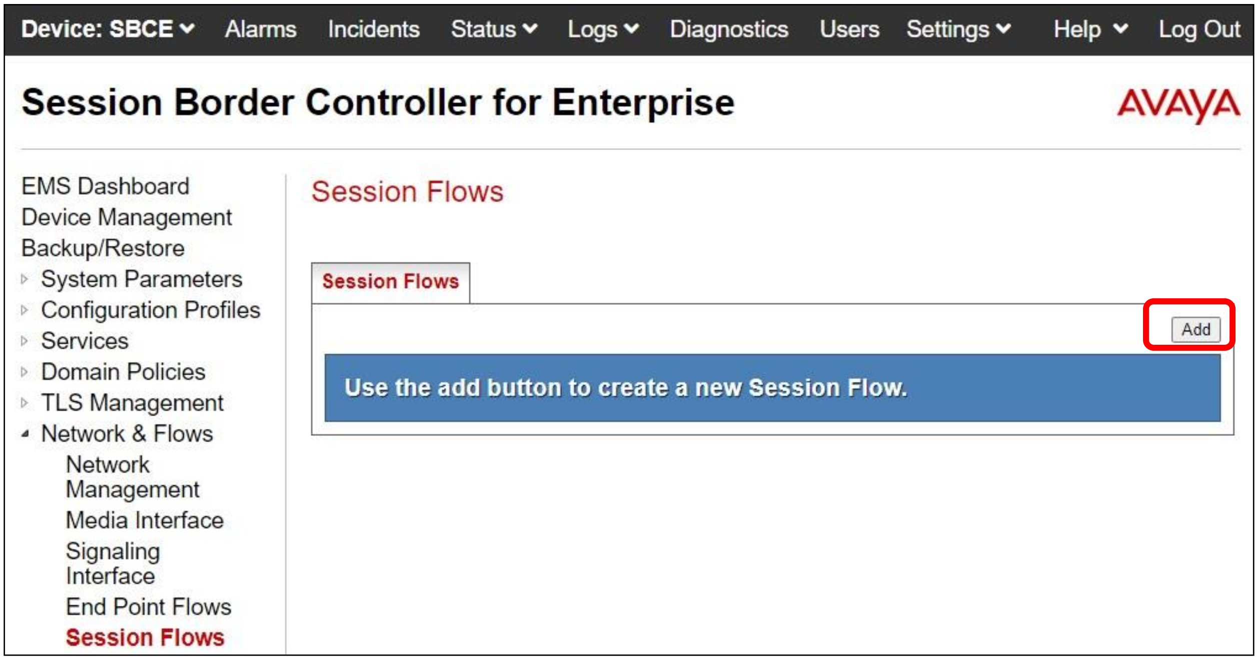


Session Policy

Media Anchoring	☑
Media Forking Profile	None
Converged Conferencing	☐
Recording Server	☑
Recording Profile	Uniphore-Recording
Media Server	☐
Routing Profile	None
Call Type for Media Unanchoring	Media Tromboning Only

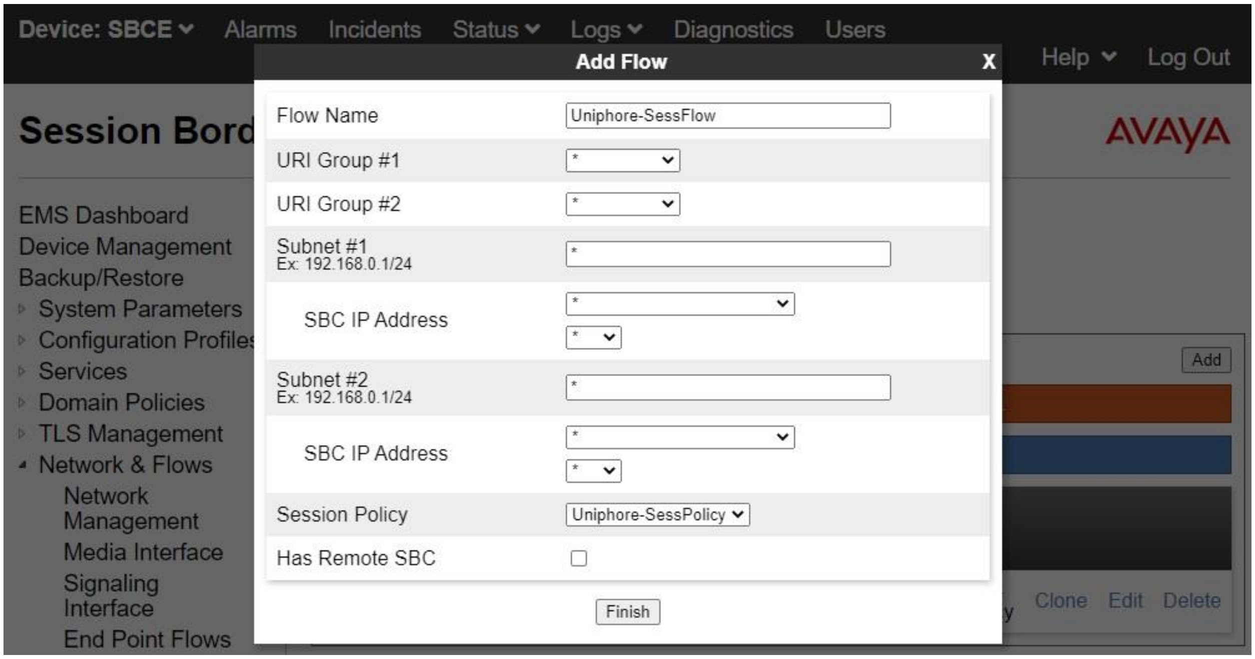
8.10. Administer Session Flows

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



Use the add button to create a new Session Flow.

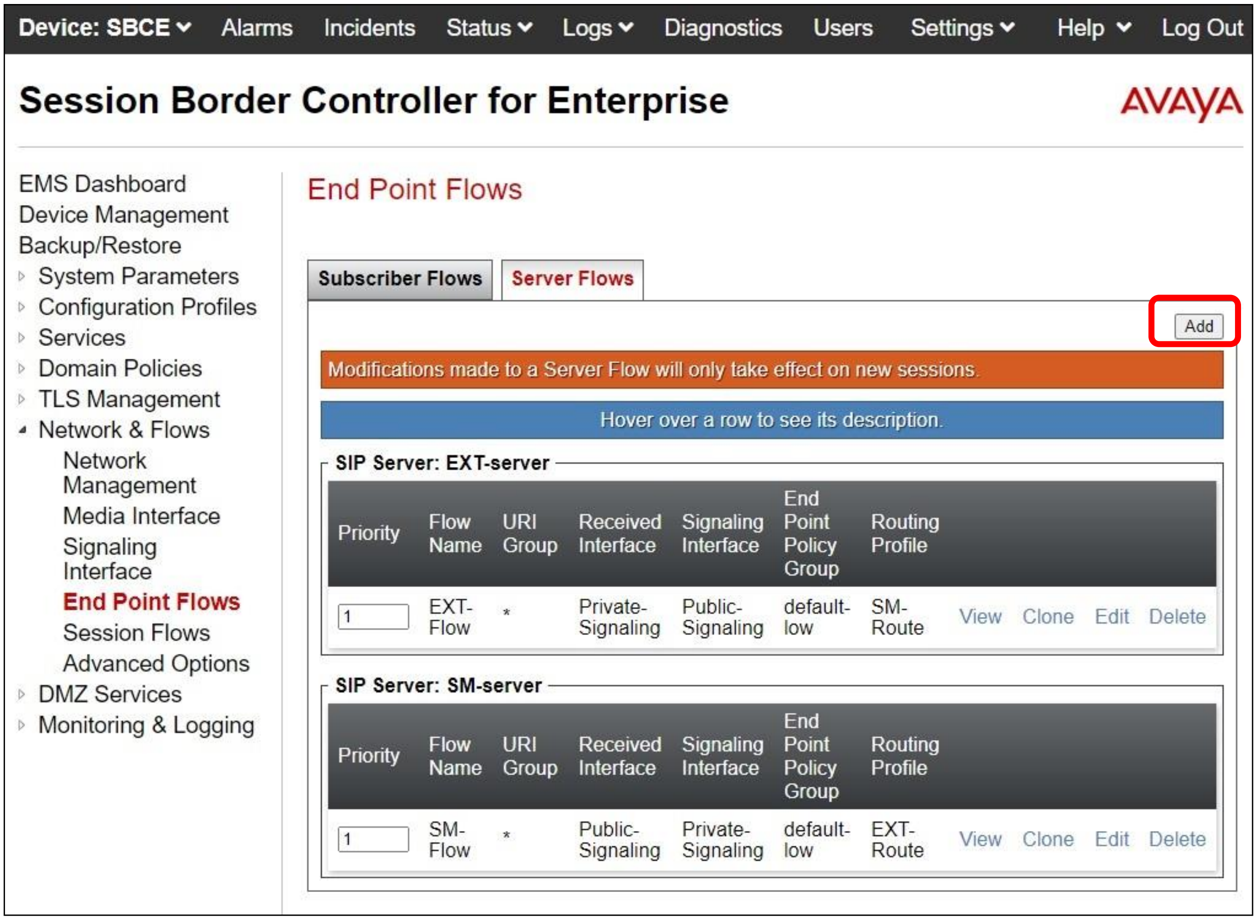
The **Add Flow** pop-up screen is displayed. For **Flow Name**, enter a desired name. For **Session Policy**, select the Uniphore session policy from **Section 8.9**. Retain the default values in the remaining fields.



Flow Name	Uniphore-SessFlow
URI Group #1	*
URI Group #2	*
Subnet #1 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Subnet #2 Ex: 192.168.0.1/24	*
SBC IP Address	* *
Session Policy	Uniphore-SessPolicy
Has Remote SBC	□

8.11. 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 Uniphore.



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

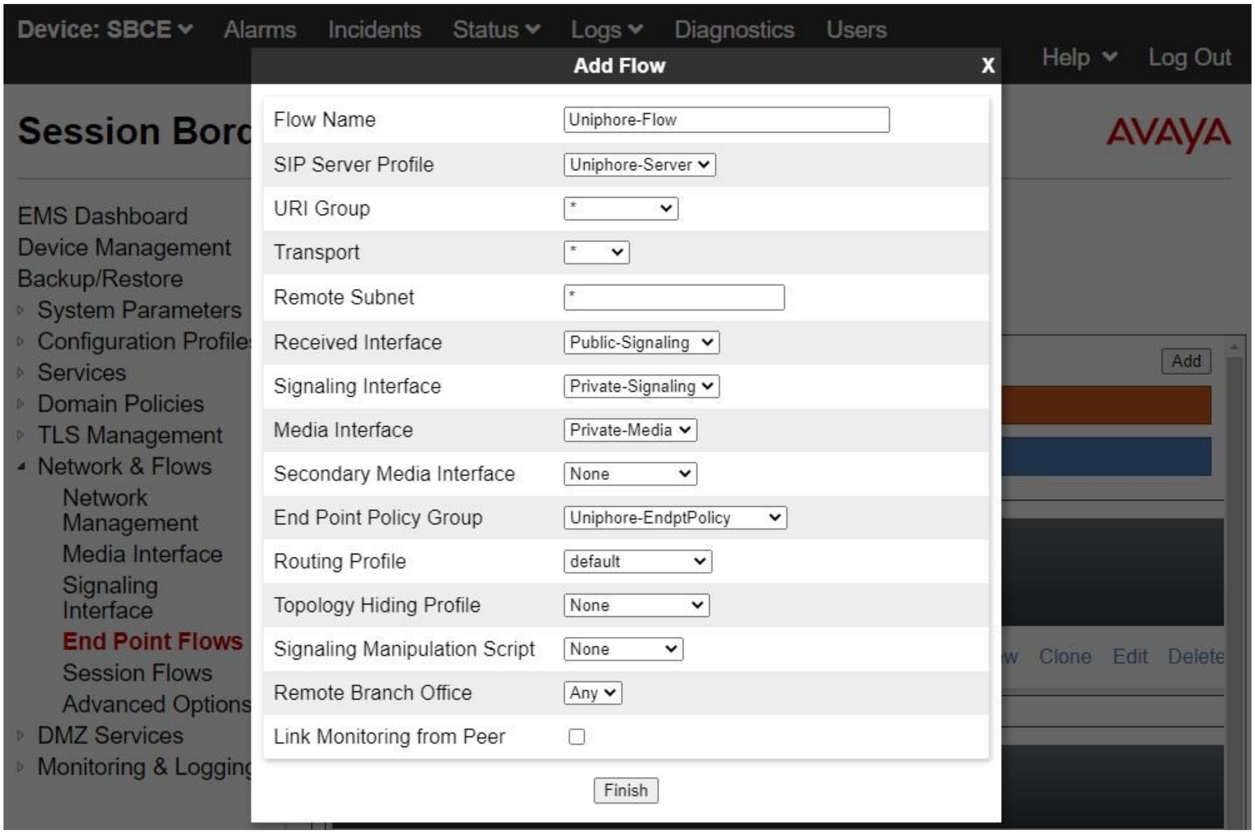
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	EXT-Flow	*	Private-Signaling	Public-Signaling	default-low	SM-Route	View	Clone	Edit	Delete

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 Uniphore SIP server profile from **Section 8.2**.
- **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 Uniphore end point policy group from **Section 8.7**.



Add Flow

Flow Name	Uniphore-Flow
SIP Server Profile	Uniphore-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	Uniphore-EndptPolicy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□

Finish

9. Configure Uniphore Real Intent

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

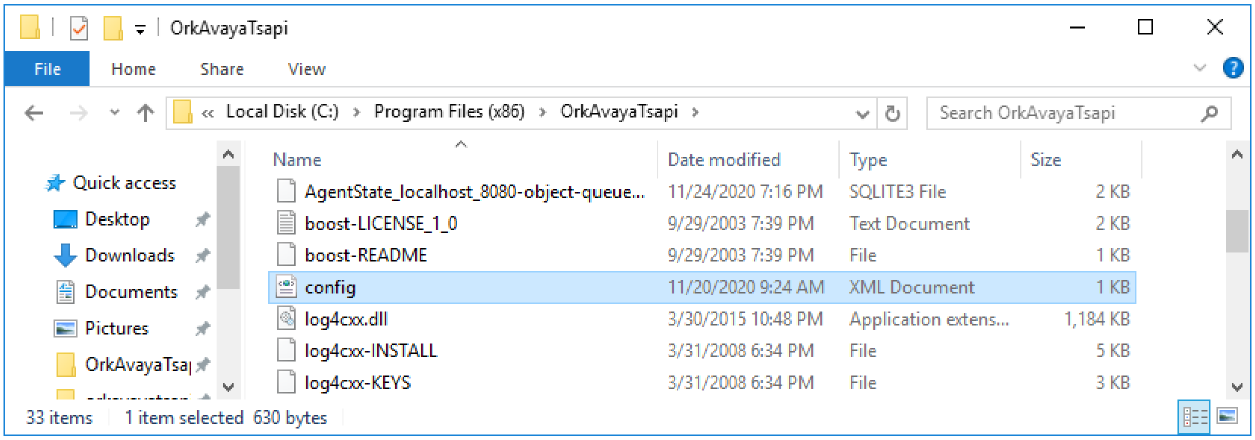
- Administer OrkAvayaTsapi
- Prepare agent user CSV file
- Launch Swagger web interface
- Import agent user CSV file

The configuration of Real Intent performed by Uniphore Services. The procedural steps are presented in these Application Notes for informational purposes.

Prior to configuration, an organizational name is assumed to be pre-configured.

9.1. Administer OrkAvayaTsapi

From the Real Intent server running the OrkAvayaTsapi component, navigate to the **C:\Program Files (x86)\OrkAvayaTsapi** directory and edit the **config** file shown below.



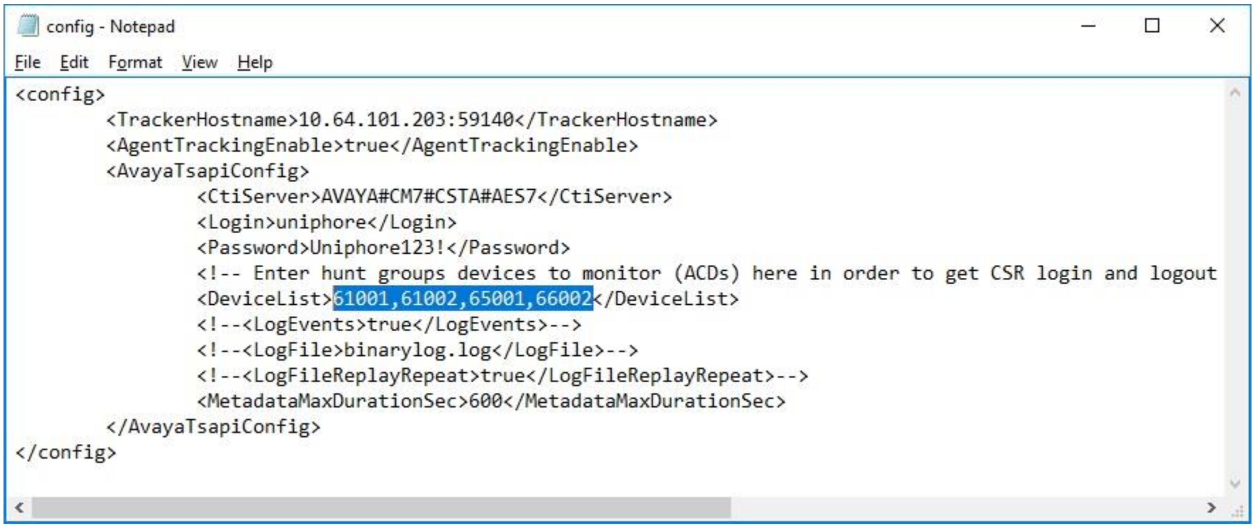
Name	Date modified	Type	Size
AgentState_localhost_8080-object-queue...	11/24/2020 7:16 PM	SQLITE3 File	2 KB
boost-LICENSE_1_0	9/29/2003 7:39 PM	Text Document	2 KB
boost-README	9/29/2003 7:39 PM	File	1 KB
config	11/20/2020 9:24 AM	XML Document	1 KB
log4cxx.dll	3/30/2015 10:48 PM	Application extens...	1,184 KB
log4cxx-INSTALL	3/31/2008 6:34 PM	File	5 KB
log4cxx-KEYS	3/31/2008 6:34 PM	File	3 KB

33 items 1 item selected 630 bytes

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **TrackerHostname:** "x:y" where "x" is IP address of this server and "y" is port "59140".
- **CtiServer:** The Tlink name from **Section 6.7**.
- **Login:** The Uniphore user credential from **Section 6.4**.
- **Password:** The Uniphore user credential from **Section 6.4**.
- **DeviceList:** Extension of skill groups and agent stations to monitor from **Section 3**.

Add the **AgentTrackingEnable** parameter and set to "true" as shown below.

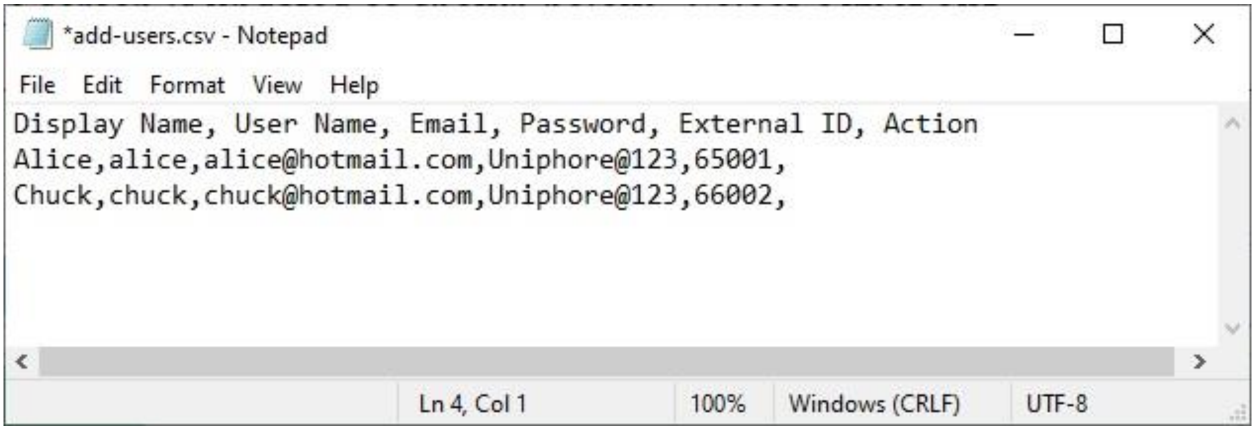


```
<config>
        <TrackerHostname>10.64.101.203:59140</TrackerHostname>
        <AgentTrackingEnable>true</AgentTrackingEnable>
        <AvayaTsapiConfig>
                <CtiServer>AVAYA#CM7#CSTA#AES7</CtiServer>
                <Login>uniphore</Login>
                <Password>Uniphore123!</Password>
                <!-- Enter hunt groups devices to monitor (ACDs) here in order to get CSR login and logout
                <DeviceList>61001,61002,65001,66002</DeviceList>
                <!--<LogEvents>true</LogEvents>-->
                <!--<LogFile>binarylog.log</LogFile>-->
                <!--<LogFileReplayRepeat>true</LogFileReplayRepeat>-->
                <MetadataMaxDurationSec>600</MetadataMaxDurationSec>
        </AvayaTsapiConfig>
</config>
```

9.2. Prepare Agent User CSV File

Follow reference [4] to prepare an agent user file in the CSV format shown below, which will be used later to import into Real Intent. Note that the actual file name can vary.

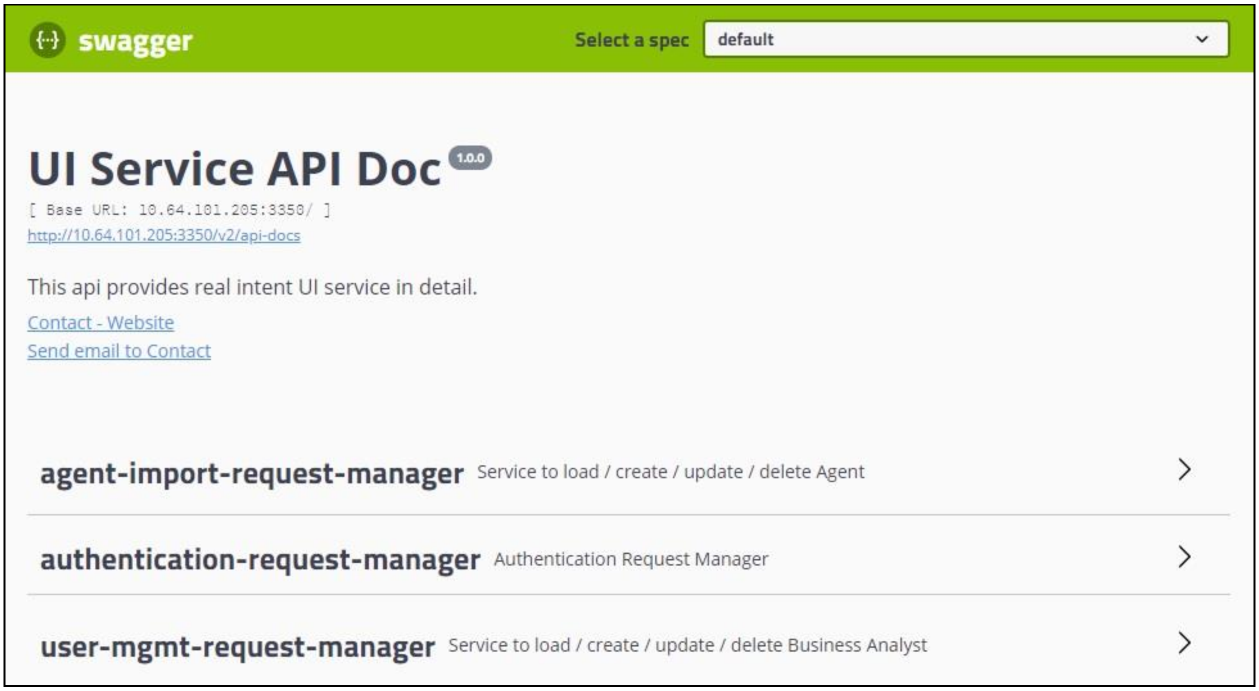
In the compliance testing, two agent user entries were created in the CSV file to correspond to the two agent users from **Section 3**.



```
Display Name, User Name, Email, Password, External ID, Action
Alice,alice,alice@hotmail.com,Uniphore@123,65001,
Chuck,chuck,chuck@hotmail.com,Uniphore@123,66002,
```

9.3. Launch Swagger Web Interface

Access the Swagger web interface by using the URL "http://ip-address:3350/swagger-ui.html" in an Internet browser window, where "ip-address" is the IP address of the Real Intent server with the User Management Service component. The screen below is displayed.



UI Service API Doc

[Base URL: 10.64.101.205:3350/]
http://10.64.101.205:3350/v2/api-docs

This api provides real intent UI service in detail.

Contact - Website
Send email to Contact

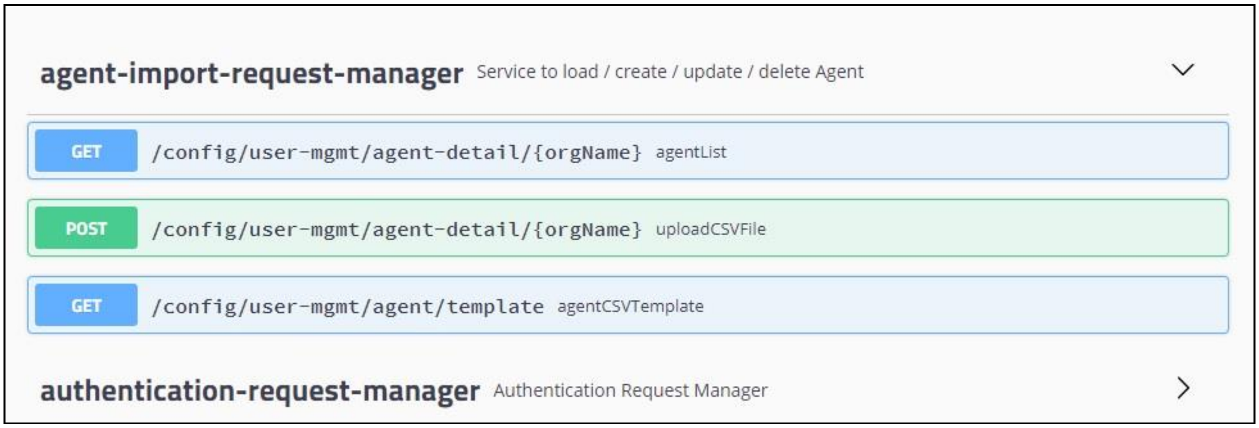
agent-import-request-manager Service to load / create / update / delete Agent

authentication-request-manager Authentication Request Manager

user-mgmt-request-manager Service to load / create / update / delete Business Analyst

9.4. Import Agent User CSV File

Expand the **agent-import-request-manager** section and select **POST**.



agent-import-request-manager Service to load / create / update / delete Agent

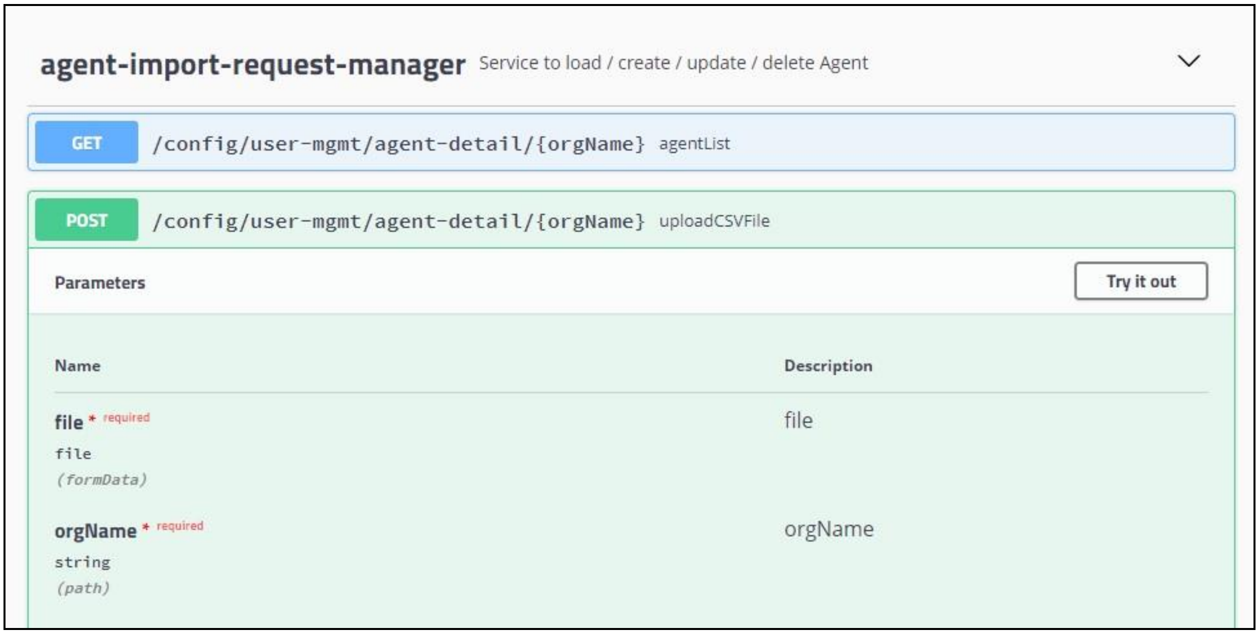
GET /config/user-mgmt/agent-detail/{orgName} agentList

POST /config/user-mgmt/agent-detail/{orgName} uploadCSVFile

GET /config/user-mgmt/agent/template agentCSVTemplate

authentication-request-manager Authentication Request Manager

The screen is updated as shown below. Select **Try it out**.



agent-import-request-manager Service to load / create / update / delete Agent

GET /config/user-mgmt/agent-detail/{orgName} agentList

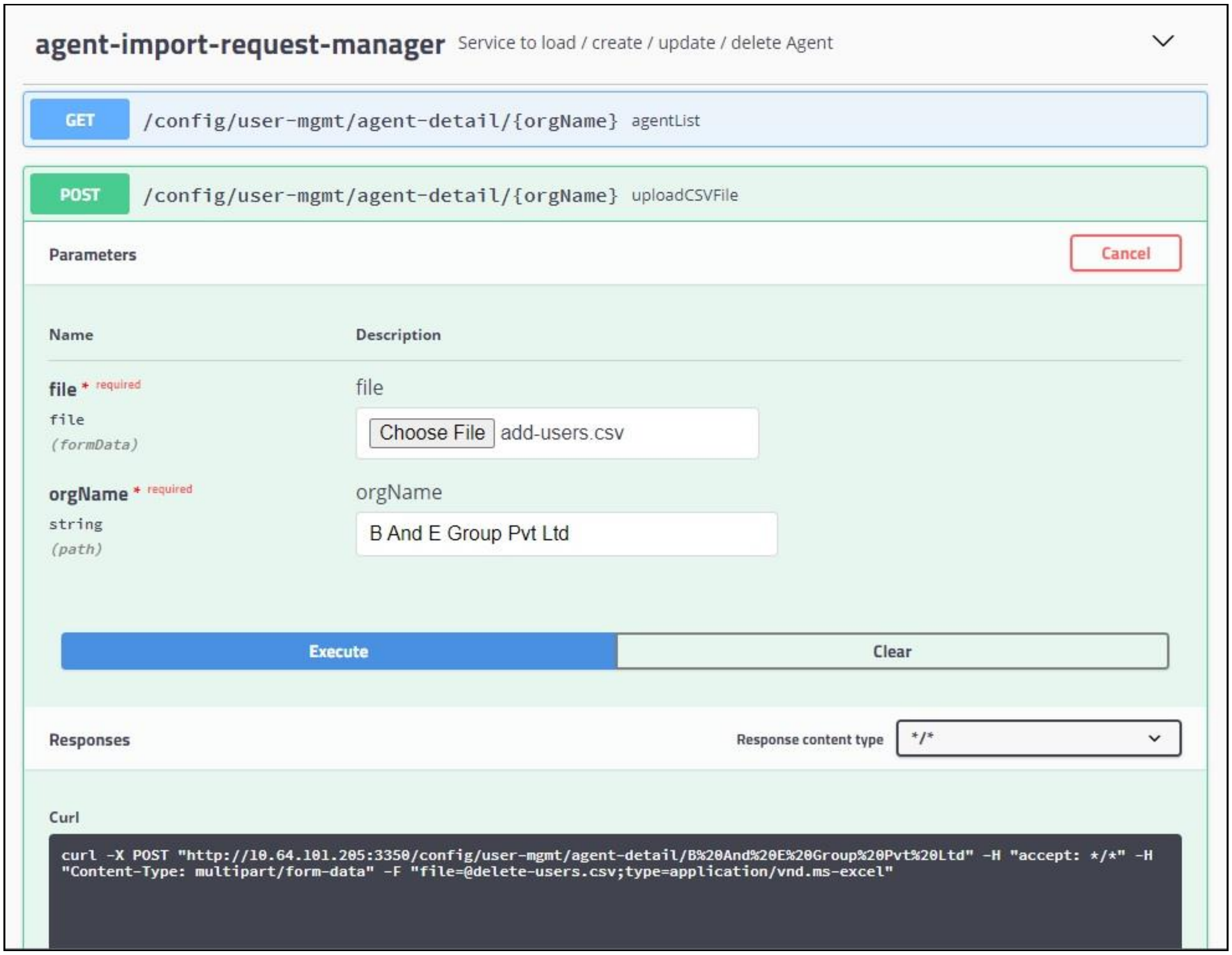
POST /config/user-mgmt/agent-detail/{orgName} uploadCSVFile

Parameters

Name	Description
file * required file *(formData)*	file
orgName * required string *(path)*	orgName

The screen is updated as shown below. For **file**, select **Choose File** and navigate to the agent user CSV file from **Section 9.2**.

Select **Execute**.



file: Choose File add-users.csv

orgName: B And E Group Pvt Ltd

Response content type: */*

```
curl -X POST "http://10.64.101.205:3350/config/user-mgmt/agent-detail/B%20And%20E%20Group%20Pvt%20Ltd" -H "accept: */*" -H
"Content-Type: multipart/form-data" -F "file=@delete-users.csv;type=application/vnd.ms-excel"
```

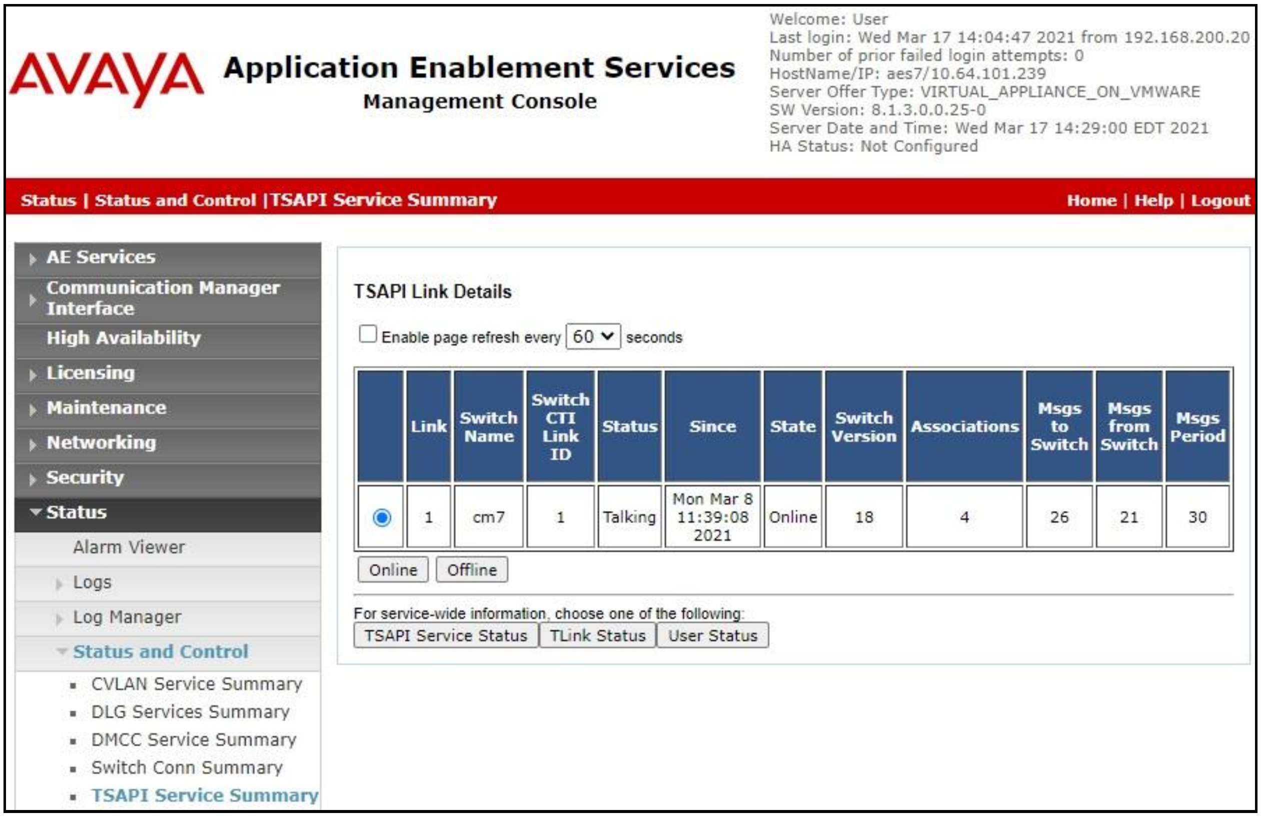
10. Verification Steps

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

10.1. 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".



Welcome: User
Last login: Wed Mar 17 14:04:47 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: Wed Mar 17 14:29:00 EDT 2021
HA Status: Not Configured

TSAPI Link Details

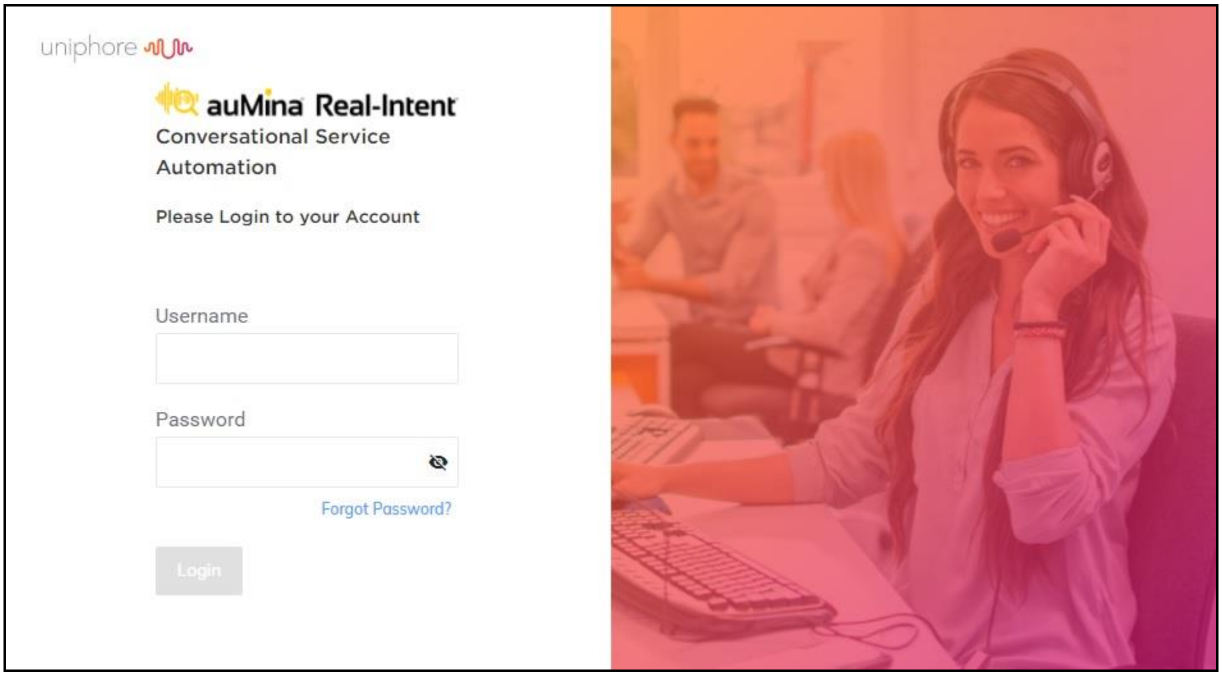
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Mon Mar 8 11:39:08 2021	Online	18	4	26	21	30

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

10.2. Verify SIPREC Transcription

From an agent PC, launch an Internet browser window and enter the URL "http://ip-address/login" where "ip-address" is the IP address of the Real Intent server with the UI component. Log in using an agent user credential from **Section 9.2**.



uniphore

auMina Real-Intent

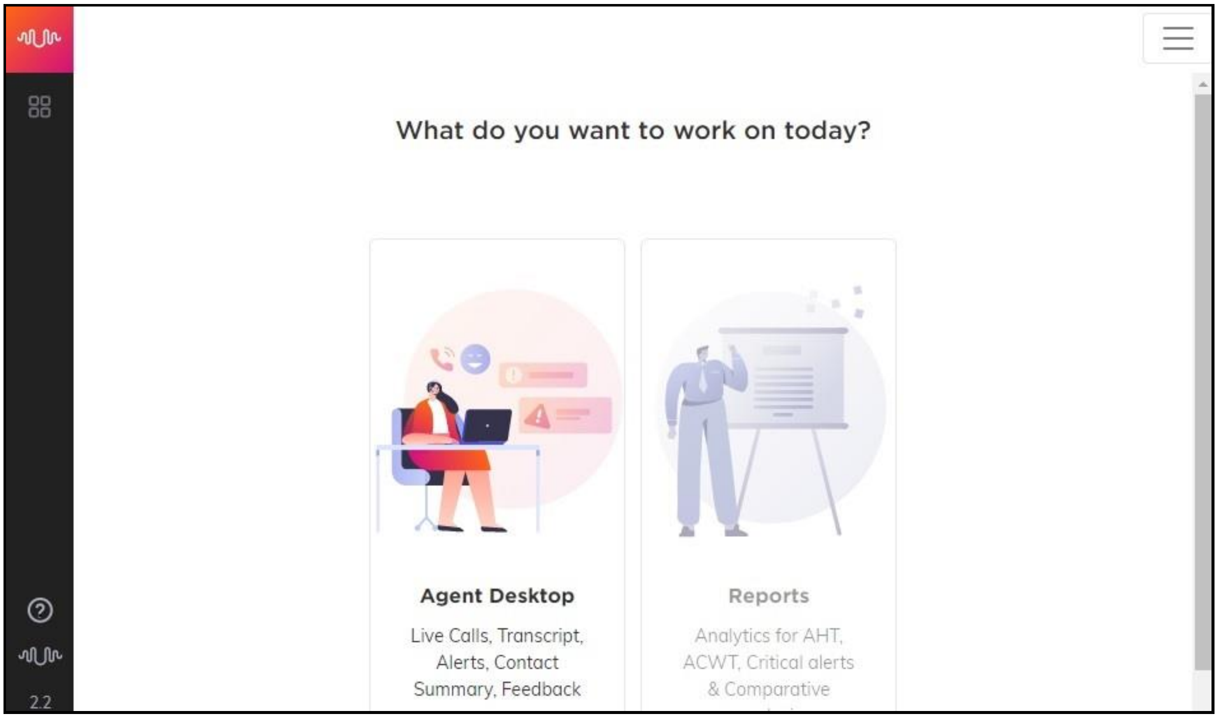
Conversational Service Automation

Please Login to your Account

Username

Password

The screen below is displayed. Click on **Agent Desktop**.



What do you want to work on today?

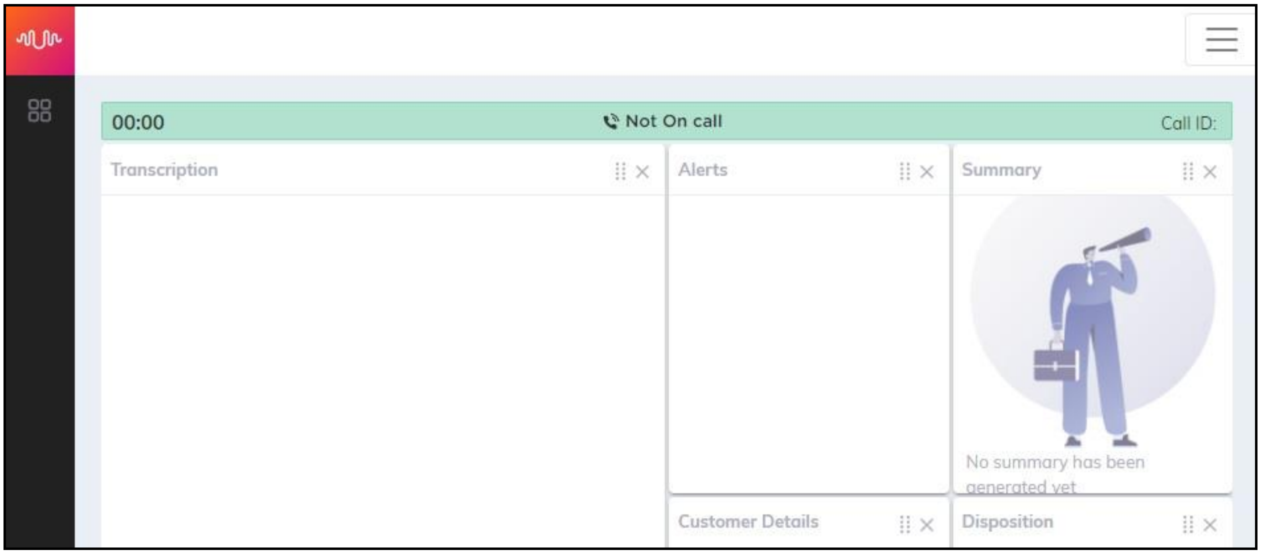
Agent Desktop

Live Calls, Transcript, Alerts, Contact Summary, Feedback

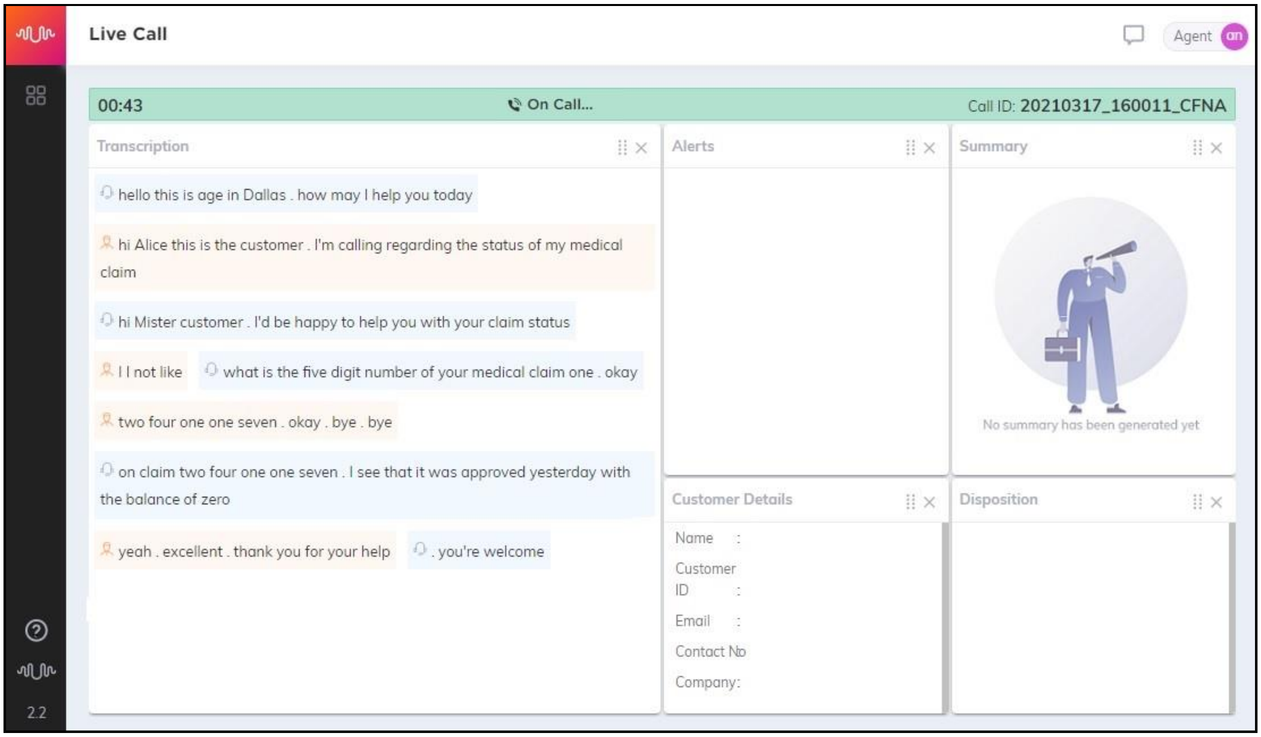
Reports

Analytics for AHT, ACWT, Critical alerts & Comparative

The screen below is displayed next.



Establish an ACD call with this agent. Verify that the screen is updated to reflect **On Call**, and that conversation text appears in the **Transcription** area as shown below.



Call ID: 20210317_160011_CFNA

hello this is age in Dallas . how may I help you today

hi Alice this is the customer . I'm calling regarding the status of my medical claim

hi Mister customer . I'd be happy to help you with your claim status

I I not like

what is the five digit number of your medical claim one . okay

two four one one seven . okay . bye . bye

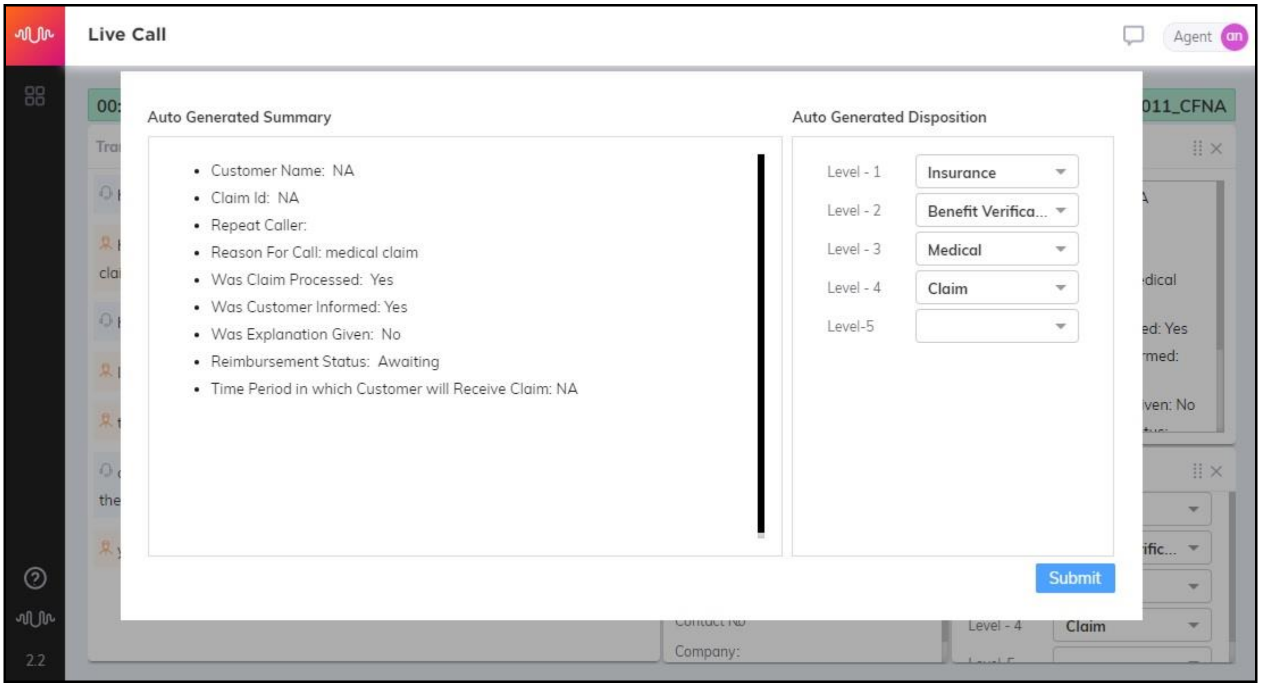
on claim two four one one seven . I see that it was approved yesterday with the balance of zero

yeah . excellent . thank you for your help

. you're welcome

Name :
Customer ID :
Email :
Contact No
Company:

Complete the active ACD call. Verify that the screen is updated with a pop-up box containing **Auto Generated Summary** and **Auto Generated Disposition** for the agent to review, update, and submit, as shown below.



Auto Generated Summary

- Customer Name: NA
- Claim Id: NA
- Repeat Caller:
- Reason For Call: medical claim
- Was Claim Processed: Yes
- Was Customer Informed: Yes
- Was Explanation Given: No
- Reimbursement Status: Awaiting
- Time Period in which Customer will Receive Claim: NA

Auto Generated Disposition

Level - 1	Insurance
Level - 2	Benefit Verifica...
Level - 3	Medical
Level - 4	Claim
Level-5	

11. Conclusion

These Application Notes describe the configuration steps required for Uniphore Real Intent 2.2 to successfully interoperate with Avaya Aura® Application Enablement Services 8.1.3 and Avaya Session Border Controller for Enterprise 8.1.3. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

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

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

4. *Uniphore Audio Logger Installation & Configuration Guide*, available at https://www.community.uniphore.com.

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.