DevConnect Program

Application Notes for IntraNext SmartSIP 10.4 with Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller 10.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IntraNext SmartSIP 10.4 to interoperate with Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller 10.1. IntraNext SmartSIP is a contact center solution.

In the compliance testing, IntraNext SmartSIP used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager to trigger start/stop of call recordings and the ability to collect DTMF digits via SIP INFO.

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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for IntraNext SmartSIP 10.4 to interoperate with Avaya Aura® Application Enablement Services 10.1, Avaya Aura® Session Manager 10.1 and Avaya Session Border Controller 10.1. IntraNext SmartSIP is a contact center solution.

In the compliance testing, IntraNext SmartSIP used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services (AES) to monitor agent stations on Avaya Aura® Communication Manager to trigger start/stop of call recordings and the ability to collect DTMF digits via SIP INFO while masking the tones from the agent on the call.

Intranext SmartSIP sits between Avaya Aura® Session Manager and Avaya Session Border Controller (SBC) and connects via SIP trunks. All inbound and outbound PSTN calls are routed through Intranext SmartSIP, which stays in the call path to facilitate call recordings.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent log in, SmartSIP used TSAPI to query and request monitoring on the agent station associated with the agent ID.

Incoming ACD calls were placed to, and outbound calls were placed from, available agents that were logged into a sample CRM system via the IntraNext Development Portal to verify the usage of the events from TSAPI to trigger stop/start of call recordings, and the ability to collect DTMF digits via SIP INFO.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the SmartSIP server.

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

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

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

For the testing associated with this Application Note, the interface between Avaya systems and SmartSIP utilized encrypted TSAPI with Application Enablement Services.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on SmartSIP:

- Use of TSAPI query services to query device information, name, agent state, and universal call ID.
- Use of TSAPI monitoring and event report services to monitor agent stations.
- Use of TSAPI snapshot services to obtain information on agent stations and existing calls.
- Ability to collect DTMF digits via SIP INFO and mask the tones to the agent.

The serviceability testing focused on verifying the ability of SmartSIP to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the SmartSIP server and clients.

2.2. Test Results

All test cases were executed and passed.

2.3. Support

Technical support on IntraNext SmartSIP can be obtained through the following:

- **Phone:** (800) 928-6398
- **Email :** support@intranext.com

3. Reference Configuration

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

In the compliance testing, SmartSIP monitored agent stations associated with the agent IDs shown in the table below. SmartSIP connects to SBC and Session Manager via SIP trunks.

Device Type	Extension
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882
Agent Password	65881, 65882

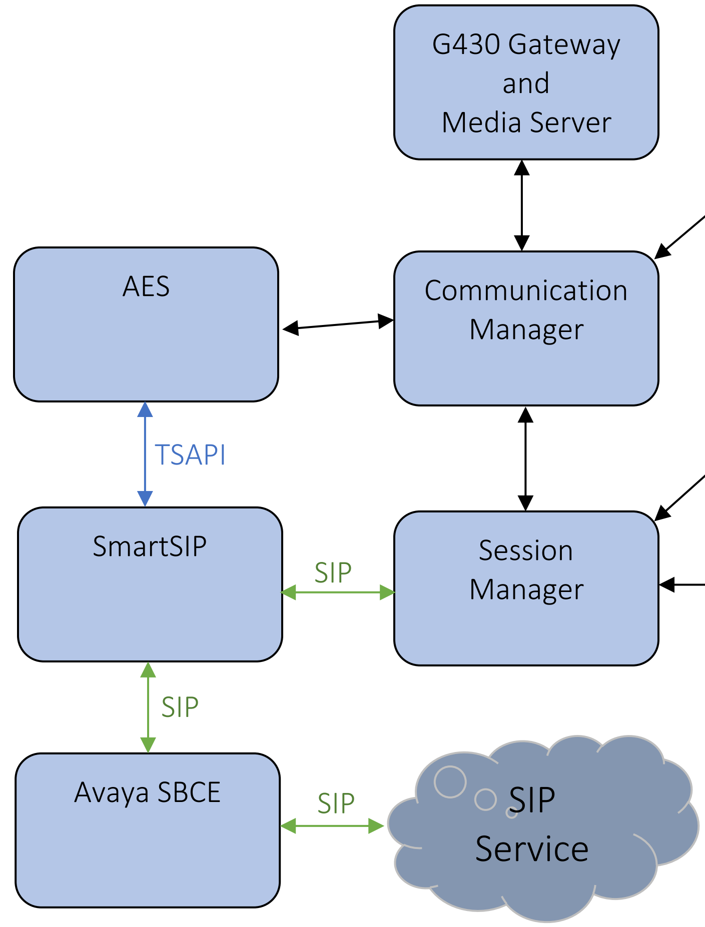


Figure 1: Test Configuration for IntraNext SmartSIP and Avaya Aura® Environment.

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	10.1.3 (10.1.3.0.1.974.27893)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1 (10.1.0.154)
Avaya Aura® Application Enablement Services in Virtual Environment	10.1. (10.1.3.0.0.11-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.3 (10.1.3.0.1013007)
Avaya Aura® System Manager in Virtual Environment	10.1.3 (10.1.3.0.0715713)
Avaya Session Border Controller in Virtual Environment	10.1 (10.1.2.0-64-23285)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Desk phone (H.323)	6.8.5.3.2
Avaya J169 IP Desk phone (SIP)	4.0.13.0.6
Avaya J179 IP Desk phone (H.323)	6.8.5.3.2
IntraNext SmartSIP Windows Server 2019 Standard • Avaya TSAPI Windows Client (csta32.dll)	10.4 Standard 8.1.3.25

5. Configure Avaya Aura® Communication Manager

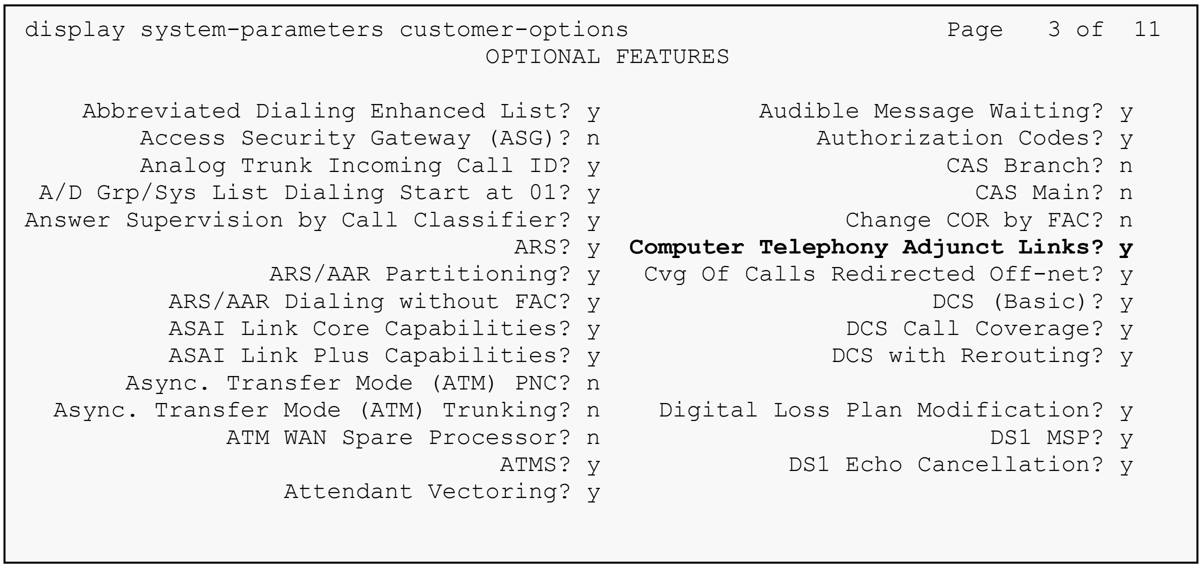
This section contains steps necessary to configure SmartSIP successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that the following features are enabled.

One Page 3, verify **Computer Telephone Adjunct Links** is set to **y.**

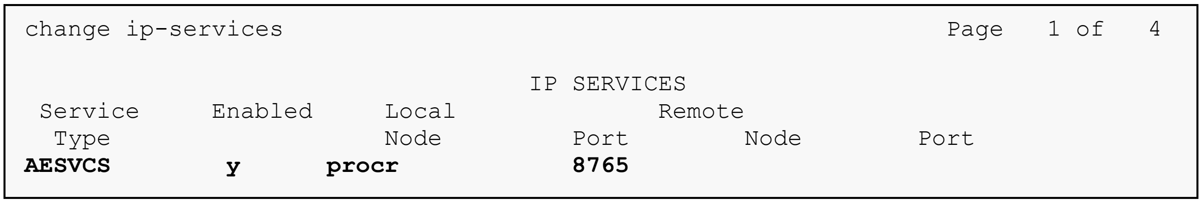


```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    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
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

5.2. Configure IP Services

CTI connectivity to AES is required as SmartSIP monitors agent stations via TSAPI. Add an IP-Services entry, using the **change ip-services** command, for AES as described below. On Page 1:

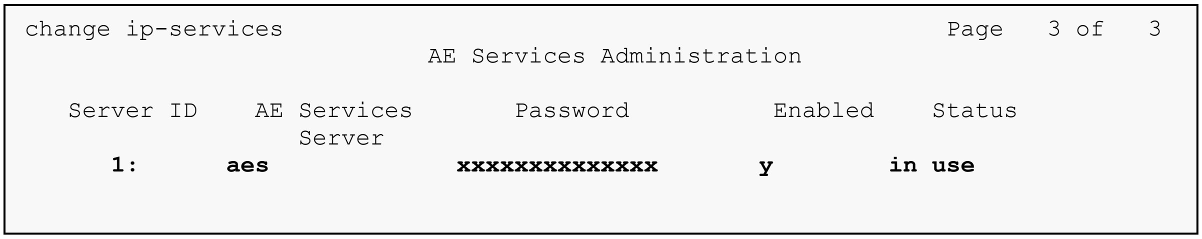
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.



```
change ip-services                                              Page   1 of   4

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

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6**, **Step 1**.
- In the **Enabled** field, type **y**.

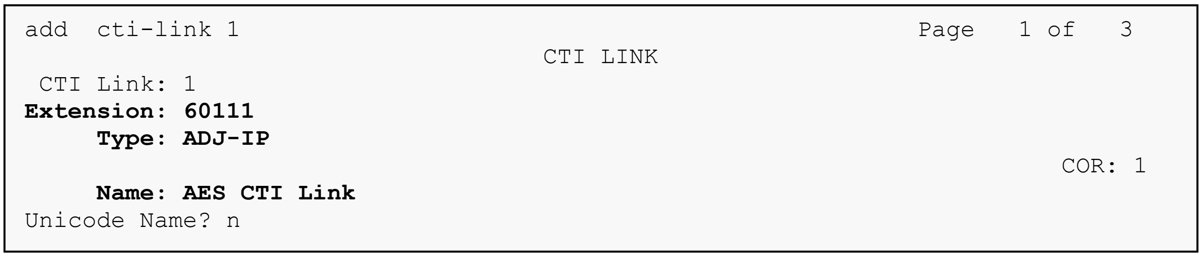


```
change ip-services                                              Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password         Enabled    Status
                   Server
      1:      aes             xxxxxxxxxxxxxx       y        in use
```

5.3. Configure CTI Link

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

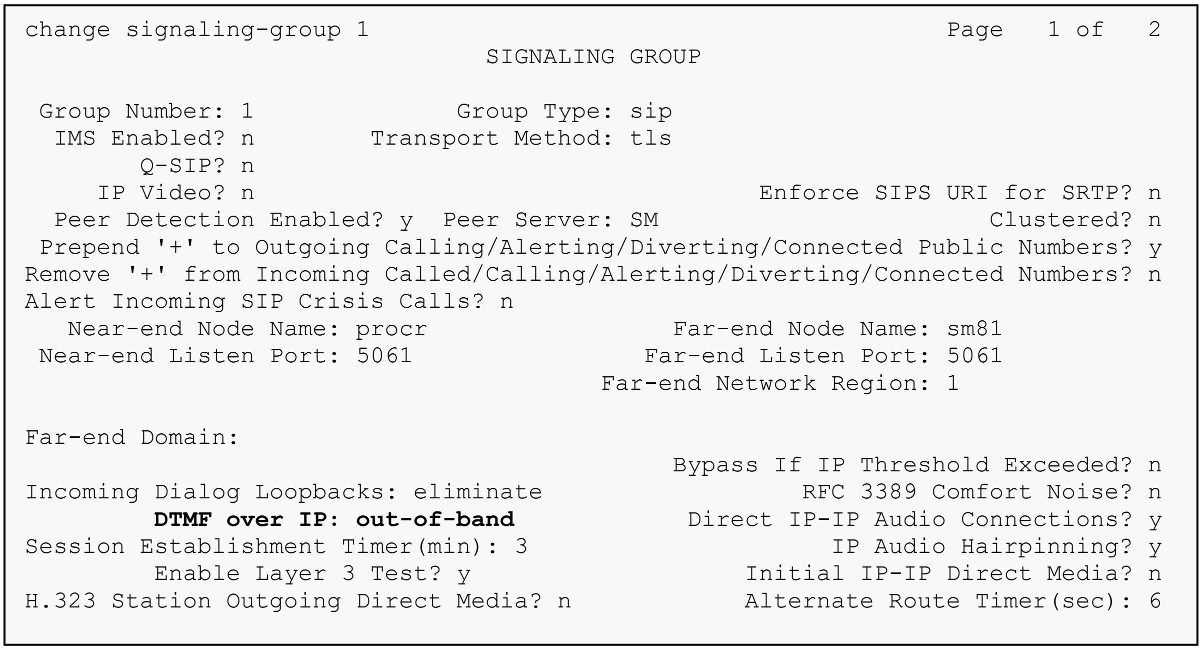
- In the **Extension** field, type a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.



```
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
```

5.4. Configure SIP INFO

During the compliance test, existing SIP signaling and trunk group to Session Manager were used. However, note that SIP INFO needs to be enabled on the signaling group. This enables all the Avaya endpoints to send SIP INFO for DTMF transmission. SIP INFO messages are used by SmartSIP to collect DTMF. Enter the **change signaling-group <n>** command where **<n>** is the signaling group used for Session Manager. Set the **DTMF over IP** to **out-of-band.** All calls that route over this trunk group will leverage SmartSIP.



```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                       Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                 Far-end Node Name: sm81
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: out-of-band            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? y
         Enable Layer 3 Test? y                   Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

6. Configure Avaya Aura® Application Enablement Services

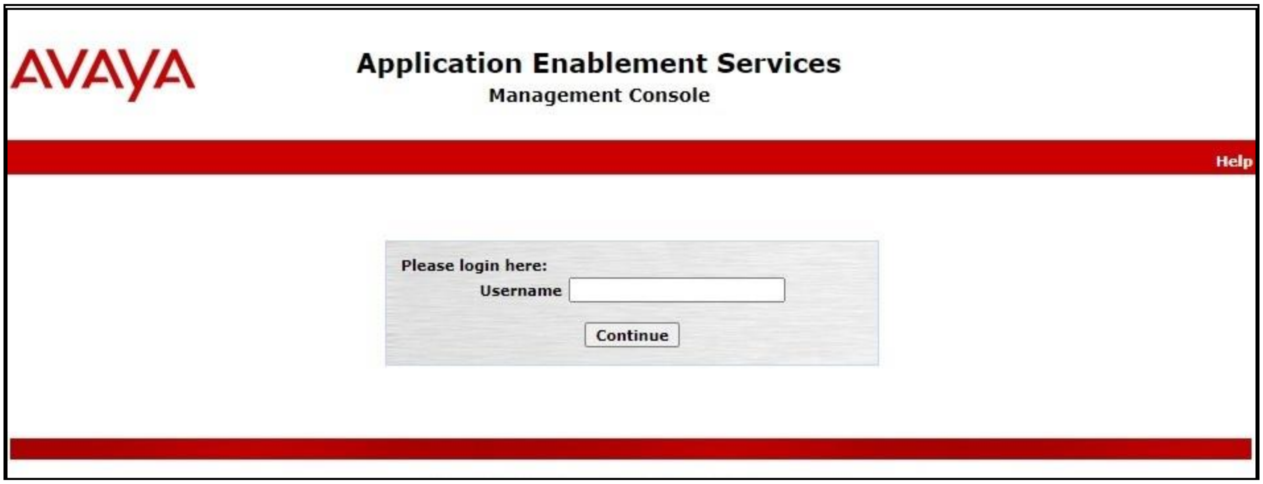
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

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

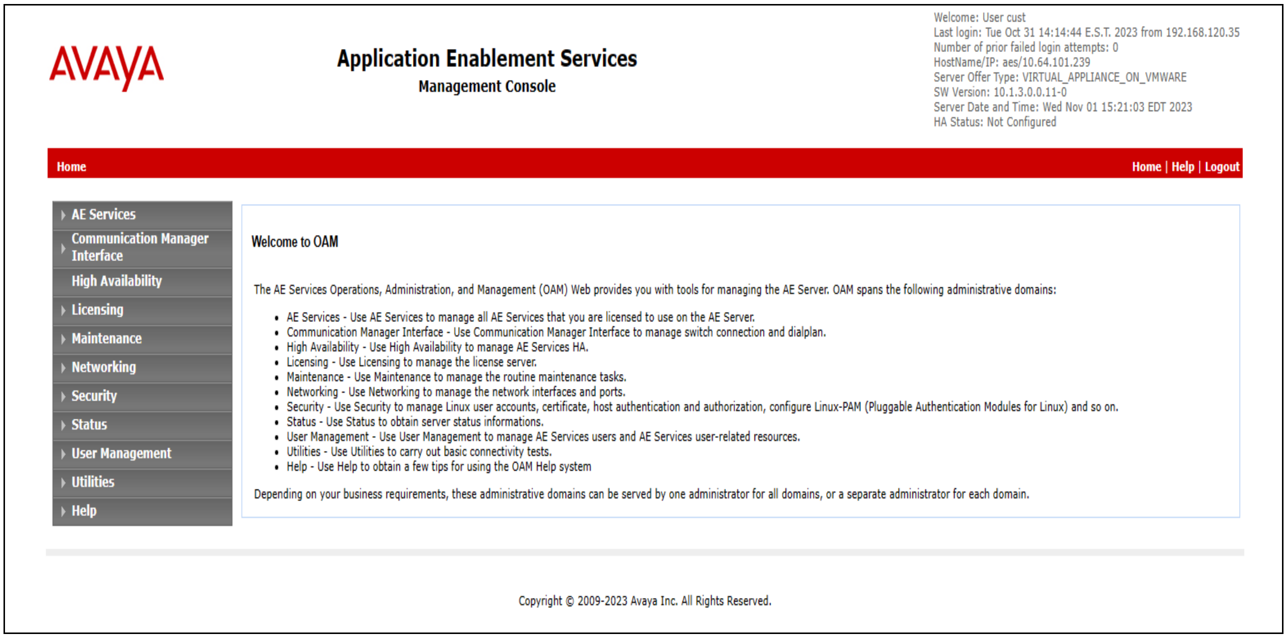
6.1. Launch OAM Interface

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 **Please login here** screen is displayed. Log in using the appropriate credentials.



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



Welcome: User cust
Last login: Tue Oct 31 14:14:44 E.S.T. 2023 from 192.168.120.35
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Wed Nov 01 15:21:03 EDT 2023
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:

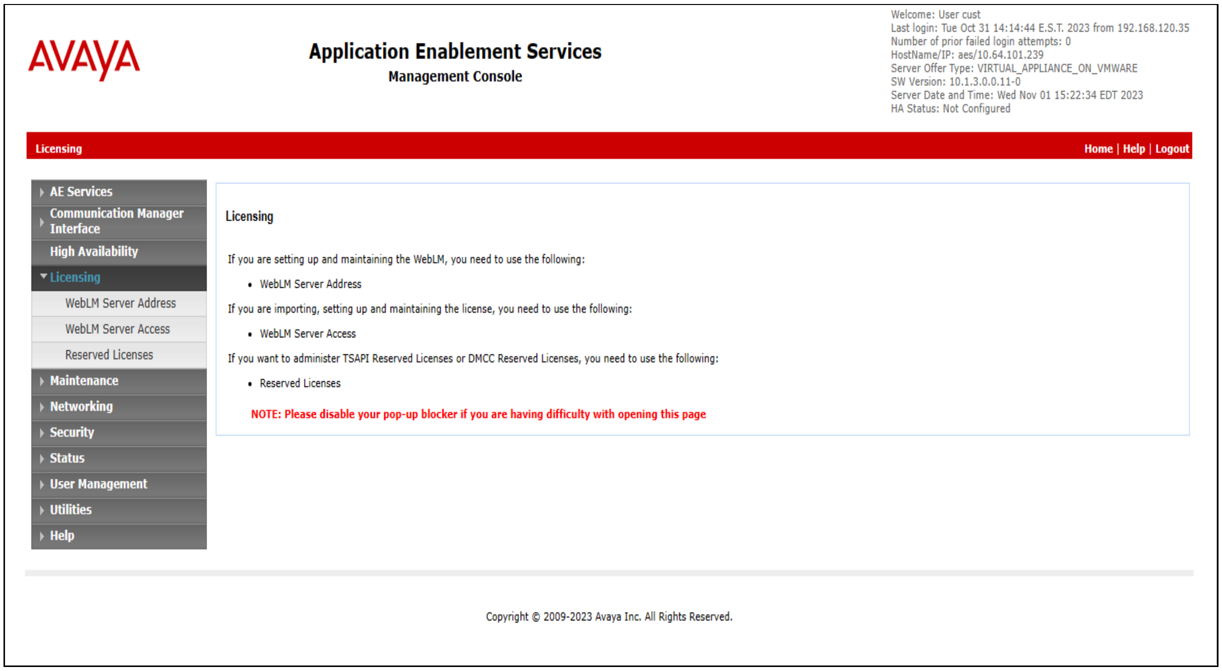
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - 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.

Copyright © 2009-2023 Avaya Inc. All Rights Reserved.

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 cust
Last login: Tue Oct 31 14:14:44 E.S.T. 2023 from 192.168.120.35
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Wed Nov 01 15:22:34 EDT 2023
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:

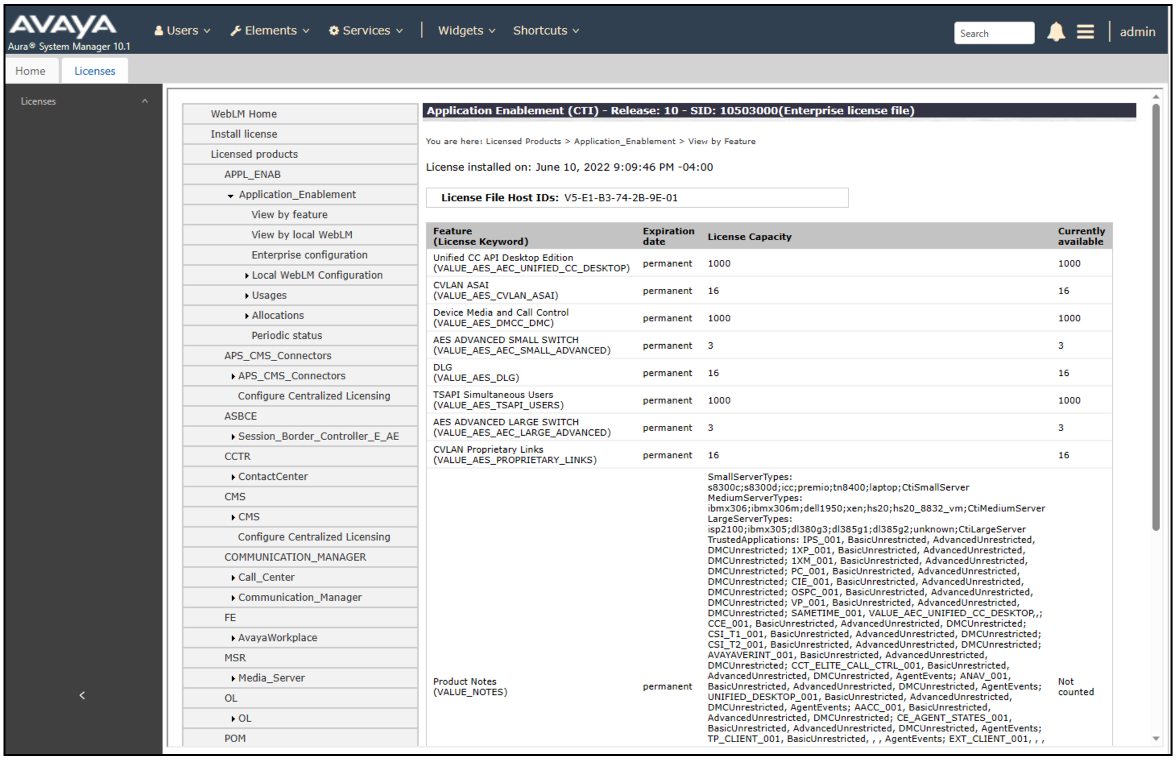
- Reserved Licenses

NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Copyright © 2009-2023 Avaya Inc. All Rights Reserved.

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: 10 - SID: 10503000(Enterprise license file)

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

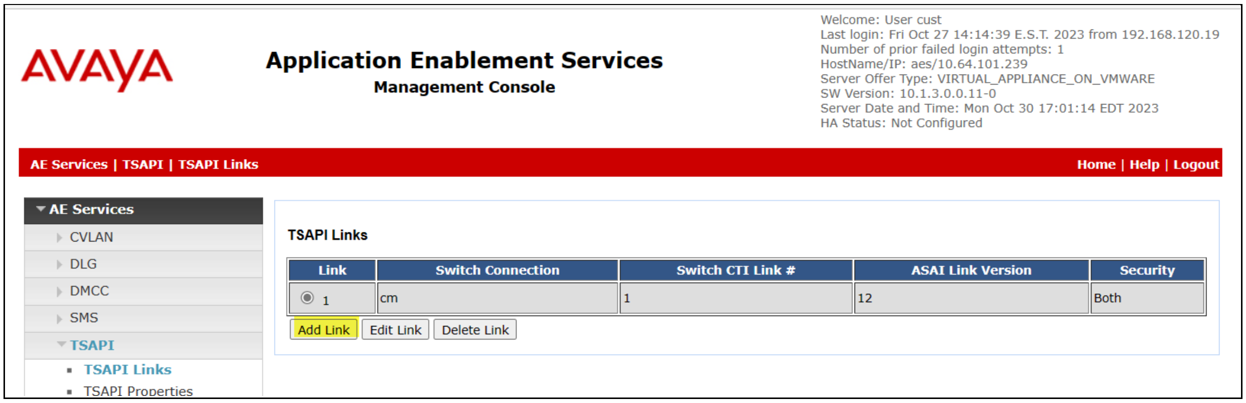
License installed on: June 10, 2022 9:09:46 PM -04:00

License File Host IDs: V5-E1-B3-74-2B-9E-01

Feature (License Keyword)	Expiration date	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	3
DLG (VALUE_AES_DLG)	permanent	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	16
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_001, , ,	Not counted

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**.



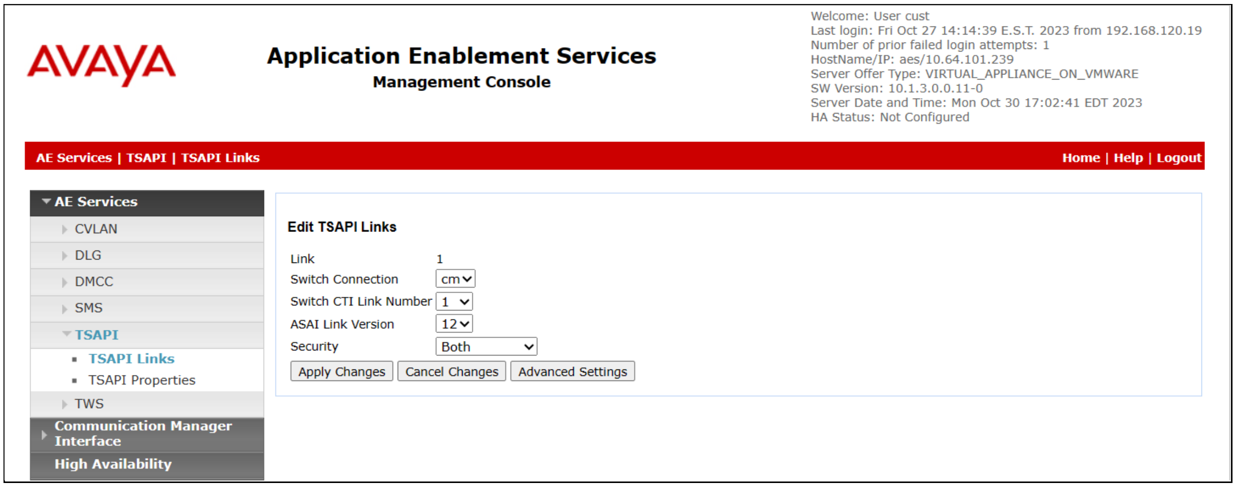
Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:01:14 EDT 2023
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
◉ 1	cm	1	12	Both

The **Add TSAPI Links** screen is displayed next. Set the following values for the specified fields and retain the default values for the remaining fields.

- **Link:** An available link number.
- **Switch Connection:** The relevant switch connection, in this case "cm."
- **Switch CTI Link Number:** The CTI link number from **Section** Error! Reference source not found..
- **ASAI Link Version:** 12
- **Security:** "Encrypted" or "Both" to allow for encrypted connection.



Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:02:41 EDT 2023
HA Status: Not Configured

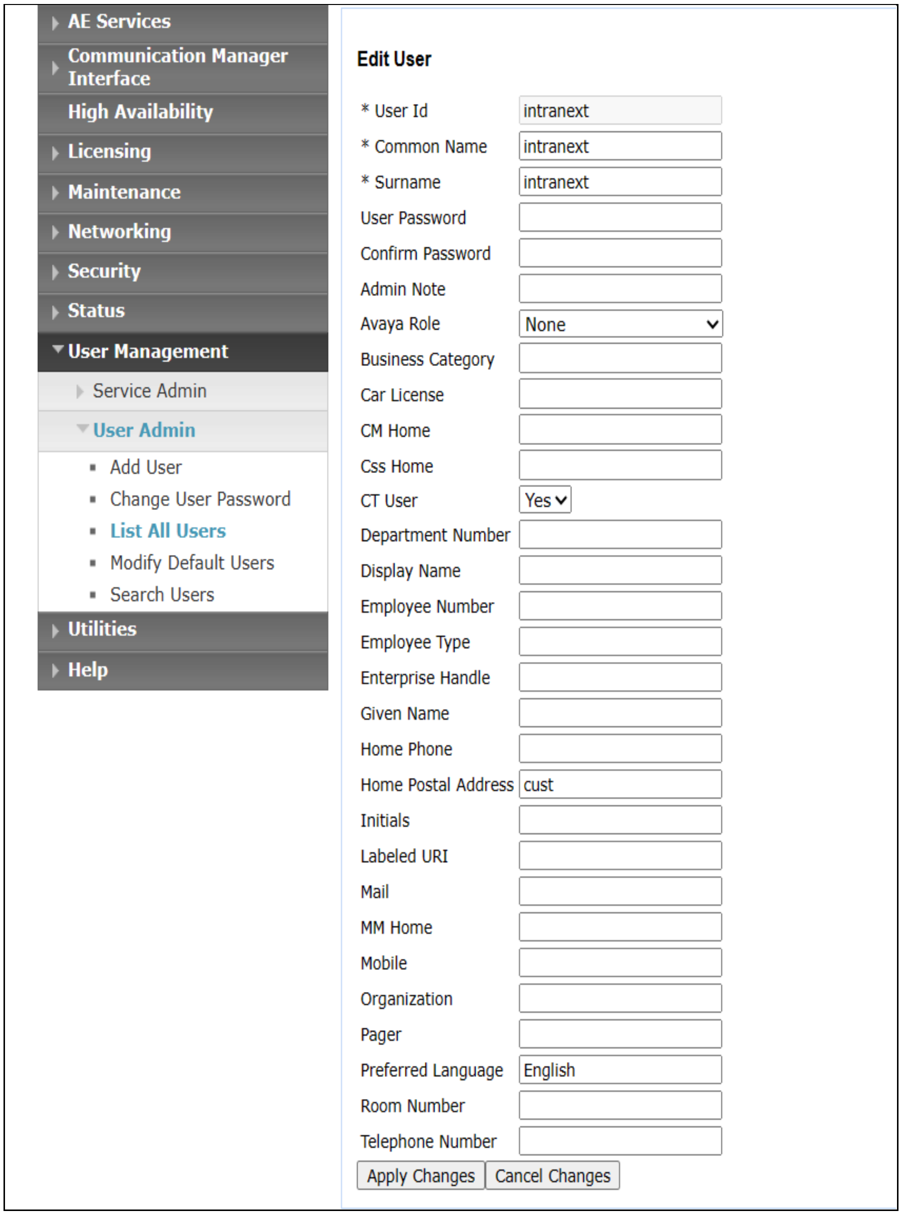
Edit TSAPI Links

Link	1
Switch Connection	cm
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

6.4. Administer IntraNext 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.



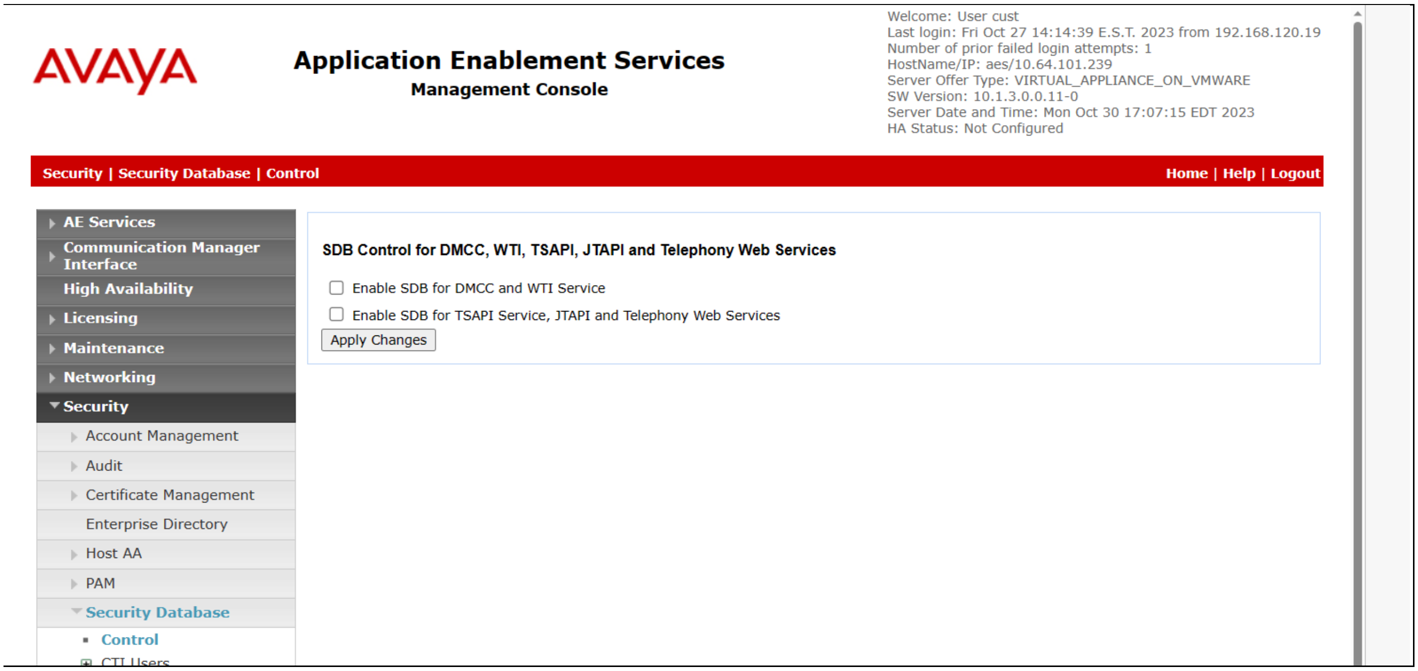
Edit User

* User Id	intranext
* Common Name	intranext
* Surname	intranext
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	
Home Phone	
Home Postal Address	cust
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

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 that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [**2**] to configure access privileges for the IntraNext user from **Section 0**.



Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:07:15 EDT 2023
HA Status: Not Configured

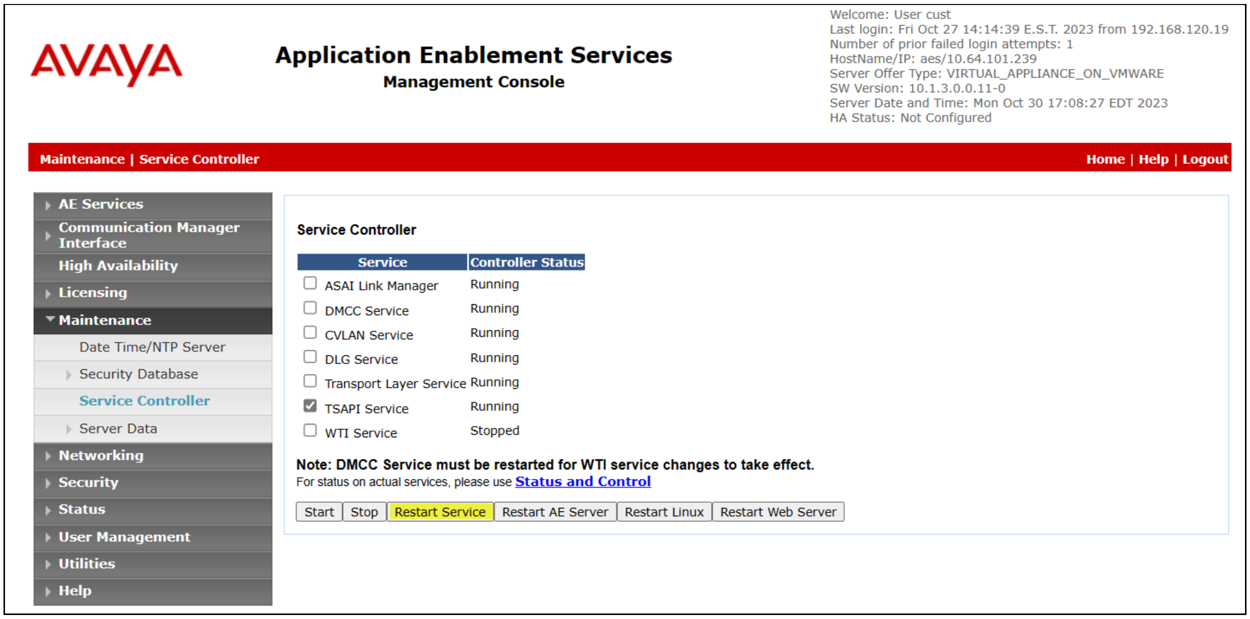
SDB Control for DMCC, WTI, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC and WTI Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

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** and click **Restart Service**.



Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:08:27 EDT 2023
HA Status: Not Configured

Service Controller

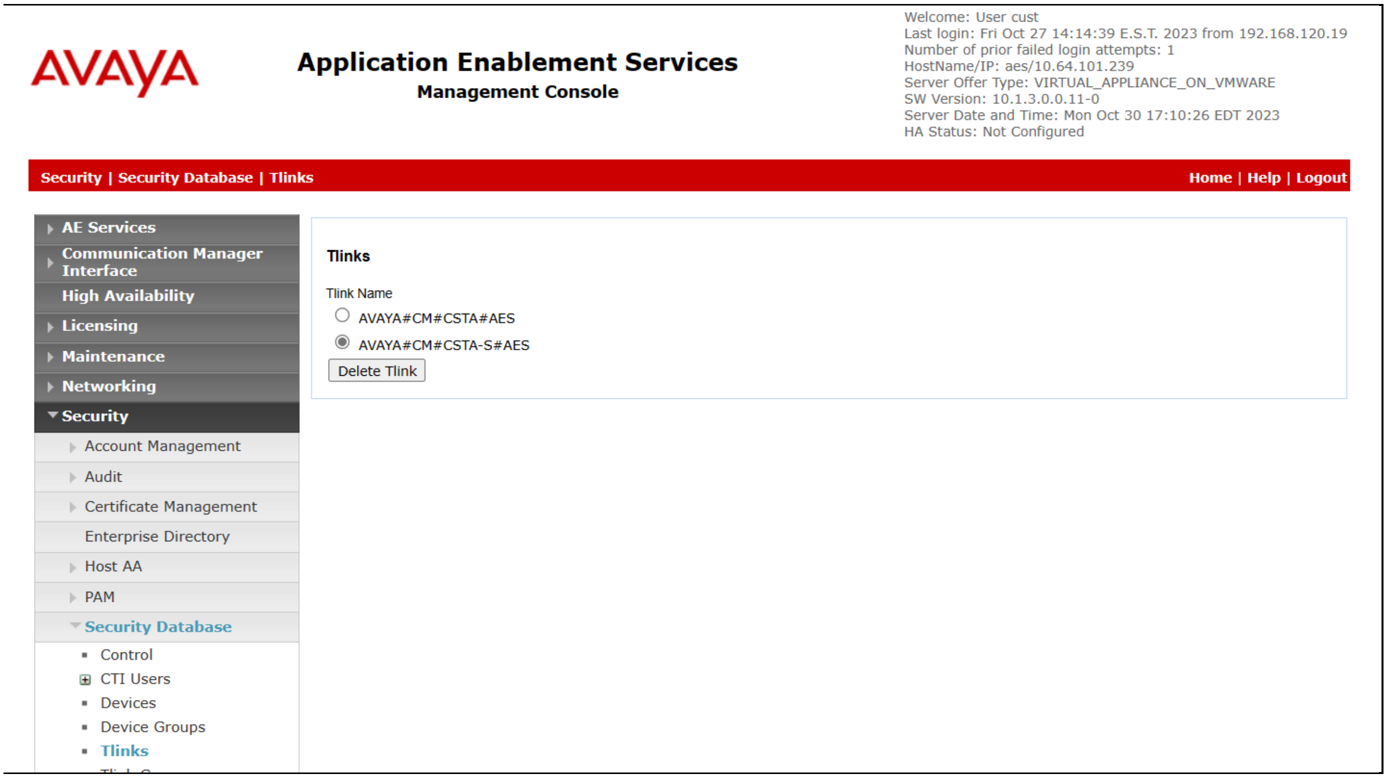
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running
□ WTI Service	Stopped

Note: DMCC Service must be restarted for WTI service changes to take effect.
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 pertinent Tlink name, to be used later to share with Event Intelligence. In this case, the pertinent Tlink name for encrypted connection is "**AVAYA#CM#CSTA-S#AES**" as shown below.



Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:10:26 EDT 2023
HA Status: Not Configured

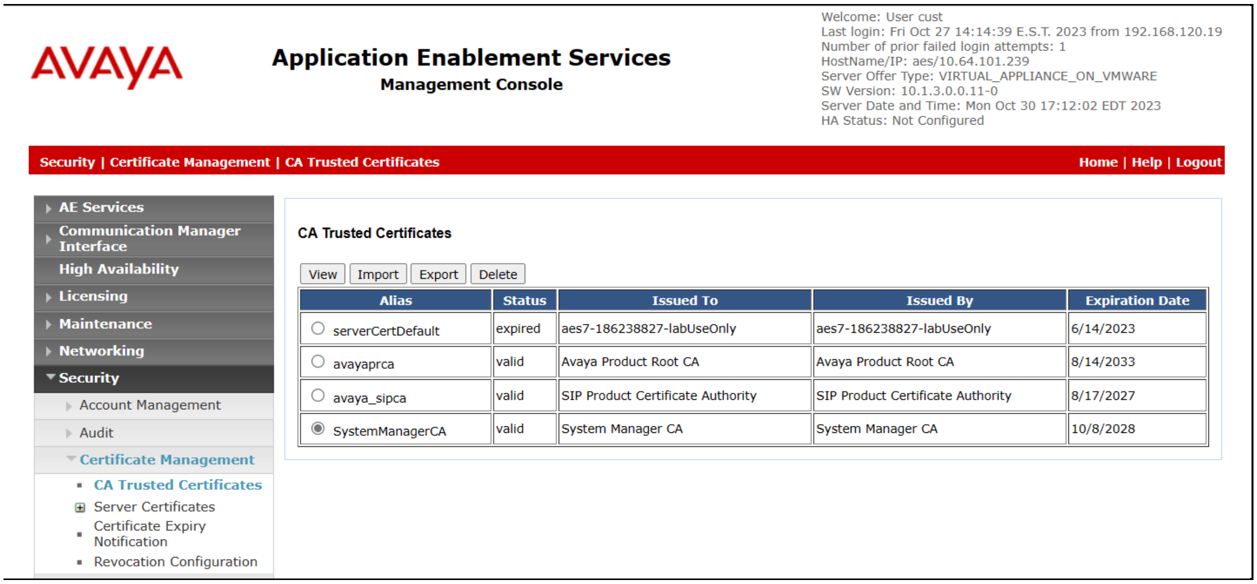
Tlinks

Tlink Name

○ AVAYA#CM#CSTA#AES
● AVAYA#CM#CSTA-S#AES

6.8. 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**.

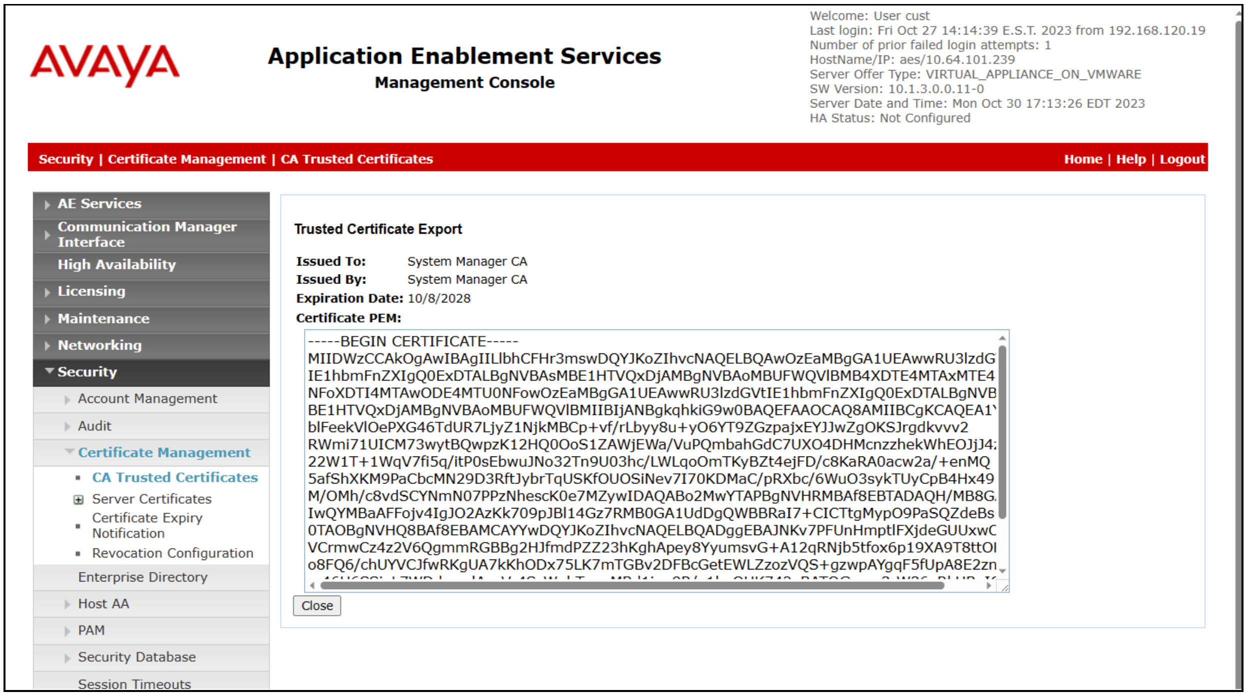


Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:12:02 EDT 2023
HA Status: Not Configured

CA Trusted Certificates

Alias	Status	Issued To	Issued By	Expiration Date
○ serverCertDefault	expired	aes7-186238827-labUseOnly	aes7-186238827-labUseOnly	6/14/2023
○ avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	8/14/2033
○ avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	8/17/2027
● SystemManagerCA	valid	System Manager CA	System Manager CA	10/8/2028

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



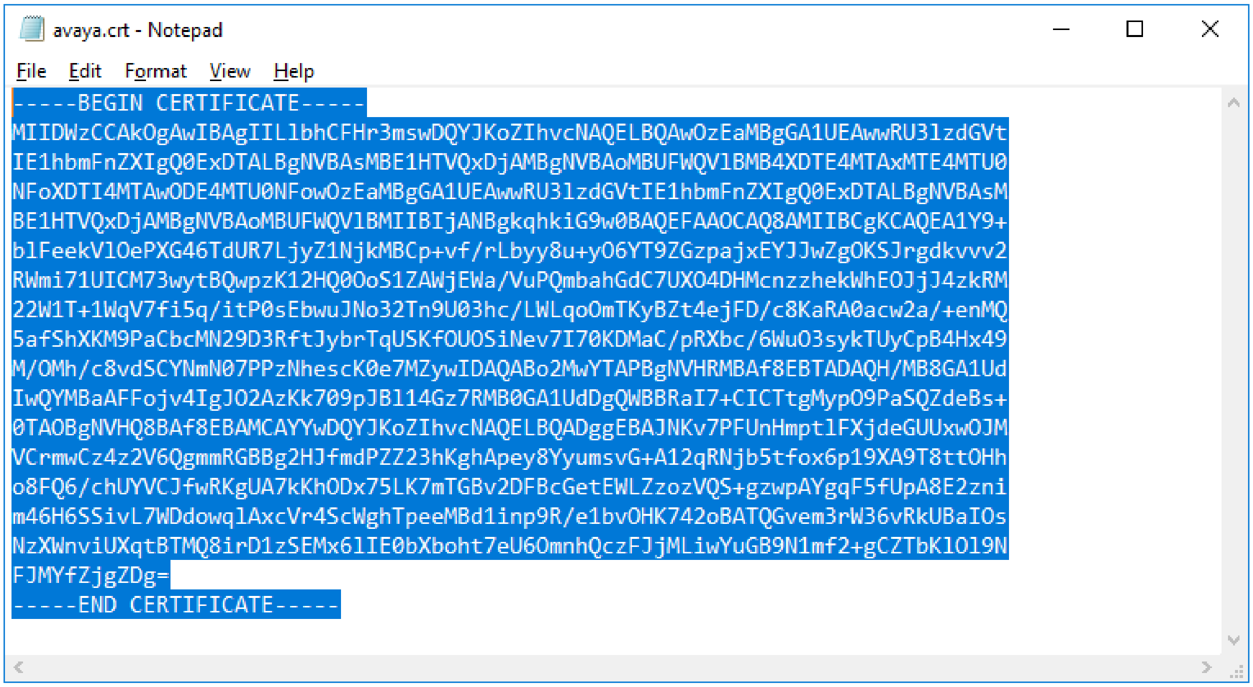
Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:13:26 EDT 2023
HA Status: Not Configured

Trusted Certificate Export

Issued To: System Manager CA
Issued By: System Manager CA
Expiration Date: 10/8/2028
Certificate PEM:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdG
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVB
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8G
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwC
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOI
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zn
```

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



```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdGVt
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQV1BMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBgNVBAoMBUFWQV1BMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs+
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOHh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx6lIE0bXboht7eU6OmnhQczFJjMLiwYuGB9N1mf2+gCZTbK1O19N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

7. Configure Avaya Aura® Session Manager

SmartSIP sits between Session Manager and Avaya SBC. All inbound and outbound calls to PSTN are routed via SmartSIP, followed by Avaya SBC. A SIP trunk needs to be configured for SmartSIP and Avaya SBC. A SIP trunk for Communication Manager was preconfigured and is out of scope for this document. All configuration for Session Manager is performed via System Manager web interface. Open a web browser session to System Manager URL.

7.1. Administer SIP Entities

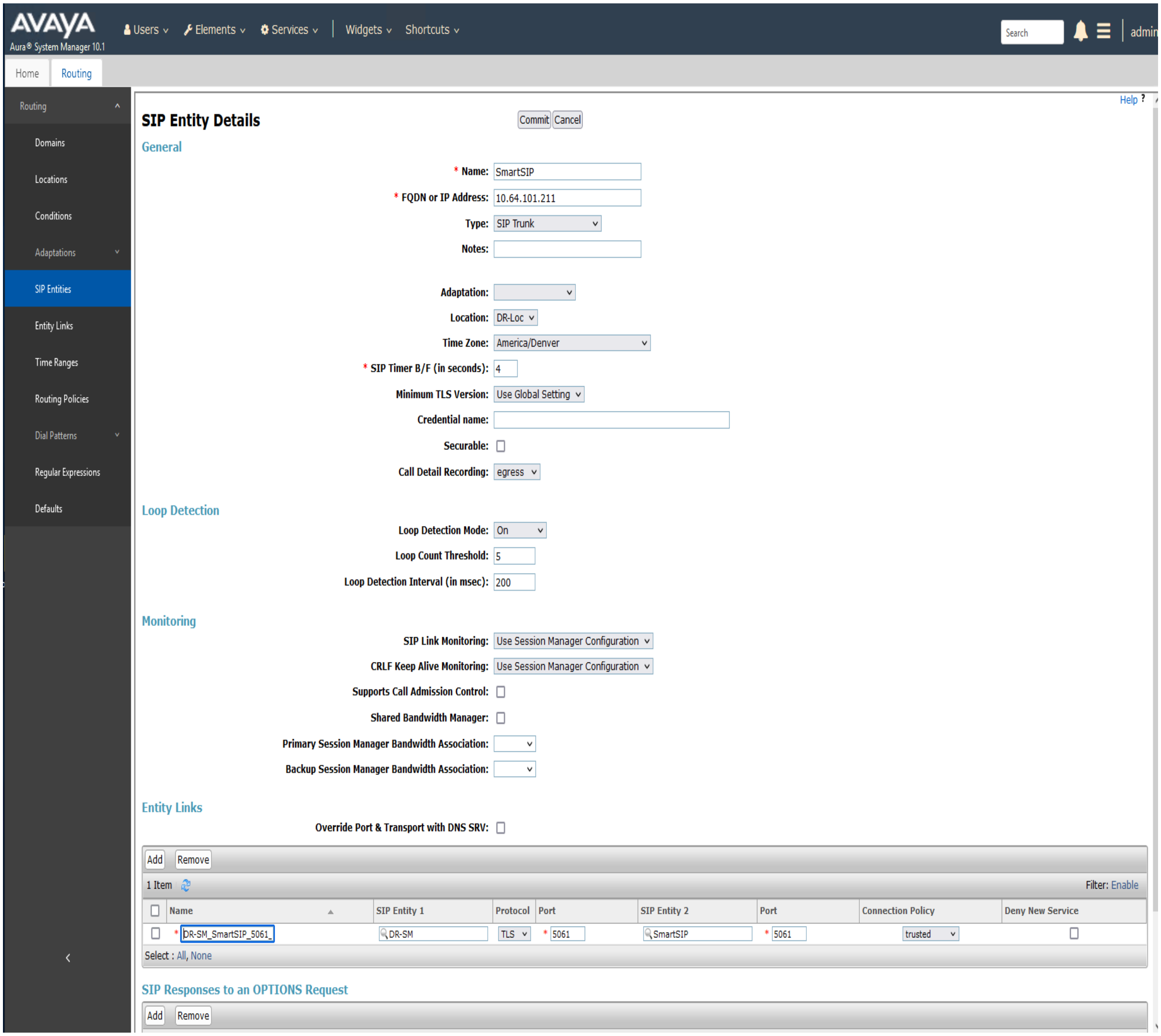
Add two new SIP entities, one for SmartSIP and another one for Avaya SBC.

7.1.1. SIP Entity for SmartSIP

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for SmartSIP.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The SIP IP address of SmartSIP.
- **Type:** "SIP Trunk"
- **Location:** Select a preconfigured Location.
- **Time Zone:** Select the applicable time zone.



SIP Entity Details

General

* Name:	SmartSIP
* FQDN or IP Address:	10.64.101.211
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	DR-Loc
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	egress

Loop Detection

Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

Monitoring

SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□
Primary Session Manager Bandwidth Association:	
Backup Session Manager Bandwidth Association:	

Entity Links

Override Port & Transport with DNS SRV: □

1 Item

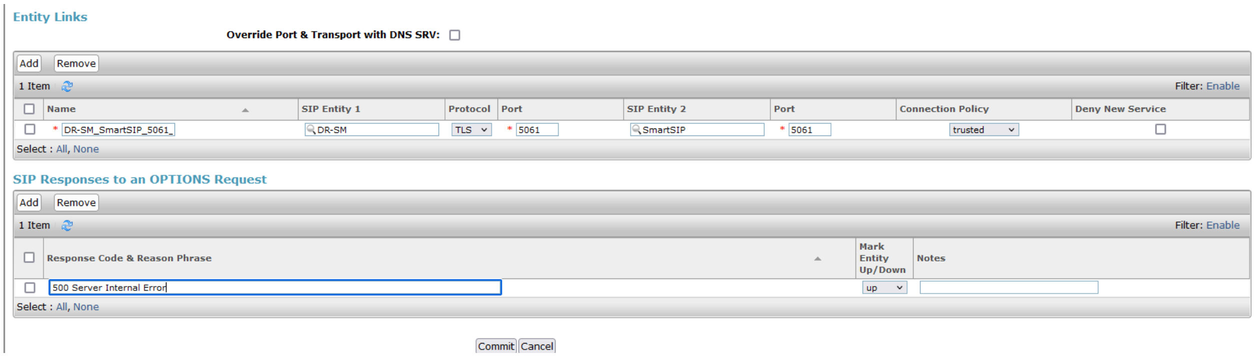
□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* DR-SM_SmartSIP_5061_	DR-SM	TLS	* 5061	SmartSIP	* 5061	trusted	□

SIP Responses to an OPTIONS Request

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

Name:	A descriptive name.
SIP Entity 1:	The Session Manager entity name, in this case "DR-SM".
Protocol:	"TLS"
Port:	"5061"
SIP Entity 2:	The SmartSIP entity name from this section.
Port:	"5061"
Connection Policy:	"trusted"

Note that SmartSIP can support TLS and TCP, but during the compliance testing TLS was used.



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* DR-SM_SmartSIP_5061_	DR-SM	TLS	* 5061	SmartSIP	* 5061	trusted	□

SIP Responses to an OPTIONS Request

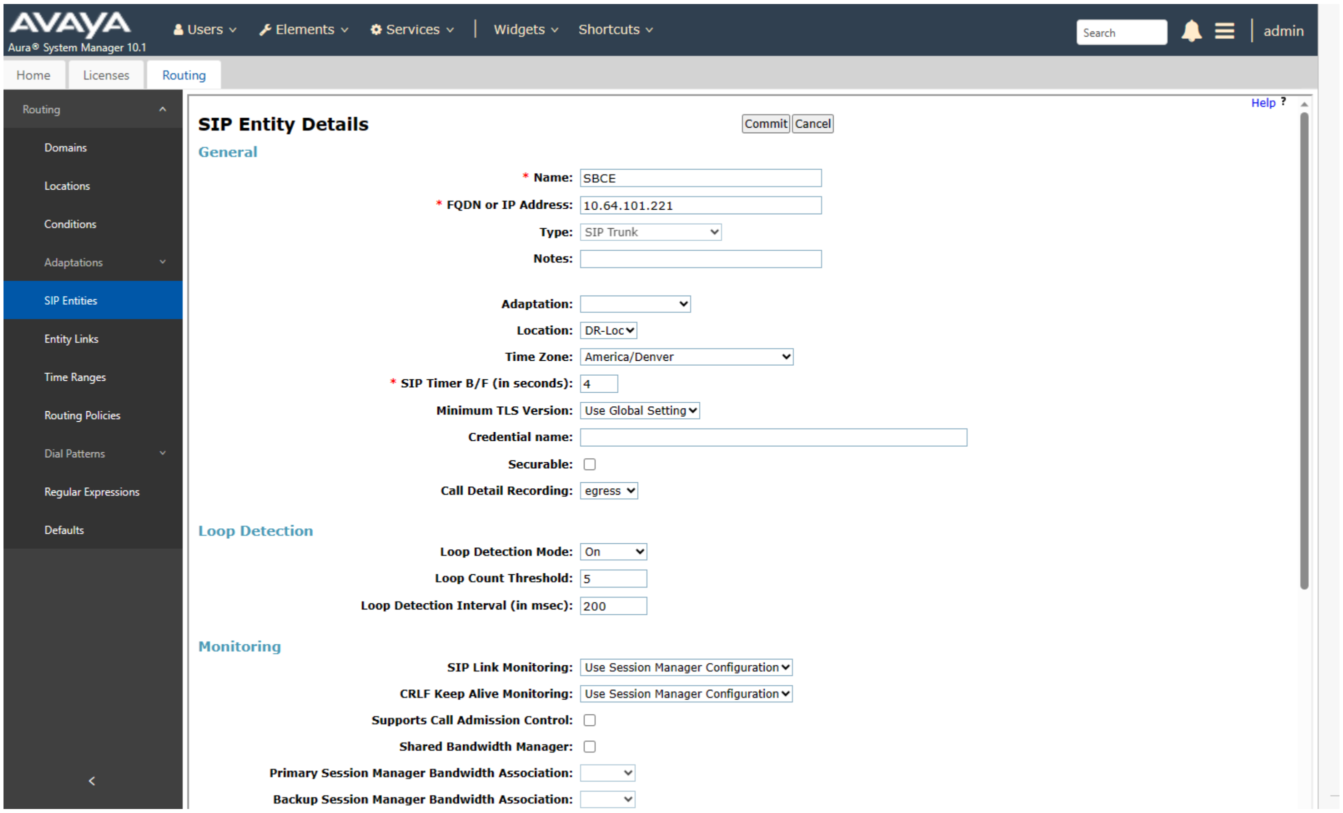
□	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
□	500 Server Internal Error	up	

7.1.2. SIP Entity for Avaya SBC

Select **Routing → SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Avaya SBC. Note that this SIP entity is used for failover purposes when connectivity to SmartSIP in unavailable.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The internal SIP IP address of Avaya SBC.
- **Type:** “SIP Trunk”
- **Notes:** Any desired notes.
- **Location:** Select the applicable location.
- **Time Zone:** Select the applicable time zone.



SIP Entity Details

General

* Name:	SBCE
* FQDN or IP Address:	10.64.101.221
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	DR-Loc
Time Zone:	America/Denver
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	egress

Loop Detection

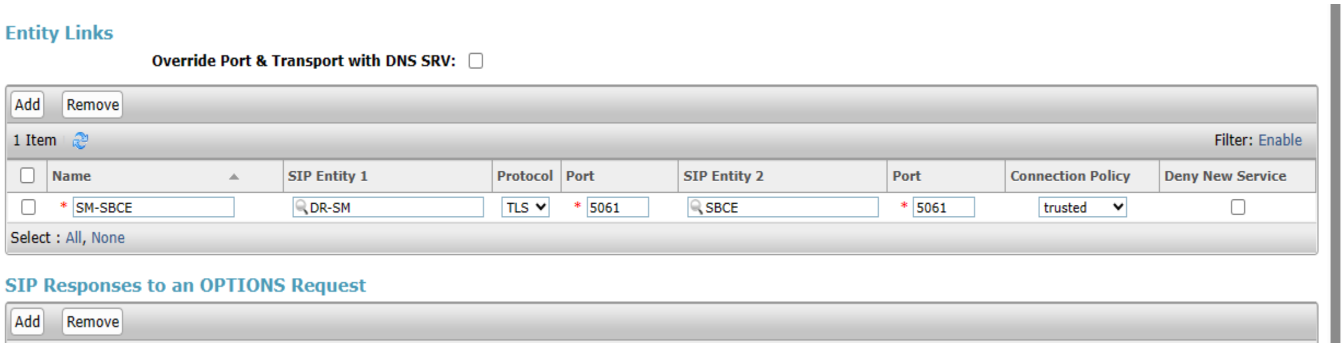
Loop Detection Mode:	On
Loop Count Threshold:	5
Loop Detection Interval (in msec):	200

Monitoring

SIP Link Monitoring:	Use Session Manager Configuration
CRLF Keep Alive Monitoring:	Use Session Manager Configuration
Supports Call Admission Control:	□
Shared Bandwidth Manager:	□
Primary Session Manager Bandwidth Association:	
Backup Session Manager Bandwidth Association:	

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case "sm81".
- **Protocol:** "TLS"
- **Port:** "5061"
- **SIP Entity 2:** The Avaya SBCE entity name from this section.
- **Port:** "5061"
- **Connection Policy:** "trusted"



Entity Links

Override Port & Transport with DNS SRV: □

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
□	* SM-SBCE	DR-SM	TLS	* 5061	SBCE	* 5061	trusted	□

SIP Responses to an OPTIONS Request

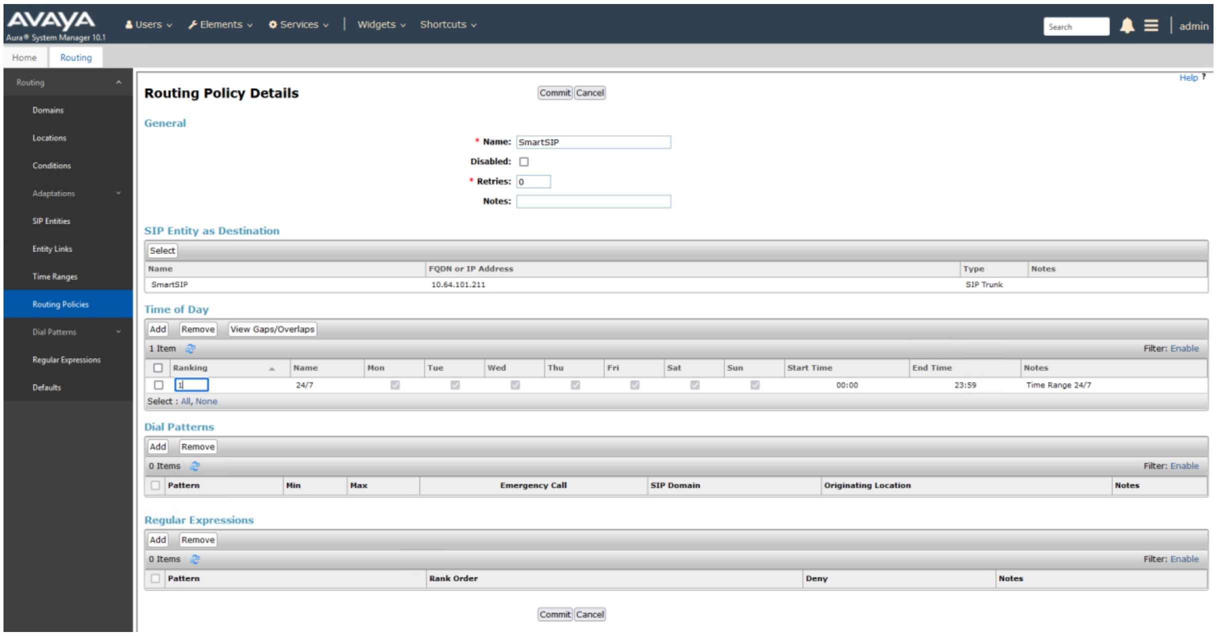
7.2. Administer Routing Policies

Add a new routing policy for routing calls to SmartSIP and Avaya SBC.

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the SmartSIP entity name from **Section 7.1.1**. The screen below shows the result of the selection. Under the **Time of Day** subsection, set the **Ranking** to **1.**



Routing Policy Details

General

* Name: SmartSIP

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SmartSIP	10.64.101.211	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	1	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

0 Items Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes

Regular Expressions

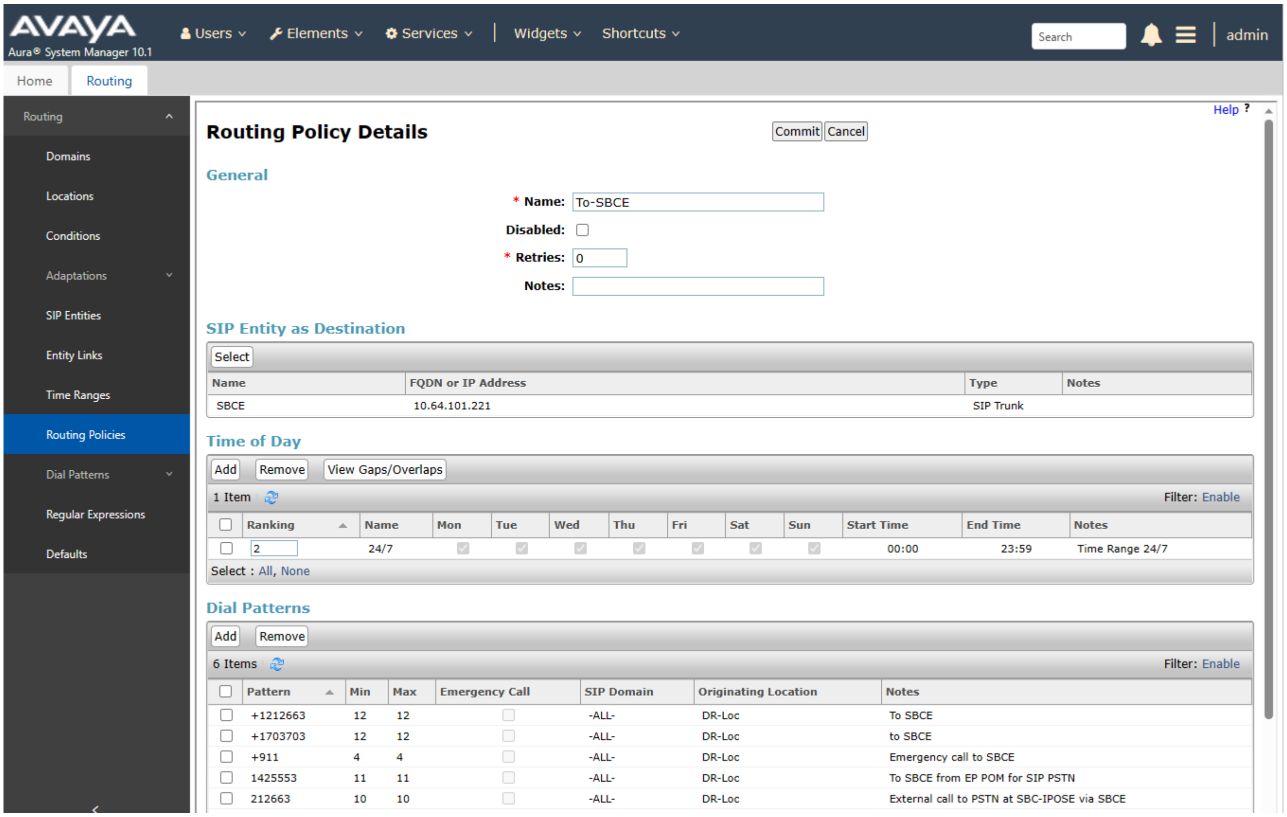
Add Remove

0 Items Filter: Enable

□	Pattern	Rank Order	Deny	Notes

Commit Cancel

Similarly, add a **Routing Policy** for Avaya SBCE and configure the **Time of Day Ranking** to **2.**



Routing Policy Details

General

* Name: To-SBCE

Disabled: □

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCE	10.64.101.221	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	2	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

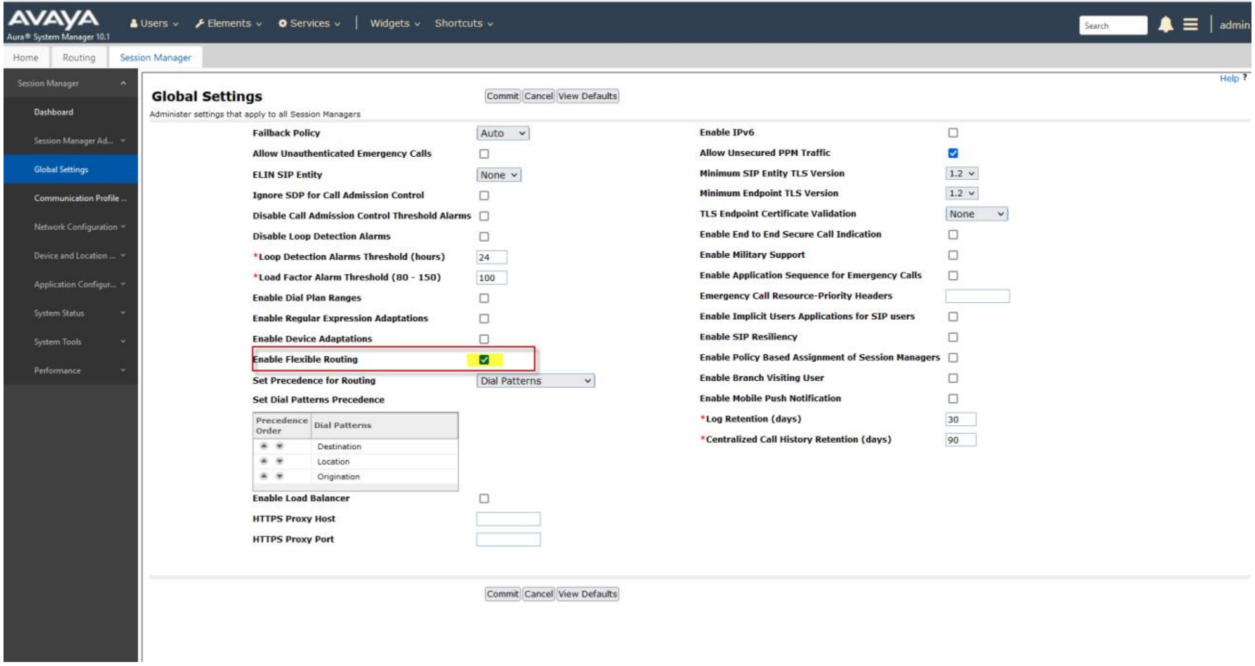
Dial Patterns

Add Remove

6 Items Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	+1212663	12	12	□	-ALL-	DR-Loc	To SBCE
□	+1703703	12	12	□	-ALL-	DR-Loc	to SBCE
□	+911	4	4	□	-ALL-	DR-Loc	Emergency call to SBCE
□	1425553	11	11	□	-ALL-	DR-Loc	To SBCE from EP POM for SIP PSTN
□	212663	10	10	□	-ALL-	DR-Loc	External call to PSTN at SBC-IPOSE via SBCE

Additionally, enable Flexible Routing. Select **Elements → Session Manager → Global Settings** and check "**Enable Flexible Routing**".



Global Settings

Administer settings that apply to all Session Managers

Failback Policy	Auto
Allow Unauthenticated Emergency Calls	□
ELIN SIP Entity	None
Ignore SDP for Call Admission Control	□
Disable Call Admission Control Threshold Alarms	□
Disable Loop Detection Alarms	□
*Loop Detection Alarms Threshold (hours)	24
*Load Factor Alarm Threshold (80 - 150)	100
Enable Dial Plan Ranges	□
Enable Regular Expression Adaptations	□
Enable Device Adaptations	□
Enable Flexible Routing	☑
Set Precedence for Routing	Dial Patterns
Set Dial Patterns Precedence	

Precedence Order	Dial Patterns
▲ ▼	Destination
▲ ▼	Location
▲ ▼	Origination

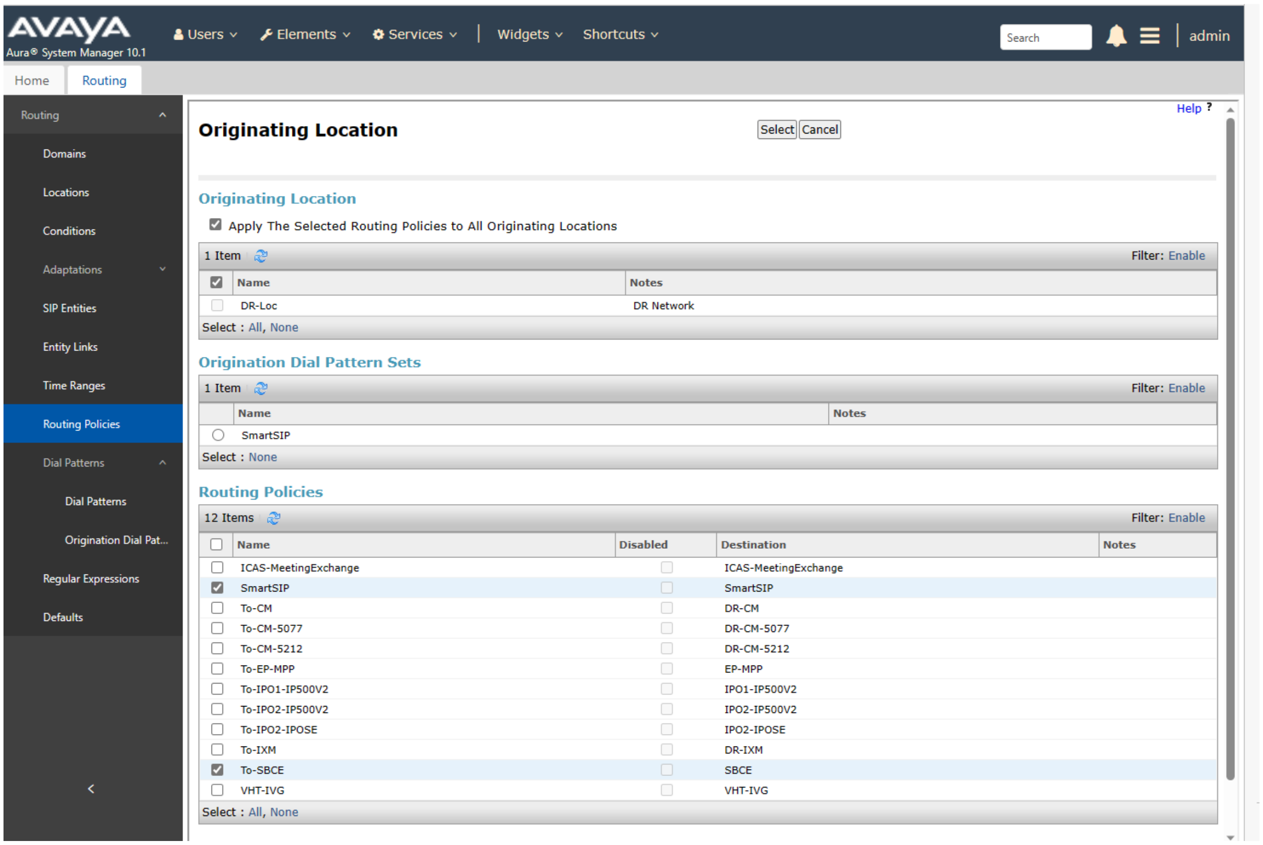
Enable Load Balancer	□
HTTPS Proxy Host	
HTTPS Proxy Port	

Enable IPv6	□
Allow Unsecured PPM Traffic	☑
Minimum SIP Entity TLS Version	1.2
Minimum Endpoint TLS Version	1.2
TLS Endpoint Certificate Validation	None
Enable End to End Secure Call Indication	□
Enable Military Support	□
Enable Application Sequence for Emergency Calls	□
Emergency Call Resource-Priority Headers	
Enable Implicit Users Applications for SIP users	□
Enable SIP Resiliency	□
Enable Policy Based Assignment of Session Managers	□
Enable Branch Visiting User	□
Enable Mobile Push Notification	□
*Log Retention (days)	30
*Centralized Call History Retention (days)	90

7.3. Administer Dial Patterns

Select **Routing → Dial Patterns** from the left pane, and add a new Dial Pattern by select **Add** (not shown). The **Dial Pattern Details** screen is displayed (not shown).

In the **Originating Locations and Routing Policies** sub-section, click **Add**. Select a preconfigured **Originating Location** and select the **Routing Polices** created in previous section for SmartSIP and Avaya SBC.



Originating Location

Originating Location

☑ Apply The Selected Routing Policies to All Originating Locations

1 Item — Filter: Enable

☑	Name	Notes
□	DR-Loc	DR Network

Select : All, None

Origination Dial Pattern Sets

1 Item — Filter: Enable

	Name	Notes
○	SmartSIP	

Select : None

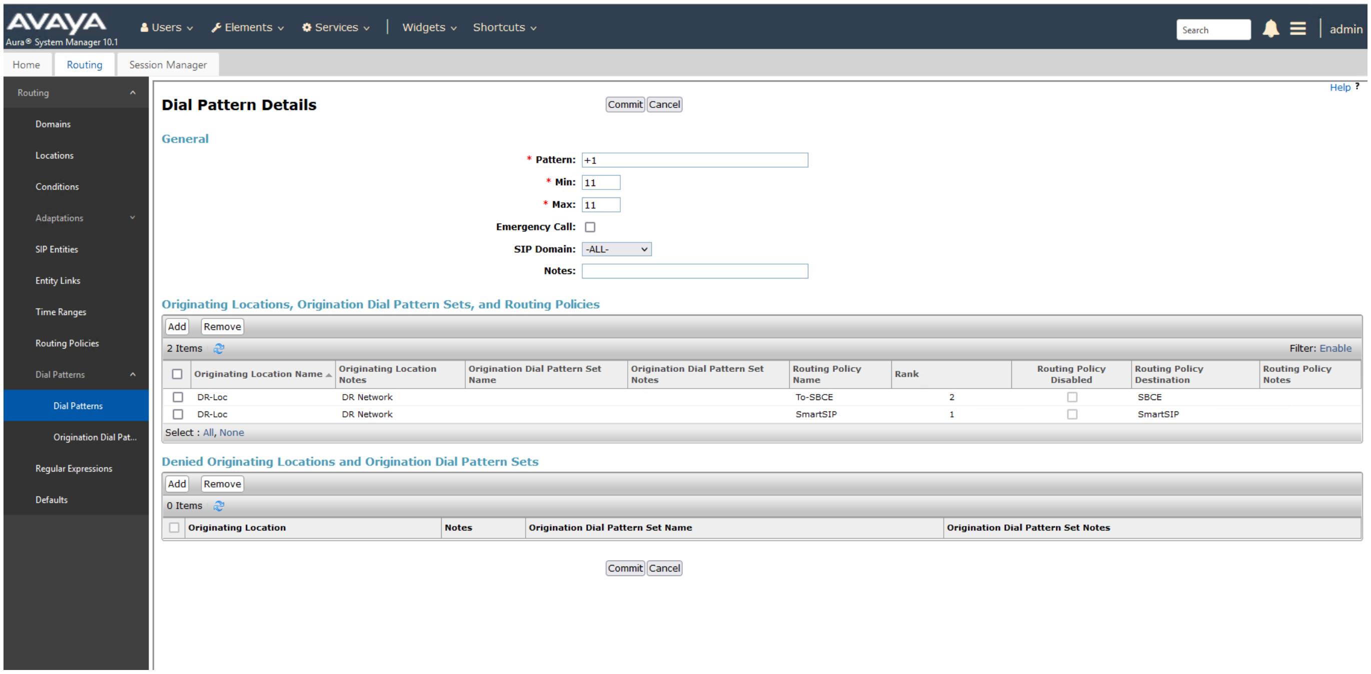
Routing Policies

12 Items — Filter: Enable

□	Name	Disabled	Destination	Notes
□	ICAS-MeetingExchange	□	ICAS-MeetingExchange	
☑	SmartSIP	□	SmartSIP	
□	To-CM	□	DR-CM	
□	To-CM-5077	□	DR-CM-5077	
□	To-CM-5212	□	DR-CM-5212	
□	To-EP-MPP	□	EP-MPP	
□	To-IPO1-IP500V2	□	IPO1-IP500V2	
□	To-IPO2-IP500V2	□	IPO2-IP500V2	
□	To-IPO2-IPOSE	□	IPO2-IPOSE	
□	To-IXM	□	DR-IXM	
☑	To-SBCE	□	SBCE	
□	VHT-IVG	□	VHT-IVG	

Select : All, None

In the compliance testing, the new entry allowed dialing for 12 digits starting with +1. Note the **Rank** order of the two routing policies. Call first attempted to route via SmartSIP, but if an error response is returned or there is no response from SmartSIP, calls are routed to Avaya SBC.



Dial Pattern Details

General

* Pattern:	+1
* Min:	11
* Max:	11
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations, Origination Dial Pattern Sets, and Routing Policies

2 Items Filter: Enable

□	Originating Location Name	Originating Location Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	DR-Loc	DR Network			To-SBCE	2	□	SBCE	
□	DR-Loc	DR Network			SmartSIP	1	□	SmartSIP	

Select : All, None

Denied Originating Locations and Origination Dial Pattern Sets

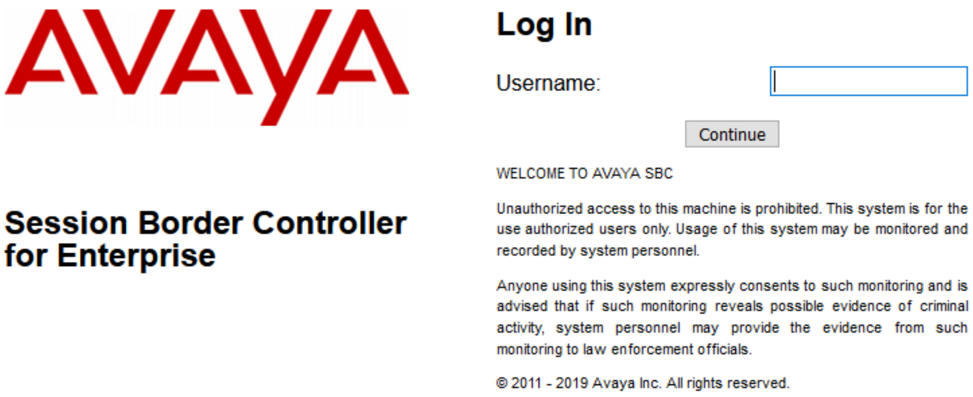
0 Items

□	Originating Location	Notes	Origination Dial Pattern Set Name	Origination Dial Pattern Set Notes

8. Configure Avaya Session Border Controller

This section describes the configuration of the Avaya SBC. The Avaya SBC provides SIP connectivity from SmartSIP and Session Manager to a SIP service provider. Configuration of SIP service provider is outside of scope for this document.

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. A log in screen is presented. Log in using the appropriate username and password.



WELCOME TO AVAYA SBC

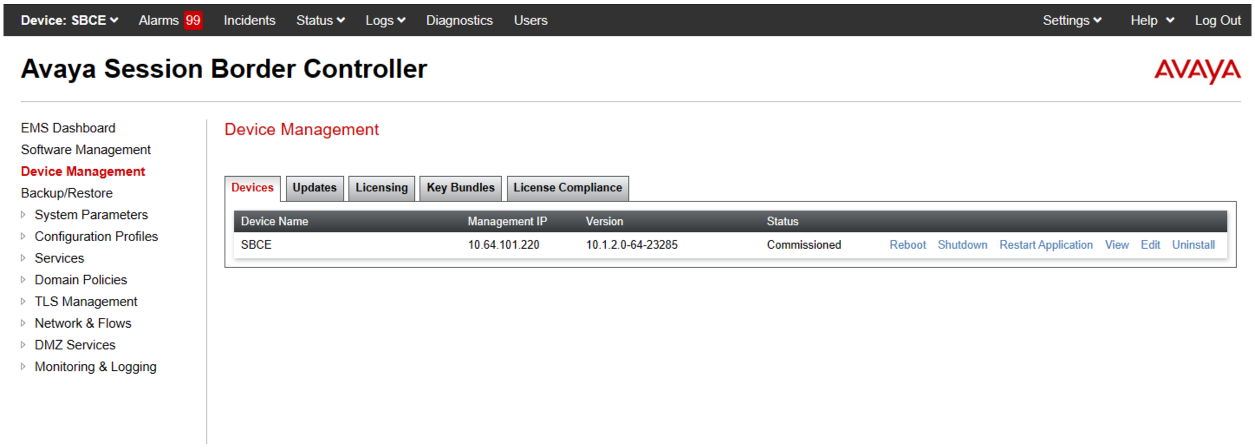
Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

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 - 2019 Avaya Inc. All rights reserved.

8.1. Access Avaya Session Border Controller for Enterprise

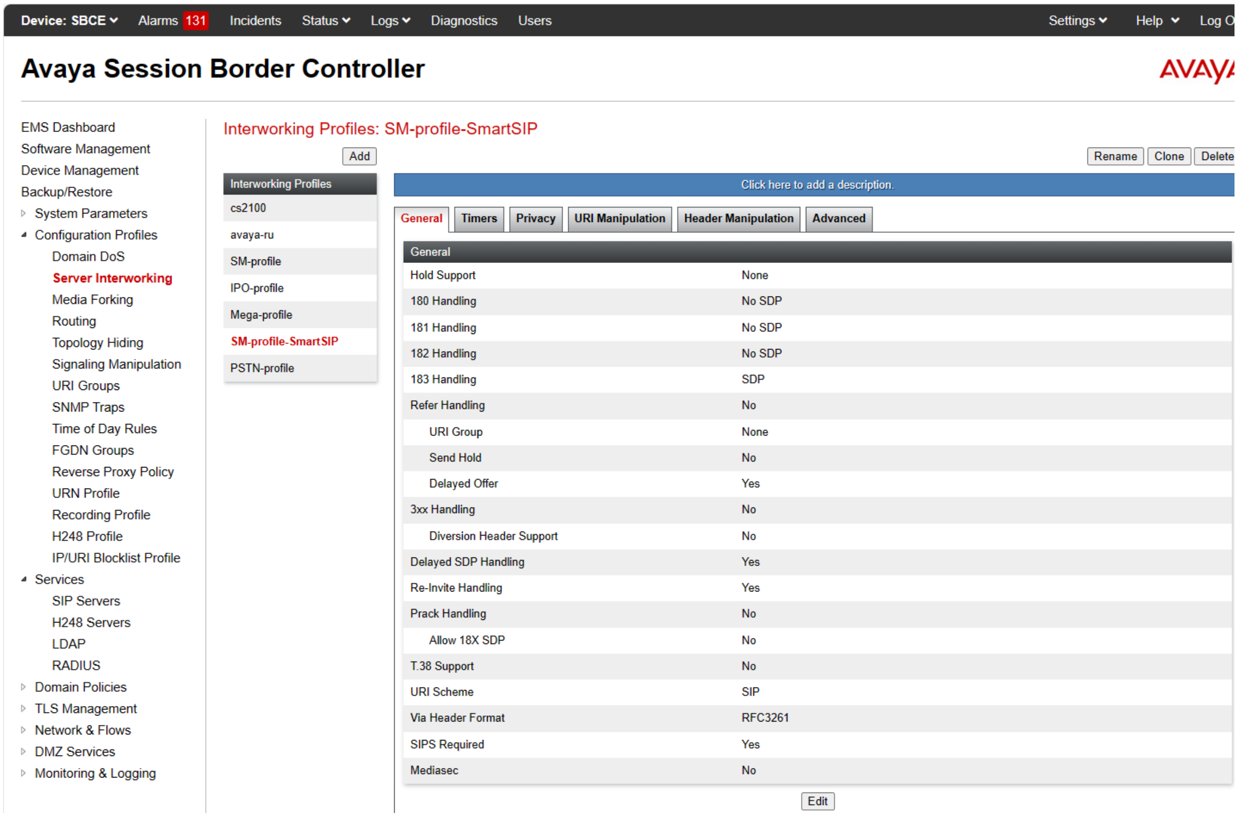
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBC.



Device Name	Management IP	Version	Status	
SBCE	10.64.101.220	10.1.2.0-64-23285	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

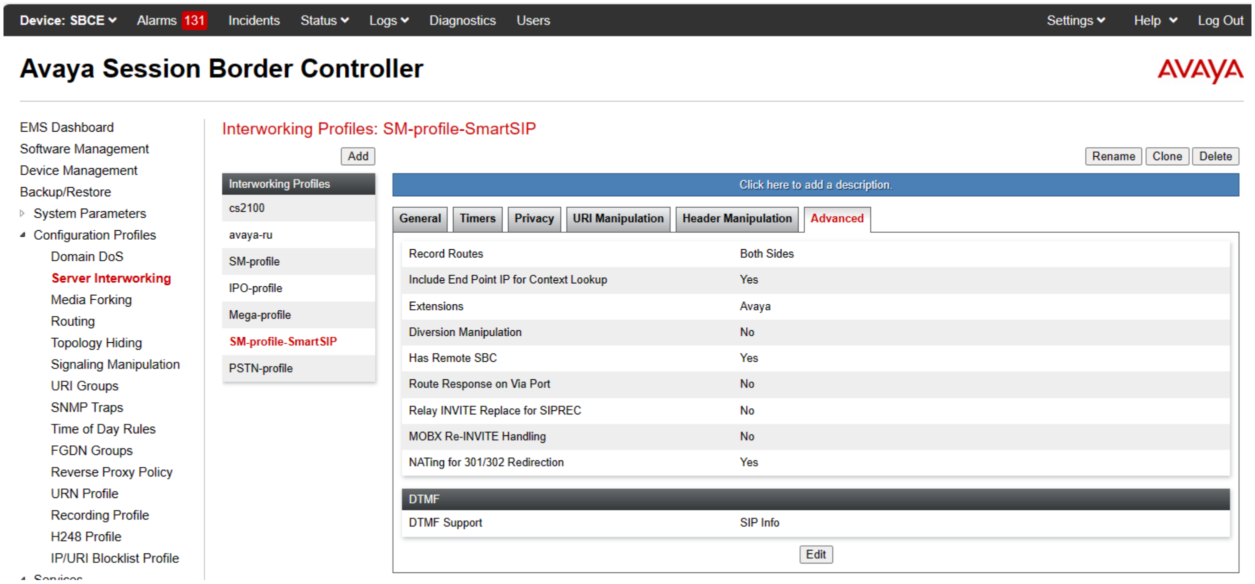
8.2. Define Interworking Profile

An interworking profile is needed for supported SIP functionality for a SIP server. During compliance test, a pre-configured profile was used. To an Interworking profile select **Configuration Profiles → Server Interworking** from the left-hand menu. Screen captures for the profile are shown below.



General	
Hold Support	None
180 Handling	No SDP
181 Handling	No SDP
182 Handling	No SDP
183 Handling	SDP
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	Yes
Re-Invite Handling	Yes
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

Click on **Next** until **DTMF Support** is displayed. Check box for **SIP Info** and click **Finish.**



Interworking Profiles: SM-profile-SmartSIP

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
Relay INVITE Replace for SIPREC	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes

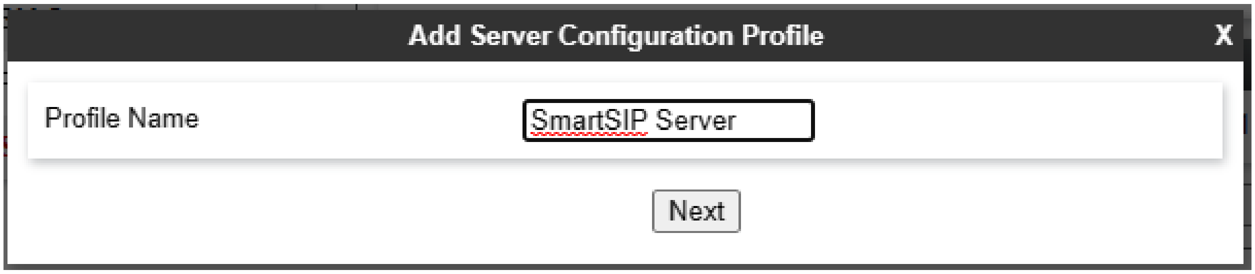
DTMF

DTMF Support	SIP Info

8.3. Define SIP Servers

A server definition is required for each server connected to the Avaya SBC.

To define the server for SmartSIP, navigate to **Services → SIP Servers** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the pop-up menu. Note that Session Manager IP address will be added as part of SmartSIP server. Defining another SIP Server is not needed. All routing to and from Avaya Aura® environment is performed using the SIP Server configured in this section.

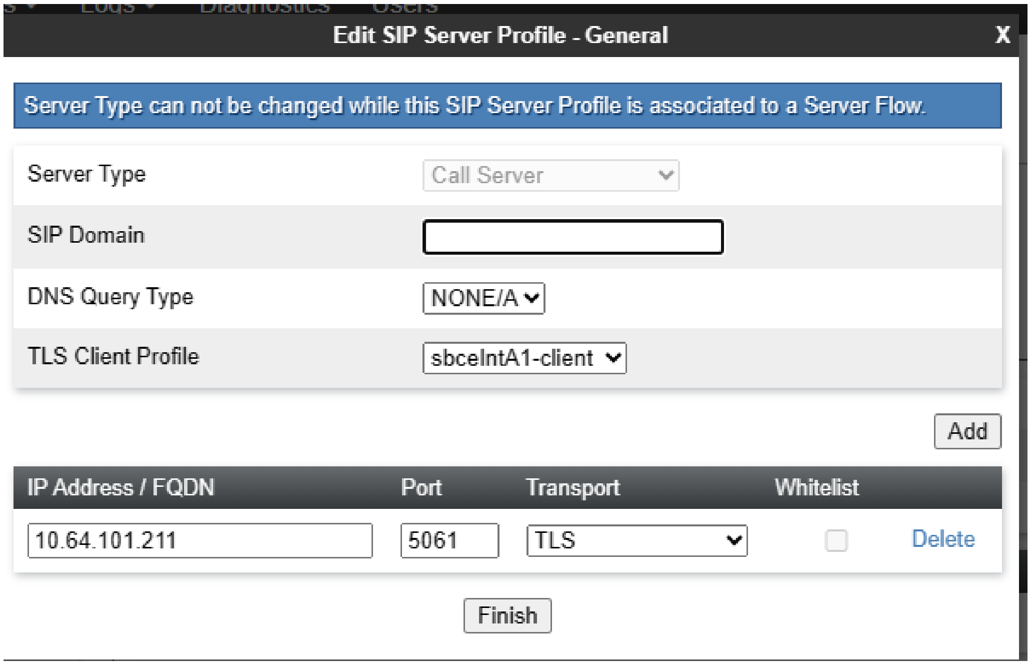


Add Server Configuration Profile

Profile Name: SmartSIP Server

Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop-down menu, select **Call Server**.
- Click on **Add** to and add two entries: SmartSIP and Session Manager.
- In the **IP Addresses / FQDN** box, type the IP Address of SmartSIP.
- In the **Port** box, enter the port to be used.
- In the **Transport** drop-down menu, select **TLS**.
- In the **TLS Client Profile** drop-down field, select the TLS client profile associated with the SBC interface connected to SmartSIP.
- Click on **Finish**.



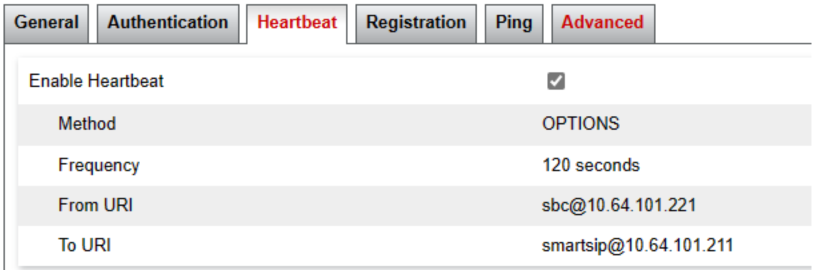
Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Call Server
SIP Domain	
DNS Query Type	NONE/A
TLS Client Profile	sbceIntA1-client

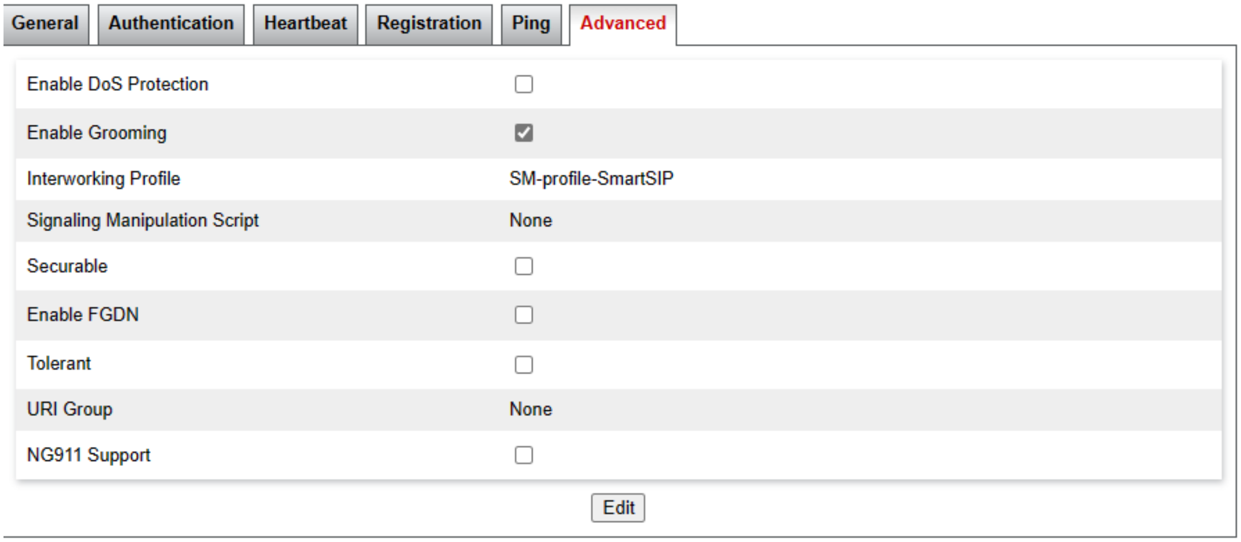
IP Address / FQDN	Port	Transport	Whitelist	
10.64.101.211	5061	TLS	□	Delete

Click on Next until **Add Heartbeat** configuration is displayed. Check box for **Enable Heartbeat** and select OPTIONS, insert desired Heartbeat frequency, From URI and To URI.



Enable Heartbeat	☑
Method	OPTIONS
Frequency	120 seconds
From URI	sbc@10.64.101.221
To URI	smartsip@10.64.101.211

Click on **Next** until **Add SIP Server Profile – Advanced** configuration is displayed. Check box for **Enable Grooming** and select an **Interworking Profile**. The configuration of the select Interworking profile is displayed in next section.



Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	SM-profile-SmartSIP
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
Tolerant	□
URI Group	None
NG911 Support	□

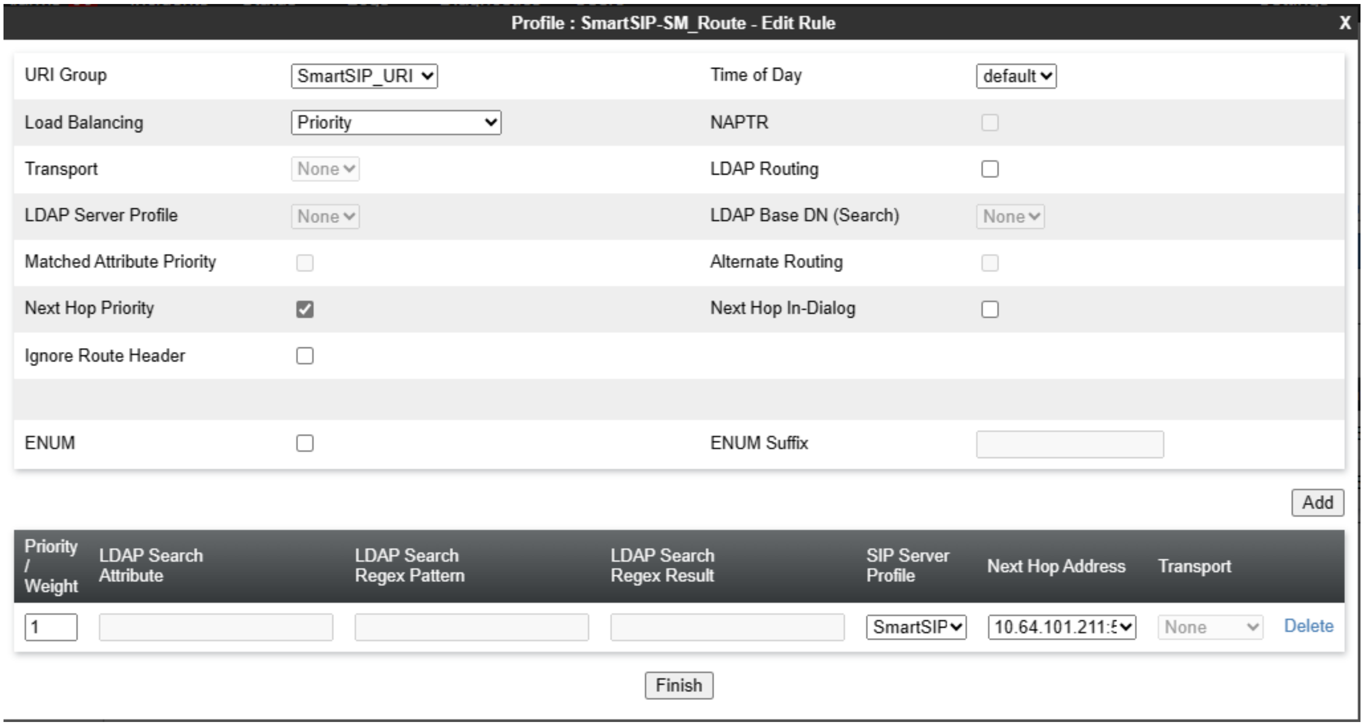
8.4. Define Routing

Routing information is required for routing calls to SmartSIP/Session Manager. The IP addresses and ports defined here will be used as the destination addresses for signalling.

To define routing to the Intelligent Virtual Assistant SIP Trunk, navigate to **Configuration Profiles → Routing** in the main menu on the left-hand side. Click on **Add** and enter an appropriate name in the dialogue box (Not shown).

Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP Address of SmartSIP.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used for SmartSIP IP address.
- Select the SmartSIP SIP Server defined in **Section 8.2** in the **SIP Server Profile** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.

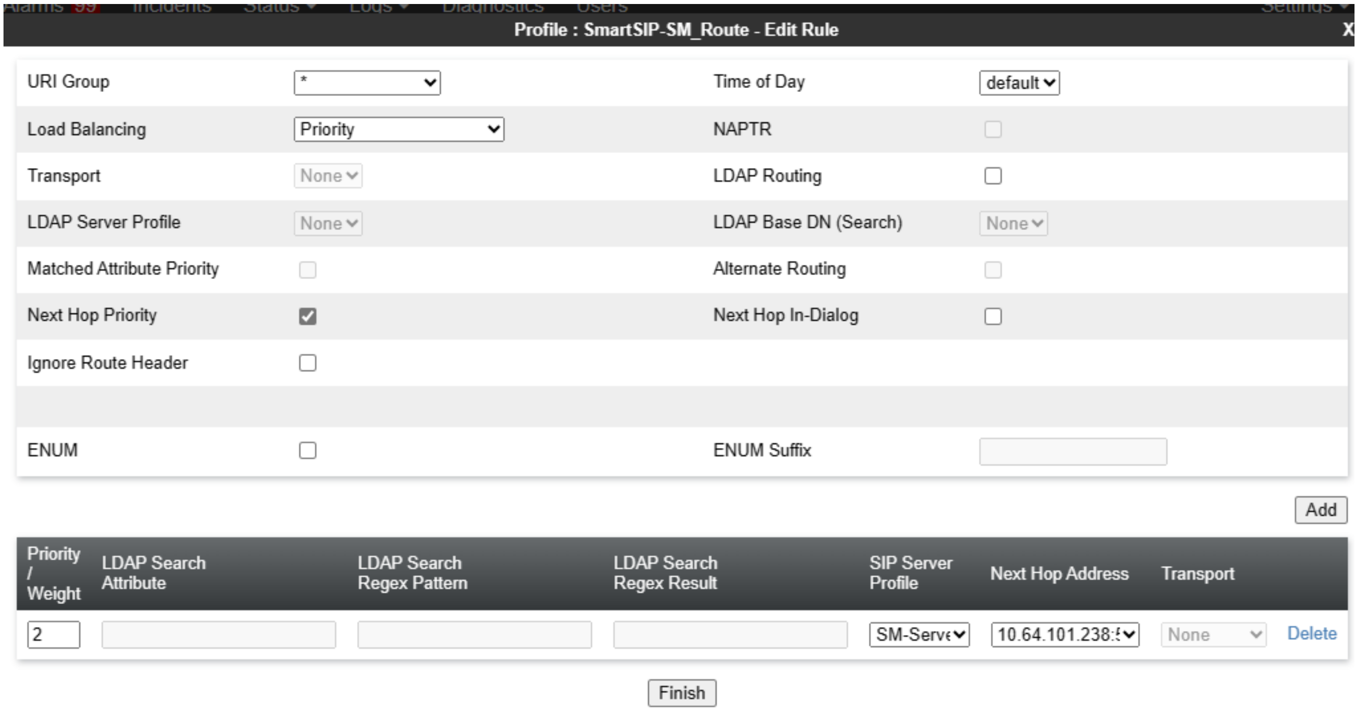


Profile : SmartSIP-SM_Route - Edit Rule

URI Group	SmartSIP_URI	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	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				SmartSIP	10.64.101.211:5	None	Delete

- Click on **Add** to specify the IP Address of Session Manger.
- Assign a priority in the **Priority / Weight** field, during testing a value of **2** was used for Session Manager IP address.
- Select the Session Manager SIP Server defined in the **SIP Server Profile** drop down menu. This automatically populates the **Next Hop Address** field
- Click **Finish**.



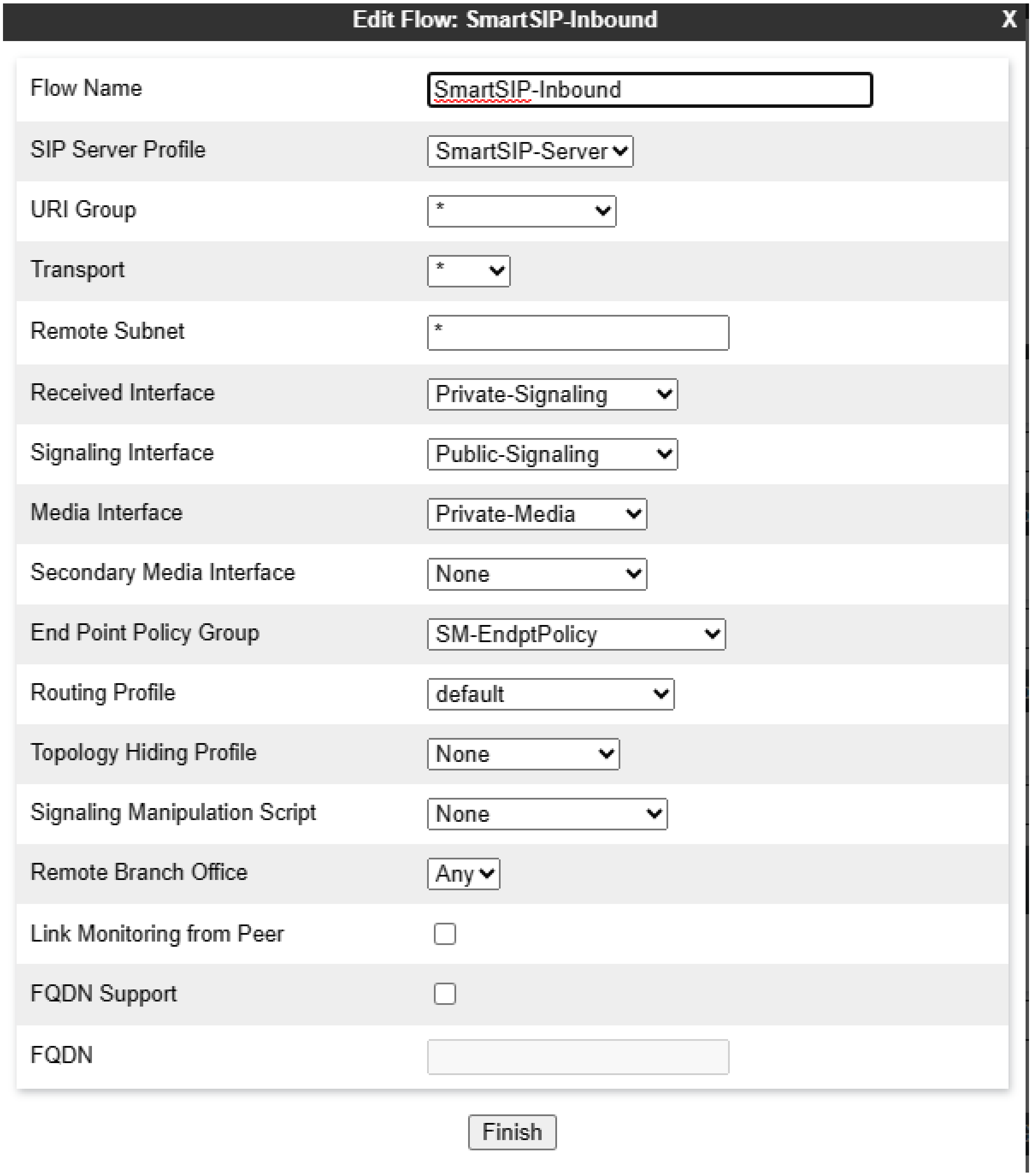
Profile : SmartSIP-SM_Route - Edit Rule

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	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
2				SM-Serve	10.64.101.238:5	None	Delete

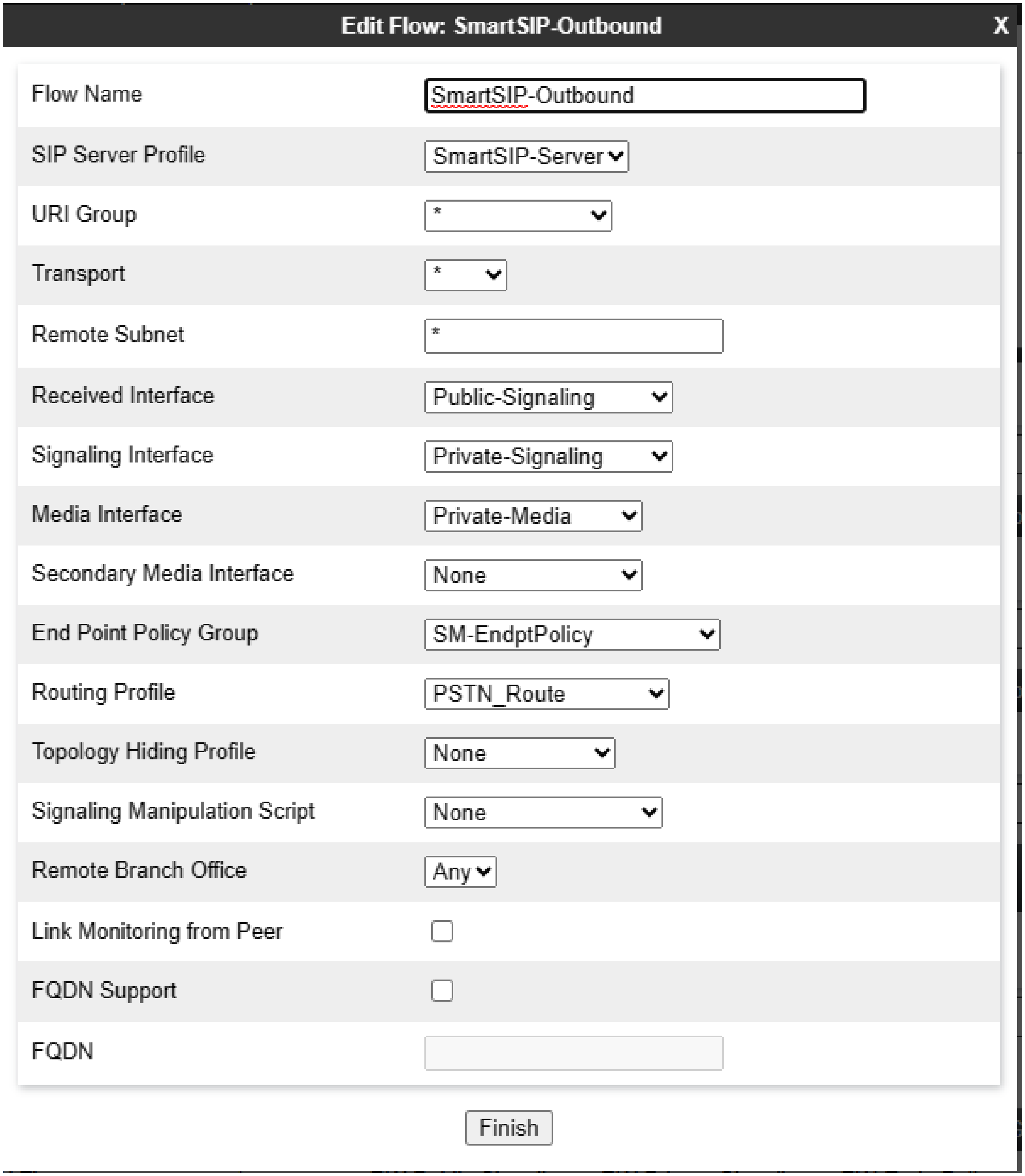
8.5. Server Flows

Server Flows combine the previously defined profiles for SmartSIP/Session Manager and SIP service provider. These End Point Server Flows allow calls to be routed to and from SmartSIP/Session Manager. Navigate to **Network & Flows → End Point Flows → Server Flows.** The screen capture below displays the configured Inbound and Outbound Server Flows. Configure the fields as shown in the screen capture.



Edit Flow: SmartSIP-Inbound

Flow Name	SmartSIP-Inbound
SIP Server Profile	SmartSIP-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Private-Signaling
Signaling Interface	Public-Signaling
Media Interface	Private-Media
Secondary Media Interface	None
End Point Policy Group	SM-EndptPolicy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	



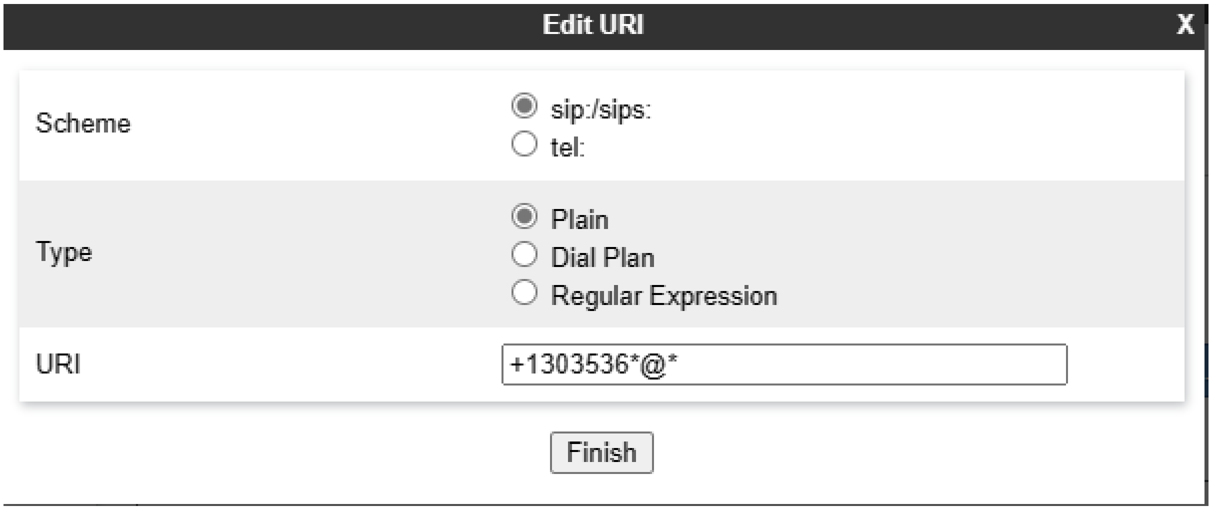
Edit Flow: SmartSIP-Outbound

Flow Name	SmartSIP-Outbound
SIP Server Profile	SmartSIP-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	SM-EndptPolicy
Routing Profile	PSTN_Route
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	□
FQDN Support	□
FQDN	

8.6. URI Group

To ensure only required calls (i.e. Call Center calls and not personal calls) are routed through SmartSIP create URI Groups.

Navigate to **Configuration Profiles → URI Groups.** Select **Add** and fill in the appropriate details for the site. This is an example from this lab.



Edit URI

Scheme: ● sip:/sips: ○ tel:

Type: ● Plain ○ Dial Plan ○ Regular Expression

URI: +1303536*@*

9. Configure IntraNext SmartSIP

All configurations related to SmartSIP are performed by IntraNext engineers as each system deployed by IntraNext is built for the client's environment.

10. Verification Steps

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

10.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify status of the administered CTI link by using the "**status aesvcs cti-link**" command. Verify that the **Service State** is "**established**" for the CTI link number administered in **Section** Error! Reference source not found., as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs
Link           Busy  Server           State         Sent     Rcvd

1     12       no    aes             established   49       49
```

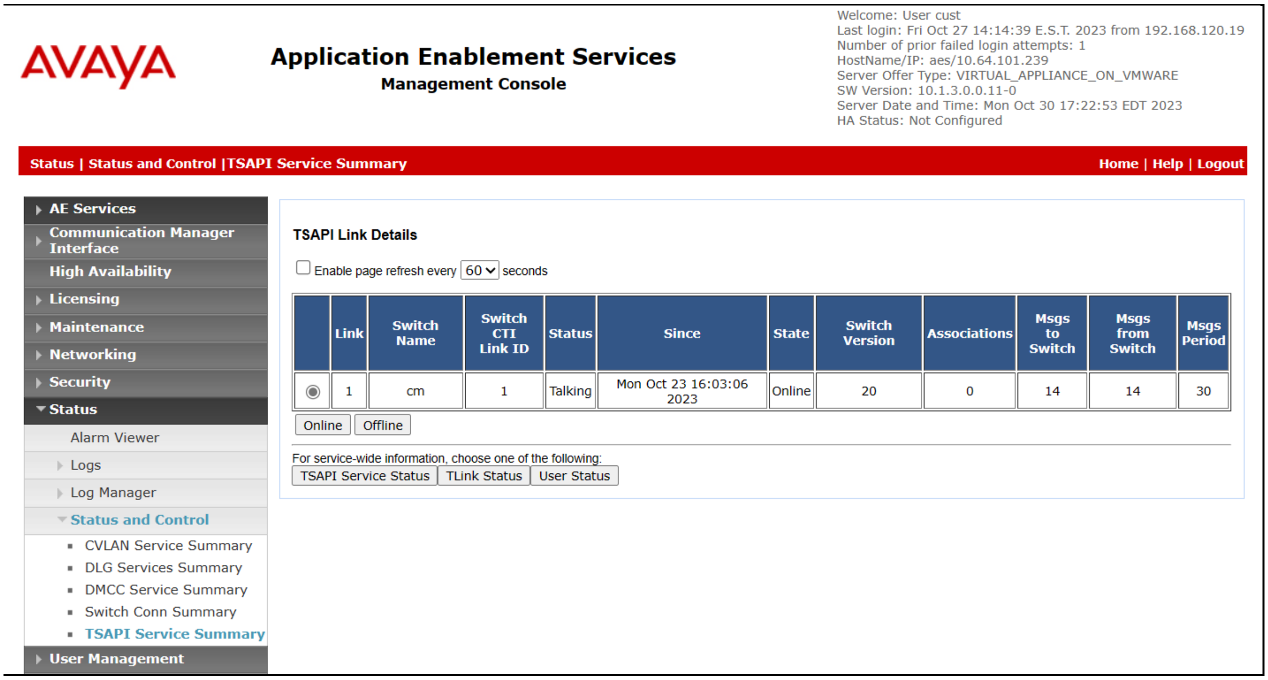
To verify SmartSIP is able to monitor the stations correctly, use the **list monitored-station** command. All the stations that are being monitored by SmartSIP are as shown below:

```
list monitored-station

                               MONITORED STATION

   Associations:     1       2       3       4       5       6       7       8
                 CTI     CTI     CTI     CTI     CTI     CTI     CTI     CTI
Station Ext      Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV Lnk CRV
---------------- ------- ------- ------- ------- ------- ------- ------- -------
65001            1  0004
            1  0009
```

10.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is "**Talking**" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of logged in agents from **Section** Error! Reference source not found., in this case "**2**".



Welcome: User cust
Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19
Number of prior failed login attempts: 1
HostName/IP: aes/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.0.0.11-0
Server Date and Time: Mon Oct 30 17:22:53 EDT 2023
HA Status: Not Configured

TSAPI Link Details

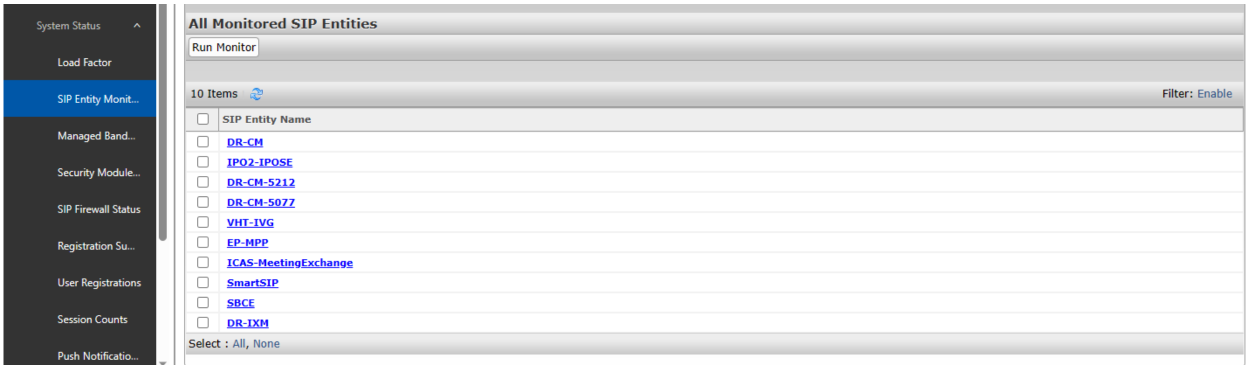
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm	1	Talking	Mon Oct 23 16:03:06 2023	Online	20	0	14	14	30

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

10.3. Verify Avaya Aura® Application Enablement Services

To verify SIP connectivity to SmartSIP, via System Manager, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring.** Under the **All Monitored SIP Entities,** select the SmartSIP SIP Entity.

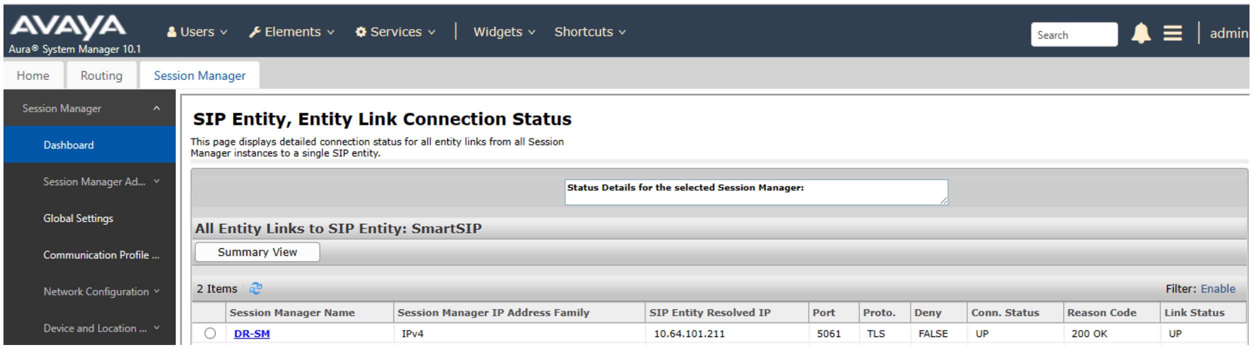


All Monitored SIP Entities

10 Items

☐	SIP Entity Name
☐	DR-CM
☐	IPO2-IPOSE
☐	DR-CM-5212
☐	DR-CM-5077
☐	VHT-IVG
☐	EP-MPP
☐	ICAS-MeetingExchange
☐	SmartSIP
☐	SBCE
☐	DR-IXM

Verify **Conn. Status** is **UP.**



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: SmartSIP

2 Items

Filter: Enable

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	DR-SM	IPv4	10.64.101.211	5061	TLS	FALSE	UP	200 OK	UP

11. Conclusion

These Application Notes describe the configuration steps required for IntraNext SmartSIP 10.4 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. All feature and serviceability test cases were completed.

12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 7, May 2023, available at http://support.avaya.com.

3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at http://support.avaya.com.

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.