**Avaya Solution & Interoperability Test Lab**

# Application Notes for IntraNext SmartSIP with Avaya Session Border Controller for Enterprise and Avaya Aura® environment – Issue 1.0


## Abstract

These Application Notes contain instructions for IntraNext SmartSIP with Avaya Session Border Controller for Enterprise and Avaya Aura® environment to successfully interoperate.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 contain instructions for IntraNext SmartSIP (SmartSIP) with Avaya Session Border Controller for Enterprise (Avaya SBCE) and Avaya Aura® environment to successfully interoperate.

SmartSIP is a patented software solution that provides a DTMF suppression and masking solution for an Avaya Aura® environment to securely handle sensitive cardholder data in attended payment interactions.

SmartSIP sits between Avaya Aura® Session Manager (Session Manager) and Avaya SBCE. All calls to and from a SIP service provider are routed via SmartSIP to Avaya Aura® environment. SmartSIP uses the received SIP INFO messages for DTMF detection and suppression. SmartSIP uses the Telephony Services Application Programming interface (TSAPI) of Avaya Aura® Application Enablement Services (AES) to monitor agent stations on Avaya Aura® Communication Manager (Communication Manager).

Refer to **Section 3** for the list of Avaya components, which make up the 'Avaya Aura® environment' that were used during compliance testing.

# 2. General Test Approach and Test Results

The feature test cases were performed manually. Each test call was handled manually on an agent station with generation of DTMF from the far end. Necessary user actions, such as hold and reconnect, were performed from the agent telephones to test different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the network to SmartSIP.

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 interface between Avaya systems and SmartSIP utilized SIP TLS encryption capabilities.

## 2.1. Interoperability Compliance Testing

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

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper transmissions of DTMF via SIP INFO; calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, conference, and transfer.

The serviceability testing focused on verifying the ability of SmartSIP to recover from adverse conditions, such as disconnecting/reconnecting the network to SmartSIP.

## 2.2. Test Results

All executed test cases were successfully passed.

## 2.3. Support

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

- **Phone:** (USA) 1-800-928-6398
- **Email:** support@intranext.com
- **Web:** http://www.intranext.com

# 3. Reference Configuration

**Figure 1** illustrates a sample configuration that consists of Avaya products and IntraNext SmartSIP. All SIP traffic between the SIP service provider and the Avaya Aura® environment was routed via SmartSIP.

During the compliance test, the Avaya Aura® environment consisted of the following components:

- Avaya Aura® Communication Manager
- Avaya Aura® System Manager
- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Media Server
- Avaya Aura® Application Enablement Services
- Avaya G450 Media Gateway
- Avaya Endpoints

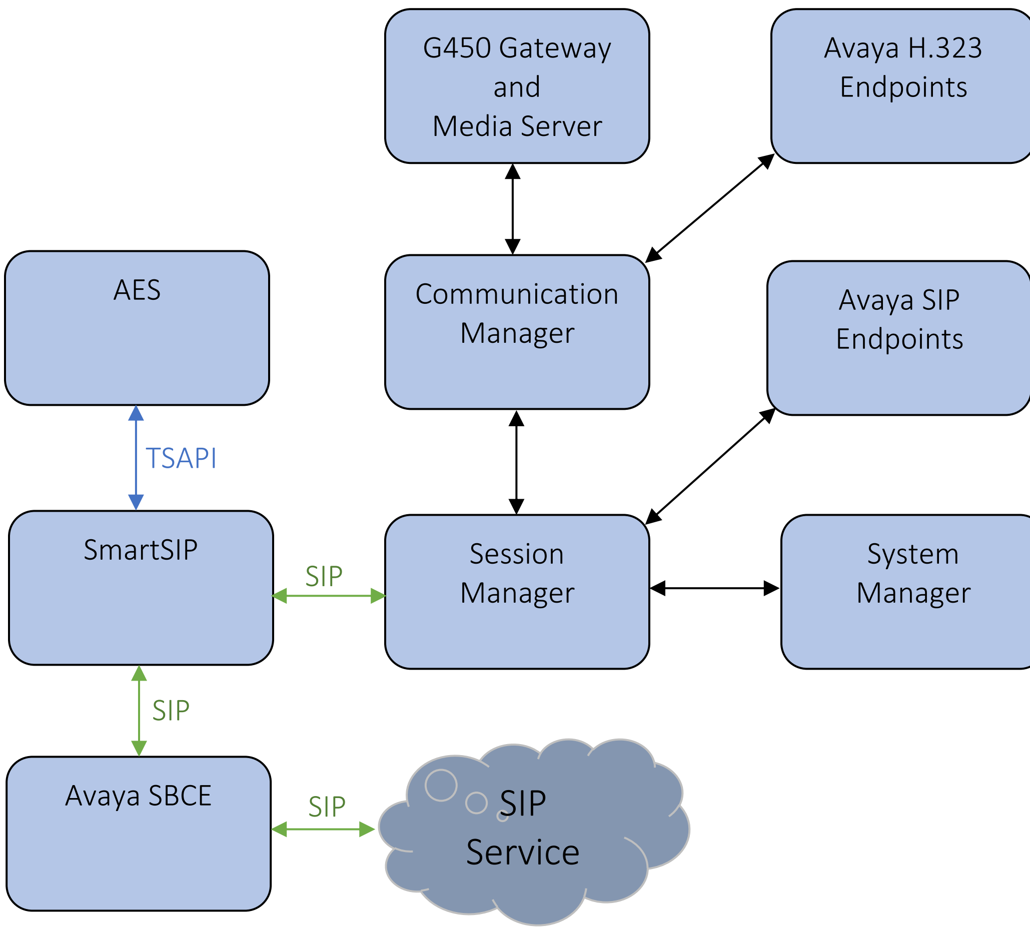



**Figure 1:** Test Configuration for IntraNext SmartSIP and Avaya Aura® Environment.

# 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 | 8.1.1.0 |
| Avaya Aura® Session Manager | 8.1.1 |
| Avaya Aura® System Manager | 8.1.1 |
| Avaya 9600 Series IP Deskphones<br>Avaya 9600 Series IP Deskphones<br>Avaya J100 Series IP Deskphones<br>Avaya J100 Series IP Deskphones | 7.1.7 (SIP)<br>6.8.3 (H.323)<br>6.8.3 (H.323)<br>4.0.3 (SIP) |
| Avaya G450 Media Gateway | 41.9.0 |
| Avaya Aura® Application Enablement Services | 8.1.1.0.1 |
| Avaya Aura® Media Server | 8.0.2.61 |
| Avaya Aura Session Border Controller for Enterprise | 8.0.1.0.10 |
| Avaya TSAPI Client | 8.1 |
| IntraNext SmartSIP | 10.3.0 |

# 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        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS         y         procr        8765
```

On Page 3 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 6.1**.
- 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:           aes81       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: 77777
     Type: ADJ-IP
                                                                        COR: 1
     Name: aes
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**.

```
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
```

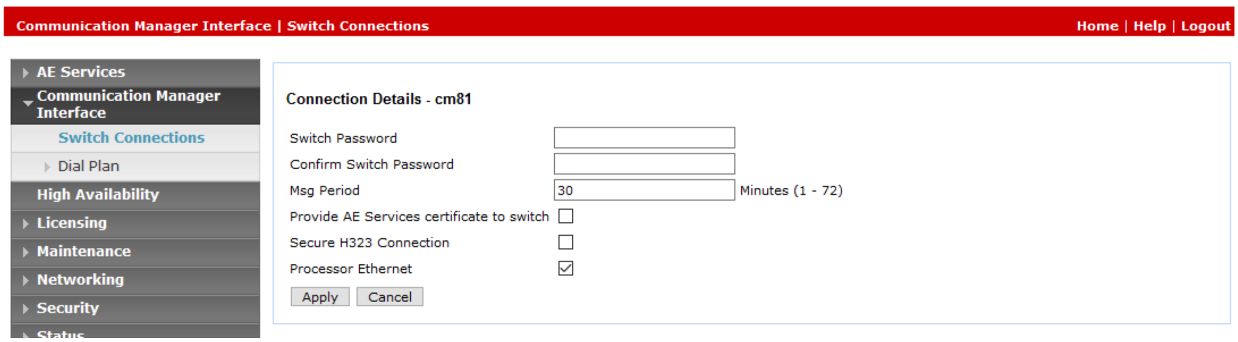
# 6. Configure Avaya Aura® Application Enablement Services

Configuration of AES requires a user account be configured for SmartSIP and CTI/TSAPI configuration for Communication Manager.

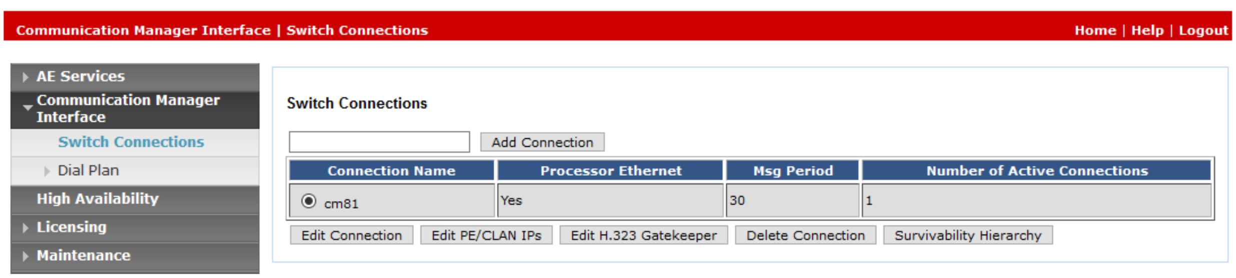
All administration is performed by web browser, https://<aes-ip-address>/

## 6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **cm**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.2** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.




The display returns to the **Switch Connections** screen which shows that the **cm81** switch connection has been added.



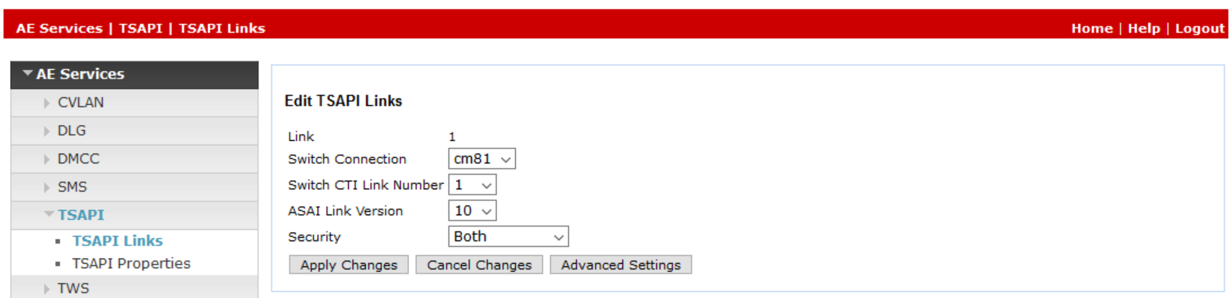
Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic. The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.


## 6.2. Add TSAPI Link

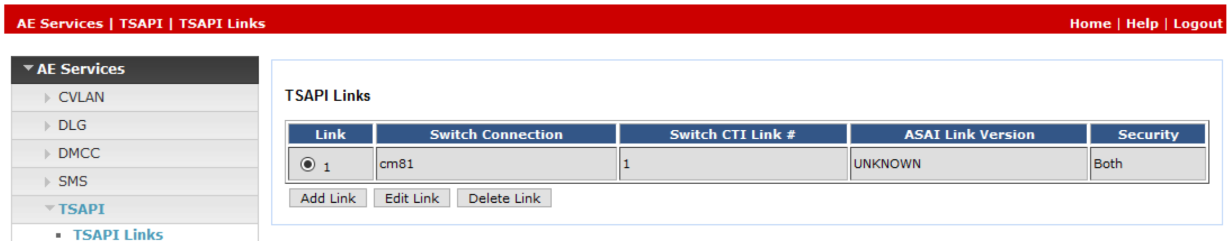
Navigate to the **AE Services →TSAPI → TSAPI Links** page to add a TSAPI CTI Link. Click **Add Link** (not shown).

Select a **Switch Connection** using the drop-down menu. Select the **Switch CTI Link Number** using the drop-down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form in **Section 5.3**. Select **Both** in the **Security** field.

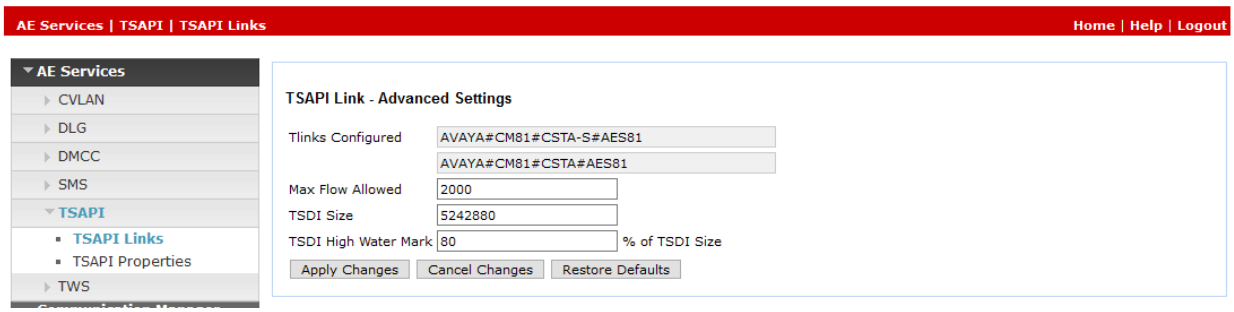
Click **Apply Changes**.



It returns to the **TSAPI Links** screen which shows that the **cm** link has been added.



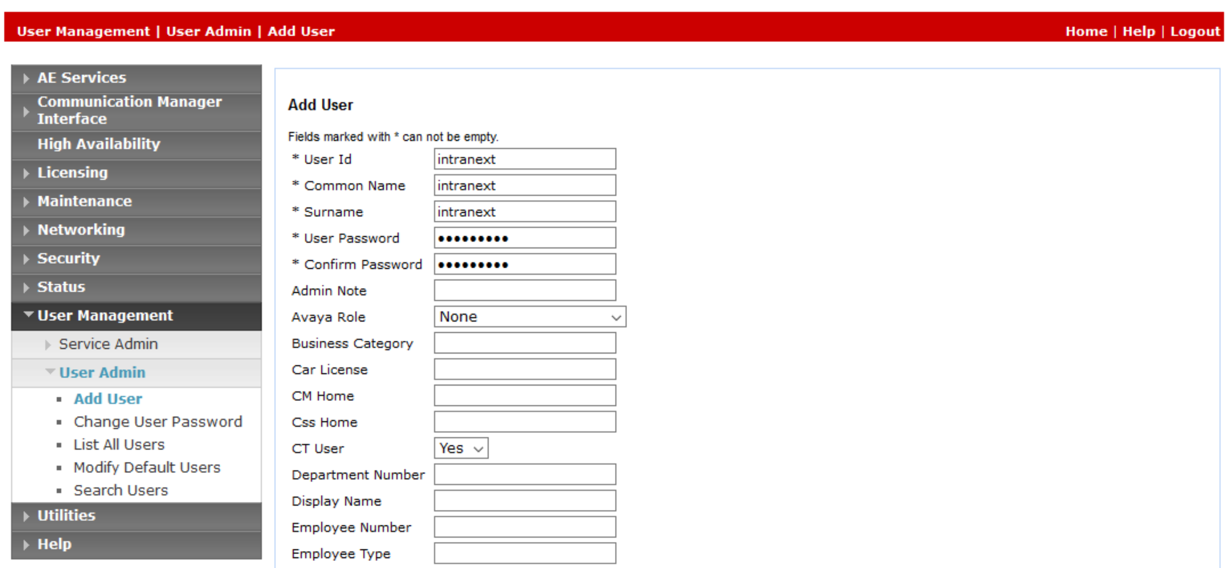

Click **Edit Link →Advanced Setting** to obtain the TSAPI Link that will be used by SmartSIP. During the compliance test, secure Tlink was used.



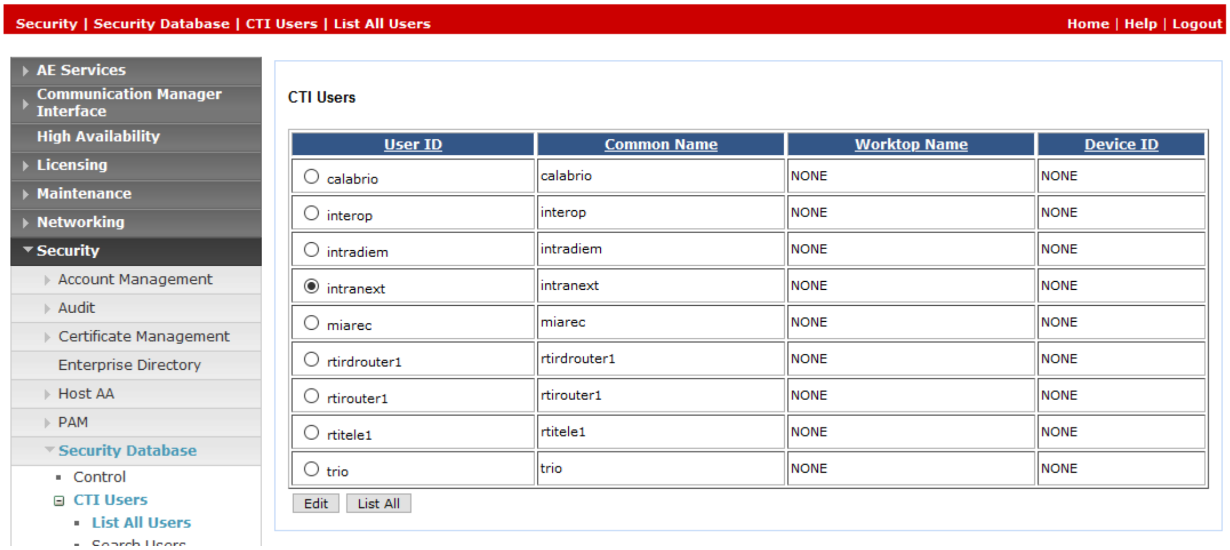

## 6.3. Configure User

A user needs to be created for SmartSIP to communicate with AES. Navigate to **User Management → User Admin → Add User**.

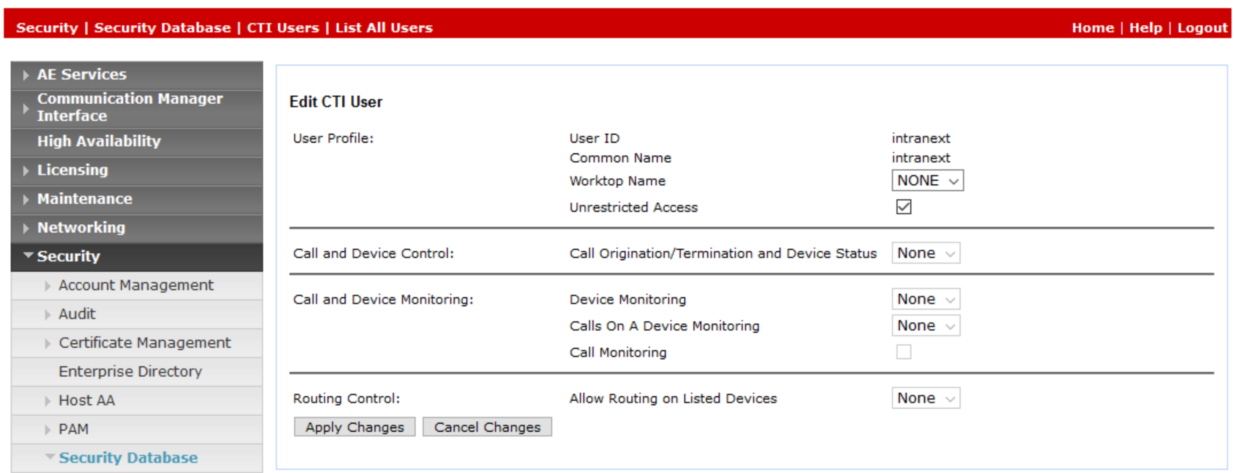
Fill in **User Id, Common Name, Surname, User Password** and **Confirm Password**. Set the **CT User** to **Yes,** and **Apply**.



Navigate to **Security → Security Database → CTI Users → List All Users**.




Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.



# 7. Configure Avaya Aura® Session Manager

SmartSIP sits between Session Manager and Avaya SBCE. All inbound and outbound calls to PSTN are routed via SmartSIP, followed by Avaya SBCE. A SIP trunk needs to be configured for SmartSIP and Avaya SBCE. 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

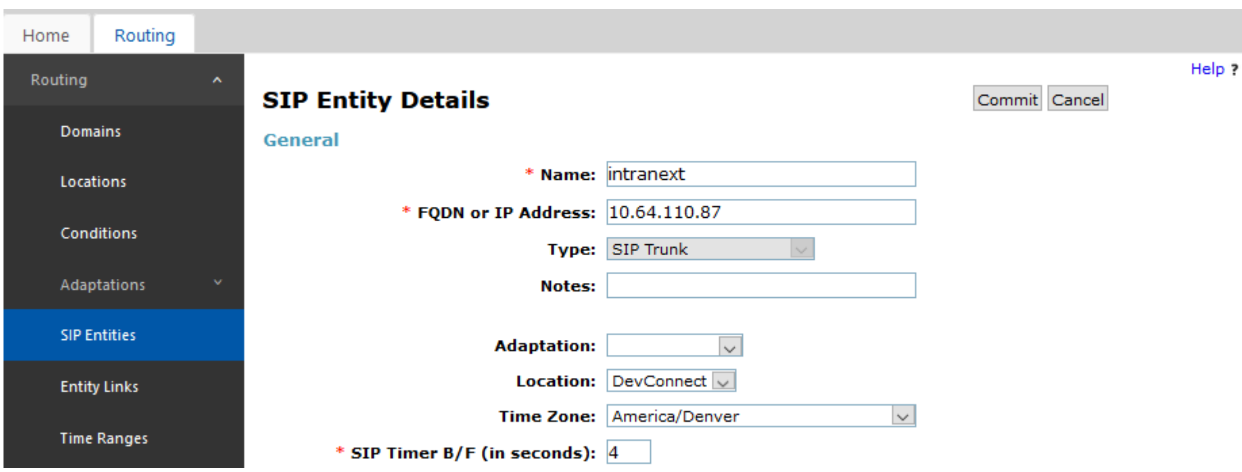
Add two new SIP entities, one for SmartSIP and another one for Avaya SBCE. Note that this SIP entity configured for Avaya SBCE is used for failover purposes when connectivity to SmartSIP in unavailable.

### 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.

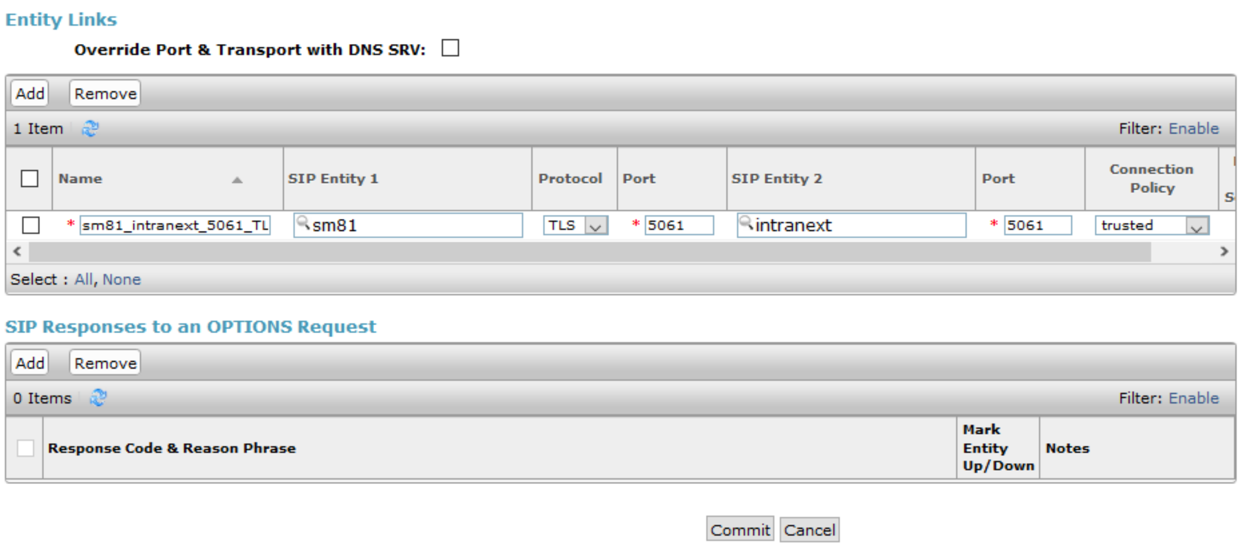
- **Name:** A descriptive name.
- **FQDN or IP Address:** The SIP IP address of SmartSIP.
- **Type:** "SIP Trunk"
- **Location:** Select a preconfigured Location.
- **Time Zone:** Select the applicable time zone.



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 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.

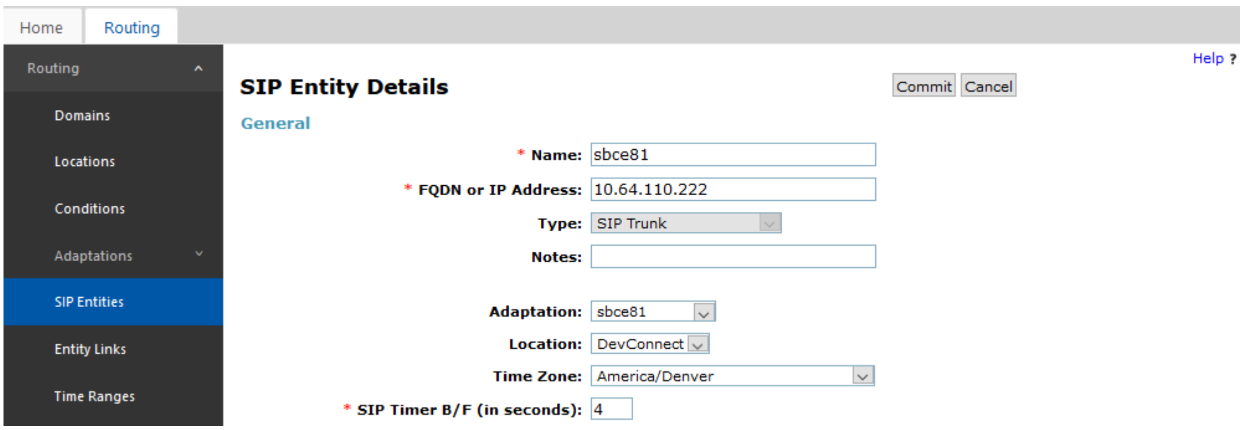


### 7.1.2. SIP Entity for Avaya SBCE

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 SBCE. Note that this SIP entity is used for failover purposes when connectivity to SmartSIP in unavailable.

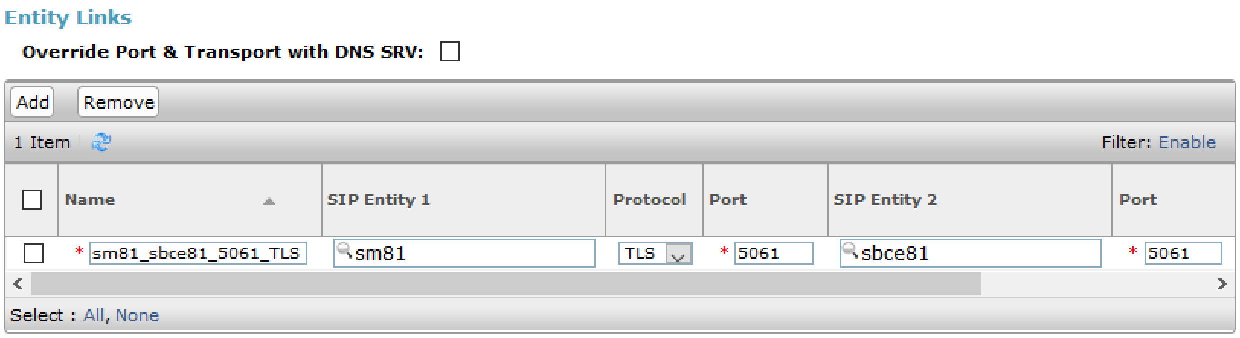
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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



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”



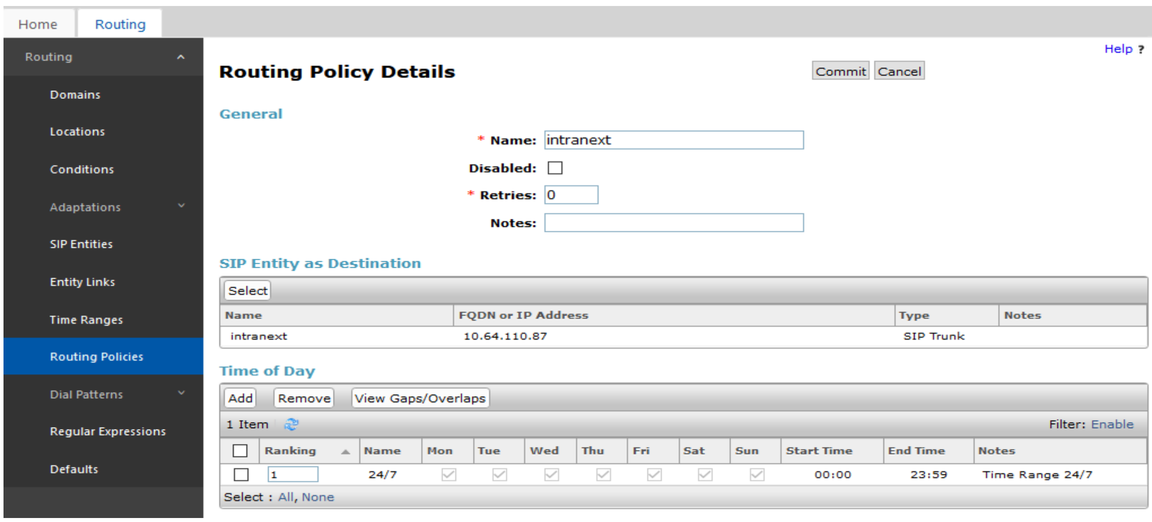
## 7.2. Administer Routing Policies

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

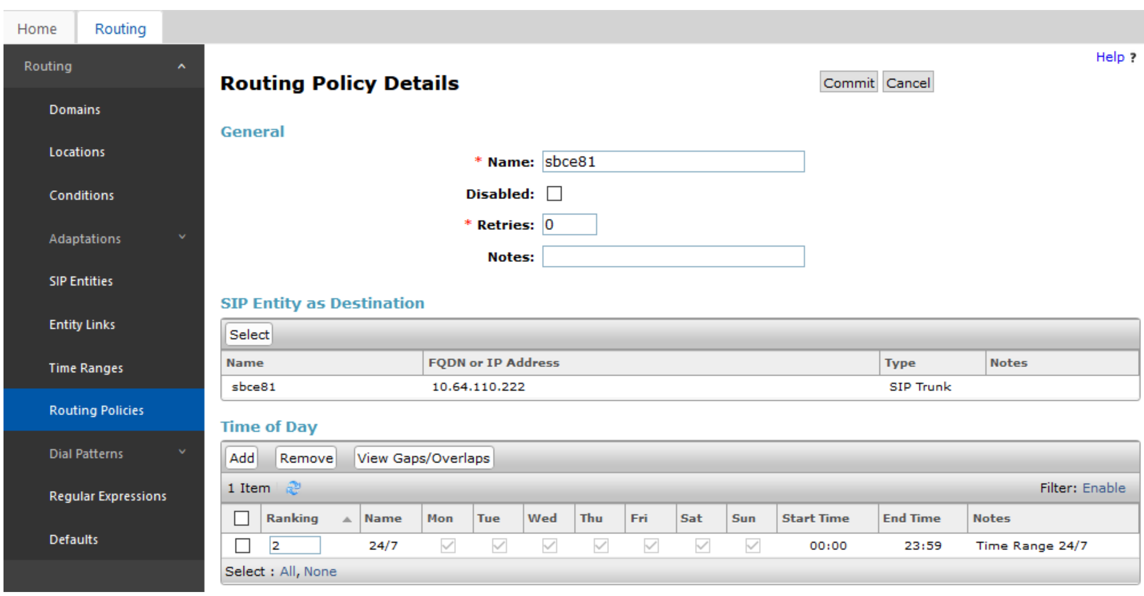
Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

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**.



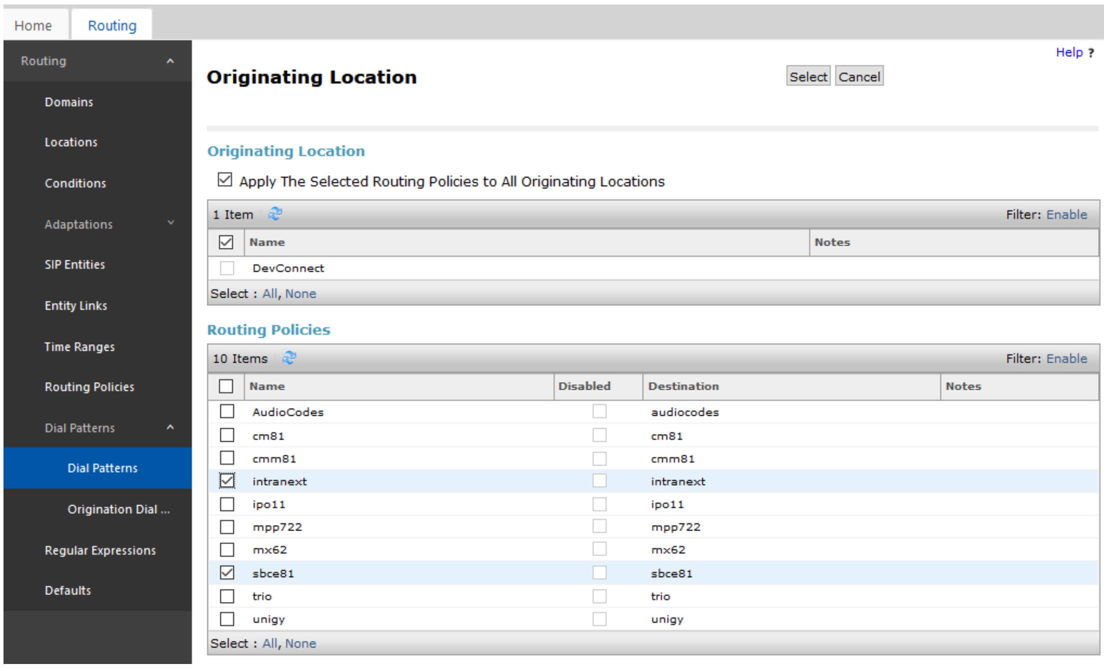

Similarly, add a **Routing Policy** for Avaya SBCE and configure the **Time of Day Ranking** to **2**.



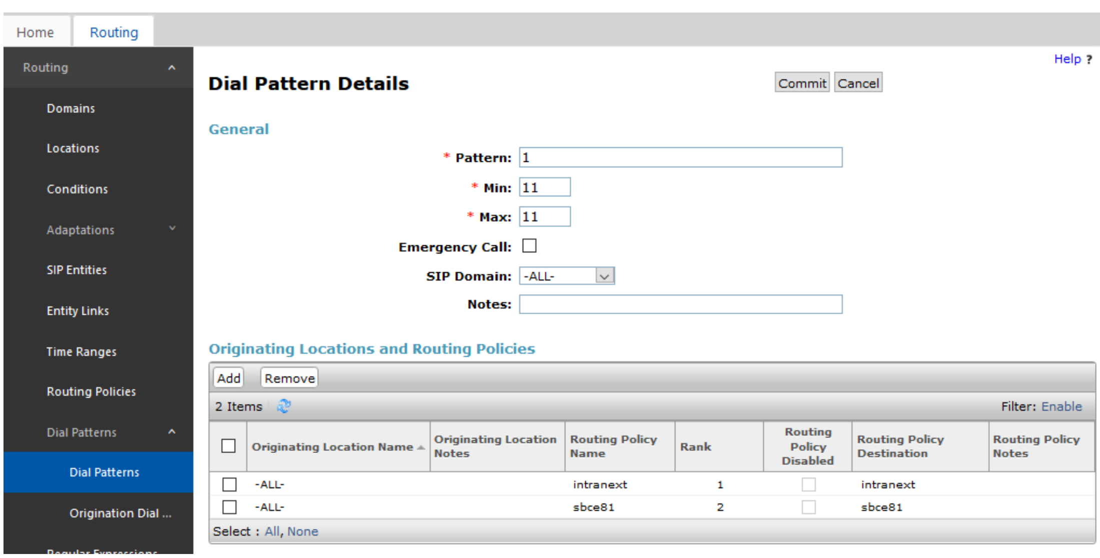
## 7.3. Administer Dial Patterns

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 SBCE.



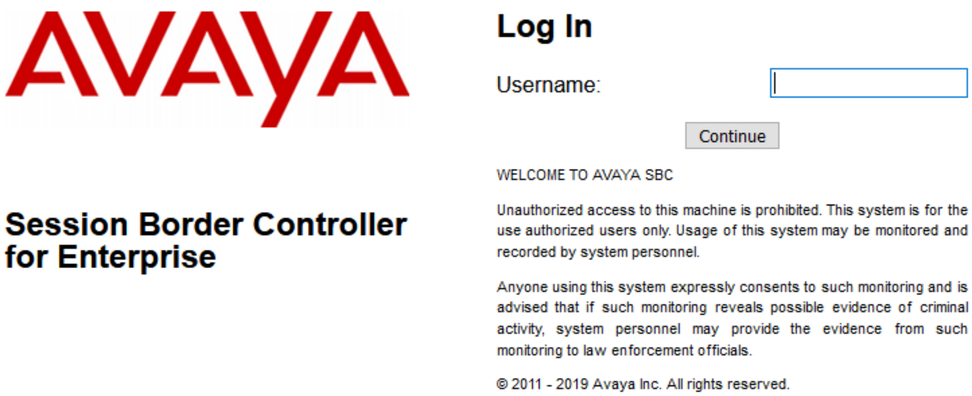

In the compliance testing, the new entry allowed dialing for **11** digits starting with **1**. Note the **Rank** order of the two routing policies. Call are first attempted to route via SmartSIP, but if an error response is returned or there is no response from SmartSIP, calls are routed to Avaya SBCE.



# 8. Configure Avaya Session Border Controller for Enterprise

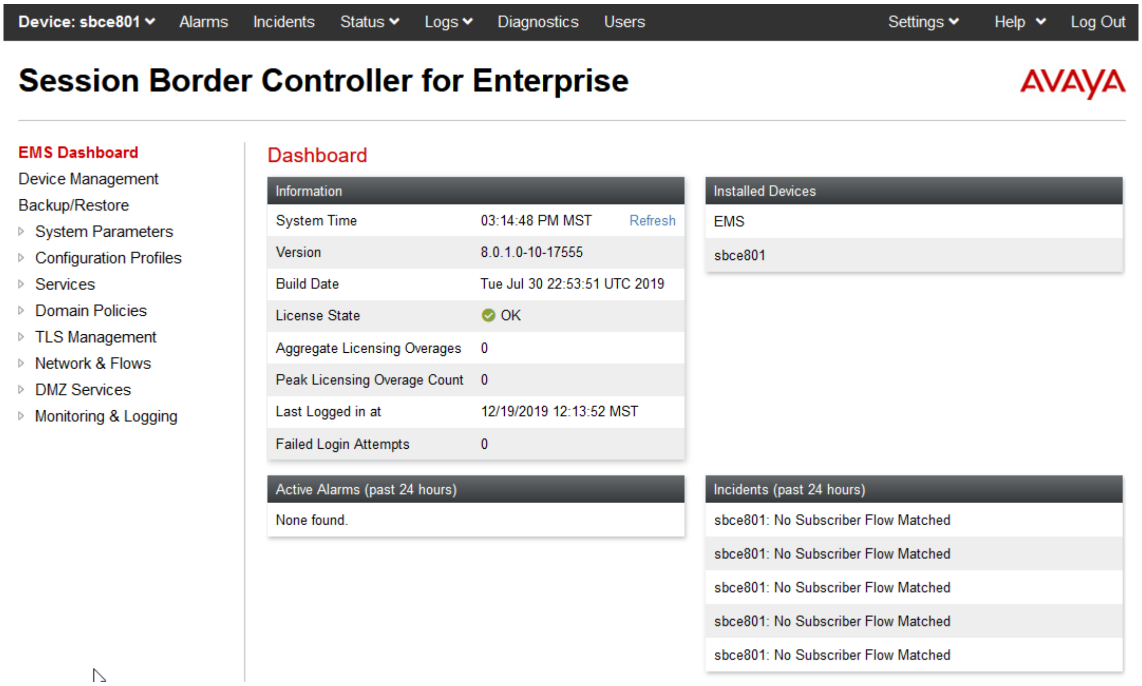
This section describes the configuration of the Avaya Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides SIP connectivity from SmartSIP and Session Manager to a SIP service provider. Configuration of SIP service provider is outside of scope for this document.

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.



## 8.1. Access Avaya Session Border Controller for Enterprise

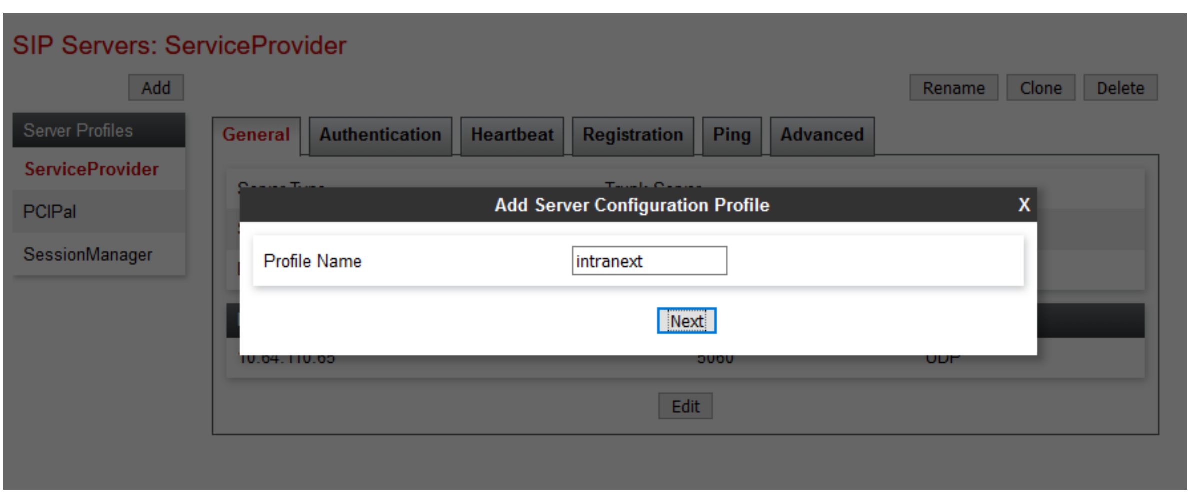
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.




## 8.2. Define SIP Servers

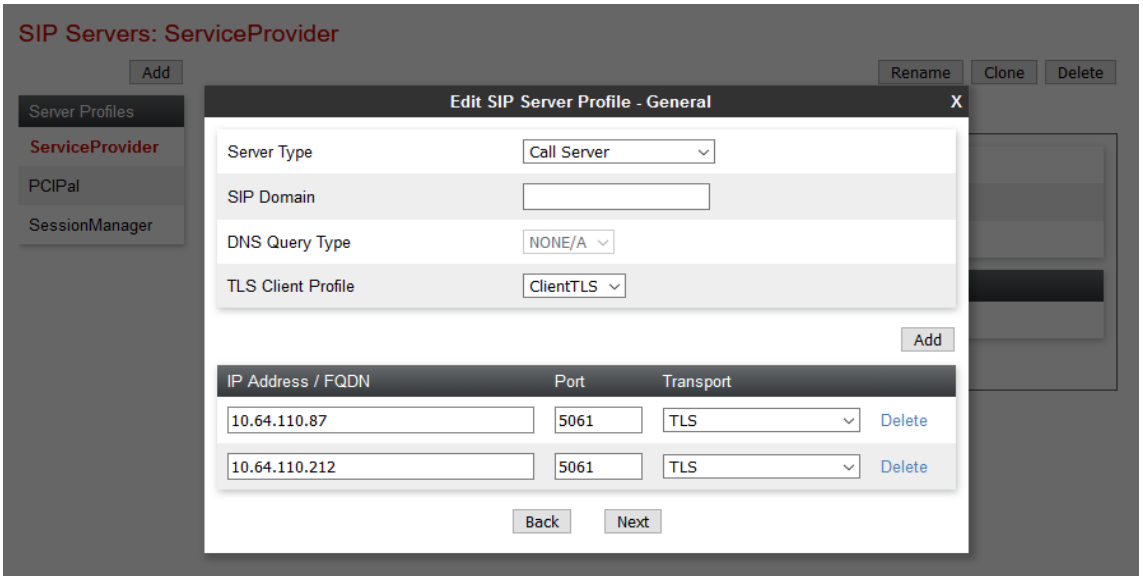
A server definition is required for each server connected to the Avaya SBCE.

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 the 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.

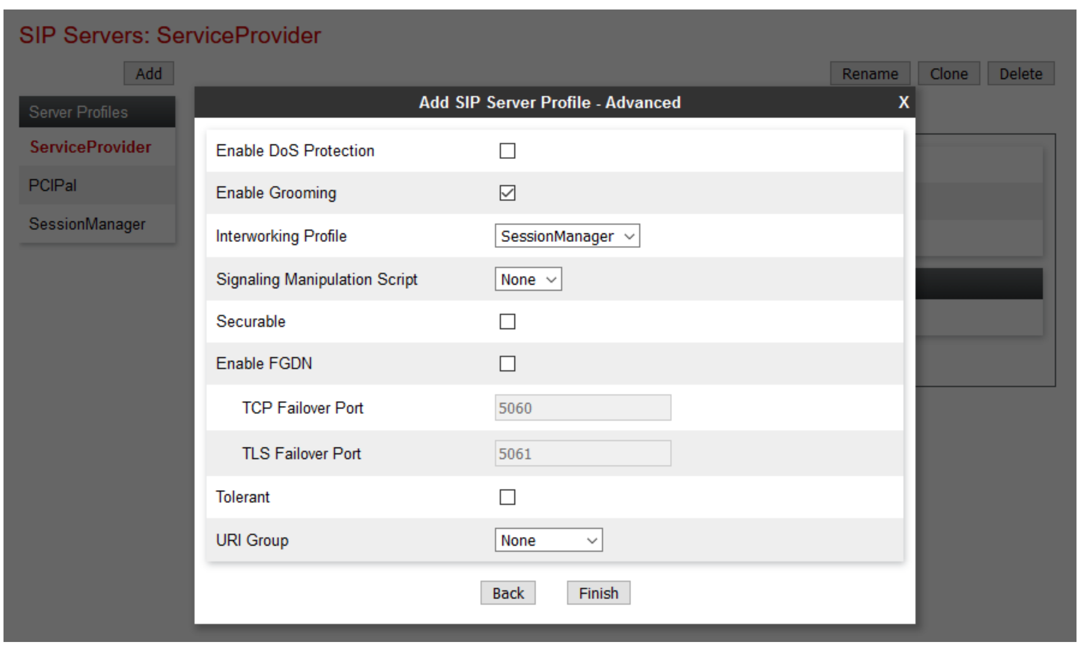


Click on **Next** and enter details in the dialogue box.

- 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 and Session Manager.
- In the **Port** box, enter the port to be used.
- In the **Transport** drop down menu, select **TLS**.
- Click on **Next**.

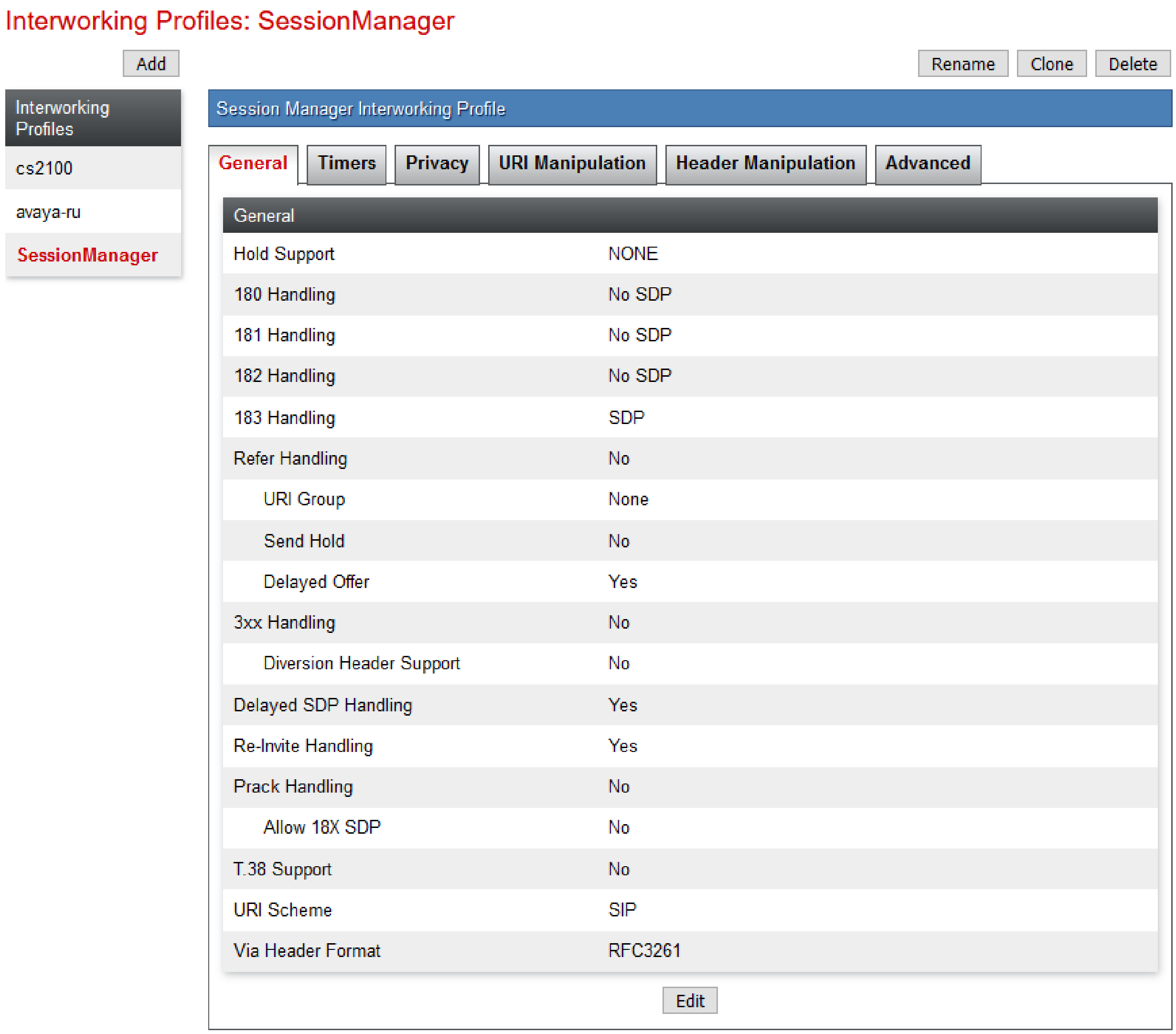


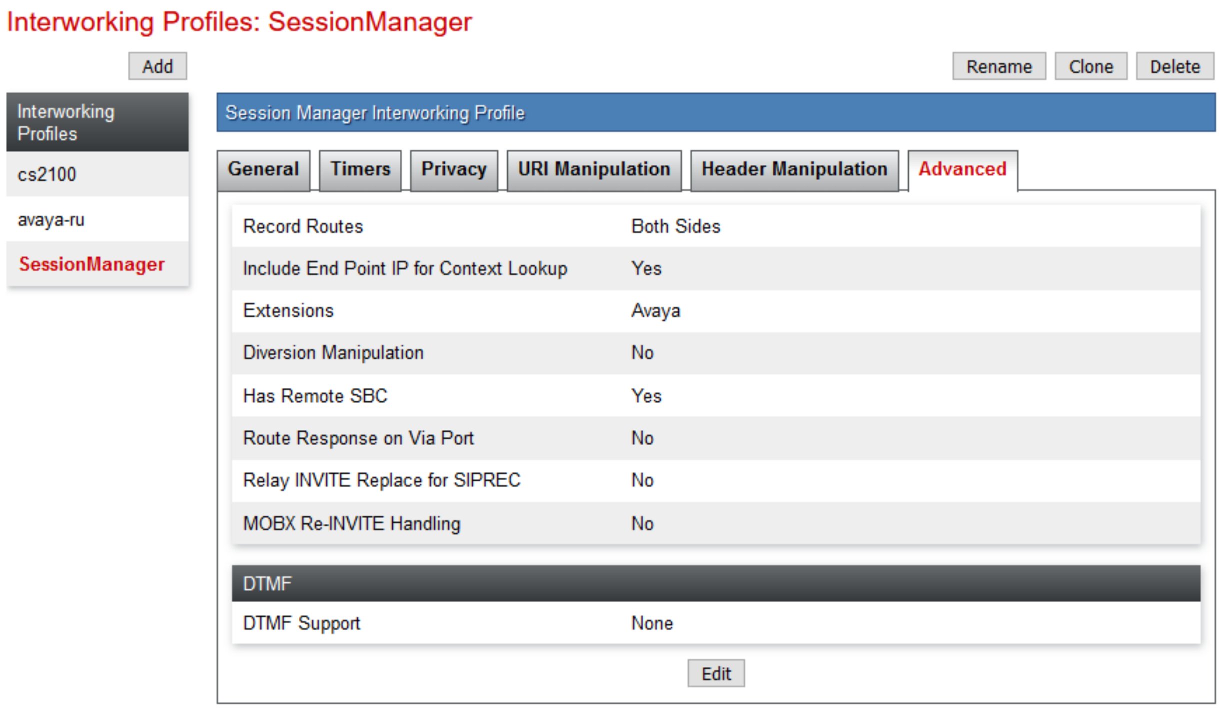

Click on **Next** until **Add SIP Server Profile – Advanced** configuration is displayed. Check box for **Enable Grooming** and select an **Interworking Profile**. The configuration of the select Interworking profile is displayed in next section.



## 8.3. 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.

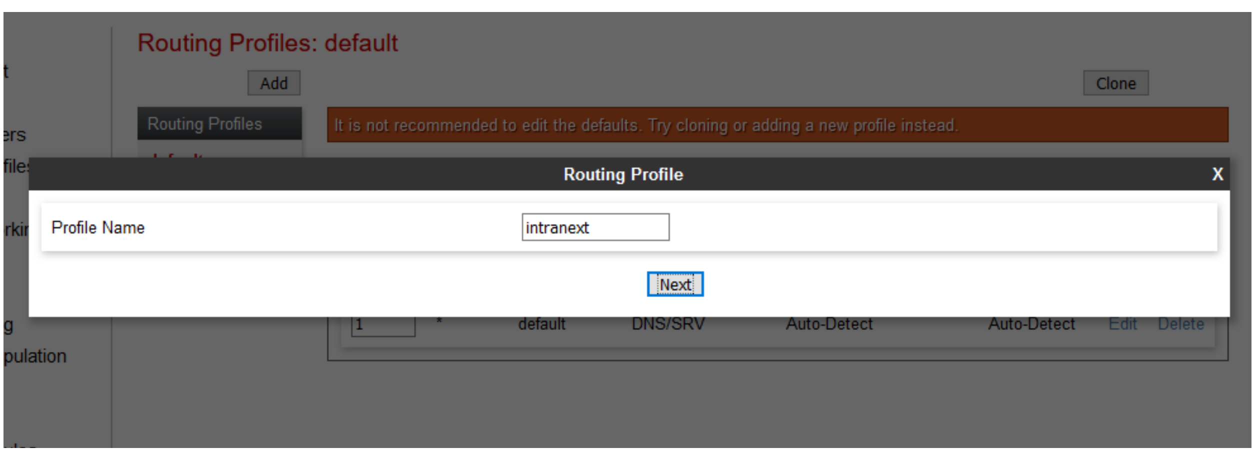





## 8.4. Define Routing

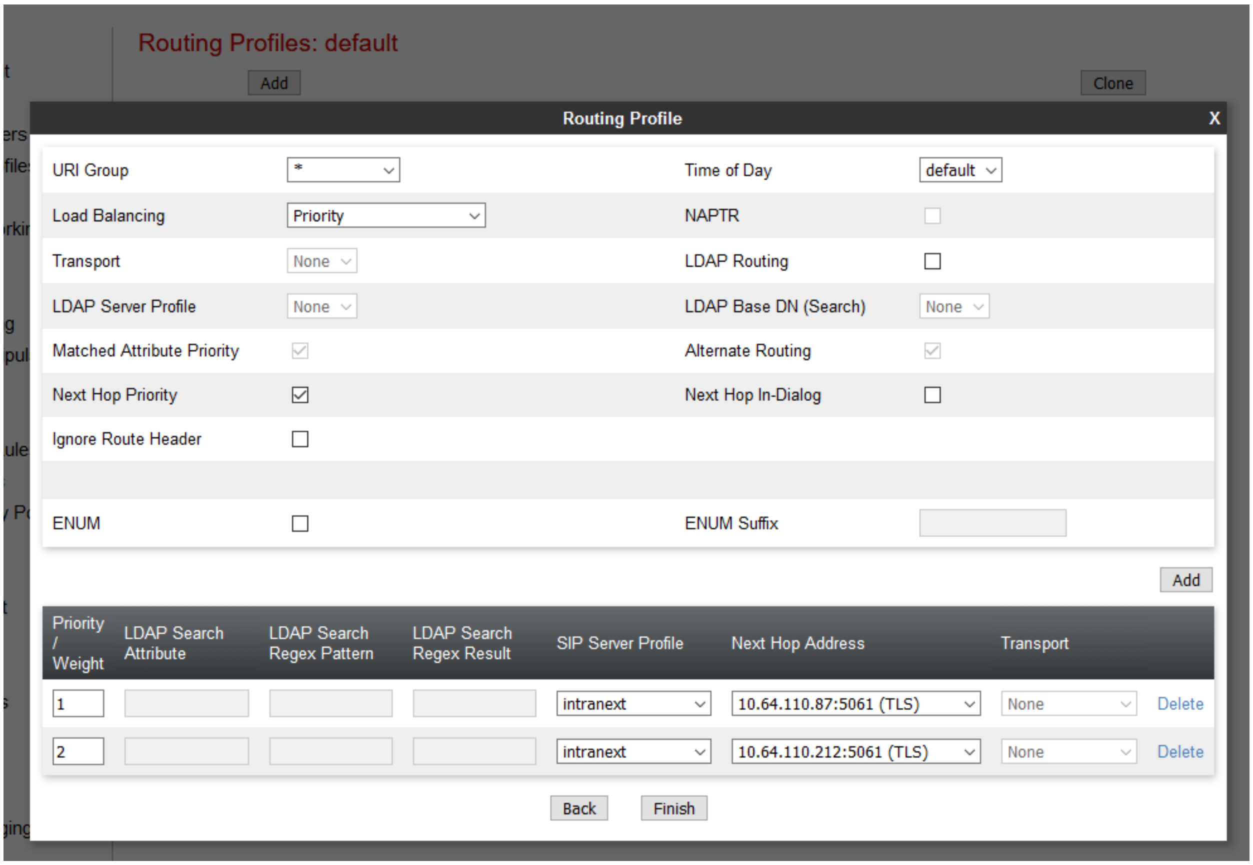
Routing information is required for routing calls to SmartSIP/Session Manager. The IP addresses and ports defined here will be used as the destination addresses for signalling.

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



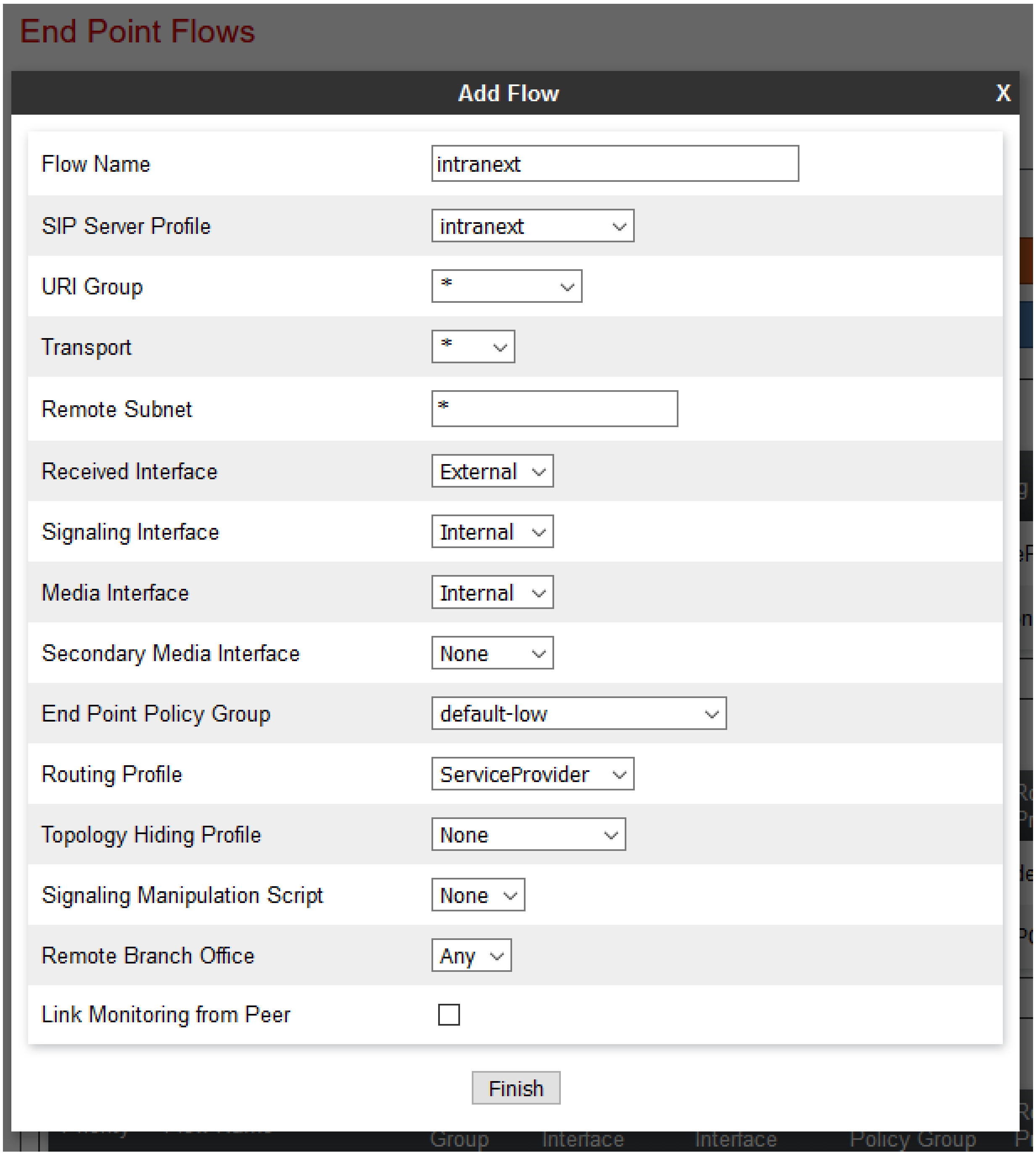
Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the 2 IP Addresses; SmartSIP and Session Manager.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used for SmartSIP IP address and **2** for Session Manager.
- Select the 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**.



## 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 Server Flows. Configure the fields as shown in the screen capture.



# 9. Configure IntraNext SmartSIP

All configuration related to SmartSIP is performed by IntraNext engineers and, thus, is not documented.

# 10. Verification Steps

To verify the status CTI Links to AES , via SAT, use the **status aesvcs cti-link**. The **Service State** of **established** indicates that the trunk is in an operational state.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     10       no    aes81             established    27       28
```

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:

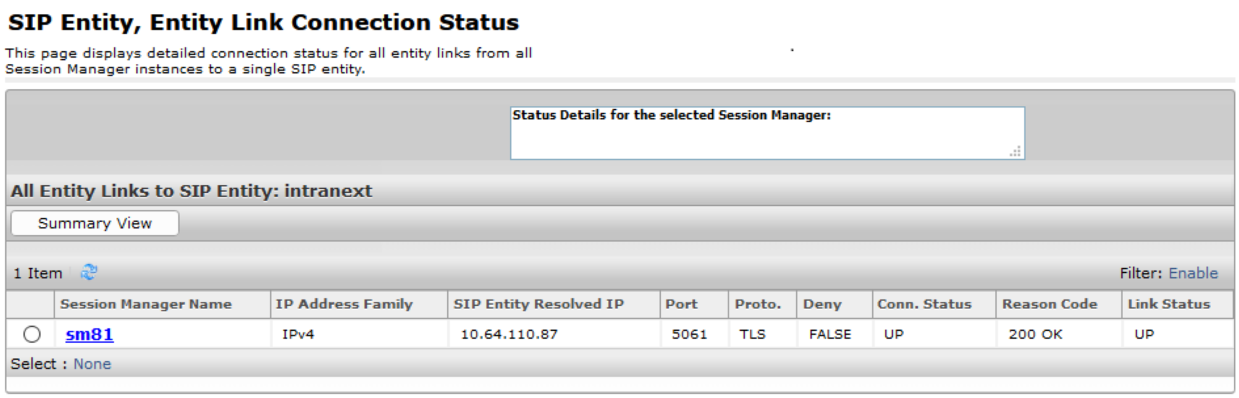
```
list monitored-station

                               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
---------------- ------- ------- ------- ------- ------- ------- ------- -------
70101            1  0004
70102            1  0009
```

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.


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



## 11. Conclusion

IntraNext SmartSIP was able to successfully interoperate with Avaya Aura® environment and Avaya Session Border Controller for Enterprise.

## 12. Additional References

Documentation related to Avaya can be obtained from https://support.avaya.com.


[1] *Administering Avaya Aura® Communication Manager, Release 8.1.x, Issue 5, November 2019.*

[2] *Administering Avaya Aura® Application Enablement Services, Release 8.1.x, Issue 3, October 2019.*

[3] *Administering Avaya Aura® Session Manager, Release 8.1.1, Issue 2, October 2019*

[4] *Administering Avaya Session Border Controller for Enterprise, Release 8.0.x, Issue 4, August 2019.*

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.