Avaya Solution & Interoperability Test Lab

Application Notes for Net Iletisim 7/24 Secure Communication Client (iOS) with Avaya Aura® Communication Manager, Avaya Aura® Session Manager via the Remote Worker Interface on Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning Net Iletisim 7/24 Secure Communication Client (iOS) R1.0.20 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 via the Remote Worker interface on Avaya Session Border Controller for Enterprise R8.1, using Avaya Aura® Web Gateway R3.8 for push notifications and Avaya Aura® Device Services R8.1 for configuration.

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 for provisioning Net Iletisim 7/24 Secure Communication Client (iOS) R1.0.20 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 via the Remote Worker interface on Avaya Session Border Controller for Enterprise R8.1, using Avaya Aura® Web Gateway R3.8 for push notifications and Avaya Aura® Device Services R8.1 for configuration. Net Iletisim 7/24 Secure Communication Client (SCC) running on Apple iOS phones behave as third-party SIP extensions on the Avaya platform. The SCC handsets are designed to make/receive internal and PSTN/external calls; however, other functions such as Transfer, Conference and Message Waiting Indication are currently not supported. The SCC handsets supports peer-to-peer and group text and multimedia messaging. SCC supports file, location and contact sharing via multimedia messaging. These features were not tested as part of the compliance testing.

Net Iletisim SCC is designed for high level security requirements. SCC protects user against man-in-the-middle attacks and complies with data privacy requirements. SCC does not include any tracking or geolocation mechanism. Information required to be kept in the mobile device is encrypted. Application data cannot be backed up to iCloud or to device disk.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of SCC handsets to make and receive calls to and from Avaya H.323, Avaya SIP, Avaya Digital and PSTN endpoints. Avaya Messaging was used to demonstrate the use of DTMF on the SCC handsets. The SCC handsets register to Session Manager as third-party SIP endpoints by connecting to the external IP interface on the Avaya Session Border Controller for Enterprise (Avaya SBCE) as remote workers. The SBCE facilitates the SIP connection to Session Manager as well as push notifications from Avaya Aura® Web Gateway (AAWG) and configuration settings from Avaya Aura® Device Services (AADS). The primary focus of the compliance testing was to ensure that the basic telephony features were observed; however, this integrated setup which involved many Avaya telephony components needed to be fully configured to allow the SCC handsets operate in any capacity.

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 Net Iletisim 7/24 Secure Communication Client (iOS) made use of TLS/SRTP as well as HTTPS connections, as requested by Net Iletisim.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/Smartphones that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/Smartphones for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP, Avaya H.323, Avaya Digital, Net Iletisim SCC and PSTN endpoints.

- Basic Calls
- Video Calls
- Long Duration Call
- Hold, Retrieve and Brokering (Toggle)
- Feature Access Code dialing
- Call Forwarding Unconditional, No Reply and Busy (PBX controlled)
- Call Waiting
- Call Park/Pickup
- EC500, where Avaya deskphone is the primary phone and SCC handset being the EC500 destination
- Calling Line Name/Identification
- Codec Support (G.711, G.729, OPUS)
- DTMF Support
- Serviceability tests

Note: Serviceability testing observed the status of the SCC phones when LAN cables were plugged out and back in again from various Avaya platforms simulating a LAN failure.

Note: Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

2.2. Test Results

The tests were all functional in nature and performance testing and redundancy testing were not included. All test cases passed successfully with the following observations/limitations noted below:

1. When a call is rejected by the SCC handset or when call is not answered it rings indefinitely. When using AAWG, Net Iletisim relies on Communication Manager to terminate the call or route to alternate point. The recommendation from Avaya is to use breeze to reject/terminate the call, where no coverage path can be used. This is an issue for all SDK clients including Avaya Workplace.
2. During registration and throughout there is a 403 Forbidden (no cellular ext) being sent from AAWG, this is a known issue and this is an issue for all SDK clients including Avaya Workplace.
3. 7/24 Secure Communication Client does not support transfers, blind or supervised.
4. 7/24 Secure Communication Client does not support 3rd party conference other than adding parties from its contacts to an existing call.
5. 7/24 Secure Communication Client does not support Message Waiting Indication.
6. 7/24 Secure Communication Client does not support local call diversion.
7. All compliance testing was carried using TLS/SRTP as the transport protocol.
8. OPUS was the preferred CODEC used throughout compliance testing as per the request of Net Iletisim.

2.3. Support

Support from Avaya is available by visiting the website http://support.avaya.com and a list of product documentation can be found in **Section 15** of these Application Notes. Technical support for the Net Iletisim 7/24 Secure Communication Client (iOS) handsets can be obtained as follows:

- Web: http://netiletisim.com.tr/#contact
- Email: netiletisim@netiletisim.com.tr
- Telephone: +90 (312) 419 29 99 | Ankara

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Secure Communication Client located in Net Iletsim Lab connects to the Avaya platform over the WAN to the Avaya Session Border Controller for Enterprise and the Net Iletisim SAS server, both located in the Avaya Lab. The Secure Communication Client registers with Session Manager to make/receive calls to and from the Avaya SIP, H.323 and Digital deskphones on Communication Manager.

Note: PSTN calls were simulated using an ISDN trunk connecting to Avaya IP Office.

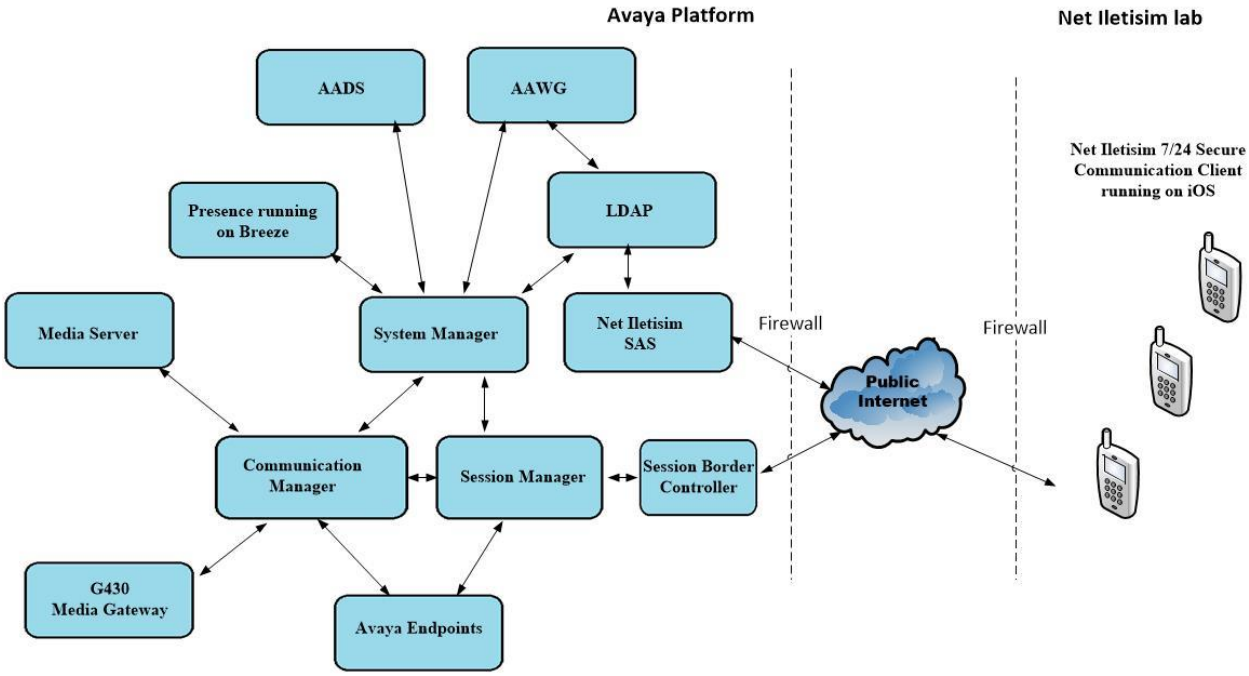


Figure 1: Network Solution of Net Iletisim 7/24 Secure Communication Client with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1

4. Equipment and Software Validated

The following equipment and software were used for the compliance test.

Avaya Equipment	Software / Firmware Version
Avaya Aura® System Manager	System Manager 8.1.3.1 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012493 Service Pack 1
Avaya Aura® Session Manager	Session Manager R8.1.3.1 Build No. – 8.1.3.1.813113
Avaya Aura® Communication Manager	R8.1.3.0.0 – FP3 R018x.01.0.890.0 Update ID 01.0.890.0-26568
Avaya Aura® Media Server	Appliance Version R8.0.0.19 Media Server 8.0.2.138 Element Manager 8.0. 2.138
Avaya G450 Media Gateway	40.20.0/2
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya Aura® Web Gateway	3.8.1.0.153
Avaya Aura® Device Services	8.1.3.0.293
Avaya Presence Services running on Avaya Breeze®	Breeze 3.7.0.0.370008 Presence Services 8.1.2.0.23
Avaya J179 H.323 Deskphone	6.8304
Avaya J189 SIP Deskphone	4.0.7.0.7
Avaya 9404 Digital Phone	2.00
Net Iletisim Equipment	**Software / Firmware Version**
Secure Communication Client running on iOS 14.6	1.0.20
SAS running on Windows 2019 Server	1.7
LDAP running on Windows 2019 Server	N/A

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with SIP trunks in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 15** of these Application Notes.

Note: A printout of the Signalling and Trunk Groups that were used during compliance testing can be found in the **Appendix** of these Application Notes.

The following sections run through the following.

- System Parameters
- Dial Plan Analysis
- Feature Access Codes
- Network Region
- IP Codec

5.1. Configure System Parameters

Ensure that the SIP endpoints license is valid as shown below by using the command **display system-parameters customer-options**.

```
display system-parameters customer-options                  Page   1 of  12
                                OPTIONAL FEATURES

     G3 Version: V18                            Software Package: Enterprise
       Location: 2                               System ID (SID): 1
       Platform: 28                              Module ID (MID): 1

                                                          USED
                                Platform Maximum Ports: 48000 168
                                      Maximum Stations: 36000 44
                             Maximum XMOBILE Stations: 36000 0
                     Maximum Off-PBX Telephones - EC500: 41000 2
                     Maximum Off-PBX Telephones -   OPS: 41000 20
                     Maximum Off-PBX Telephones - PBFMC: 41000 0
                     Maximum Off-PBX Telephones - PVFMC: 41000 0
                     Maximum Off-PBX Telephones - SCCAN: 0     0
                          Maximum Survivable Processors: 313   1
```

5.2. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **21**. Feature Access Codes (**fac**) use digits **8** and **9** and use characters ***** or **#**.

```
change dialplan analysis                                        Page   1 of  12
                              DIAL PLAN ANALYSIS TABLE
                                    Location: all            Percent Full: 5

    Dialed   Total  Call     Dialed   Total  Call     Dialed   Total  Call
    String   Length Type     String   Length Type     String   Length Type
   21          4   ext
   3           4   udp
   8           1   fac
   9           1   fac
   *8          4   dac
   *           3   fac
   #           3   fac
```

5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure access codes which can be entered from the SCC handsets to initiate Communication Manager Call features. These access codes must be compatible with the dial plan described in **Section 5.2**. Some of the access codes configured during compliance testing are shown below.

```
change feature-access-codes                                     Page   1 of  12
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *11
         Abbreviated Dialing List2 Access Code: *12
         Abbreviated Dialing List3 Access Code: *13
Abbreviated Dial - Prgm Group List Access Code: *10
                      Announcement Access Code: *27
                       Answer Back Access Code: #02
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *05    Deactivation: #05
Call Forwarding Activation Busy/DA: *03    All: *04    Deactivation: #04
   Call Forwarding Enhanced Status: *73    Act: *74    Deactivation: #74
                         Call Park Access Code: *02
                       Call Pickup Access Code: *09
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code: *14
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

5.4. Configure Network Region

Use **change ip-network-region x** (where x is the network region to be configured) to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnectprogram.com** is used. Note that this domain is also configured in **Section 7.1.1**.

```
change ip-network-region 1                                     Page   1 of  20
                                IP NETWORK REGION
  Region: 1       NR Group: 1
Location: 1       Authoritative Domain: devconnectprogram.com
    Name: Remote Worker         Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
```

5.5. Configure IP-Codec

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the SCC. During compliance testing the preferred codec was **OPUS-WB2 0K** and **G.711A**, **G.711MUA** and **G.729** were tested. Media Encryption was set to use **1-srtp-aescm128-hmac80** as the preferred encryption.

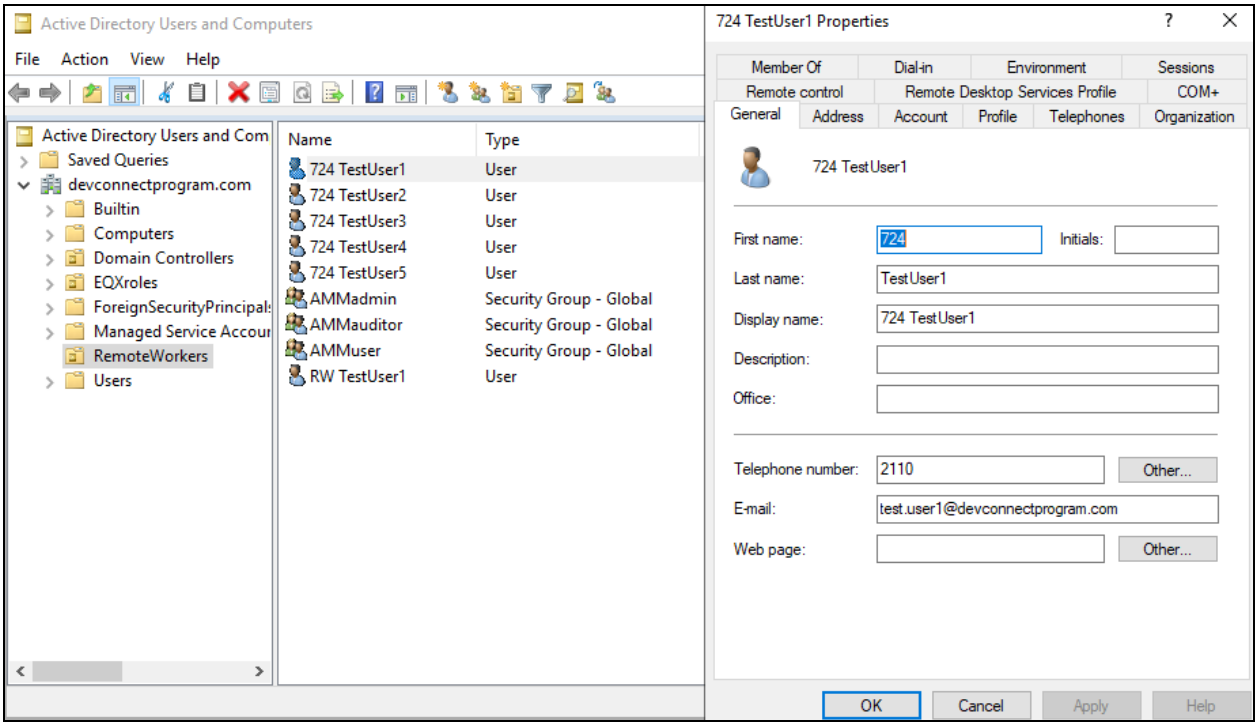
```
change ip-codec-set 1                                          Page   1 of   2
                           IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: OPUS-WB2 0K       n         1        20
 2: G.711A            n         2        20
 3: G.711MU           n         2        20
 4: G.729             n         2        20
 5:
     Media Encryption                   Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
 4:
```

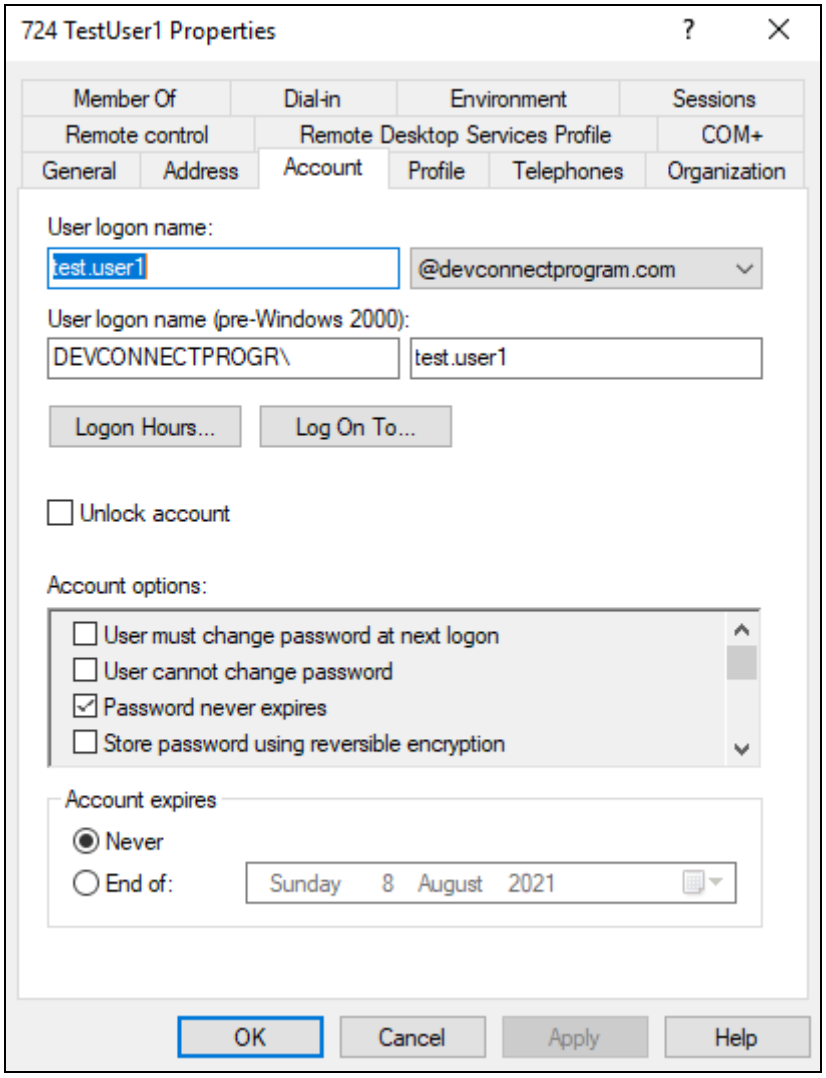
6. Adding Net Iletisim 7/24 Secure Communication Client Users on LDAP Server

The Net Iletisim 7/24 Secure Communication Client users are added to the domain as domain users. These users are then synchronized with the users on System Manager as shown in **Section 7.2**. To allow System Manager to synchronize with the LDAP server correctly, the users should be added here first.

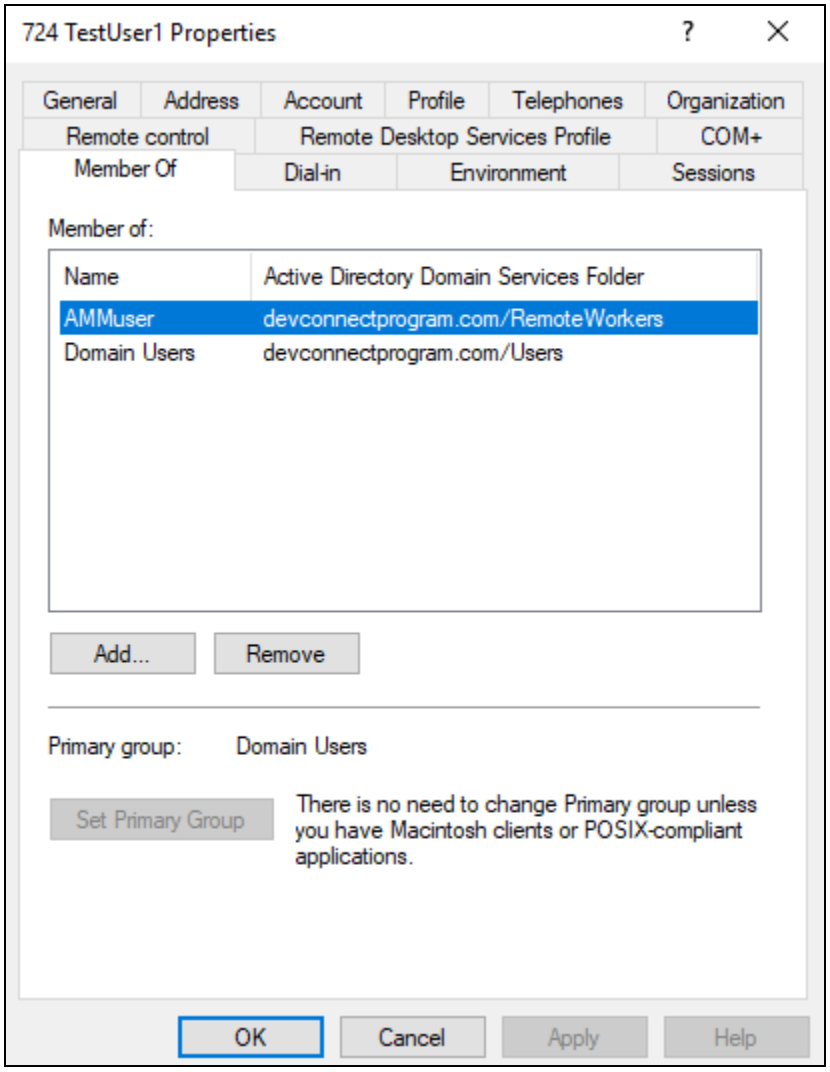
Five users were added, **724 TestUser1** to **724 TestUser5**. 724TestUser1 is opened below to show the details of these users. Enter a suitable name and ensure that the **Telephone number** is allocated correctly to this user, this will be the same number added for the user configured in System Manager as per **Section 7.3**.



The **User logon name** should be noted as it will be required for the configuration of the SAS server.

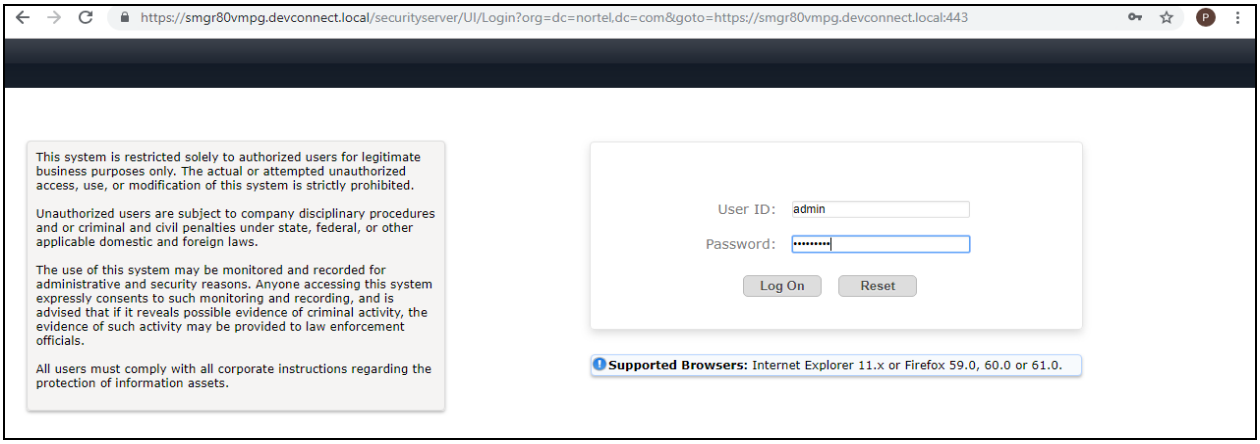


These users for Net Iletisim are all added to the **Domain Users** by default but are also added to **AMMuser,** which is a group set up specially for these Remote Worker users.

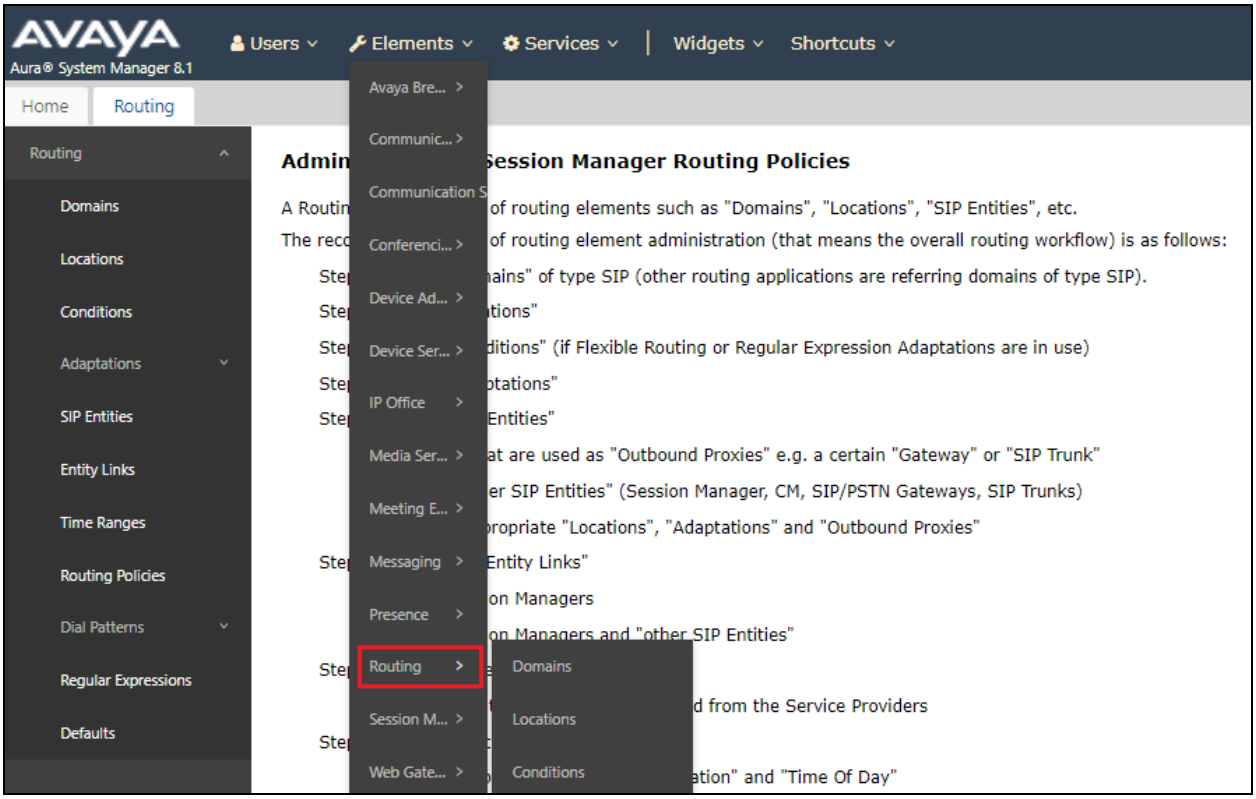


7. Configure Avaya Aura® System Manager

The SCC handsets are added to Session Manager as SIP users. To make changes on Session Manager a web session is established to System Manager. Log into System Manager by opening a web browser and navigating to https://<System Manager FQDN>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



Once logged in navigate to **Elements** and click on **Routing** highlighted below.

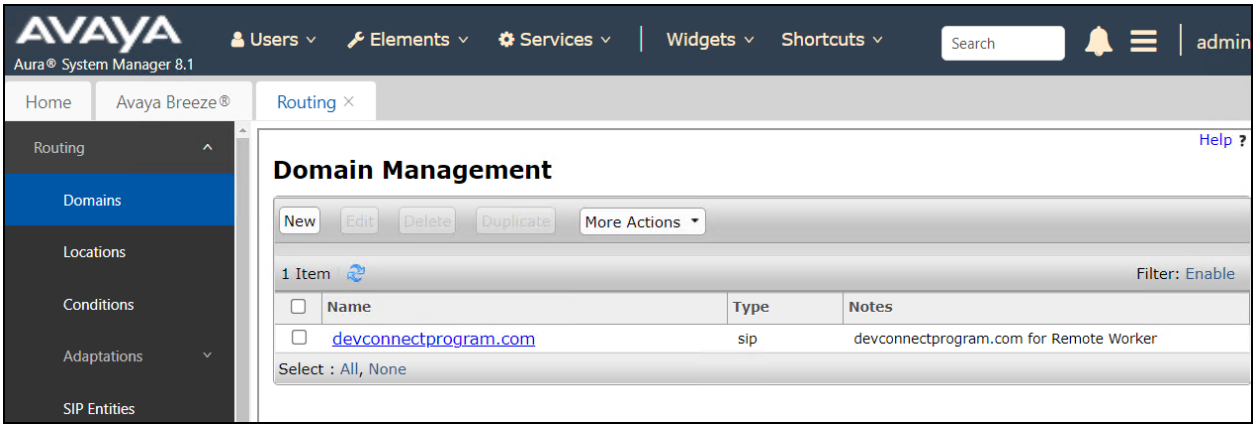


7.1. Domains and Locations

Note: It is assumed that a domain and a location have already been configured, therefore a quick overview of the domain and location that was used in compliance testing is provided here.

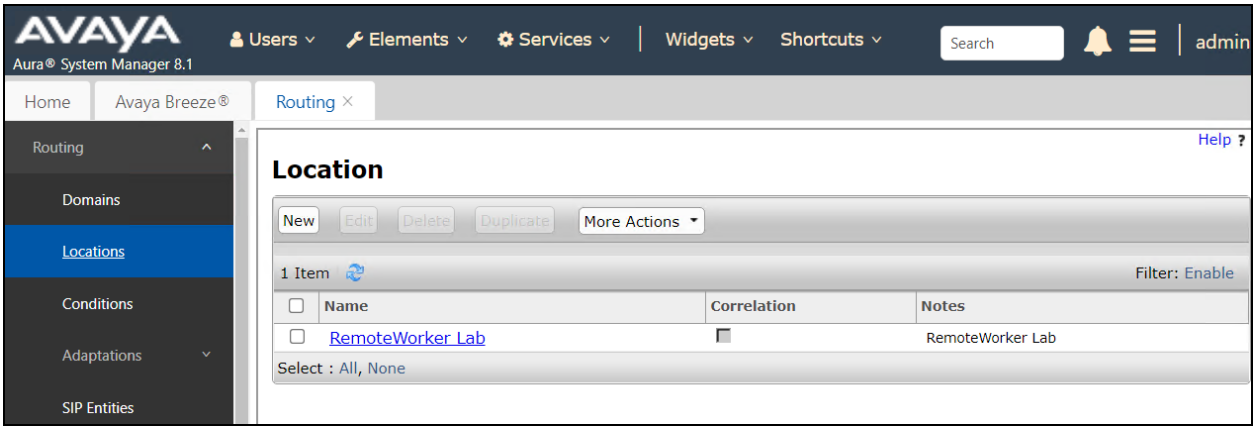
7.1.1. Display the Domain

Select **Domains** from the left window. This will display the domain configured on Session Manager. For compliance testing this domain was **devconnectprogram.com** as shown below. If a domain is not already in place, click on **New**. This will open a new window (not shown) where the domain can be added.



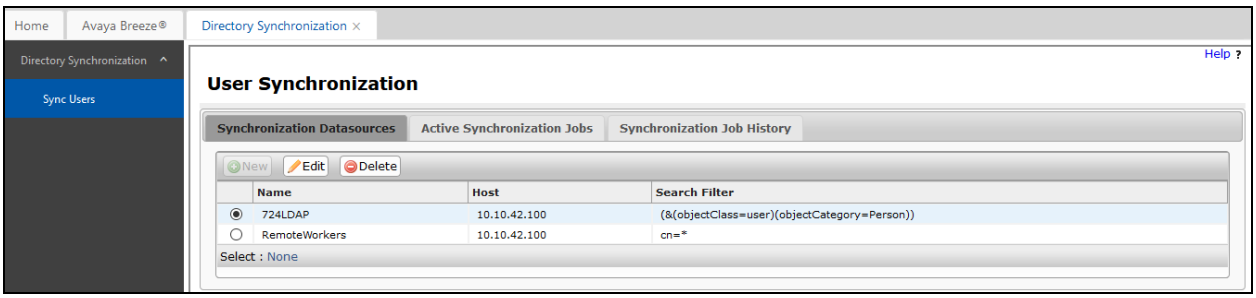
7.1.2. Display the Location

Select **Locations** from the left window and this will display the location setup. The example below shows the location **RemoteWorker Lab** which was used for compliance testing. If a location is not already in place, then one must be added to include the IP address range of the Avaya solution. Click on **New** to add a new location.



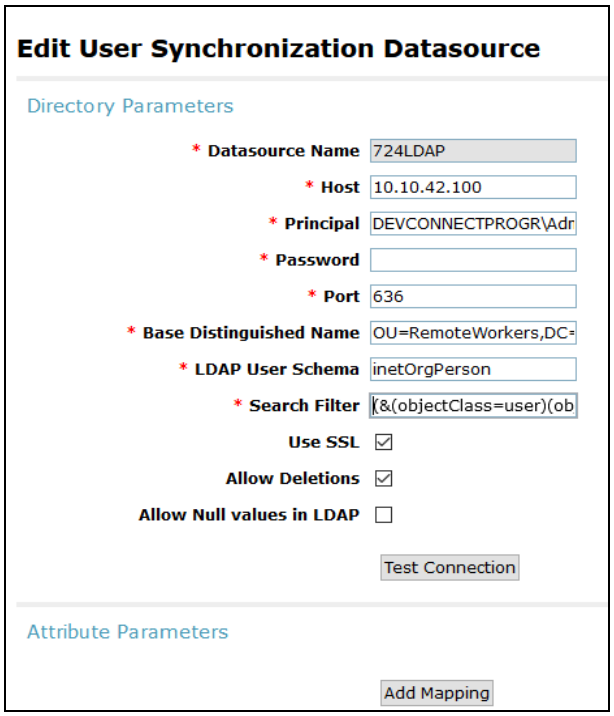
7.2. Synchronizing System Manager Users and LDAP Users

The users added to the domain need to be synchronised to System Manager to allow the SCC handsets to verify their credentials using Active Directory. Once they are synchronised, they can be amended to add some more telephony details. Navigate to **Users → Directory Synchronization → Sync Users** (not shown), and the **User Synchronization** page is shown below. The current synchronization called **724LDAP** is already present, but clicking on **New** will create a new window where a new user synchronization can be added. The following screen shots will show the information on the existing user synchronization.

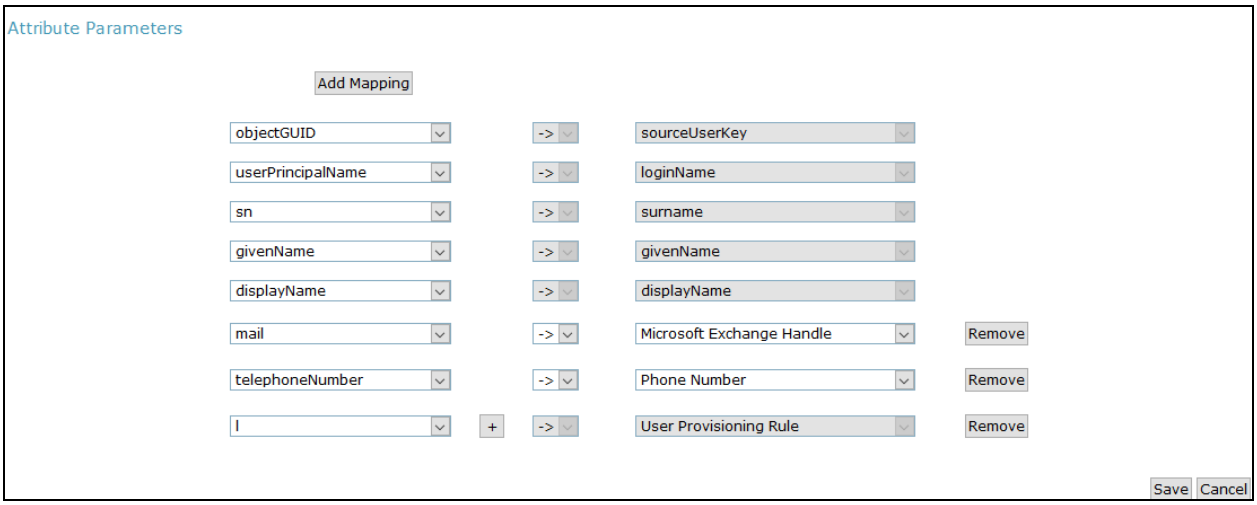


Enter a suitable **Datasource Name** and the **Host** will be the IP address of the LDAP server. The **Principle** and **Password** is the administrator user and password for the LDAP server. The **Port** is set to **636** and the following are set.

- **Base Distinguished Name**: ou=RemoteWorkers,dc=devconnectprogram,dc=com
- **LDAP User Schema**: inetOrgPerson
- **Search Filter**: (&(objectClass=user)(objectCategory=Person))



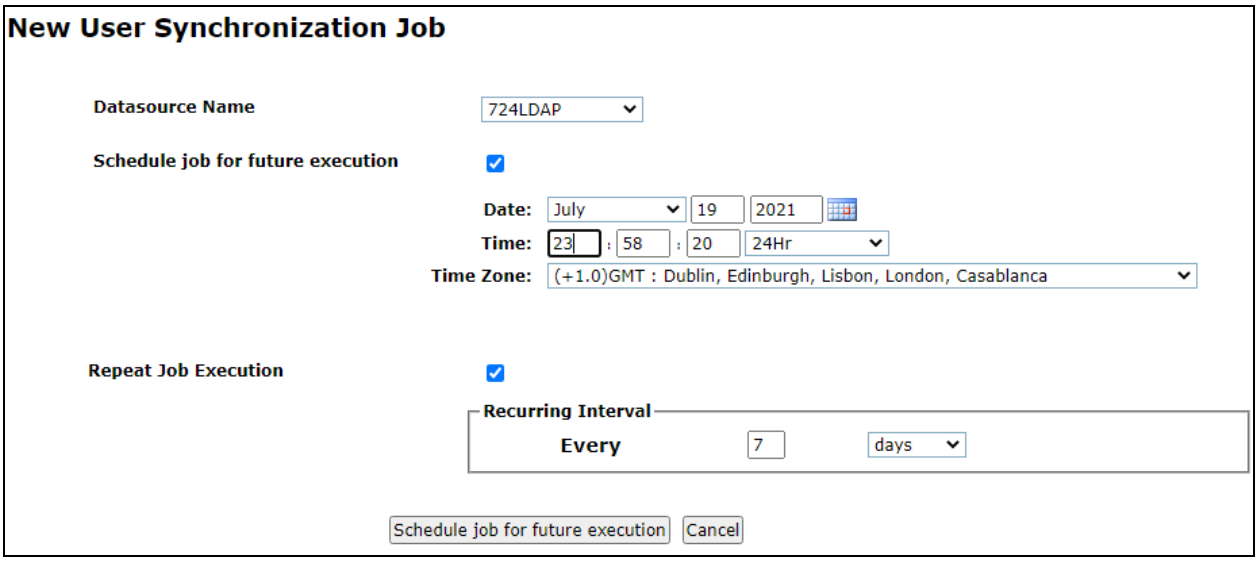
A number of **Attribute Parameters** are mapped to allow the synchronization take place, click on **Add Mapping** to add a new mapping for each attribute. There are eight added as shown below and these are the suggested mappings to correctly synchronize the users. Click on **Save** once this is complete as shown below.



Once the users are ready to be synchronized a new job can be added to begin the synchronization. Click on the **Active Synchronization Jobs** tab and then click **Create New Job**.

Select the **Datasource Name** from the drop-down menu, which was previously created. The new job can either by run immediately by pressing the **Run Job** button, as shown below, or this can be scheduled to run by ticking the **Schedule job for future execution** box.

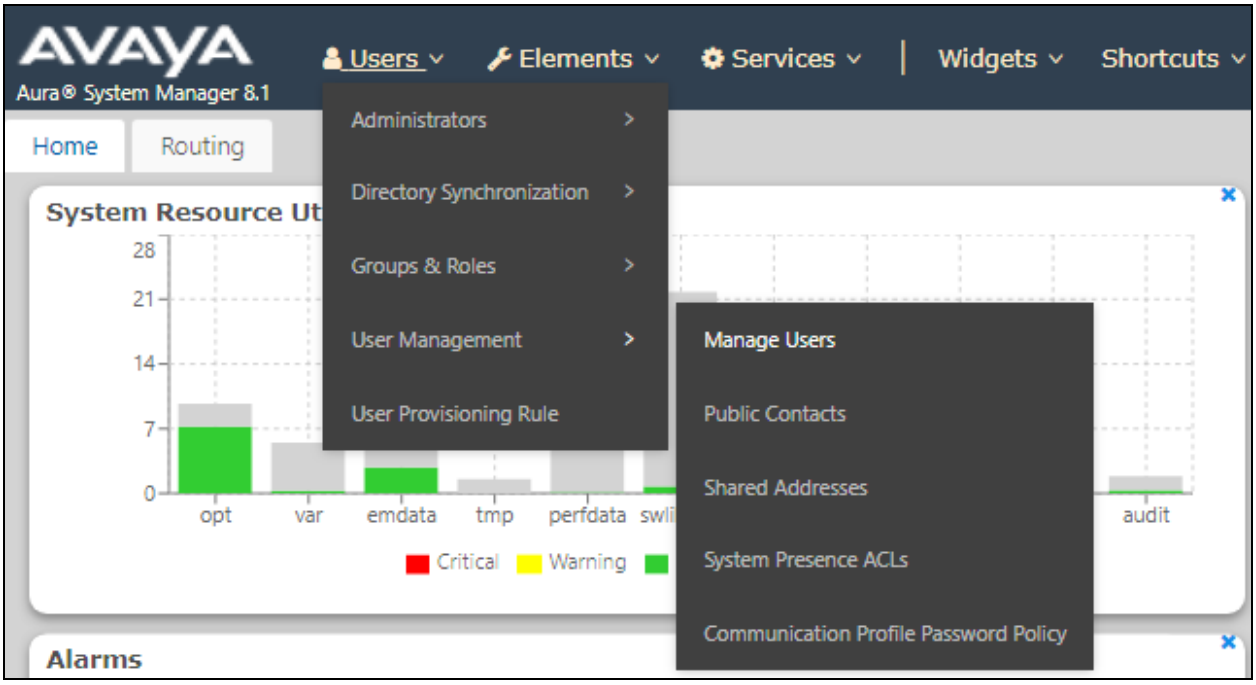
The job can be scheduled to run once or can be reoccurring by ticking the **Repeat Job Execution** box, as shown below.



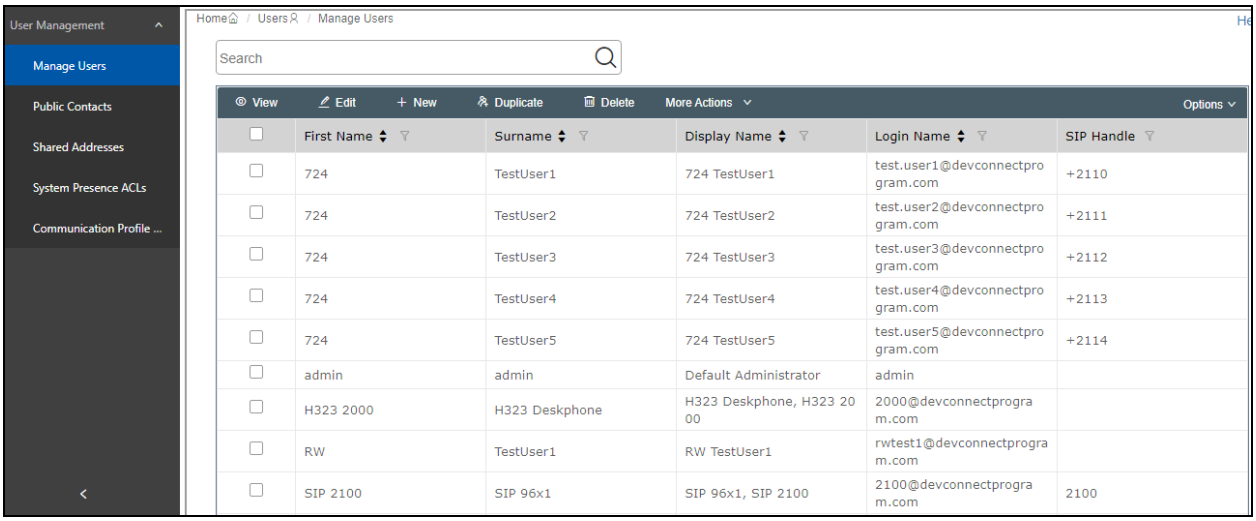
Once the synchronization is complete the users created on the LDAP server should appear under **Users** on System Manager. These users will still need to be amended to add some SIP telephony features and allow the phones register to Session Manager.

7.3. Manage Net Iletisim 7/24 Secure Communication Client Users

From the home page, click on **Users → User Management → Manager Users** shown below.

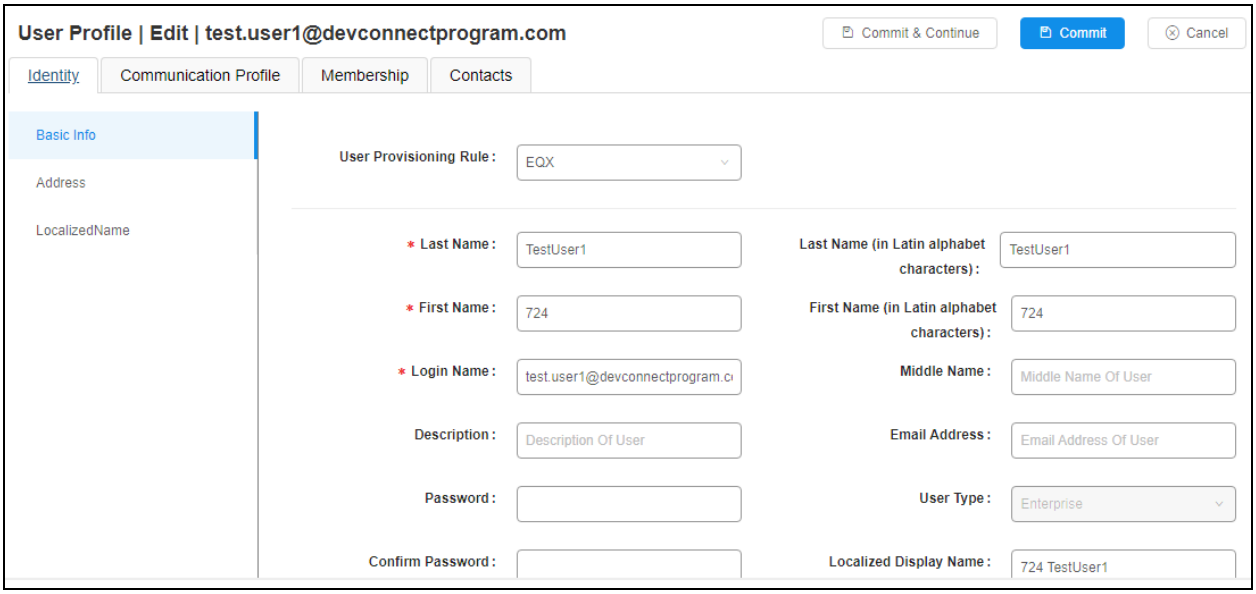


From **Manager Users** section, all the 724 SCC users should be visible as shown. These users were all added to the LDAP server and are all now present on System Manager. These users will need to be amended to add some telephony features and can be done so by clicking on the box beside the user in question and clicking on **Edit**.

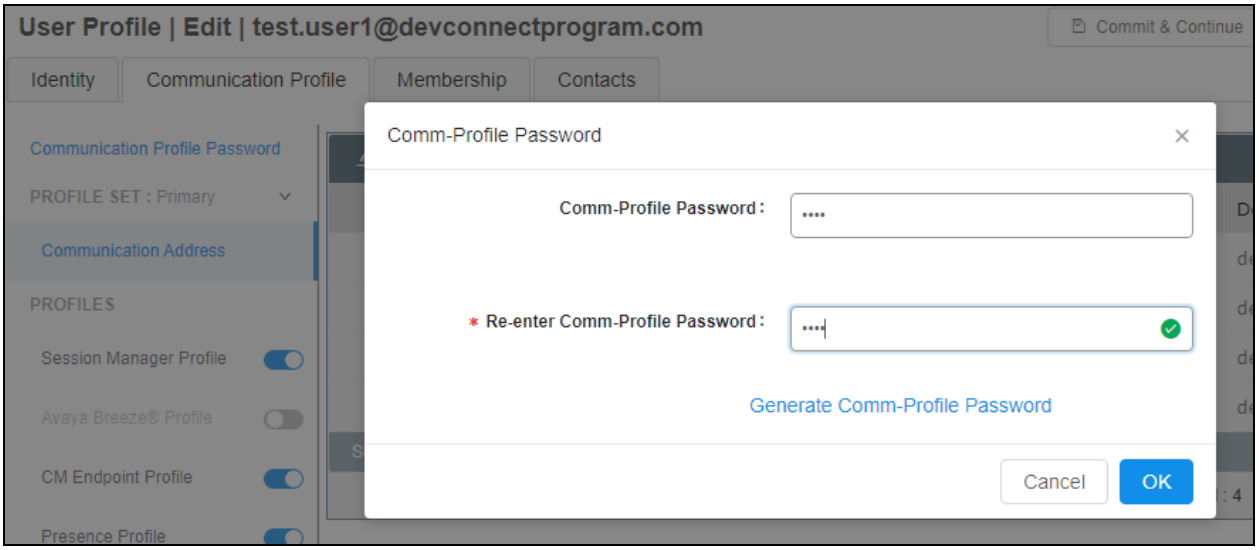


First Name	Surname	Display Name	Login Name	SIP Handle
724	TestUser1	724 TestUser1	test.user1@devconnectprogram.com	+2110
724	TestUser2	724 TestUser2	test.user2@devconnectprogram.com	+2111
724	TestUser3	724 TestUser3	test.user3@devconnectprogram.com	+2112
724	TestUser4	724 TestUser4	test.user4@devconnectprogram.com	+2113
724	TestUser5	724 TestUser5	test.user5@devconnectprogram.com	+2114
admin	admin	Default Administrator	admin	
H323 2000	H323 Deskphone	H323 Deskphone, H323 2000	2000@devconnectprogram.com	
RW	TestUser1	RW TestUser1	rwtest1@devconnectprogram.com	
SIP 2100	SIP 96x1	SIP 96x1, SIP 2100	2100@devconnectprogram.com	2100

The details in the **Identity** tab should show the same information as that filled out during the creation of the user on the LDAP server as per **Section 6**. Nothing more should need to be added here but can be done should it be required.



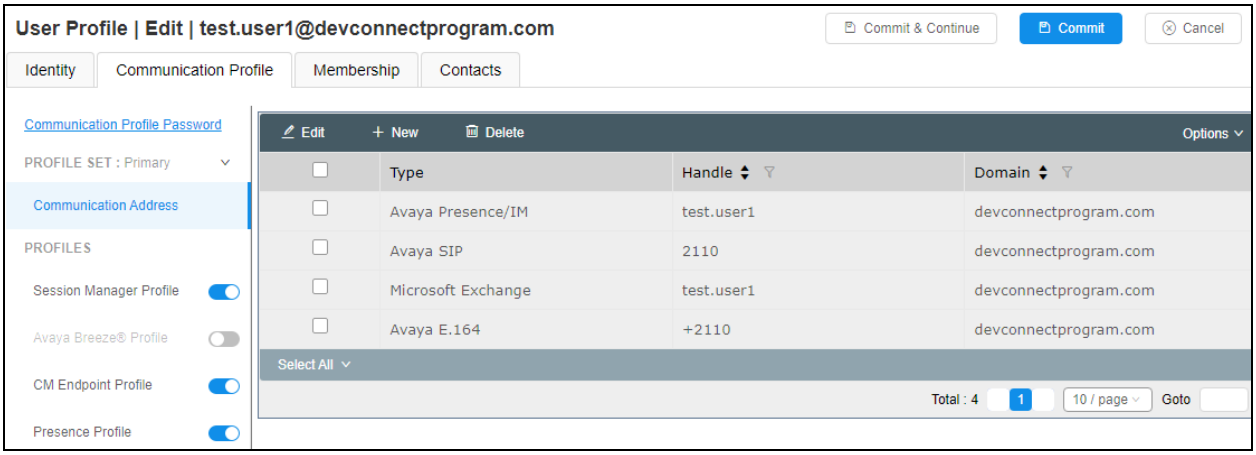
Under the **Communication Profile** tab enter **Communication Profile Password** and **Confirm Password**, note that this password is required when configuring the SCC handset.



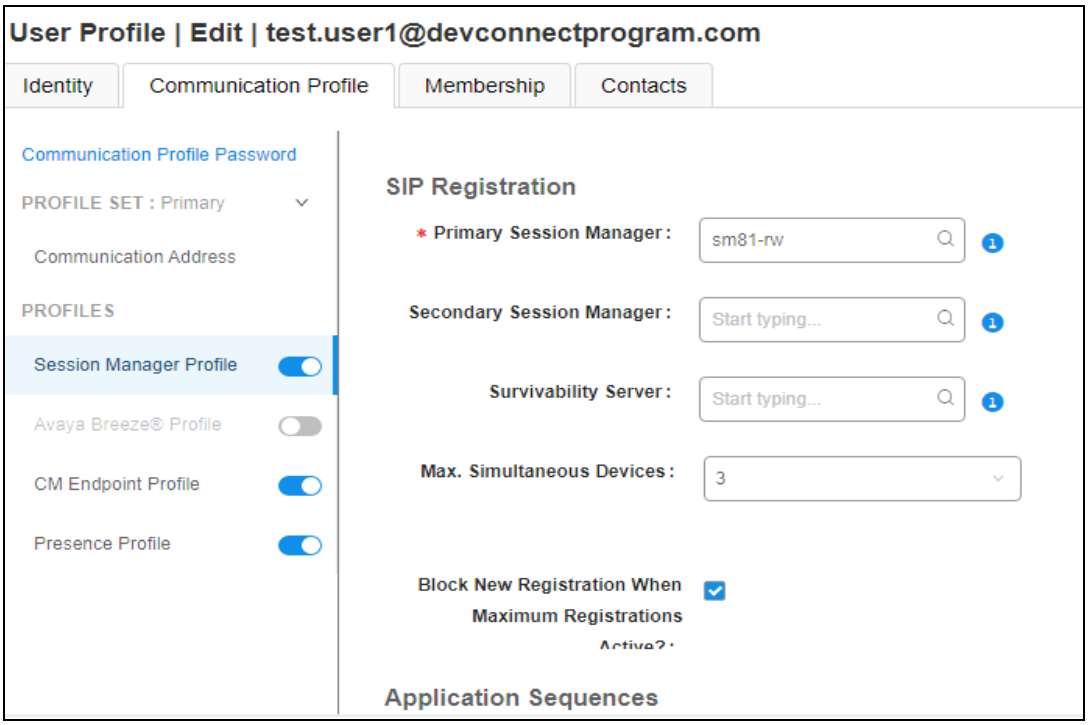
Staying on the **Communication Profile** tab, click on **New** to add a new **Communication Address**. The following four addresses should be added.

- Avaya Presence/IM
- Avaya SIP
- Microsoft Exchange
- Avaya E.164

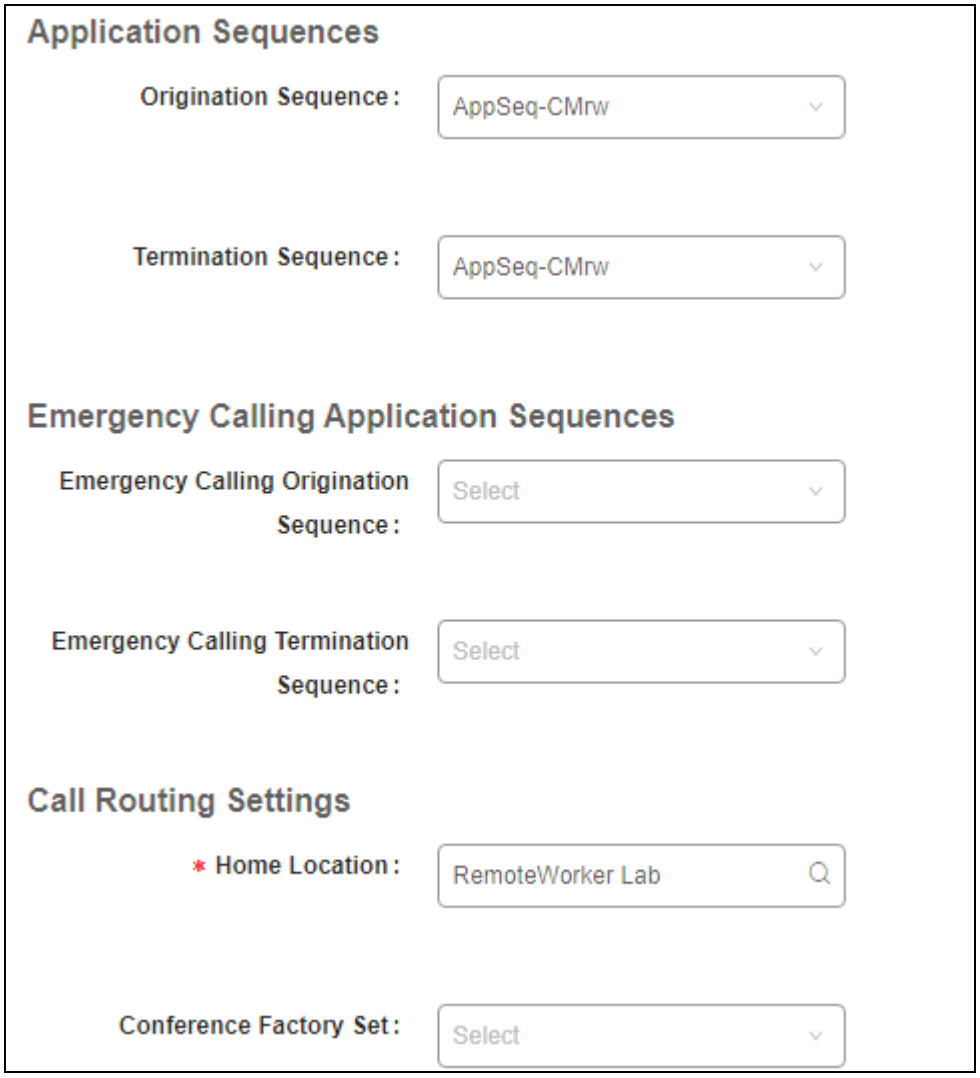
These are shown below fully configured for the **devconnectprogram.com** domain.



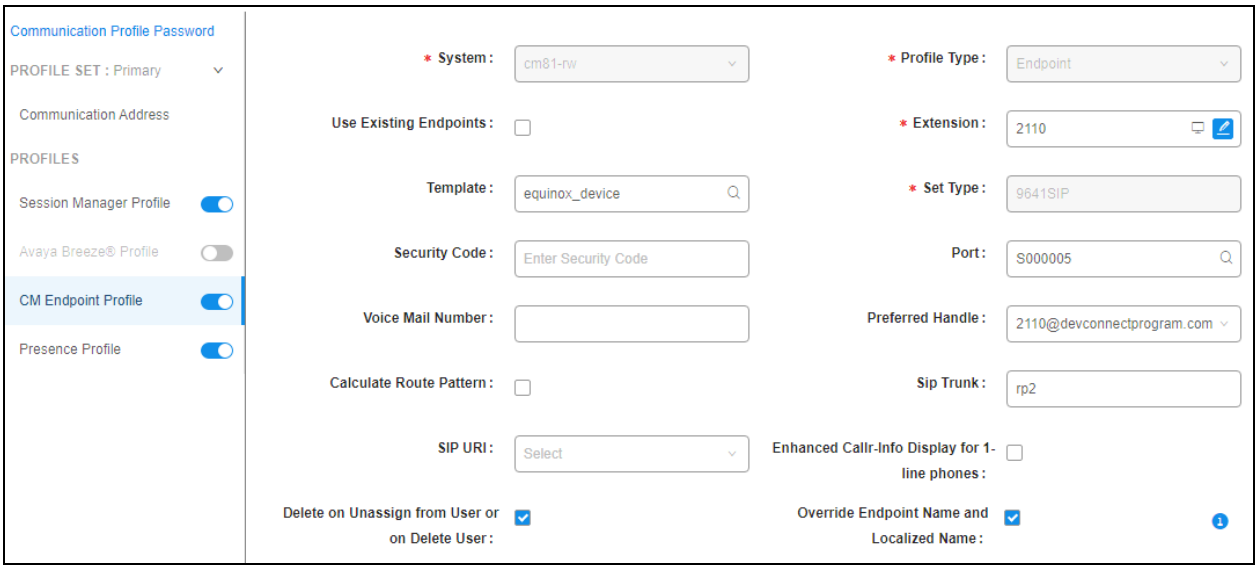
Ensure **Session Manager Profile** is checked and enter the **Primary Session Manager** details and scroll down to complete the profile.



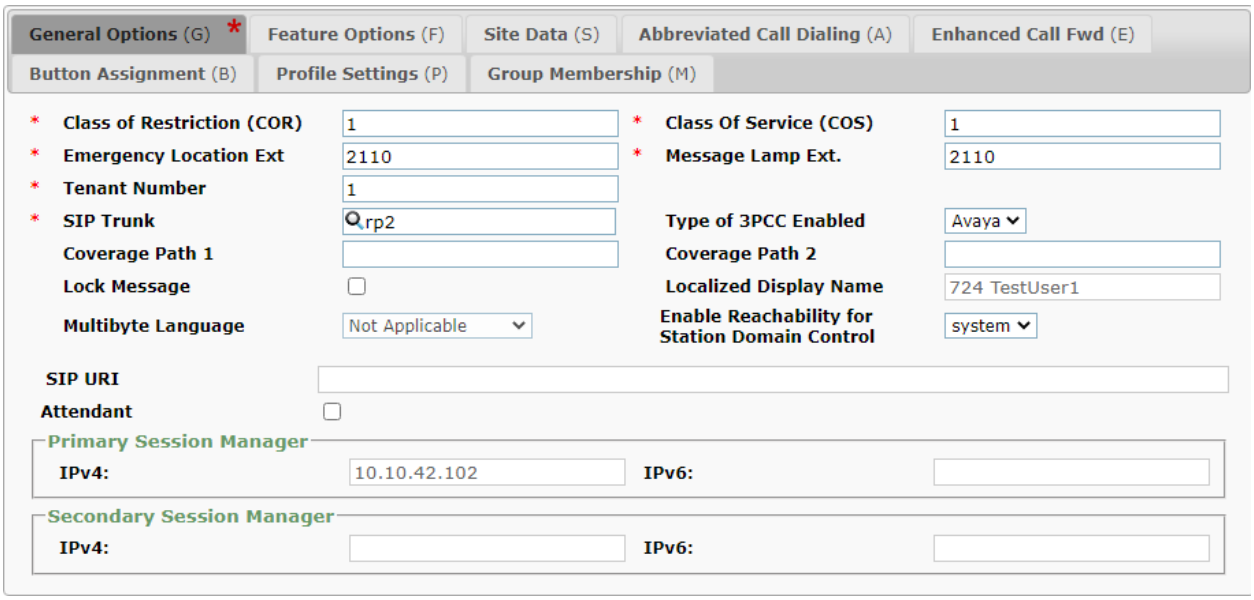
The appropriate **Application Sequences** are selected as well as the **Home Location** as per **Section 7.1.2**.



Ensure that **CM Endpoint Profile** is selected in the left window. Select the Communication Manager that is configured for the **System** and choose **equinox_device** as the **Template**. The other values should be added by default. Click on **Endpoint Editor** to configure the buttons and features for that handset on Communication Manager.

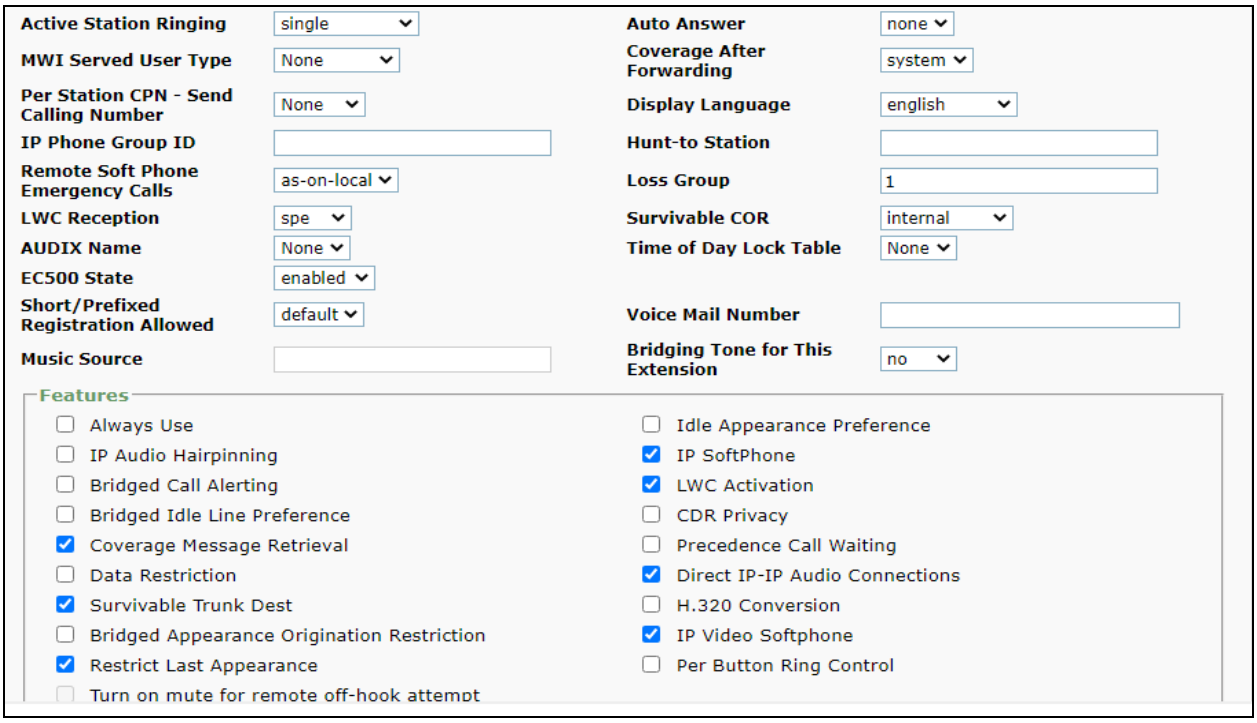


Under the **General Options** tab, the **Type of 3PCC Enabled** should be set to **Avaya**.

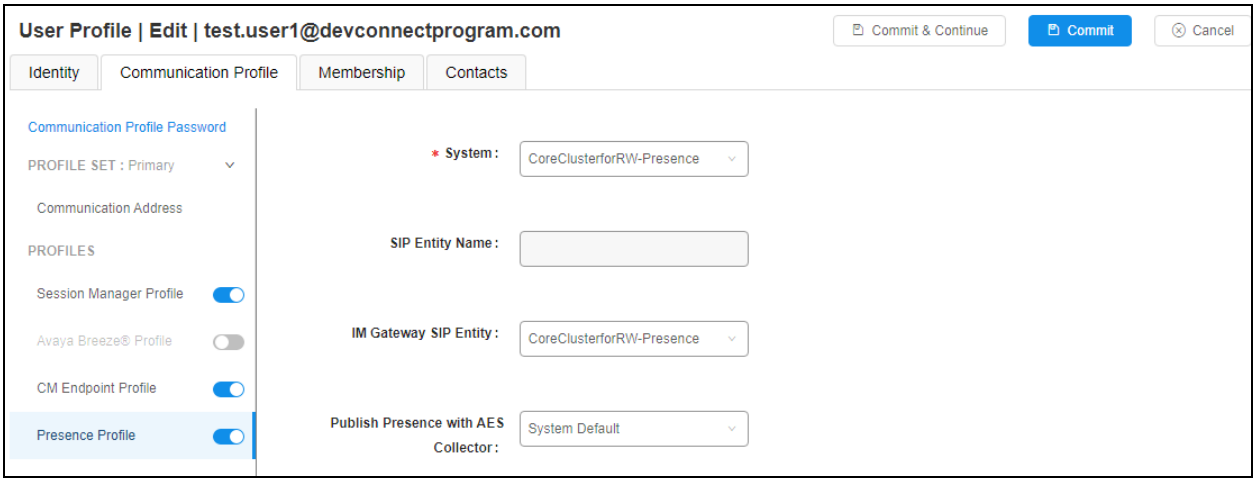


Under the **Feature Options** tab (see previous page) ensure that **IP Softphone** and **IP Video Softphone** are ticked. Other tabs can be checked but for compliance testing the values were left as default. Click on **Done** (not shown) to complete.

Note: For compliance testing the default value of three call appearance buttons were used. This can be changed under the **Button Assignment** tab.

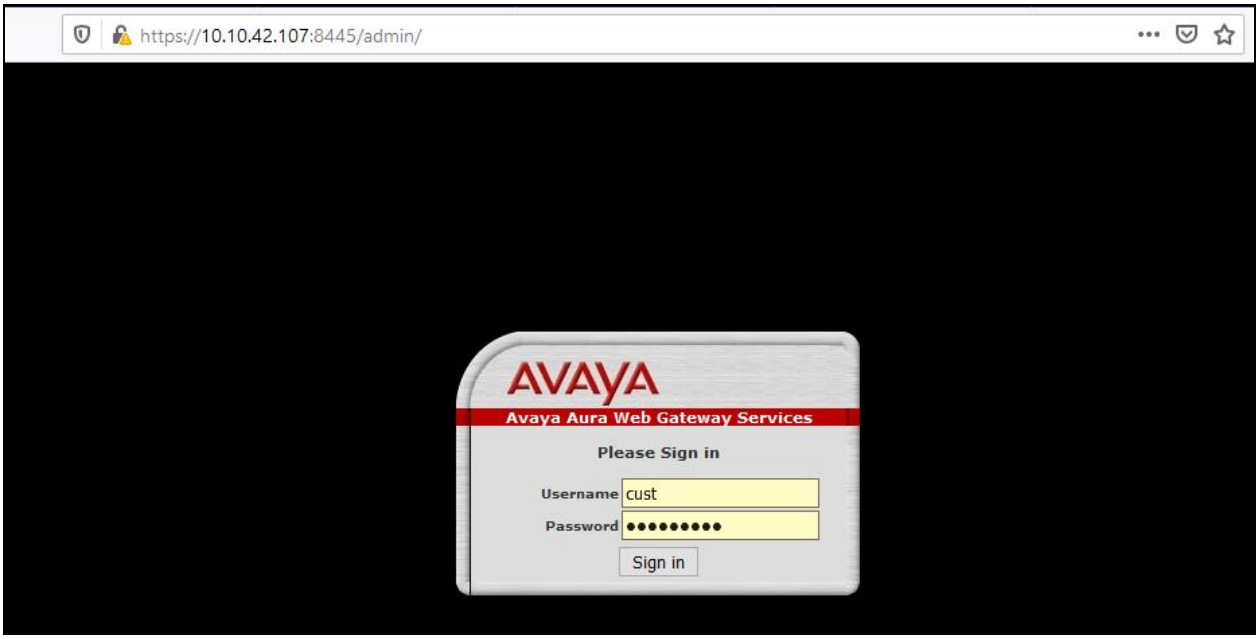


Once the **CM Endpoint Profile** is completed correctly, click on **Presence Profile** in the left window and set the appropriate values. The setup of the Avaya Presence Server is outside the scope of these Application Notes, typically this is set up on an Avaya Breeze Cluster and that is what is shown below. Click on **Commit** to save the new user.

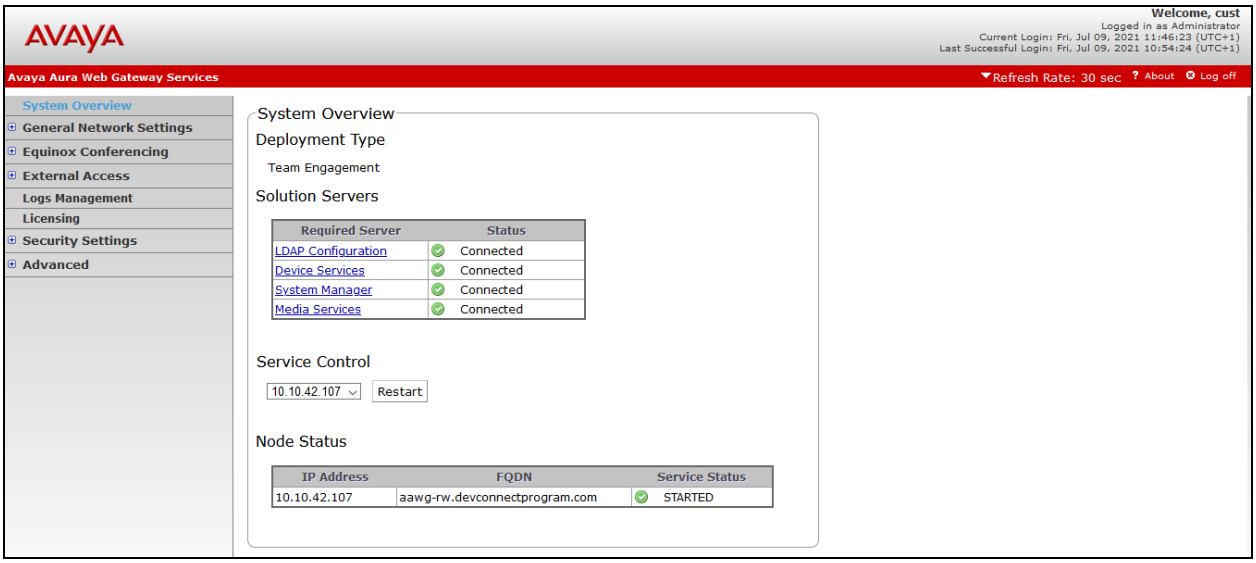


8. Configure Avaya Aura® Web Gateway

To log into AAGW, open a web browser to **https://<AAWGIPorFQDN>:8445/admin** as shown below. Enter the appropriate credentials and click on **Sign in**.



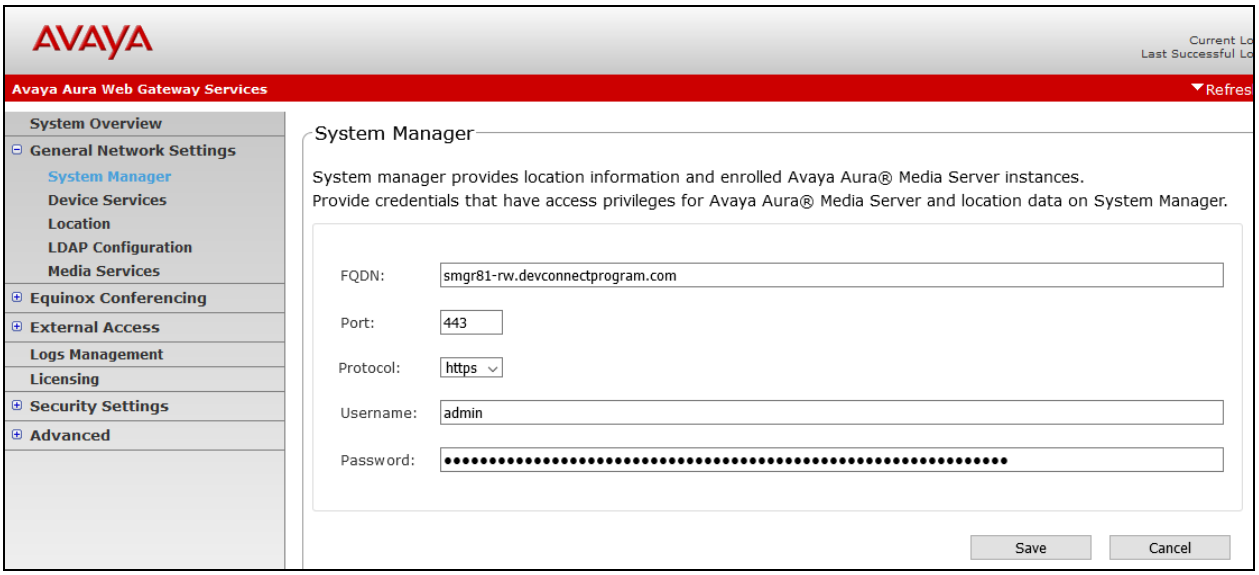
Once logged in, the following screen is shown where all the various **Solution Servers** show **Connected**.



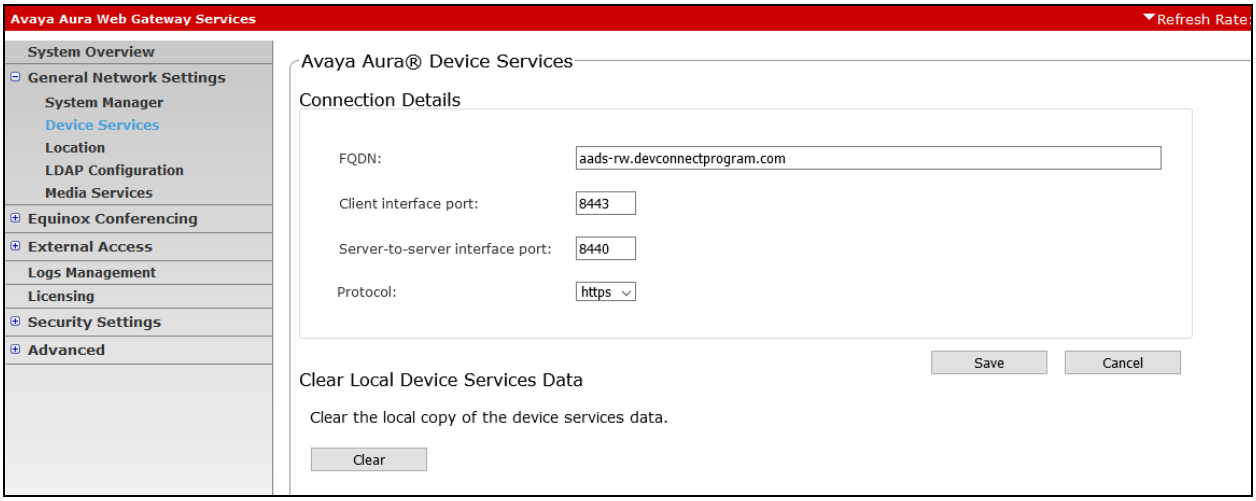
Note: The installation and configuration of AAWG is outside the scope of these Application Notes, please see **Section 15** for further information on AAWG. However, it is important to note the following is part of the overall setup for this solution.

8.1. General Network Settings

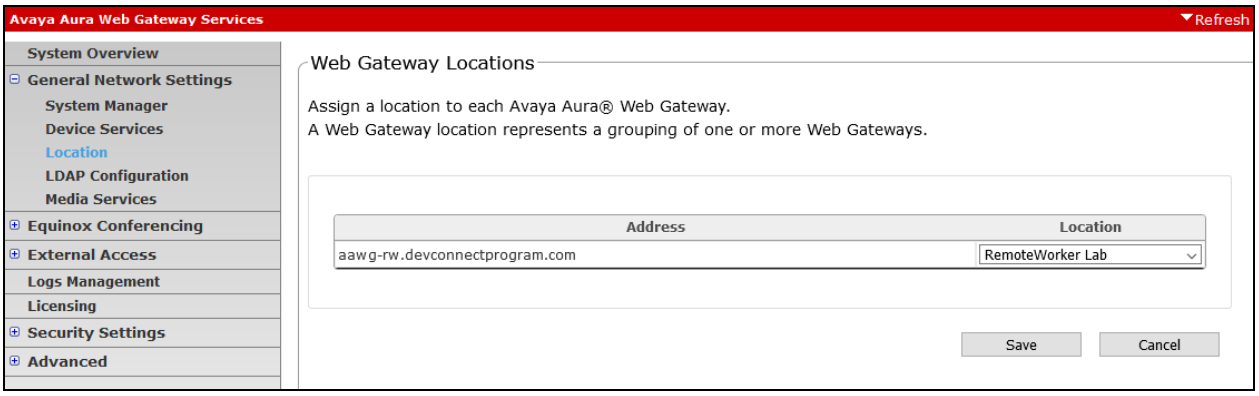
The connection to System Manager is configured under **General Network Settings → System Manager**. The connection information used for compliance testing is shown below.



The connection to **Device Services** is shown below.

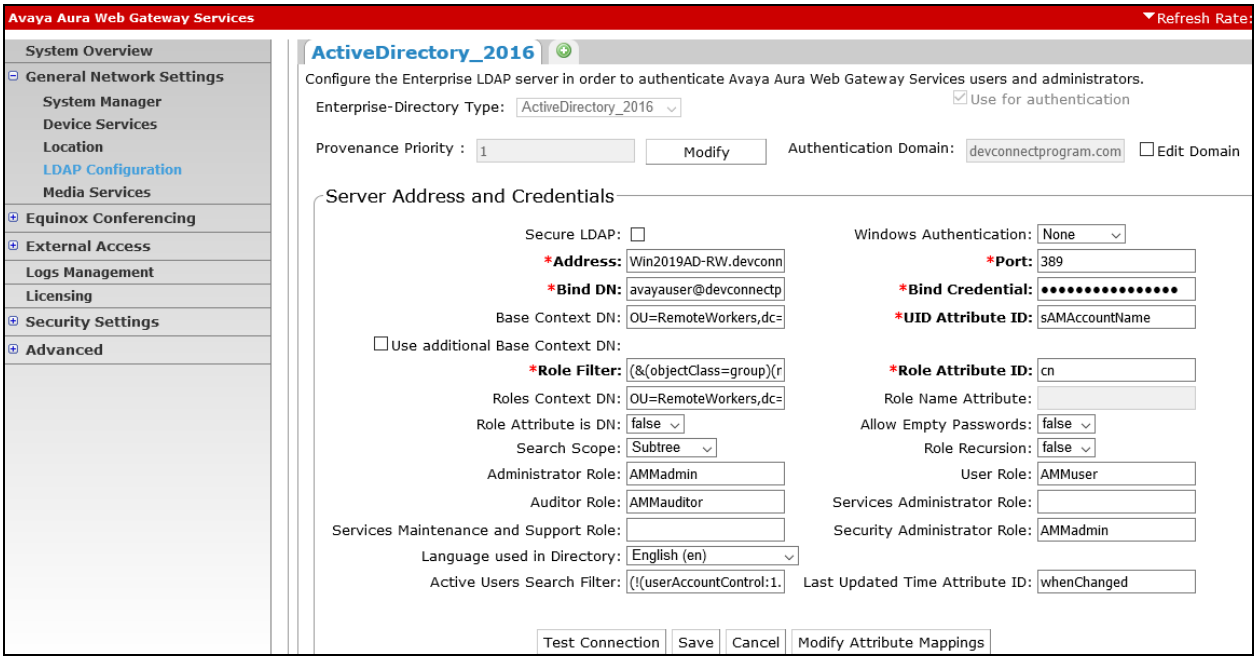


The **Location** setup is shown below.



The **LDAP Configuration** is shown below. This may look something similar to the mappings that were set in **Section 7.2** for the synchronization between the LDAP and System Manager. The following are important to note for this setup.

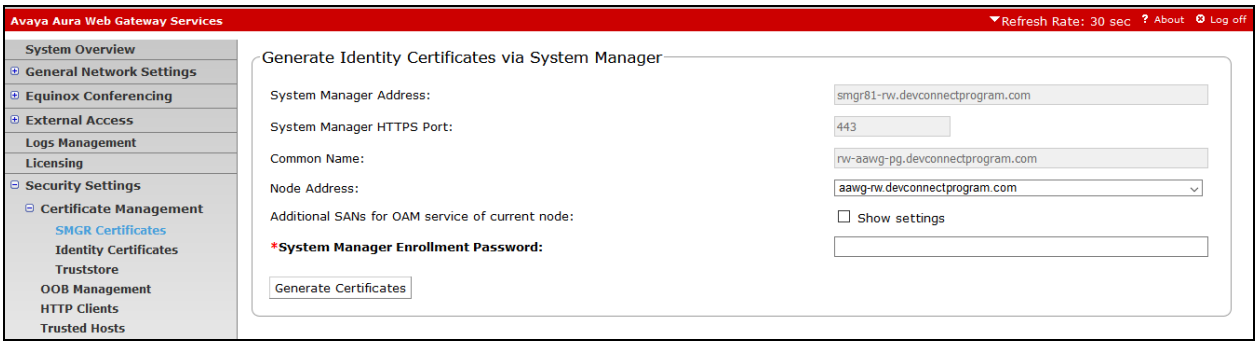
- **Address**: Win2019AD-RW.devconnectprogram.com
- **Port**: 389
- **Bind DN**: avayauser@devconnectprogram.com
- **Bind Credential**: Password for the 'avayauser'
- **UID Attribute ID**: sAMAccountName
- **Role Filter**: (&(objectClass=group)(member={1}))
- **Role Attribute ID**: cn
- **Roles Context DN**: OU=RemoteWorkers,dc=devconnectprogram,dc=com



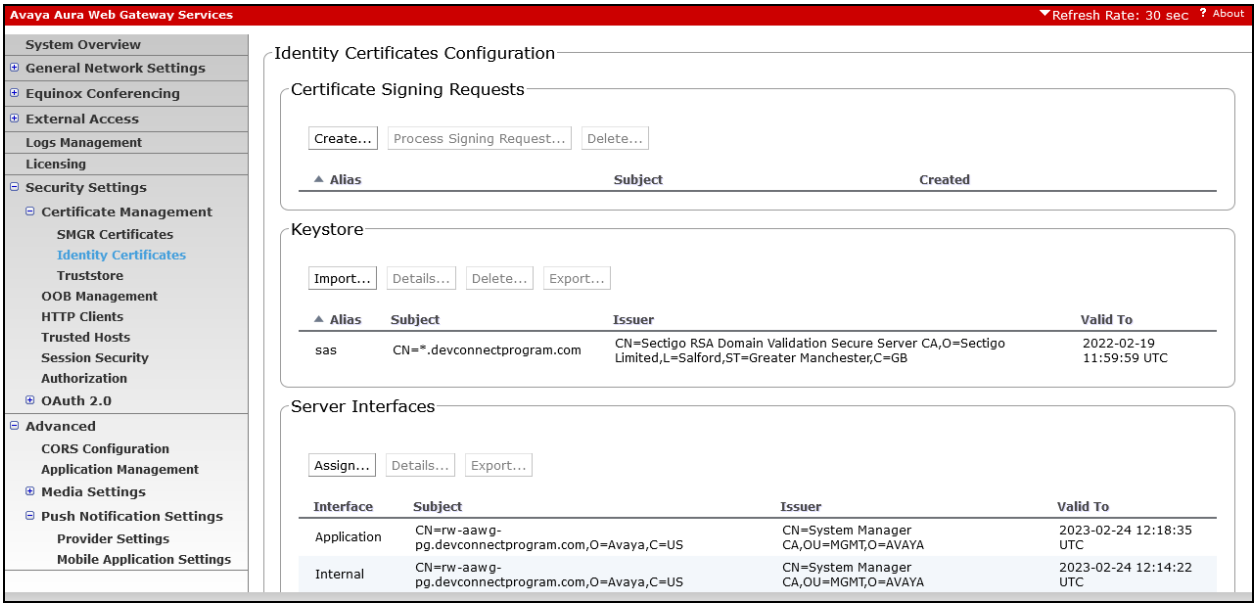
The final configuration under **General Network Settings** is that for **Media Services**. The Media Server associated with this platform is added here.

8.2. Security Settings

Like the network settings, the security settings are configured as part of the initial installation and configuration of AAWG; however, it is important to note the following security settings. The secure connections are configured under **Security Settings**. The connection to System Manager is over a secure link and so **Certificate Management** is required. Navigate to **Security Settings → Certificate Management → SMGR Certificates** in the left window. From the main window the System Managers details are added, and the **Enrollment Password** is entered to allow the AAWG register with System Manager.



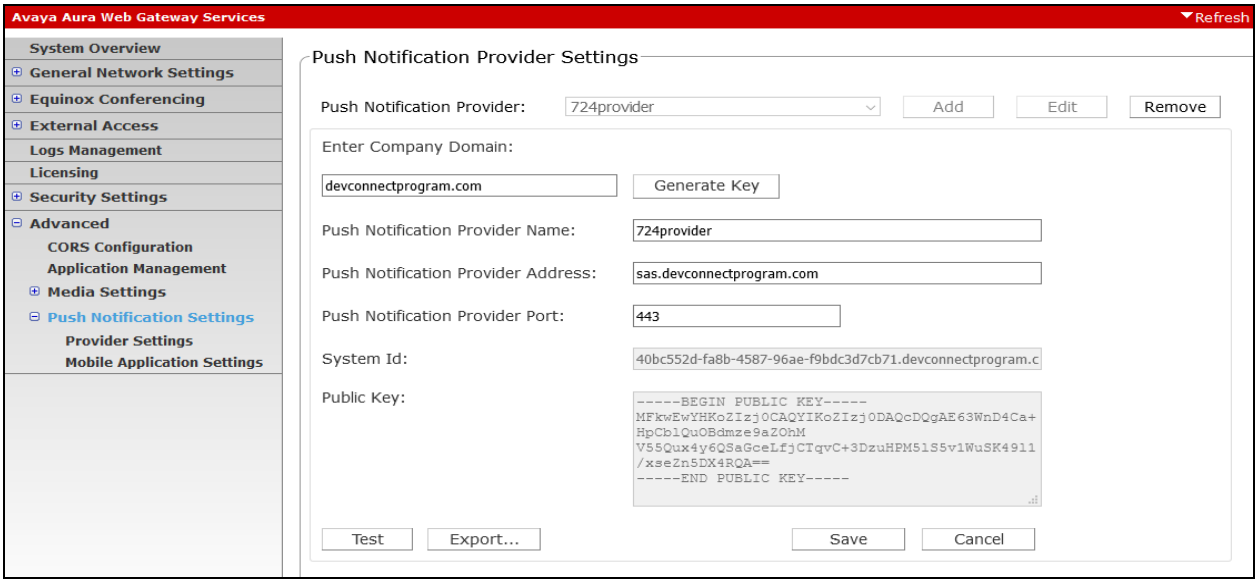
Click on **Identity Certificates** in the left window and the SAS certificate can be added into the **Keystore** to allow for secure communication between the AAWG and the Net Iletisim SAS.



8.3. Push Notification Settings

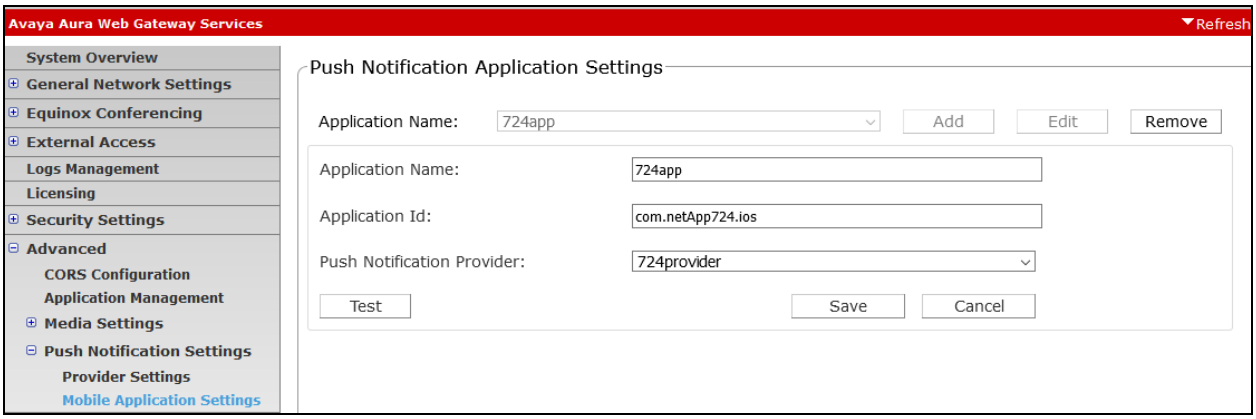
This section serves to illustrate the setup of the Push Notification Settings to allow notifications to get sent to the SCC handsets.

To configure the Push Notification Provider Settings, from the left window, navigate to **Advanced → Push Notification Settings → Provider Settings**. A new **Push Notification Provider** can be added by clicking on **Add**. The screenshot below shows the details that were entered for the **724provider** that was previously created. The domain referred to throughout this document is **devconnectprogram.com** and this is added under **Enter Company Domain**. The **Push Notification Provider Name** is given a suitable name and the **Push Notification Provider Address** should be the FQDN of the Net Iletisim SAS server. The **Push Notification Provider Port** is set to **443**. When **Generate Key** is pressed the remaining information is filled in automatically. This connection to the SAS server can be tested before saving.



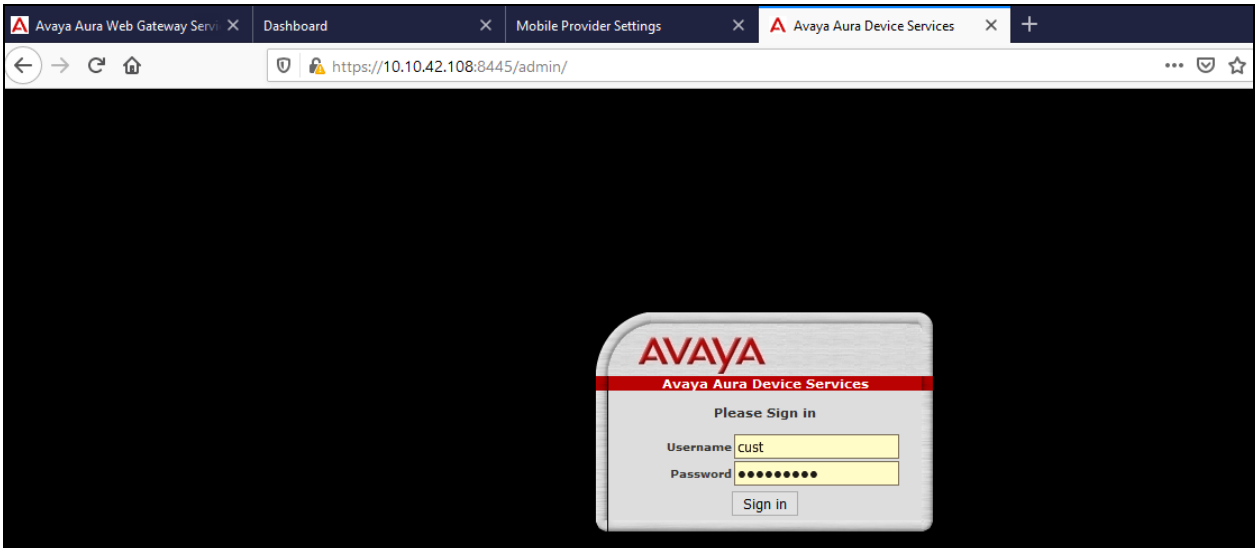
To configure the Push Notification Mobile Application Settings, from the left window, navigate to **Advanced → Push Notification Settings → Mobile Application Settings**. A new **Push Notification Application** can be added by clicking on **Add**. The screenshot below shows the details that were entered for the **724app** that was previously created. A suitable **Application Name** is added, and the **Push Notification Provider** created above is selected. The **Application Id** is **com.netApp724.ios**. This connection to the SCC handset can be tested before saving.

Note: com.netApp724.ios is an application identifier for the Apple developer, which is defined on XCode when creating the iOS project. The Avaya platform uses this as User-Agent ID.

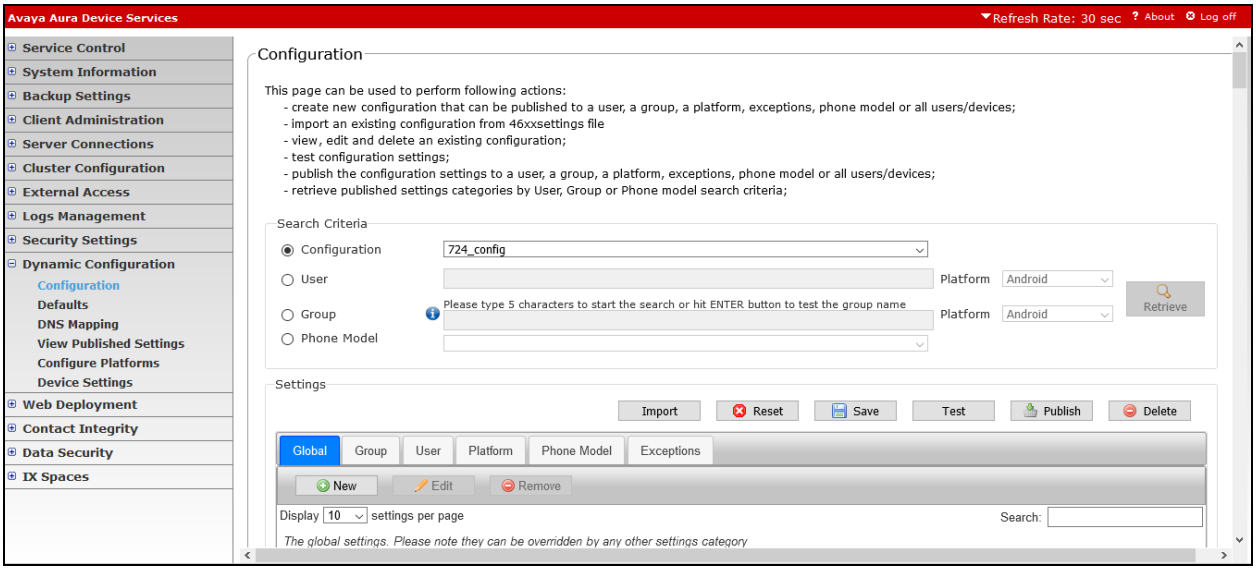


9. Configure Avaya Aura® Device Services

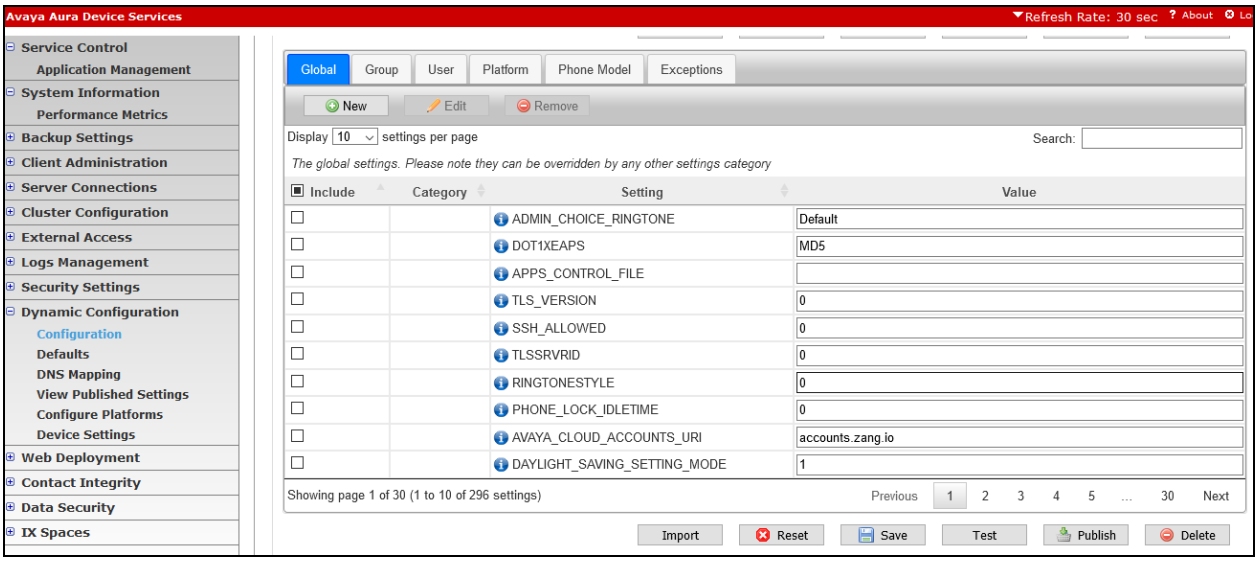
Log into AADS by opening a web browser to the IP Address of the AADS server in the format https://<serverIP>:8445/admin. Enter the appropriate credentials and click on **Sign In**.



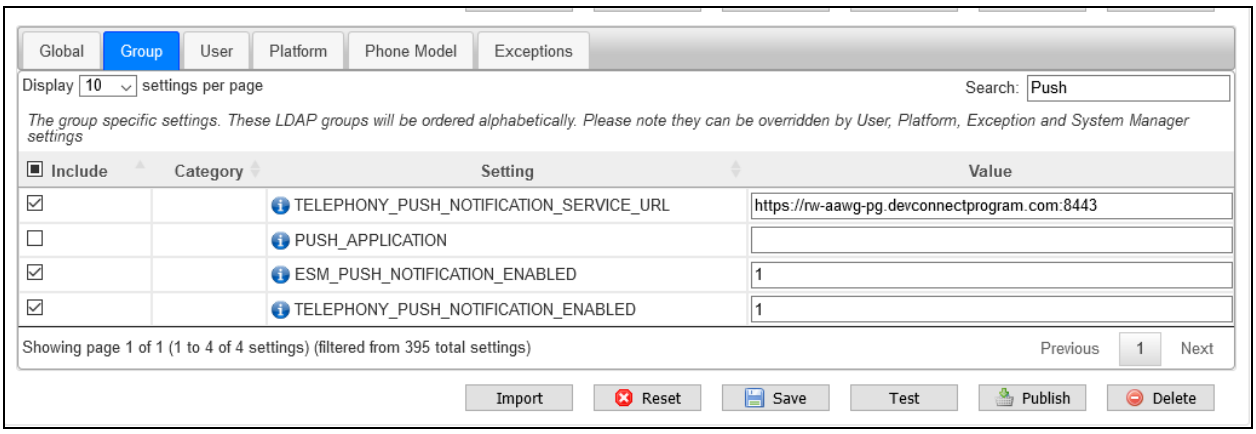
Navigate to **Dynamic Configuration → Configuration** in the left window. A configuration is already present for the SCC users called **724_config**.



The Global settings can be observed under the **Global** tab, as shown.

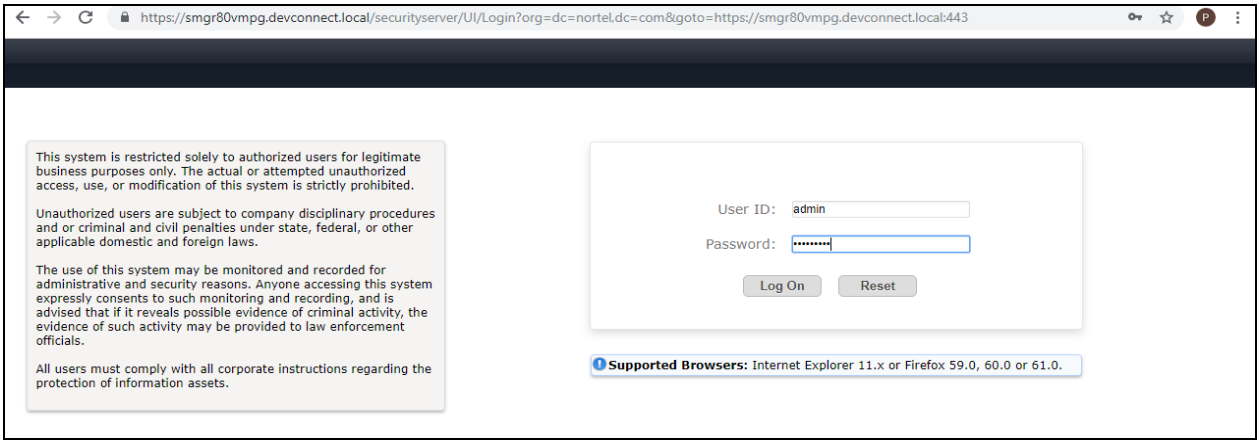


The Push Notification settings are added/viewed in the **Group** tab. The following were added to allow Device Services to use the AAGW to push notifications to the SCC handsets. Note the FQDN of the AAWG is added as the **Telephony_Push_Notification_Service_URL**.

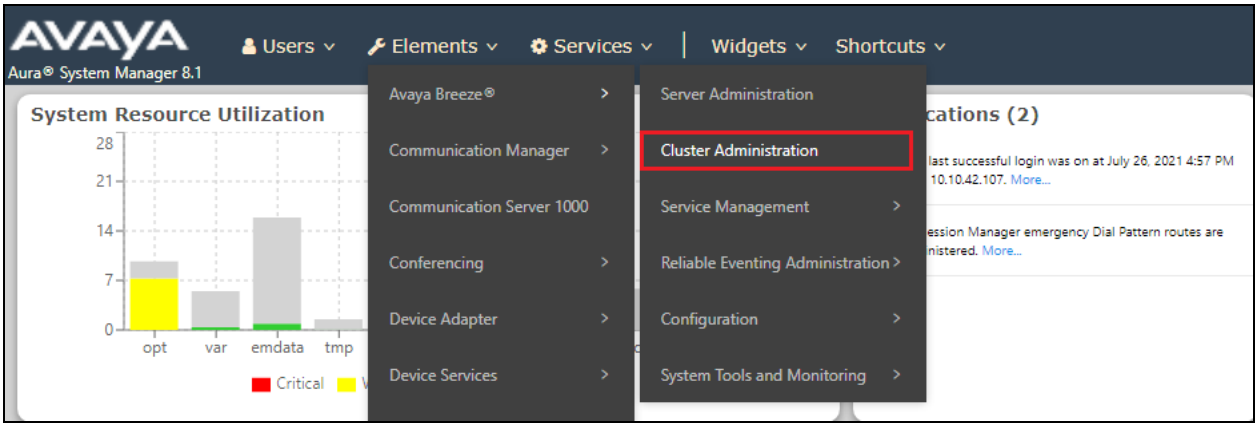


10. Configure Avaya Presence Services for Push Notifications

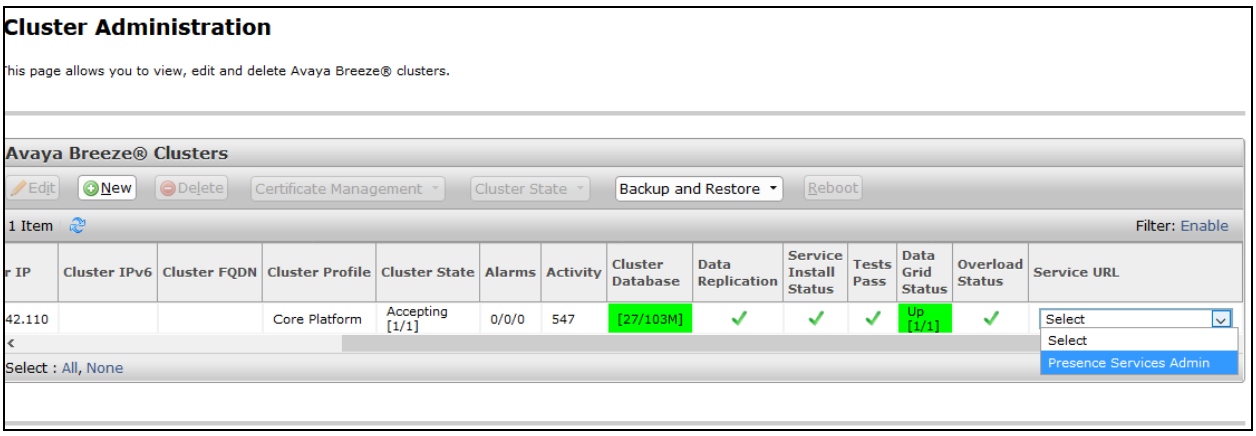
Presence Services runs on Avaya Breeze® and the access to Presence Services is from the Breeze Cluster running on System Manager. Log into System Manager by opening a web browser and navigating to https://<System Manager FQDN>/SMGR. Enter the appropriate credentials for the **User ID** and **Password** and click on **Log On**.



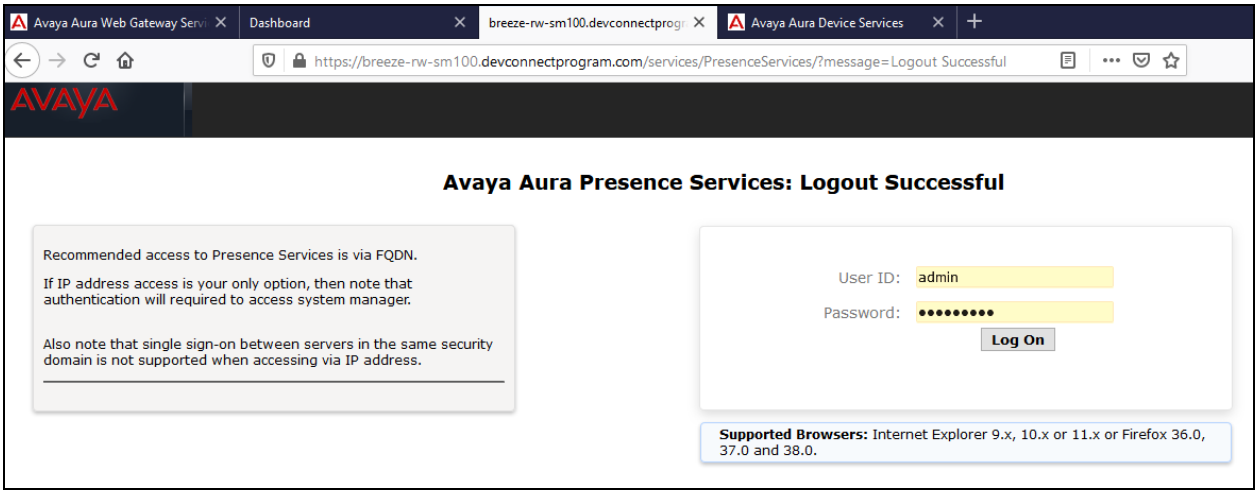
From the top menu, navigate to **Avaya Breeze®** via **Elements** and open **Cluster Administration**.



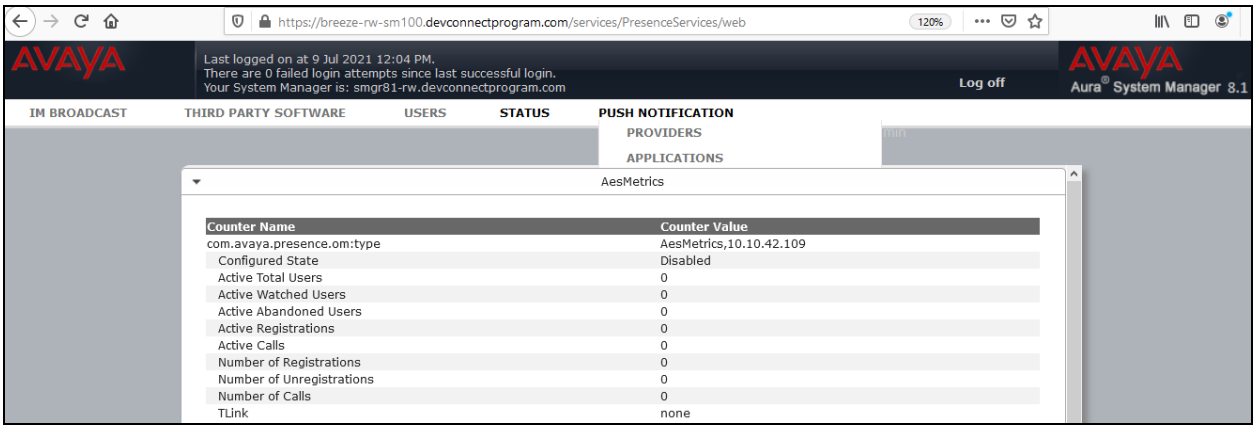
Scroll across to the right of the page and select **Presence Services Admin** from the **Service URL** drop-down menu.



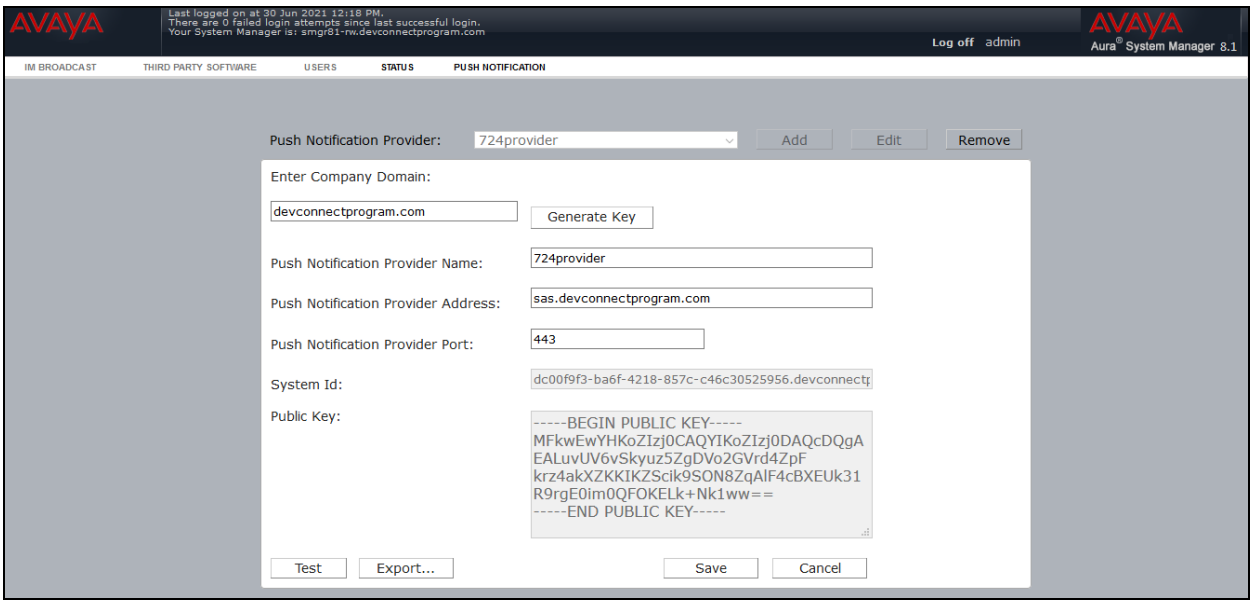
A new web page should be opened to the Breeze cluster, but specifically for **Presence Services** as shown below. Enter the appropriate credentials and click on **Log On**.



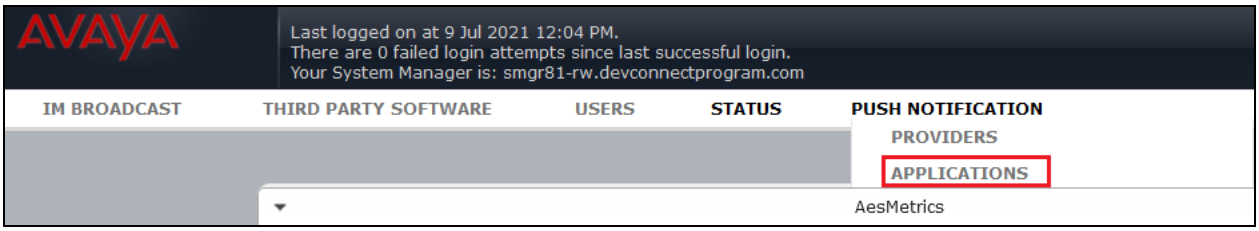
Once logged in, navigate to **Push Notification** from the menu at the top and select **Providers**.



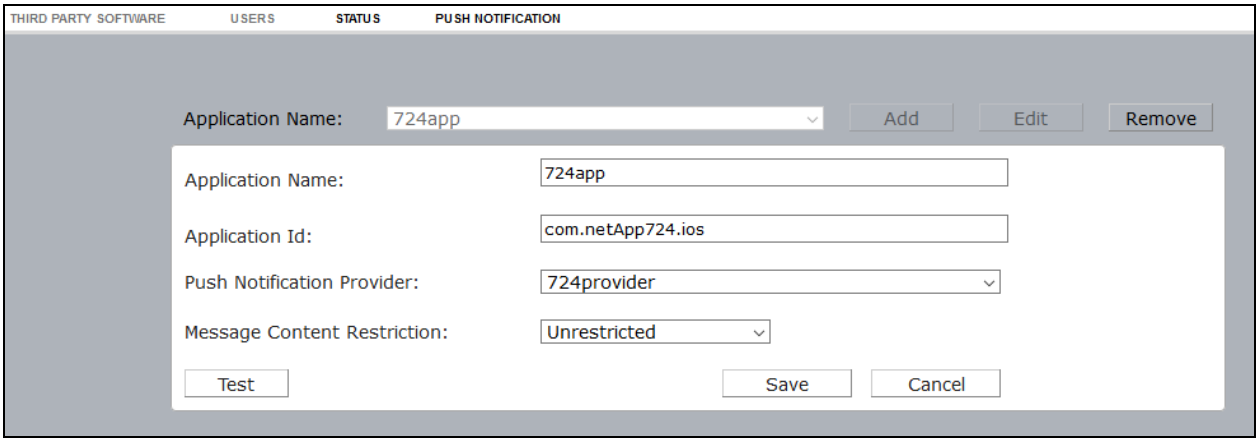
A new Provider can be added by clicking **Add**. The details here are very similar to that on the AAWG with the domain set to **devconnectprogram.com** and the Name, Address and Port set the same as done in **Section 8.3.** Click on **Generate Key** and export to the SAS server, if required. The connection can be tested before it is saved.



By selecting **Applications** from the **Push Notification** menu, a new Application can be added.



Similar to AAWG, a **Push Notification Application** is also created with the same information as the AAWG Push Notification Application in **Section 8.3**.



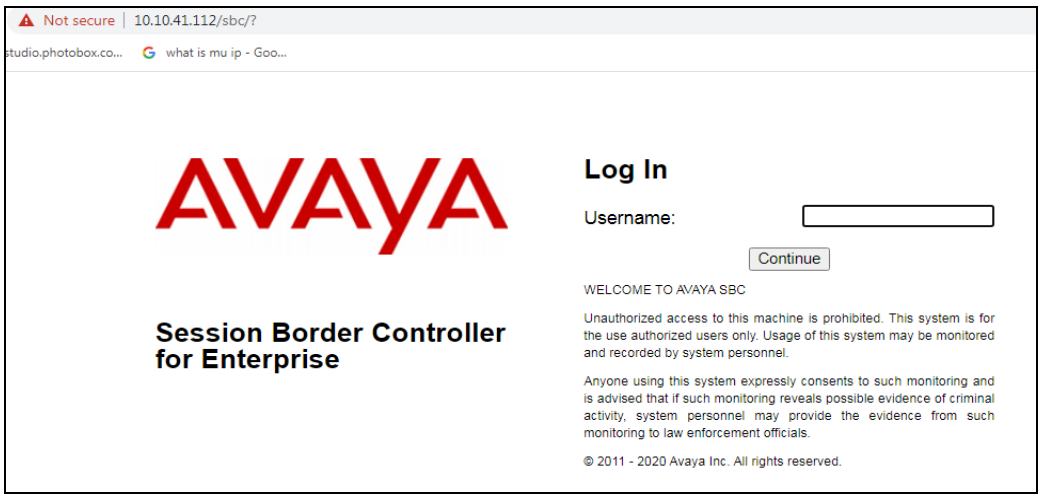
11. Configure Avaya Session Border Controller for Enterprise

This section describes the required configuration of Avaya SBCE for the support of Remote Workers, specifically for the 724 SCC. The configuration steps on Avaya SBCE include the following:

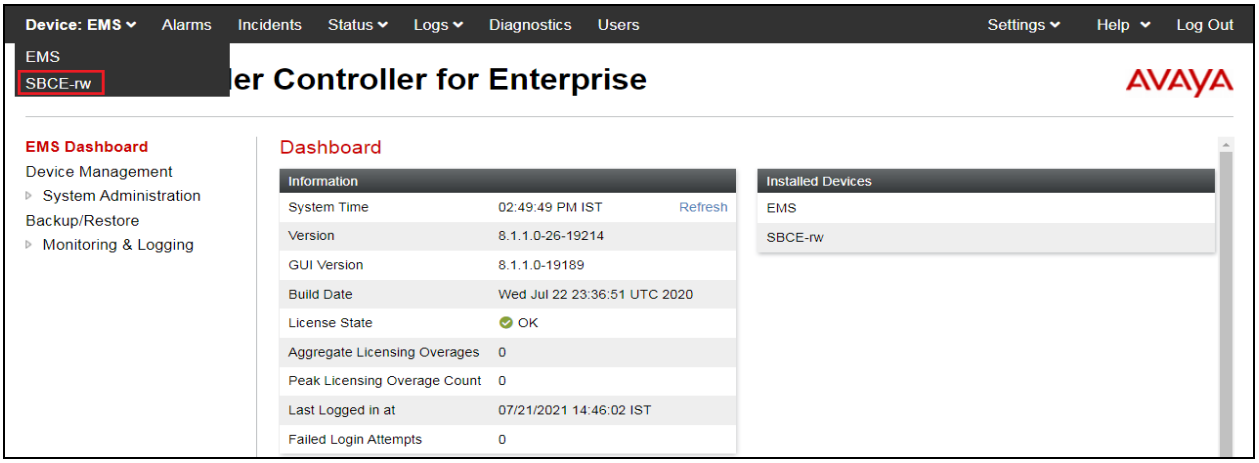
- Networking Interface
- User Agents
- Server Interworking Profile
- SIP Server Profile
- Routing Profile
- Application Rules
- Media Rules
- Signaling Rules
- Security Rules
- Endpoint Policy Group
- Media and Signaling Interfaces
- End Point Flows
- PPM Services
- Relays Services

Note: The Avaya SBCE referenced in the screen shots in this section has previously been provisioned to support the Remote Worker functionality. The configuration is therefore complete, and the screen shots will therefore show no new additions only edited, existing configuration to show how to set up the SBCE for Remote Worker to function as this previously provisioned SBCE.

Log into the SBCE by opening a URL to the management IP address followed by /sbc as shown.



Once logged in, the following screen is presented, and the device must be set to the SBCE before any further configuration can take place.

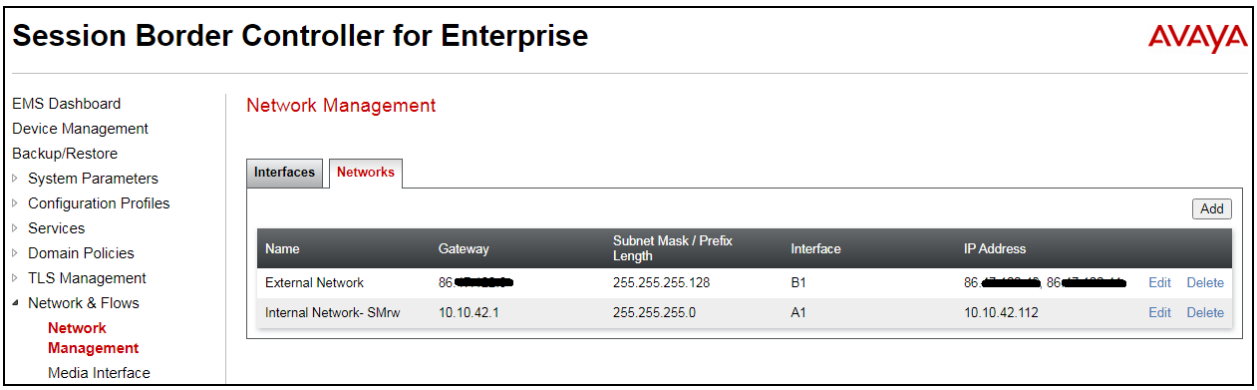


Network Management is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is this information that populates the various Network Management tab displays, which can be edited as needed to optimize device performance and network efficiency.

11.1. Networking Interface

Navigate to **Networks & Flows → Network Management**. On the **Networks** tab, select **Add** to add a new interface entry, or **Edit** to add or change IP addresses on an existing interface.

The following screen shows the enterprise interface assigned to **A1** and the interface towards the Remote Workers assigned to **B1**.

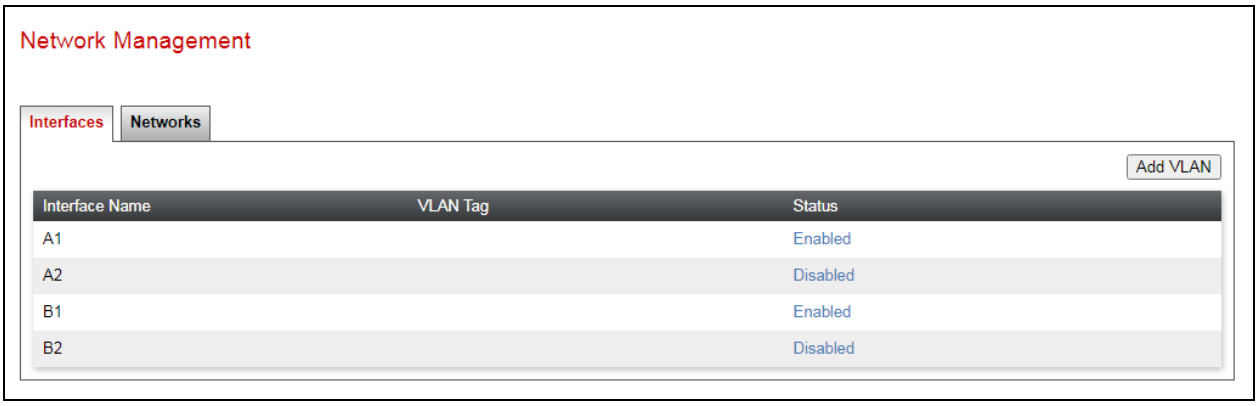


The following are the IP addresses and associated interfaces used in the reference configuration:

- **86.x.x.x**: IP Address of Public Interface B1 (Remote Workers SIP and File Transfer)
- **10.10.42.112**: IP Address of Private Interface A1 (Remote Workers, all traffic)

Note: Some of the External IP addresses are blanked out or in the format x.x.x.x, this is normal procedure for public IP addresses illustrated in DevConnect Application Notes.

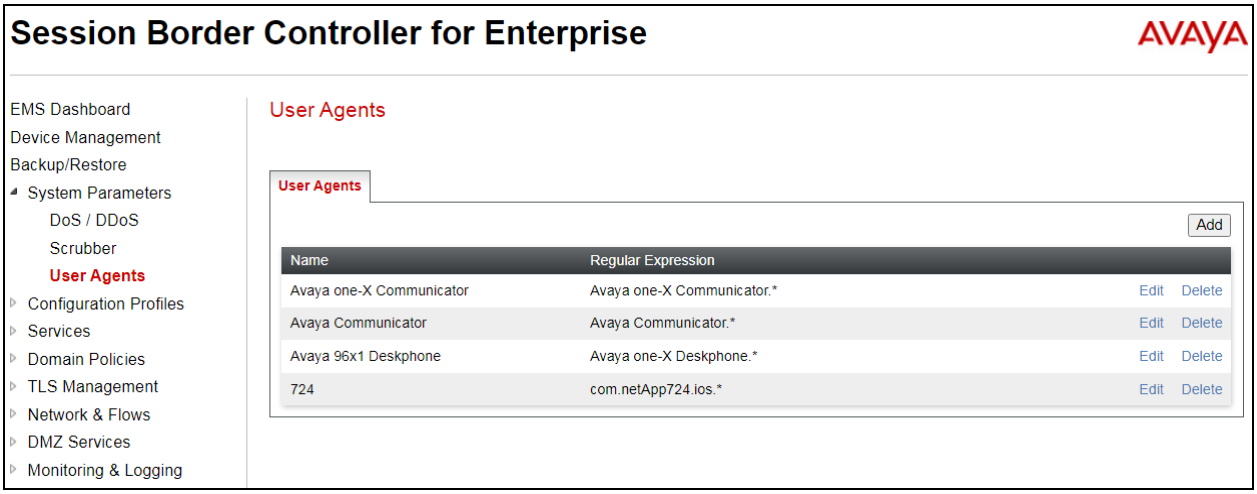
Verify that the interfaces are enabled on the **Interfaces** tab. The following screen shows interfaces **A1** and **B1** with status **Enabled**. To enable an interface, click the corresponding **Disabled** link under the **Status** column to change it to **Enabled**.



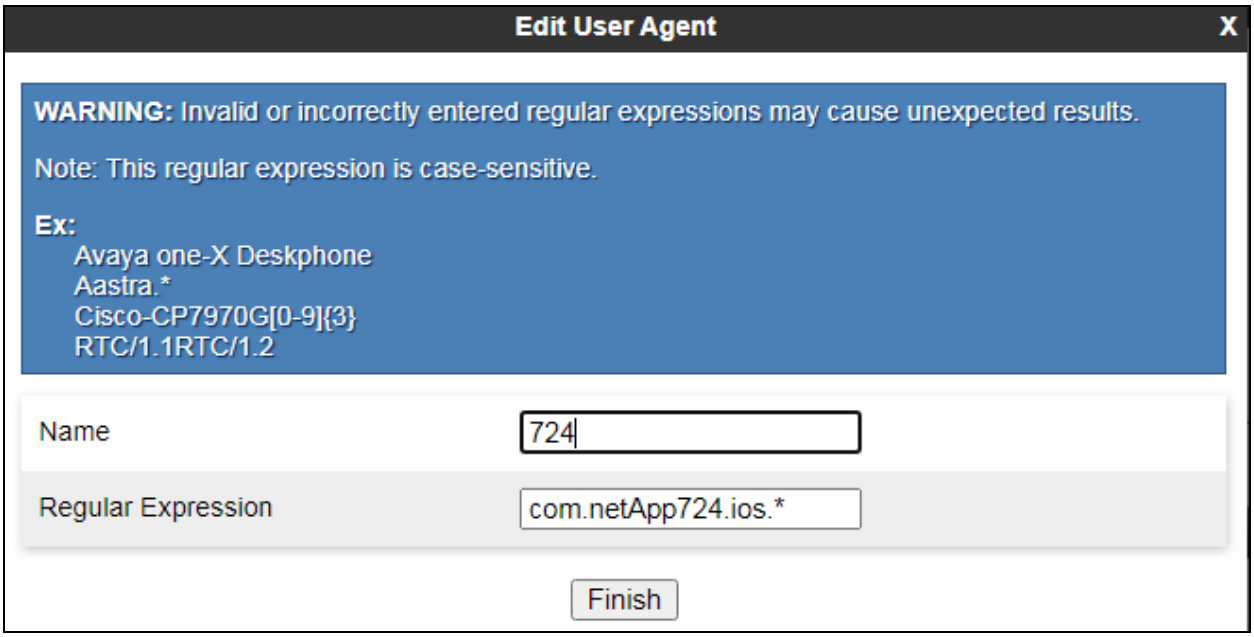
11.2. User Agents

User Agents can be created for each type of remote endpoint connecting to the Avaya SBCE. This would allow for different policies to be applied based on the type of device being used, if necessary. The following screen shows the values used in the reference configuration. The **Regular Expression** field is used to match the information contained in the User-Agent header arriving from the endpoint. Some examples are:

- Avaya one-X Communicator.*
- Avaya Communicator.* (User-Agent header used by Avaya Workplace Client for Windows)
- Avaya one-X Deskphone.*



The following **User Agent** was added specifically for the SCC handsets.



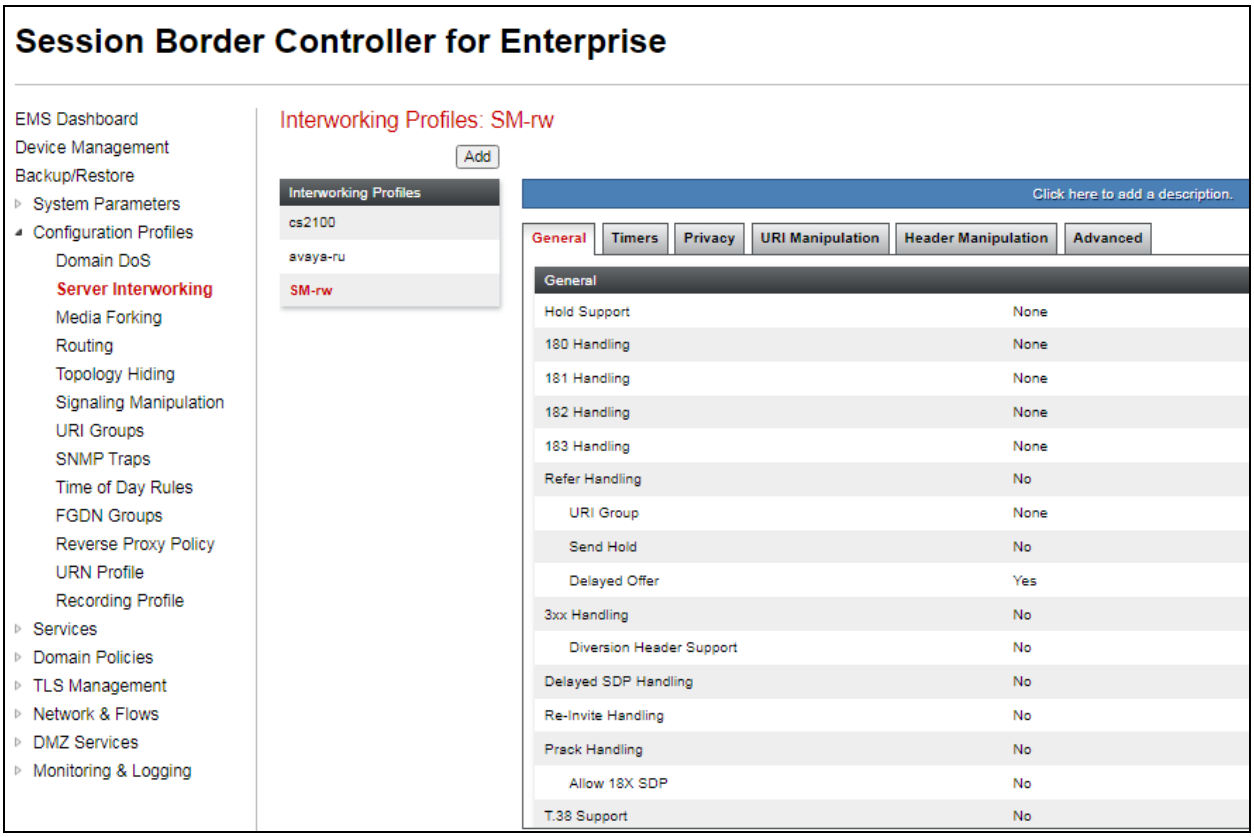
11.3. Server Interworking Profile

The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, cloned and modified, or new profiles can be added as needed.

A Server Interworking profile for Session Manager may have already been created, as part of the Avaya SBCE provisioning for SIP Trunking. If there is no existing Server Interworking Profile for Session Manager, the default **avaya-ru** profile can be cloned to create a new profile.

Navigate to **Configuration Profiles → Server Interworking**. Select the avaya_ru profile and click the Clone button (not shown). Enter a profile name (e.g., **SM-rw**), and click **Finish** (not shown).

Default values were used for all fields. The profile will later be added to the SIP Server Configuration for Session Manager in **Section 11.4**.

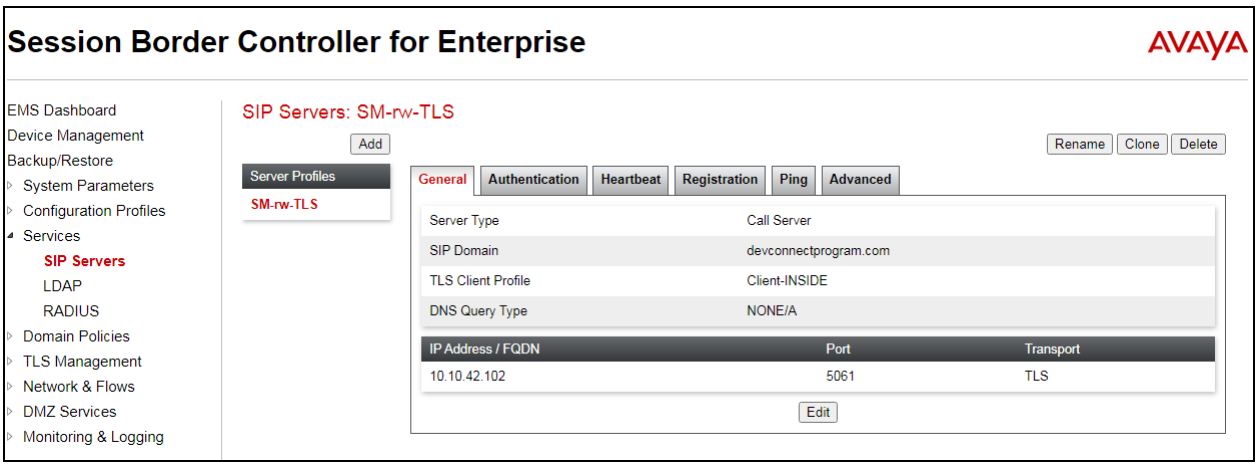


11.4. SIP Server Profile

The SIP server profile contains parameters to configure and manage various SIP call server-specific parameters such as port assignments, heartbeat signaling parameters, DoS security statistics, and trusted domains.

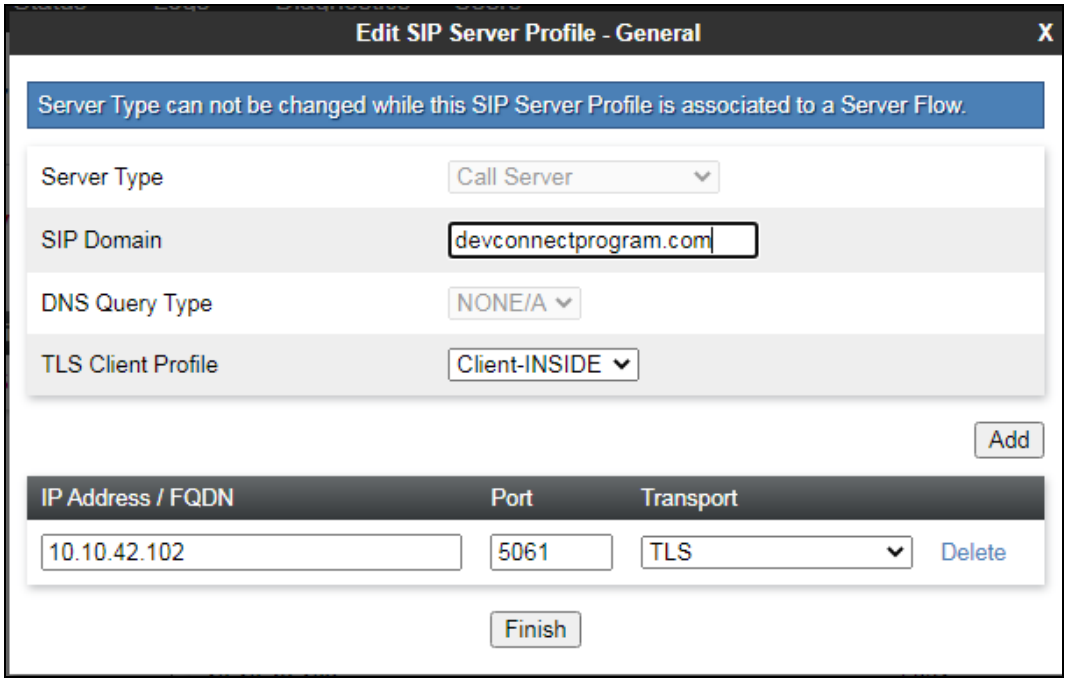
As outlined at the beginning of the section, this will have been created as part of the Avaya SBCE provisioning for Remote Workers, and so the existing profile will be examined to show what settings are required should a new profile be created. If there is no existing SIP Server profile for Session Manager, follow the steps below to create a new profile.

Select **Services → SIP Servers** from the left-hand menu. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **SM-rw-TLS**) and click **Next** (not shown).



The **Add Server Configuration Profile** window will open.

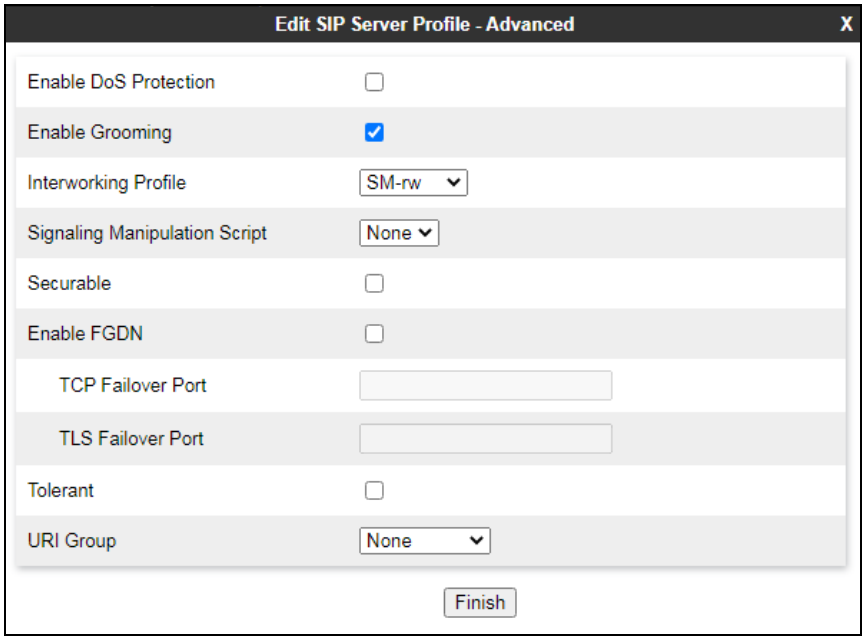
- Select **Server Type**: **Call Server**.
- **SIP Domain**: Leave blank (default).
- **DNS Query Type**: Select **NONE/A** (default).
- **TLS Client Profile**: Select the profile created in **Section 17.5** (e.g., **Client-INSIDE**).
- **IP Address**: **10.10.42.102** (Session Manager Security Module IP address).
- Select **Port**: **5061**, **Transport**: **TLS**.
- If adding the profile, click **Next** (not shown) to proceed. If editing an existing profile, click **Finish** and proceed to the next tab.



Default values can be used on the **Authentication** tab and default values are used on the **Registration** and **Ping** tabs.

On the **Advanced** tab:

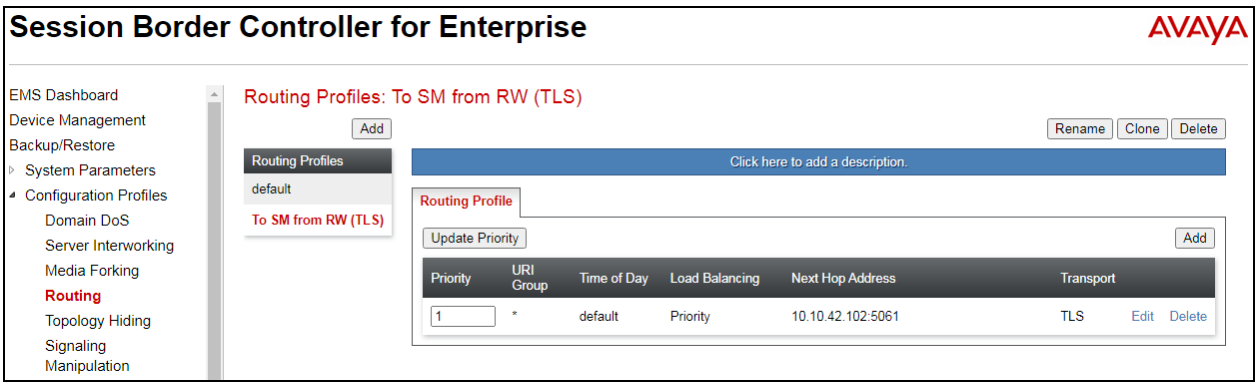
- Select the **SM-rw** (created in **Section 11.3**), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.



11.5. Routing Profile

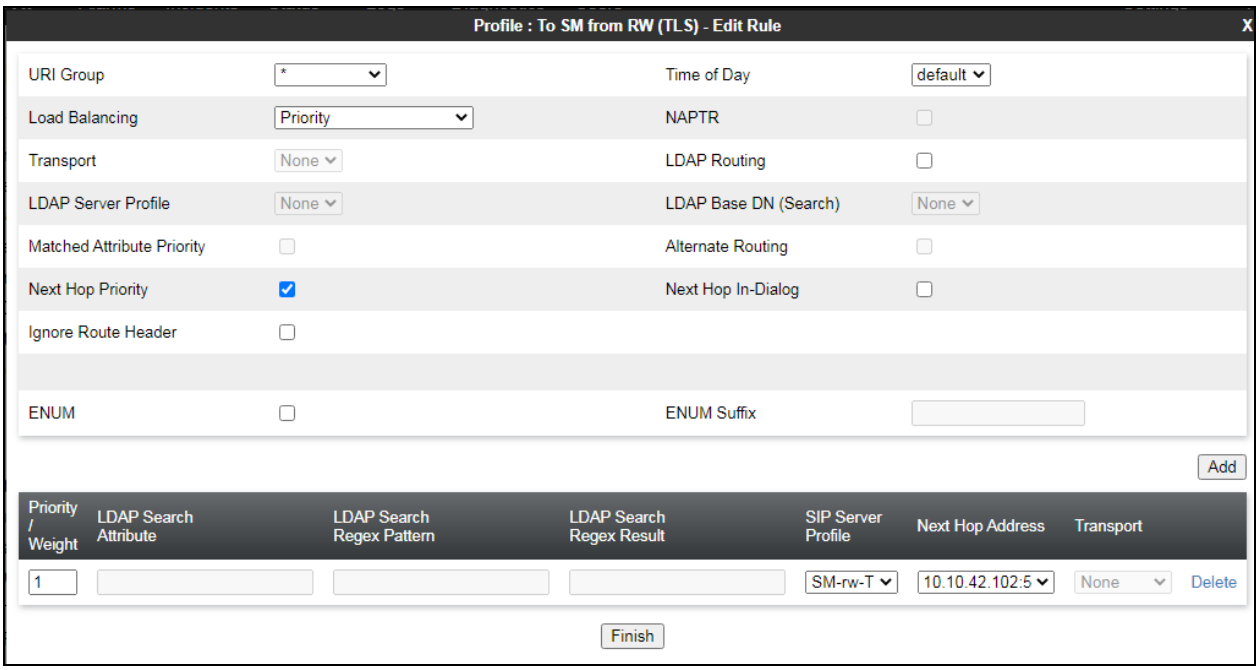
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

The existing Routing Profile is shown below; however, to create a Routing Profile to Session Manager, if one doesn't exist already, navigate to **Configuration Profiles → Routing** and select **Add**. Enter a **Profile Name** and click **Next** to continue.



The Routing Profile window will open. The parameters in the top portion of the profile are left at their default settings. Click the **Add** button. The **Next-Hop Address** section will open at the bottom of the profile. Populate the following fields:

- **Priority/Weight**: **1**.
- **SIP Server Profile: SM-rw-TLS** (from **Section 11.4**).
- **Next Hop Address:** Verify that the **10.10.42.102:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
- Click **Finish**.

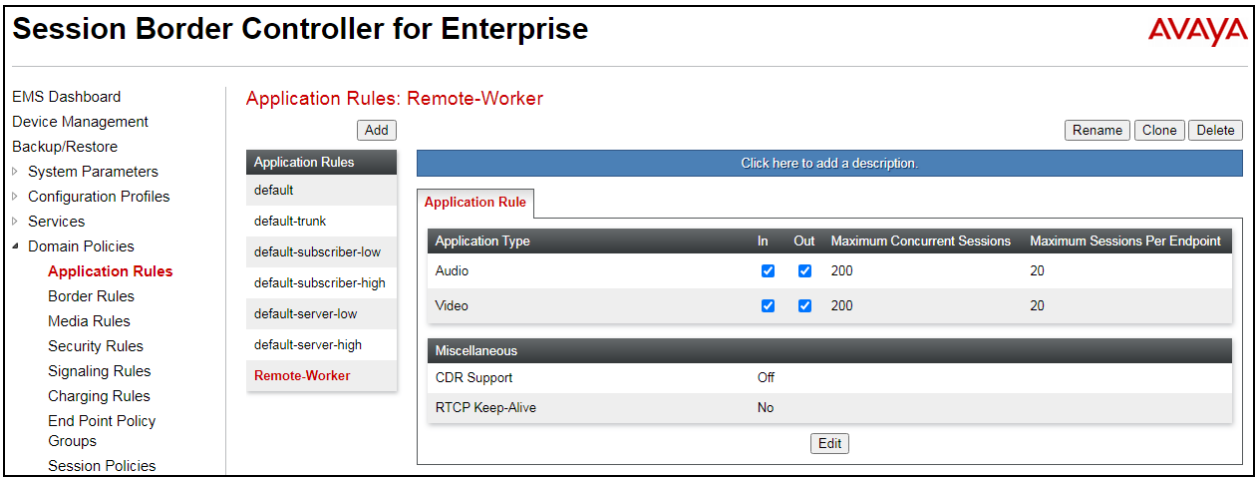


11.6. Application Rule

Application Rules define which type of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect, voice, video, and/or Instant Messaging (IM). In addition, the maximum number of concurrent voice and video sessions the network will process can be determined in order to prevent resource exhaustion.

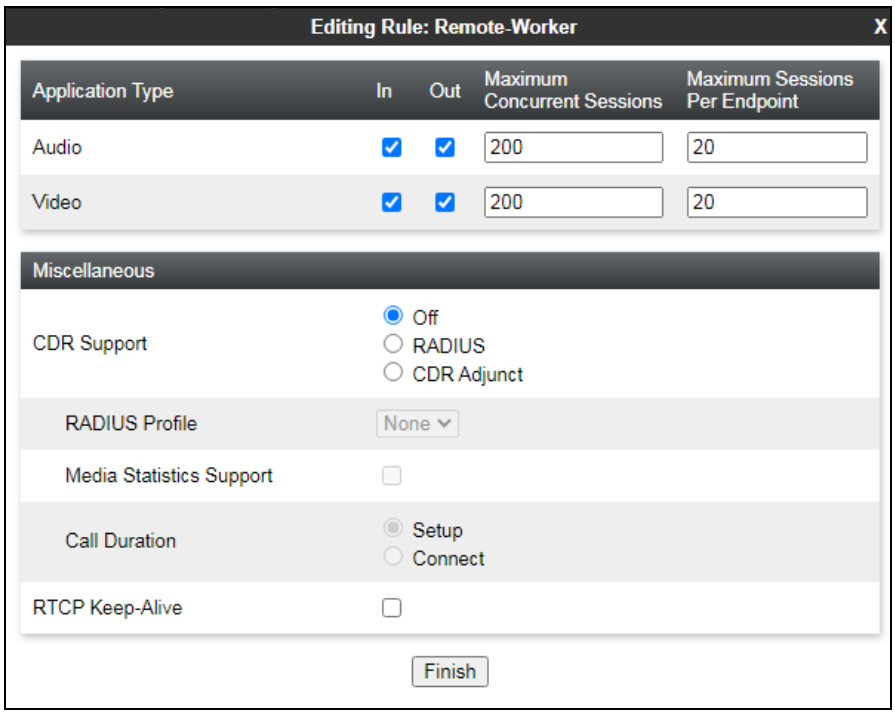
Note: The **Maximum Concurrent Sessions** and the **Maximum Sessions Per Endpoint** for Audio and Video should be set per the customer licenses purchased for the specific enterprise site. The values shown below are just an example; they represent the values used in the reference configuration.

From the navigation menu on the left-hand side, select **Domain Policies → Application Rules**. The **default** rule in the **Application Rules** list can be cloned to create a new rule, this was done for the **Remote-Worker** rule below. Click the **Clone** button and enter the name of the profile e.g., **Remote-Worker** and click **Finish** (not shown).



The newly created Application Rule can then be edited by clicking **Edit** (not shown).

- For **Audio**, set the **Maximum Concurrent Sessions** to **200** and **Maximum Sessions Per Endpoint** to **20**.
- If **Video** is required, check the **In** and **Out** boxes, set the **Maximum Concurrent Sessions to 200** and **Maximum Sessions Per Endpoint** to **20**.
- Click **Finish**.



11.7. Media Rules

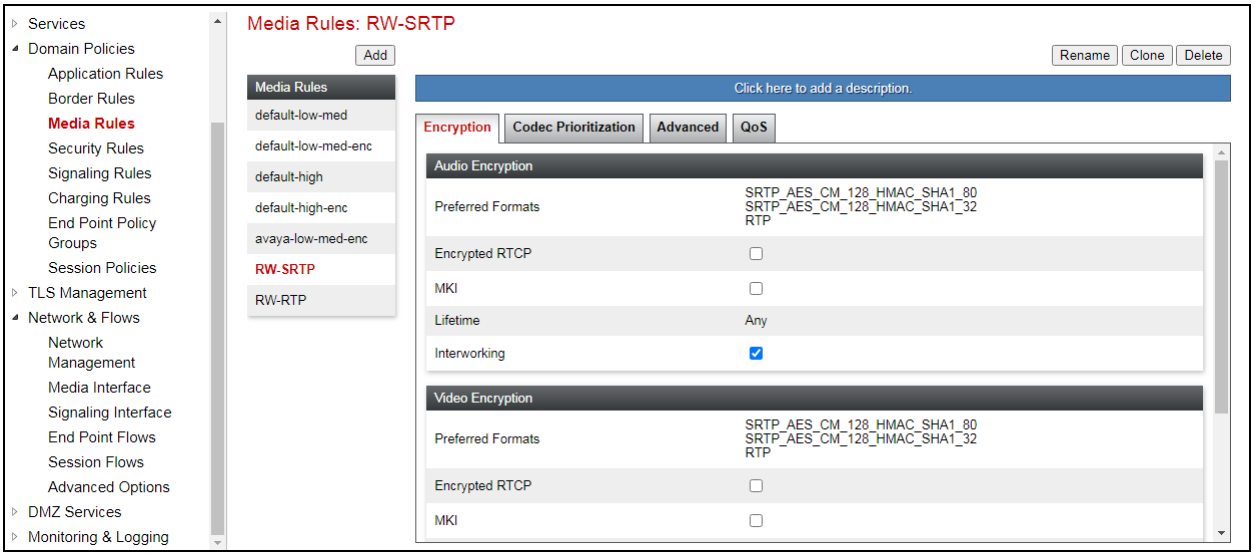
Media Rules define RTP media packet parameters such as prioritizing and packet encryption techniques. These rules will be applied to the End Point Policy Groups and ultimately to the Subscriber and Server Flows, defined later in this document.

In the sample configuration two media rules are defined by cloning the default rule called **avaya-low-med-enc**, and editing the cloned rules as follows:

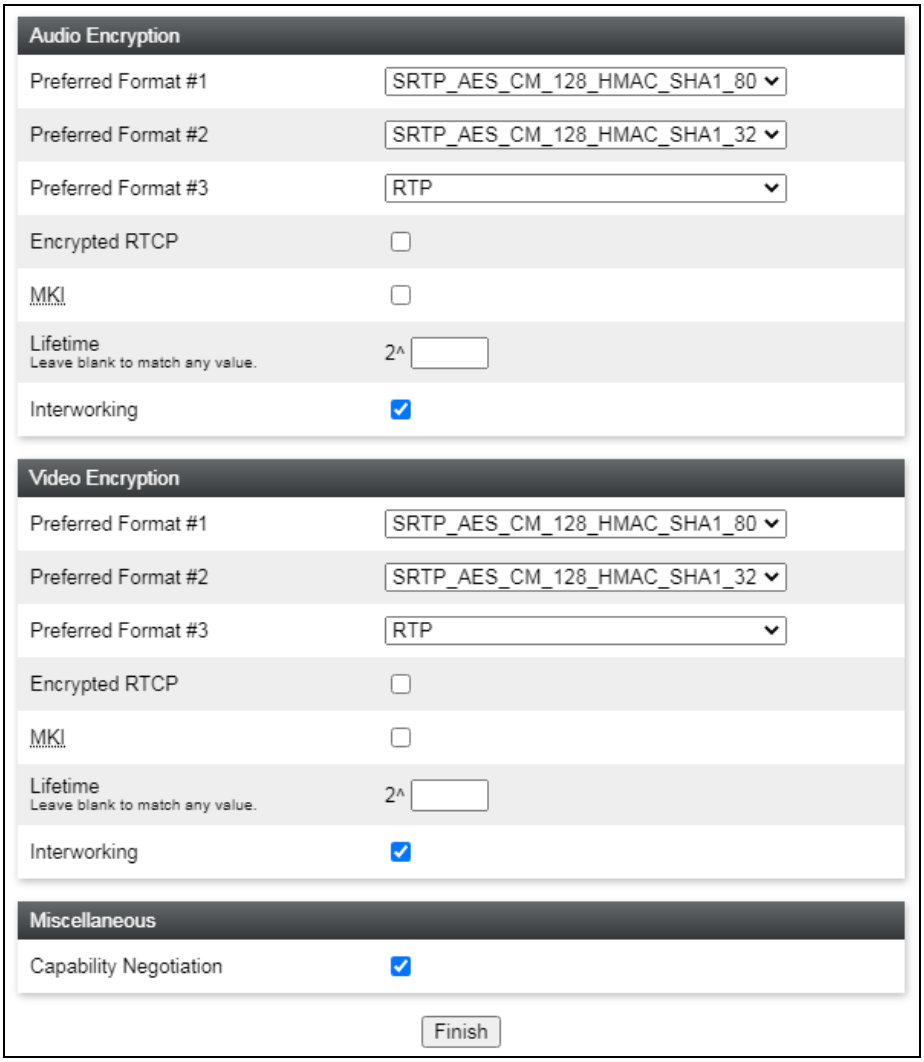
- A more restrictive media rule, selecting SRTP media as the preferred media.
- A less restrictive media rule that allows RTP only.

To add a Media Rule towards the Remote Workers, select **Media Rules** under the **Domain Policies** menu on the left-hand navigation pane. Select the **avaya-low-med-enc** rule from the list and click the **Clone** button. Under **Cloned Name**, enter the name of the profile e.g., **RW-SRTP** and click **Finish** (not shown).

The screen below shows the values on the **RW-SRTP** used in the reference configuration. On the **Encryption** tab, **RTP_AES_CM_128_HMAC_SHA1_80** is selected as the **Preferred Format** for **Audio** and **Video Encryption**. Verify **Interworking** is checked, and **Capability Negotiation** is unchecked. To alter any of these values click on **Edit** (not shown).



Clicking **Edit** from the previous page will bring up the following window, where the **Preferred Format** can be changed. The example below will cater for both **SRTP SHA1_80**, **SHA1_32** and **RTP**. Both **Internetworking** and **Capability Negotiation** are ticked.

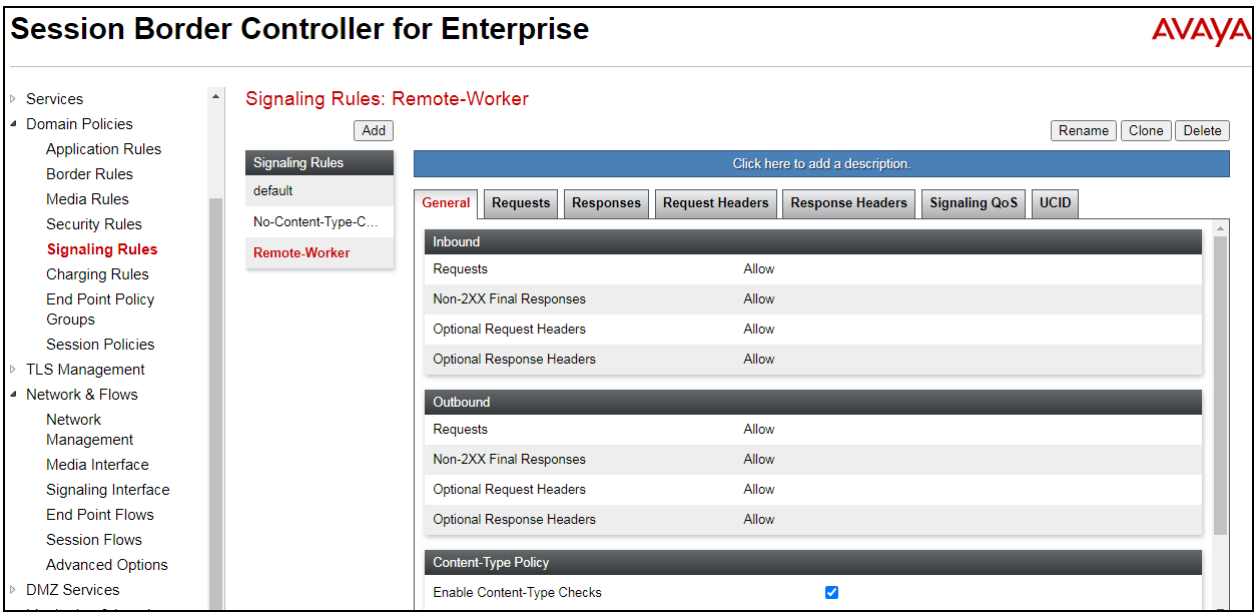


11.8. Signaling Rule

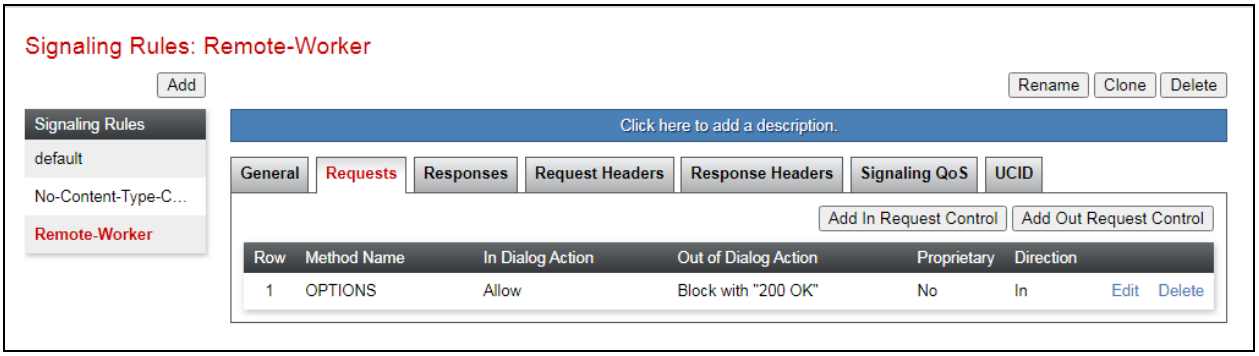
Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. They also allow the control of the Quality of Service of the signaling packets.

To create a signaling rule, navigate to **Domain Policies → Signaling Rules**. In the sample configuration, a signaling rule was created by cloning the default rule called **default**. Select the default rule and click the **Clone** button and enter a suitable name, e.g., **Remote-Worker** and click **Finish** (not shown).

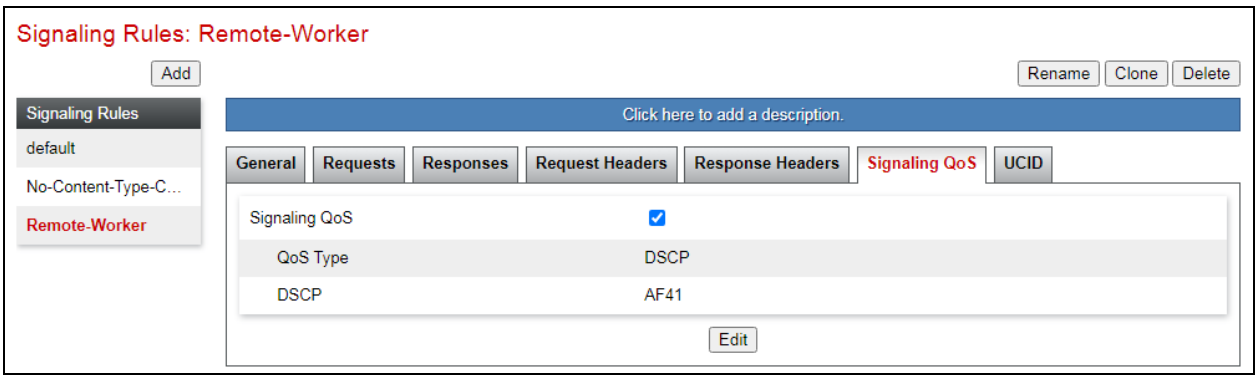
The screen below shows the values on the **Remote-Worker** used for compliance testing. Default values were used for all parameters in this rule.



The following was set under the **Requests** tab to allow **OPTIONS** to get responded to with a **200 OK**. This will simply let Session Manager know that when it sends Options that the SBCE will respond with a 200 OK allowing the link to get established.



The following was set under the **Signaling QoS** tab. This is simply to give priority to voice and video by setting **DSCP** to **AF41**.



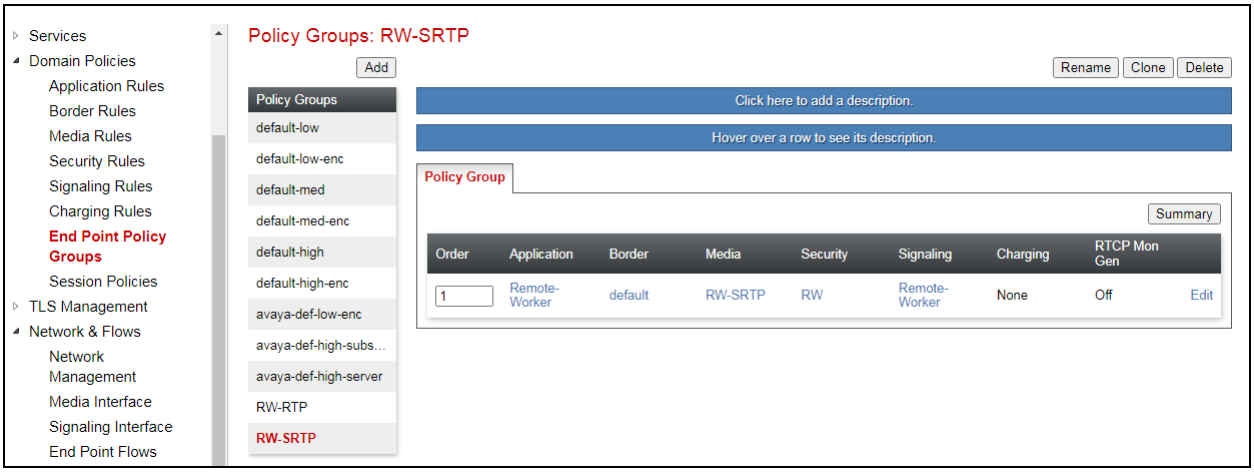
11.9. End Point Policy Group

End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. The Endpoint Policy Group is then applied in following Sections to a Subscriber Flow or a Server Flow. Create separate Endpoint Policy Groups for the remote endpoints and for the enterprise.

To create a new policy group towards the Remote Workers, navigate to **Domain Policies → Endpoint Policy Groups** and select the **Add** button.

The screen below shows the **RW-SRTP** group defined in the reference configuration, using the following rules:

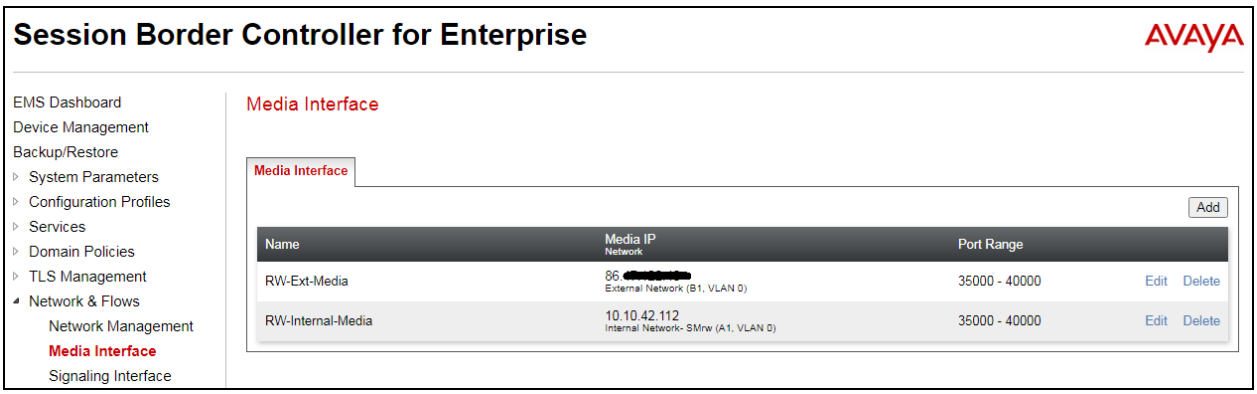
- **Application**: **Remote-Worker** created in **Section 11.6**.
- **Media: RW-SRTP** created in **Section 11.7**.
- **Security: RW** this was simply cloned from the default and was not shown.
- **Signaling: Remote-Worker** created in **Section 11.8**.
- Other rules used default values.



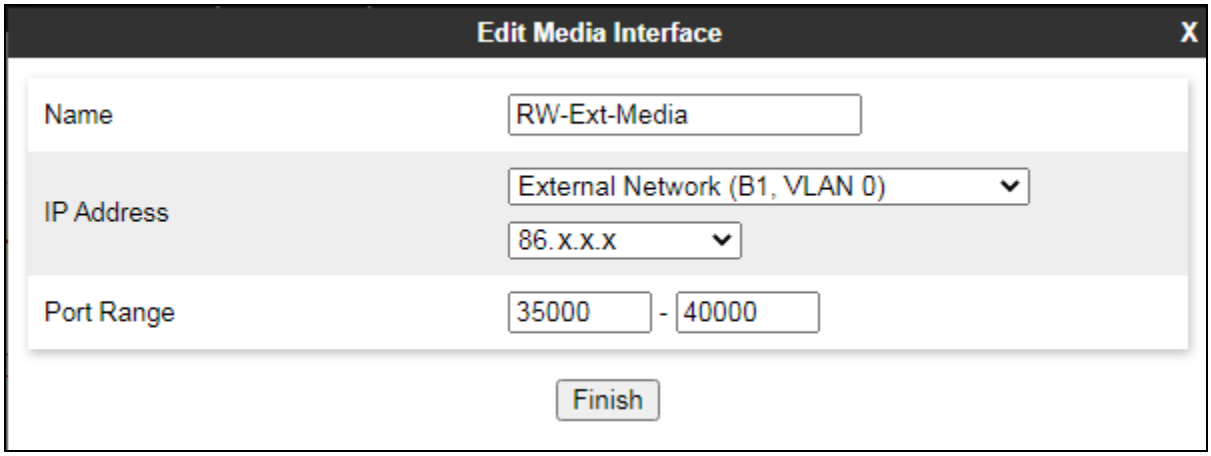
11.10. Media Interfaces

Media Interfaces are created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Create separate Media Interfaces for the public and private IP interfaces used to support the Remote Workers.

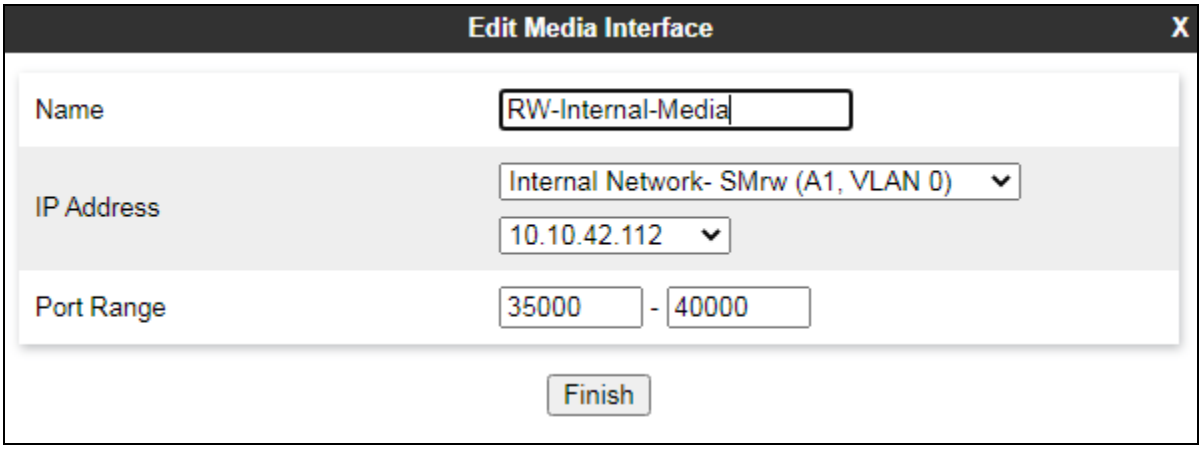
To add a Media Interface for the outside network, navigate to **Network & Flows → Media Interface** and click the **Add** button. The screen below shows the two Media Interfaces that were previously configured for compliance testing.



On the **Media Interface** screen, enter an appropriate **Name** for the Media Interface, e.g., **RW-Ext-Media.** Select the public IP Address for Avaya SBCE used for Remote Worker traffic from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.



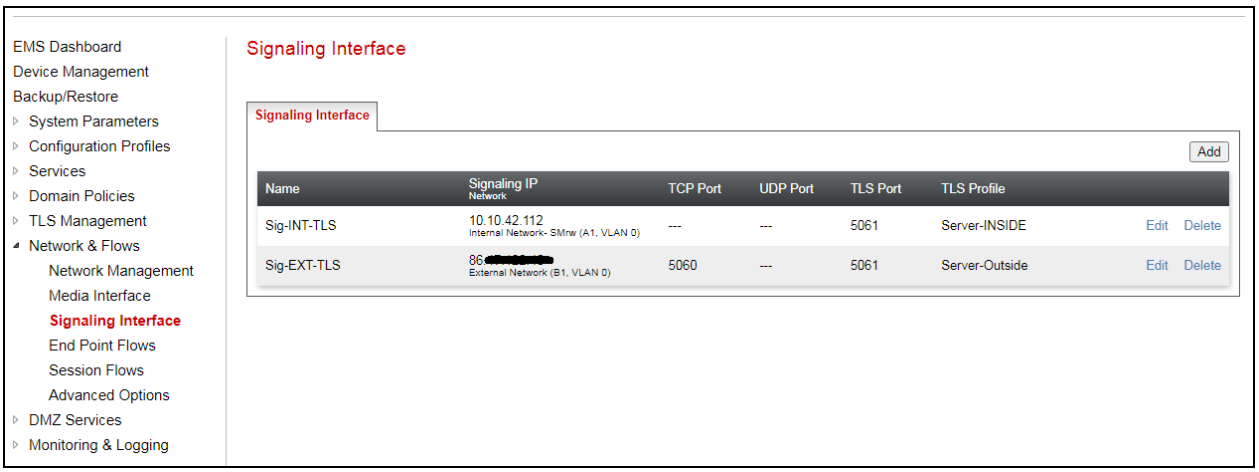
A Media Interface facing the enterprise network side named **RW-Internal-Media** was similarly created. The inside IP Address of Avaya SBCE used for Remote Worker traffic was selected from the drop-down menu. The **Port Range** was left at the default values. Click **Finish**.



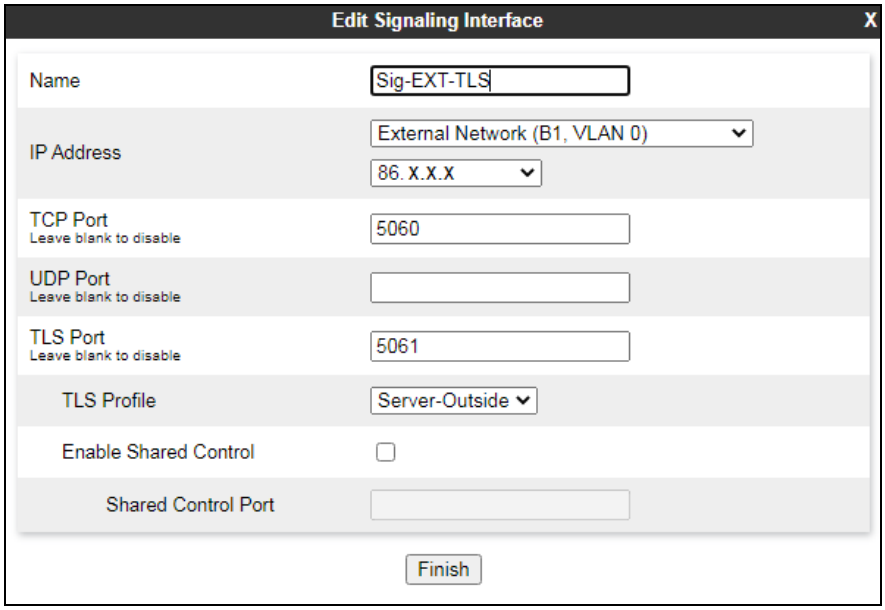
11.11. Signaling Interfaces

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a Signaling Interface for both the outside and inside IP interfaces.

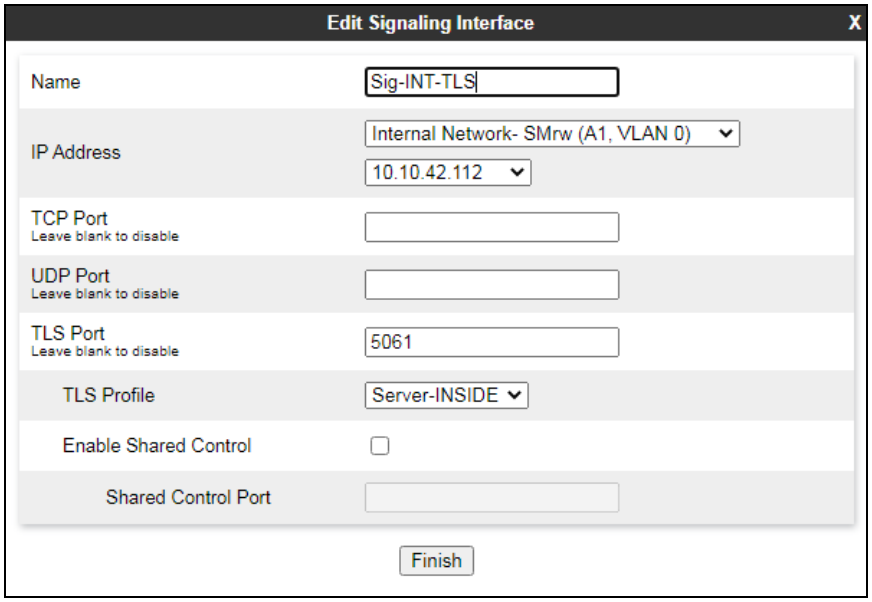
To create a signaling interface facing the public network, navigate to **Network & Flows → Signaling Interface** and click the **Add** button. The screen below shows the two Signaling Interfaces that were previously configured for compliance testing.



On the **Signaling Interface** screen, enter an appropriate **Name** for the interface, e.g., **Sig-EXT-TLS**. Select the public IP Address of Avaya SBCE used for Remote Workers from the **IP Address** drop-down menu. For compliance testing, **TLS Port 5061** was used to listen for Remote Worker signaling traffic. Under **TLS Profile**, select the **Server-Outside** profile created in **Section 17.6** . Click **Finish**.



A Signaling Interface facing the enterprise network side named **Sig-INT-TLS** was similarly created. The inside IP Address of Avaya SBCE used for Remote Worker traffic was selected from the drop-down menu. **TLS Port 5061** was used to listen for Remote Worker signaling traffic. Under **TLS Profile**, select the **Server-INSIDE** profile created in **Section 17.6**. Click **Finish**.

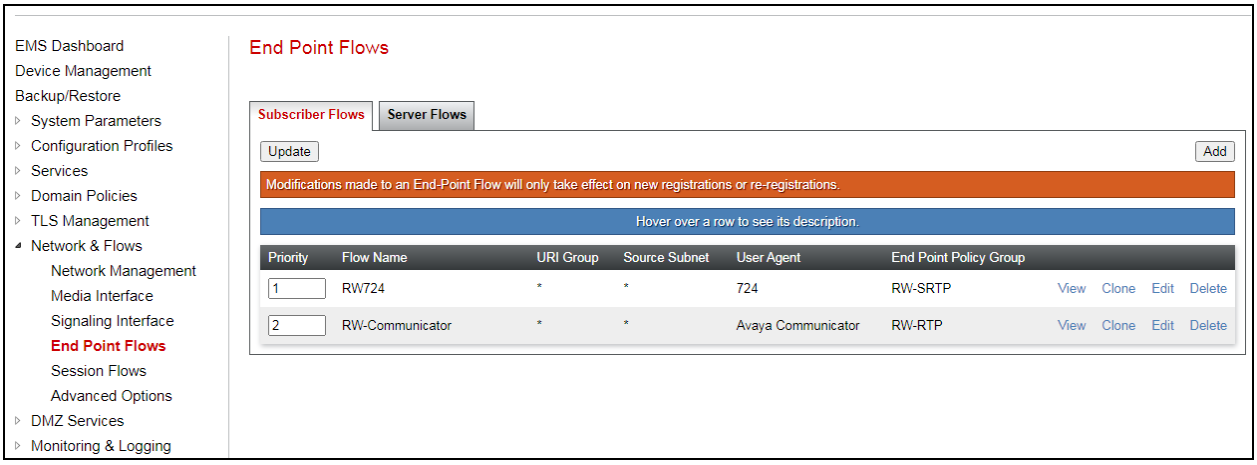


11.12. End Point Flows

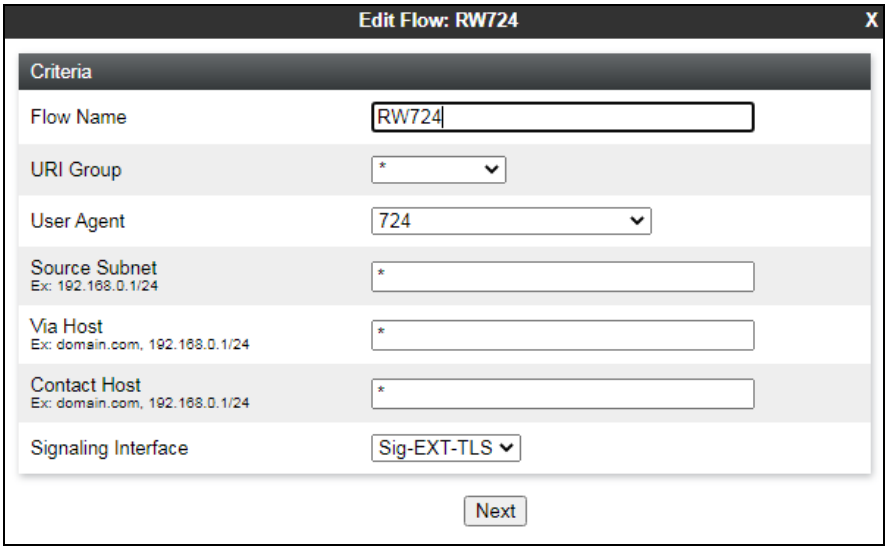
End Point Flows determine the path to be followed by the packets traversing through Avaya SBCE. These flows combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

11.12.1. Subscriber Flow

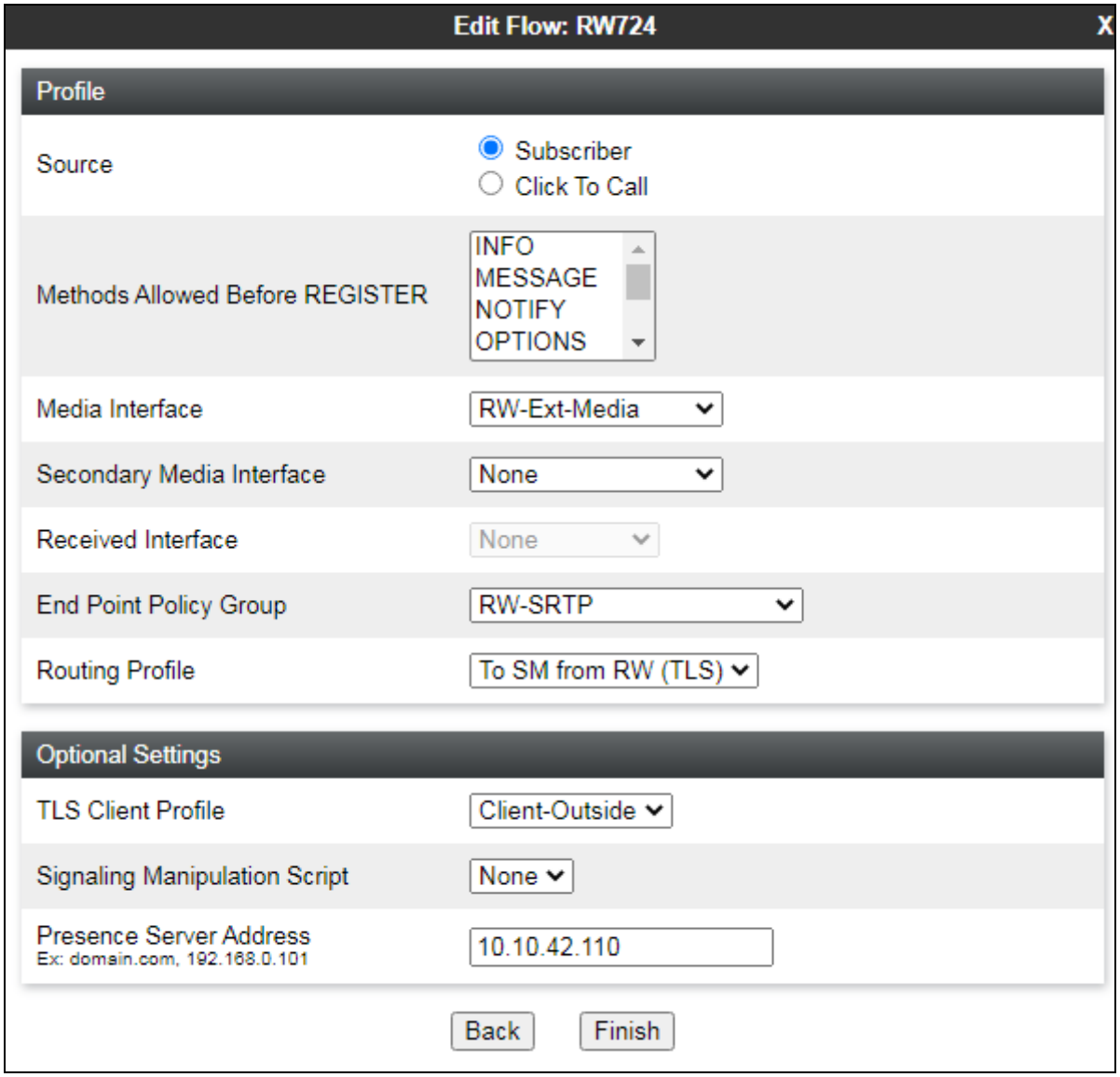
To create a new Subscriber Flow, navigate to **Network & Flows → End Point Flows**, select the **Subscriber Flows** tab and click the **Add** button. The screen below shows the two Subscriber Flows that were previously configured for compliance testing. This section will show the configuration of the **RW724** Subscriber flow as this was created specifically for this compliance test.



The following screen shows the **RW724** Subscriber Flow created specifically for the SCC handsets. This flow uses the interfaces, policies, and profiles defined in previous sections.



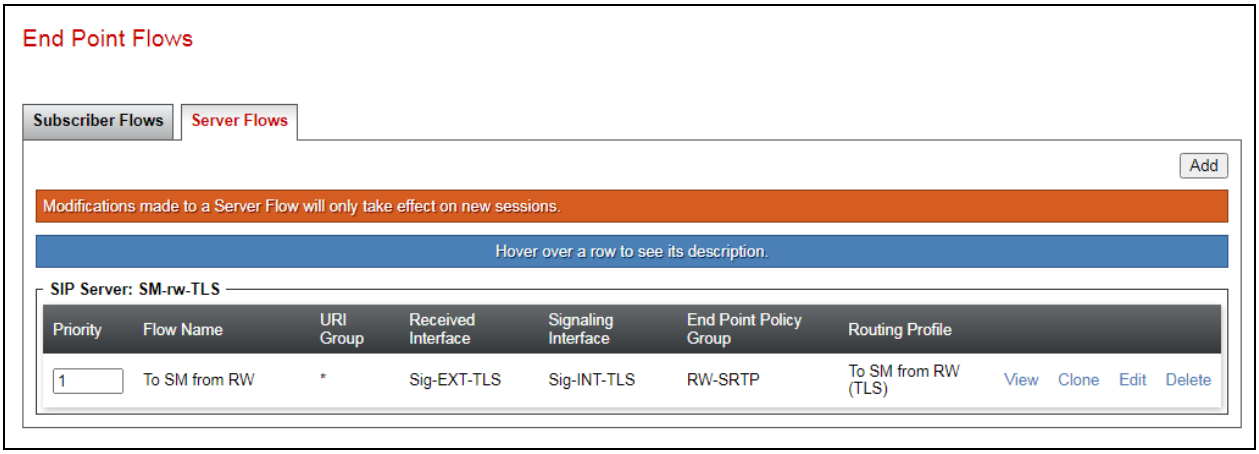
Clicking on **Next** from the previous page shows the following that was configured for the **RW724** Subscriber Flow.



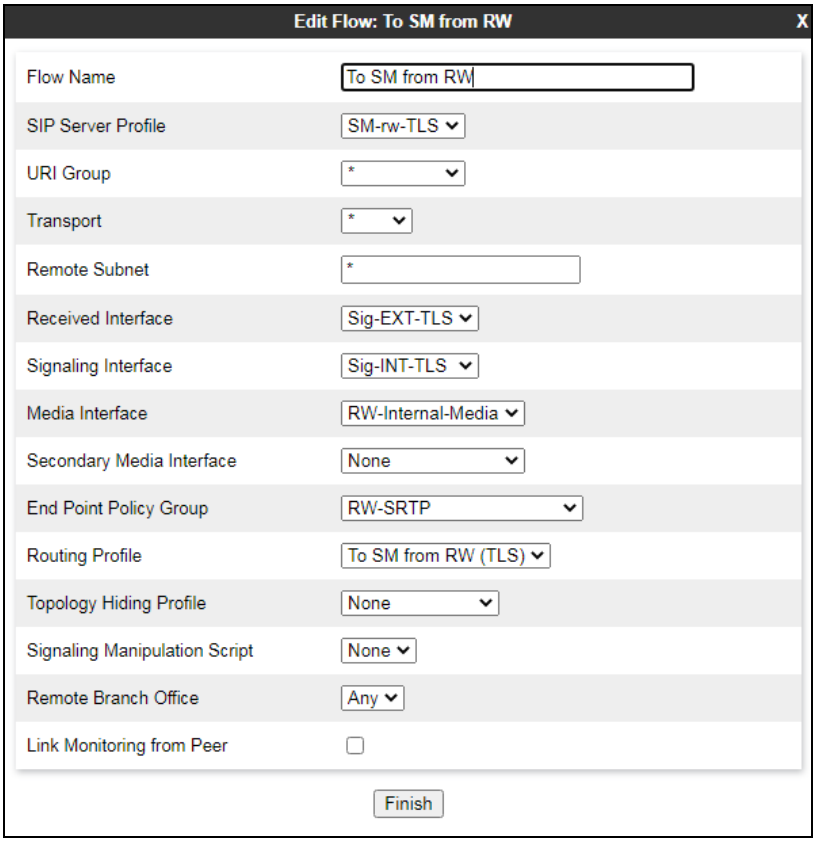
Note: The **Client-Outside** profile, created in **Section 17.5**, is selected under TLS Client Profile when mutual authentication is used between the Avaya SBCE and the Remote Workers. If one-way authentication is used, this field can be left with the default **None**.

11.12.2. Server Flow

To create a Server Flow, navigate to **Network & Flows → End Point Flows**. Select the **Server Flows** tab and click the **Add** button (not shown).



The following screen shows the **To SM from RW** Server Flow that was created for compliance testing. This flow uses the interfaces, policies, and profiles defined in previous sections.

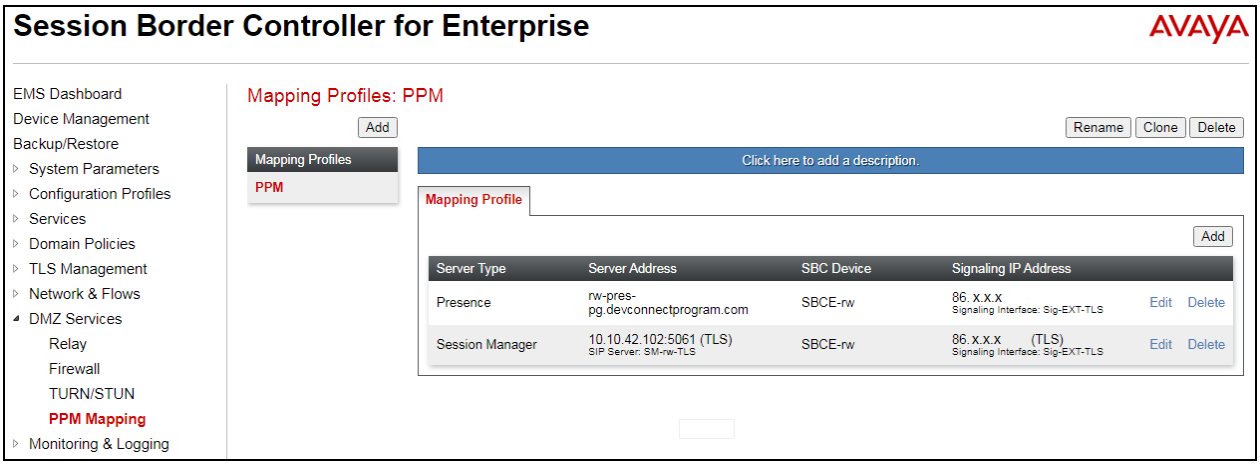


11.13. PPM Mapping

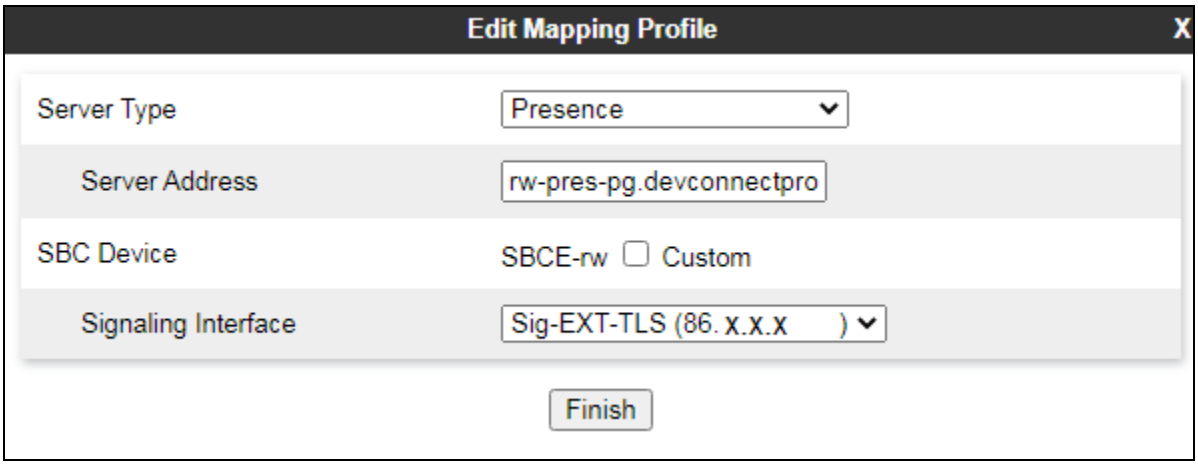
Use the steps in this section to create a Personal Profile Manager (PPM) Mapping Profile. This profile determines how PPM data is routed between Session Manager and the Remote Worker endpoints via the Avaya SBCE.

Note: All public IP addresses are either blanked out or marked with 'x.x.x.x' as these are public IP addresses and this is usual DevConnect procedure.

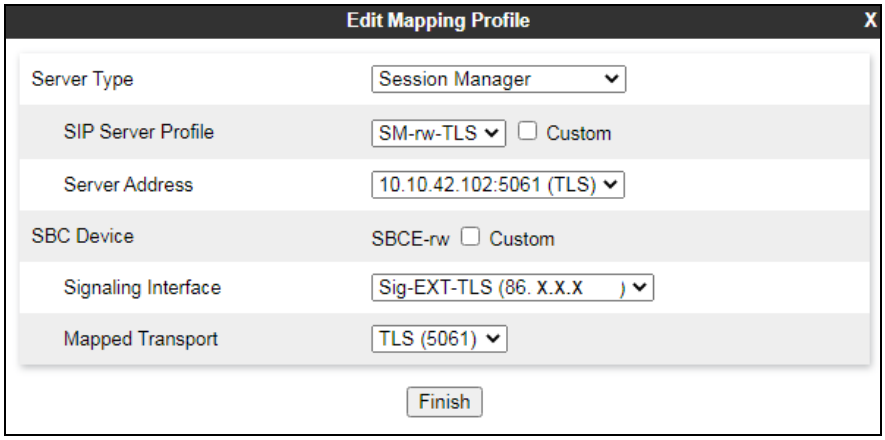
Navigate to **DMZ Services → PPM Mapping** and click the **Add** button. Enter a descriptive Profile Name, e.g., **Session Manager** and click **Next** (not shown). The screen below shows the two Mapping Profiles that were used for compliance testing, the details of which are illustrated in this section.



Below shows the Mapping Profile for **Presence**, which is selected for **Server Type**. The **Server Address** is set to that of the Presence FQDN. Under **Signaling Interface**, select the **Sig-EXT-TLS** interface and **TLS (5051)** port as created in **Section 11.11**. Click **Finish**.



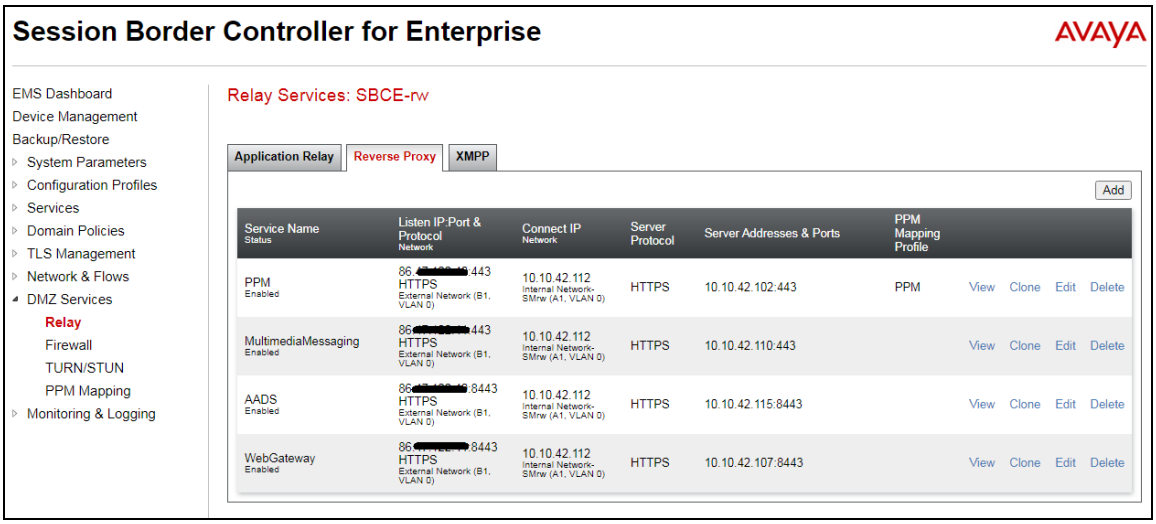
Below shows the Mapping Profile for **Session Manager**, which is selected for **Server Type**. Under **SIP Server Profile** select the **SM-rw-TLS** Session Manager profile created in **Section 11.4**. The **Server Address** is automatically populated with the Session Manager IP address and port**.** Under **Signaling Interface** and **Mapped Transport**, select the **Sig-EXT-TLS** interface and **TLS (5061)** port as created in **Section 11.11**. Click **Finish**.



11.14. Relay Services

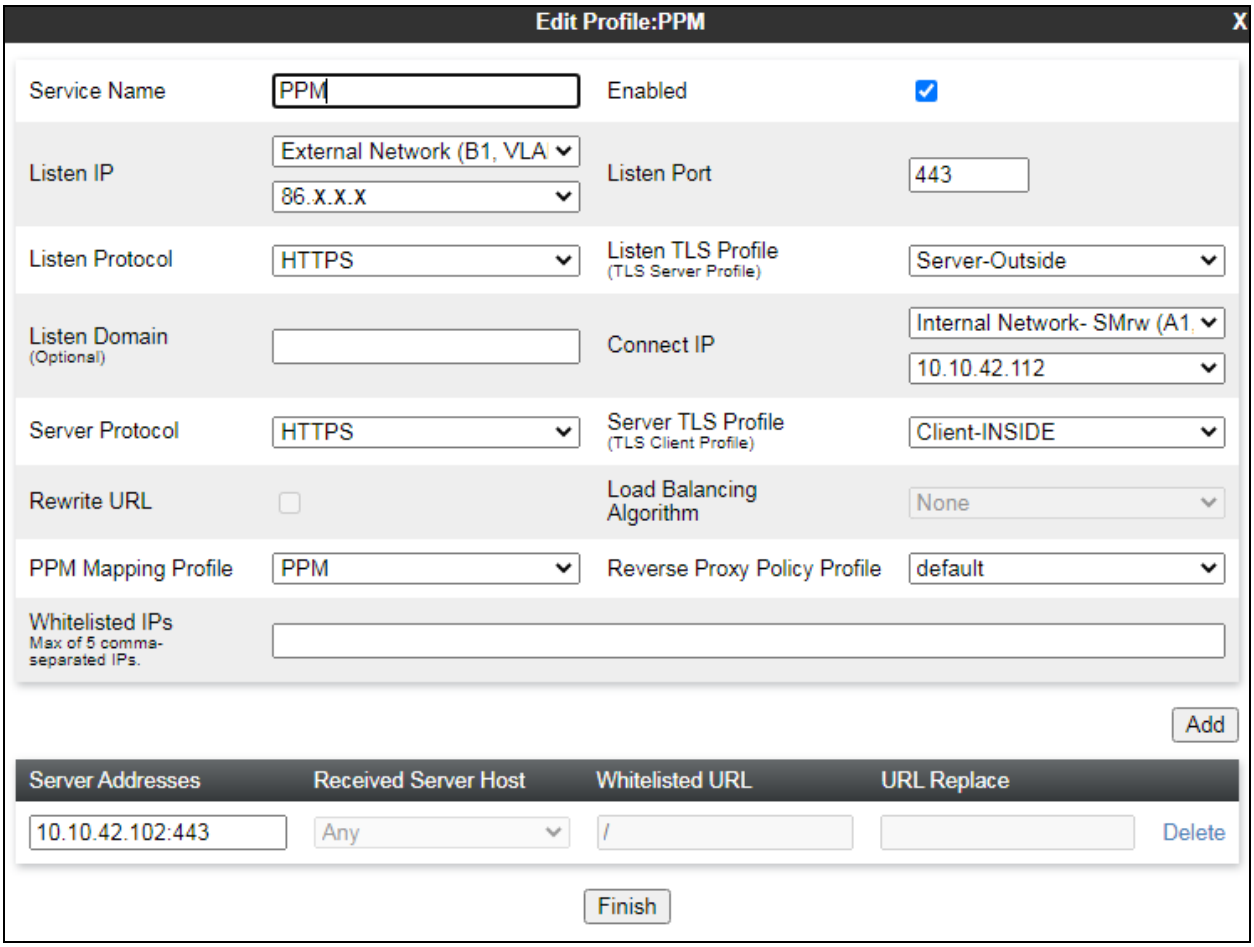
Relay Services contain the Application Relay and Reverse Proxy Policies. They are used to define how non-SIP related IP traffic is routed for remote endpoints, such as firmware updates, security settings, configuration data, etc. Only Reverse Proxy Relays were used for compliance testing.

Navigate to **DMZ Services → Relay** and select the **Reverse Proxy** tab. Click **Add** to configure new Reverse Proxy policies. The following shows the Reverse Proxy policies created for compliance testing, all of which will be shown in greater detail in this section. The external IP addresses are all blocked out as they are public IP addresses. Two separate IP addresses were used with two separate ports on each to allow for the four services shown below.

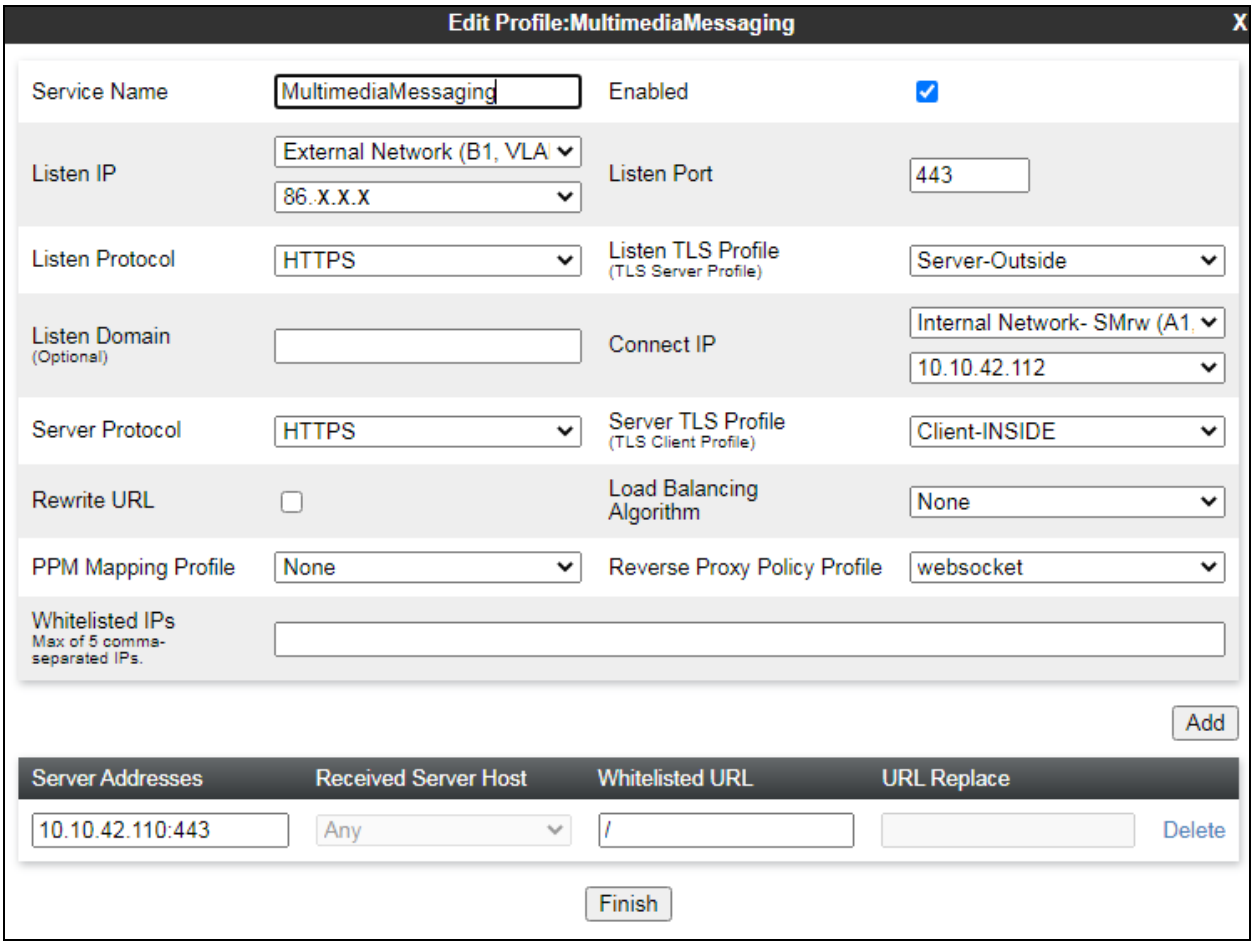


A policy named **PPM** is used for PPM traffic between Session Manager and the remote endpoints.

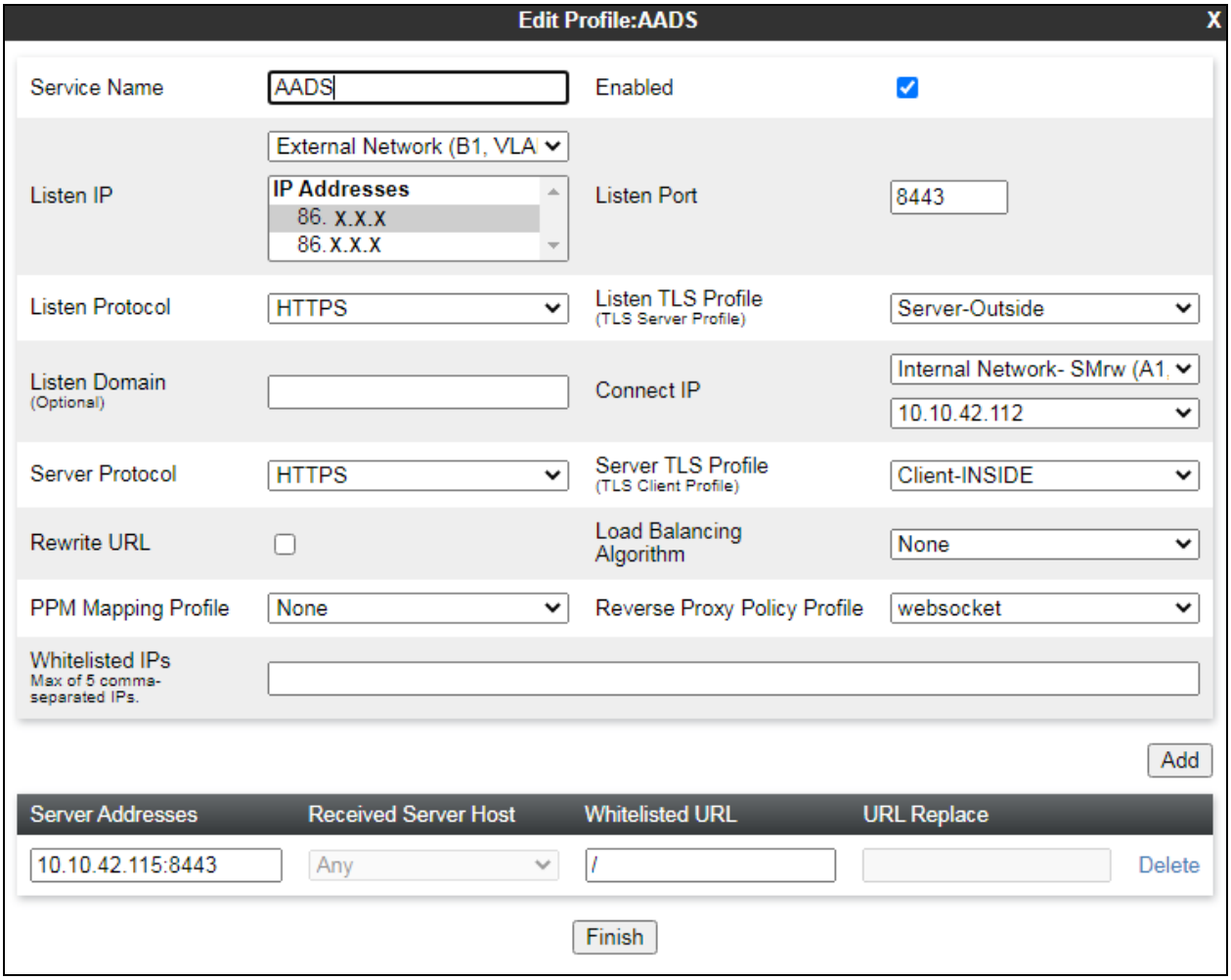
- Under **Listen IP** the **Public B1** network and the IP address of the external signaling interface configured for Remote Workers are selected. **Listen Port** is set to **443** and **Listen Protocol** to **HTTPS**. Under **Listen TLS Profile**, the **Server-Outside** profile is selected.
- The **Connect IP** is set to the internal IP address of the Avaya SBCE used for Remote Workers (**10.10.42.112**) on network **Inside A1**. Under **Server Protocol**, **HTTPS** is selected.
- Under **PPM Mapping Profile** select the **PPM** previously created.
- The **Server Protocol** is set to **HTTPS** and the **Server TLS Profile** to the **Client-INSIDE** profile. The **Server Address** is set to the IP address and port of Session Manager, **10.10.42.102:443**.
- Click **Finish**.



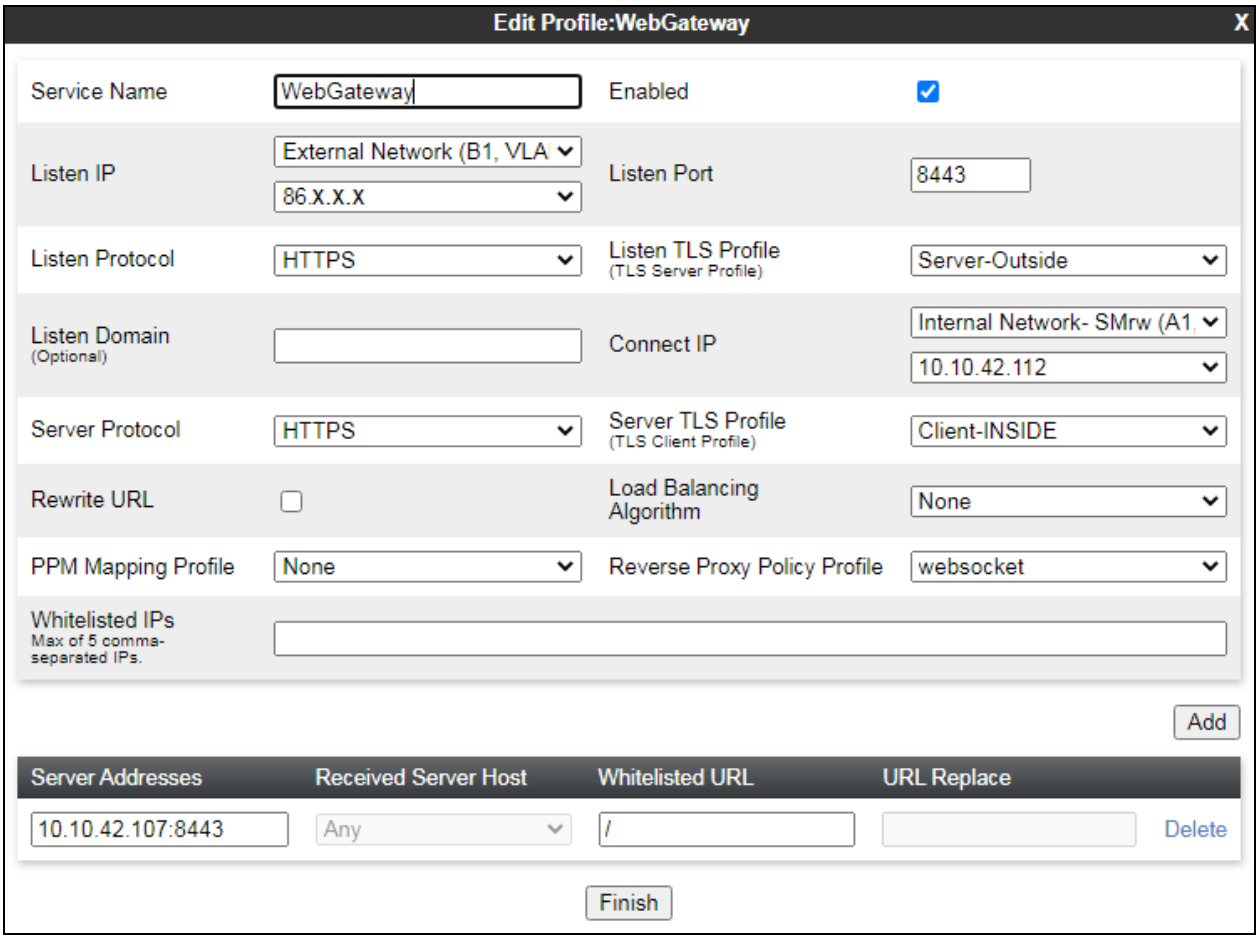
The policy named **MultimediaMessaging** was created, used for Presence Services and Push Notifications for presence. In this case **Listen IP** is set to the external Avaya SBCE IP address used for file transfers and **Listen Port 443**. The **Server Address** is set to the IP address and port of the Presence Server, **10.10.42.110:443** at the enterprise.



The policy named **AADS** was created, used for HTTPS traffic (e.g., settings files, telephone firmware upgrades), between a Utility server at the enterprise (AADS) and the remote endpoints. In this case **Listen IP** is set to the external Avaya SBCE IP address used for file transfers and **Listen Port 8443**. The **Server Address** is set to the IP address and port of the Utility server, which is the AADS IP address, **10.10.42.115:8443** at the enterprise.



The policy named **WebGateway** was setup for Push Notifications. The **Listen IP** is set to the external Avaya SBCE IP address used for file transfers. The **Listen Port** is set to **8443**. The **Server Address** is set to the IP address and port of the AAWG at the enterprise **10.10.42.107** again using port **8443**.



12. Configuration of Net Iletisim Secure Communication Server and 7/24 Secure Communication Client

The Secure Communication Server and 7/24 Secure Communication Client is provided, installed and implemented by Net Iletisim. Due to the complex nature of these configurations, it was deemed unnecessary to show any configuration steps on these Application Notes. For all information on the installation and configuration of the Net Iletisim Secure Communication Server and 7/24 Secure Communication Client, contact Net Iletisim, as per **Section 2.3**.

13. Verification Steps

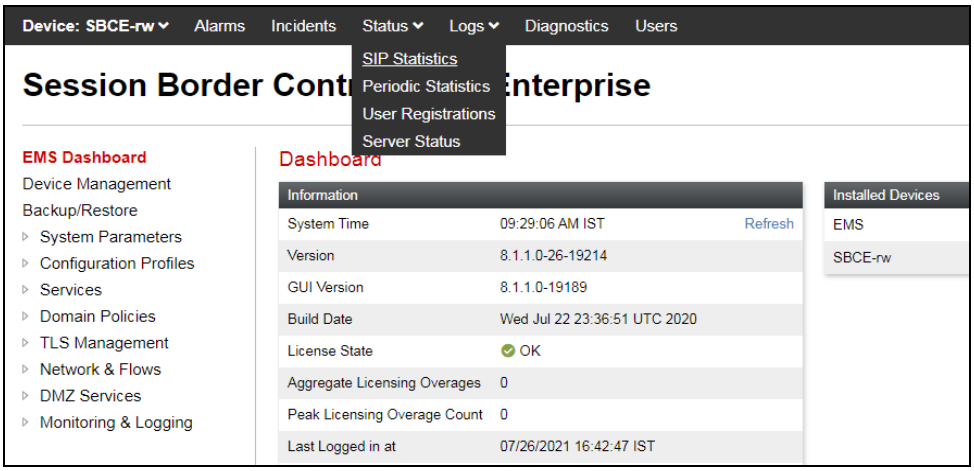
The following steps can be taken to ensure that connections between Net Iletisim SCC handsets and the Avaya platform are established correctly.

13.1. Avaya Session Border Controller for Enterprise Verification

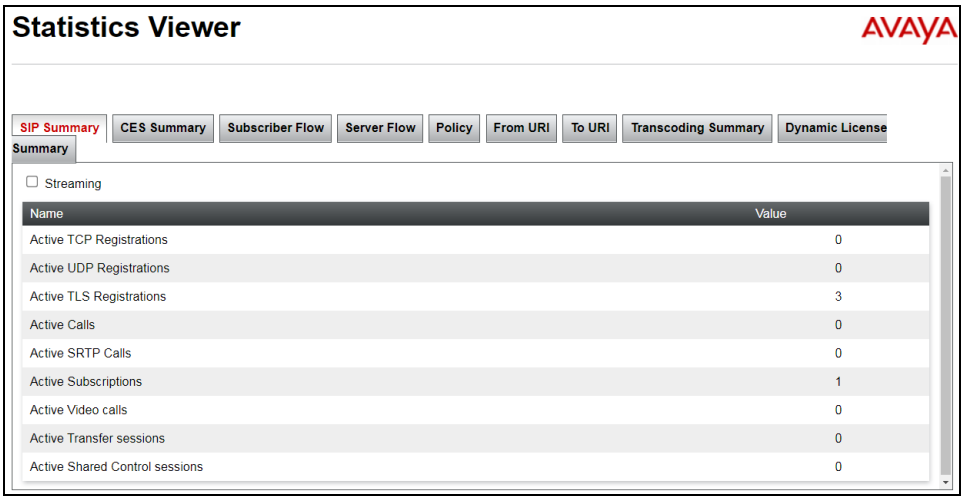
This section contains verification steps that may be performed using Avaya Session Border Controller for Enterprise.

13.1.1. Statistics Viewer

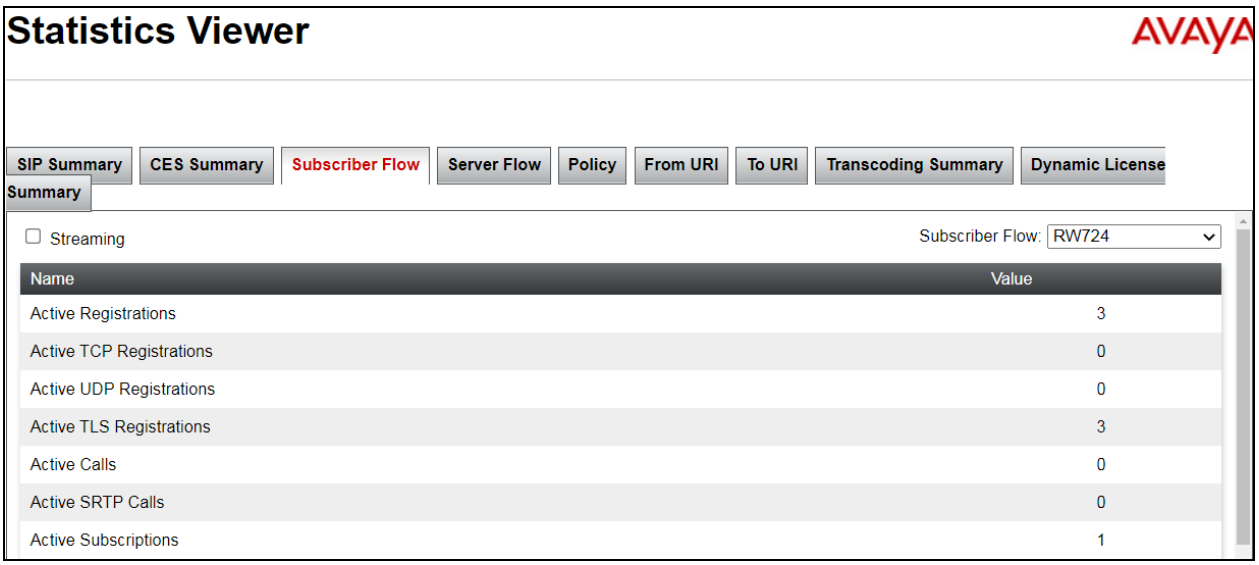
The **Statistics Viewer** can be accessed from the Avaya SBCE top navigation menu by selecting the **Status** menu, and then **SIP Statistics**.



There are a number of tabs that display information on registrations and subscriptions, the **SIP Summary** tab is a useful place to start and shows that there are three registrations currently using a TLS connection.

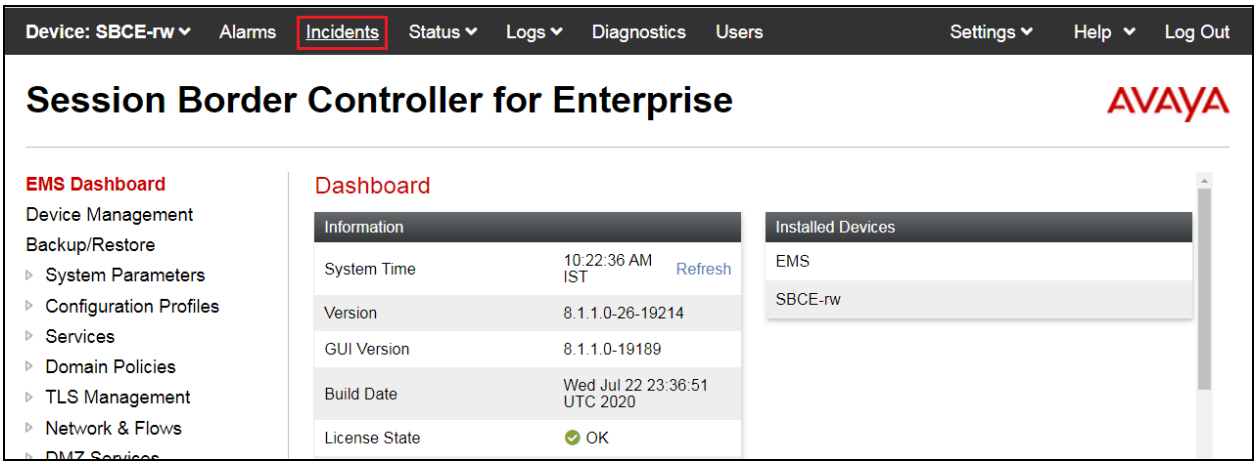


The **Subscriber Flow** tab on the **Statistics Viewer** will show **Active Registrations, Active Calls** and other information about subscribers on the selected flow.



13.1.2. Incidents Viewer

The **Incident Viewer** can be accessed from the top navigation menu as highlighted in the screenshot below.



Use the **Incident Viewer** to troubleshoot possible failures. Further Information can be obtained by clicking on an incident in the incident viewer.

Incident Viewer

AVAYA

Device All Category All Clear Filters Refresh Generate Report

Displaying results 1 to 15 out of 2000.

ID	Device	Date & Time	Category	Type	Cause
813731944491506	SBCE-rw	Jul 28, 2021, 10:18:08 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed
813731618068292	SBCE-rw	Jul 28, 2021, 10:07:16 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed
813731362217101	SBCE-rw	Jul 28, 2021, 9:58:44 AM	Policy	Call Denied	INVITE from subscriber, but no existing subscription
813731308066956	SBCE-rw	Jul 28, 2021, 9:56:56 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed
813730940388725	SBCE-rw	Jul 28, 2021, 9:44:40 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed
813730358547435	SBCE-rw	Jul 28, 2021, 9:25:17 AM	Policy	Call Denied	INVITE from subscriber, but no existing subscription
813730296551122	SBCE-rw	Jul 28, 2021, 9:23:13 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed
813729929625686	SBCE-rw	Jul 28, 2021, 9:10:59 AM	DoS	Domain DoS	Domain DOS Detected,Pending Threshold Crossed

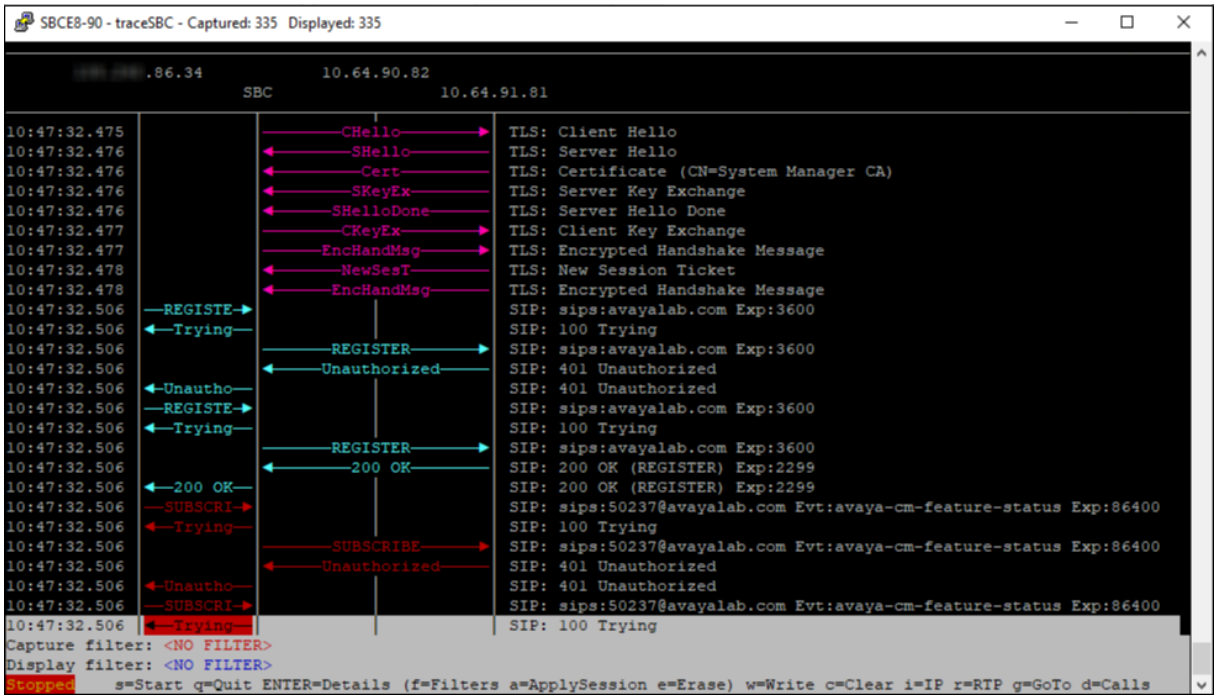
13.1.3. traceSBC Tool

Because of the normally encrypted nature of the traffic used in Remote Workers configurations, traditional network capture tools like Wireshark are usually unable to provide help when troubleshooting or monitoring this type of messages.

The Avaya SBCE traceSBC tool is a perl script that parses Avaya SBCE log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, the tool can be used even in case of TLS and HTTPS.

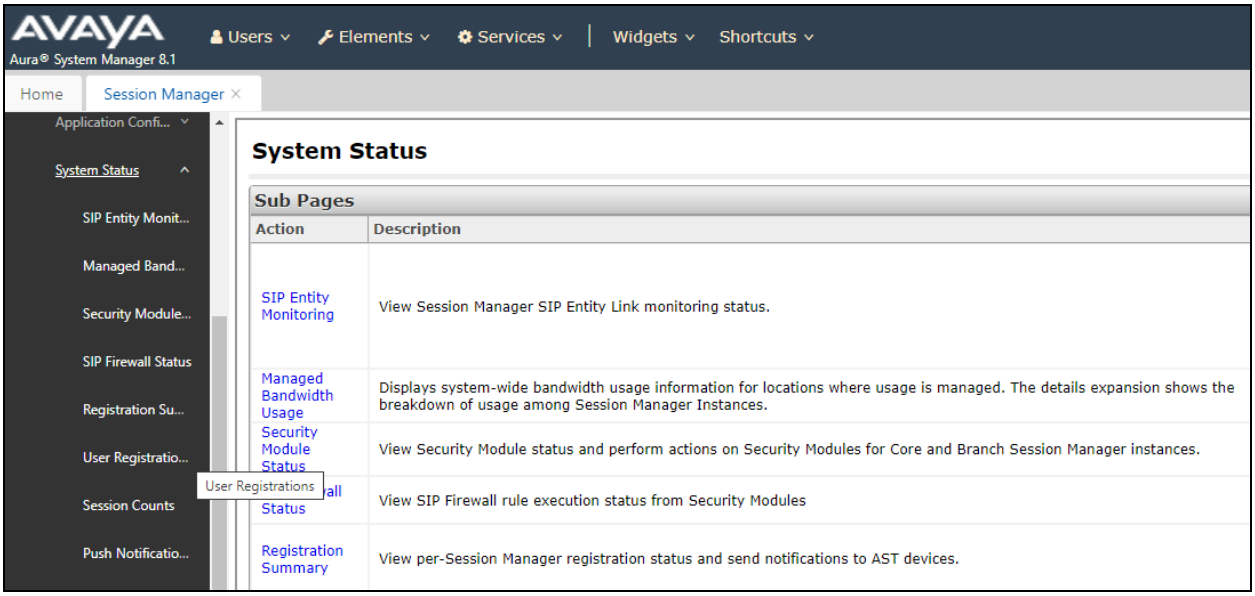
To run the traceSBC tool, log into SBCE command line interface using SSH client as user **ipcs**. Issue the command **sudo su** to change to **root** user. Start the tool by issuing the **traceSBC** command.

Note: The screen shot below is an example of such a trace and was not taken as part of the compliance testing.

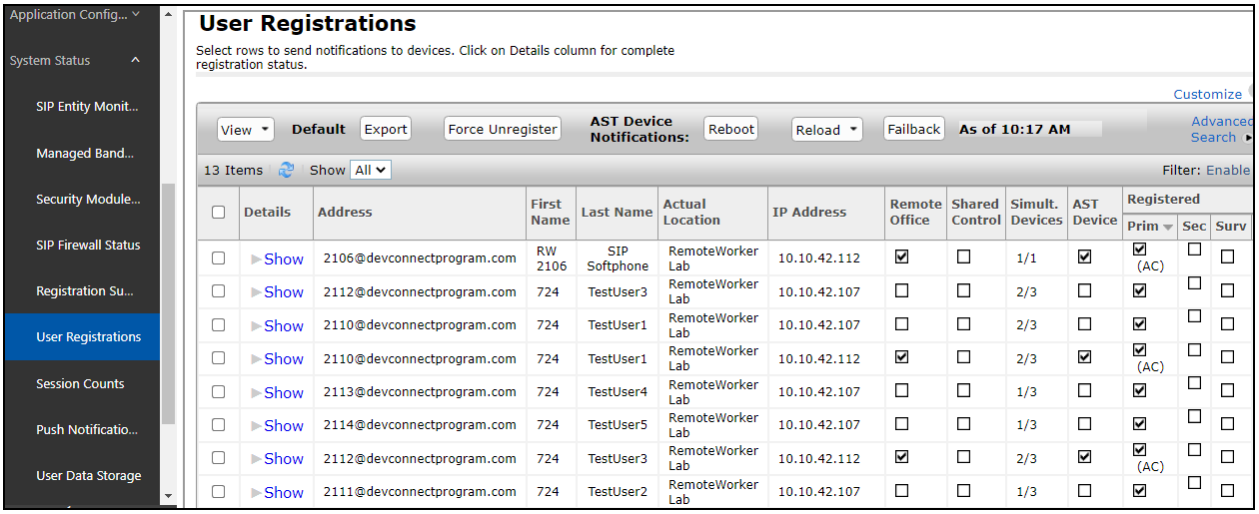


13.2. Session Manager Verification

To view the Remote Workers registration status in Session Manager, from the System Manager GUI **Home** page, navigate to **Elements → Session Manager → System Status → User Registrations**.



The following is an abbreviated screen capture showing some of the Remote Workers and local enterprise users in the reference configuration. Note that the **IP Address** column for all Remote Workers users will always show the inside IP Address of an SBC, e.g., **10.10.42.112** as shown below.



14. Conclusion

These Application Notes describe the configuration steps for provisioning Net Iletisim 7/24 Secure Communication Client (iOS) R1.0.20 with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Session Manager R8.1 via the Remote Worker interface on Avaya Session Border Controller for Enterprise R8.1, using Avaya Aura® Web Gateway R3.8 for push notifications and Avaya Aura® Device Services R8.1 for configuration. Please refer to **Section 2.2** for test results and observations.

15. Additional References

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

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Deploying Avaya Aura® Communication Manager*, Release 8.1
2. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 8.1
3. *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, August 2020
4. *Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise*, Release 8.1.x., August 2020
5. *Avaya SBCE 8.1 Security Configuration and Best Practices Guide*, Release 8.1, February 2020
6. *Administering Avaya Aura® Session Manager*, Release 8.1.x, October 2020
7. *Avaya Aura® Session Manager Security Design*, Release 8.1.x, April 2020
8. *Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.1.11, October 2020
9. *Installing and Administering Avaya J100 Series IP Phones*, Release 4.0.7, November 2020
10. *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac and Windows*, September 2020
11. *Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 7.0, Avaya Aura® Communication Manager Rel. 7.0 and Avaya Aura® Session Managers Rel. 7.0* – Issue 1.0, Application Notes, June 2016
12. *Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform*

Documentation for Net Iletisim products can be obtained as follows:

- Web: http://www.netiletisim.com.tr/#contact
- Email: netiletisim@netiletisim.com.tr
- Telephone: +90 (312) 419 29 99 | Ankara

Appendix

16. SIP Trunk Configuration

These are the settings used for the SIP trunk setup for compliance testing. This contains information on the Signaling Group as well as the Trunk Group.

16.1. Signaling Group

```
display signaling-group 1                                        Page   1 of   3
                              SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        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: sm81xvmpg
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1

Far-end Domain: devconnectprogram.com
                                          Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                    IP Audio Hairpinning? n
         Enable Layer 3 Test? y                  Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 12
```

16.2. Trunk Group

The following pages show the configuration of the Trunk Group used during compliance testing.

Page 1

```
display trunk-group 1                                            Page   1 of   4
                              TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SIP Phones                  COR: 1        TN: 1        TAC: *801
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                         Member Assignment Method: auto
                                                  Signaling Group: 1
                                                Number of Members: 10
```

Page 2

```
display trunk-group 1                                          Page   2 of   4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                          Redirect On OPTIM Failure: 32000

            SCCAN? n                              Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


             XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n





 Caller ID for Service Link Call to H.323 1xC: station-extension
```

Page 3

```
display trunk-group 1                                          Page   3 of   4
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                            UUI Treatment: service-provider

                                             Replace Restricted Numbers? n
                                            Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no



 Show ANSWERED BY on Display? y

 DSN Term? n
```

Page 4

```
trunk-group 1                                                    Page   4 of   4
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? y
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                  Support Request History? y
                              Telephone Event Payload Type: 101


                        Convert 180 to 183 for Early Media? n
                  Always Use re-INVITE for Display Updates? n
    Resend Display UPDATE Once on Receipt of 481 Responses? n
                        Identity for Calling Party Display: P-Asserted-Identity
            Block Sending Calling Party Location in INVITE? n
                 Accept Redirect to Blank User Destination? n
                                           Enable Q-SIP? n

          Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                                Request URI Contents: may-have-extra-digits
```

17. TLS Certificates Management

In the reference configuration, the Avaya SBCE uses TLS transport to securely communicate with Session Manager on the enterprise network, and with the Remote Workers on the public network.

For TLS protocol usage, Avaya recommends using unique digital identity certificates, signed by a trusted Certificate Authority (CA). This section describes the procedures to install and configure TLS certificates on the Avaya SBCE public and private interfaces, using the Avaya System Manager built-in Certificate Authority to generate the identity certificates.

The following tasks are performed:

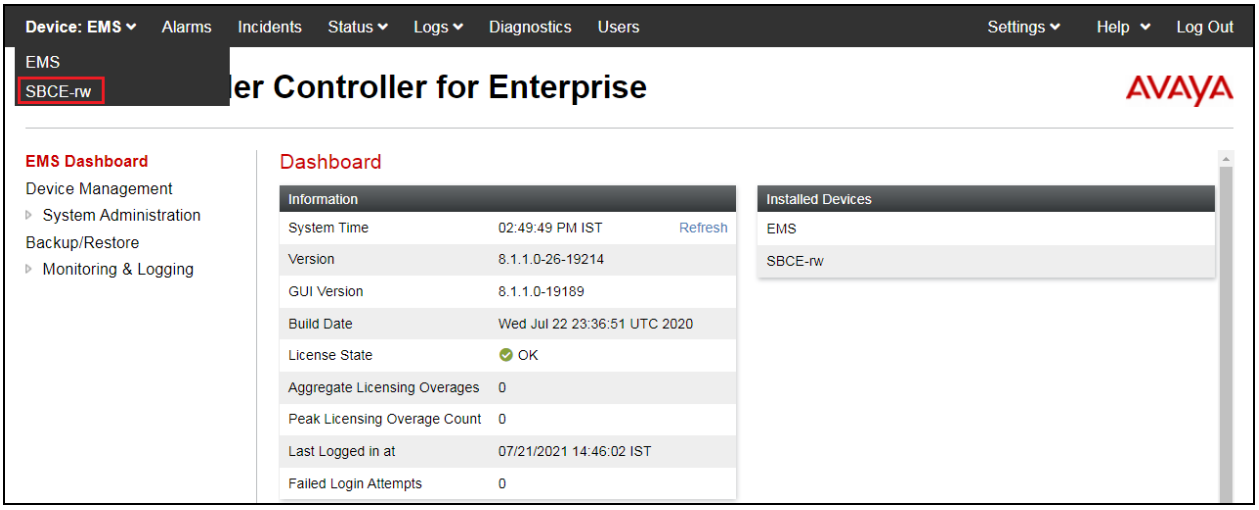
- Network Management
- Create Certificate Signing Requests in Avaya SBCE
- Install Identity Certificates issued by the System Manager CA in Avaya SBCE
- Install System Manager CA root certificate in Avaya SBCE
- Create TLS Client Profiles in Avaya SBCE
- Create TLS Server Profiles in Avaya SBCE

17.1. Network Management

Use a Web browser to access the Element Management Server (EMS) web interface and enter https://*ipaddress*/sbc in the address field of the web browser, where *ipaddress* is the management LAN IP address of the Avaya SBCE.

Log in using the appropriate credentials.

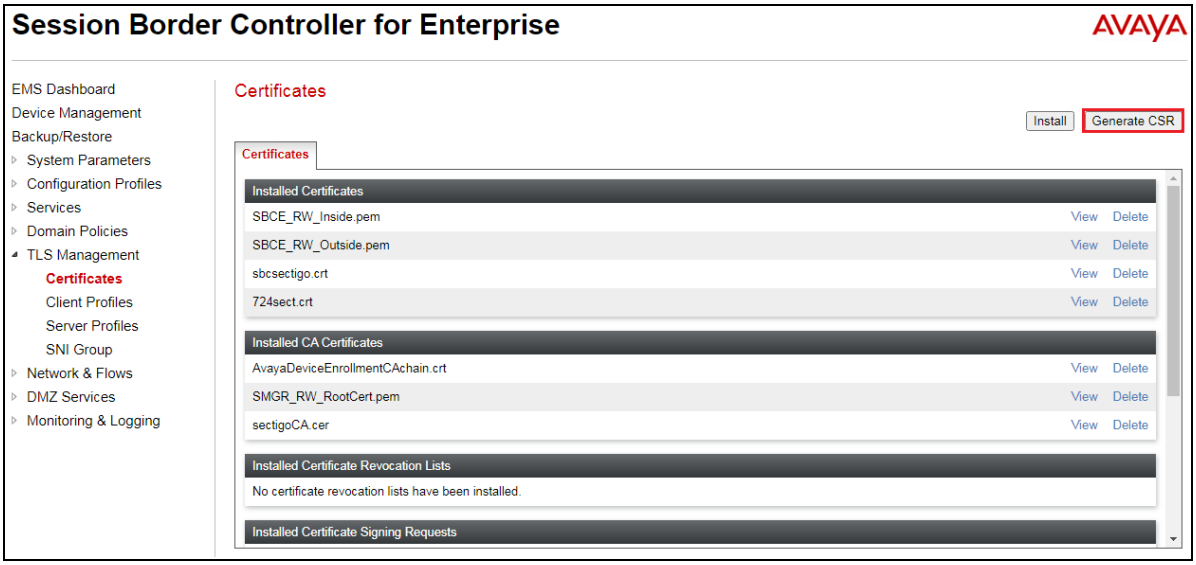
Once logged in, the following screen is presented, and the device must be set to the SBCE before any further configuration can take place.



17.2. Create Certificate Signing Requests for Avaya SBCE interfaces

Follow the steps in this section to create Certificates Signing Requests (CSR) for the Avaya SBCE external interface. This CSR will later be signed by the Avaya System Manager Certificate Authority.

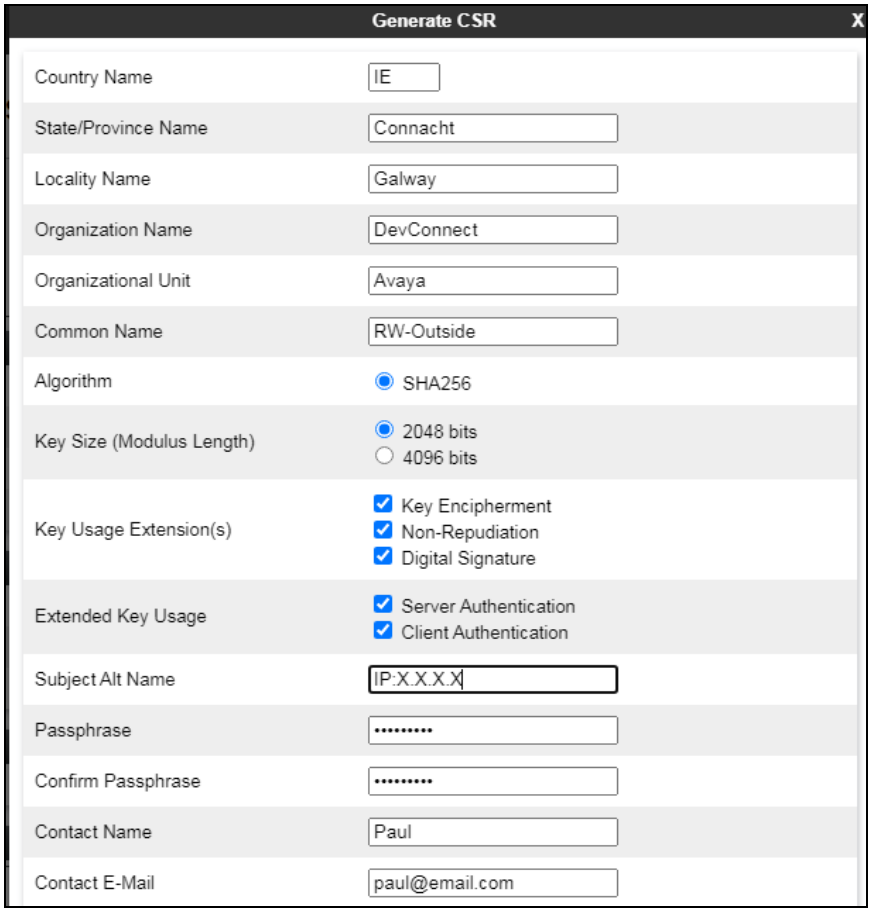
Navigate to **TLS Management → Certificates** and click the **Generate CSR** button. The screen below shows all the certificates that were configured and installed as part of the compliance testing. This section will run through the procedure to create a new CSR and install the resulting Identity Certificate as well as the Root Certificate.



On the **Generate CSR** form that appears, fill the information as required:

- Enter the information on the location and organization fields as appropriate.
- Under **Common Name**, enter a descriptive name, e.g., **RW-Outside**.
- **Algorithm**: **SHA256**.
- **Key Size**: **2048 bits**.
- **Key Usage Extension(s)** and **Extended Key Usage**: check all options.
- **Subject Alt Name**: using format **IP:<value>**, enter the IP addresses of the external interface of the Avaya SBCE used by Remote Workers for HTTPS and for SIP traffic.
- **Passphrase**: Enter a password, used to encrypt the private key.
- **Contact Name** and **Contact Email**: Enter information as appropriate.

The following screen illustrate the parameters used in the sample configuration. Click **Generate CSR**.



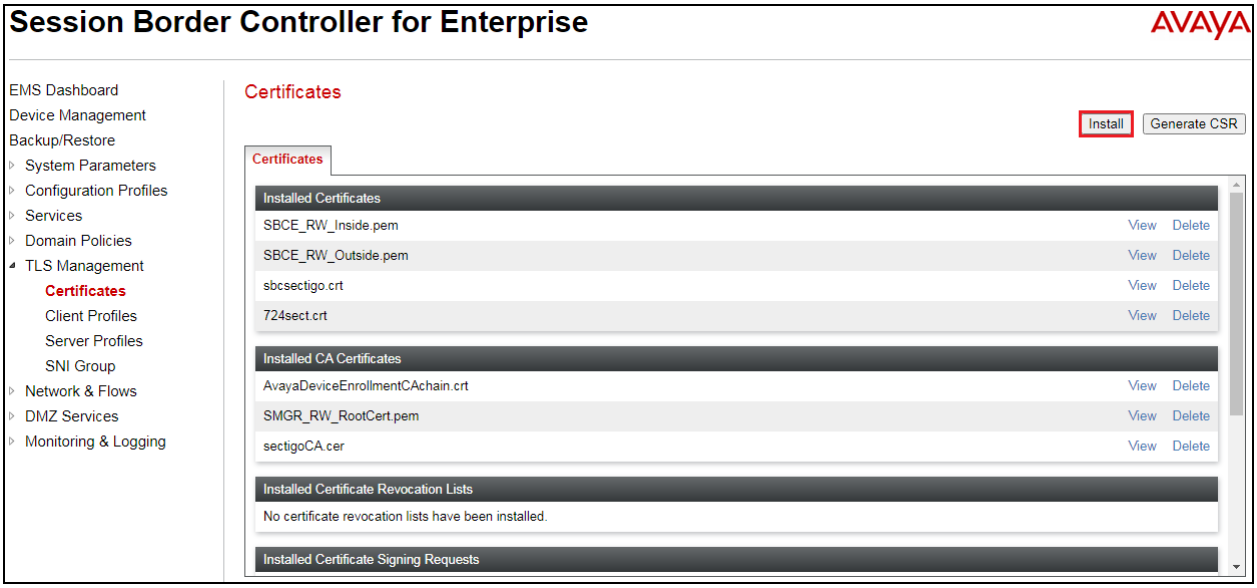
After clicking **Generate CSR**, a pop-up window showing the details of the CSR will appear (not shown). Click on **Download** to extract the CSR file from the Avaya SBCE. Save the generated CSR file, e.g., **SBCE_RW_Outside.req**, to the local PC. This will be used to generate the ID Certificate.

17.3. Install Identity Certificate on Avaya SBCE

Follow the steps in this section to install the identity certificate on the Avaya SBCE.

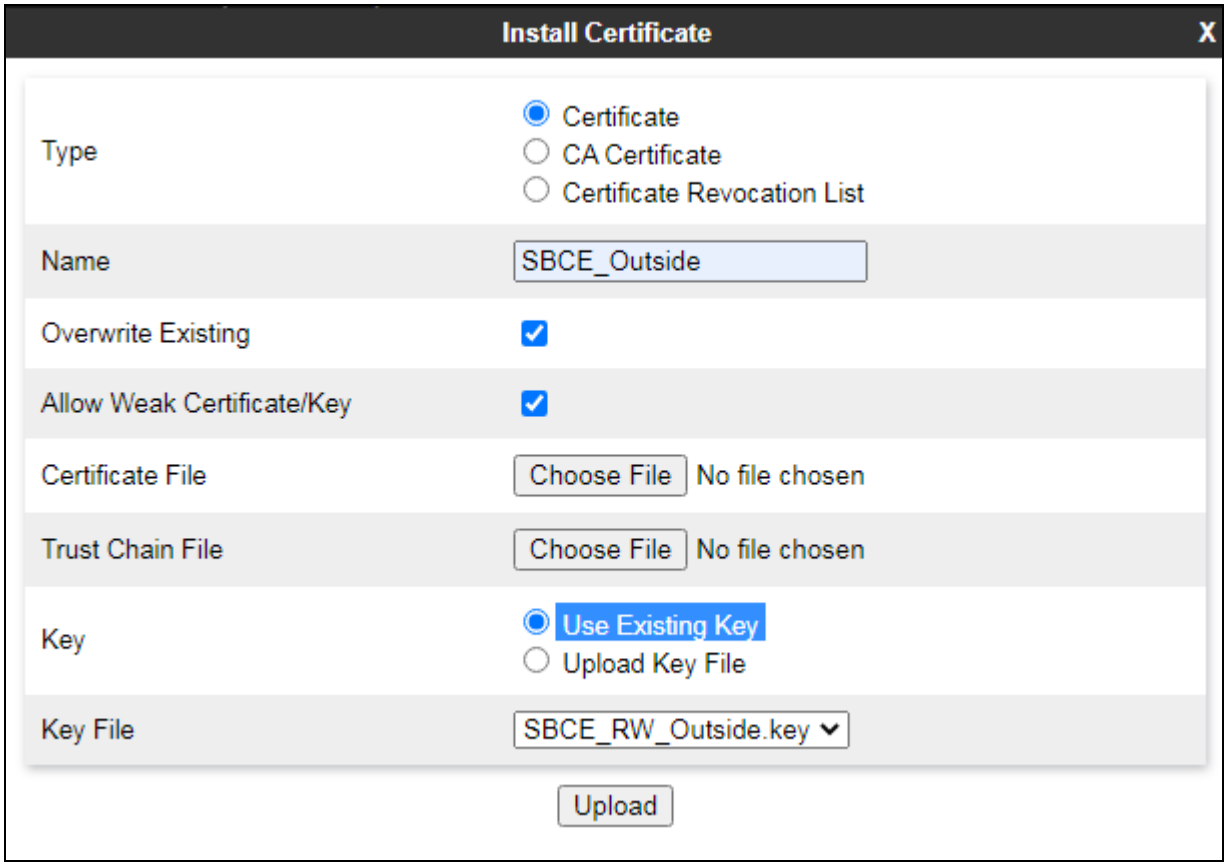
Note: The steps used to create the identity certificates are outside the scope of these Application Notes. System Manager was the CA used to create the identity certs for the internal profiles. Net Iletisim used their own 3rd party certificate authority to create an identity certificate for the outside/external profile, used in the connection to their SCC handsets.

On the Avaya SBCE web interface, navigate to **TLS Management → Certificates** and click the **Install** button. The screen below shows all the certificates that were present for compliance testing.



In the **Install Certificate** screen, select the following:

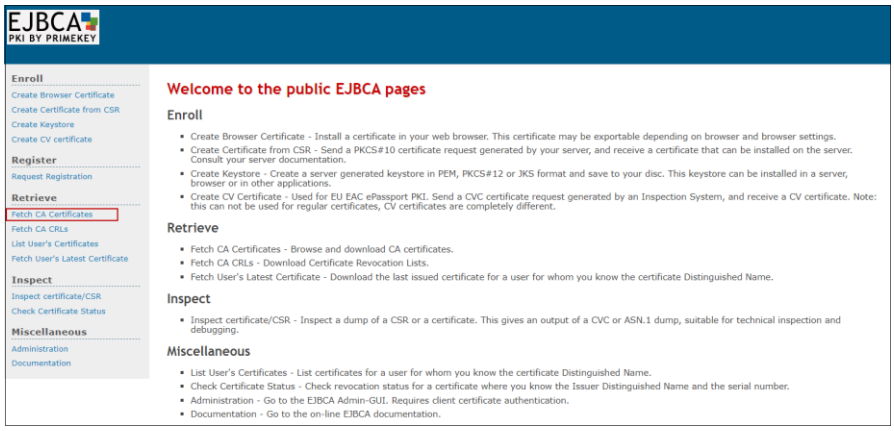
- **Type**: **Certificate**.
- **Name**: enter a descriptive name, e.g., **SBCE_Outside**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- **Certificate File**: click **Browse** to select the identity certificate file previously saved on the local PC (not shown below).
- **Key**: Select **Use Existing Key**, to use one of the key files automatically generated during the CSR creation.
- **Key File**: Select **SBCE_RW_Outside.key** from the drop-down menu.
- Click **Upload**.
- Click **Install** (not shown).



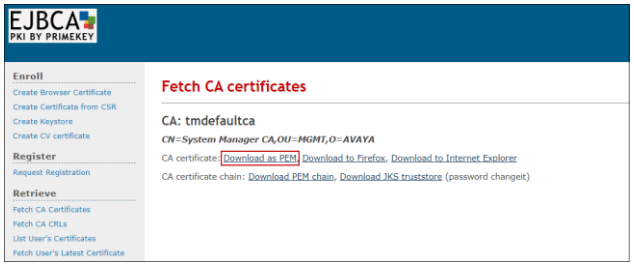
Note: The installation of the "Inside" identity certificate follows the same procedure, but uses the key generated for the inside cert instead.

17.4. Install System Manager CA Root Certificate

From the System Manager **Home** page, navigate to **Services → Security → Certificates → Authority**. Select **Public Web** (not shown). Select **Fetch CA Certificates**.



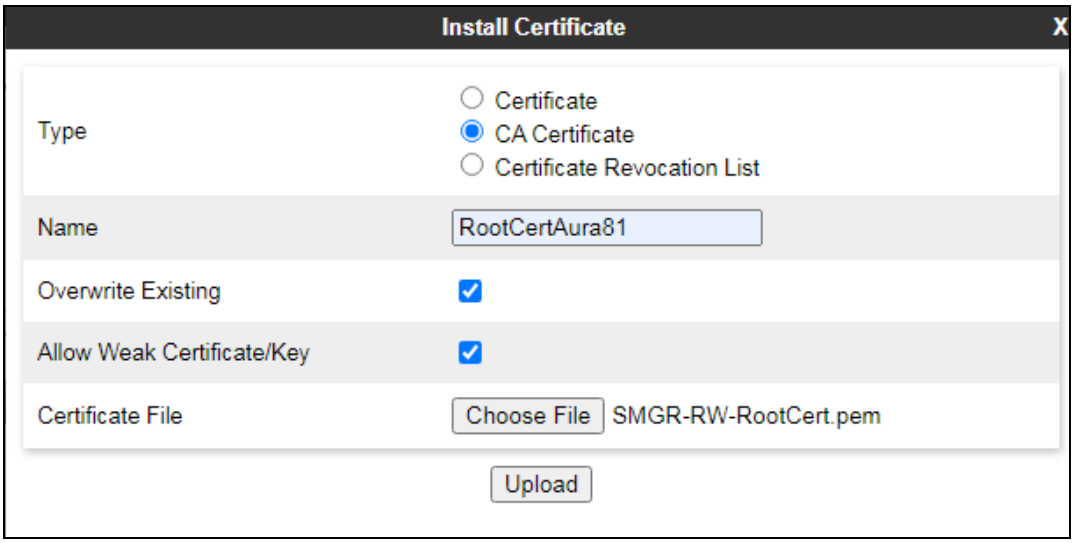
Click **Download as PEM**.



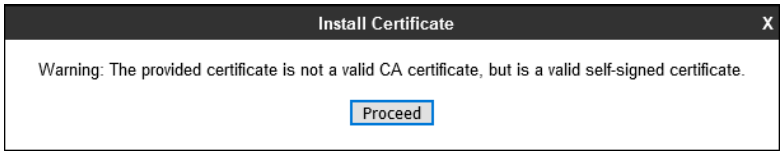
Save the .pem file to the local PC, e.g., **SystemManagerCA.pem** in the reference configuration.

On the Avaya SBCE web interface, navigate to **TLS Management → Certificates** and click the **Install** button (not shown). In the **Install Certificate** screen select the following:

- **Type**: **CA Certificate**.
- **Name**: enter a descriptive name, e.g., **RootCertAura81**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- Click **Browse** to select the System Manager CA certificate previously downloaded, in this case **SMGR-RW-RootCert.pem**.
- Click **Upload**.



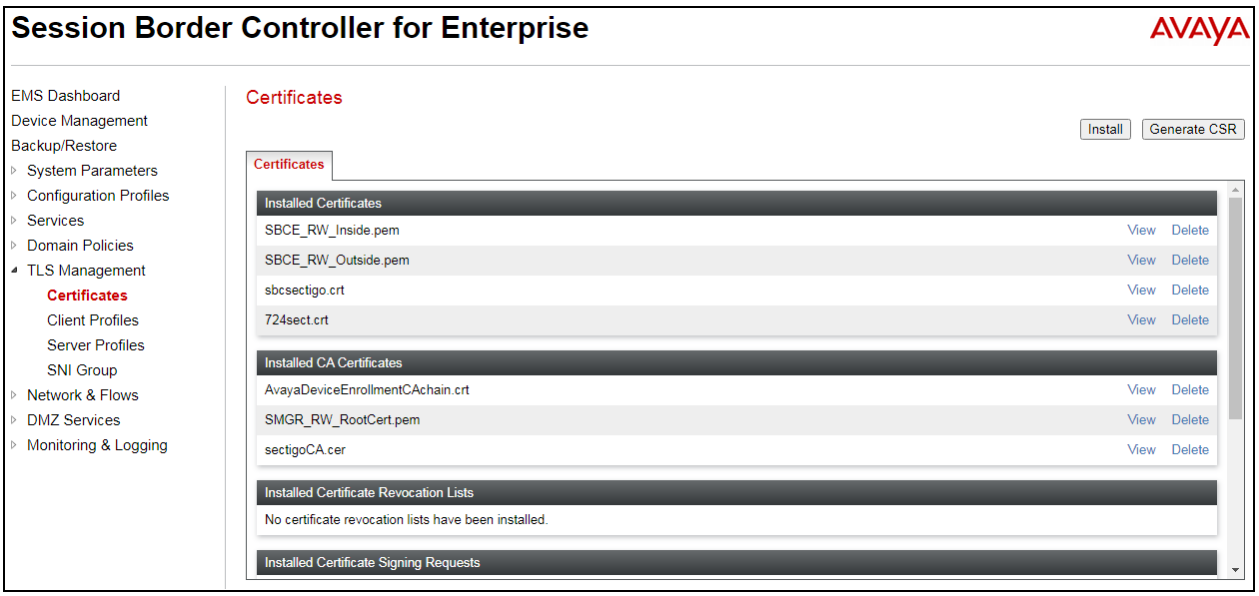
Select **Proceed** on the next screen.



Select **Install**.

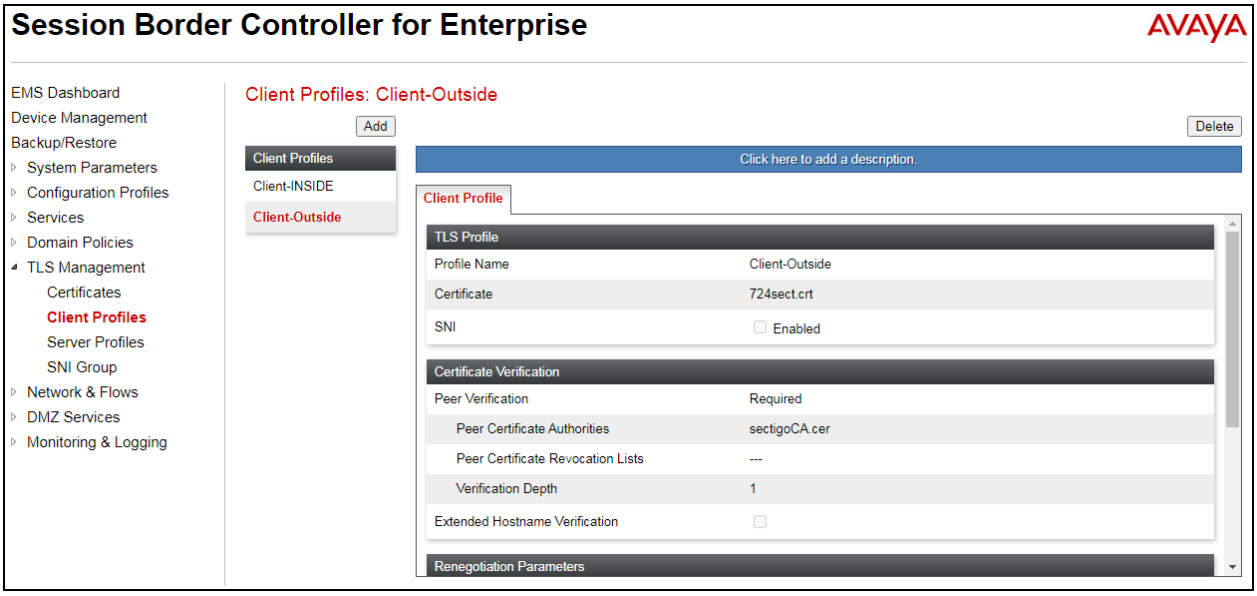
On the Avaya SBCE web interface, select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- System Manager CA signed identity certificates are present in the **Installed Certificates** area.
- System Manager CA certificate is present in the **Installed CA Certificates** area.



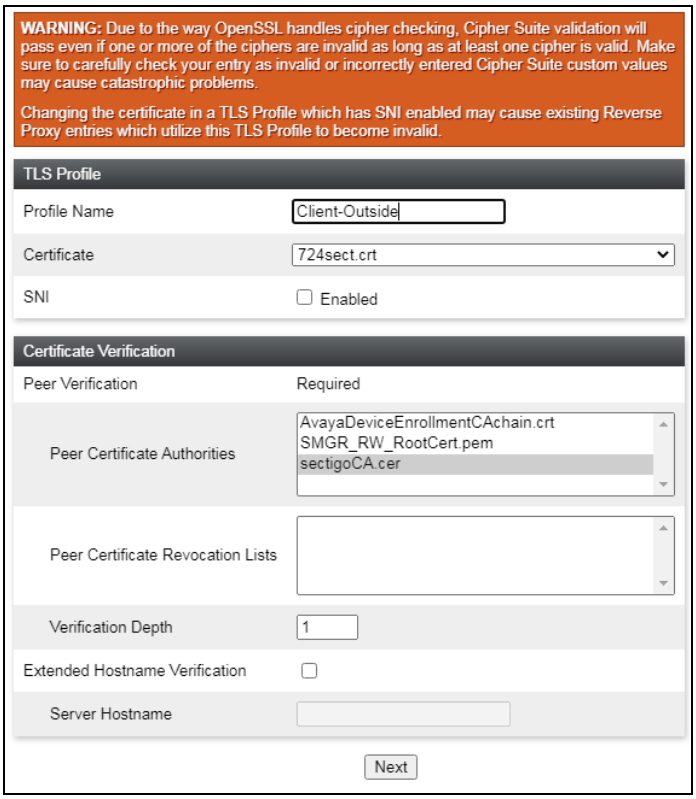
17.5. Configure Avaya SBCE TLS Client Profiles

The screen below shows the two Client Profiles that were used during compliance testing with Net Iletisim, the **Client Profile** highlighted below shows the identity cert (**724sect.crt**) used by Net Iletisim for the SCC handsets. This identity cert was created using a CSR from the SBCE but signed by a third-party certificate authority used by Net Iletisim. The inside profiles use the identity certificates signed by the local System Manager acting as a certificate authority.

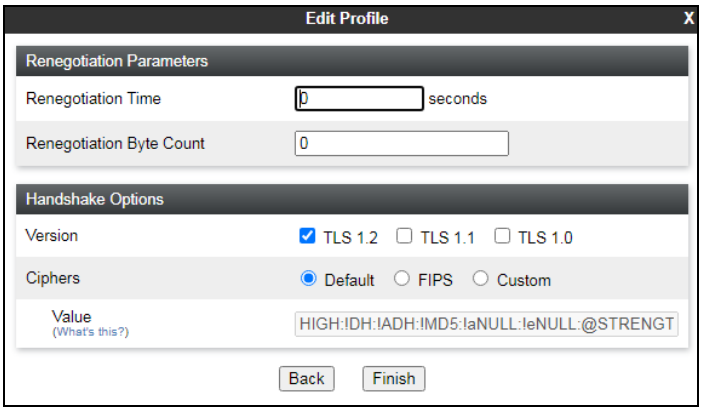


To add a new certificate, select **TLS Management → Client Profiles** from the left-hand menu to add the Avaya SBCE TLS Client Profiles. Click **Add** (shown above).

- **Profile Name:** enter descriptive name, e.g., **Client-Outside**.
- **Certificate:** select the identity certificate, e.g., **724sect.crt**, from pull down menu.
- **Peer Verification** is always required for TLS Client Profiles, so it is set to **Required** by default. Under **Peer Certificate Authorities** select the CA certificate installed previously, (for this example the third-party root certificate from Net iletisim was installed).
- Set **Verification Depth** to **1**.
- Click **Next**.

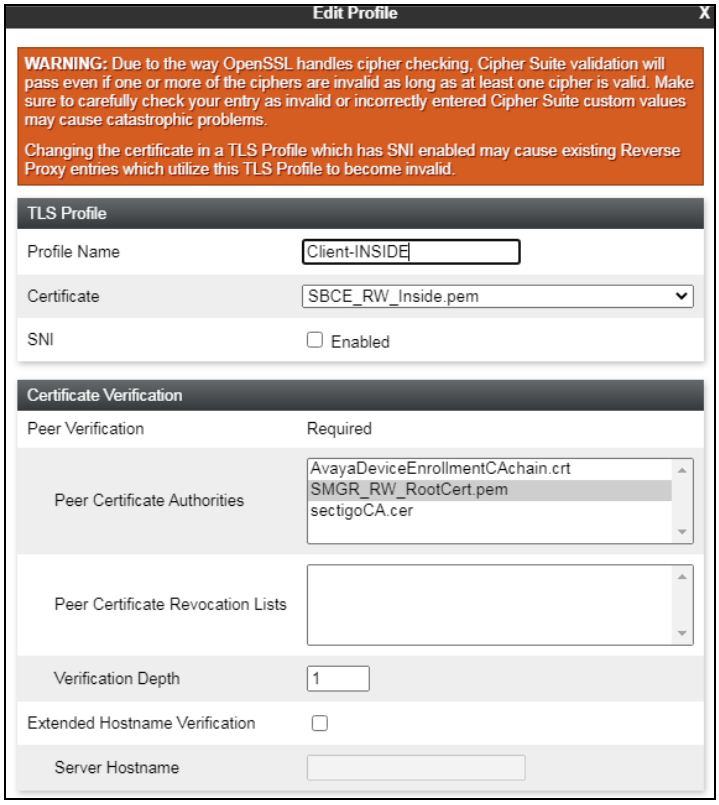


Accept default values for the next screen and click **Finish** (not shown).

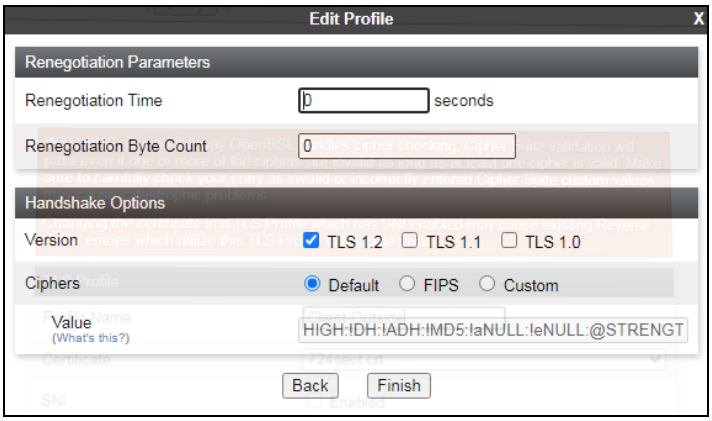


Back at the **Client Profiles** screen, select **Add** one more time and enter the following:

- **Profile Name:** enter descriptive name, e.g., **Client-INSIDE**.
- **Certificate:** select the identity certificate, e.g., **SBCE_RW_Inside.pem**.
- **Peer Verification** is set to **Required** by default. Under **Peer Certificate Authorities** select the CA certificate installed previously, e.g., **SMGR_RW_RootCert.pem**. Set **Verification Depth** to **1**.
- Click **Next**.

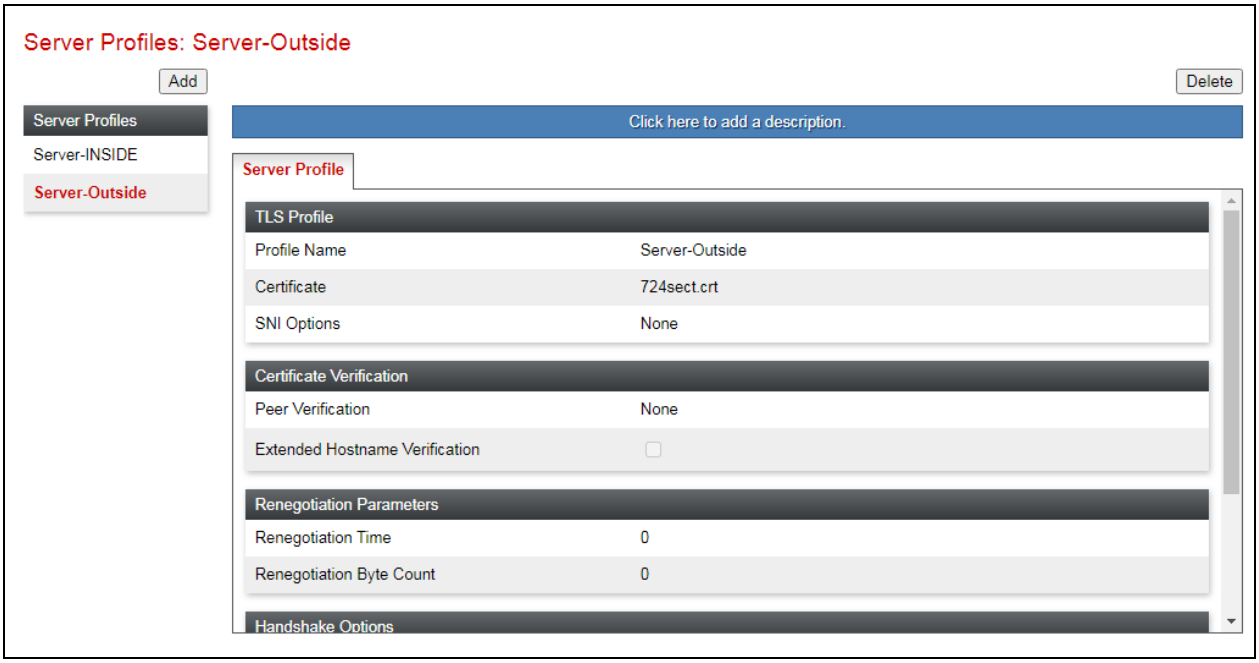


Accept default values for the next screen and click **Finish** (not shown).



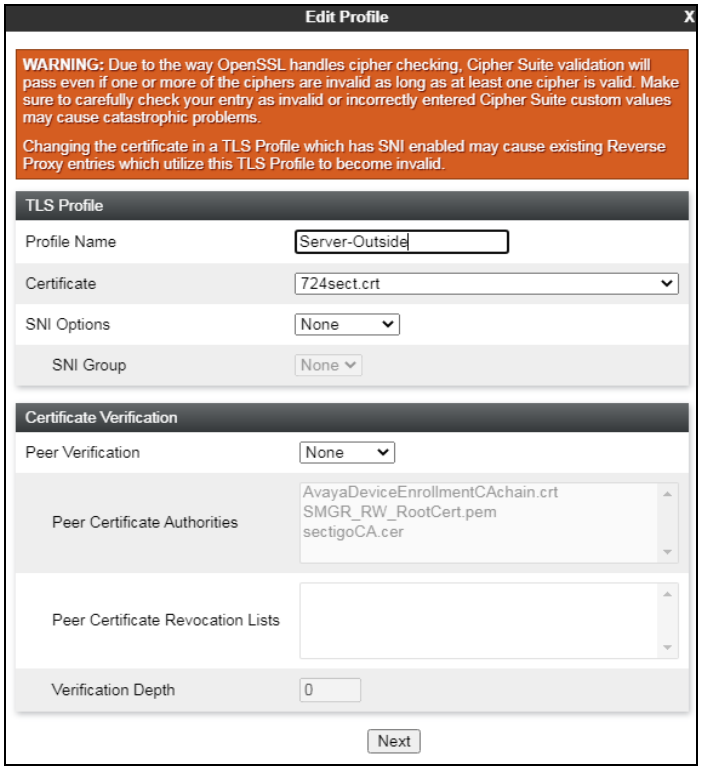
17.6. Configure Avaya SBCE TLS Server Profiles

The screen below shows the two Server Profiles that were used during compliance testing with Net Iletisim, the **Server Profile** highlighted below shows the identity cert (**724sect.crt**) used by Net Iletisim for the SCC handsets. This identity cert was created using a CSR from the SBCE but signed by a third-party certificate authority used by Net Iletisim. The inside profiles use the identity certificates signed by the local System Manager acting as a certificate authority



To add a new identity cert, select **TLS Management → Server Profiles** from the left-hand menu and click **Add** (shown above).

- **Profile Name:** enter descriptive name, e.g., **Server-Outisde**.
- **Certificate:** select the identity certificate, e.g., **734sect.crt**, from the menu.
- **Peer Verification:** Set to **None**, (see note below).



- Click **Next**. Accept default values for the next screen and click **Finish** (not shown).

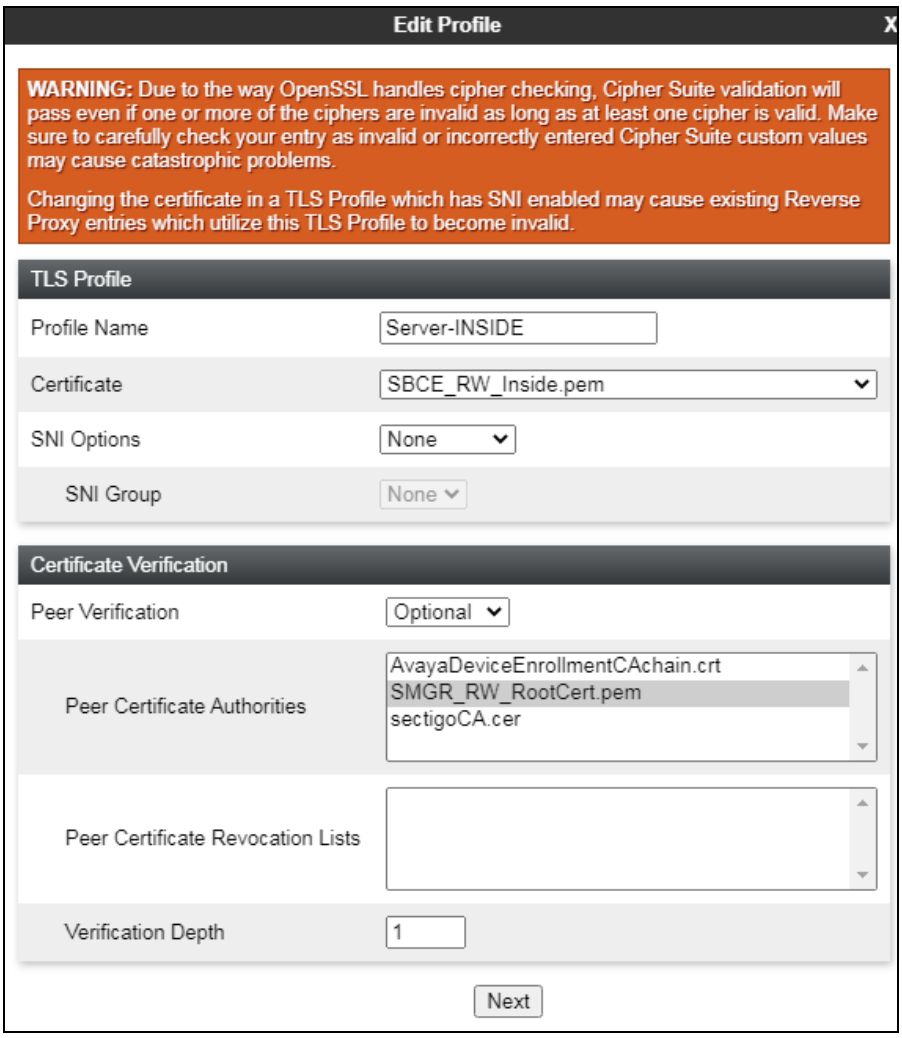
Note: The Avaya SBCE can be configured to support TLS Mutual Authentication, for an additional layer of security. To enable Mutual Authentication for the remote workers, set **Peer Verification** to **Required**, select the CA certificate, e.g., **SMGR_RW_RootCert.pem** under **Peer Certificate Authorities**, and set **Verification Depth** to **1**, as shown below. Otherwise, if Mutual Authentication is not to be used, leave **Peer Verification** set as **None**.

Note: In TLS Server (one-way) Authentication, SIP endpoints need to have a copy of the trusted root CA certificate, downloaded from the enterprise file server during the booting process, to be able to validate the certificate presented by the server. With TLS Mutual Authentication, SIP endpoints are additionally required to present to the server its own unique identity certificate, issued by the Certification or Registration Authority. Avaya endpoints can be configured to use Simple Certificate Enrollment Protocol (SCEP) to obtain an identity certificate from the Certificate Authority. In the test environment used in the reference configuration, Mutual Authentication was initially disabled to allow the endpoints to retrieve their identity certificates via SCEP. Mutual Authentication was re-enabled once the identity certificates were downloaded.

Note: The endpoints configuration and process to obtain identity certificates from a Certification or Registration Authority, using SCEP or by other "in-band" or "out-of-band" methods, is not covered in these Application Notes. For information about configuring the endpoint to obtain identity certificates, consult the endpoint specific documentation.

Back at the **Server Profiles** screen, select **Add** one more time and enter the following:

- **Profile Name:** enter descriptive name, e.g., **Server-INSIDE**.
- **Certificate:** select the identity certificate, e.g., **SBCE_RW_Inside.pem**, from the menu.
- **Peer Verification**: **Optional**.
- **Peer Verification Authorities**: Select the System Manager root certificate installed earlier, in this instance **SMGR_RW_RootCert.pem**.
- Click **Next**.



- Accept default values for the next screen and click **Finish** (not shown).

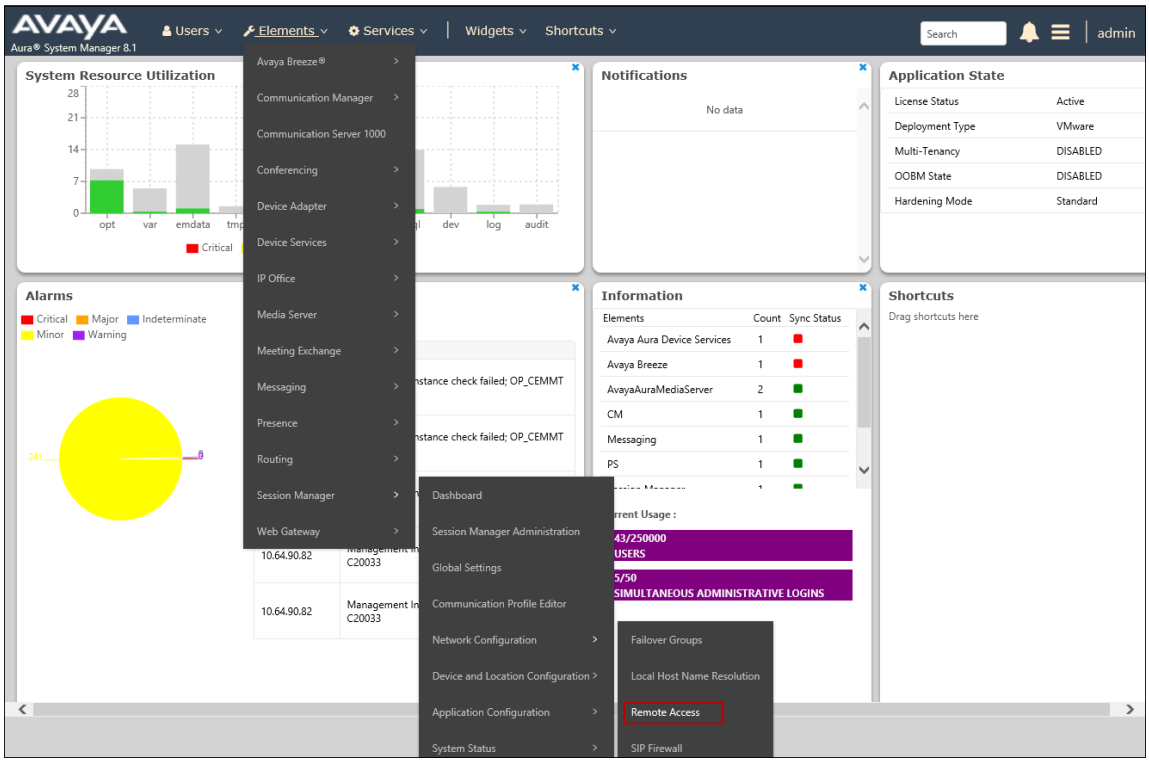
18. Session Manager Configuration for the Support of Remote Workers

This section describes the required configuration of Session Manager for the support of Remote Workers using the Avaya SBCE.

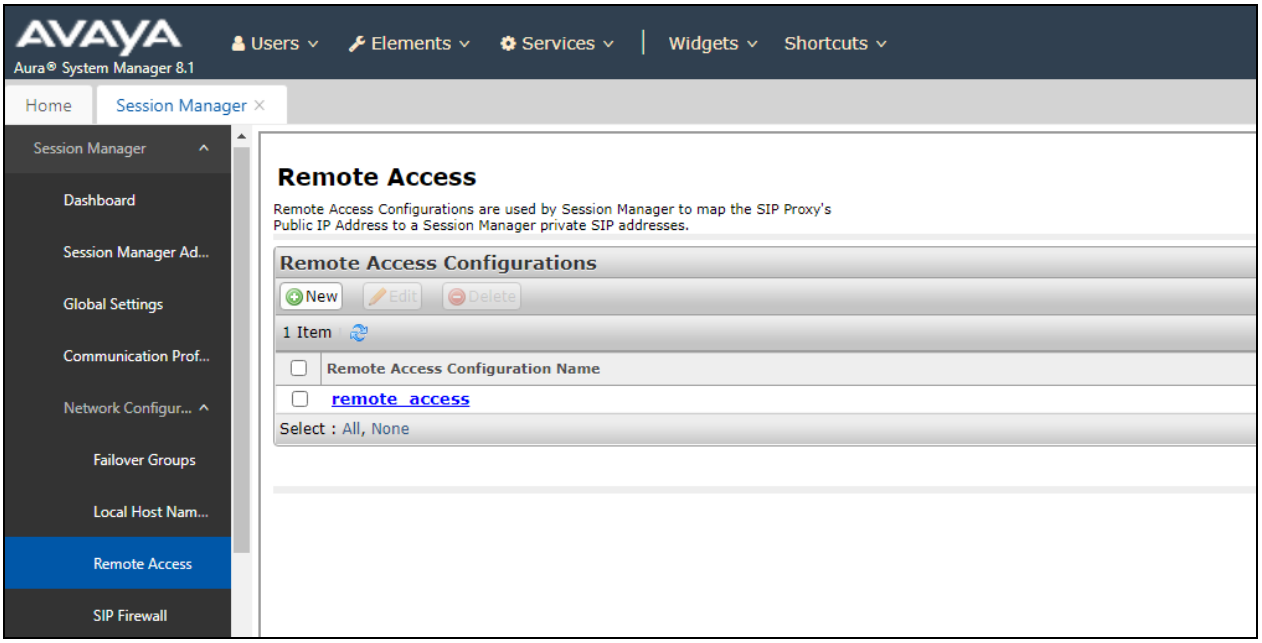
18.1. Remote Access Configuration

Remote Access Configurations are used by Session Manager to map a SIP Proxy's Public IP Address to a Session Manager private SIP addresses.

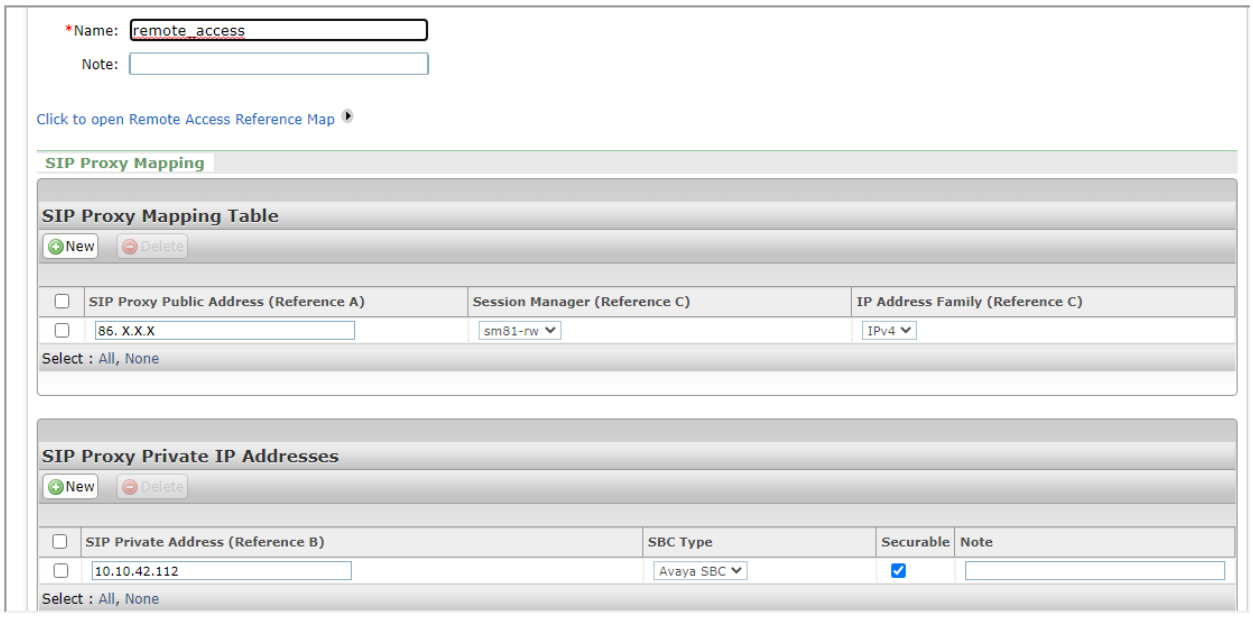
In the System Manager **Home** page, navigate to **Elements → Session Manager → Network Configuration → Remote Access**.



On the **Remote Access Configuration** screen, click **New**. The screen below shows the existing configuration used for compliance testing.



Enter a descriptive name, e.g., **remote_access**. On the **SIP Proxy Mapping Table** section, select **New** and enter the Avaya SBCE public IP address used for remote workers, e.g., **86.x.x.x**. Under **Session Manager (Reference C)** select the Session Manager instance being used. In the reference configuration a single Session Manager instance is used, and it is already selected. On the **SIP Proxy Private IP Addresses** section, select **New** and enter the Avaya SBCE private IP address used for remote workers, e.g., **10.10.42.112**. Click **Add**.

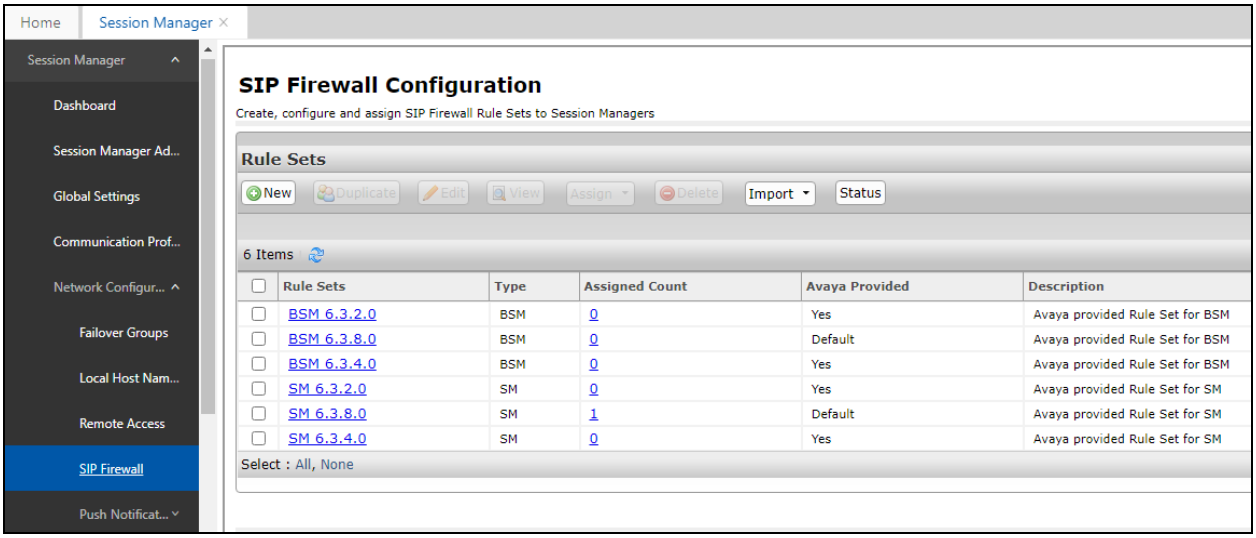


18.2. SIP Firewall Configuration

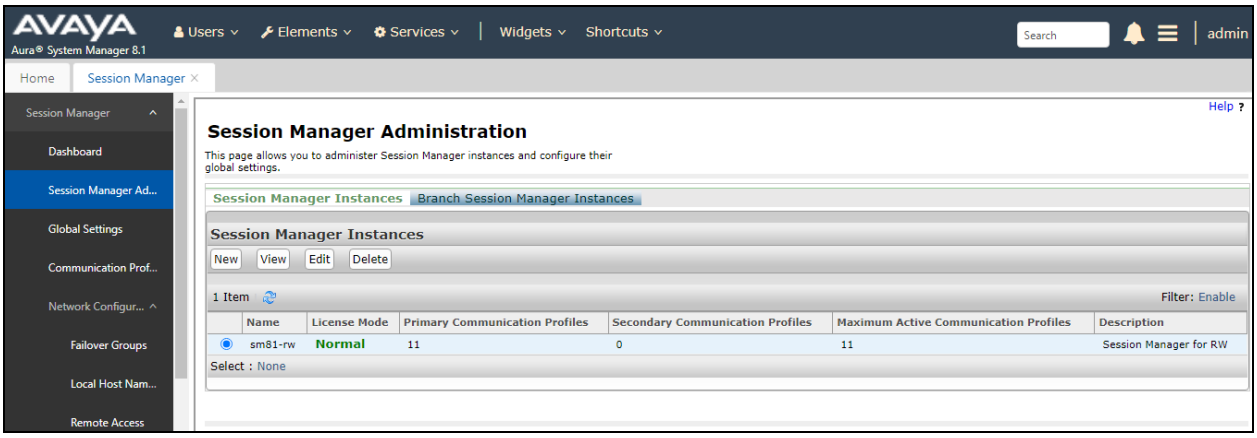
The SIP Firewall controls the flow of SIP traffic into Session Manager, based on configured rule sets. Due to the possible high volume of Remote Worker associated traffic arriving to Session Manager from the IP address of Avaya SBCE inside interface, the Session Manager firewall may tag the traffic as suspicious and may block it. To avoid this issue, it is recommended to configure a SIP Firewall rule to whitelist the IP address of the Avaya SBCE internal interface on the Session Manager SIP firewall.

In the System Manager **Home** page, navigate to **Elements → Session Manager → Network Configuration → SIP Firewall** (not shown).

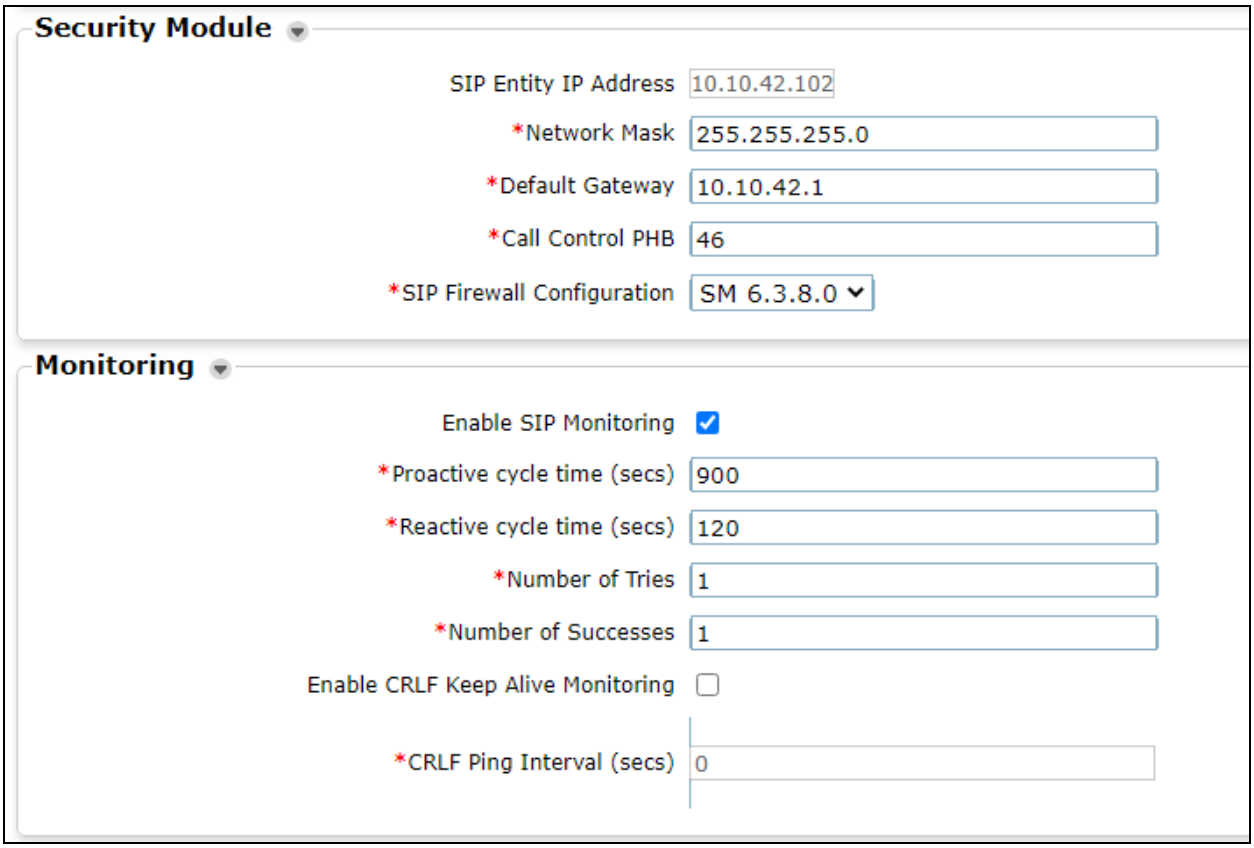
On the **SIP Firewall Configuration** page, the right side of the screen shows the existing defaults or previously added rules under **Rule Sets**. If a new rule needs to be created, consult **4** on the **Additional References** section for more information. For compliance testing no new Firewall was created, **SM 6.3.8.0** was assigned to Session Manager as the Firewall in use.



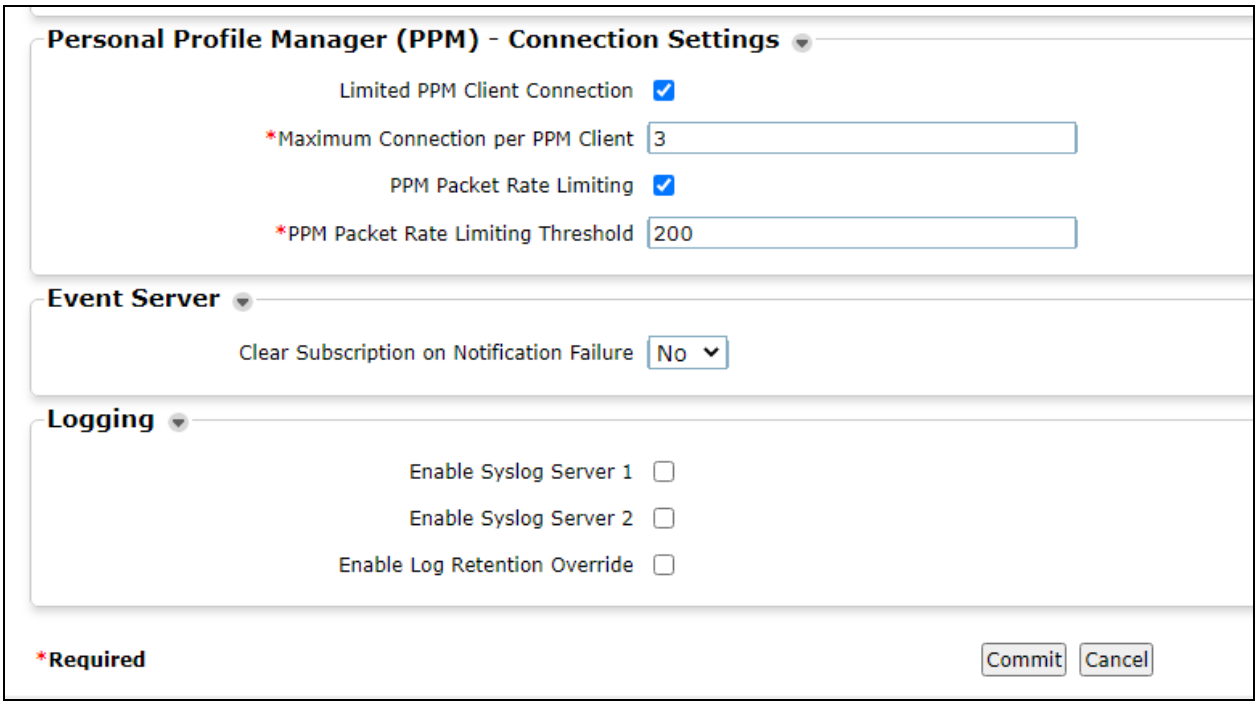
To verify the current SIP Firewall rule used by Session Manager, or to assign a new rule, navigate to **Elements → Session Manager Administration** from the System Manager **Home** page. On the **Session Manager Administration** screen, select the Session Manager instance and click **Edit**.



Under the **Security Module** section, the **SIP Firewall Configuration** field shows the **SM 6.3.8.0 Firewall** rule set in use.



Scrolling further down, the **PPM Connection Settings** are observed.



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.