Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform – Issue 1.0

Abstract

These Application Notes describe the procedures necessary to support Remote Workers using Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform.

The reference Avaya Aura® Platform consists of Avaya Aura® Communication Manager, Avaya Aura® System Manager and Avaya Aura® Session Manager. The SIP endpoints used as Remote Workers included Avaya Workplace Client for Windows, Avaya Agent for Desktop, Avaya J100 and Avaya 96x1 Series IP Deskphones.

Testing was performed to verify SIP registration and basic functionalities in audio calls for the remote endpoints. Calls were placed to and from the Remote Workers residing outside of the enterprise, across the public internet, to various Avaya endpoints located at the enterprise.

These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning steps described in this document. Testing of additional supported Remote Worker SIP endpoints, not listed under these Application Notes, is outside the scope of this document.

Readers should pay attention to **Section 2** in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Table of Contents

1. Introduction

These Application Notes describe the procedures necessary to support Remote Workers using Avaya Session Border Controller for Enterprise 10.1 (Avaya SBCE) on the Avaya Aura® Platform.

A Remote Worker is a SIP endpoint that resides in the untrusted network, registered to Session Manager at the enterprise via the Avaya SBCE. Remote Workers offer the same functionality as any other endpoint at the enterprise. The SIP endpoints used as Remote Workers included Avaya Workplace Client for Windows, Avaya Agent for Desktop, Avaya J169 and Avaya 96x1 Series IP Deskphones.

The Avaya Aura® SIP reference architecture consists of Avaya Aura® Communication Manager, (Communication Manager), Avaya Aura® System Manager (System Manager) and Avaya Aura® Session Manager (Session Manager). Communication Manager is configured as an evolution server and acts as the telephony application server for Session Manager. The role of Session Manager in the reference architecture is to act as a Registrar for Avaya SIP endpoints and provide a centralized dial-plan for least-cost and time-of-day based routing. System Manager provides a web-based interface for the provisioning and maintenance of the solution. System Manager includes EJBCA, an open source PKI Certificate Authority (CA), that can be used to issue and manage client and server certificates.

The Avaya SBCE functioned as the enterprise edge device providing protection against any external SIP-based attacks. The Avaya SBCE acts as a proxy, passing SIP signaling and related media messages that it receives from the endpoints, via the public/outside interface, to Session Manager via its private/inside interface. For secure communication over the public Internet, the public side of the Avaya SBCE facing the remote endpoints should be configured to use the recommended values of Transport Layer Security (TLS) for Signaling, and Secure Real-time Transport Protocol (SRTP) for media encryption. In the configuration depicted in these Application Notes, TLS is used for signaling and SRTP is used for media encryption on both the enterprise network and also to the Remote Workers across the public Internet. HTTPS protocol was used for Remote Workers access to a Utility file server located at the enterprise for file downloads.

For TLS protocol usage, Avaya recommends using unique digital identity certificates, signed by a trusted Certificate Authority (CA). **Section 5** in these Application Notes describe the process of creating identity certificates for the Avaya SBCE, signed by the System Manager CA, needed to support the Remote Workers to connect securely to the enterprise network across the public Internet.

TLS sessions use a client-server model. When the clients (i.e., remote users) contact a server (i.e., Avaya SBCE) they are offered an identity certificate as proof of the server's integrity. Clients verify the offered certificate by testing authenticity against a common trusted root CA certificate. This is known as one-way authentication. To provide an increased level of security, TLS protocol allows the option for servers to additionally request an identity certificate from the

client and authenticate it using a trusted root CA certificate. This method is known as mutual authentication. The configuration steps required on the Avaya SBCE to support both the one-way and mutual authentication methods are covered in these Application Notes.

Note: The process to obtain identity certificates from a Certification or Registration Authority for the remote users is not covered in this document. For information about configuring the endpoint to obtain identity certificates, consult the endpoint specific documentation.

2. General Test Approach and Test Results

A simulated enterprise site containing Communication Manager, System Manager, Session Manager and the Avaya SBCE was installed at the Avaya Solution and Interoperability Lab. A separate location containing the Remote Workers was configured to connect via the public network to the Avaya SBCE at the simulated enterprise site.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these Application Notes included the enablement of supported encryption capabilities (TLS/SRTP) inside of the enterprise (private network side) and outside of the enterprise (public network side). Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

Note: Testing covered under these Application Notes included the following SIP endpoints at the remote site location: Avaya 96x1 SIP Deskphones, Avaya J169 SIP Deskphones, Avaya Workplace Client for Windows and Avaya Agent for Desktop. Testing of additional supported Remote Worker SIP endpoints not listed in this document is outside the scope of these Application Notes.

This document will highlight system programming relevant to the addition of Remote Workers to an existing Avaya Aura® solution. It is assumed that initial provisioning of Communication Manager, System Manager, Session Manager and the Avaya SBCE is already completed, and it is not discussed here. For detailed configuration information consult the documentation for the relevant system on the **References** section.

Note: The purpose of these Application Notes is to illustrate common provisioning steps that are required on the Avaya SBCE to support Remote Workers on an Avaya Aura® enterprise solution consisting of Communication Manager, System Manager and Session Manager. The settings presented here are based on the reference configuration and are not intended to be prescriptive. Remote Worker integration with SIP Trunking was not part of the reference configuration. Interoperability testing of Remote Worker endpoints with SIP Trunking should be performed separately with each Service Provider.

Note: Although the configuration of the Remote Worker endpoints is beyond the scope of these Application Notes, a sample portion of the 46xxsettings.txt file used by Avaya SIP Deskphones is shown on **Section 8**, to illustrate relevant configuration settings used in the reference configuration.

2.1. Test Coverage

To verify Remote Worker basic functionality, the following areas were tested:

- Remote phones registration to Session Manager via Avaya SBCE. Both TLS one-way and mutual authentication methods were tested.
- Download of Personal Profile Manager (PPM) data using HTTPS, via Reverse Proxy policy on the Avaya SBCE.
- Download of CA root certificate, 46xxsettings file and firmware upgrades to remote deskphones, using HTTPS via Reverse Proxy policy on Avaya SBCE.
- TLS identity certificates download using SCEP, via Application Relay on the Avaya SBCE.
- Avaya Agent for Desktop obtaining license from the System Manager WebLM at the enterprise.
- Inbound and outbound calls to and from Remote Workers to different types of Avaya endpoints located at the enterprise, using TLS for signaling and SRTP for the media.
- Media redirection verification (media un-anchoring) for calls between Remote Workers.
- Avaya Agent for Desktop Remote Worker login to Communication Manager skill, handling of incoming and outgoing calls, changes to different work states, etc.
- Basic call handling features, such as hold, transfer, call forward, and conference were tested.
- Call coverage to Avaya Messaging. Message Waiting Indicator (MWI) activation/ deactivation.
- Voicemail navigation and DTMF transmission using RFC 2833.

2.2. Test Results

Basic Remote Worker functionality was verified successfully with the following observations:

- During testing it was observed that when Mutual Authentication was used between the Avaya SBCE and the Remote Workers, the Avaya Agent for Desktop remote client failed to obtain its license from the WebLM server located at the enterprise. This occurred when the license requests are routed via the Avaya SBCE using a Reverse Proxy policy (**Section 7.17.2**). If Mutual Authentication is enabled between the Avaya SBCE and the Remote Workers (**Section 5.8**), it is recommended to route the licenses requests from the Avaya Agent for Desktop clients directly from the enterprise firewall to the WebLM server, and not through the Avaya SBCE.

2.3. Support

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.

3. Reference Configuration

In the reference configuration, an existing Avaya SBCE already supporting SIP trunking is configured to additionally allow Remote Workers on the public Internet to securely access the private enterprise network, without the need of VPN.

For Remote Workers, Standard and Advanced Session Licenses are required on the Avaya SBCE. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

Figure 1 below illustrates the Remote Worker topology used in the reference configuration.

The Avaya components used to create the simulated enterprise site included:

- Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Aura® Media Server.
- Avaya G430 Media Gateway.
- Avaya Session Border Controller for Enterprise.
- Avaya Messaging.
- Avaya Aura® Utility Services.
- Avaya 96x1-Series IP Deskphones (H.323 and SIP) at the enterprise site.
- Avaya 96x1-Series IP Deskphones (SIP) at the Remote Worker location.
- Avaya J100 Series IP Deskphones (SIP) at the Remote Worker location.
- Avaya Workplace Client for Windows at the Remote Worker location.
- Avaya Agent for Desktop at the Remote Worker location.

Internet access for the Remote Workers is achieved by a Router/NAT/Firewall, located at the remote site between the Remote Worker private network and the public Internet. The router also provides DHCP service to the SIP endpoints.

Note – These Application Notes describe the provisioning used for the sample configuration shown in **Figure 1**. Other configurations may require modifications to the provisioning described in this document. Only tasks related to the addition of the Remote Workers to the solution are described in this document. It is assumed that initial provisioning of Communication Manager, System Manager, Session Manager and the Avaya SBCE is already completed, and it is not discussed here.

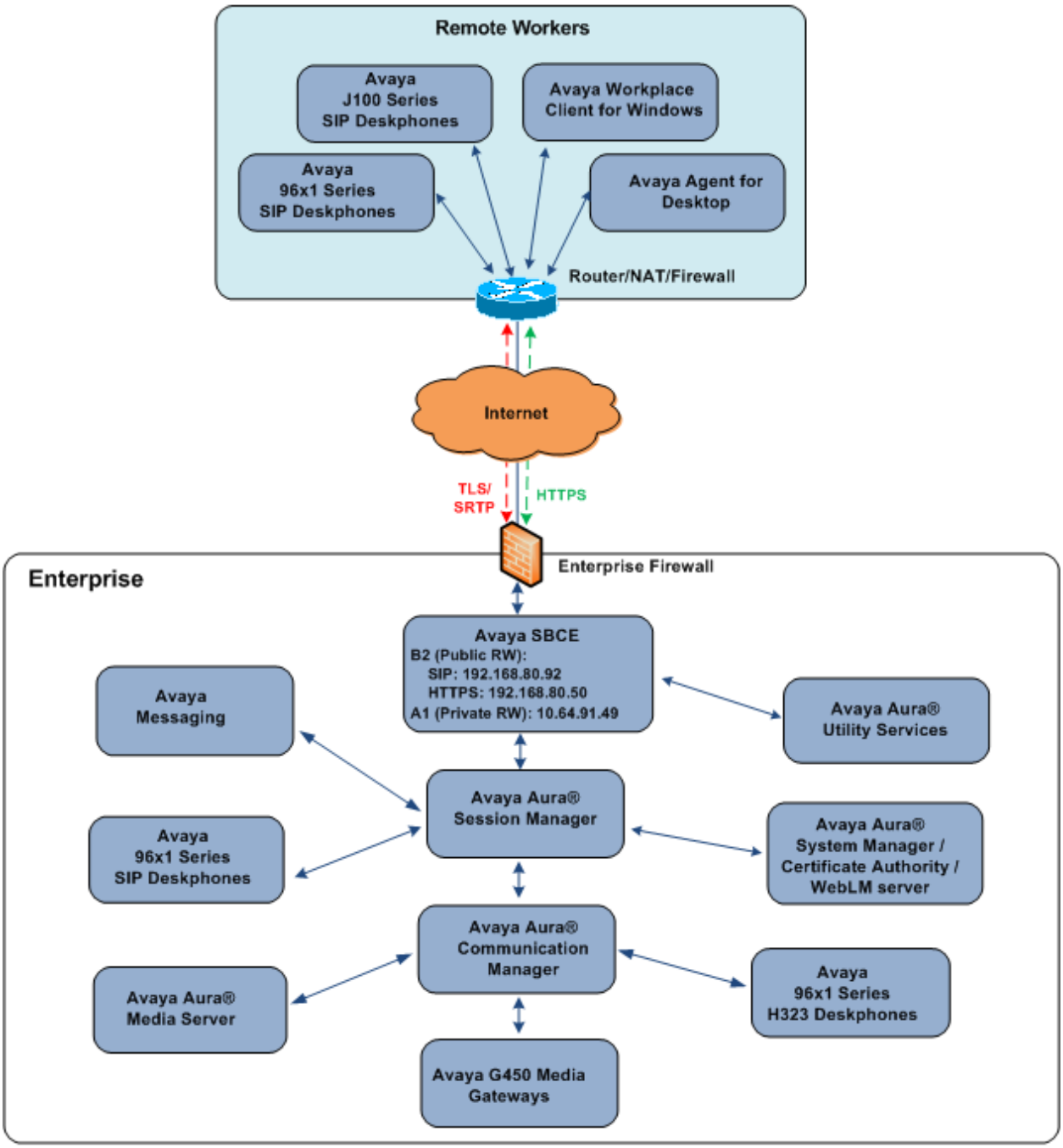


Figure 1: Remote Worker topology used in the reference configuration

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes and are for illustrative purposes only.

Component	Illustrative Value in these Application Notes
Avaya Aura® Session Manager	
IP Address	10.64.91.85
Avaya Aura® System Manager	
IP Address	10.64.90.84
Avaya Session Border Controller for Enterprise (SBCE)	
IP Address of Public Interface B2 (Remote Workers, SIP traffic)	192.168.80.92
IP Address of Public Interface B2 (Remote Workers, file transfer)	192.168.80.50
IP Address of Private Interface A1 (Remote Workers, all traffic)	10.64.91.49
IP Address of Private Interface A1 (SIP Trunking)	10.64.91.48, 10.64.91.50
Avaya Aura® Utility Services	
IP Address	10.64.91.116
Remote Router/NAT	
Public IP Address	172.16.86.34

Table 1: Network Values Used in these Application Notes

Note – For security reasons, public IP addresses used in the reference configuration on the Avaya SBCE are not included in this document. However, as placeholders in the following configuration sections, the IP addresses **192.168.80.92** (Avaya SBCE "Public" interface B2, for Remote Workers SIP traffic), **192.168.80.50** (Avaya SBCE "Public" interface B2, for Remote Workers file transfer) and **172.16.86.34** (Router/NAT at remote location) are specified.

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya Aura® System Manager	10.1.0.1.0614394
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Communication Manager	10.1.0.10-SP1 Update ID 10.1.0.974.0-27372
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya Messaging	10.8 SP1
Avaya Aura® Media Server	10.1.0.77
Avaya G450 Media Gateway	42.4.0
Avaya Aura® Utility Services	7.1.3
Avaya 9608 Series IP Deskphone (H.323)	6.8511
Avaya 9611 Series IP Deskphone (SIP)	7.1.15.0.14
Avaya J169 Series IP Deskphone (SIP)	4.0.12.0.6
Avaya Workplace Client for Windows	3.26.0.64
Avaya Agent for Desktop	2.0.6.20.3004

Table 2: Equipment and Software Used in the Sample Configuration

5. 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:

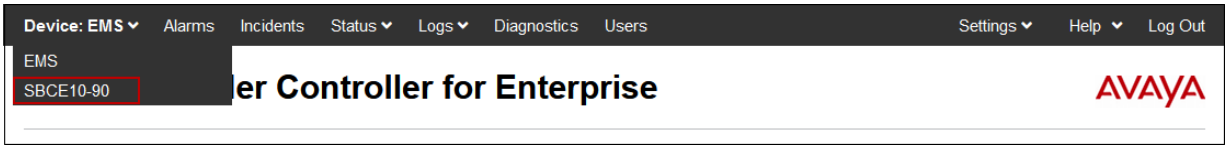
- Network Management
- Create Certificate Signing Requests in Avaya SBCE
- Add End Entities in System Manager
- Create Identity Certificates in System Manager
- Install Identity Certificates issued by the System Manager CA in Avaya SBCE
- Install System Manager CA root certificate in Avaya SBCE
- Create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

5.1. 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.

To access the SBCE configuration menus, select the SBCE device from the top navigation menu.

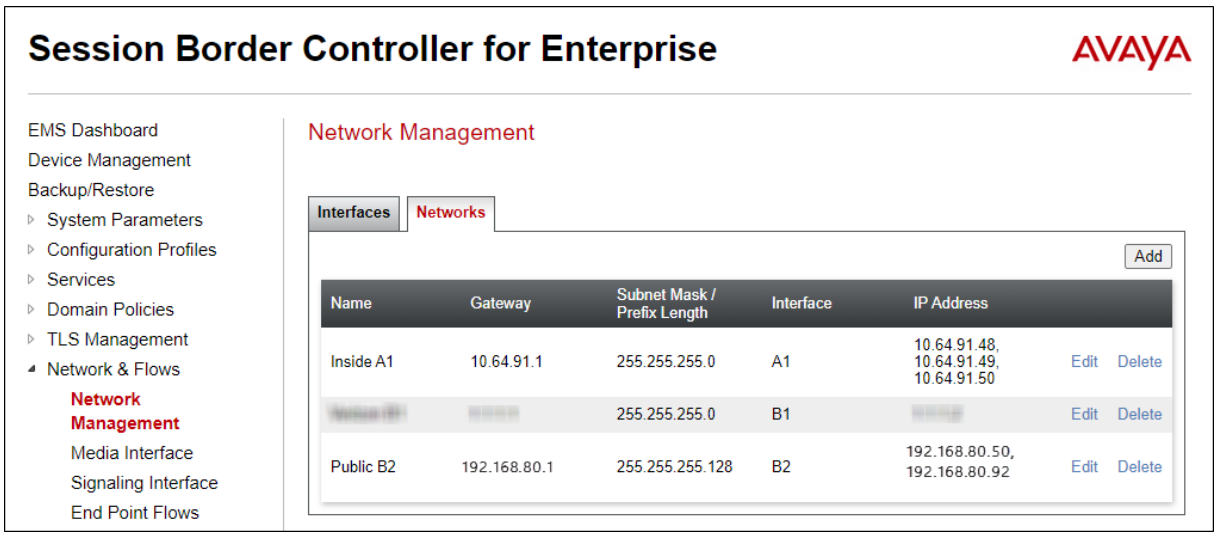


The Network Management screen is where the network interface settings are configured and enabled. During the installation process, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc., to interface the device to the network. It is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

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 **B2**.

Note – For security reasons, public IP addresses used on the Avaya SBCE interface B2 in the reference configuration are masked in this document.



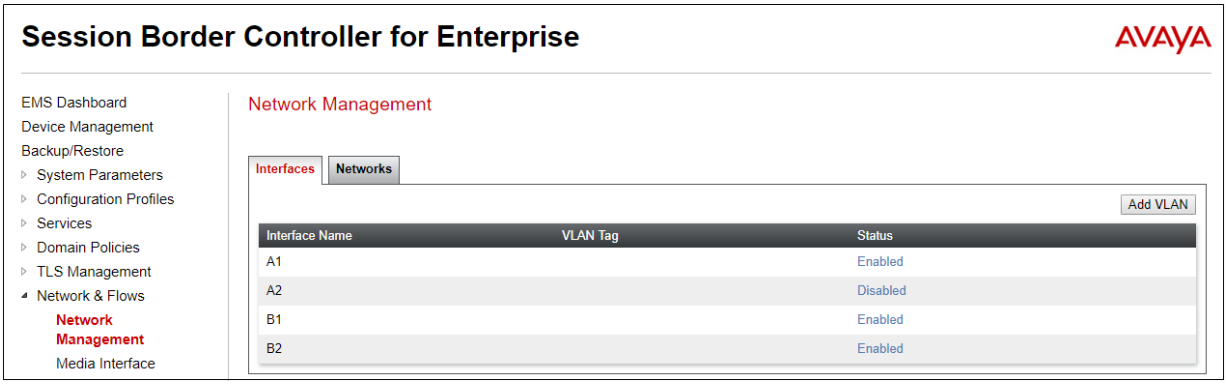
The following are the IP addresses and associated interfaces used in the reference configuration:

- **192.168.80.92**: IP Address of Public Interface B2 (Remote Workers SIP)
- **192.168.80.50**: IP Address of Public Interface B2 (Remote Workers file transfer)
- **10.64.91.49**: IP Address of Private Interface A1 (Remote Workers, all traffic)

Note: the Avaya SBCE used in the reference configuration is deployed on a mixed environment, supporting SIP Trunking in addition to Remote Workers. IP Addresses **10.64.91.48** and **10.64.91.50** on the Private Interface A1 are used for SIP Trunking on the enterprise side and they are not directly related to the Remote Worker configuration. Since these addresses were optionally used in the TLS certificate creation process, they are shown here for completeness.

Interface **B1** is associated to a public IP address used for SIP trunking, and it is not relevant to this Application Notes.

Verify that the interfaces are enabled on the **Interfaces** tab. The following screen shows interfaces **A1** and **B2** with status **Enabled**. To enable an interface, click the corresponding **Disabled** link under the Status column to change it to **Enabled**.

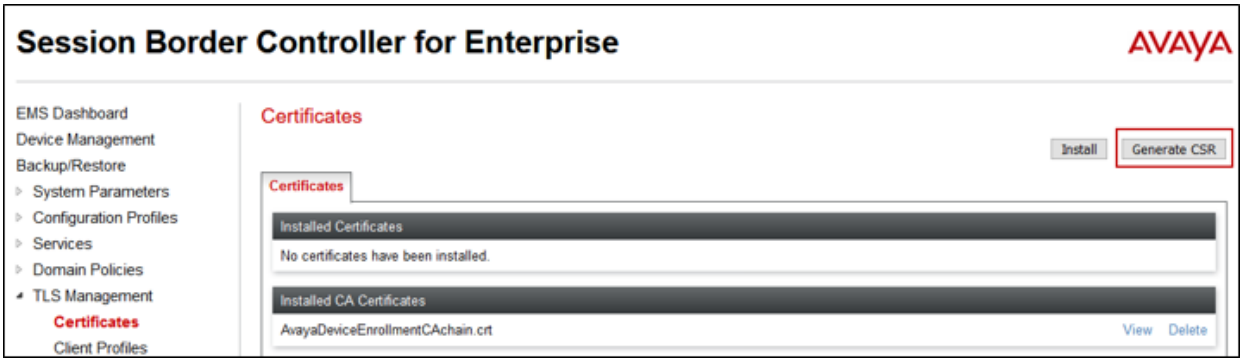


5.2. Create Certificate Signing Requests for Avaya SBCE interfaces

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

5.2.1. Create Certificate Signing Request for the Avaya SBCE External Interface

Navigate to **TLS Management → Certificates** and click the **Generate CSR** button.



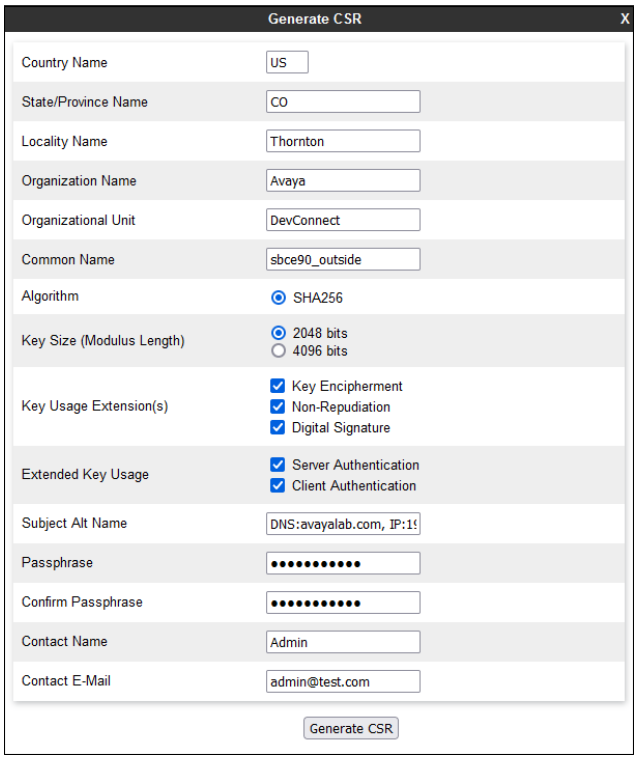
On the **Generate CSR** form that appears, fill the information as required:

- Enter the information on the location and organization fields as appropriate.
- Under **Common Name**, enter a descriptive name, e.g., **sbce90_outside**.
- **Algorithm**: **SHA256**.
- **Key Size**: **2048 bits**.
- **Key Usage Extension(s)** and **Extended Key Usage**: check all options.
- **Subject Alt Name**: using format **DNS:<value>**, **IP:<value>**, enter the SIP domain name used by the remote endpoints (e.g., "avayalab.com"), and the IP addresses of the external interface of the Avaya SBCE used by Remote Workers for HTTPS and for SIP traffic (192.168.80.50 and 192.168.80.92 in the reference configuration), e.g., **DNS:avayalab.com, IP:192.168.80.50, IP:192.168.80.92**.

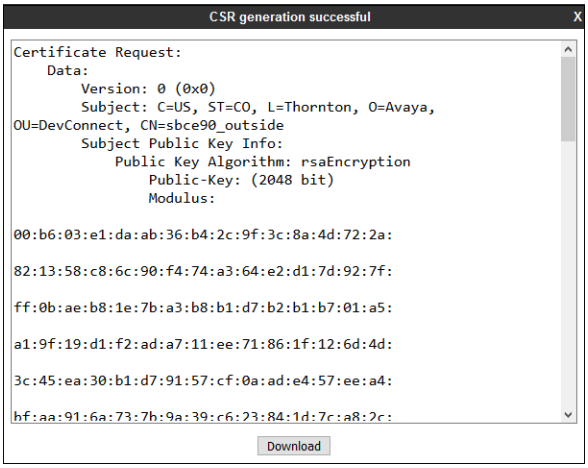
Note: Avaya 96x1 and J100 Deskphones by default will validate the certificate offered by the Avaya SBCE by matching one of the IP addresses included on the **Subject Alt Name** with the physical IP address from where the certificate was received. For SIP over TLS connections the phones will also compare the domain present on the certificate and the SIP domain configured on the phones, received via 46xxsettings file.

- **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 similar to the one below. Click on **Download** to extract the CSR file from the Avaya SBCE. The file name will be <CN>.req, where <CN> is the **Common Name** entered in the Generate CSR form. In the sample configuration, this is "sbce90_outside". The corresponding private key e.g., "sbce90_outside.key" is automatically placed in the key directory of the Avaya SBCE.

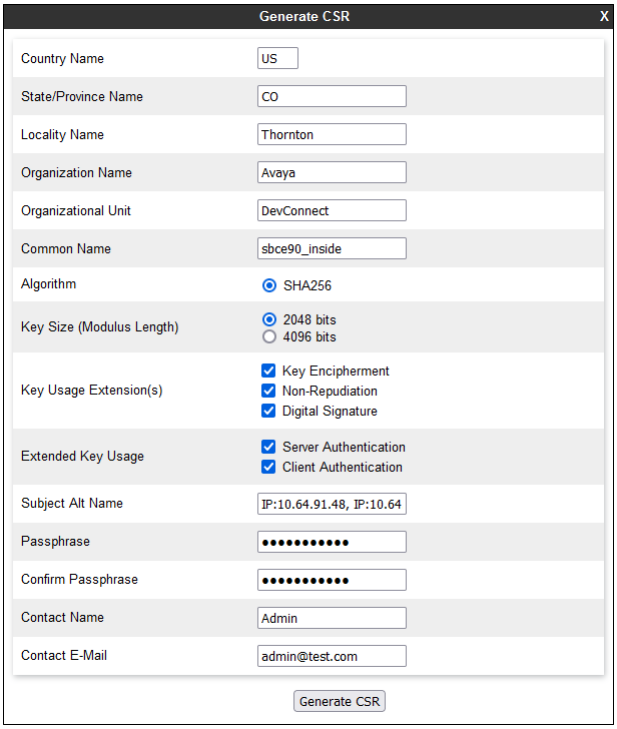


Save the generated CSR file, e.g., **sbce90_outside.req**, to the local PC.

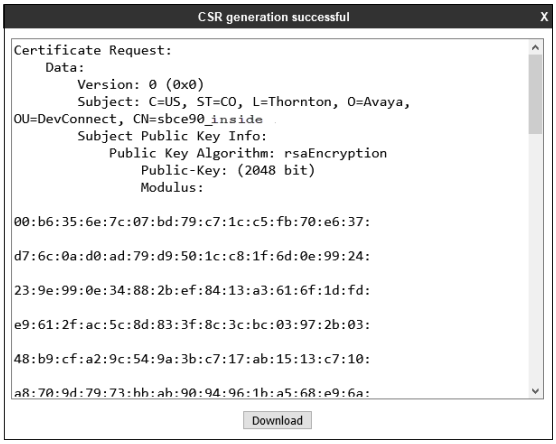
5.2.2. Create Certificate Signing Request for the Avaya SBCE Internal Interface

Repeat the steps described in **Section 5.2.1** with the following changes:

- **Common Name**: enter a descriptive name, e.g., **sbce90_inside**.
- **Subject Alt Name** field, enter the IP addresses of the private interface of the Avaya SBCE, used for SIP trunking (if used) and Remote Workers. In the reference configuration this is **IP:10.64.91.48, IP:10.64.91.49, IP:10.64.91.50**. Note that by including all these IP addresses, a single certificate can be used on the private interface to support both Remote Workers and SIP trunking, if desired.



Click **Download** to save the generated CSR file, e.g., **sbce90_inside.req**, to the local PC.



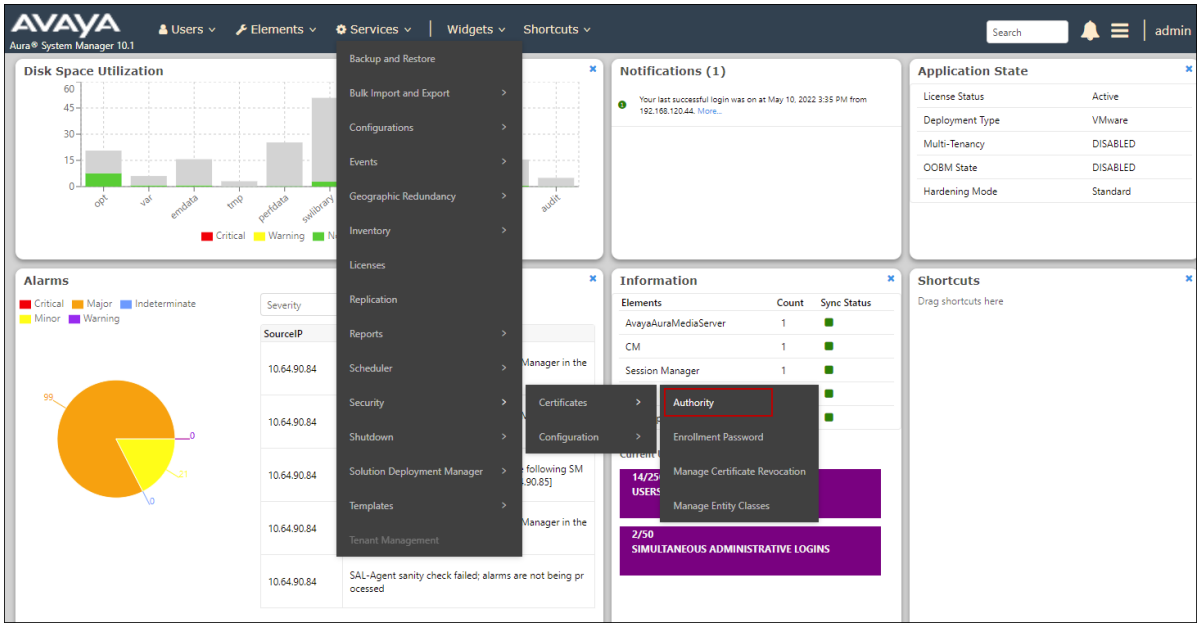
5.3. Add End Entities in System Manager CA

Follow the steps in this section to create the End Entities in the System Manager Certificate Authority web page. These End Entities correspond to the Avaya SBCE external and internal interfaces, and they are required to sign the CSRs created in **Section 5.2**.

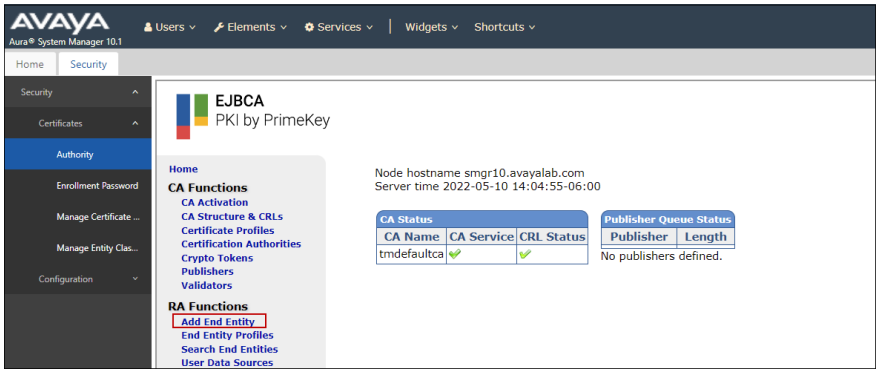
5.3.1. Add End Entity for Avaya SBCE External Interface

Use a browser to connect to the System Manager GUI, using the URL "https://<ip-address> /SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown).

In the System Manager **Home** page, navigate to **Services → Security → Certificates → Authority**.



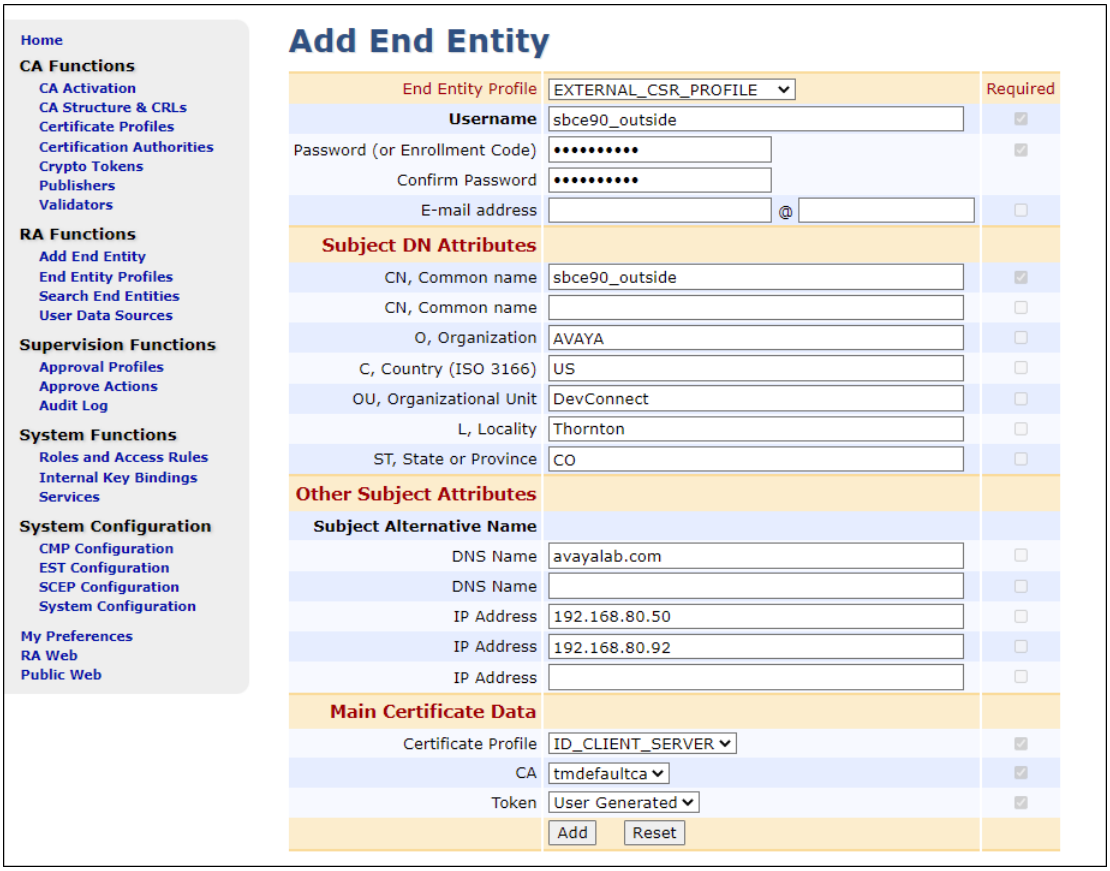
On the **Authority** screen, select **Add End Entity**.



On the **Add End Entity** form, enter the appropriate information as needed:

- **End Entity Profile**: Select **EXTERNAL_CSR_PROFILE** from the scroll down menu.
- Enter a **Username** and **Password (or Enrollment Code)**. Take note of these values, as they will be required later to generate the identity certificate.
- **CN, Common name**: Enter the Common Name entered when creating the CSR in **Section 5.2.1**, e.g. **sbce90_outside**.
- Enter organization and location information as needed.
- Under **Subject Alternative Name**, on the **DNS name** enter the domain used on the remote endpoints, e.g., **avayalab.com**. Under **IP Address** enter the IP addresses of the SBCE external interface used for remote workers, e.g., **192.168.80.50** (HTTPS traffic) and **192.168.80.92** (SIP traffic). See note on **Section 5.2.1**.
- **Certificate Profile**: **ID_CLIENT_SERVER**.
- **CA**: **tmdefaultca**.
- **Token**: **User Generated**.
- Click **Add**.

The following screen illustrate the parameters used in the sample configuration:

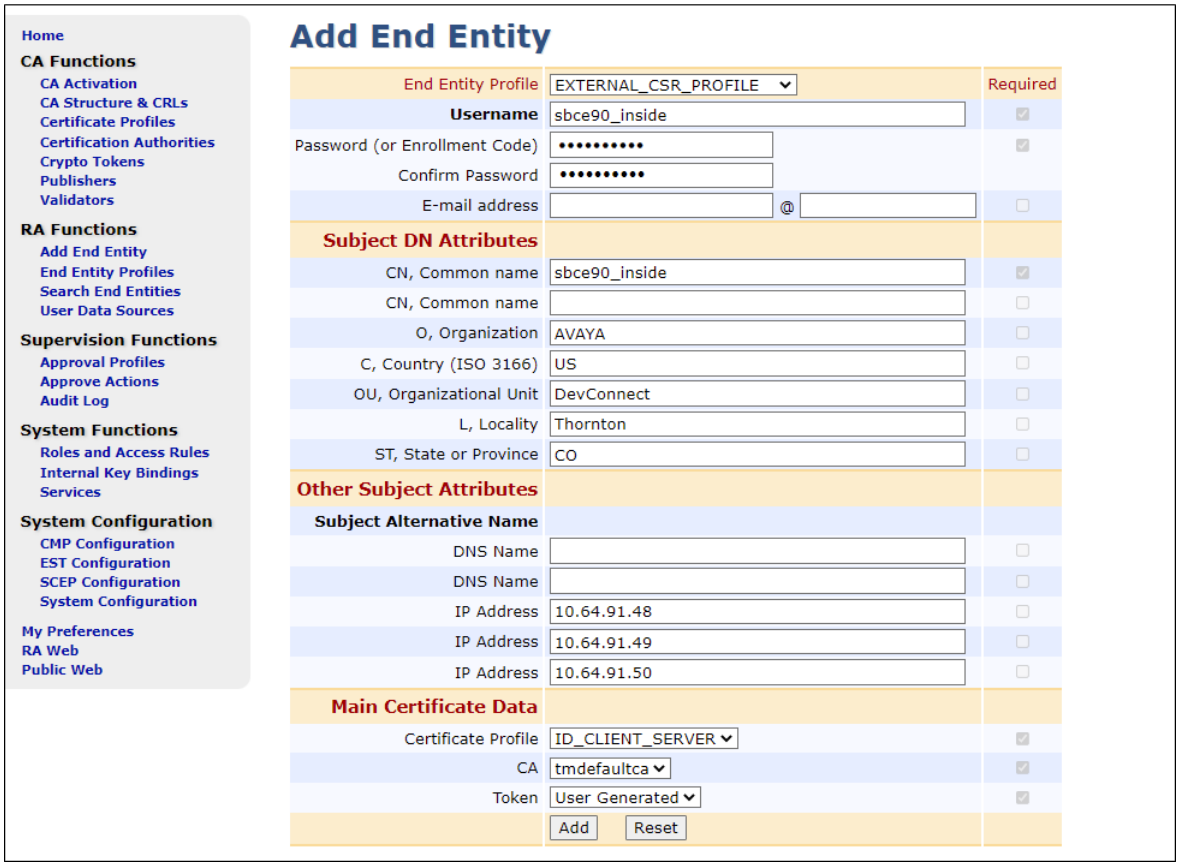


Note: By default, only one **IP Address** field appears under the **Subject Alternative Name**. More **IP Address** fields can be added if needed, by modifying the corresponding End Entity Profile. Select **End Entity Profiles** on the Menu on the left, choose the profile from the list and click **Edit End Entity Profiles** to make the necessary changes if needed (not shown).

5.3.2. Add End Entity for Avaya SBCE Internal Interface

Repeat the steps described in **Section 5.3.1**, with the following changes:

- **CN, Common name**: Enter the Common Name entered when creating the CSR in **Section 5.2.2**, e.g. **sbce90_inside**.
- Under **Subject Alternative Name**, enter all the IP addresses used on the private interface of the Avaya SBCE. In the reference configuration, IP address **10.64.91.49** is used by the Remote Workers, while **10.64.91.48** and **10.64.91.50** are used for SIP trunking, on the private side of the Avaya SBCE.

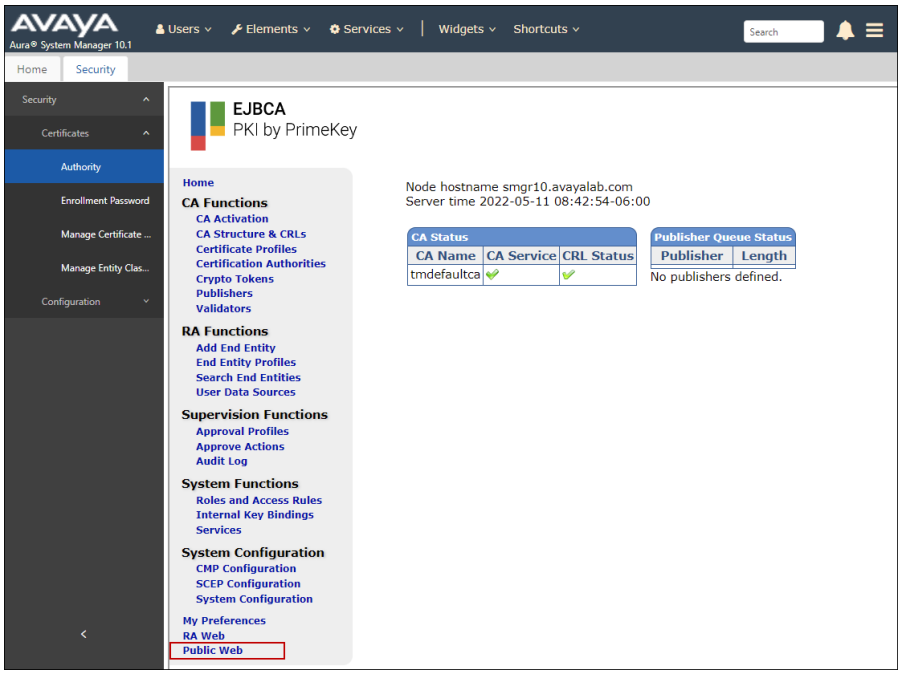


5.4. Create Signed Identity Certificates

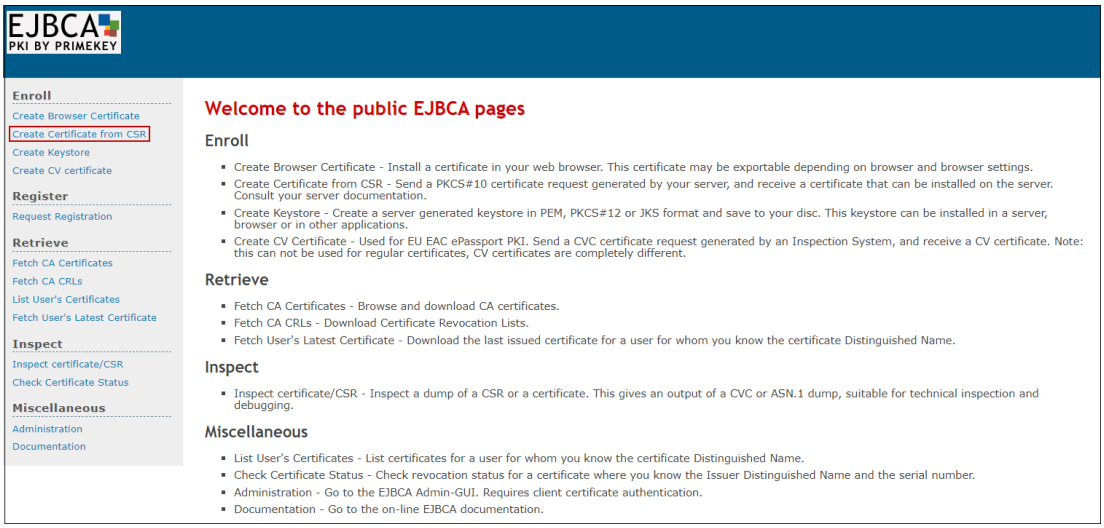
Signed Identity Certificates are generated in the System Manager Certificate Authority, by associating the Certificate Signing Requests (CSRs) created in the Avaya SBCE (**Section 5.2**) and the corresponding End Entities in the System Manager CA (**Section 5.3**).

5.4.1. Create identity Certificate – Avaya SBCE External Interface

From the System Manager **Home** screen, navigate to **Services → Security → Certificates → Authority**. Select **Public Web**.

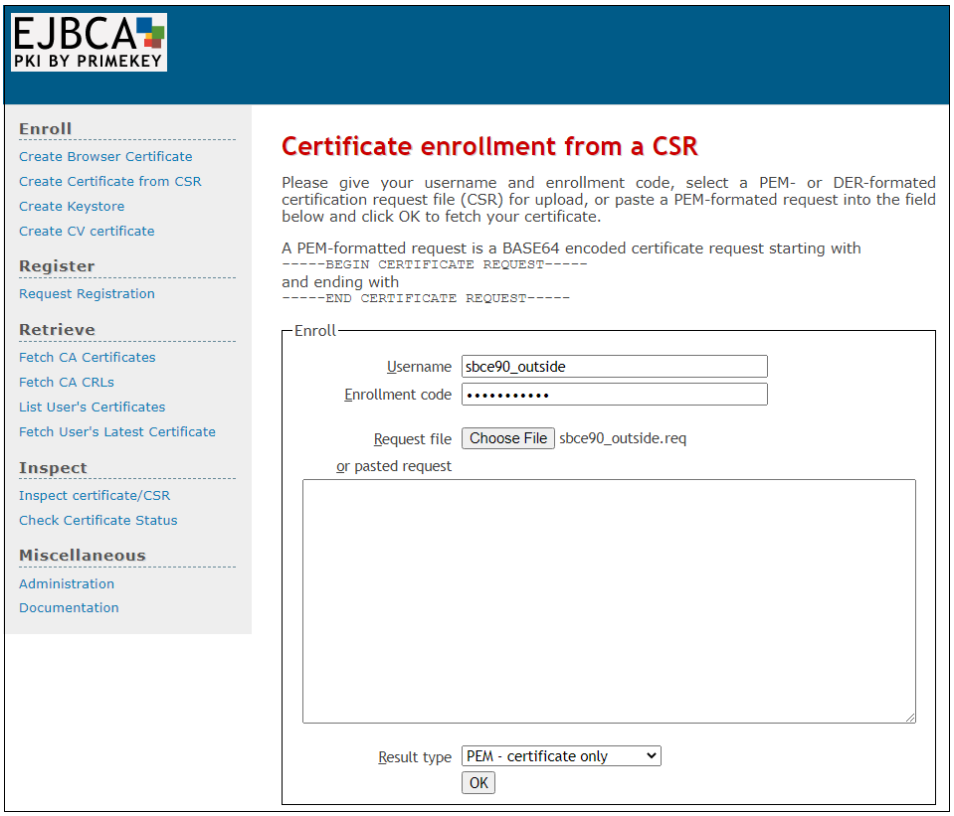


Select **Create Certificate from CSR**.

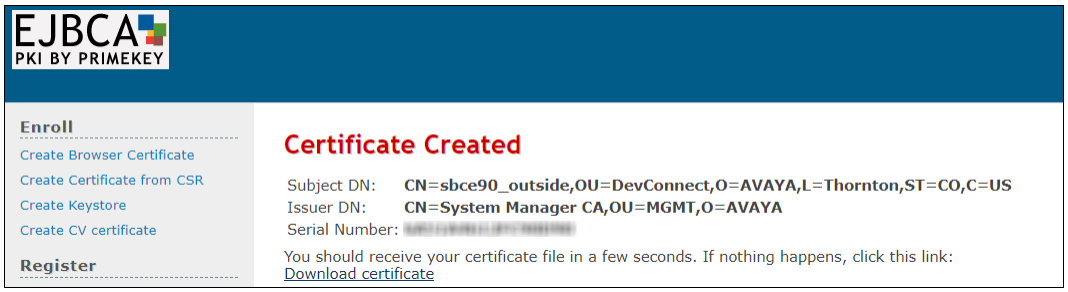


On the **Certificate Enrollment from CSR** page:

- Enter the **Username** and **Enrollment Code** (password) configured on the End Entity corresponding to the SBCE external interface, in **Section 5.3.1**.
- Click **Choose File**. Browse and select the CSR file created in **Section 5.2.1**, e.g., **sbce90_outside.req** on the local PC.
- **Result type**: Select **PEM – certificate only**.
- Click **OK**.



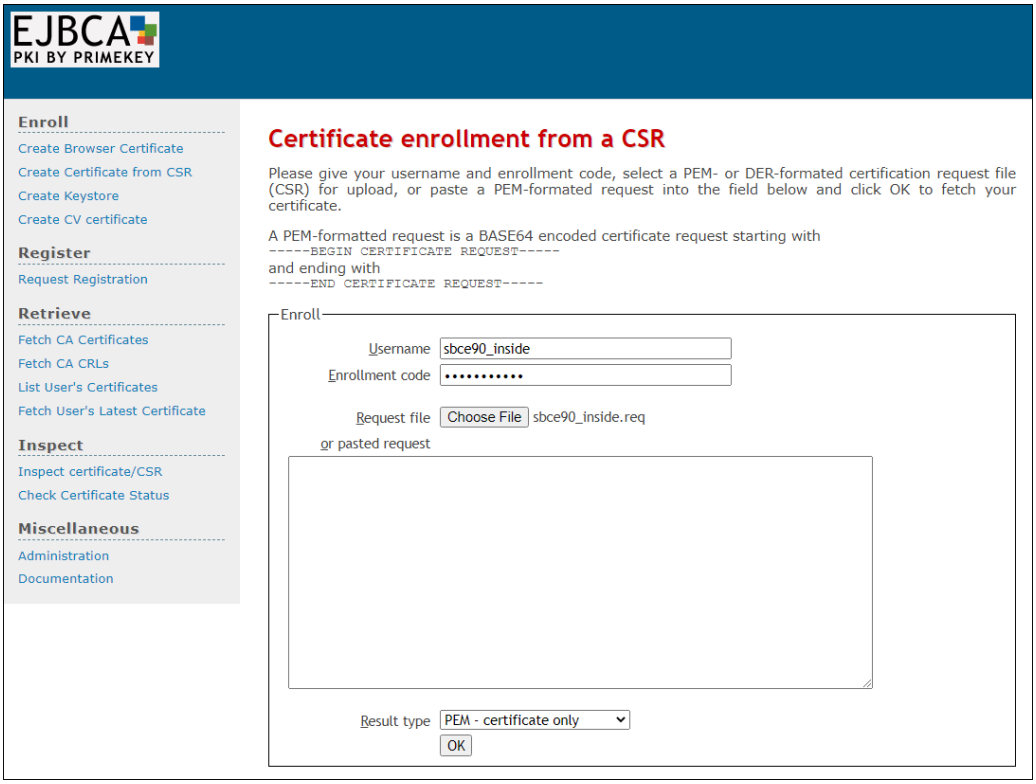
The identity certificate, e.g., **sbce90_outside.pem**, signed by the System Manager CA is created. The file should download automatically to the local PC. Alternatively, click the **Download certificate** link if needed, to save the file to the PC.



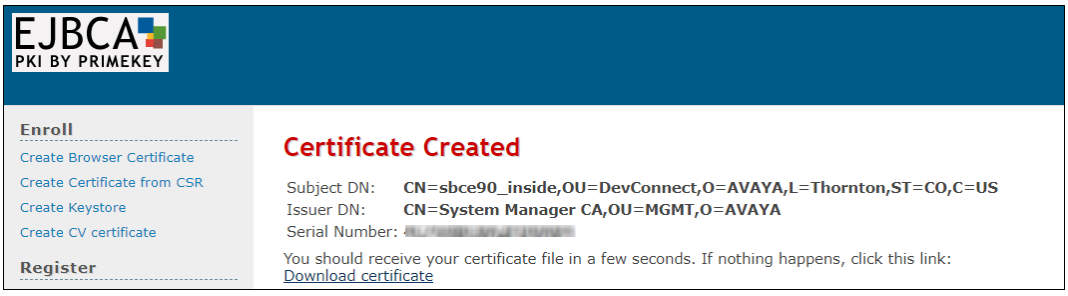
5.4.2. Create Identity Certificate – Avaya SBCE Internal Interface

Repeat the steps described in **Section 5.4.1**, with the following changes.
On the **Certificate Enrollment from CSR** page:

- Enter the same **Username** and **Enrollment Code** (password) configured on the End Entity corresponding to the SBCE internal interface in **Section 5.3.2**.
- Click **Choose File**. Browse and select the CSR file created in **Section 5.2.2**, e.g., **sbce90_inside.req** on the local PC.
- **Result type**: Select **PEM – certificate only**.
- Click **OK**.



The identity certificate, e.g., **sbce90_inside.pem**, signed by the System Manager CA is created. The file should download automatically to the local PC. Alternatively, click the **Download certificate** link if needed, to save the file to the PC.

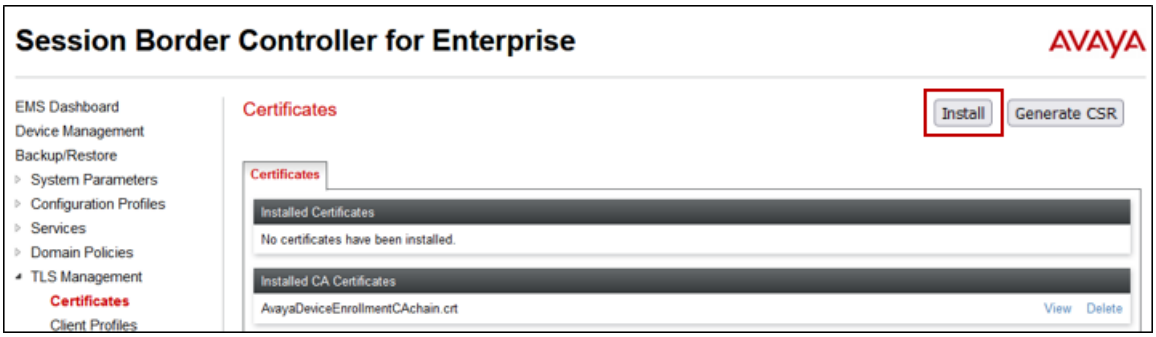


5.5. Install Identity Certificates on Avaya SBCE

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

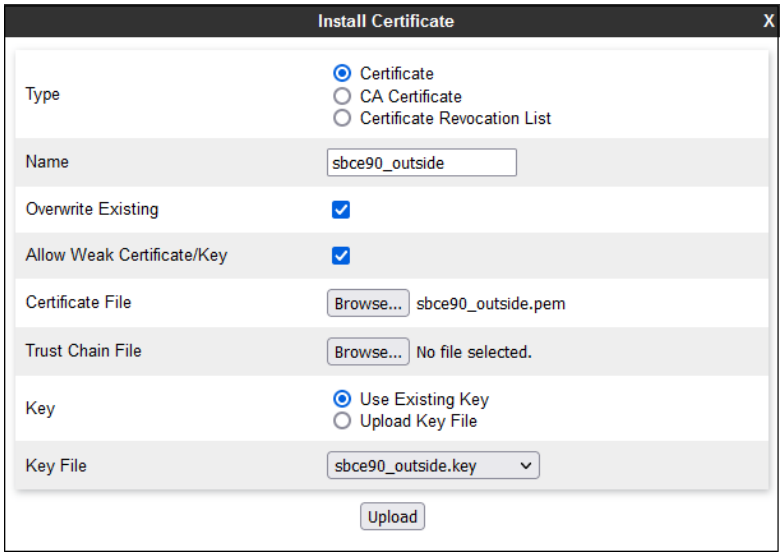
5.5.1. Install Identity Certificate - Avaya SBCE External Interface

On the Avaya SBCE web interface, navigate to **TLS Management → Certificates** and click the **Install** button.

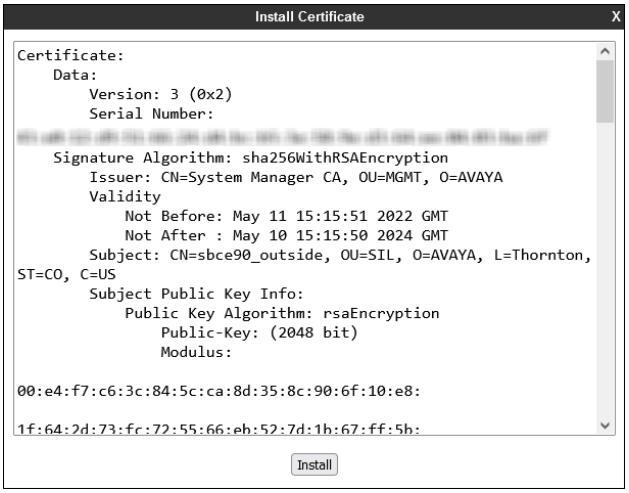


In the **Install Certificate** screen, select the following:

- **Type**: **Certificate**.
- **Name**: enter a descriptive name, e.g., **sbce90_outside**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- **Certificate File**: click **Browse** to select the identity certificate file previously saved**,** e.g., **sbce90_outside.pem**, on the local PC.
- **Key**: Select **Use Existing Key**, to use one of the key files automatically generated during the CSR creation.
- **Key File**: Select **sbce90_outside.key** from the drop-down menu.
- Click **Upload**.



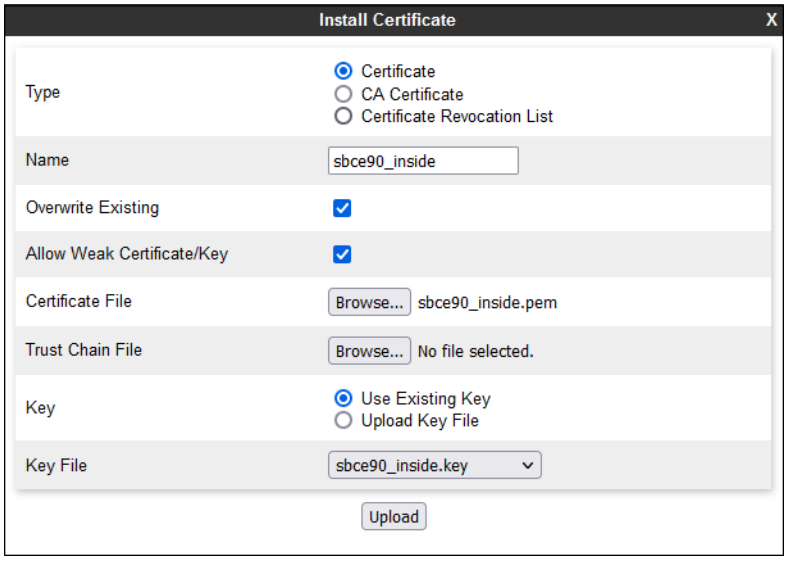
Click **Install**.



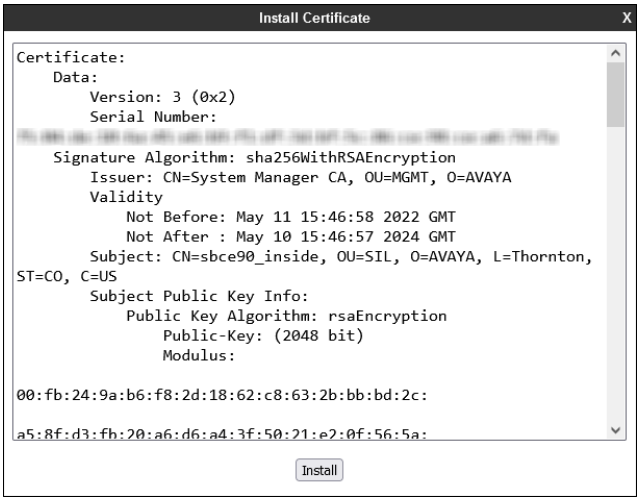
5.5.2. Install Identity Certificate - Avaya SBCE Internal Interface

Repeat the steps described in **Section 5.5.1** with the following changes:

- **Name**: enter a descriptive name, e.g., **sbce90_inside**.
- **Certificate File**: click **Browse** to select the identity certificate file previously saved**,** e.g., **sbce90_inside.pem**.
- **Key File**: Select **sbce90_inside.key** from the drop-down menu.
- Click **Upload**.



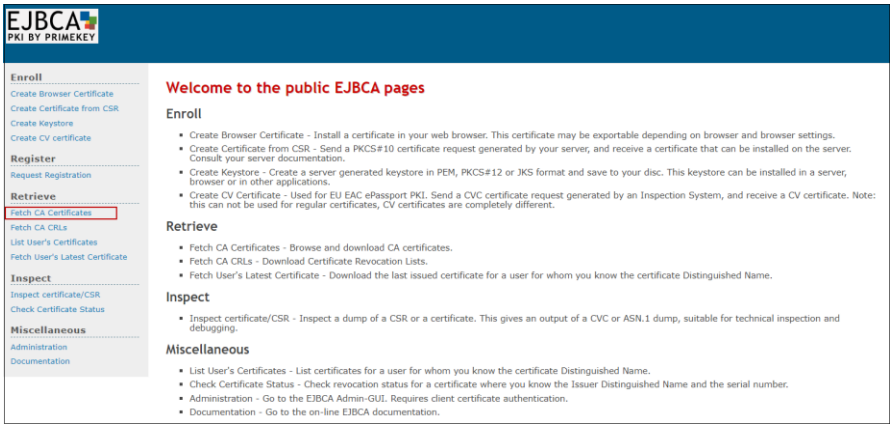
Click **Install**.



5.6. Install System Manager CA Root Certificate

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

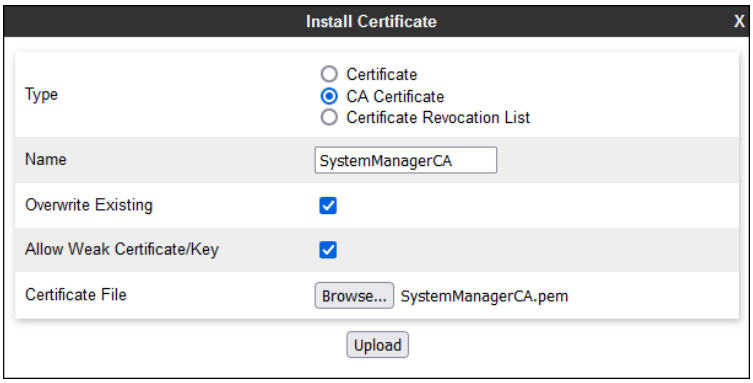
Select **Fetch CA Certificates**.



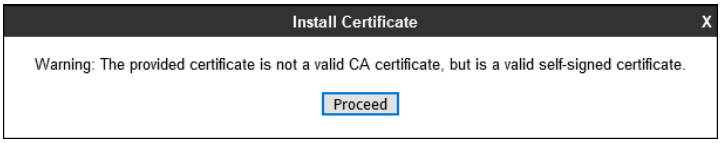
Click **Download as PEM**.

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:

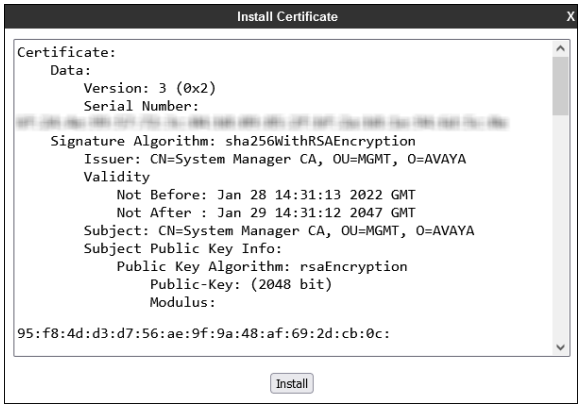
- **Type**: **CA Certificate**.
- **Name**: enter a descriptive name, e.g., **SystemManagerCA**.
- Check the boxes for **Overwrite Existing** and **Allow Weak Certificate/Key**.
- Click **Browse** to select the **SystemManagerCA.pem** certificate previously downloaded.
- Click **Upload**.



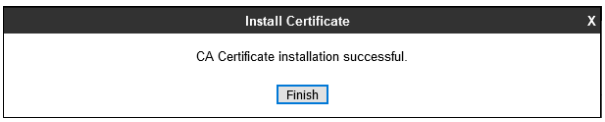
Select **Proceed** on the next screen.



Select **Install**.

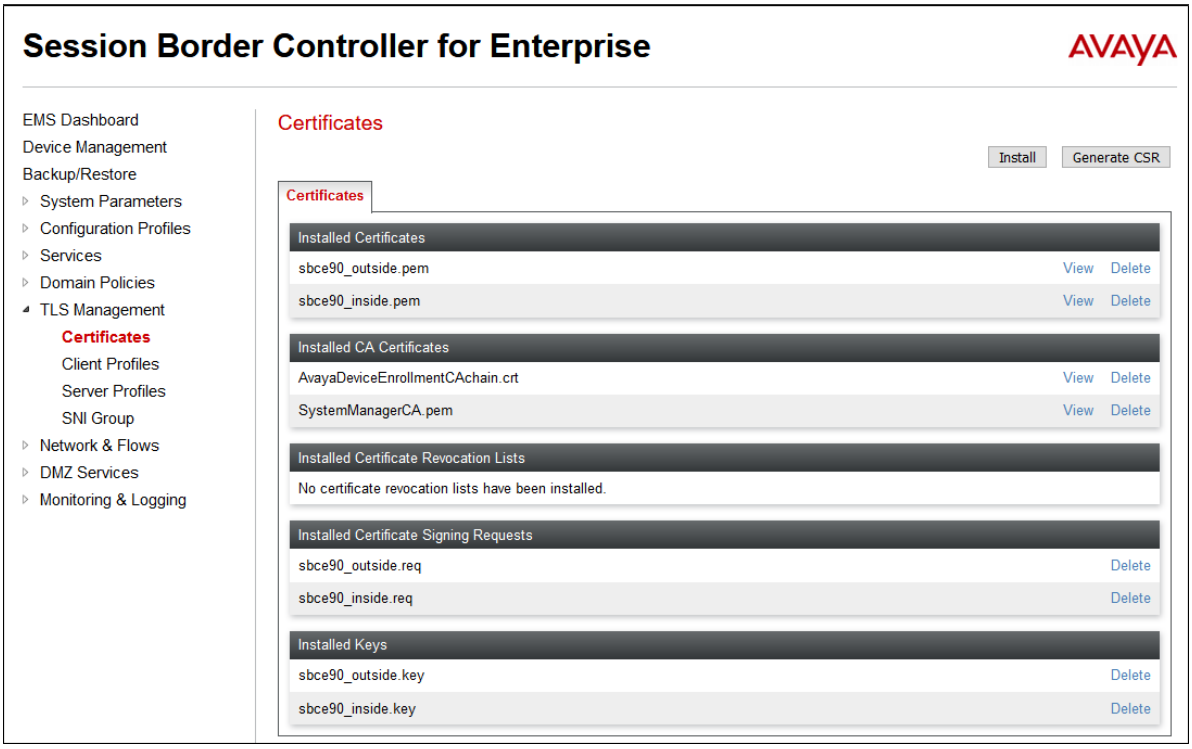


Click **Finish**.



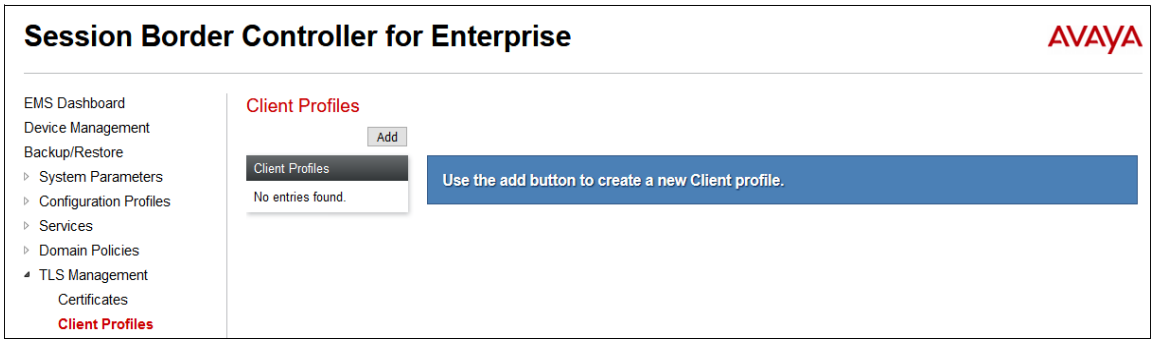
On the Avaya SBCE web interface, select **TLS Management → Certificates** from the left-hand menu. Verify the following:

- 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.
- Private keys associated with the identity certificates are present in the **Installed Keys** area.

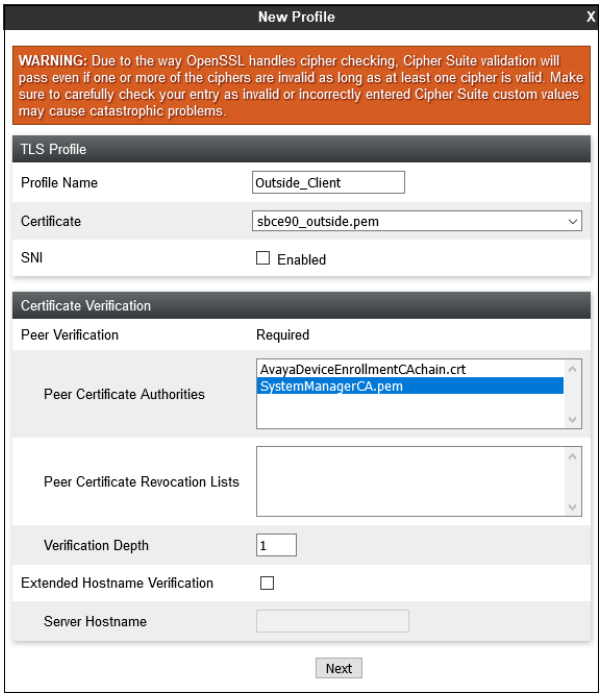


5.7. Configure Avaya SBCE TLS Client Profiles

Select **TLS Management → Client Profiles** from the left-hand menu to add the Avaya SBCE TLS Client Profiles. Click **Add**.



- **Profile Name:** enter descriptive name, e.g., **Outside_Client**.
- **Certificate:** select the identity certificate, e.g., **sbce90_outside.pem**, 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, e.g., **SystemManagerCA.pem**. Set **Verification Depth** to **1**.
- Click **Next**.

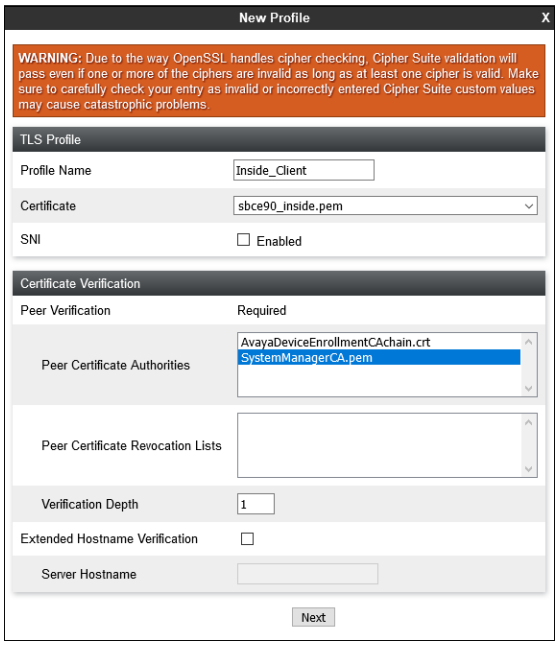


Accept default values for the next screen and click **Finish** (not shown).

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

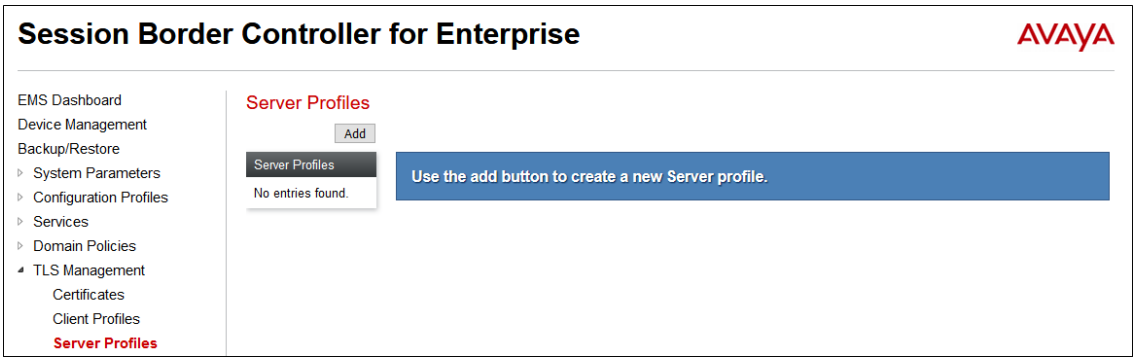
- **Profile Name:** enter descriptive name, e.g., **Inside_Client**.
- **Certificate:** select the identity certificate, e.g., **sbce90_inside.pem**.
- **Peer Verification** is set to **Required** by default. Under **Peer Certificate Authorities** select the CA certificate installed previously, e.g., **SystemManagerCA.pem**. Set **Verification Depth** to **1**.
- Click **Next**.

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



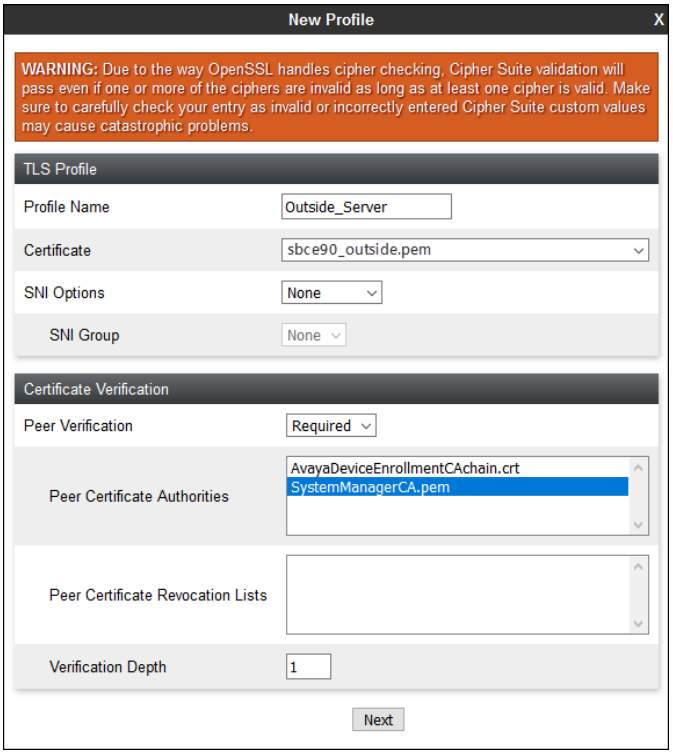
5.8. Configure Avaya SBCE TLS Server Profiles

Select **TLS Management → Server Profiles** from the left-hand menu to add the Avaya SBCE TLS Server Profiles. Click **Add**.



- **Profile Name:** enter descriptive name, e.g., **Outside_Server**.
- **Certificate:** select the identity certificate, e.g., **sbce90_outside.pem**, from the menu.

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., **SystemManagerCA.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**.



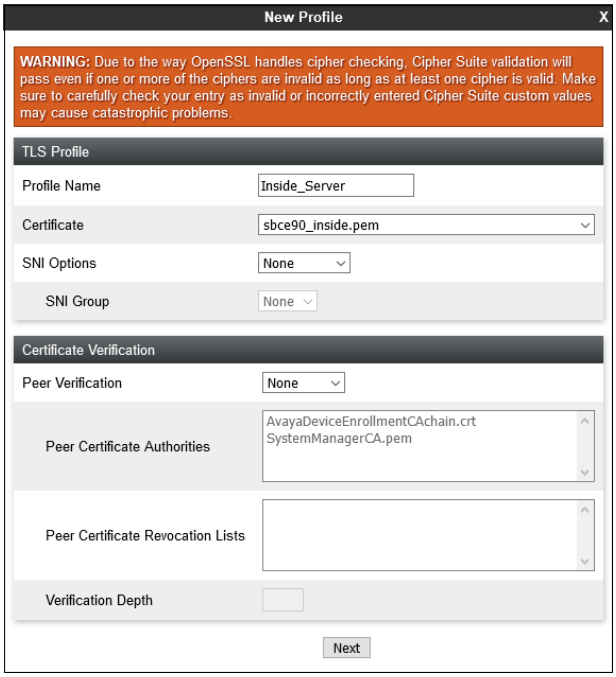
- Click **Next**. Accept default values for the next screen and click **Finish** (not shown).

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., **Inside_Server**.
- **Certificate:** select the identity certificate, e.g., **sbce90_inside.pem**, from the menu.
- **Peer Verification** = **None**.
- Click **Next**.



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

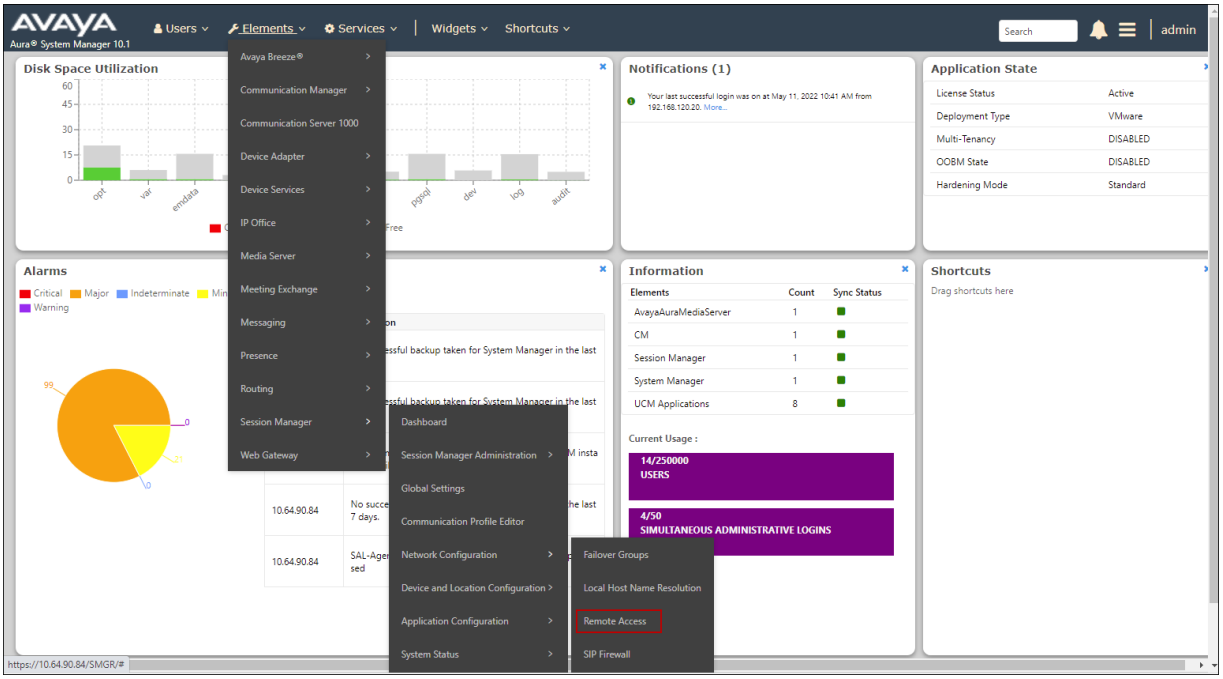
6. Session Manager Configuration

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

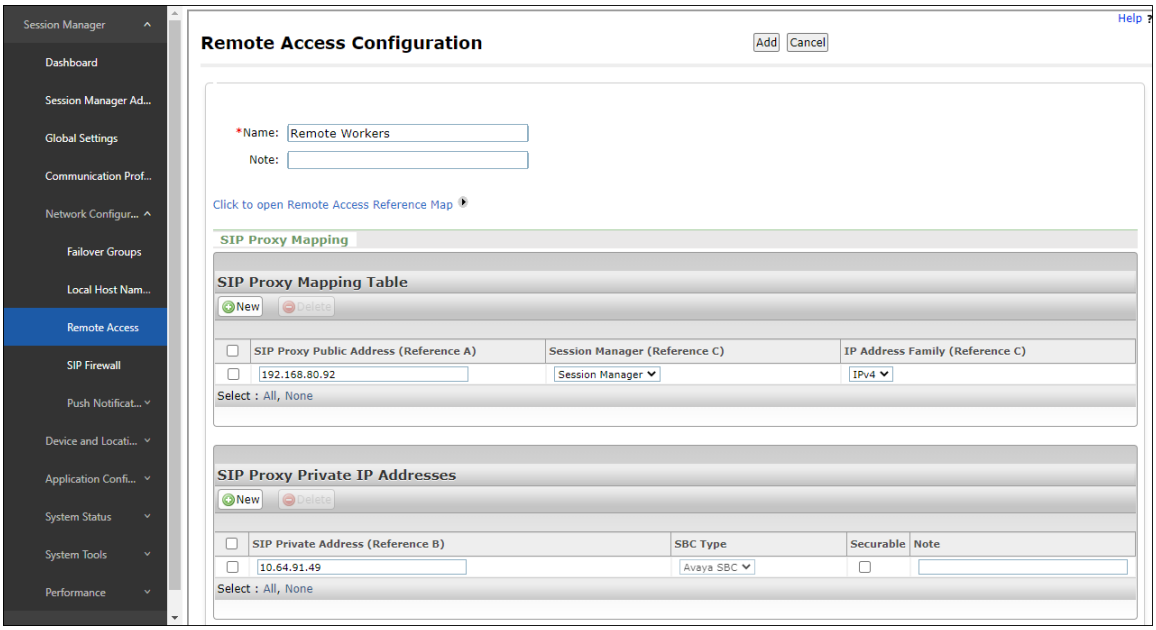
6.1. Remote Access Configuration

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** (not shown). Enter a descriptive name, e.g., **Remote Workers**. On the **SIP Proxy Mapping Table** section, select **New** and enter the Avaya SBCE public IP address used for remote workers, e.g., **192.168.80.92**. 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., **10.64.91.49**. Click **Add**.

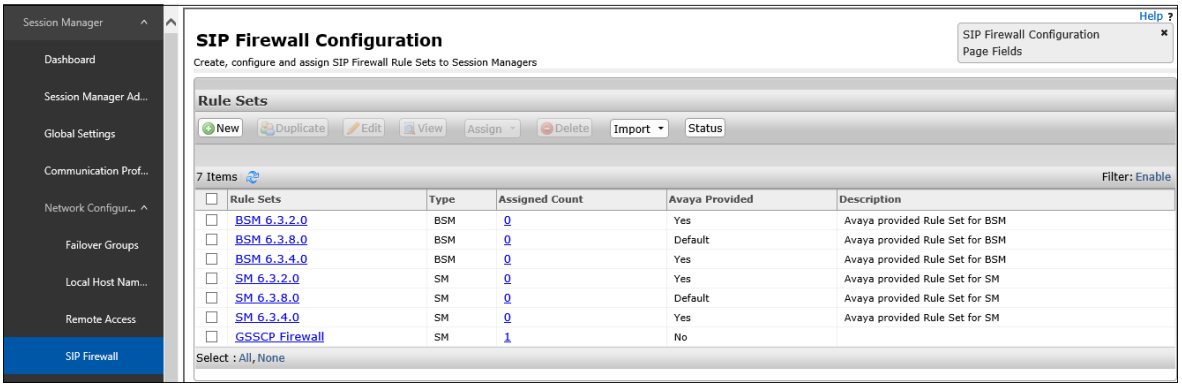


6.2. SIP Firewall Configuration

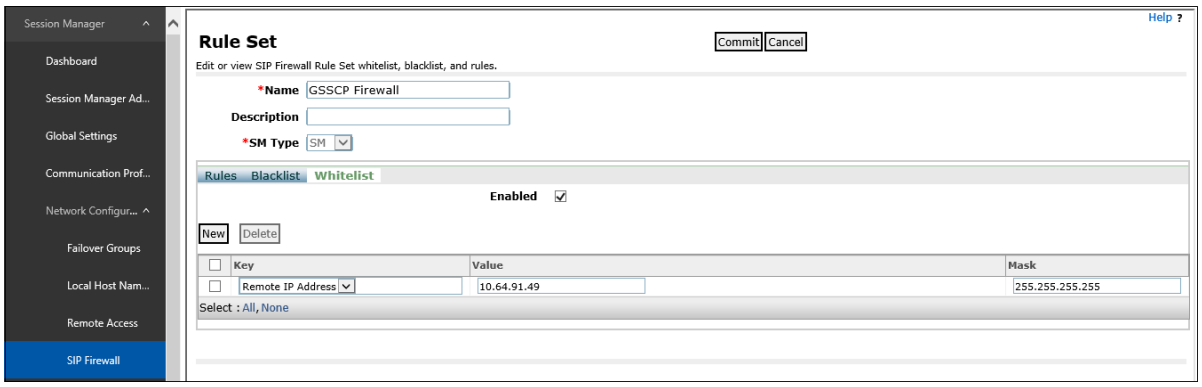
The SIP Firewall controls the flow of SIP traffic into Session Manager, based on configures sets of rules. Due to the possible high volume of Remote Worker associated traffic arriving to Session Manager from the IP address of Avaya SBCE inside interface, the Session Manager firewall may tag the inbound 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).

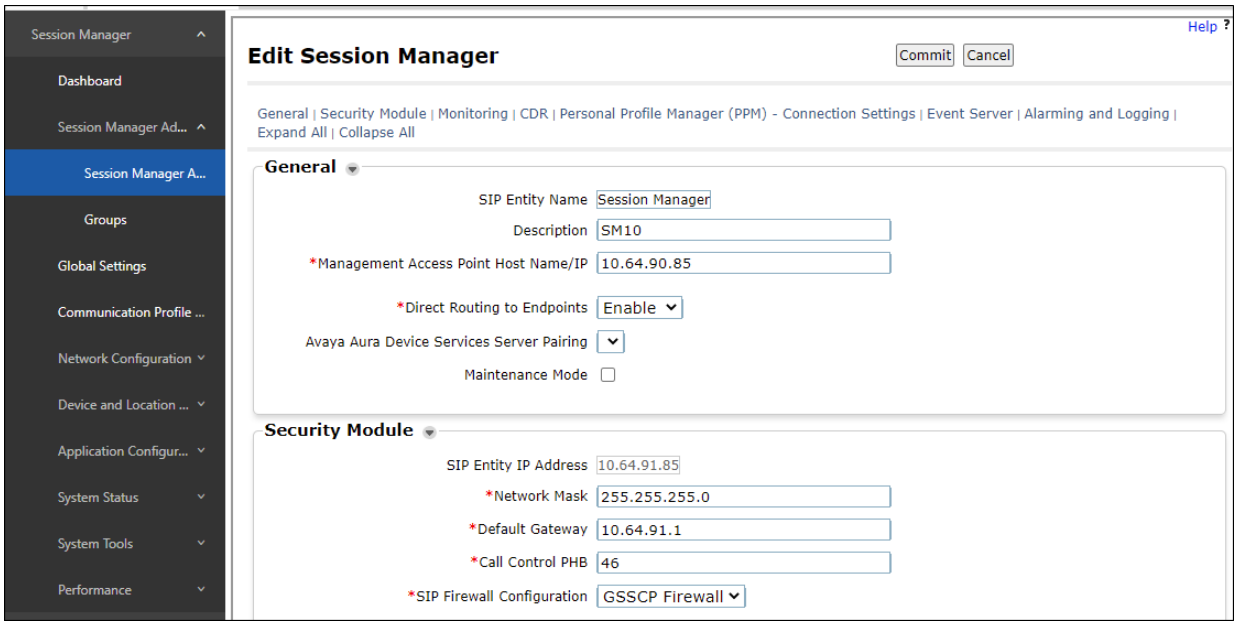
On the **SIP Firewall Configuration** page, **t**he right side of the screen shows the existing defaults or previously added rules under **Rule Sets**. If a new rule needs to be created, consult **4** on the **Additional References** section for more information. In the reference configuration, a previously defined rule set named **GSSCP Firewall** was modified to add the required entry to the Whitelist.



The screen below shows the modified Whitelist tab of the **GSSCP Firewall** Rule set. The entry shows the **Remote IP Address** with the assigned **Value** for the Avaya SBCE private IP address used for remote workers, e.g., **10.64.91.49**.



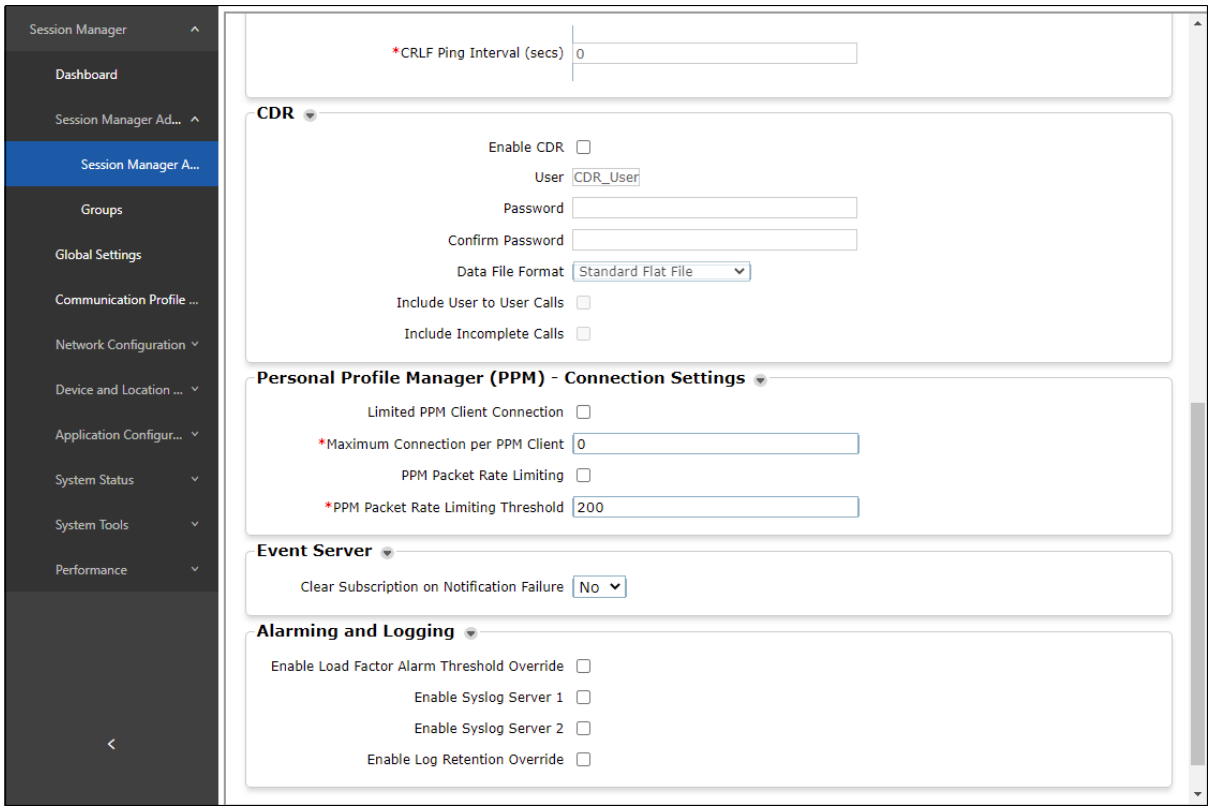
To verify the current SIP Firewall rule used by Session Manager, or to assign a new rule, navigate to **Elements → Session Manager Administration** from the System Manager **Home** page. On the **Session Manager Administration** screen, select the Session Manager instance and click **Edit** (not shown). Under the **Security Module** section, the **SIP Firewall Configuration** field shows the **GSSCP Firewall** rule set in use in the sample configuration.



6.3. Disable PPM Limiting

On the System Manager **Home** page navigate to **Elements → Session Manager Administration**. On the **Session Manager Administration** screen, select the Session Manager instance and click **Edit** (not shown).

On the **Edit Session Manager** screen, scroll down to the **Personal Profile Manager (PPM) – Connection Settings** section. Uncheck the **Limited PPM Client Connections** and **PPM Packet Rate Limiting** boxes. Click **Commit**.



7. Configure the Avaya Session Border for Enterprise

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

The configuration steps on the Avaya SBCE include the following:

- User Agents.
- IP/URI Blocklist Profile
- Server Interworking Profile.
- SIP Server Profile.
- Routing Profile.
- Application Rules.
- Media Rules.
- Signaling Rules.
- Security Rules.
- Endpoint Policy Group.
- Session Policy.
- Media and Signaling Interfaces.
- End Point Flows.
- Session Flow.
- PPM Services.
- Relays Services.

Note: The Avaya SBCE used in the reference configuration had previously been provisioned to support SIP Trunking. Some of the items on the list above (e.g., Server Interworking, SIP Server, Routing Profiles, etc.) may already be present in the configuration, and can be used or edited if necessary, to additionally support the Remote Worker functionality.

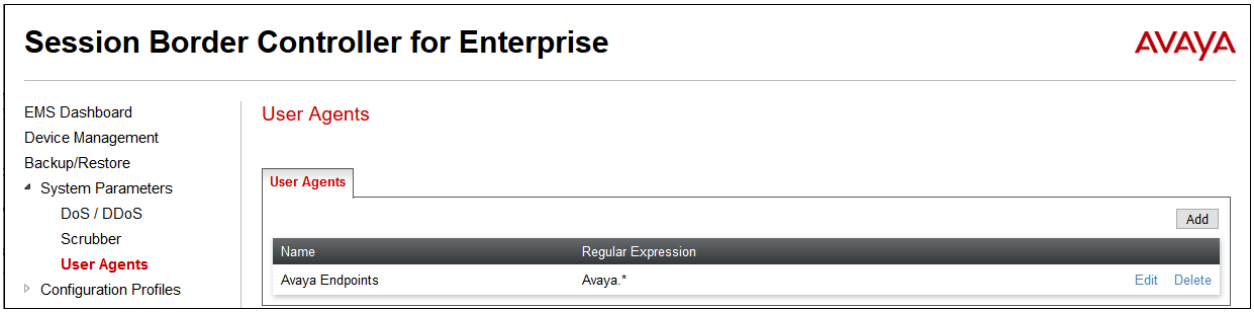
7.1. User Agents

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.

In the reference configuration, a single User Agent was created for all the Avaya endpoints.

Navigate to **System Parameters → User Agents**, select **Add** (not shown).

The following screen shows the values used in the reference configuration. The **Regular Expression** field is used to match the information contained on the User-Agent header arriving from the endpoint. Note the **Regular Expression** used **Avaya.***, common for all the Avaya endpoints.



If differentiated or more specific treatment is preferred for each type of endpoint, other User Agents could be created, using more granular Regular Expressions. Some examples are:

- Avaya one-X Deskphone.*
- Avaya J169 IP Phone.*
- Avaya Communicator.* (User-Agent header used by Avaya Workplace Client for Windows)
- Avaya Agent for Desktop.*

7.2. IP/URI Blocklist Profile

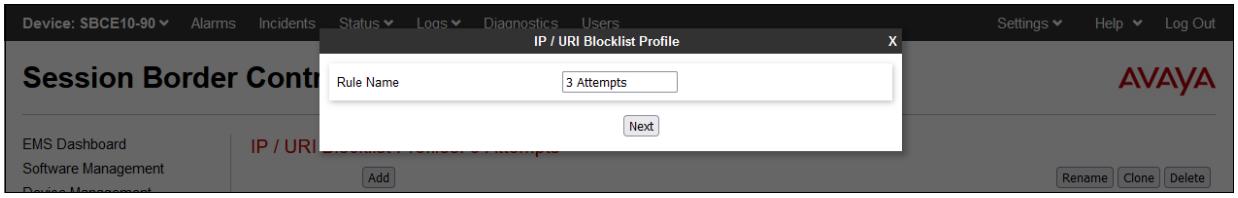
As a new feature in release 10.1, the Avaya SBCE offers automatic blacklisting of source IP/URI after multiple unsuccessful SIP/PPM login attempts. This feature is applicable to Remote Worker Deployments only.

Blacklisting of an IP/URI is based on two policies:

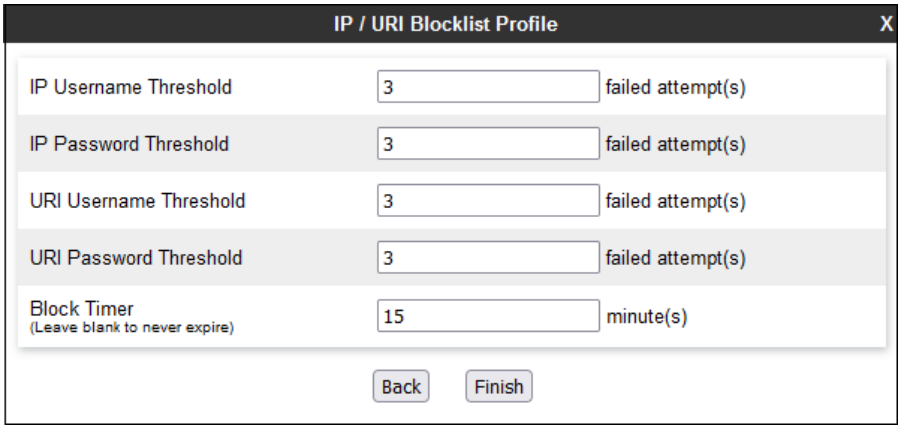
- SBCE should automatically blacklist the source IP of an endpoint for multiple login failures due to wrong username or wrong password.
- SBCE should automatically blacklist the source URI of an endpoint from a trusted IP or from different source IP for multiple login failures due to wrong username or wrong password.

In the reference configuration, an IP/URI Blocklist Profile was created. This configuration is optional.

Navigate to **Configuration Profiles → IP/URI Blocklist Profile** and select **Add.** Enter a Rule Name (e.g., **3 Attempts**) and click **Next**.



In the reference configuration, the threshold value for invalid username and password attempts was set to **3**, and the **Block Timer** was set to **15** minutes, as shown on the screen below. Click **Finish**.



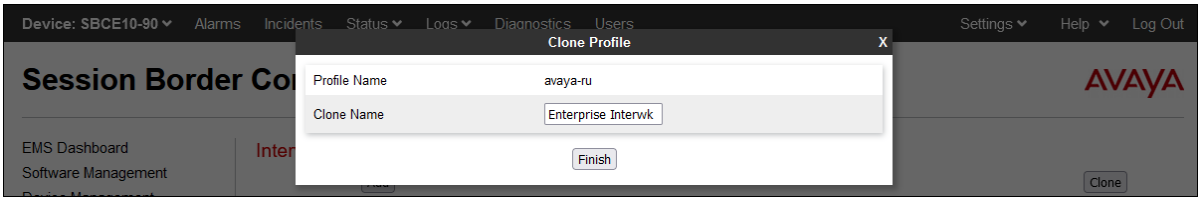
This profile will later be associated to the corresponding Subscriber Flow, in **Section 7.14.1**, and Reverse Proxy Profiles, **Section 7.17.2** in this document.

7.3. Server Interworking Profile

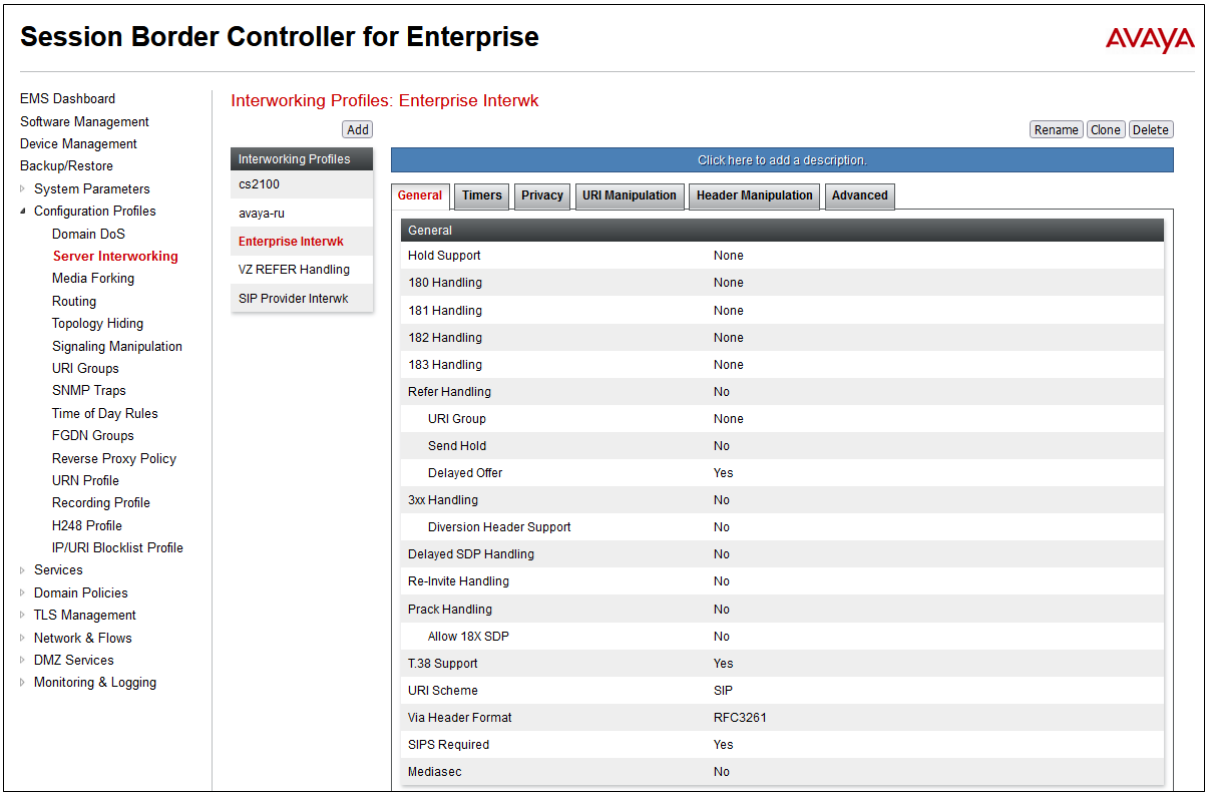
The Server Internetworking profile includes parameters to make the Avaya SBCE function in an enterprise VoIP network using different implementations of the SIP protocol. There are default profiles available that may be used as is, cloned and modified, or new profiles can be added as needed.

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. Enter a profile name (e.g., Enterprise Interwrk), and click Finish.



Default values were used for all fields. The profile will later be added to the SIP Server Configuration for Session Manager in **Section 7.4**.

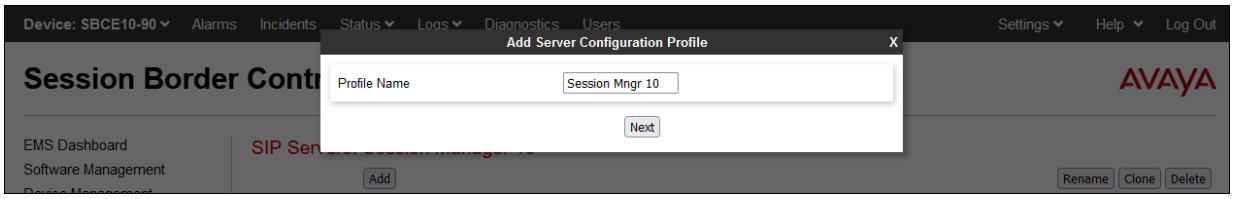


7.4. SIP Server Profile

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.

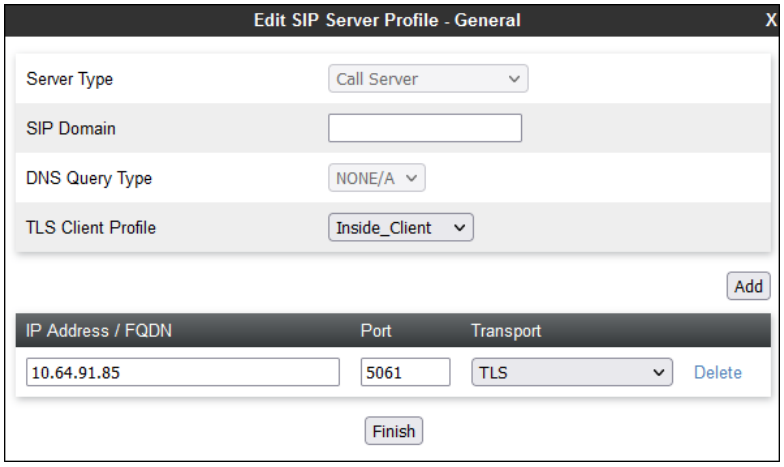
A SIP Server profile for Session Manager may have already been created, as part of the Avaya SBCE provisioning for SIP Trunking. If there is no existing SIP Server profile for Session Manager, follow the steps below to create a new profile.

Select **Services → SIP Servers** from the left-hand menu. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Mngr 10**) and click **Next**.



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

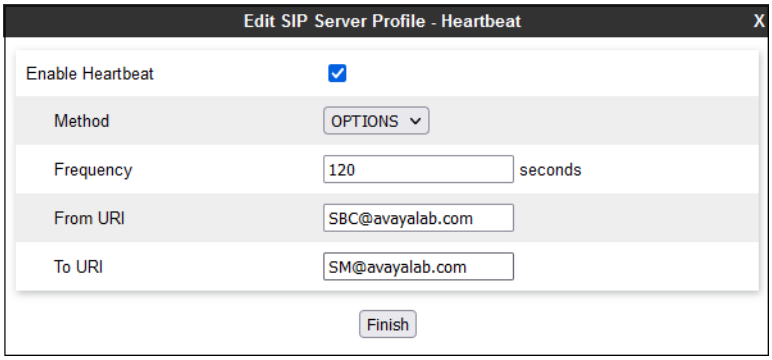
- Select **Server Type**: **Call Server**.
- **SIP Domain**: Leave blank (default).
- **DNS Query Type**: Select **NONE/A** (default).
- **TLS Client Profile**: Select the profile created in **Section 5.7** (e.g., **Inside_Client**).
- **IP Address**: **10.64.91.85** (Session Manager Security Module 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.

On the **Heartbeat** tab, check the **Enable Heartbeat** box to have the Avaya SBCE source "heartbeats" toward Session Manager. This configuration is optional.

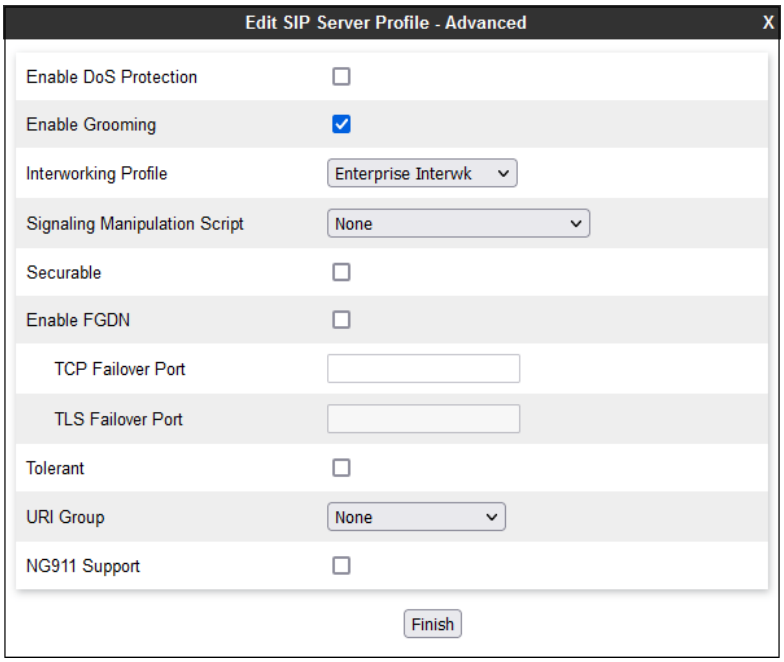
- Select **OPTIONS** from the **Method** drop-down menu.
- Select the desired frequency that the SBCE will source OPTIONS toward Session Manager.
- Make logical entries in the **From URI** and **To URI** fields that will be used in the OPTIONS headers.



Default values are used on the **Registration** and **Ping** tabs.

On the **Advanced** tab:

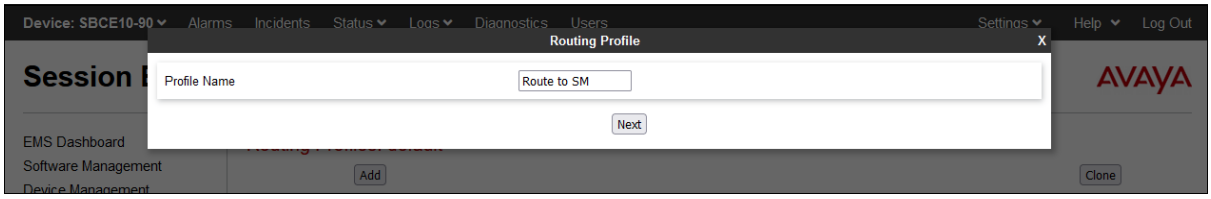
- Select the **Enterprise Interwk** (created in **Section 7.3**), for **Interworking Profile**.
- Since TLS transport is specified, then the **Enable Grooming** option should be enabled.
- In the **Signaling Manipulation Script** field select **none**.
- Select **Finish**.



7.5. Routing Profile

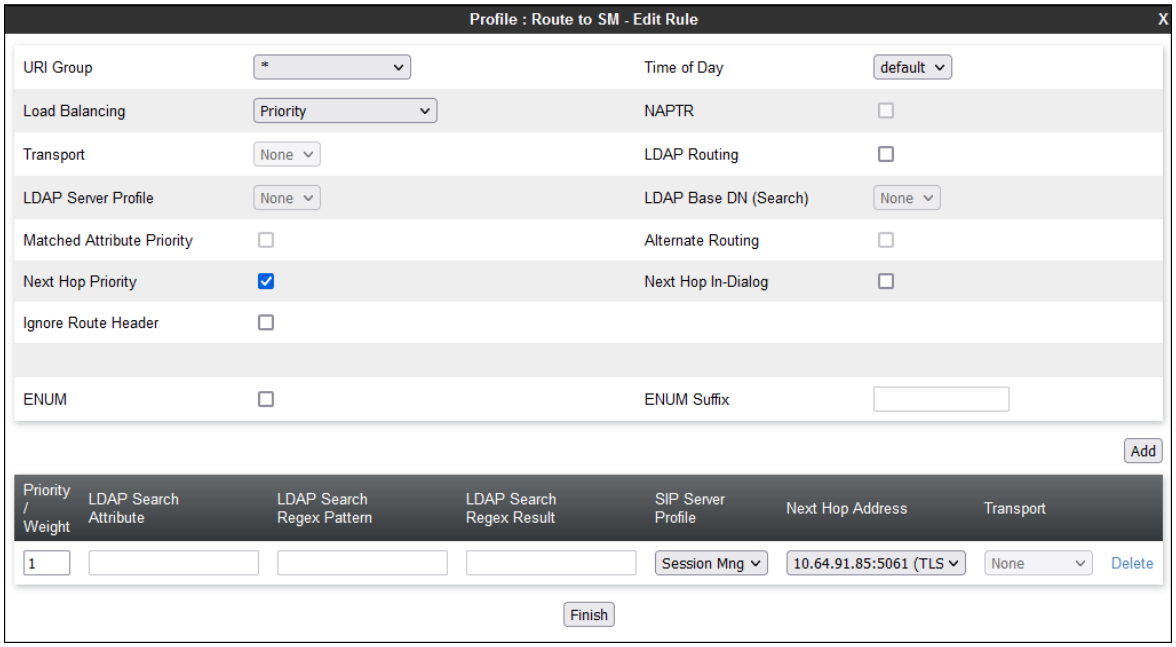
Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport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

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** = **Session Mngr 10** (from **Section 7.4**).
- **Next Hop Address:** Verify that the **10.64.91.85:5061 (TLS)** entry from the drop-down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
- Click **Finish**.

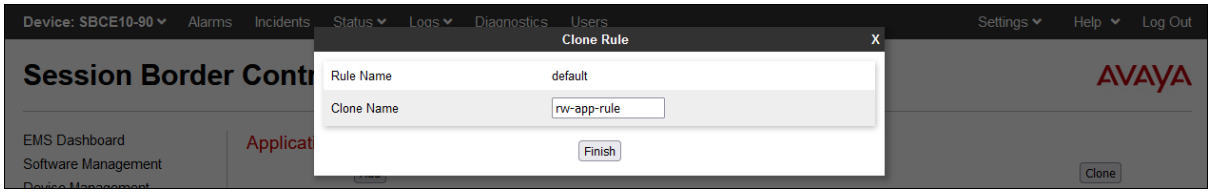


7.6. Application Rule

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

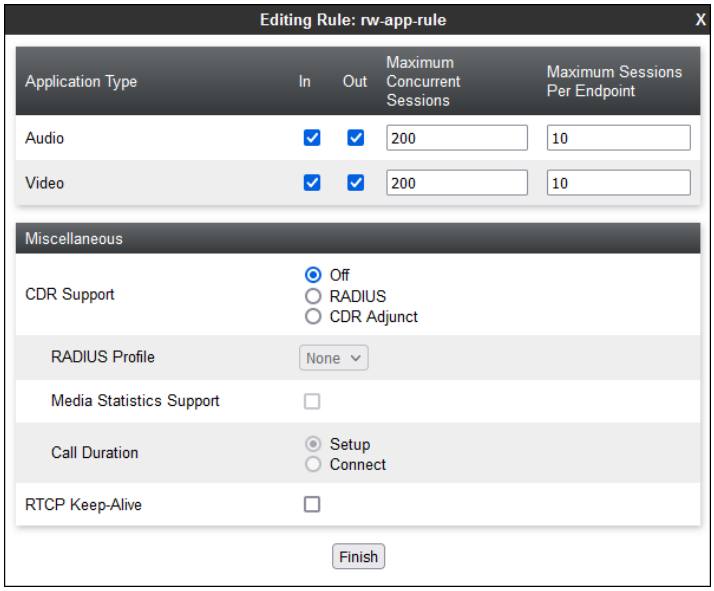
Note: The **Maximum Concurrent Sessions** and the **Maximum Sessions Per Endpoint** for Audio and Video should be set per the customer licenses purchased for the specific enterprise site. The values shown below are just an example; they represent the values used in the reference configuration.

From the navigation menu on the left-hand side, select **Domain Policies → Application Rules**. Select **default** in the **Application Rules** list. Click the **Clone** button. Under **Clone Name** enter the name of the profile (e.g., **rw-app-rule**). Click **Finish**.



Select the newly created Application Rule and Click **Edit** (not shown).

- Under **Audio**, set the **Maximum Concurrent Sessions** to **200** and **Maximum Sessions Per Endpoint** to **10**.
- If **Video** is required, check the **In** and **Out** boxes, set the **Maximum Concurrent Sessions to 200** and **Maximum Sessions Per Endpoint** to **10**.
- Click **Finish**.



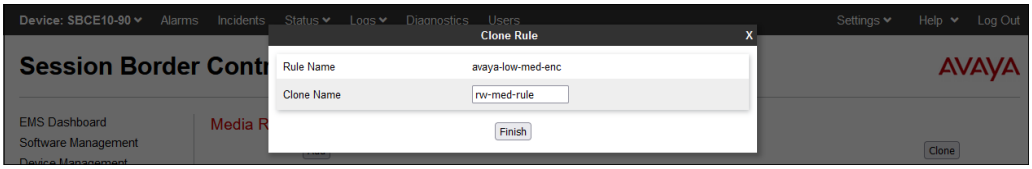
7.7. Media Rules

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

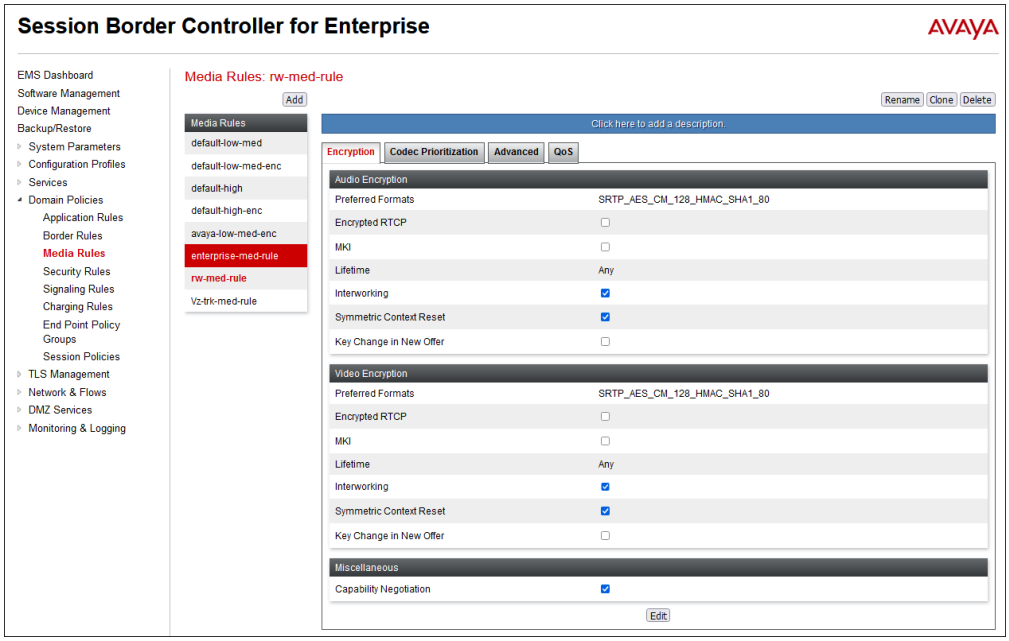
In the sample configuration, two media rules are defined, by cloning the default rule called **avaya-low-med-enc**, and editing the cloned rules as follows:

- A more restrictive media rule, allowing SRTP media only, towards the Remote Workers, to be used on the End Point Policy Group assigned to the Subscriber Flow.
- A less restrictive media rule that allows SRTP and also RTP, towards Session Manager, to be used in the End Point Policy Group assigned to the Server Flow.

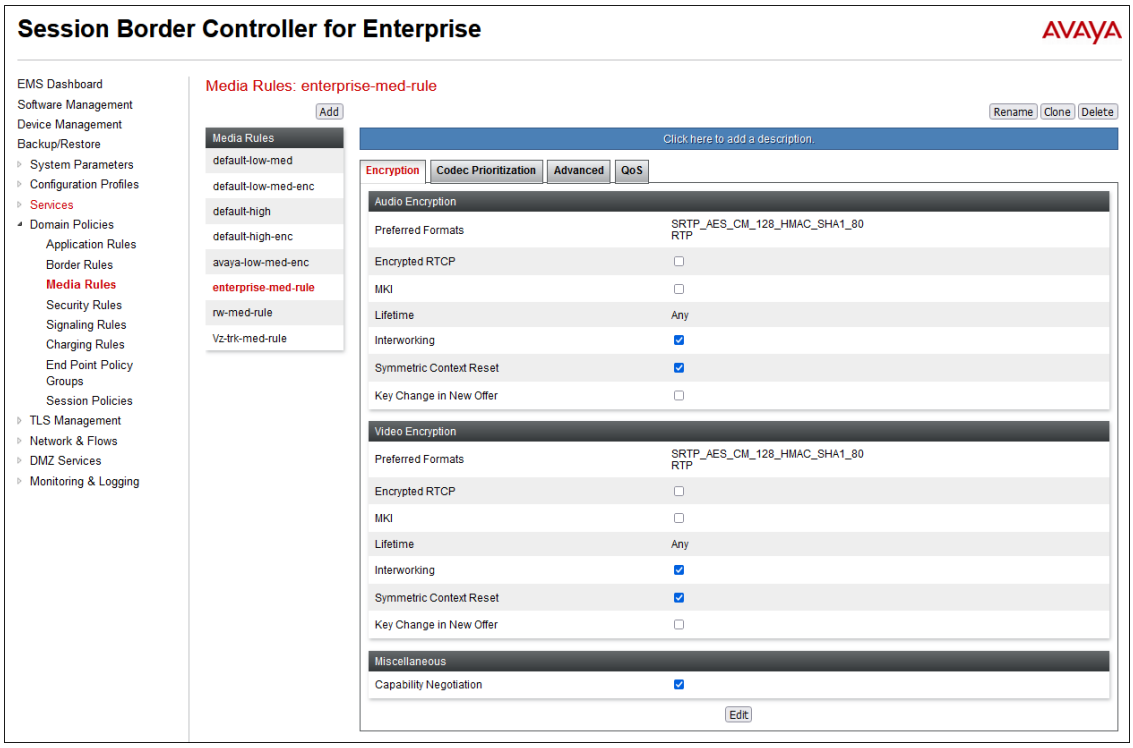
To add a Media Rule towards the Remote Workers, select **Media Rules** under the **Domain Policies** menu on the left-hand navigation pane. Select the **avaya-low-med-enc** rule from the list and click the **Clone** button. Under **Cloned Name**, enter the name of the profile (e.g., **rw-med-rule**). Click **Finish**.



The screen below shows the values on the **rw-med-rule** 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. Other parameters kept the default values from the cloned profile.



The **enterprise-med-rule** Media Rule towards Session Manager was similarly cloned from the **avaya-low-med-enc** rule. Both **SRTP_AES_CM_128_HMAC_SHA1_80** and **RTP** are selected as **Preferred Formats** for **Audio Encryption** and **Video Encryption**. Also, the **Capability Negotiation** setting is checked. Other tabs not shown have the default values from the cloned profile.



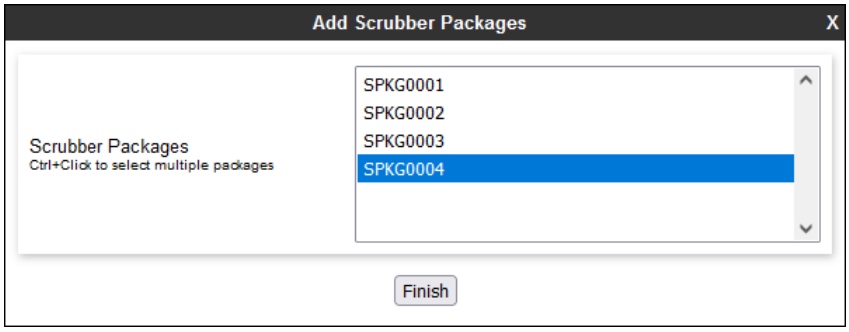
7.8. Security Rule

Security Rules can be used to define which enterprise-wide security features like Authentication, Compliance, Scrubber, and Domain DoS to be applied to a particular call flow.

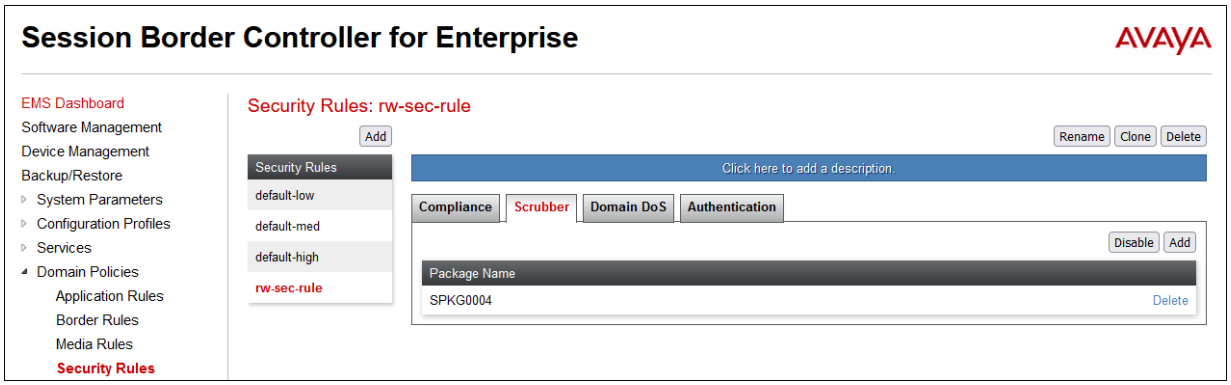
In the reference configuration, a Security Rule was created to use the Scrubber functionality for the detection and drop of malformed messages. Protocol scrubbing verifies certain message characteristics, such as proper message formatting, message sequence, field length, and content, against editable templates.

Navigate to **Domain Policies → Security Rules**, select the **default-med** rule from the list and select **Clone**. Enter a descriptive name under **Rule Name**, e.g., **rw-sec-rule**, and click **Finish**.

On the newly created **rw-sec-rule**, select the **Scrubber** tab. Select the **SPKG0004** package as shown on the screen below. Click **Finish**.



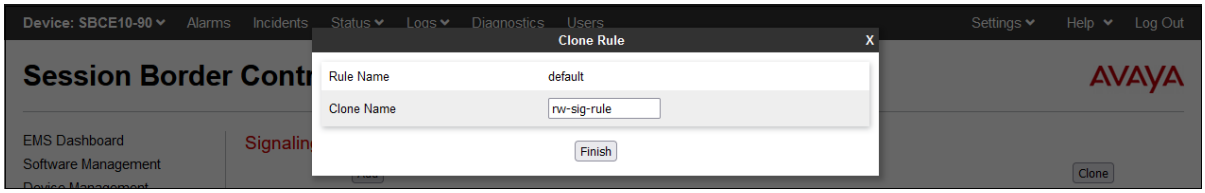
The screen below shows the values on the **rw-sec-rule** used in the reference configuration. The other tabs not shown were kept at the default values.



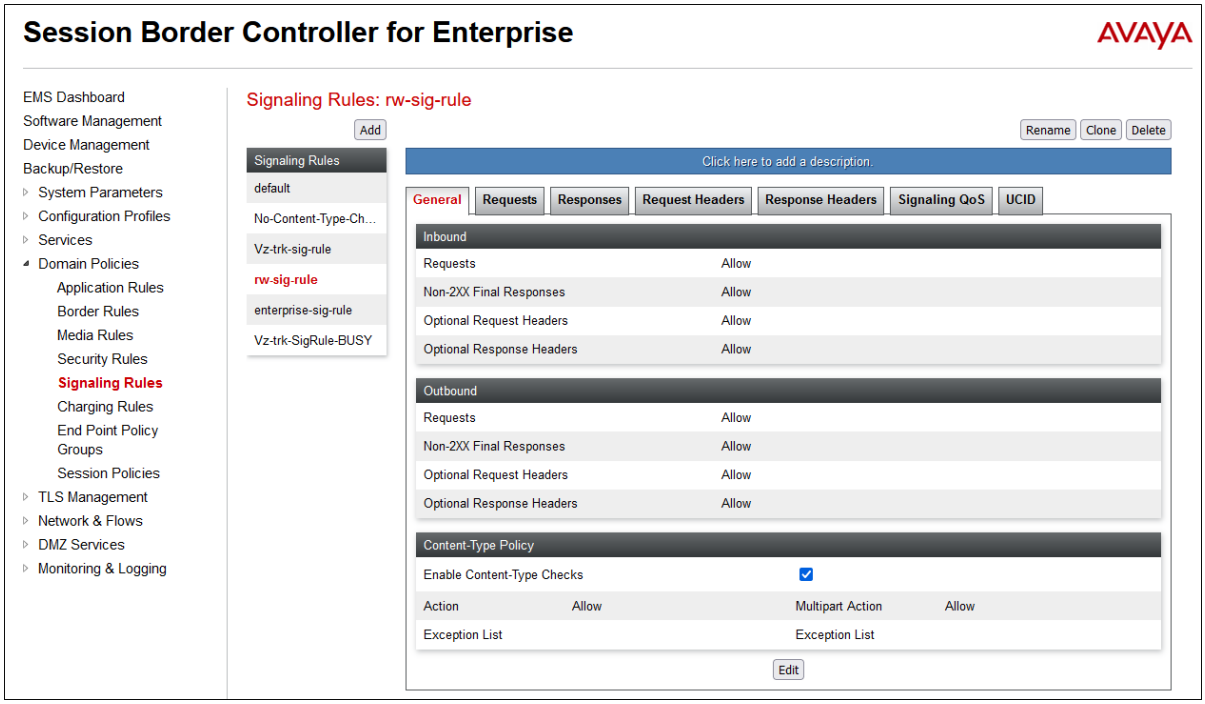
7.9. Signaling Rule

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. Enter a name in the **Clone Name** field, e.g., **rw-sig-rule** as shown below. Click **Finish**.



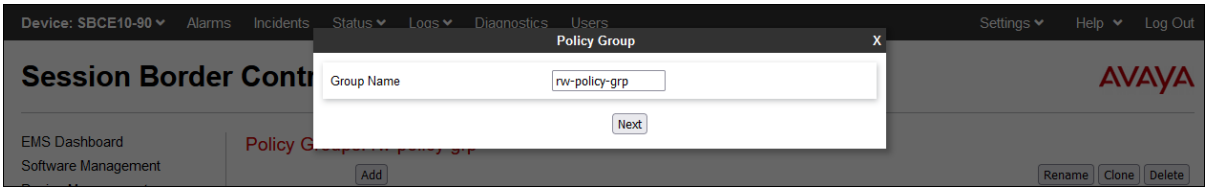
The screen below shows the values on the **rw-sig-rule** used in the reference configuration Default values were used for all parameters in this rule.



7.10. End Point Policy Group

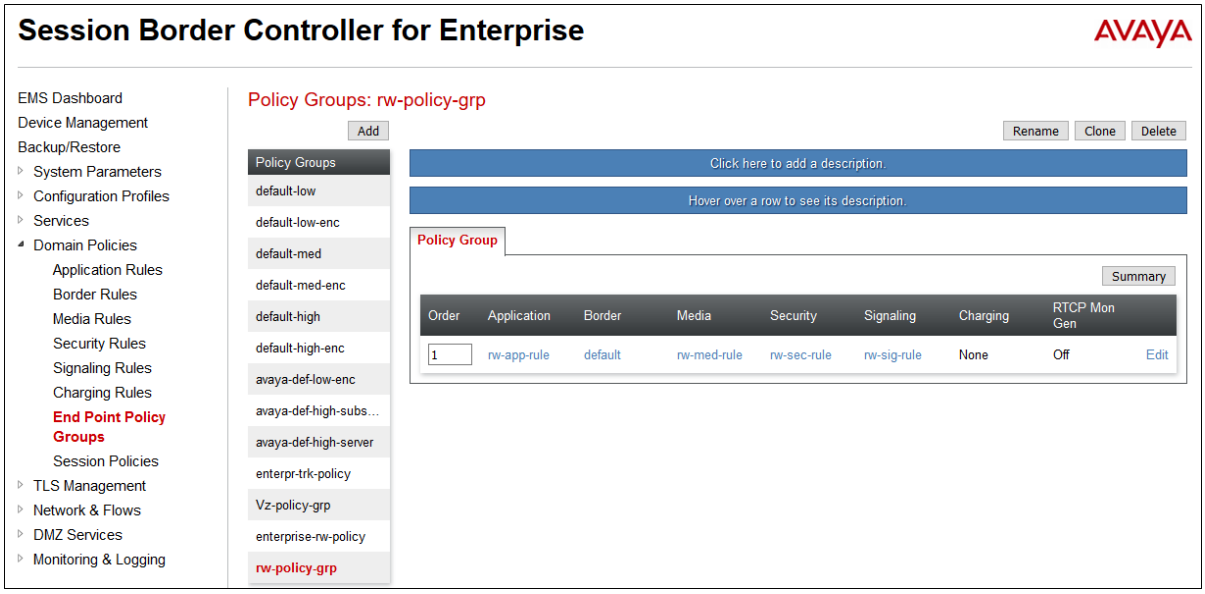
End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc.) to be applied to specific SIP messages traversing through the Avaya SBCE. The Endpoint Policy Group is then applied in following Sections to a Subscriber Flow or a Server Flow. Create separate Endpoint Policy 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**. Select the **Add** button. Enter a name in the **Group Name** field, e.g., **rw-policy-grp** as shown below. Click **Next**.



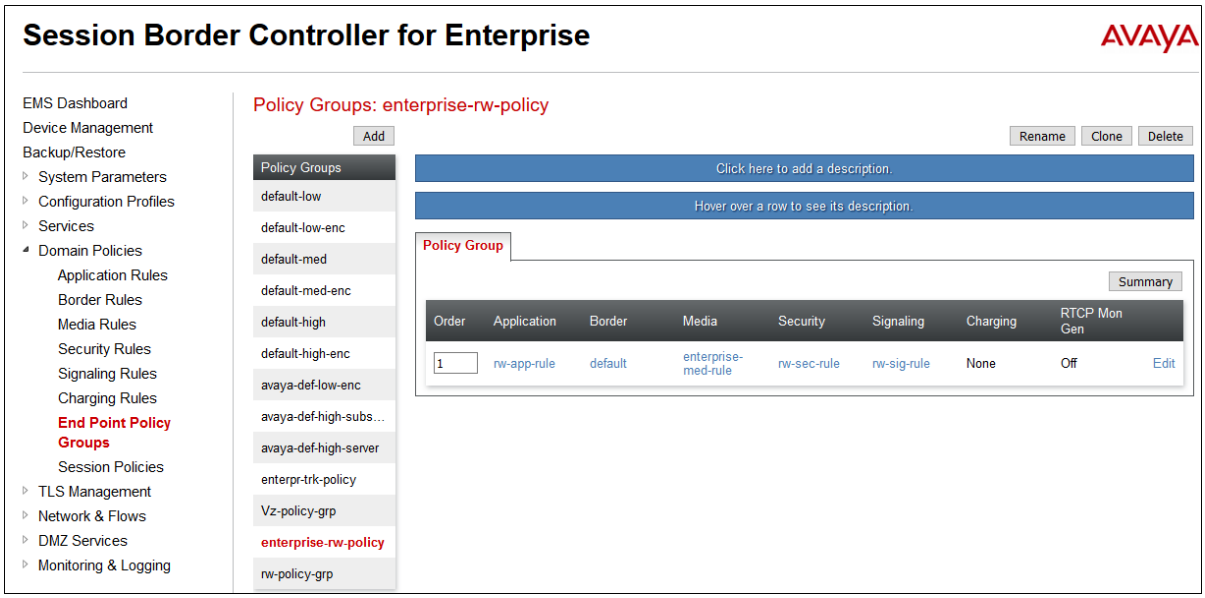
The screen below shows the **rw-policy-grp** defined in the reference configuration, using the following rules:

- **Application**: **rw-app-rule** created in **Section 7.6**.
- **Media: rw-med-rule** created in **Section 7.7**.
- **Security: rw-sec-rule** created in **Section 7.8**.
- **Signaling: rw-sig-rule** created in **Section 7.9**.
- Other rules used default values.



The screen below shows the **enterprise-rw-policy** defined in the reference configuration, towards the enterprise, using the following rules:

- **Application**: **rw-app-rule** created in **Section 7.6**.
- **Media: enterprise-med-rule** created in **Section 7.7**.
- **Security: rw-sec-rule** created in **Section 7.8**.
- **Signaling: rw-sig-rule** created in **Section 7.9**.
- Other rules used default values.

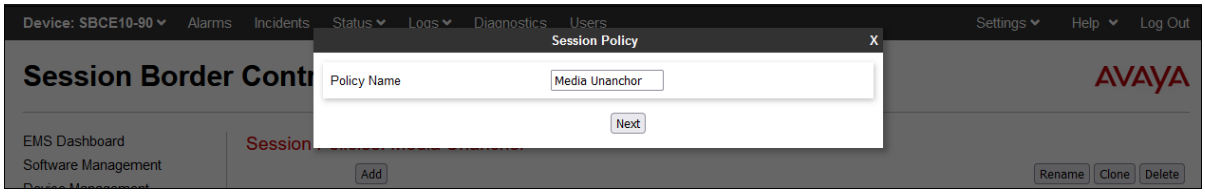


7.11. Session Policy

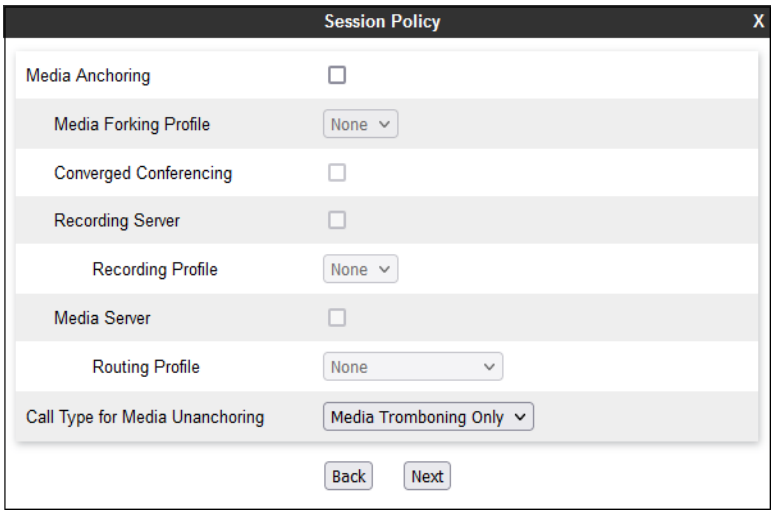
In the reference configuration, the remote workers were located on a common remote location. The Avaya SBCE can be configured to allow media to flow directly on calls between remote workers that are located on one subnet behind a router/NAT device. The result is improved bandwidth utilization and conservation of media resources at the enterprise

A Session Policy can be configured so when the Avaya SBCE detects that both remote workers on a call are behind the same NAT device, it can enable the media to flow directly between the remote workers. The media is un-anchored from the SBCE for these sessions, effectively releasing the SBCE from the media path.

Navigate to **Domain Policies → Session Policies** and select **Add**. Enter a **Policy Name**, e.g. **Media Unanchor** and click **Next** to continue.



On the **Session Policy** screen, verify that **Media Anchoring** is unchecked. Default values were used for all other parameters. Click **Next** and **Finish** (not shown).



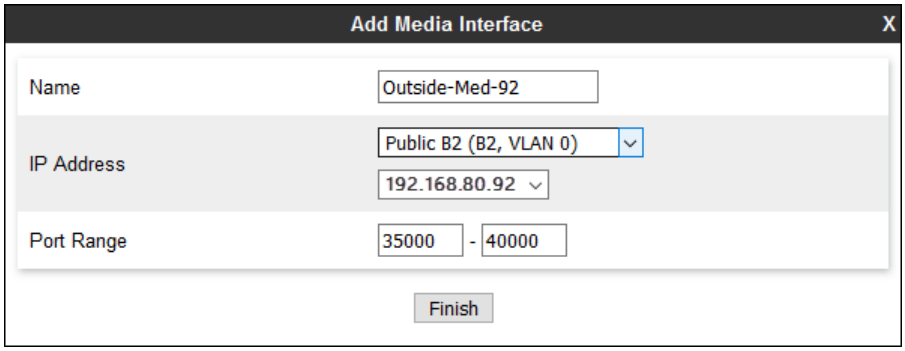
This Session Policy will be applied to a corresponding Session Flow, later on **Section 7.15**.

Note: The Session Policy and Session Flow configuration shown in these document is optional. For more information on supported un-anchoring scenarios for the media, consult [**1**] on the **References** section.

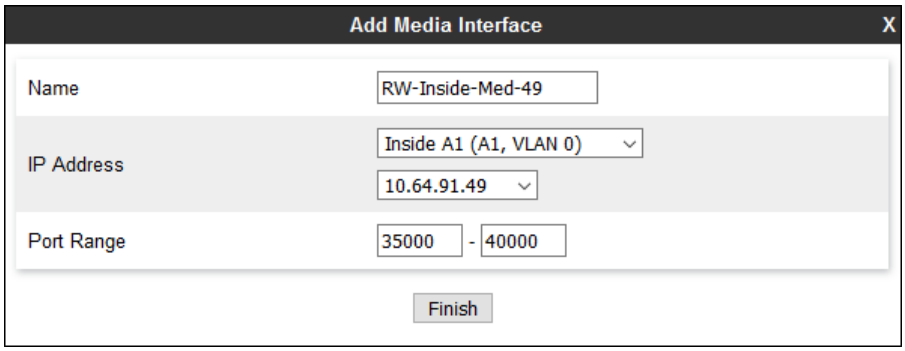
7.12. Media Interfaces

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. On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface, e.g., **Outside-Med-92**. Select the public IP Address for the 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**.



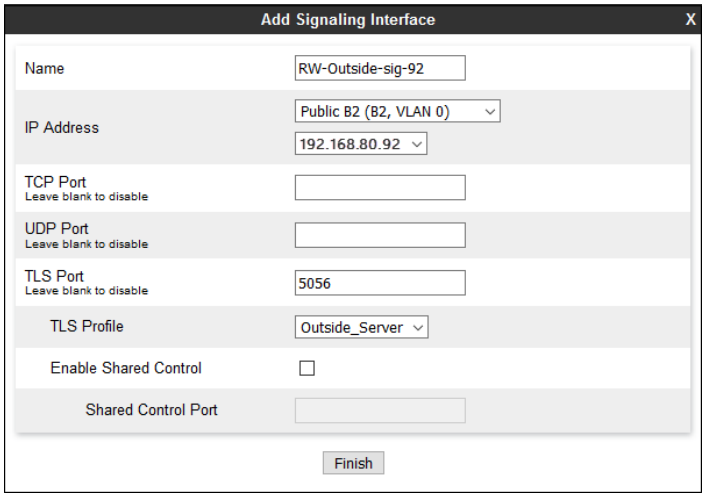
A Media Interface facing the enterprise network side named **RW-Inside-Med-49** was similarly created. The inside IP Address of the Avaya SBCE used for Remote Worker traffic was selected from the drop-down menu. The **Port Range** was left at the default values. Click **Finish**.



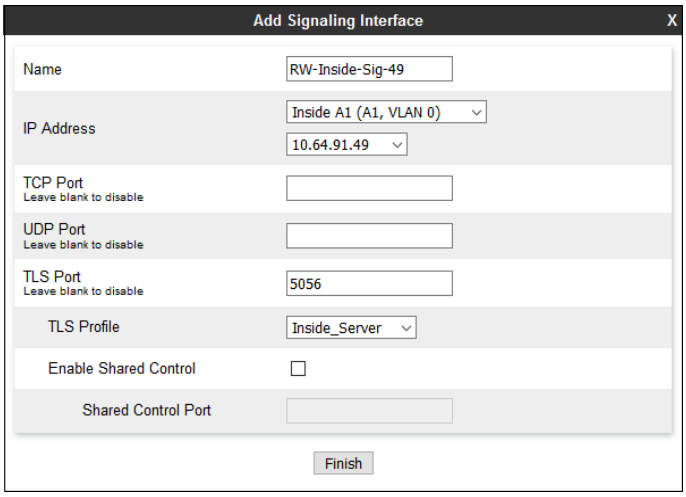
7.13. Signaling Interfaces

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. On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface, e.g., **RW-Outside-sig-92** Select the public IP Address of the Avaya SBCE used for Remote Workers from the **IP Address** drop-down menu. In the reference configuration, **TLS Port 5056** was used to listen for Remote Worker signaling traffic. Under **TLS Profile**, select the **Outside_Server** profile created in **Section 5.8** . Click **Finish**.



A Signaling Interface facing the enterprise network side named **RW-Inside-Sig-49** was similarly created. The inside IP Address of the Avaya SBCE used for Remote Worker traffic was selected from the drop-down menu. **TLS Port 5056** was used to listen for Remote Worker signaling traffic. Under **TLS Profile**, select the **Inside_Server** profile created in **Section 5.8**. Click **Finish**.

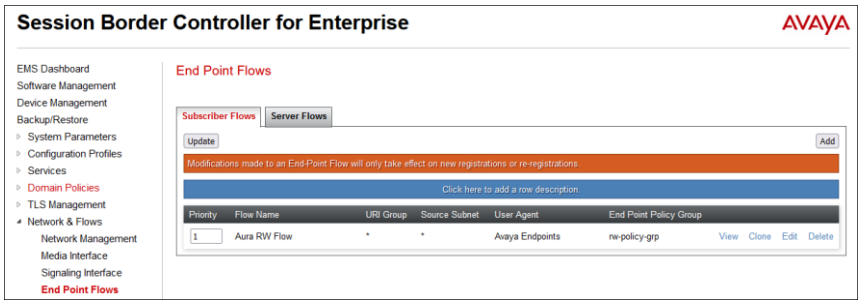


7.14. End Point Flows

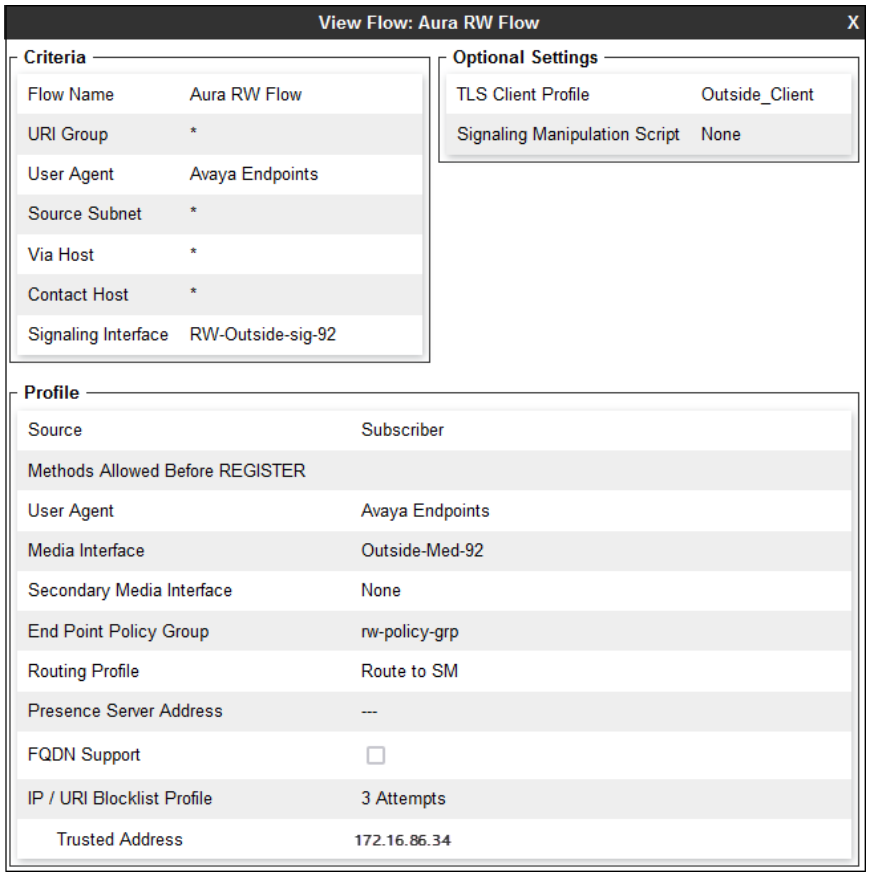
End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. These flows combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

7.14.1. 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 following screen shows the **Aura RW Flow** Subscriber Flow created in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.



Note: The **Outside_Client** profile**,** created in **Section 5.7**, 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**.

Note: Under **IP/URI Blocklist Profile**, the **3 Attempts** profile optionally created in **Section 7.2** was selected. Under **Trusted Address**, the public address of the router/NAT at the remote location can be entered. With this setting, the SBCE should automatically blacklist the source URI of an endpoint for multiple login failures due to wrong username or wrong password exceeding the configured threshold, but it will not block registration attempts from other users at the same location using the same router/NAT.

7.14.2. 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 **SM Flow for RW** Server Flow created in the sample configuration. This flow uses the interfaces, policies, and profiles defined in previous sections.

View Flow: SM Flow for RW X

Criteria

Flow Name	SM Flow for RW
Server Configuration	Session Mngr 10
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	RW-Outside-sig-92

Profile

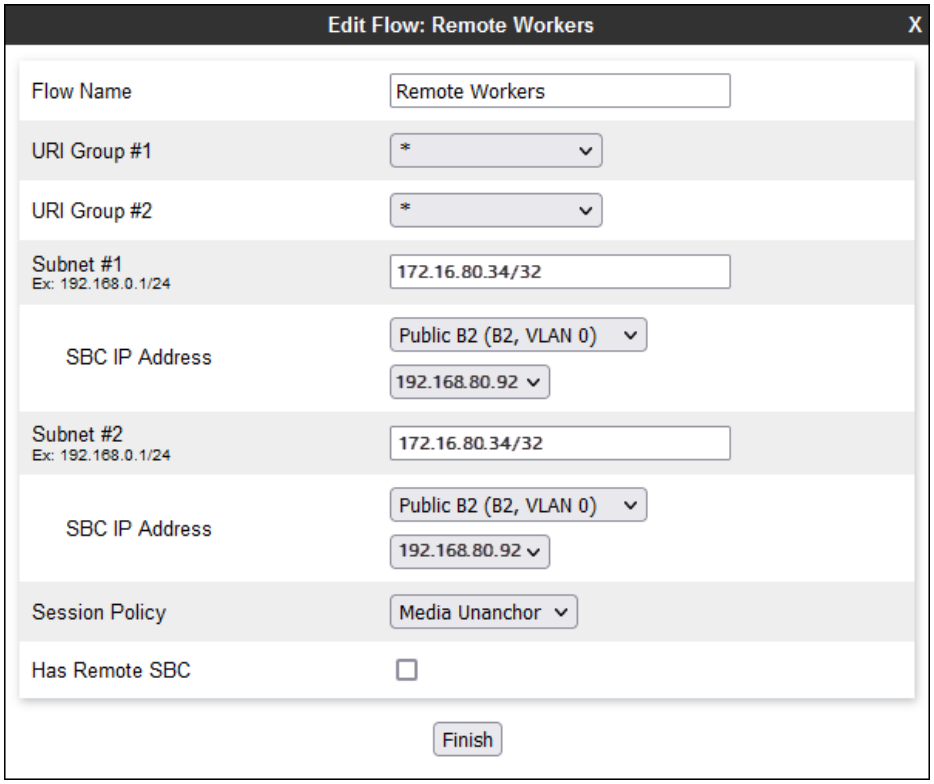
Signaling Interface	RW-Inside-Sig-49
Media Interface	RW-Inside-Med-49
Secondary Media Interface	None
End Point Policy Group	enterprise-rw-policy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐

7.15. Session Flow

In the reference configuration, a Session Flow was created to allow the media to be redirected on calls between remote workers at the remote location.

To create a new Session Flow, navigate to **Network & Flows → Session Flows** and click the **Add** button.

The following screen shows the **Remote Workers** Session Flow created in the sample configuration. The value entered under the **Subnet #1** and **Subnet #2** fields, **172.16.80.34/32**, correspond to the Internet facing public IP address of the Router/NAT at the remote workers location. Under **SBC IP Address**, the public IP Address of the Avaya SBCE used for Remote Workers is selected from the drop-down menu. Under **Session Policy**, select the **Media Unanchor** policy created on **Section 7.11**.

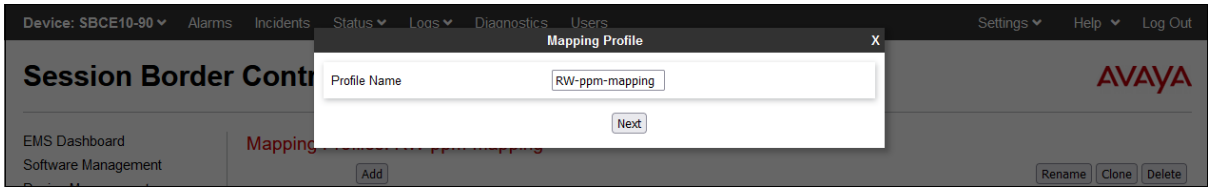


Note – For security reasons, the public IP addresses used on the Router/NAT at the remote location and the Avaya SBCE interface B2 are masked in the screen above.

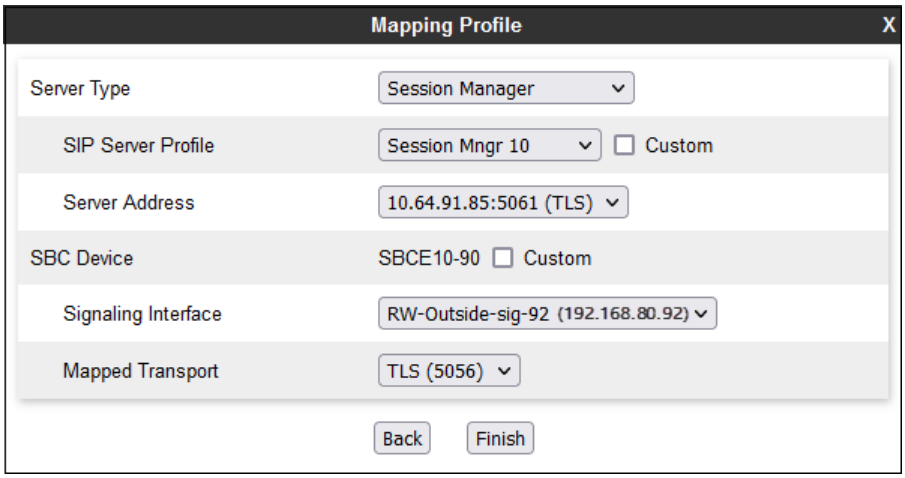
7.16. PPM Mapping

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.

Navigate to **DMZ Services → PPM Mapping** and click the **Add** button. Enter a descriptive Profile Name, e.g., **RW-ppm-mapping** and click **Next**.



On the Mapping Profile screen, **Session Manager** is selected for **Server Type**. Under **SIP Server Profile** select the Session Manager profile created in **Section 7.4**. The **Server Address** is automatically populated with the Session Manager IP address and port **10.64.91.85:5061 (TLS)**. Under **Signaling Interface** and **Mapped Transport**, select the **RW-Outside-sig-92 (192.168.80.92)** interface and **TLS (5056)** port as created in **Section 7.13**. Click **Finish**.



7.17. 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.

7.17.1. Application Relay

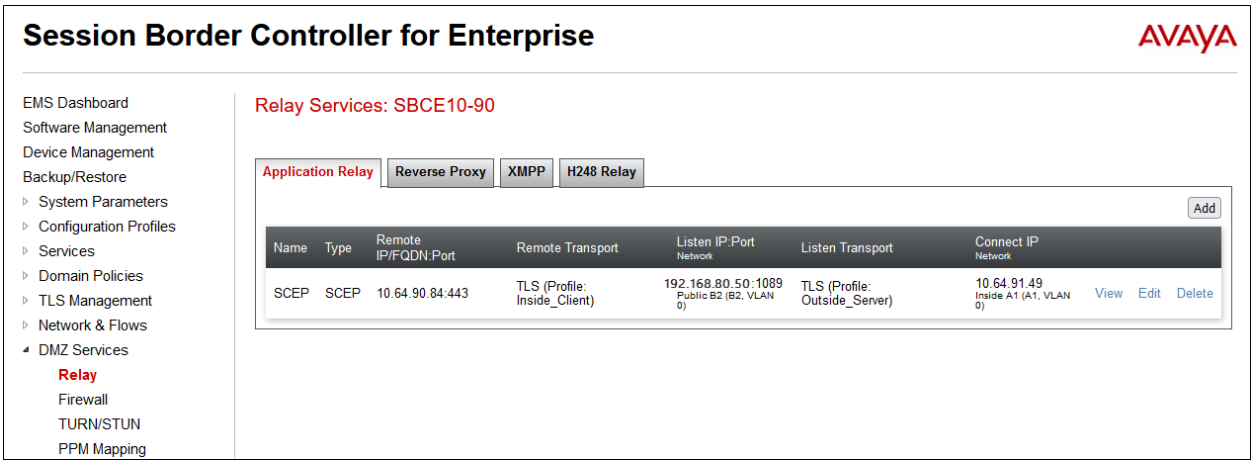
In the sample configuration, an Application Relay policy was used on the Avaya SBCE to forward SCEP requests from SIP endpoints to obtain identity certificates from a Certificate Authority server.

Navigate to **DMZ Services → Relay**. Select the **Application Relay** tab and click **Add** to add a new entry.

In the example below, the Avaya SBCE will listen for SCEP requests from the endpoints on **Listen IP Port 192.168.80.50**:**1089** on network **Public B2** (the remote phones are instructed via 46xxsettings file to send SCEP requests to this IP address and port). The **Listen Transport** is set to **TLS** and **Profile**: **Outside_Server**.

The SBCE will forward the SCEP requests to the **Remote IP/FQDN Port 10.64.90.84**, port **443**, corresponding to the IP address and port of the Certificate Authority server on the enterprise network. The **Remote Transport** is set to **TLS (Profile: Inside_Client)**.

The connection to the enterprise network is achieved via the **Connected IP 10.64.91.49** interface on the **Inside A1** network.

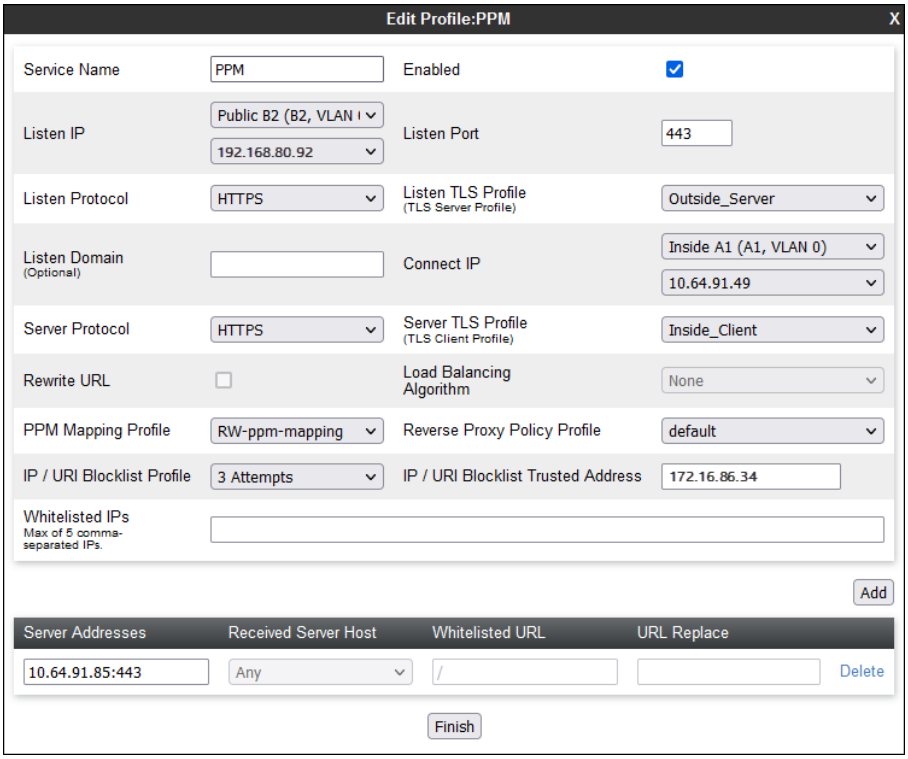


7.17.2. Reverse Proxy

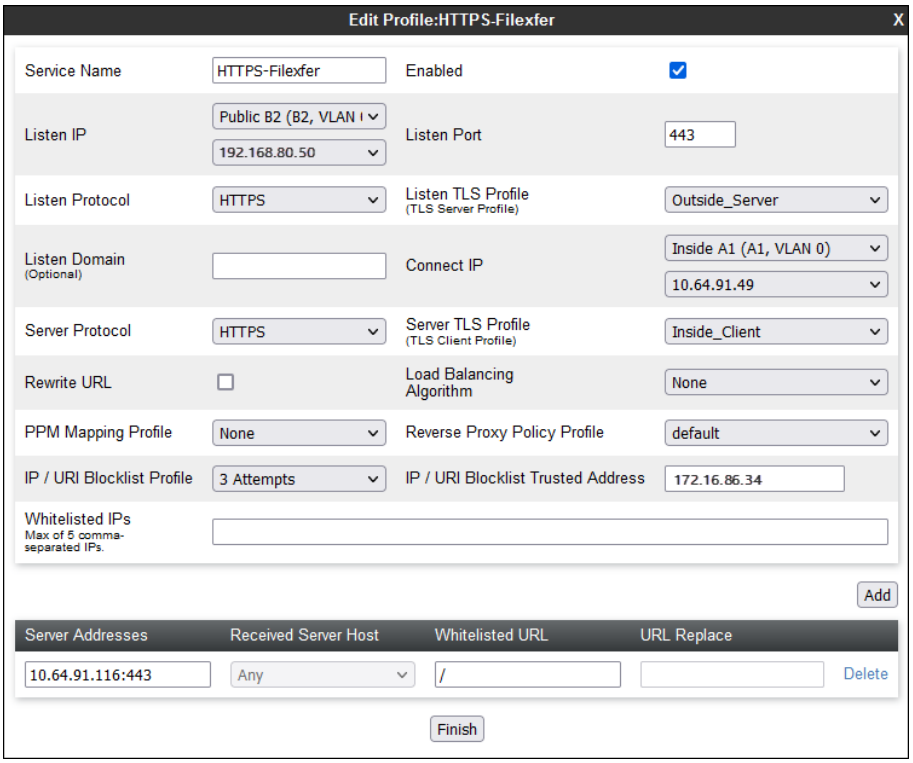
Navigate to **DMZ Services → Relay** and select the **Reverse Proxy** tab. Click **Add** to configure new Reverse Proxy policies. The following shows the Reverse Proxy policies created in the sample configuration.

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

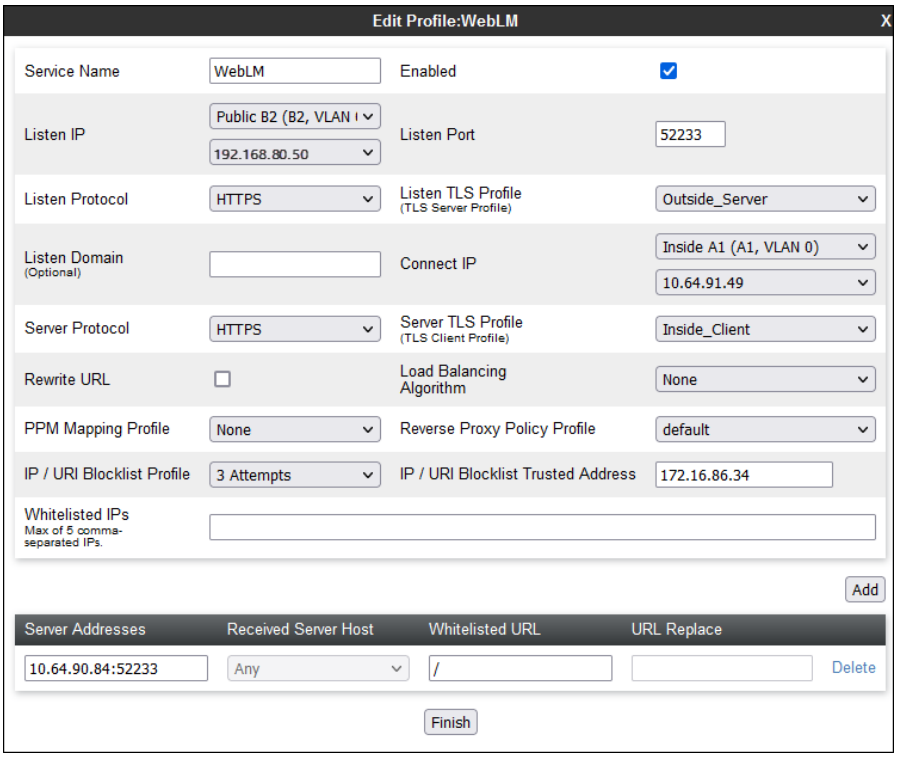
- Under **Listen IP** the **Public B2** network and the IP address of the external signaling interface configured for Remote Workers, **192.168.80.92** are selected. **Listen Port** is set to **443** and **Listen Protocol** to **HTTPS**. Under **Listen TLS Profile**, the **Outside_Server** profile is selected.
- The **Connect IP** is set to the internal IP address of the Avaya SBCE used for Remote Workers (**10.64.91.49**) on network **Inside A1**. Under **Server Protocol**, **HTTPS** is selected.
- Under **PPM Mapping Profile** select the **RW-ppm-mapping** profile previously created.
- The **Server Protocol** is set to **HTTPS** and the **Server TLS Profile** to the **Inside_Client** profile.
- Under **IP/URI Blocklist Profile**, the **3 Attempts** profile created in **Section 7.2** is selected. Under **Trusted Address**, the public address of the router/NAT at the remote location can optionally be entered.
- The **Server Address** is set to the IP address and port of Session Manager, **10.64.91.85:443**.
- Click **Finish**.



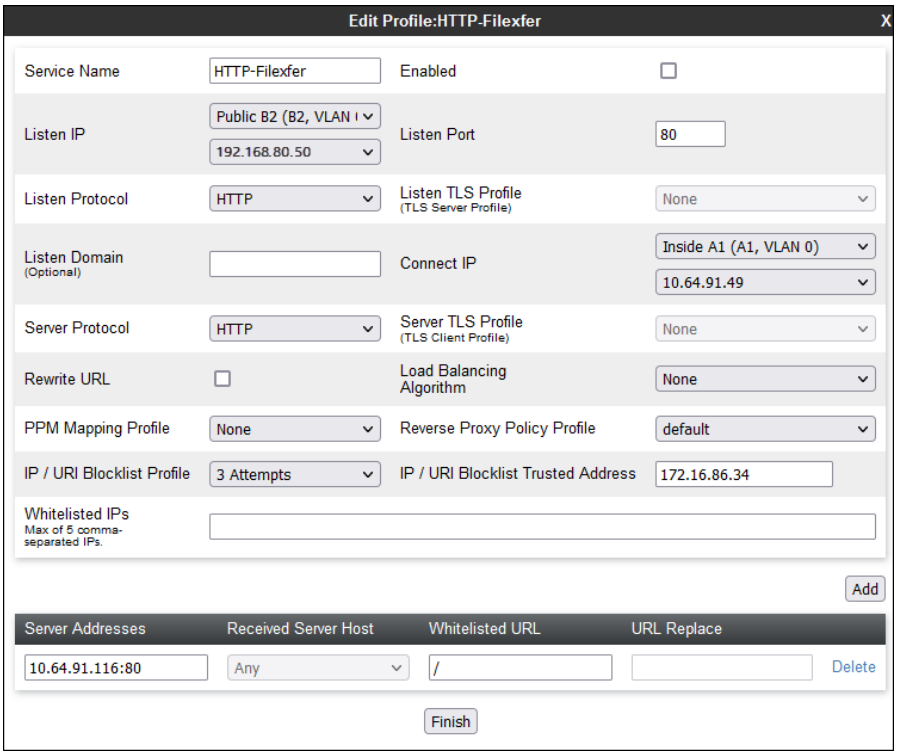
The policy named **HTTPS-Filexfer** was similarly created, used for HTTPS traffic (e.g., settings files, telephone firmware upgrades), between a Utility server at the enterprise and the remote endpoints. In this case **Listen IP** is set to **192.168.80.50**, the external Avaya SBCE IP address used for file transfers, and **Listen Port 443**. The **Server Address** is set to the IP address and port of the Utility server, **10.64.91.116:443** at the enterprise.



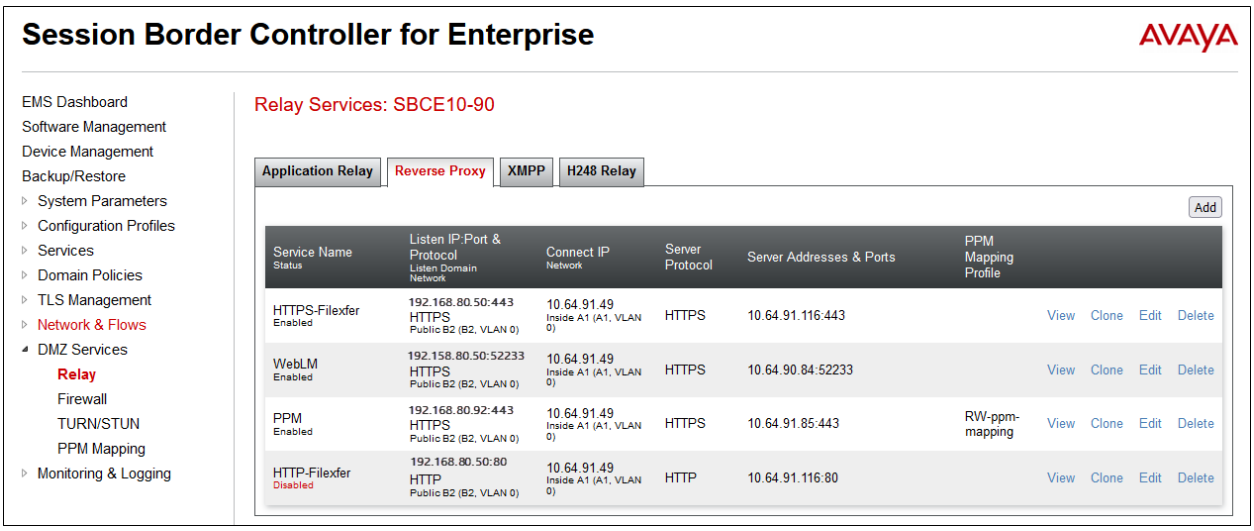
The policy named **WebLM** was created for Avaya Aura Agent for Desktop clients to be able to retrieve their licenses from a WebLM server at the enterprise. **Listen IP** is set to **192.168.80.50**, the external Avaya SBCE IP address used for file transfers. The **Listen Port** is set to **52233**. The **Server Address** is set to the IP address and port of the WebLM server at the enterprise, **10.64.90.84:52233**. See note in **Section 2.2** for limitations.



The policy named **HTTP-Filexfer** was temporarily used for testing. The **Listen IP** is set to **192.168.80.50**, the external Avaya SBCE IP address used for file transfers. The **Listen Port** is set to **80**. The **Server Address** is set to the IP address and port of the Utility server at the enterprise **10.64.91.116:80**. The policy was subsequently disabled, by unchecking the **Enabled** box.



The completed Reverse Proxy policies are shown on the screen below.



8. Avaya IP Deskphones 46xxsettings Configuration File

Although the configuration of the Remote Workers endpoints is beyond the scope of these Application Notes, a sample portion of the 46xxsettings.txt file used by Avaya SIP Deskphones is shown below, to document configuration relevant to the Avaya SBCE settings illustrated in the previous sections.

The 46xxsettings.txt file contains configuration parameters used by the Avaya IP endpoints. In the reference configuration, this file resides in the Utility file server on the enterprise network. The endpoints obtain the HTTPS Server IP address, where they need to download the settings file from, via DHCP server or by manual configuration. For the remote workers, this address is the Avaya SBCE external IP address and port configured for HTTPS file downloads, e.g. 192.168.80.50:443 in the sample configuration. The Avaya SBCE will forward the requests to the enterprise file server, by using the Reverse Proxy policy "HTTPS-Filexfer" created in **Section 7.17.2**.

Groups are used to allow configuration settings for remote IP Deskphones and core enterprise IP Deskphones on the same 46xxsettings file. In this example, Group 79 is used for the remote site group number, manually entered into the phone configuration menu.

```
IF $GROUP SEQ 79 GOTO REMO
GOTO DEFAULT

# REMO
SET SIP_CONTROLLER_LIST 192.168.80.92:5056;transport=tls
SET SIPDOMAIN avayalab.com
SET MEDIAENCRYPTION 1
SET TLSSRVRID 1
SET TRUSTCERTS SystemManagerCA.pem
SET MYCERTURL "https://192.168.80.50:1089/ejbca/publicweb/apply/scep/pkiclient.exe"
SET MYCERTCN $SERIALNO
SET MYCERTKEYLEN 2048
SET MYCERTRENEW 90
SET MYCERTWAIT 1
SET MYCERTDN /C=US/ST=CO/L=Thornton/O=Avaya/OU=SIL
SET SCEPPASSWORD $SERIALNO
GOTO ENDREMO
```

- The **IF $GROUP SEQ 79 GOTO REMO** line specifies the section of the file containing the parameters specifically used by Remote Worker endpoints. Other non-Remote Worker endpoints use the **DEFAULT** section (not shown).
- The **SIP_CONTROLLER_LIST** parameter is set to the IP addresses of the external interface on the Avaya SBCE used for Remote Worker SIP traffic.

- **MEDIAENCRYPTION** is set to **1** to specify option “aescm128-hmac80” for SRTP encryption. This matches the SRTP option configured in the Communication Manager ip-codec-set. See **Appendix A**. The default parameter is 9 (no encryption).
- **TLSSRVRID** is set to **1** (default value). This setting specifies that certificate identity match is performed. The phones will validate the validity of the certificate offered by the Avaya SBCE by matching one of the IP addresses included in the certificate Subject Alt Name with the physical IP address from where the certificate was received. For SIP over TLS, the phones will also check the domain present on the Subject Alt Name of the certificate, and match it to the domain configured on the phones, on the **SET SIPDOMAIN** line, e.g., **avayalab.com**. See **Section 5.2.1**.
- The **TRUSTCERTS** instructs the phone to download the CA trusted root certificate, e.g., **SystemManagerCA.pem** in the reference configuration. The certificate is downloaded from the Utility file server.
- The **MYCERTURL** setting is configured to direct SCEP requests to the Avaya SBCE external IP address and port (e.g., **192.168.80.50:1089**. An Application Relay is configured on the Avaya SBCE to direct the SCEP requests onto the SCEP service on the Certificate Authority server. The CA server will assign a unique identity certificate to the phone based on the serial number of the phone, according to the **MYCERTCN** setting. Consult **References 6-7** for details on other “MYCERT” parameters, related to the SCEP certificate requests.

9. Verification Steps

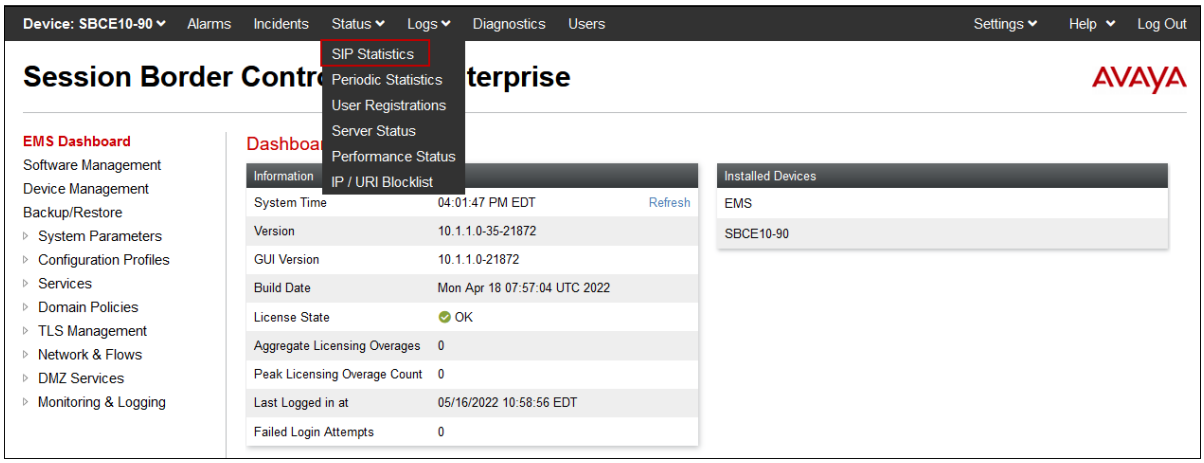
This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

9.1. Avaya Session Border Controller for Enterprise Verification

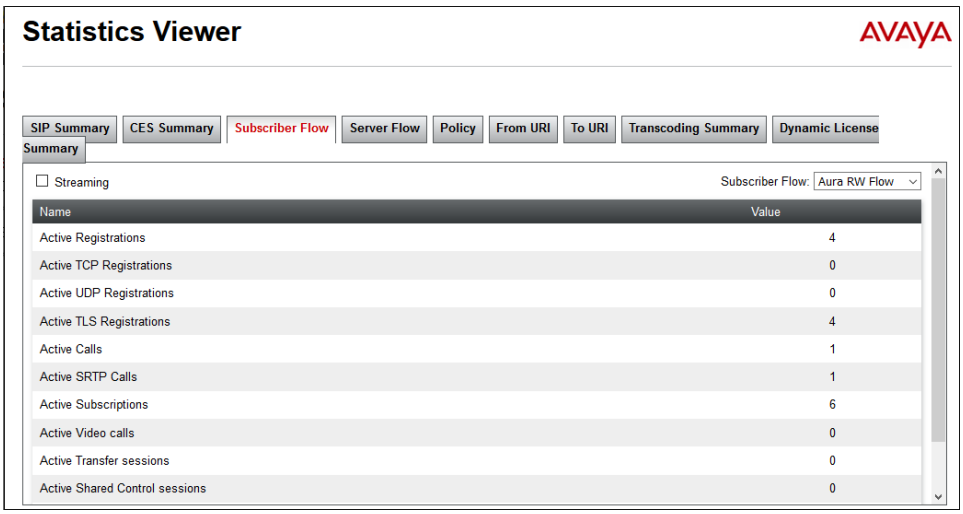
This section contains verification steps that may be performed using Avaya Session Border Controller for Enterprise.

9.1.1. Statistics Viewer

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

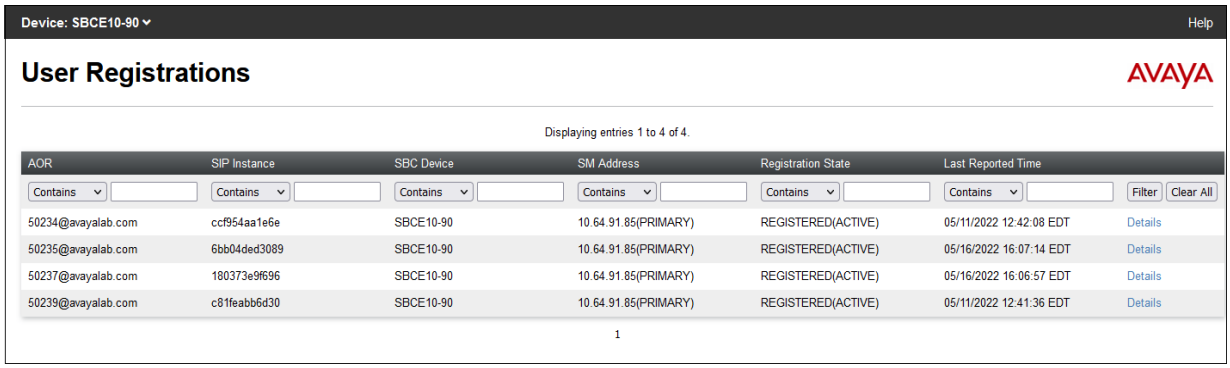


The **Subscriber Flow** tab on the **Statistics Viewer** will show **Active Registrations, Active Calls** and other information about subscribers on the selected flow.

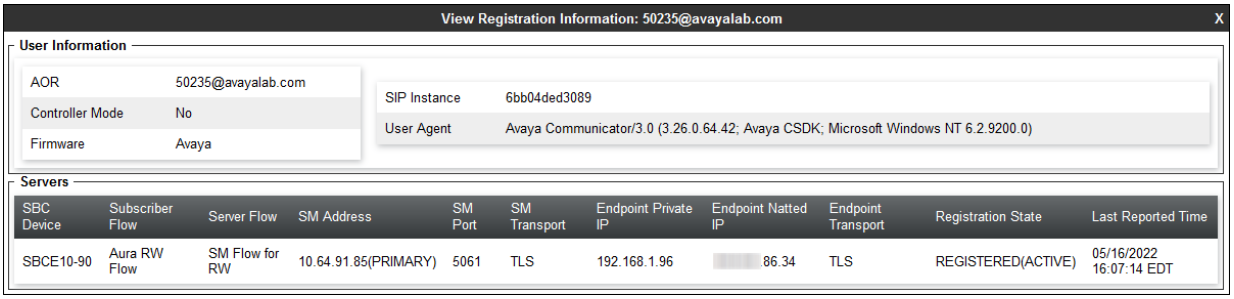


9.1.2. User Registrations

The **User Registrations** screen can be accessed from the Avaya SBCE top navigation menu also under the **Status** menu (not shown). The screen displays the list of endpoints registered through the Avaya SBCE with details for each registration.

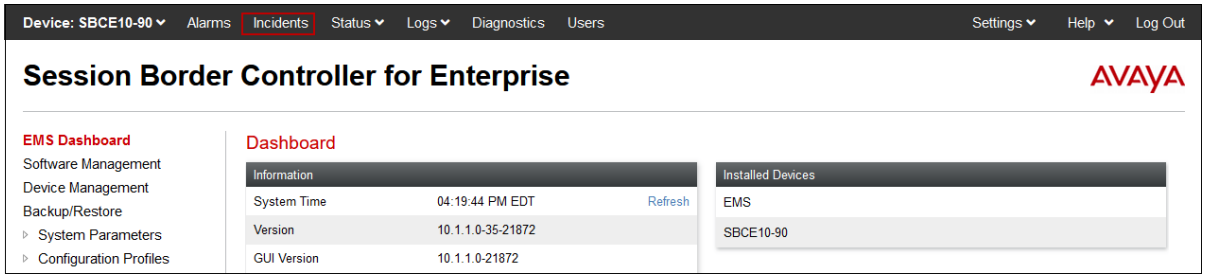


Additional endpoint information can be obtained clicking the **Details** link for a specific user. On the screen below, the **Endpoint Natted IP** is blurred for security reasons:

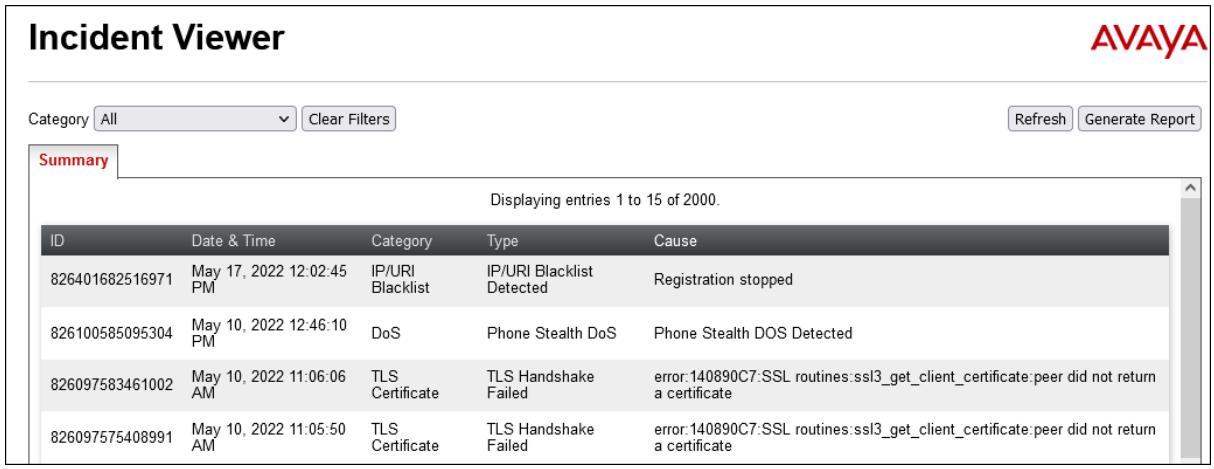


9.1.3. Incidents Viewer

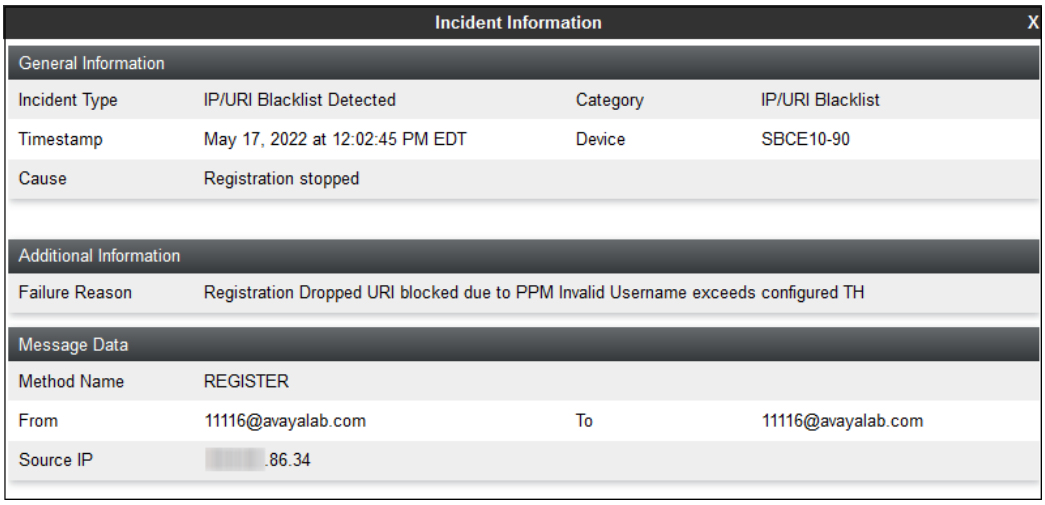
The **Incident Viewer** can be accessed from the top navigation menu as highlighted in the screenshot below.



Use the **Incident Viewer** to troubleshoot policies issues, TLS handshake and other failures.



Further Information can be obtained by clicking on an incident in the incident viewer.

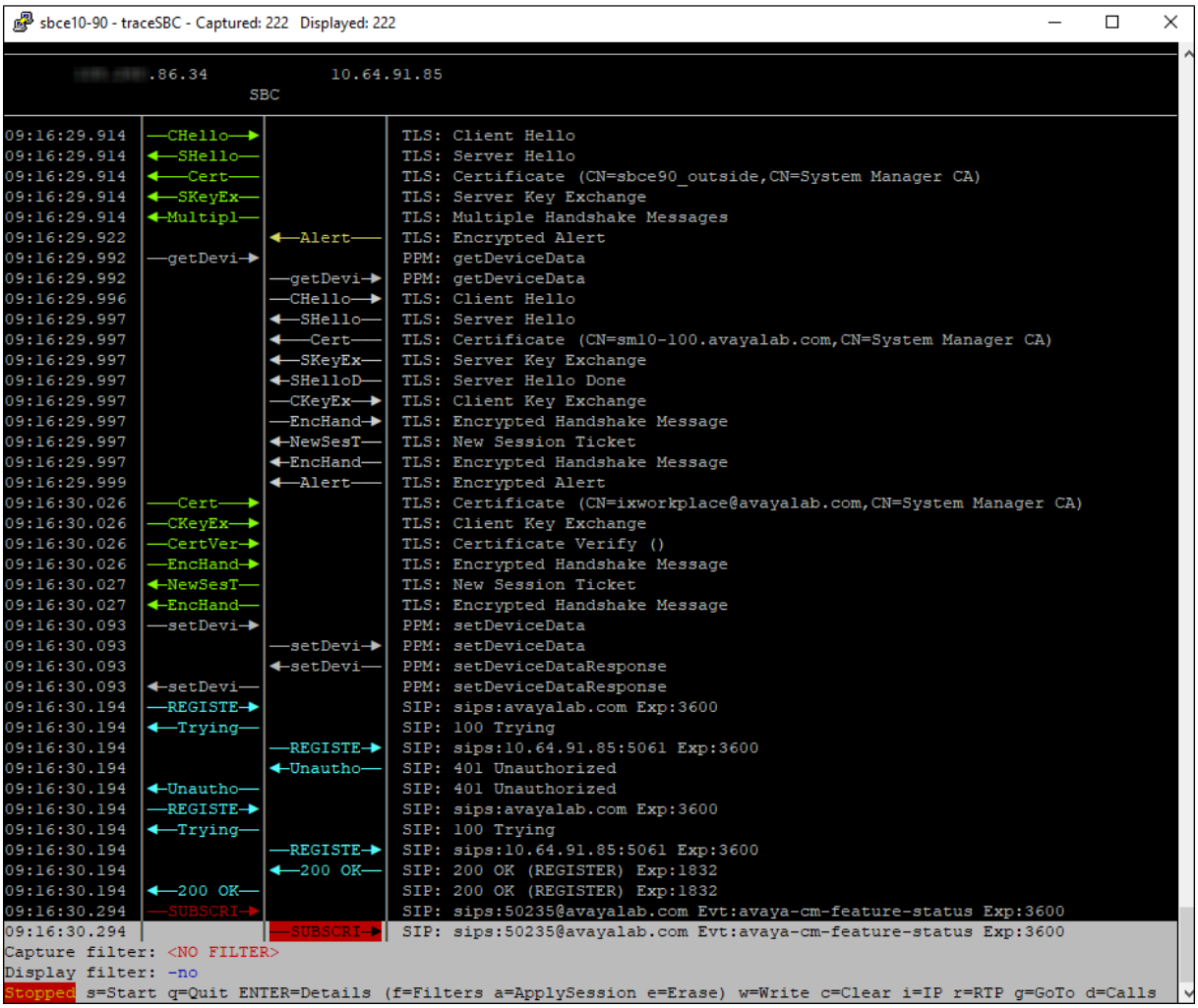


9.1.4. traceSBC Tool

Since the IP traffic in Remote Workers configurations is normally encrypted, 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.

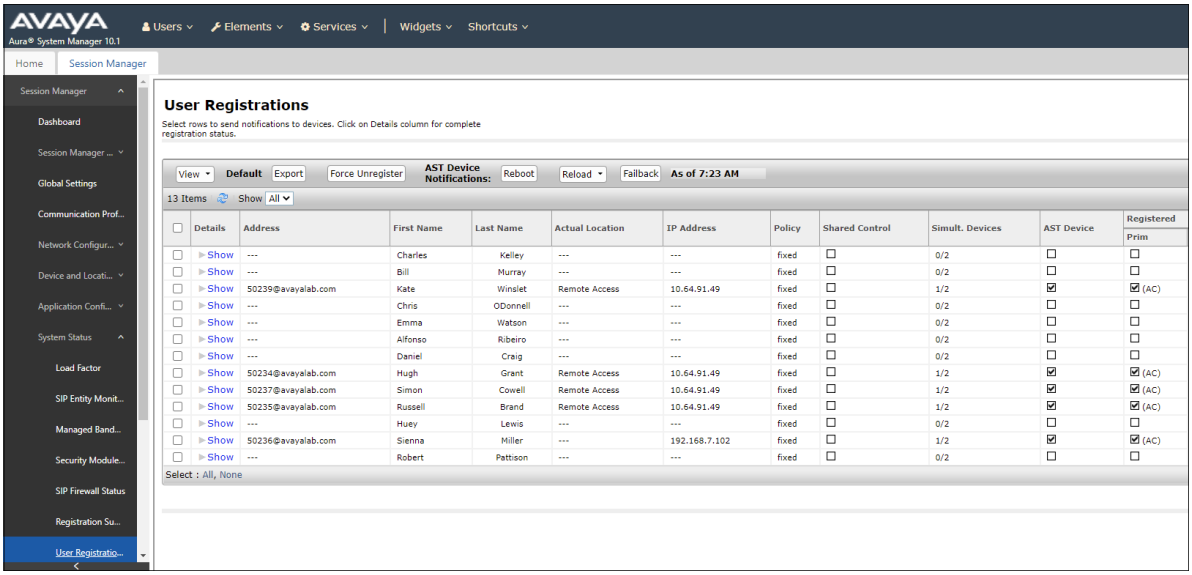
To run the traceSBC tool, log into SBCE command line interface using SSH client as user **ipcs**. Issue the command **sudo su** to change to **root** user. Start the tool by issuing the **traceSBC** command.



9.2. 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., 10.64.91.49 as shown below.



Another Session Manager useful verification and troubleshooting tool is **traceSM**.

traceSM is the Session Manager command line tool for traffic analysis. Login to the Session Manager command line management interface to run this command. This tool can be used to monitor SIP packets from the Avaya SBCE to Session Manager and can also be used to verify PPM information is exchanged successfully between the remote user and Session Manager.

10. Conclusion

The sample configuration presented in these Application Notes describe the procedures necessary to support Remote Workers, using Avaya Session Border Controller for Enterprise 10.1 on the Avaya Aura® Platform.

Testing was performed to verify SIP registration and basic functionalities in audio calls for the remote endpoints. Calls were placed to and from the Remote Workers residing outside of the enterprise, across the public internet, to various Avaya endpoints located at the enterprise, as described in **Section 2.1**.

11. Additional References

[1] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, December 2021

[2] *Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise*, Release 10.1.x., December 2021

[3] *Avaya SBCE 8.1 Security Configuration and Best Practices Guide*, Release 8.1, February 2020

[4] *Administering Avaya Aura® Session Manager*, Release 10.1.x, April 2022

[5] *Avaya Aura® Session Manager Security Design*, Release 10.1.x, December 2021

[6] *Installing and Administering Avaya 9601/9608/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Release 7.1.15, April 2022

[7] *Installing and Administering Avaya J100 Series IP Phones in Avaya Aura®*, Release 4.0.12, April 2022

[8] *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac and Windows*, June 2021

[9] *Deploying and configuring Avaya Agent for Desktop*, Release 2.0.6.20, April 2022

[10] *Using Avaya Agent for Desktop*, Release 2.0.6, September 2020

[11] *Application Notes for Configuring Remote Workers with Avaya Session Border Controller for Enterprise 8.1 on the Avaya Aura® Platform* – Issue 1.0, February 2021

12. Appendix A. Communication Manager ip-codec-set

The screen below shows the Communication Manager **change ip-codec-set 1** screen, as used in the reference configuration.

This IP-codec-set is used for calls within the enterprise, in addition to calls to/from the Remote Workers. Under Media Encryption, the first option is selected as **1-srtp-aescm128-hmac80** for SRTP. The second option is set to **none** (no encryption), to support devices within the enterprise that do not support SRTP.

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

                        IP MEDIA PARAMETERS
   Codec Set: 1

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.722-64K                  2        20
 2: G.711MU           n        2        20
 3: G.729A            n        2        20
 4: G.729B            n        2        20
 5:
 6:
 7:

    Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
```

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 Solution & Interoperability Test Lab at interopnotesdl@avaya.com