Avaya Solution & Interoperability Test Lab

Application Notes for configuring MiaRec with Avaya IP Office and Avaya Session Border Controller for Enterprise - Issue 1.0

Abstract

These Application Notes describe the steps used to configure SIP-based Media Recording (SIPREC) between MiaRec and an Avaya SIP enabled Enterprise Solution. The Avaya platform consisted of Avaya IP Office and Avaya Session Border Controller for Enterprise.

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps used to configure SIP-based Media Recording (SIPREC) between MiaRec and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of the following:

- Avaya IP Office solution (IP Office)
- Avaya Session Border Controller for Enterprise (Avaya SBCE)

IP Office solution consisted of IP Office Server Edition and IP Office 500v2.

MiaRec is a call recording and quality management solution. Using the SIPREC interface of Avaya SBCE, MiaRec provides centralized call recording solutions for the enterprises that use SIP trunking services and Remote Workers.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of IP Office and Avaya SBCE. The enterprise site was configured to connect to a simulated service provider's SIP trunking service. MiaRec recorded calls to/from the enterprise site using the SIPREC interface on the Avaya SBCE. Calls were placed to and from IP Office via Avaya SBCE; Remote Worker and SIP trunk.

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and MiaRec did not include use of any specific encryption features as requested by MiaRec.

2.1. Interoperability Compliance Testing

The interoperability test included the call recording scenarios for the following:

- Recording of incoming calls to the enterprise site from simulated service provider SIP trunk, calls made to SIP and H.323 telephones at the enterprise.
- Recording of outgoing calls from the enterprise site to remote destinations through the simulated service provider SIP trunking service, calls made from SIP and H.323 telephones.
- Recording of incoming and outgoing calls to/from SIP Remote Worker.
- Recording of calls using the G.711U and G.729A codecs.
- Recording of call scenarios involving the user features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID and DNIS presentation of recorded calls.
- Recording of call scenarios involving the call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent to MiaRec.
- Call recordings using combination of SIP (TCP) and RTP (UDP).

Serviceability tests were performed to test MiaRec's ability to recover from adverse conditions, such as, server reboot and network connectivity loss.

Note that, testing of audio quality of the call recording was not part of the test.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the MiaRec solution with the following observations:

- Certain conference calls and transfer calls initiated from Remote Worker, resulted in duplicate recording on MiaRec. This is due to Avaya SBCE sending separate streams to MiaRec for each call leg.
- Calls placed via SIP trunk to Remote Workers resulted in duplicate call recordings. This due to Avaya SBCE sending separate streams for each call leg; one for the SIP trunk and another for Remote Worker.

2.3. Support

For technical support on MiaRec products please contact MiaRec.
Email: support@miarec.com
Phone: 866-324-6717
Web: www.miarec.com

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the simulated SIP trunking service through the Avaya SBCE. Located at the Enterprise site is an Avaya IP Office environment, Avaya Session Border Controller for Enterprise and MiaRec server. Endpoints are Avaya 9600 series, Avaya 1100 Series IP Deskphones and Avaya one-X® Communicator. The Remote Workers are connecting to the Enterprise site through Avaya SBCE.

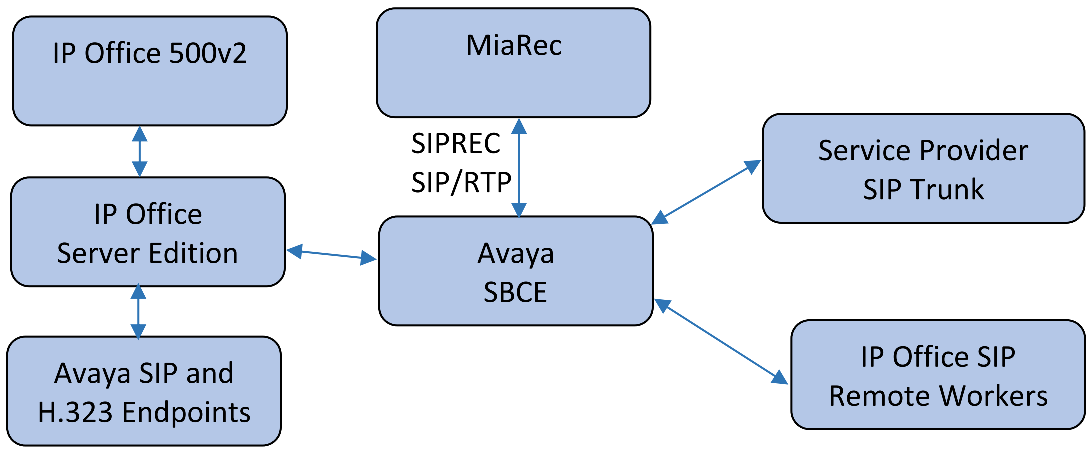


Figure 1: Test Setup MiaRec with Avaya Enterprise

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya IP Office Server Edition	11.0.0.2.0 build 23
Avaya IP Office 500v2	11.0.0.2.0 build 23
Avaya IP Office Manager	11.0.0.2.0 build 23
Avaya Session Border Controller for Enterprise	7.2.2.0
Avaya 96x1 IP Deskphone (H.323)	6.7104
Avaya J169 IP Deskphone (SIP)	3.0.0.2.2
Avaya 1100 IP Deskphone (SIP)	4.4 SP10
Avaya one-X® Communicator (SIP)	6.2 SP13
MiaRec: Web Portal Recorder	 7.0.0.107 7.0.0.10

5. Configure Avaya IP Office

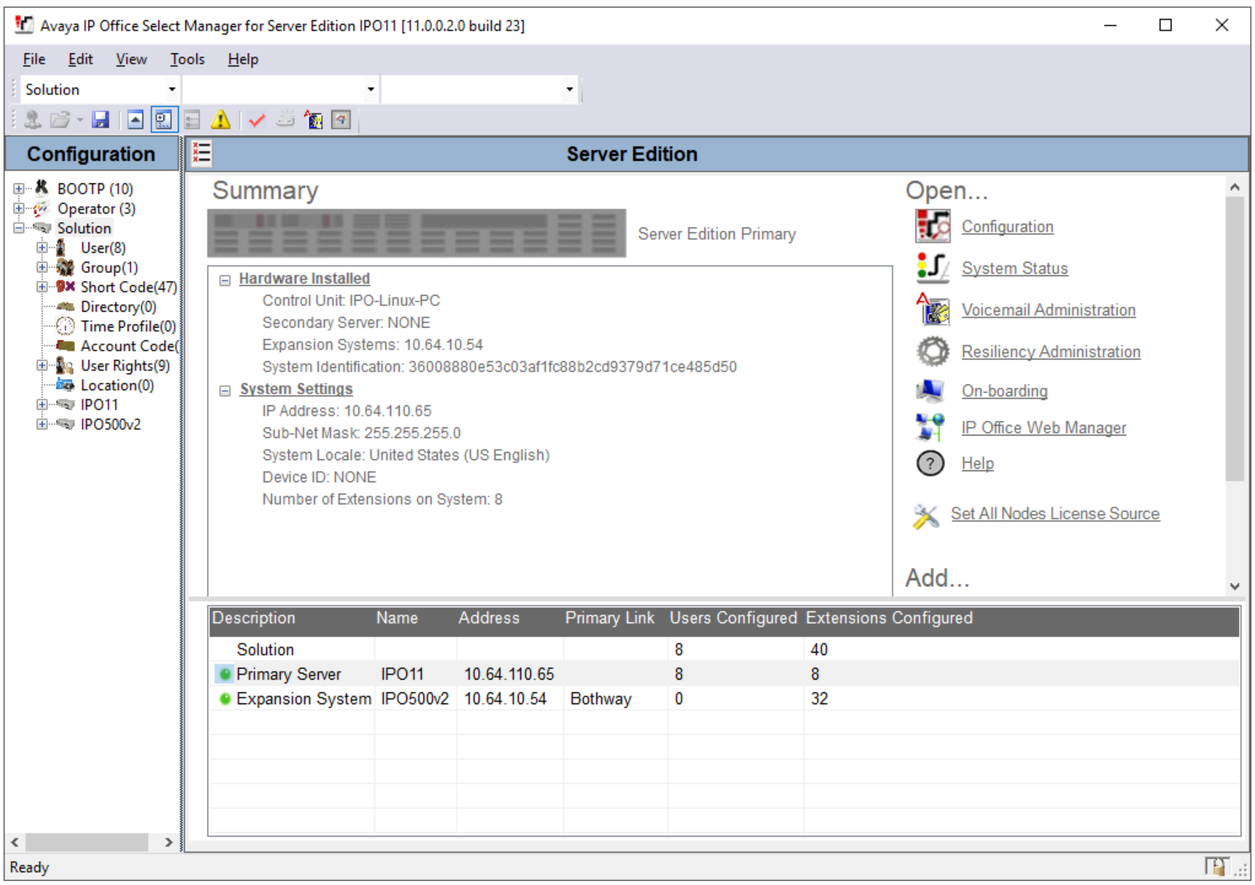
This section provides the procedures for configuring Avaya IP Office. The procedures include the following areas:

- Verify IP Office license
- Configure System
- Configure SIP Line

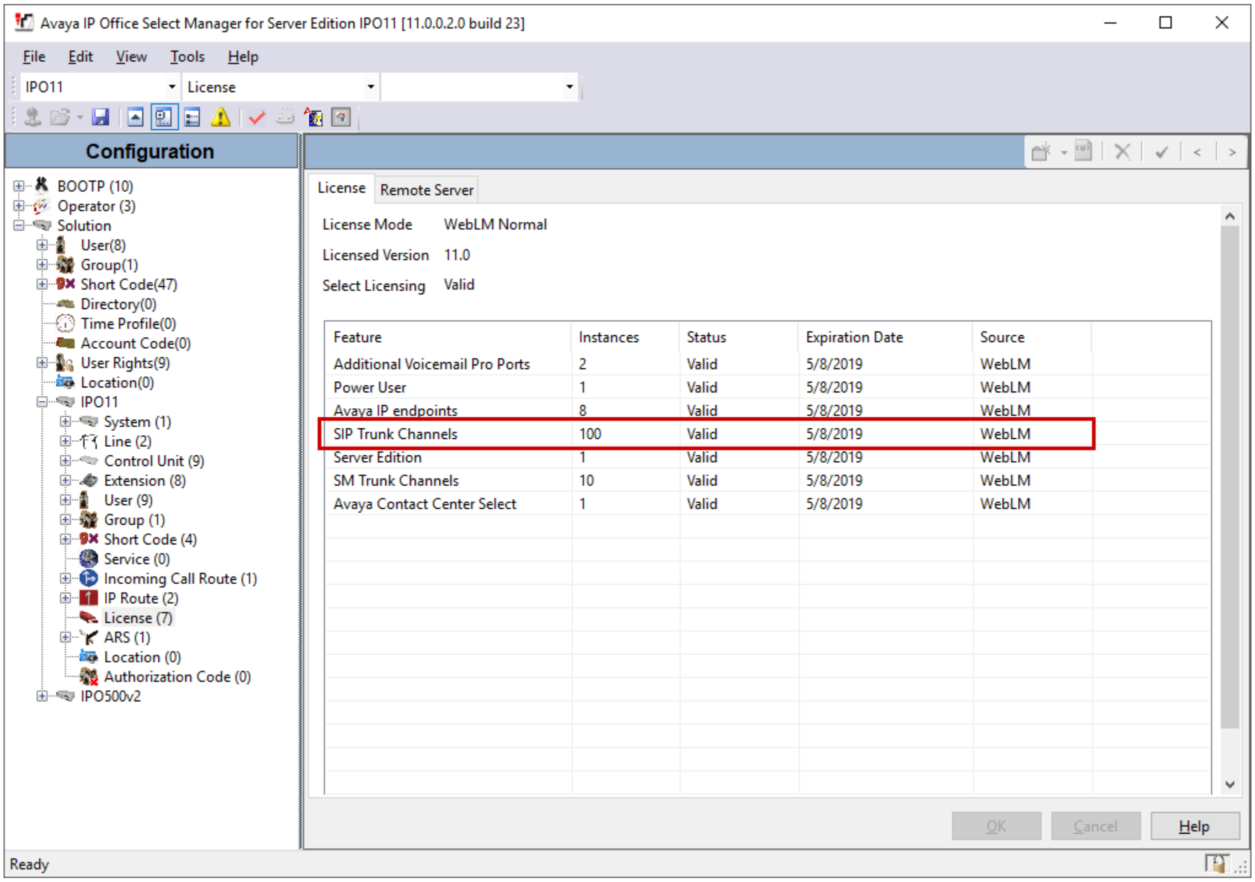
5.1. Verify IP Office License

From a PC running the Avaya IP Office Manager application, select **Start → IP Office → Manager** to launch the Manager application. Select the proper Avaya IP Office system and log in with the appropriate credentials.

The **Avaya IP Office Manager for Server Edition** screen is displayed.

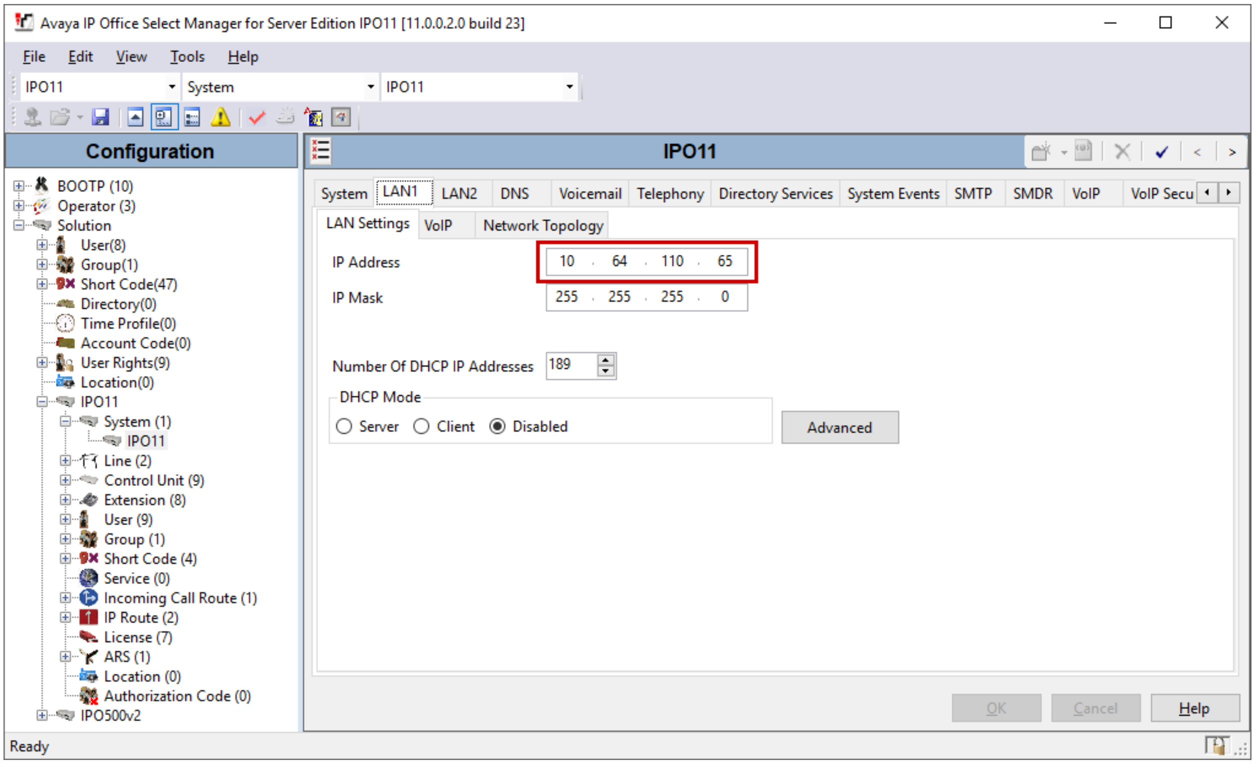


From the configuration tree in the left pane, expand IP Office Server Edition, **IPO11** in this case. Select **License** to display the license screen in the right pane. Verify that the **Status** for **SIP Trunk Channels** is "Valid" and has enough instances.

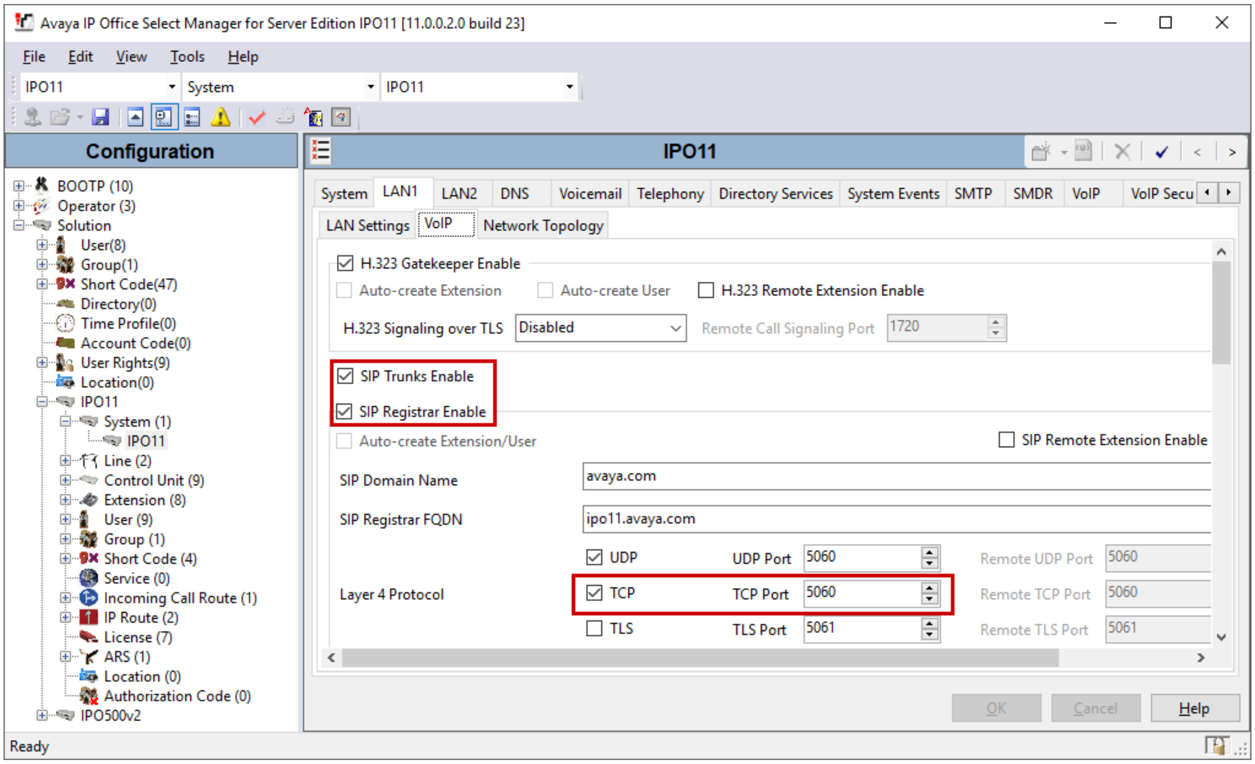


5.2. Configure System

From the configuration tree in the left pane, select **System** to display the **System** screen for the Avaya IP Office Server Edition in the right pane. Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later to configure Avaya SBCE.



Select the **VoIP** sub-tab. Ensure that **SIP Trunks Enable,** and **SIP Registrar Enable** boxes are checked. Also, ensure that **TCP** is enabled as shown below.



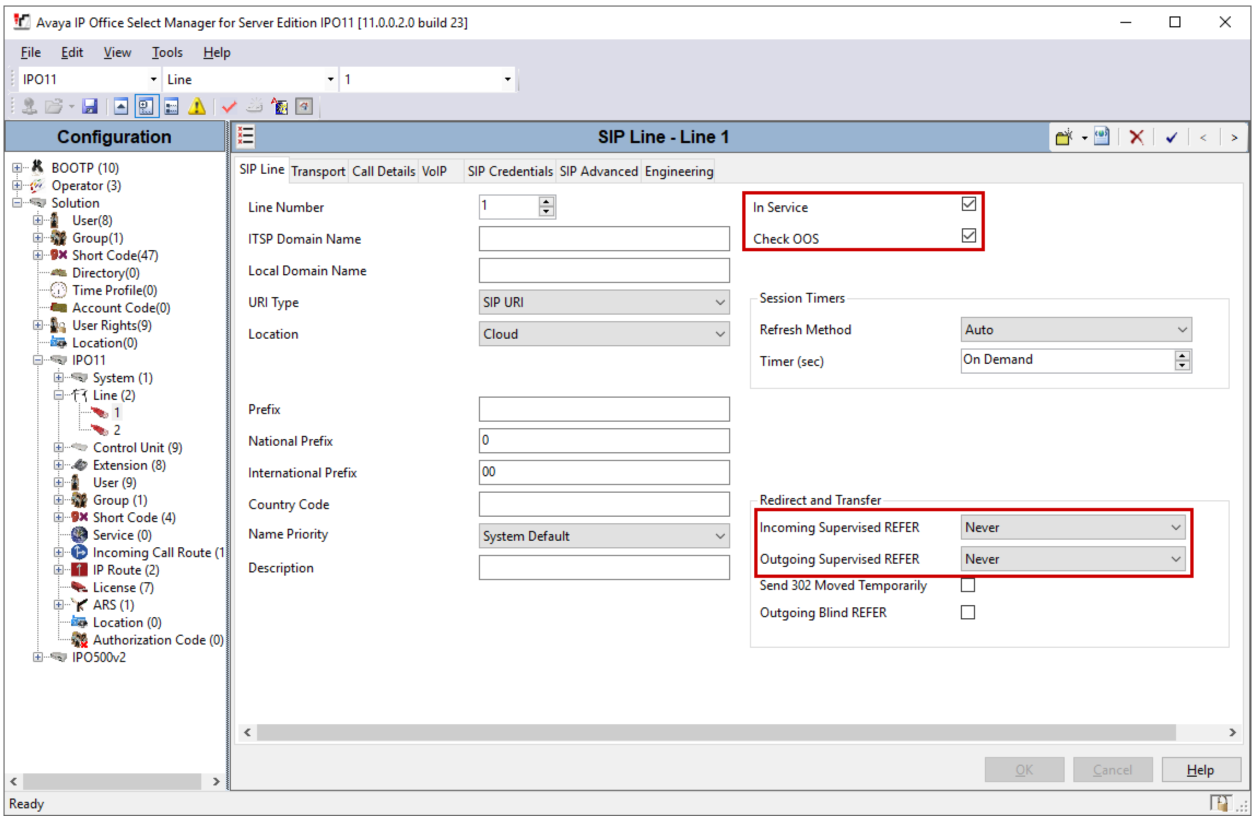
5.3. Configure SIP Line

A SIP line is needed to establish the SIP connectivity between IP Office and Avaya SBCE. From the configuration tree in the left pane, right-click on **Line** and select **New→ SIP Line** from the pop-up list to add a new SIP line (not shown). The **SIP Line** tab is displayed.

5.3.1 SIP Line – SIP Line Tab

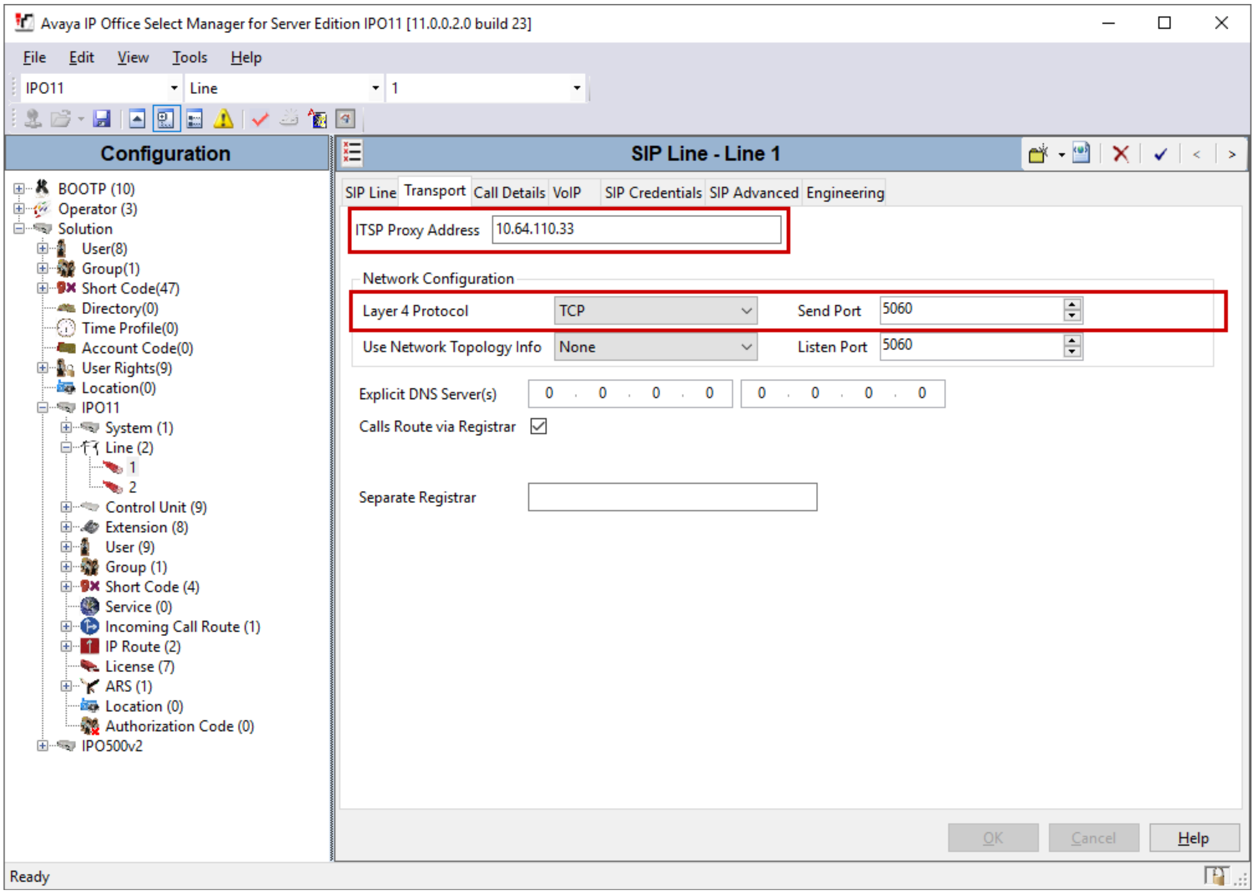
Set both **Incoming Supervised REFER** and **Outgoing Supervised REFER** to "Never". Check boxes for **In Service** and **Check OOS**.

Retain the default values in the remaining fields.



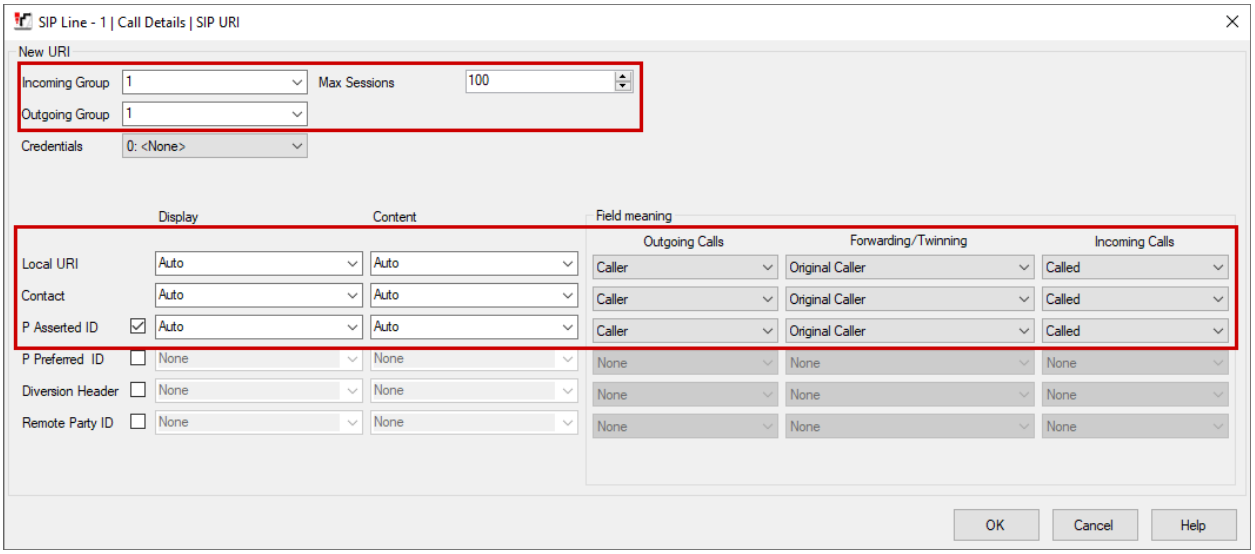
5.3.2 SIP Line – Transport Tab

Select the **Transport** tab in the right pane. For **ITSP Proxy Address**, enter the IP address of Avaya SBCE from **Section 6.2**. For **Layer 4 Protocol**, select "TCP", and set **Send Port** to "5060".



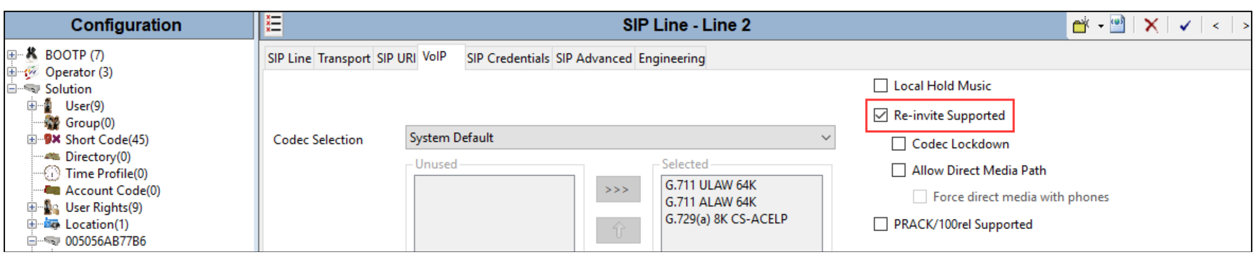
5.3.3 SIP Line – Call Details

Select the **Call Details** tab, and click **Add** to display the **SIP URI** window. Set **Incoming Group** and **Outgoing Group** to an available **Group** number. Set **Max Sessions** according to customer requirements. Configure the fields as shown below and retain the default values for the remaining fields.

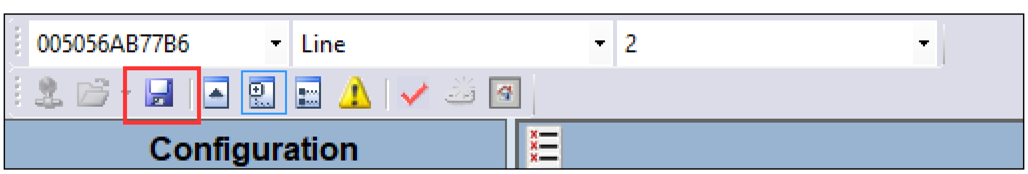


5.3.4 SIP Line – VoIP Tab

Select the **VoIP** tab, and check box for **Re-invite Supported**. Retain the default values for the remaining fields.



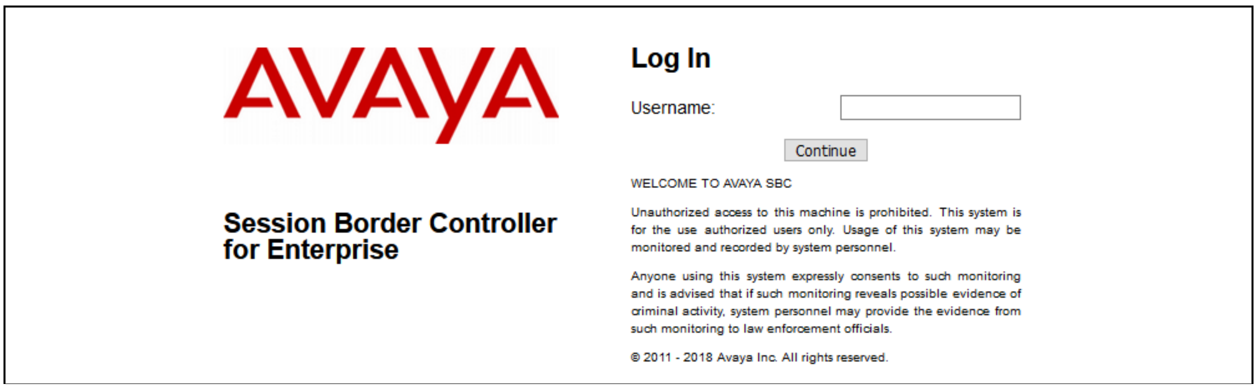
Once done click Save to save the configuration on Avaya IP Office.



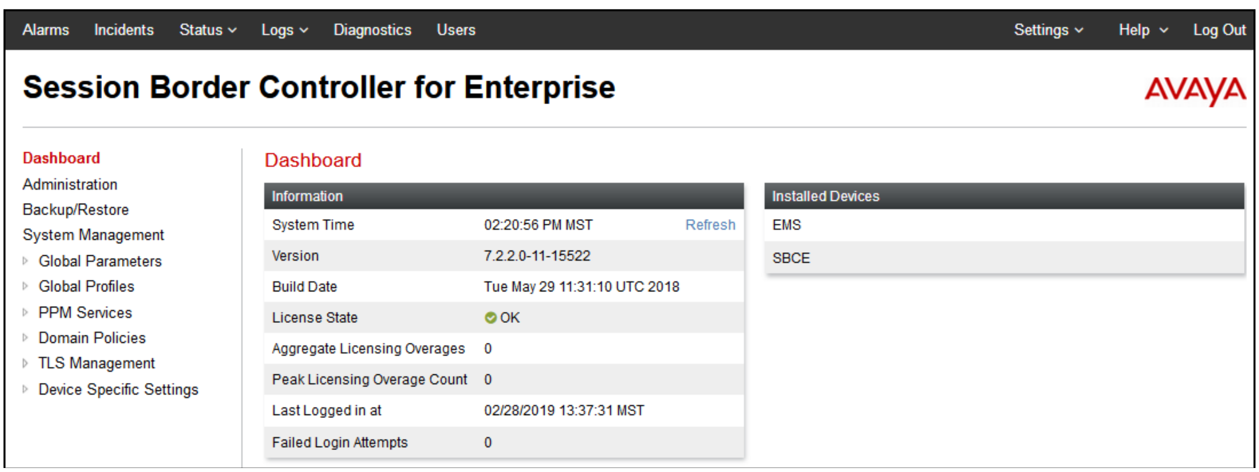
6. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP trunk and IP Office Remote Workers. Avaya SBCE also provides the SIPREC interface that is used by MiaRec to record calls. Note that configuration for service provider SIP trunk is not shown is this section as such configuration can vary.

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



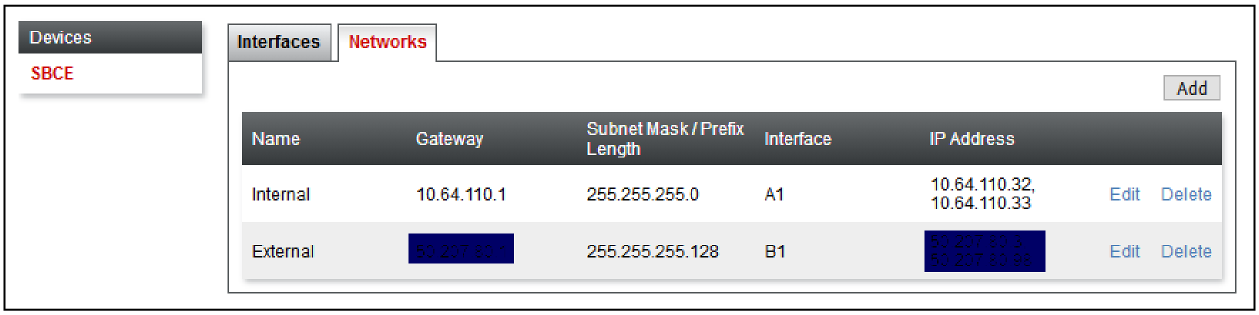
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



6.1. Define Network Management

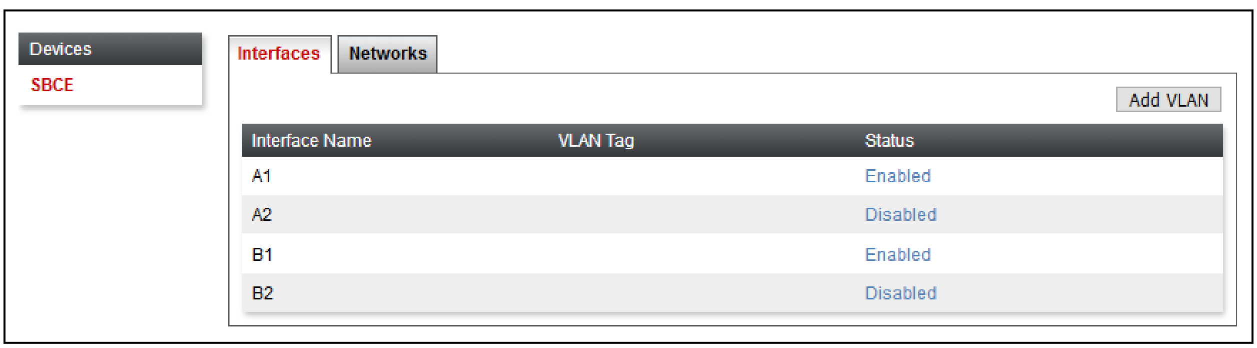
Network information is required on the Avaya SBCE to allocate IP addresses and subnet masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one physical interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the main menu on the left hand side and click on **Add**. The following interfaces were added for IP Office SIP trunk, IP Office Remote Workers and simulated service provider's SIP trunk. 10.64.110.32 was used for Remote Workers SIP Registrations to IP Office and for MiaRec, while 10.64.110.33 was used for SIP trunk to IP Office



Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address		
Internal	10.64.110.1	255.255.255.0	A1	10.64.110.32, 10.64.110.33	Edit	Delete
External	[redacted]	255.255.255.128	B1	[redacted]	Edit	Delete

Select the **Interfaces** tab and click on the **Status** of the physical interface to toggle it. A status of **Disabled** will be changed to **Enabled**.



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

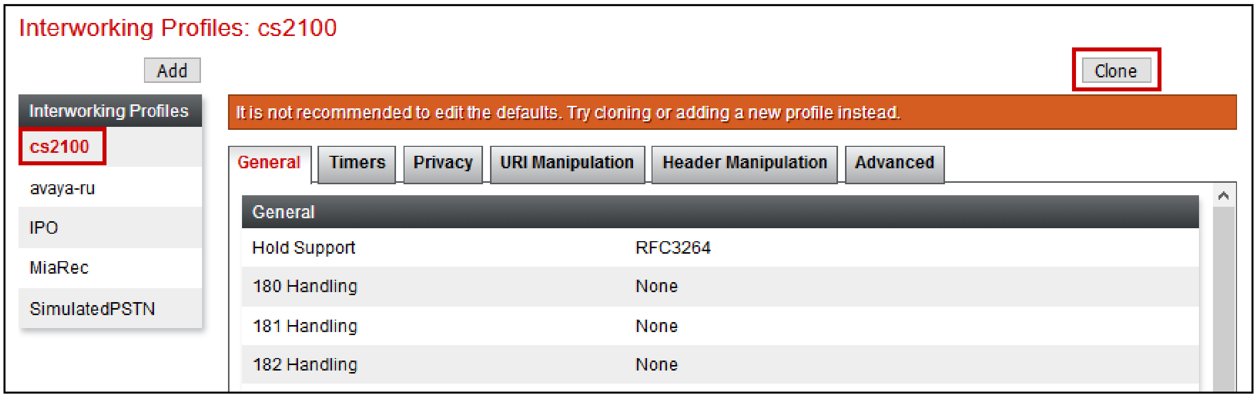
Note: to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).

A status box will appear (not shown) that will indicate when the application has restarted.

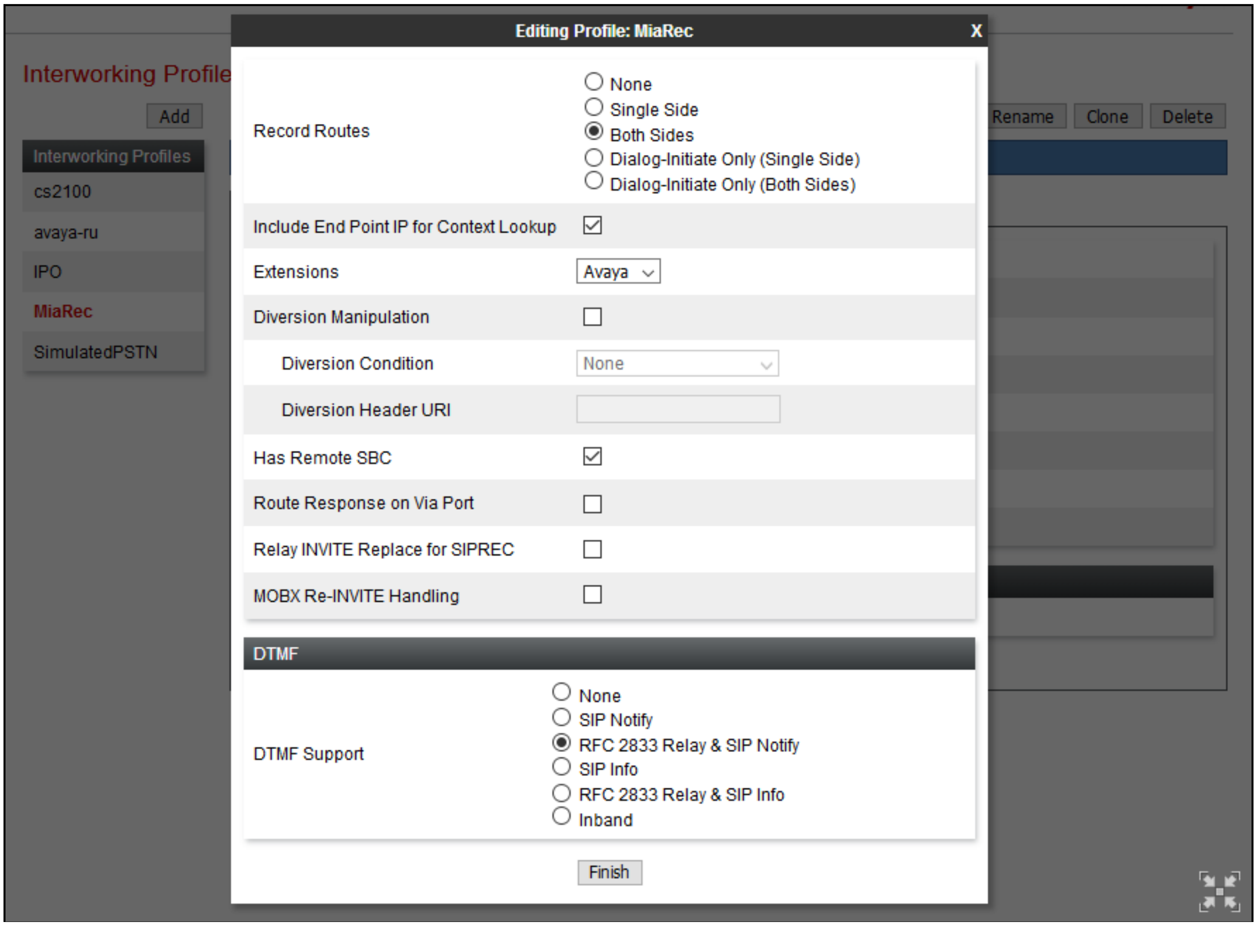
6.2. Access Avaya Session Border Controller for Enterprise

A Server Interworking profile needs to be created for MiaRec and IP Office SIP trunks. To define a new Server Interworking profile, navigate to **Global Profiles → Server Interworking**. Select the **cs2100** profile and select **Clone**.



Type in a name for profile and select **Finish.**

Select the recently created profile and edit the **Advanced** options. Set the **Extensions** to **Avaya**.

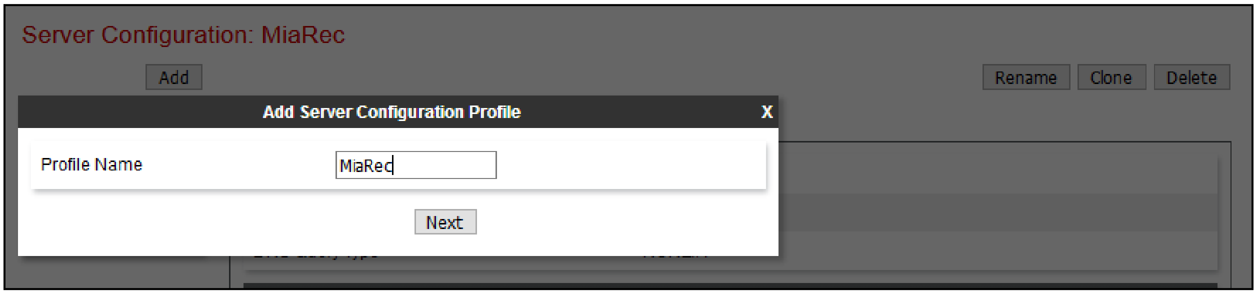


Similarly, create another Server Interworking profile for IP Office.

6.3. Define Servers

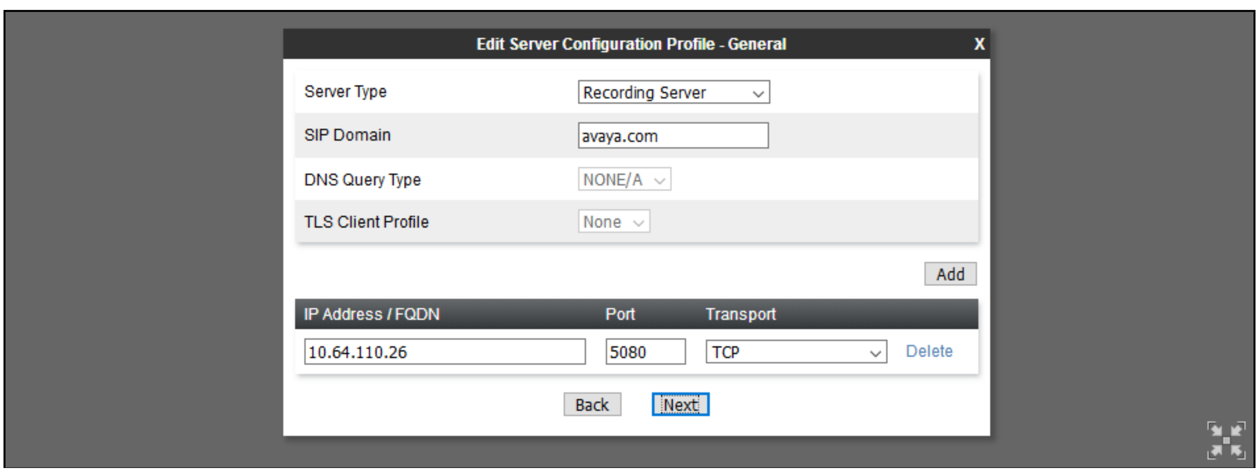
A server definition is required for each server connected to the Avaya SBCE. In this case, the MiaRec is configured as a **Recording Server** and two IP Office servers are configured as a **Trunk Server** and **Call Server**, respectively. **Trunk Server** is used for SIP trunk call recording and **Call Server** is used for Remote Workers call recording.

To define the MiaRec Recording Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.

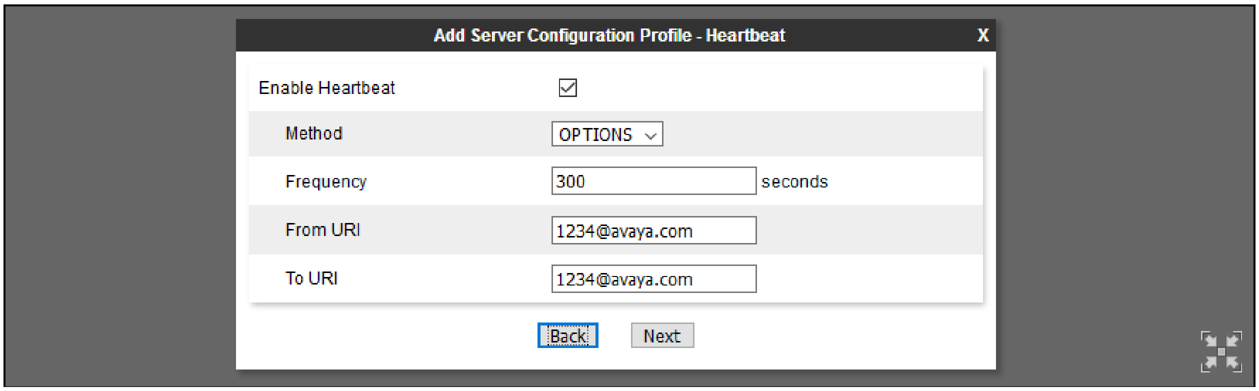


Click on **Next** and enter details in the dialogue box.

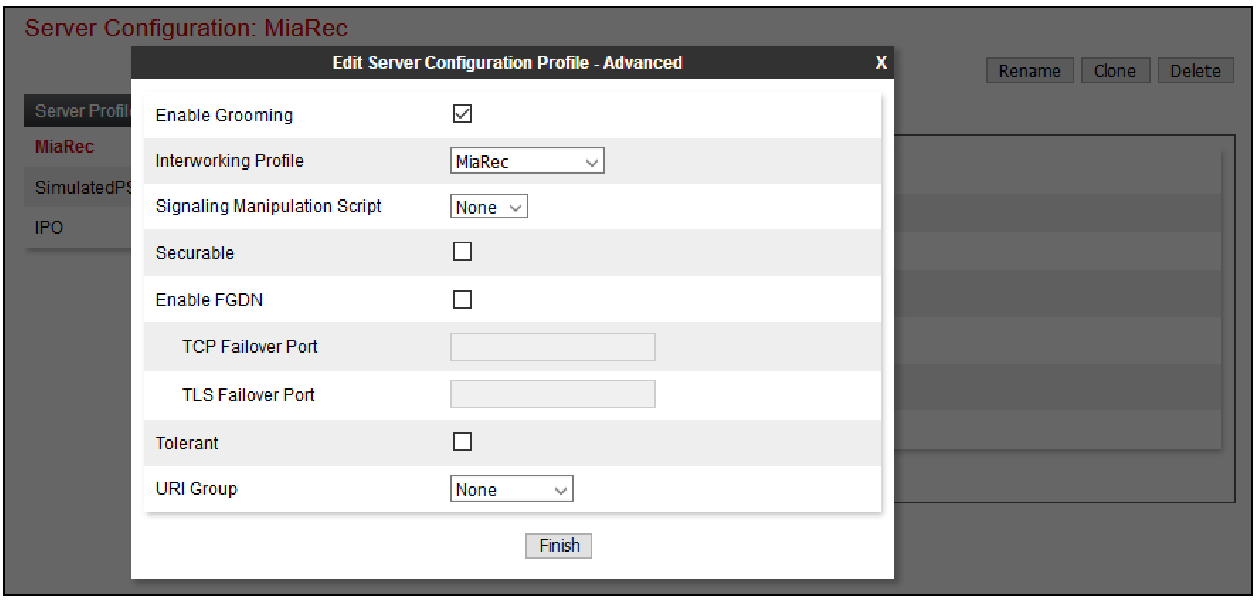
- In the **Server Type** drop down menu, select **Recording Server**.
- In the **SIP Domain** type in the domain used in the environment.
- Click on **Add** to enter an IP address.
- In the **IP Addresses / FQDN** box, type the MiaRec recording server interface address.
- In the **Port** box, enter the port to be used for the listening port configured on the MiaRec from **Section 7**.
- In the **Transport** drop down menu, select **TCP**.
- Click on **Next**.



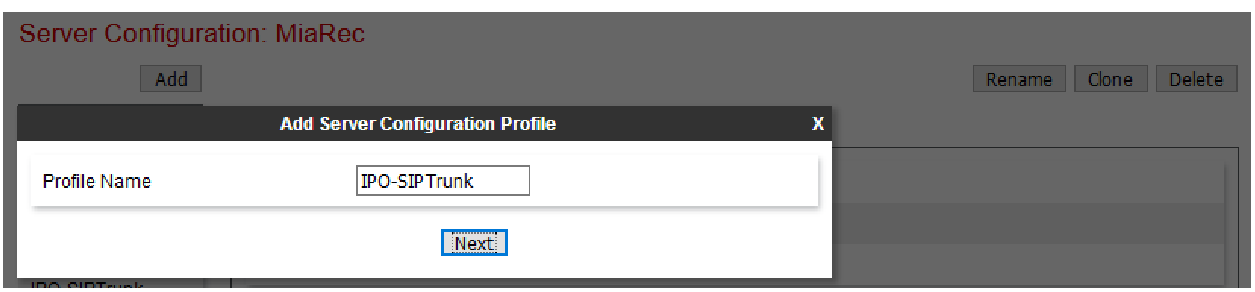
Click on **Next** and configure **From URI** and **To URI** as follows. Instead of a domain, an IP Address can also be used in the URI.



Select **Next** and select the **Interworking Profile** configured in previous section for MiaRec. Select **Finish** once done.

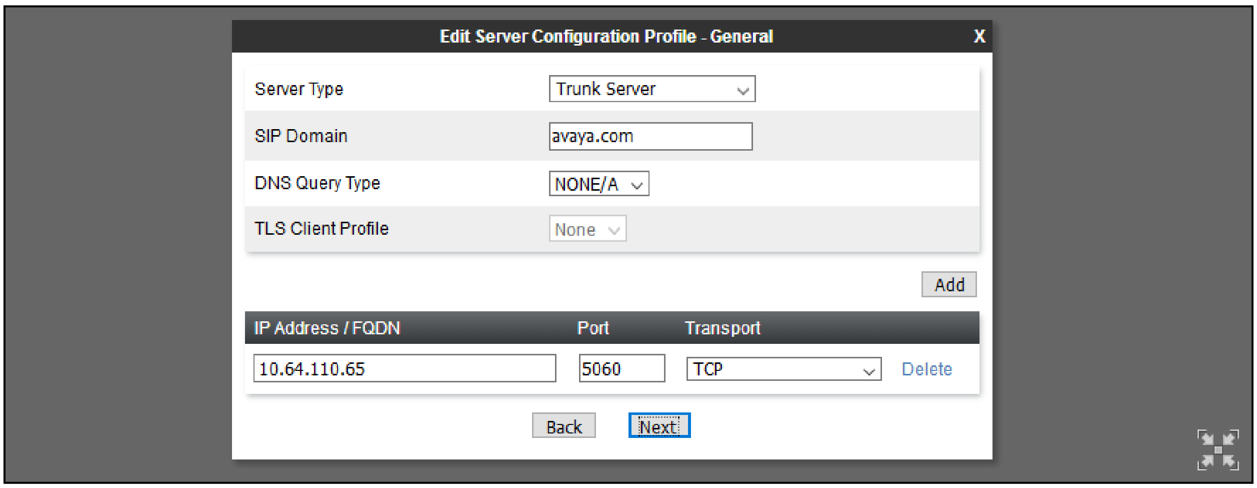


To define a Server for IP Office, click on **Add** and enter an appropriate name in the pop-up menu.

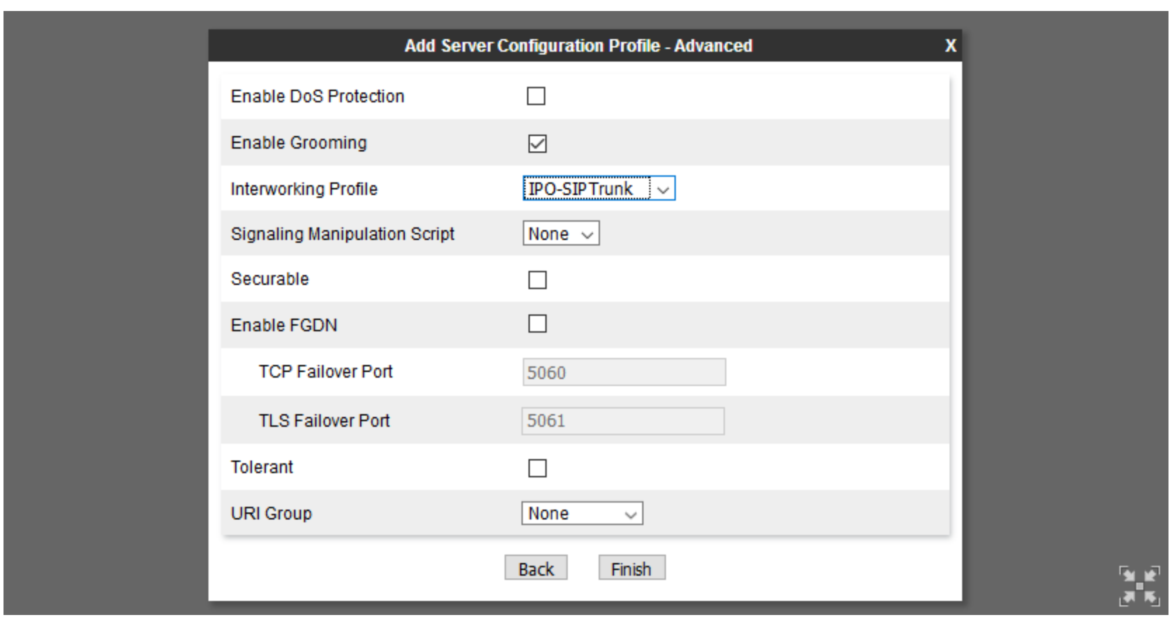


Click on **Next** and enter details in the dialogue box.

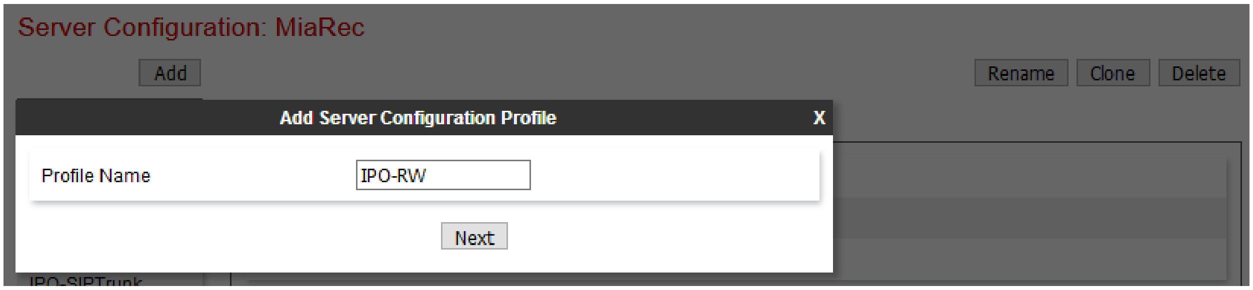
- In the **Server Type** drop down menu, select **Trunk Server**.
- In the **SIP Domain** type in the domain used in the environment.
- Click on **Add** to enter an IP address.
- In the **IP Addresses / FQDN** box, type the IP Address from **Section 5.2**.
- In the **Port** box, enter the port to be used for the listening port configured on the IP Office from **Section 5.3.2**.
- In the **Transport** drop down menu, select **TCP**.
- Click on **Next**.



Select **Next** and configure the **Interworking Profile** configured in previous section for IP Office. Select **Finish** once done.

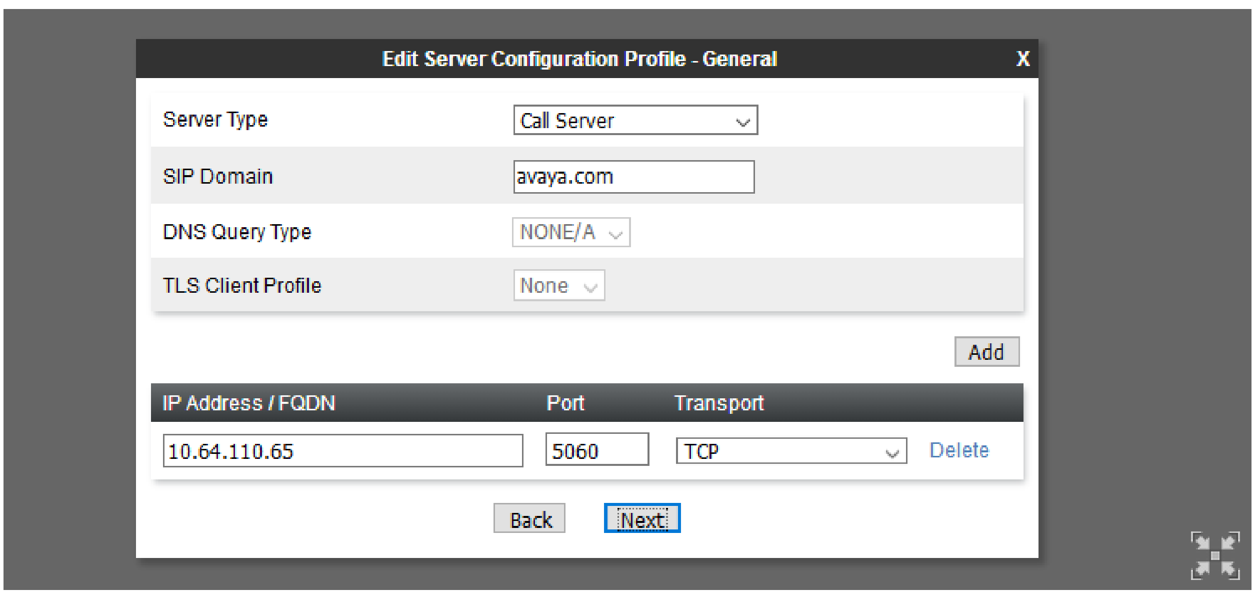


To define another Server for IP Office, click on **Add** and enter an appropriate name in the pop-up menu.

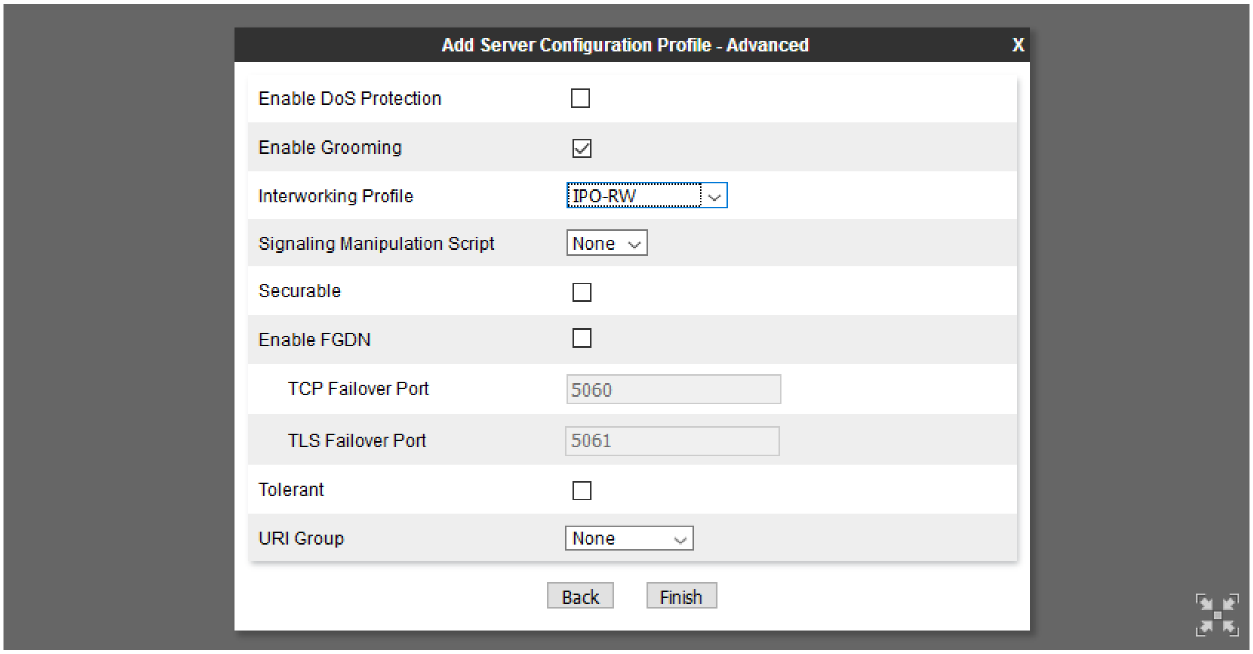


Click on **Next** and enter details in the dialogue box.

- In the **Server Type** drop down menu, select **Call Server**.
- In the **SIP Domain** type in the domain used in the environment.
- Click on **Add** to enter an IP address.
- In the **IP Addresses / FQDN** box, type the IP Address from **Section 5.2**. This is the same IP Office server from **Section 5**.
- In the **Port** box, enter the port to be used for the listening port configured on the IP Office from **Section 5.3.2**.
- In the **Transport** drop down menu, select **TCP**.
- Click on **Next**.



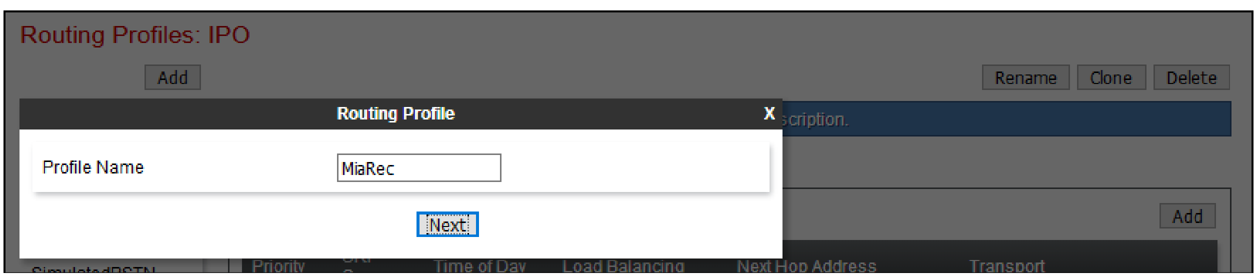
Select **Next** and configure the **Interworking Profile** configured in previous section for IP Office. Select **Finish** once done.



6.4. Define Routing

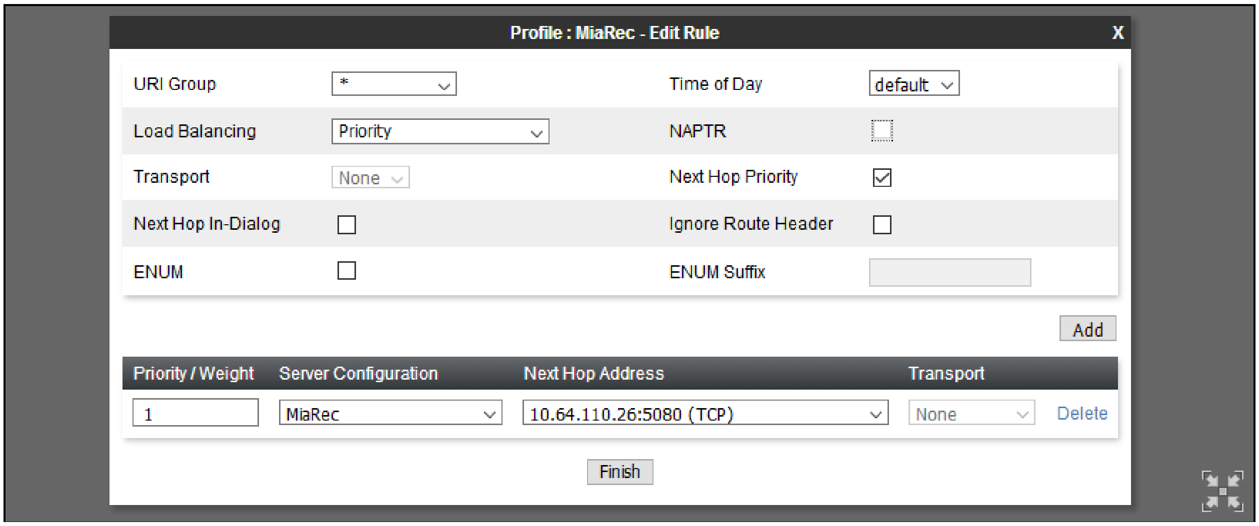
Routing information is required for routing recordings to MiaRec and calls to IP Office (Remote Workers and SIP trunk). The IP addresses and ports defined here will be used as the destination addresses for SIP signalling.

To define routing to the MiaRec SIP trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.

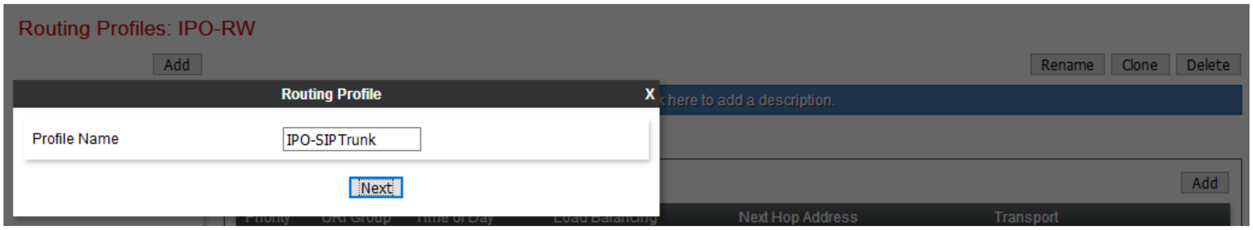


Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP address for the MiaRec SIP trunk.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the MiaRec Server Configuration defined in **Section 6.3** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.
- Click **Finish**.

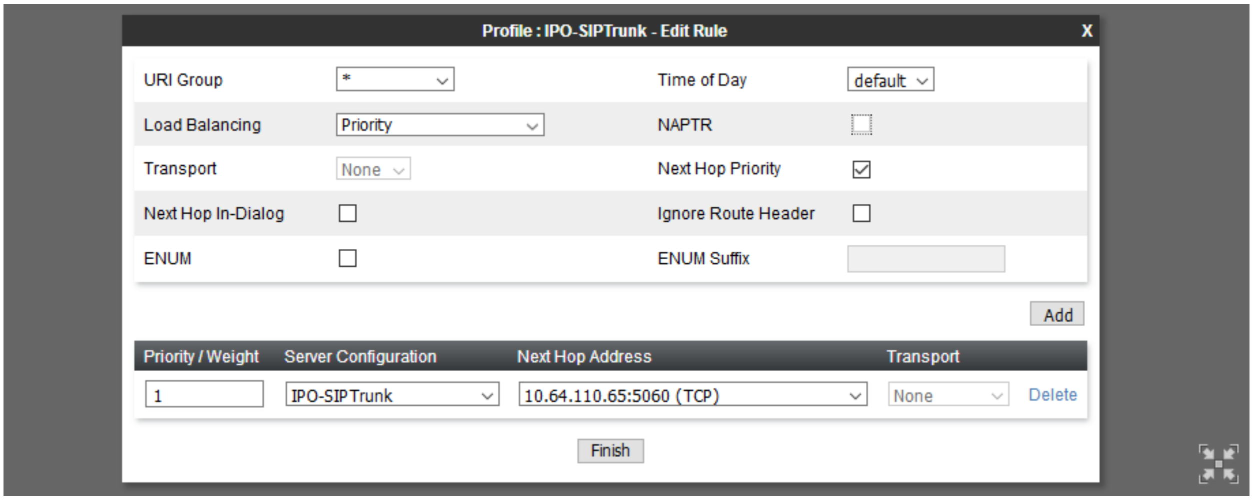


To define routing to the IP Office SIP trunk, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.

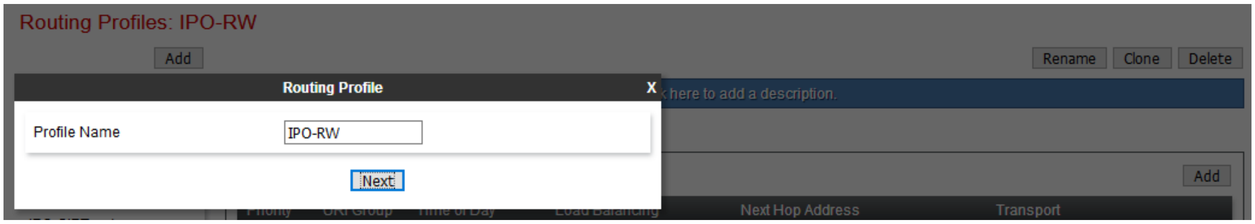


Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP address for the IP Office SIP trunk.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the IP Office Server Configuration defined in **Section 6.3** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.
- Click **Finish**.

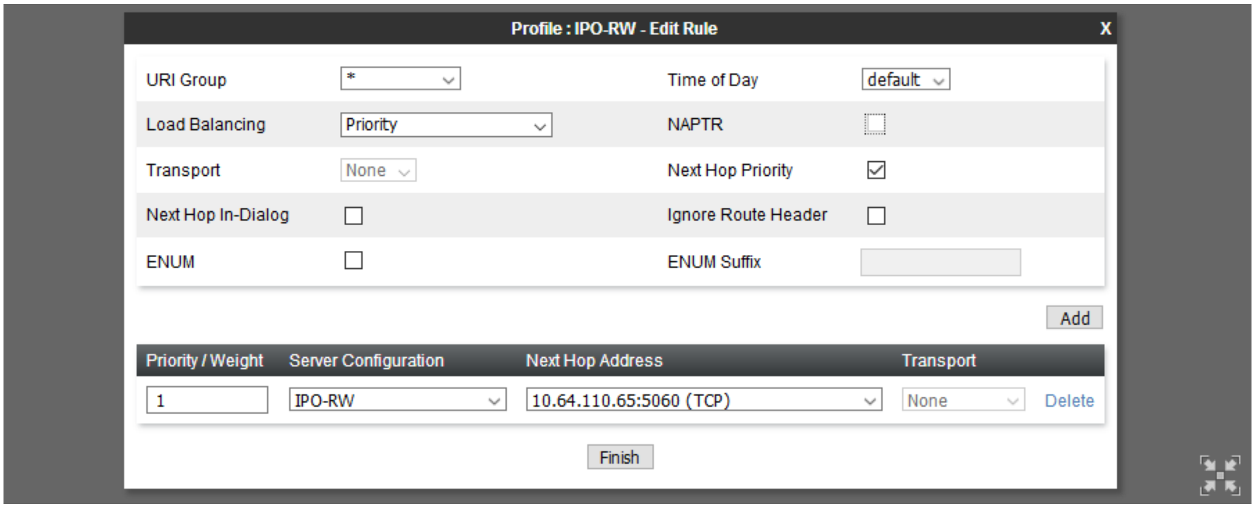


To define routing to the IP Office Remote Workers, navigate to **Global Profiles → Routing** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the dialogue box.



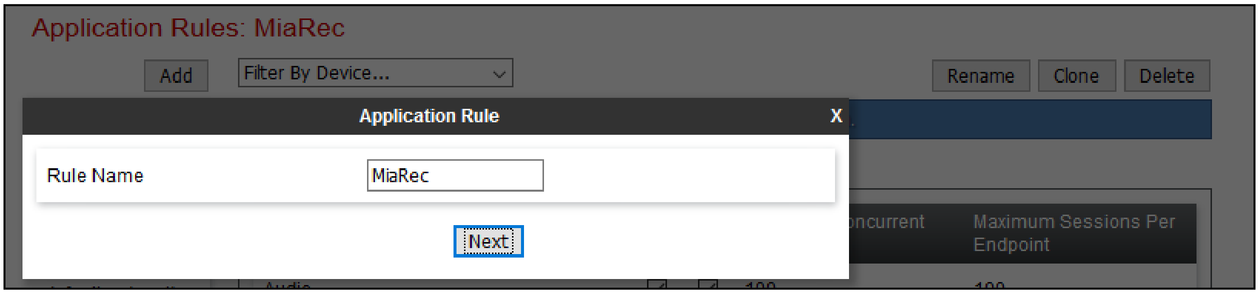
Click on **Next** and enter details for the Routing Profile:

- Click on **Add** to specify the IP address for the IP Office.
- Assign a priority in the **Priority / Weight** field, during testing a value of **1** was used.
- Select the IP Office Server Configuration defined in **Section 6.3** in the **Server Configuration** drop down menu. This automatically populates the **Next Hop Address** field.
- Click **Finish**.

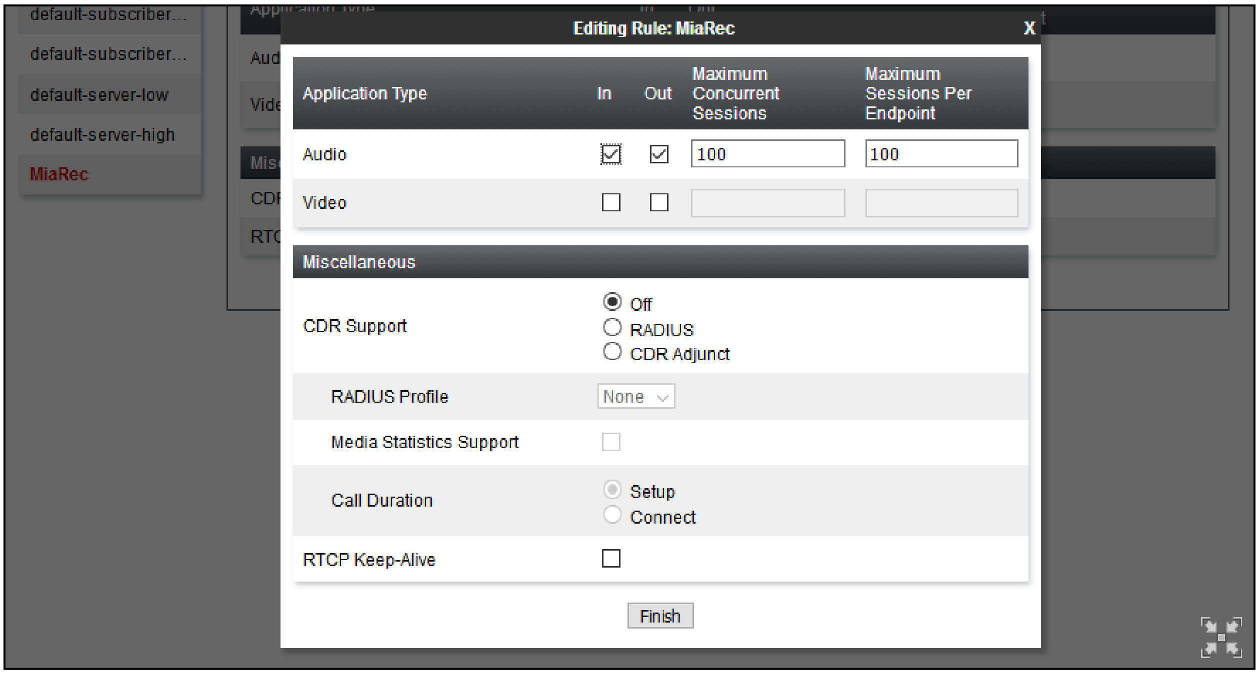


6.5. Define Application Rules

An application rule needs to be defined for MiaRec. To create a new Application Rule, navigate to **Domain Policies → Application Rules**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.



On the **Application Rule** pop-up windows check **In** and **Out** boxes for **Audio**, and select **Finish**.



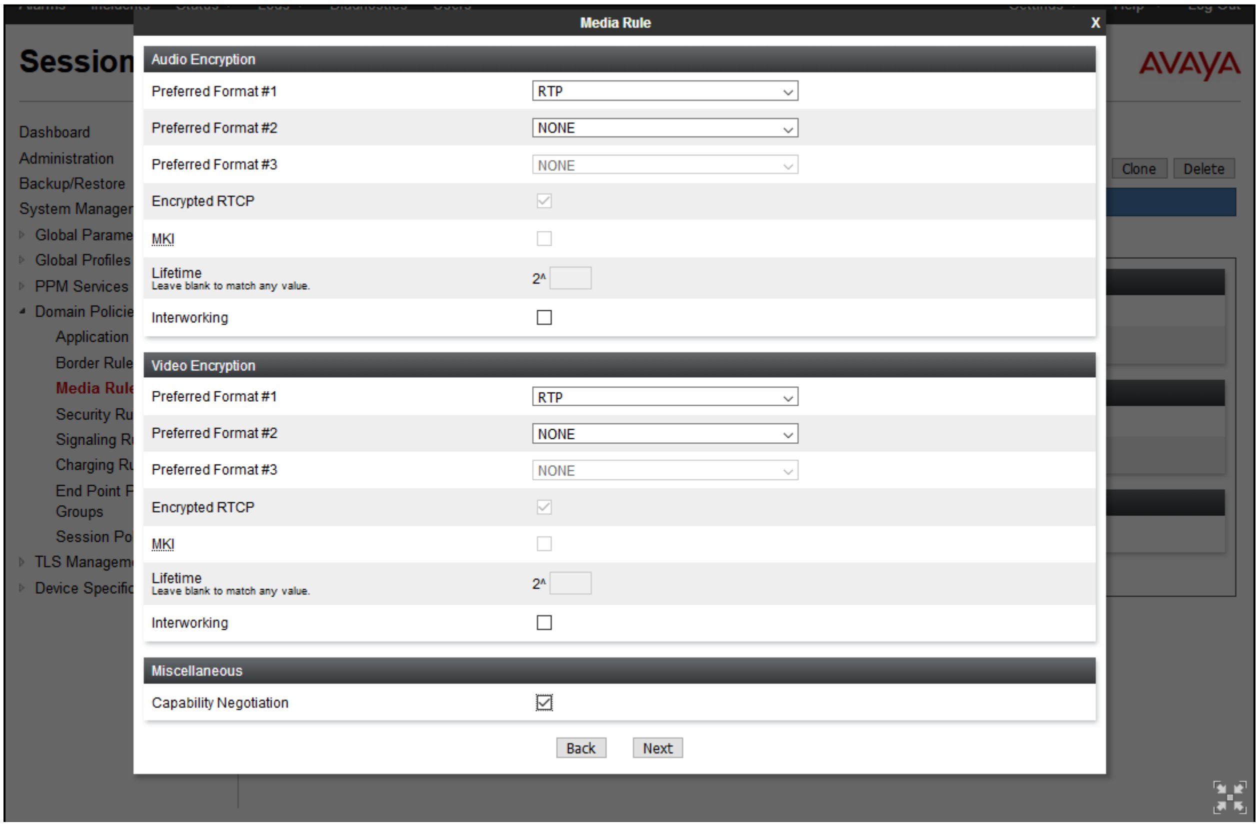
For IP Office, default Application profile was used.

6.6. Define Media Rules

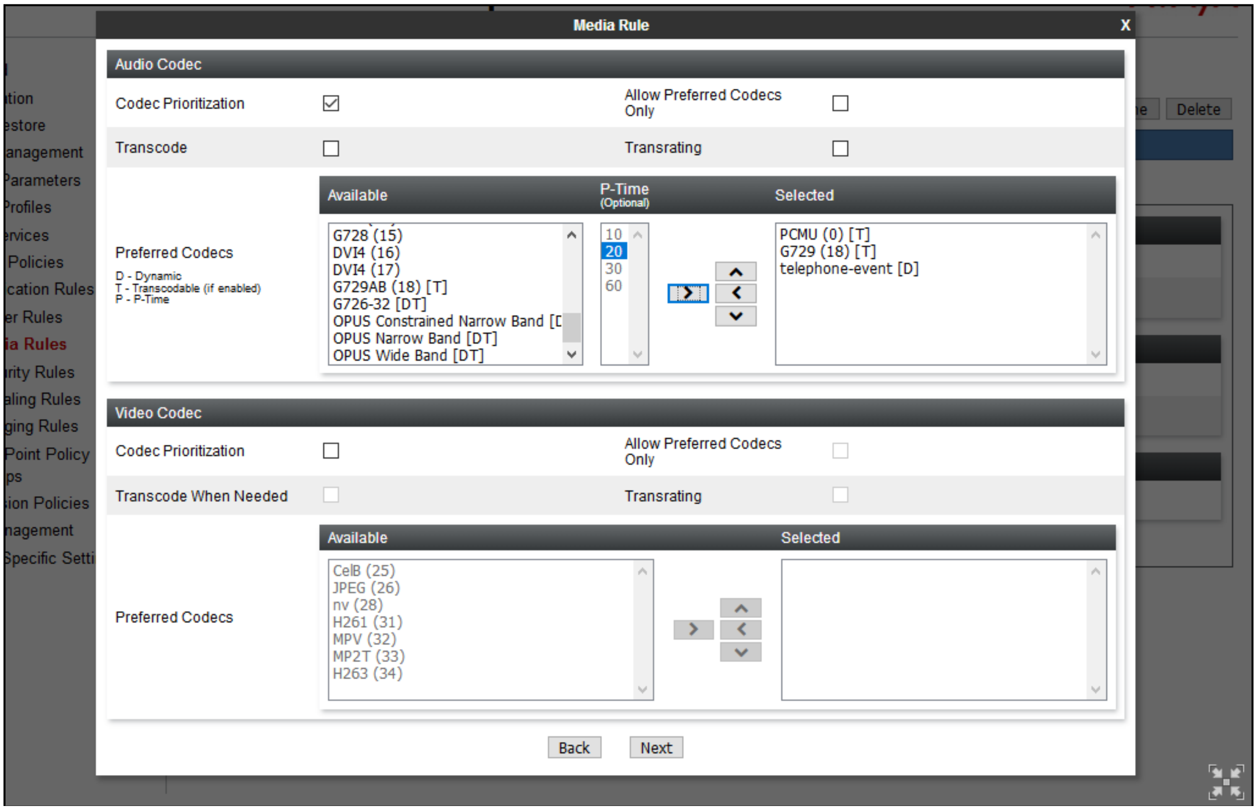
Audio formats need to be specified for MiaRec and IP Office.

To create a Media Rule for MiaRec, navigate to **Domain Policies → Media Rules**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.

On the **Media Rule** pop-up, under **Audio Encryption**, select a **Preferred Format #1** and select continue.



On the **Media Rule** pop-up, under the **Audio Codec** section, select box for **Codec Prioritization**. For **Preferred Codecs** select **PCMU**, **G729** and **telephone-event**, and click >. Select **Next** and **Finish** to save the configuration (not shown).

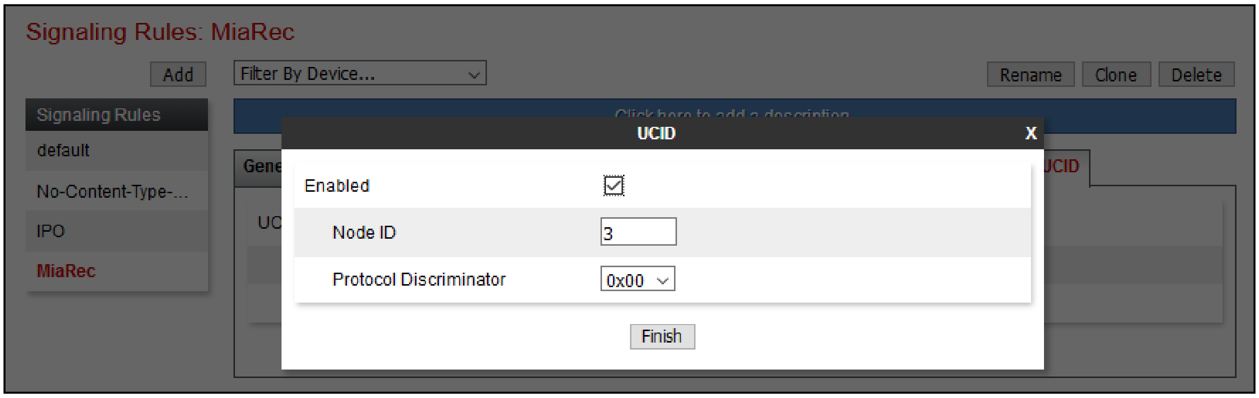


Similarly, create an Application Rule for IP Office. Only one Application Rule is needed for both Remote Workers and SIP trunks.

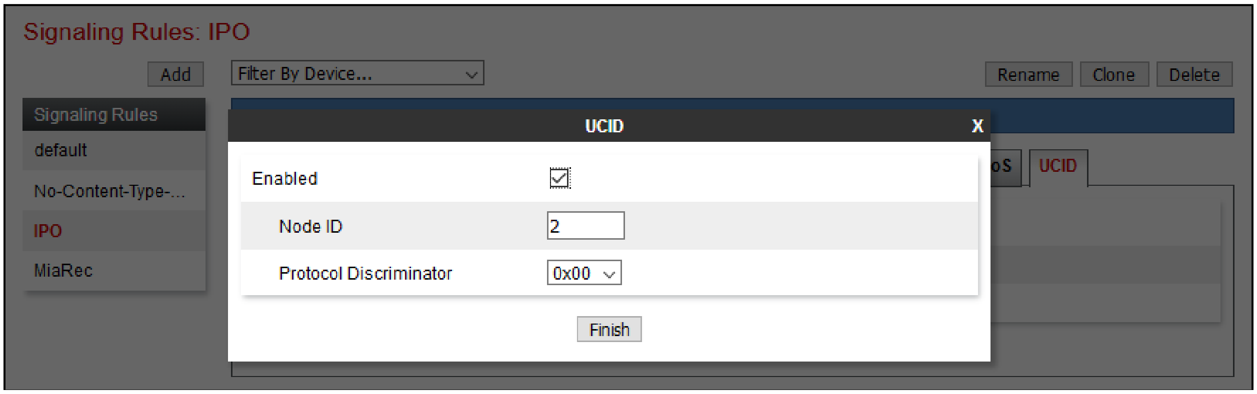
6.7. Configure UCID

UCID needs to be enabled for Signaling Rules that are defined for IP Office and MiaRec. Navigate to **Domain Policies → Signaling Rules**.

Clone the default Signaling Rule and select the **UCID** tab. Click **Edit**, check box for **Enabled** and type in a unique value in **Node ID** field. Select **Finish** to save configuration.

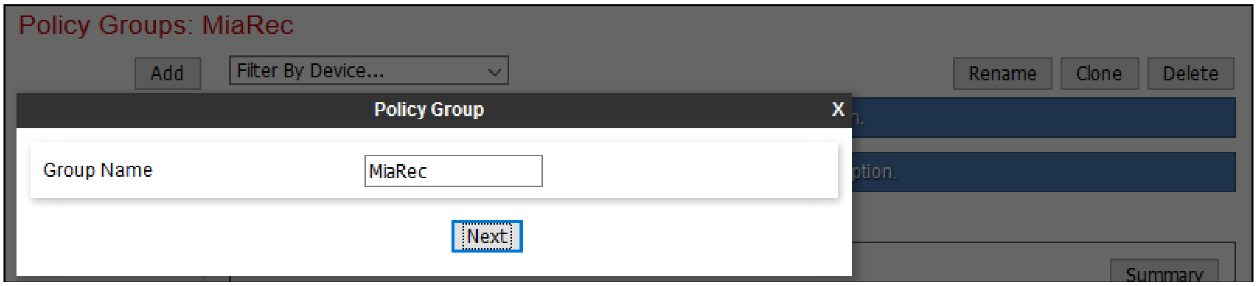


Perform similar steps for IP Office Signaling Rule.

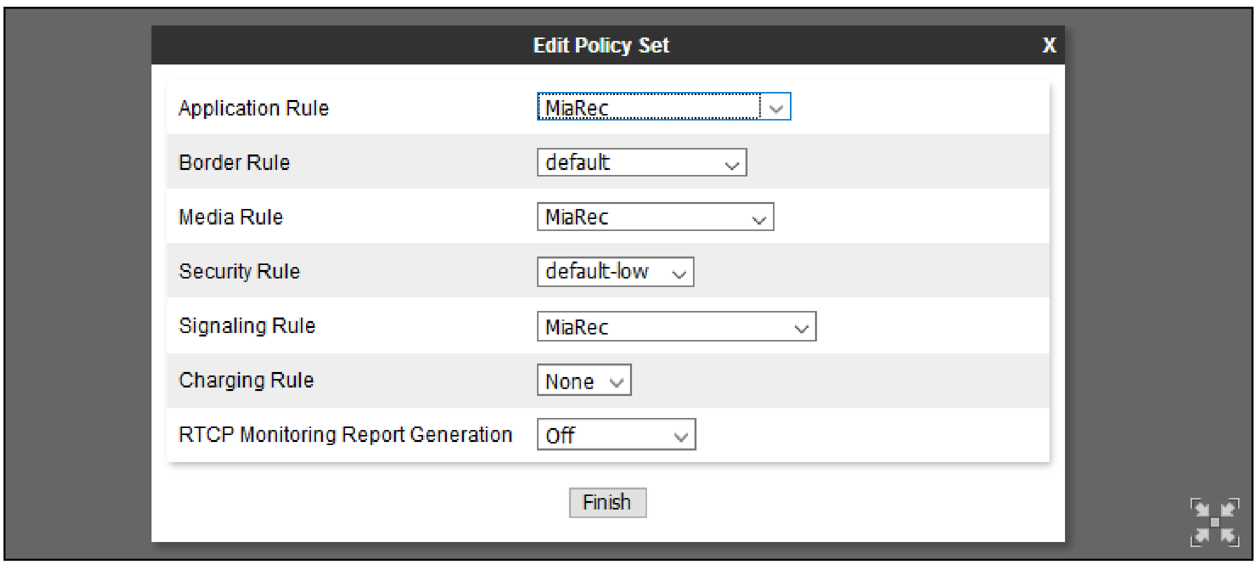


6.8. Define End Point Policy Group

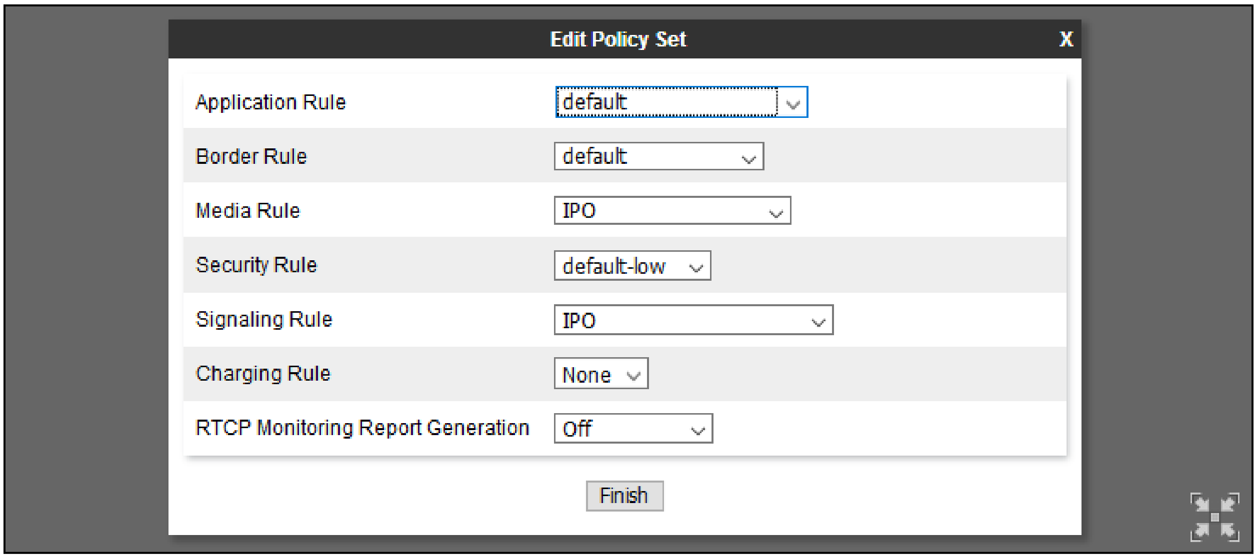
To define an End Point Policy Group for MiaRec, navigate to **Domain Policies → End Point Policy Group** and select **Add**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.



On the **Edit Policy Set** pop-up, select the **Application Rule** defined in **Section 6.5** and select the **Media Rule** defined in **Section 6.6**. Select **Finish** to save configuration.

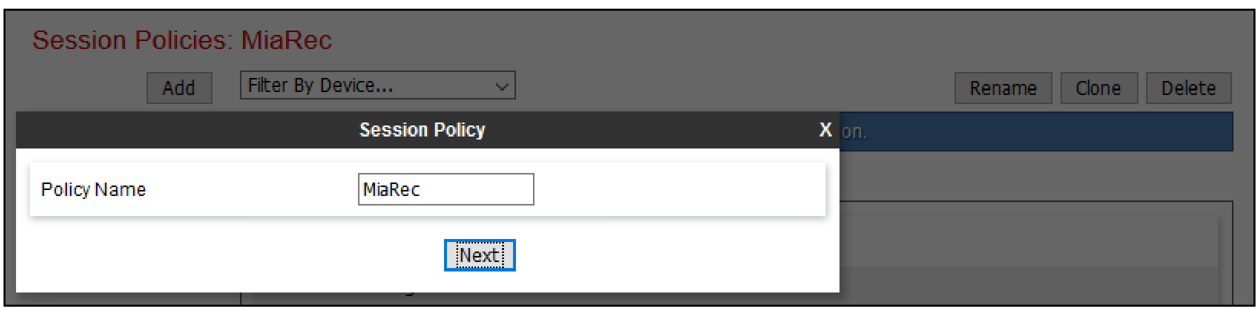


Similarly, create a new End Point Policy Group for IP Office. Only one Policy Group is needed for both Remote Workers and SIP trunk calls.

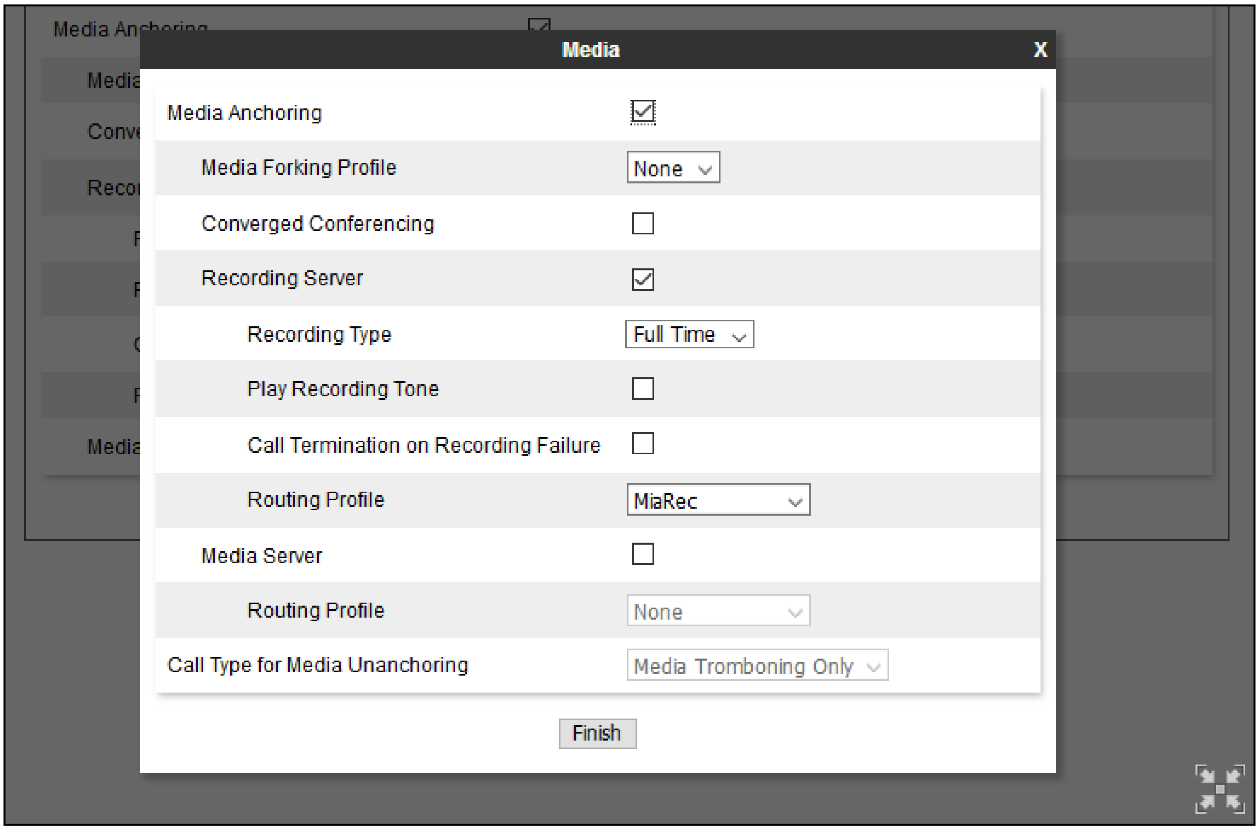


6.9. Define Session Policies

To define Session Policy for MiaRec, navigate to **Domain Policies → Session Policies** and select **Add**. Click on **Add** and enter an appropriate name in the pop-up menu and select **Next**.

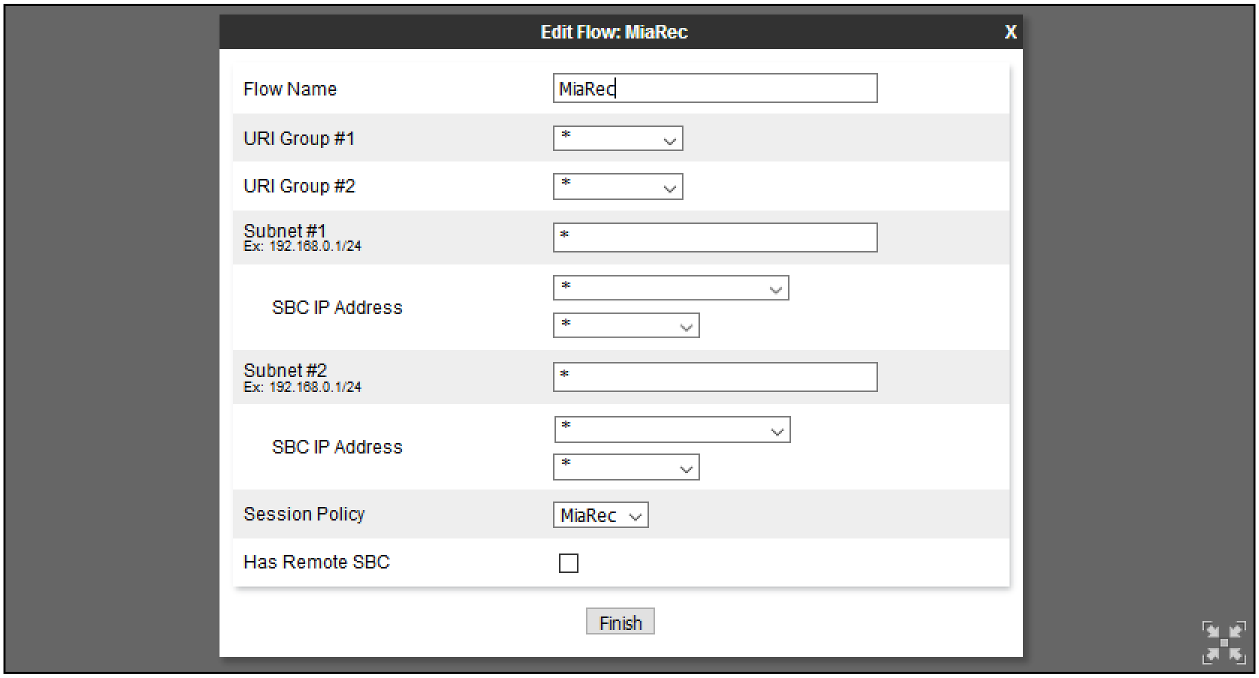


On the **Media** pop-up, select box for **Media Anchoring** and **Recording Server**. For **Routing Profile** select the MiaRec Routing profile configured in **Section 6.4**.



6.10. Define Session Flows

A Session Flow needs to be defined for MiaRec for call recording. To define Session Flow for MiaRec, navigate to **Device Specific Settings → Session Flows** and select **Add**. Click on **Add** and enter an appropriate **Flow Name** in the pop-up menu and select the **Session Policy** defined in **Section 6.9**. Select **Finish** to save the configuration.

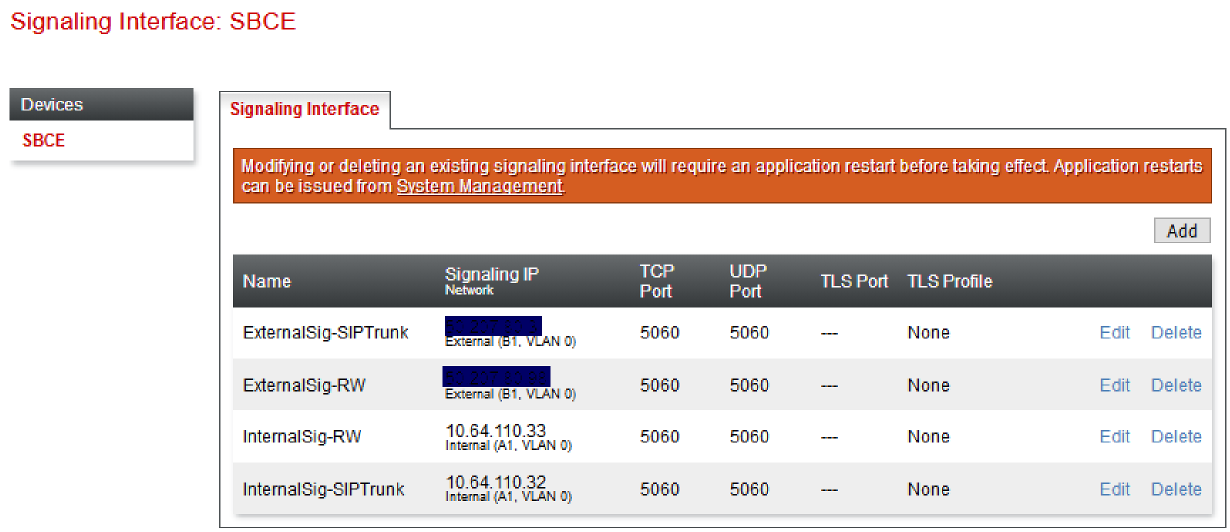


6.11. Signaling Interface

Signaling interfaces on Avaya SBCE need to be defined for SIP trunks and Remote Workers. During this compliance test the following interfaces were defined. To **Add** a new signaling interface navigate to **Device Specific Settings → Signaling Interface**.

- **InternalSig-RW**: SIP interface Remote Workers to IP Office.
- **InternalSig-SIPTrunk**: SIP interface to send and receive calls to IP Office.
- **ExternalSig-SIPTrunk**: SIP interface to send and receive calls to service provider.
- **ExternalSig-RW**: SIP interface for Remote Workers to register over the internet.

Note that for security purposes, Public IP Address is not shown.

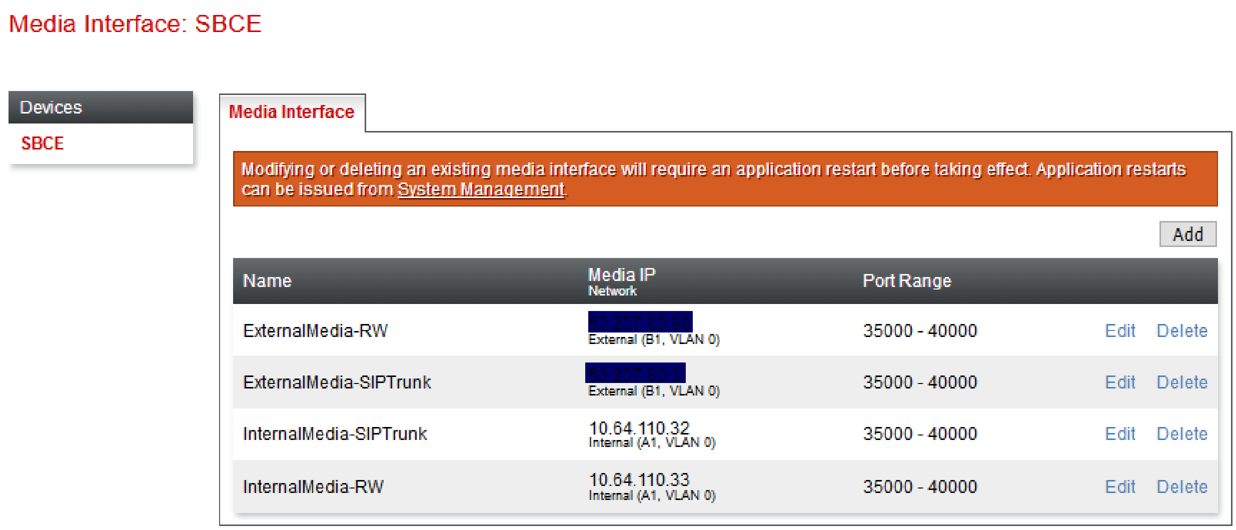


6.12. Media Interface

Media interfaces on Avaya SBCE need to be defined for SIP trunks and Remote Workers. During this compliance test the following interfaces were defined. To **Add** a new media interface navigate to **Device Specific Settings → Media Interface**.

- **InternalMedia-RW**: Media interface Remote Workers to IP Office.
- **InternalMedia-SIPTrunk**: Media interface to send and receive calls to IP Office.
- **ExternalMedia-SIPTrunk**: Media interface to send and receive calls to service provider.
- **ExternalMedia-RW**: Media interface for Remote Workers for calls over the internet.

Note that for security purposes, Public IP Address is not shown.

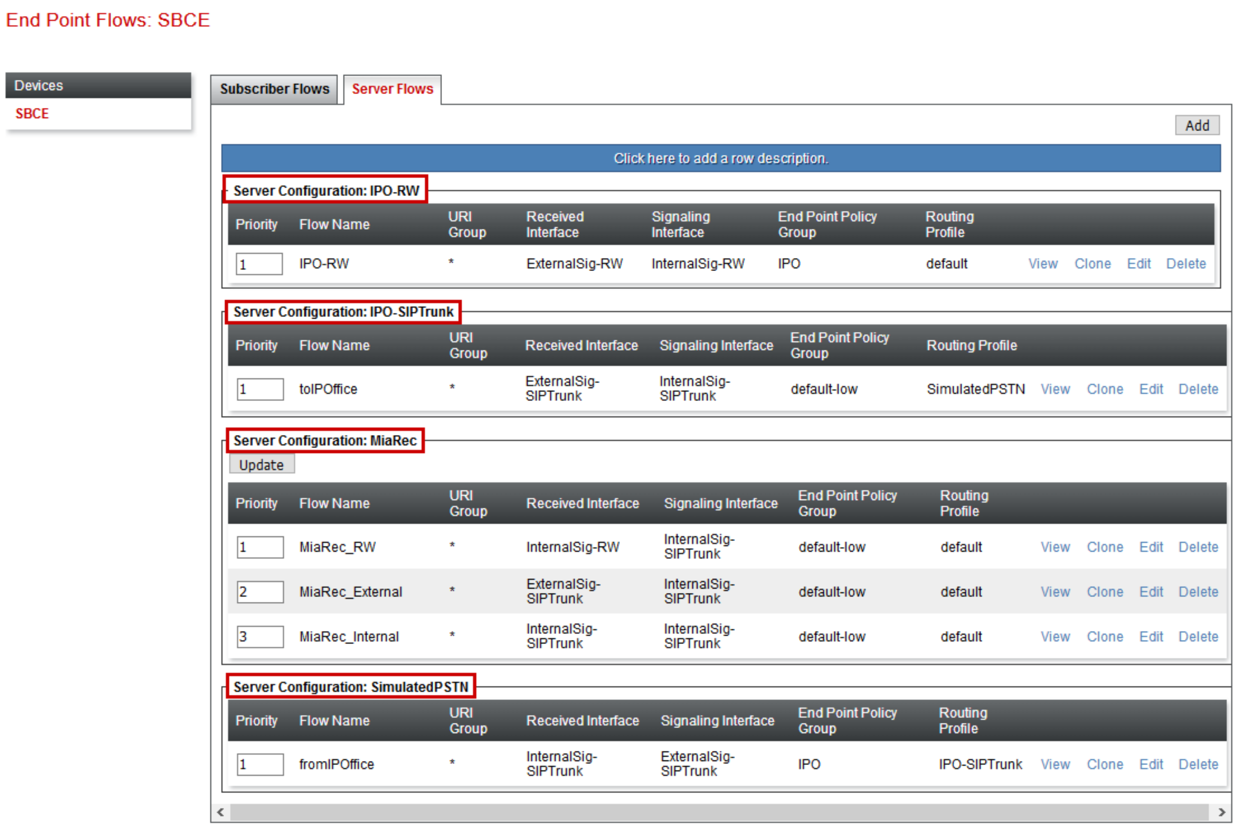


6.13. Server Flows

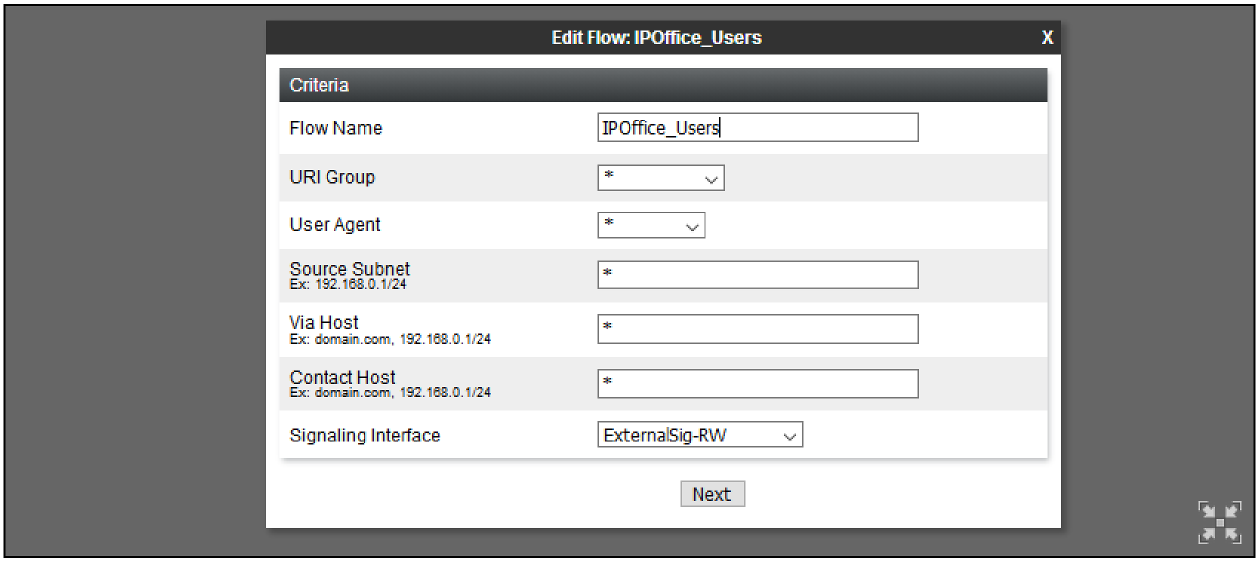
Server Flows combine the previously defined profiles for IP Office and service provider's SIP trunk. These End Point Server Flows allow calls to be recorded by MiaRec when they are passing through Avaya SBCE. Navigate to **Device Specific Setting → End Point Flows → Server Flows**. There were six Server Flows added during compliance test:

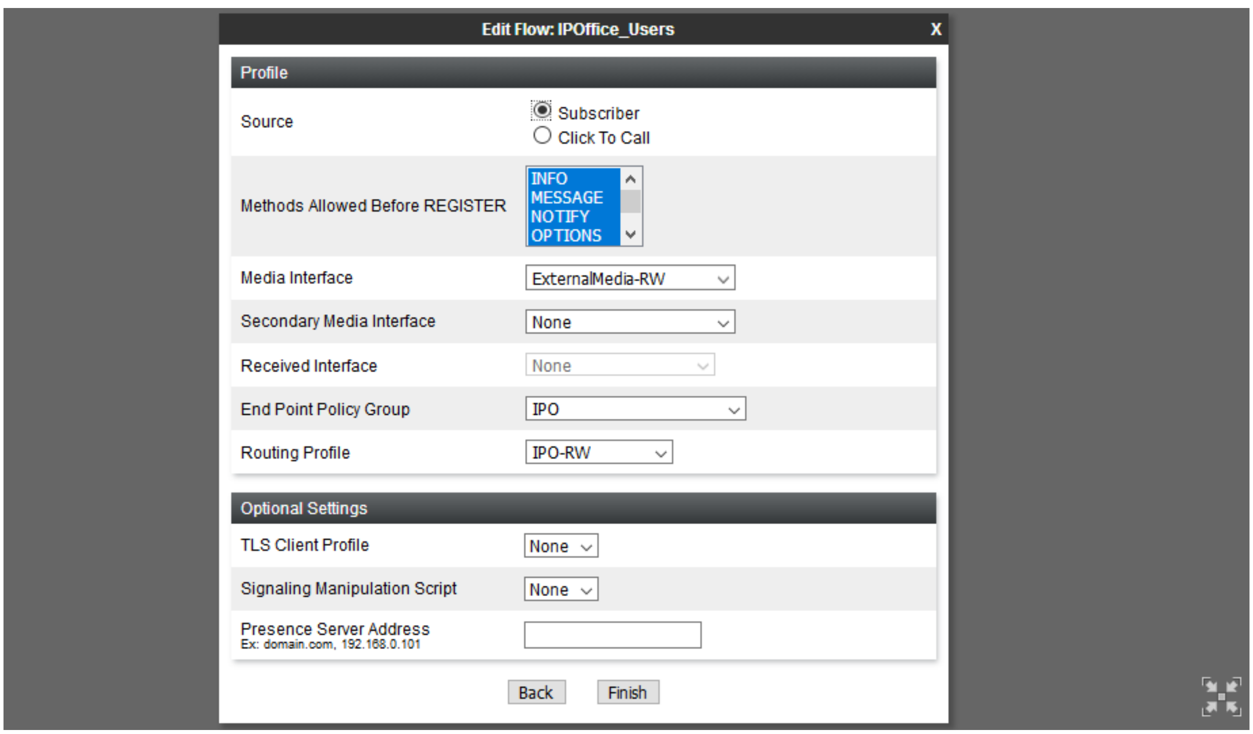
- IP Office – Remote Workers:
  - **IPO-RW**: To send calls to IP Office for registered Remote Workers.
- IP Office – SIP trunk:
  - **toIPOffice**: To send call to IP Office received via service provider SIP trunk.
- MiaRec:
  - **MiaRec_RW**: To record Remote Worker calls.
  - **MiaRec_External**: To record calls received from service provider SIP trunk.
  - **MiaRec_Internal**: To record calls received from IP Office.
- Simulated Service Provider:
  - **fromIPOffice**: To send calls to service provider SIP trunk.

The screen capture below displays the configured Session Flows. Configure the fields as shown in the screen capture.



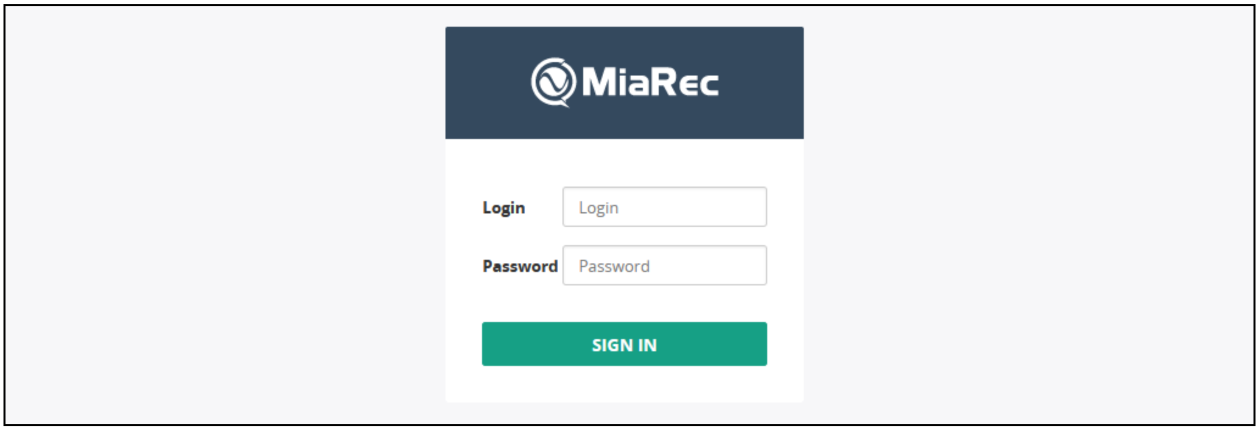
Additionally, a **Subscriber Flow** was added for Remote Workers, as shown below. The Subscriber Flow allows Remote Workers to register to IP Office over the internet, via Avaya SBCE and also SIPREC recordings for MiaRec.



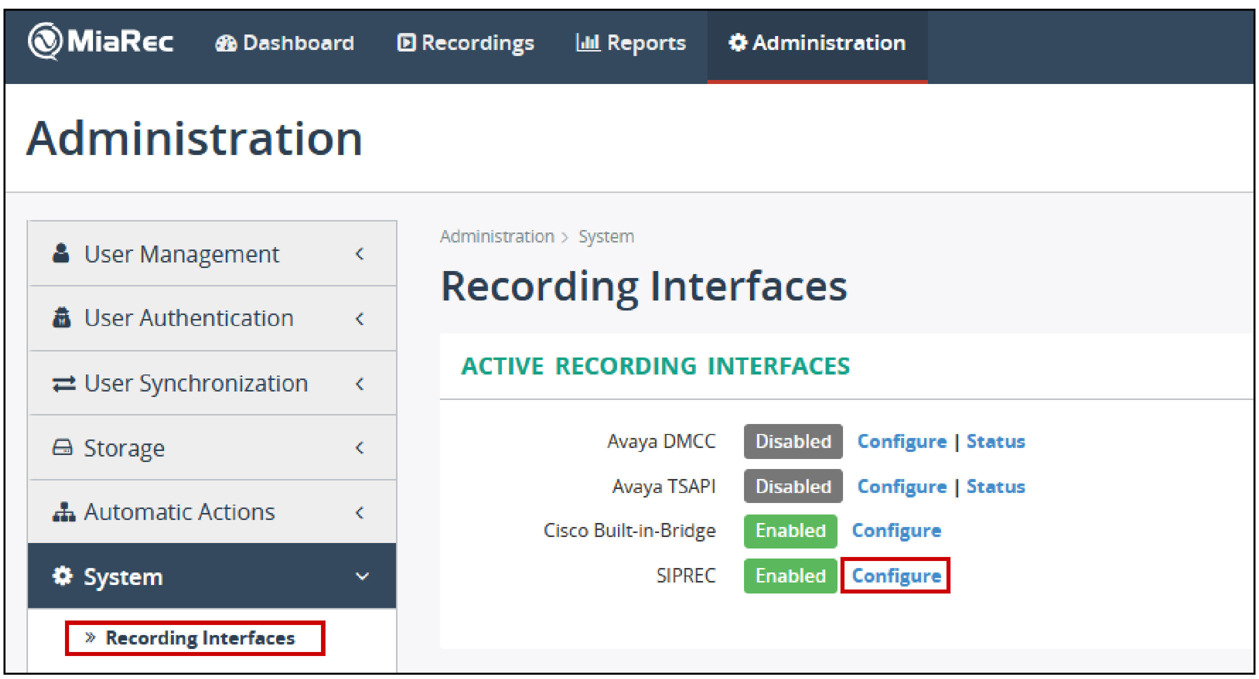


7. Configure the MiaRec

MiaRec was deployed as a virtual machine on a virtualization platform. Configuration for MiaRec is performed via MiaRec web user interface which can be accessed through a browser. Point the browser to **http://<ip-address>**, where ip-address is the IP Address of MiaRec server. Log on using appropriate credentials.



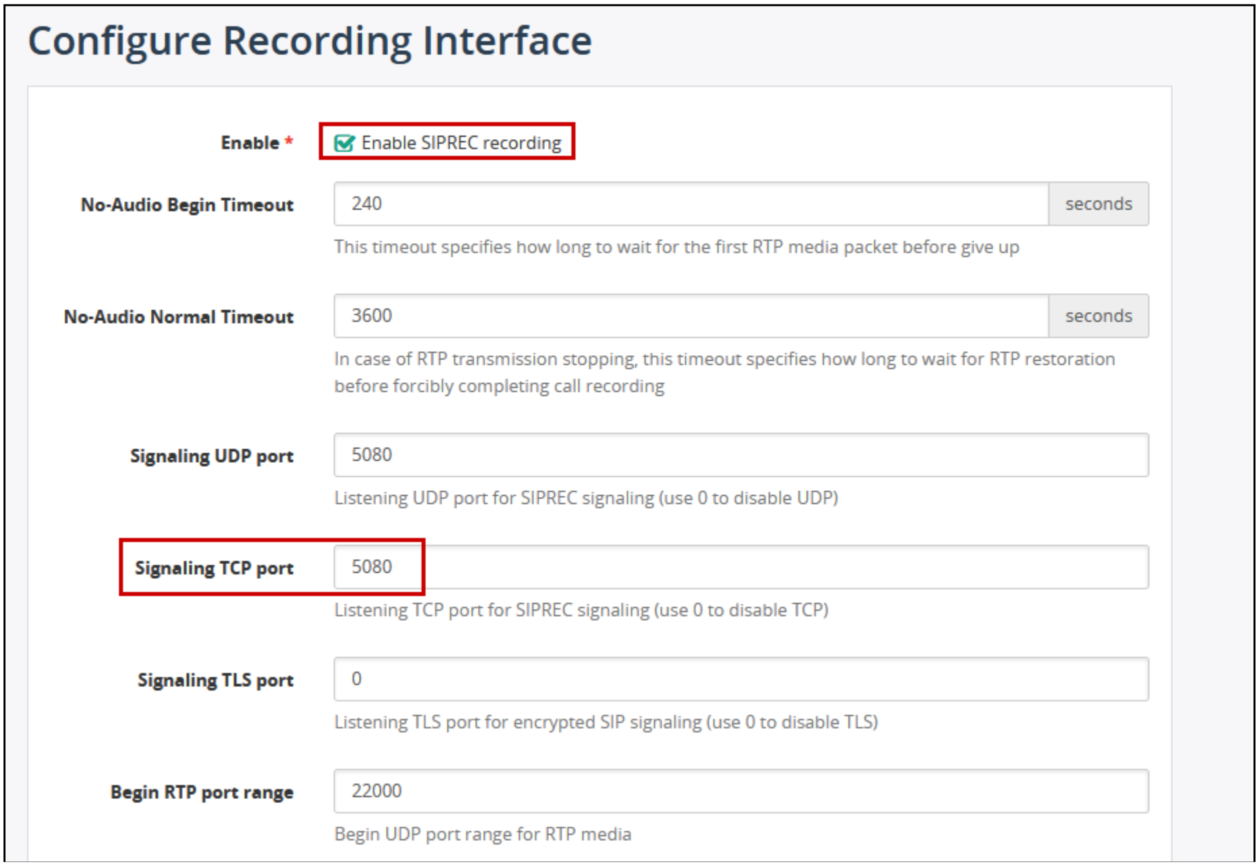
Navigate to **Administration → System → Recording Interfaces** and select **Configure** for **SIPREC**.



On the **Configure Recording Interface** page:

- Check box for **Enable SIPREC recording**.
- Type in port values for the signaling port depending on whether TCP or TLS is being used. TCP was used during compliance test

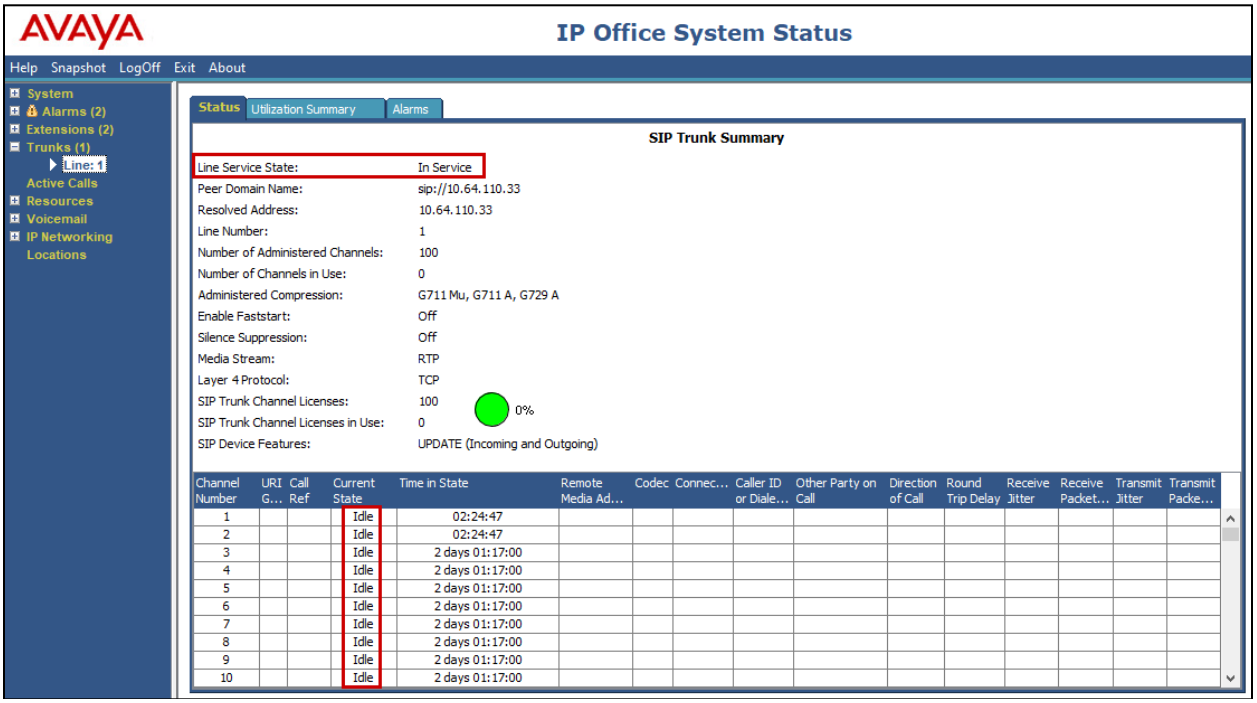
Select **Save** once done (not shown).



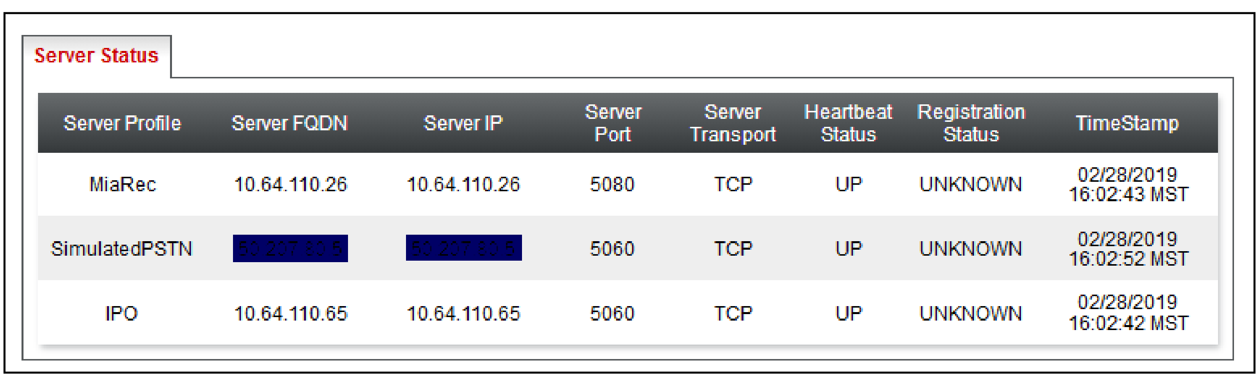
8. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

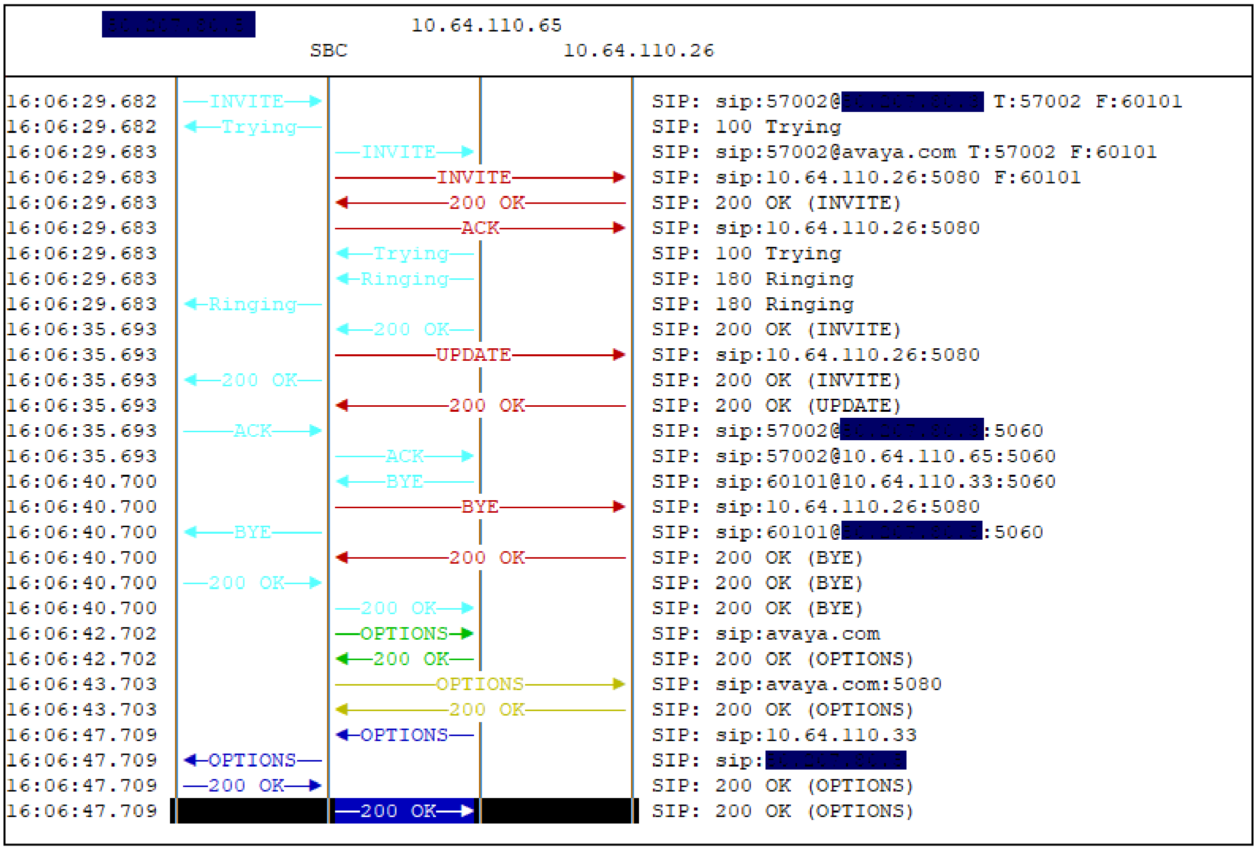
To verify SIP trunks state to Avaya SBCE from IP Office, open **IP Office System Status** application and log on using appropriate credentials. Navigate to **Trunks → Line**. Verify the **Line Service State** is **In Service** and the **Current State** of SIP channels is **Idle**.



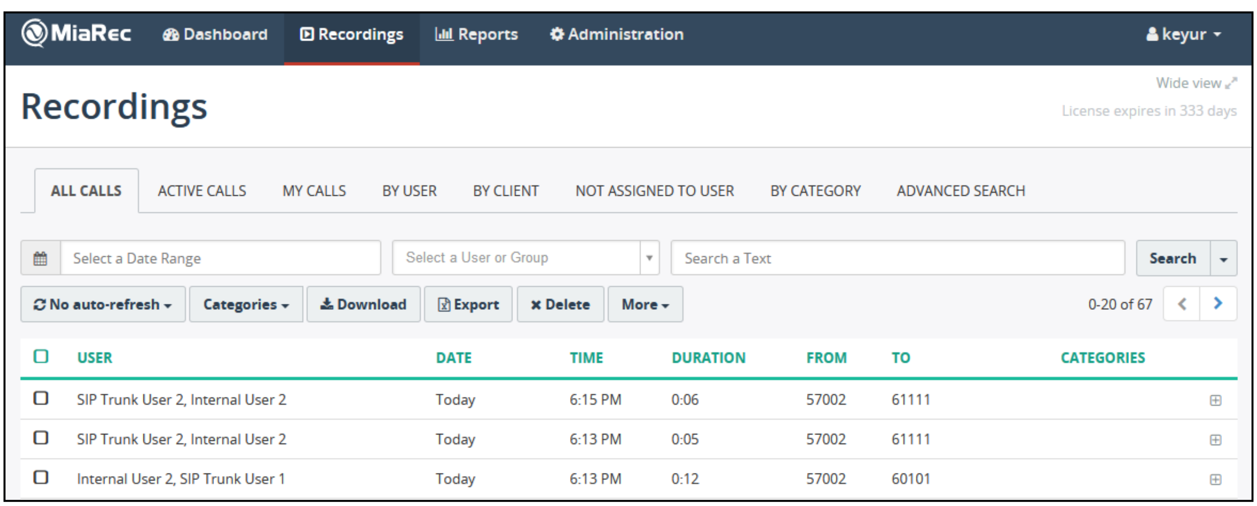
To verify SIP trunks state from Avaya SBCE to MiaRec, IP Office and service provider SIP trunk, via Avaya SBCE web administration portal, navigate to **Status → Server Status**. Verify the **Heartbeat Status** is **UP**.



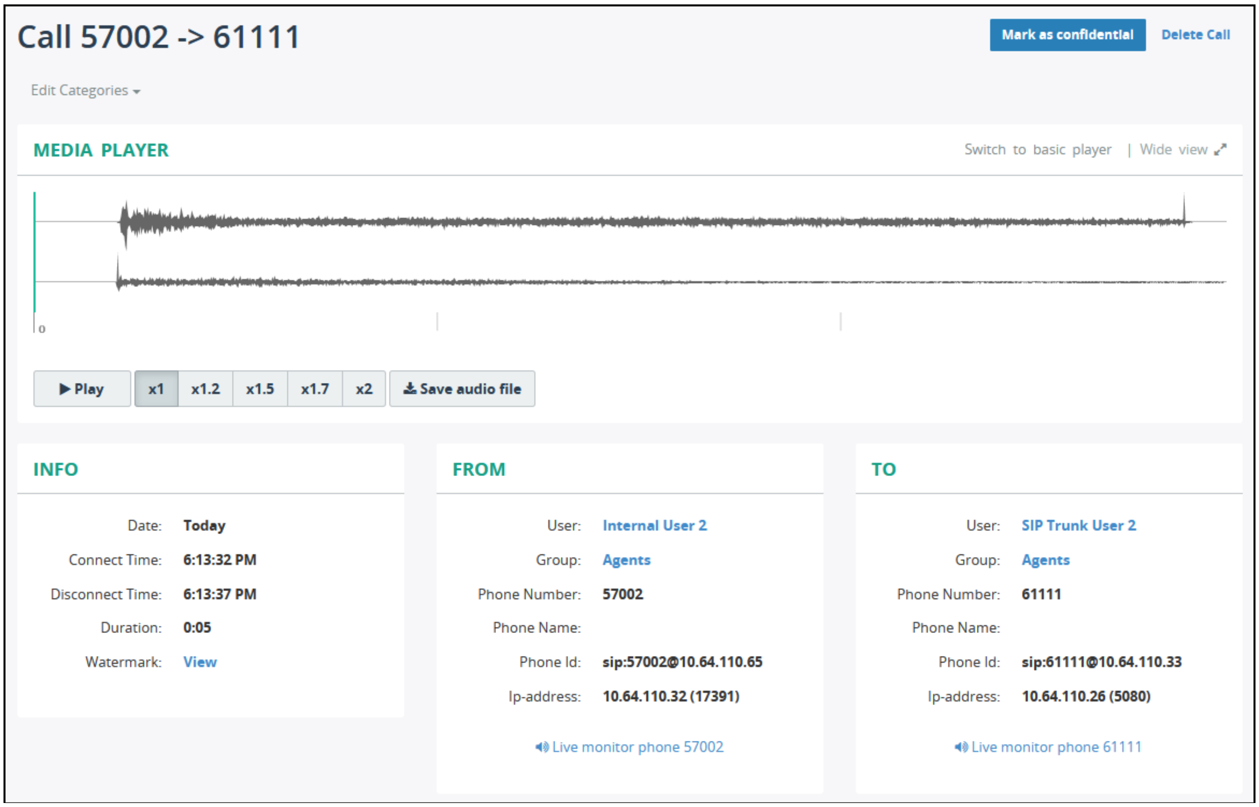
To verify SIP connectivity to MiaRec, logon to Avaya SBCE via secure shell and run **tracesbc** command. Place a call to route via Avaya SBCE. Verify SIP signaling between Avaya SBCE and MiaRec.



To verify MiaRec is recording calls successfully, via the MiaRec web interface, select **Recordings**.



Select a recording to view the details and play the recorded audio.



9. Conclusion

These Application Notes describe the configuration necessary to record calls using MiaRec in the Avaya SIP based solution consisting of Avaya IP Office and Avaya Session Border Controller for Enterprise. The MiaRec call recording and quality management solutions help businesses to record, analyze and access important interactions to meet regulatory compliance requirements, enhance customer service and increase agent productivity. The software was successfully tested with observations listed in **Section 2.2**.

10. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Administering Avaya IP Office™ Platform with Manager,* Release 11.0 FP4, February 2019.

[2] *Deploying Avaya Session Border Controller for Enterprise,* Release 7.2.2.2, Issue 11, April 2019.

[3] *Administering Avaya Session Border Controller for Enterprise,* Release 7.2.2.2, Issue 12, April 2019.

[4] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.