



## **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.

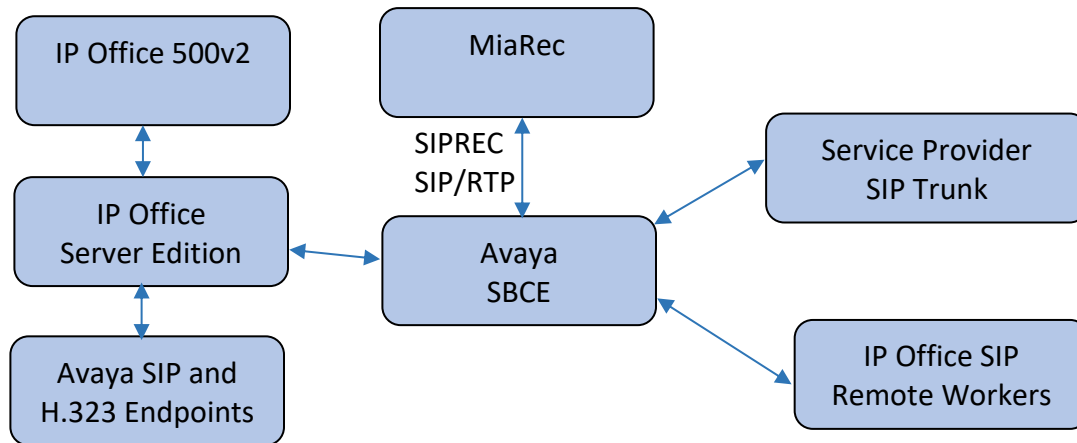
Email: [support@miarec.com](mailto:support@miarec.com)

Phone: 866-324-6717

Web: [www.miarec.com](http://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	7.0.0.107
Recorder	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.

Avaya IP Office Select Manager for Server Edition IPO11 [11.0.0.2.0 build 23]

File Edit View Tools Help

Solution

**Configuration**

- BOOTP (10)
- Operator (3)
- Solution
- User(8)
- Group(1)
- Short Code(47)
- Directory(0)
- Time Profile(0)
- Account Code
- User Rights(9)
- Location(0)
- IPO11
- IPO500v2

**Server Edition**

**Summary**

Server Edition Primary

**Hardware Installed**

- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: 10.64.10.54
- System Identification: 36008880e53c03af1fc88b2cd9379d71ce485d50

**System Settings**

- IP Address: 10.64.110.65
- Sub-Net Mask: 255.255.255.0
- System Locale: United States (US English)
- Device ID: NONE
- Number of Extensions on System: 8

**Open...**

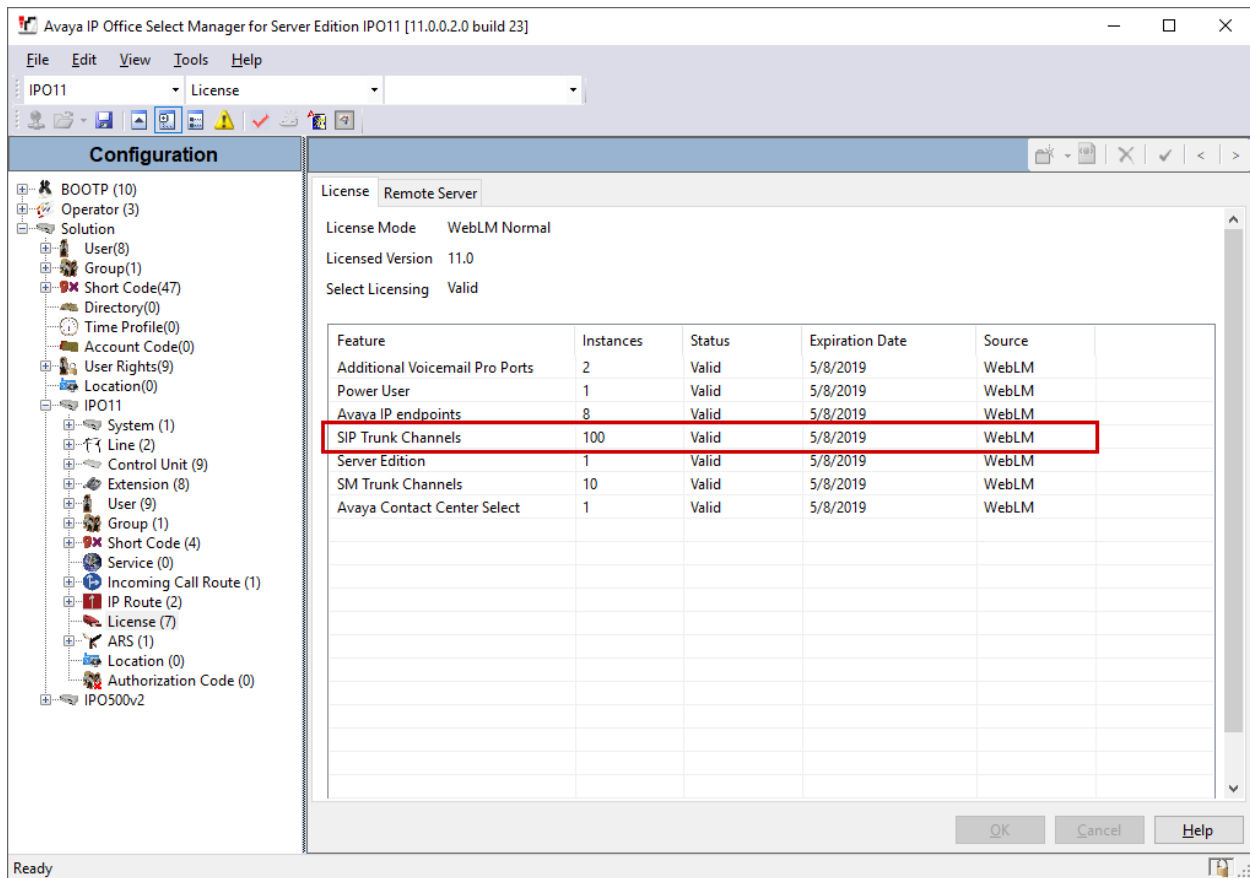
- Configuration
- System Status
- Voicemail Administration
- Resiliency Administration
- On-boarding
- IP Office Web Manager
- Help
- Set All Nodes License Source

**Add...**

Description	Name	Address	Primary Link	Users Configured	Extensions Configured
Solution				8	40
Primary Server	IPO11	10.64.110.65		8	8
Expansion System	IPO500v2	10.64.10.54	Bothway	0	32

Ready

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.

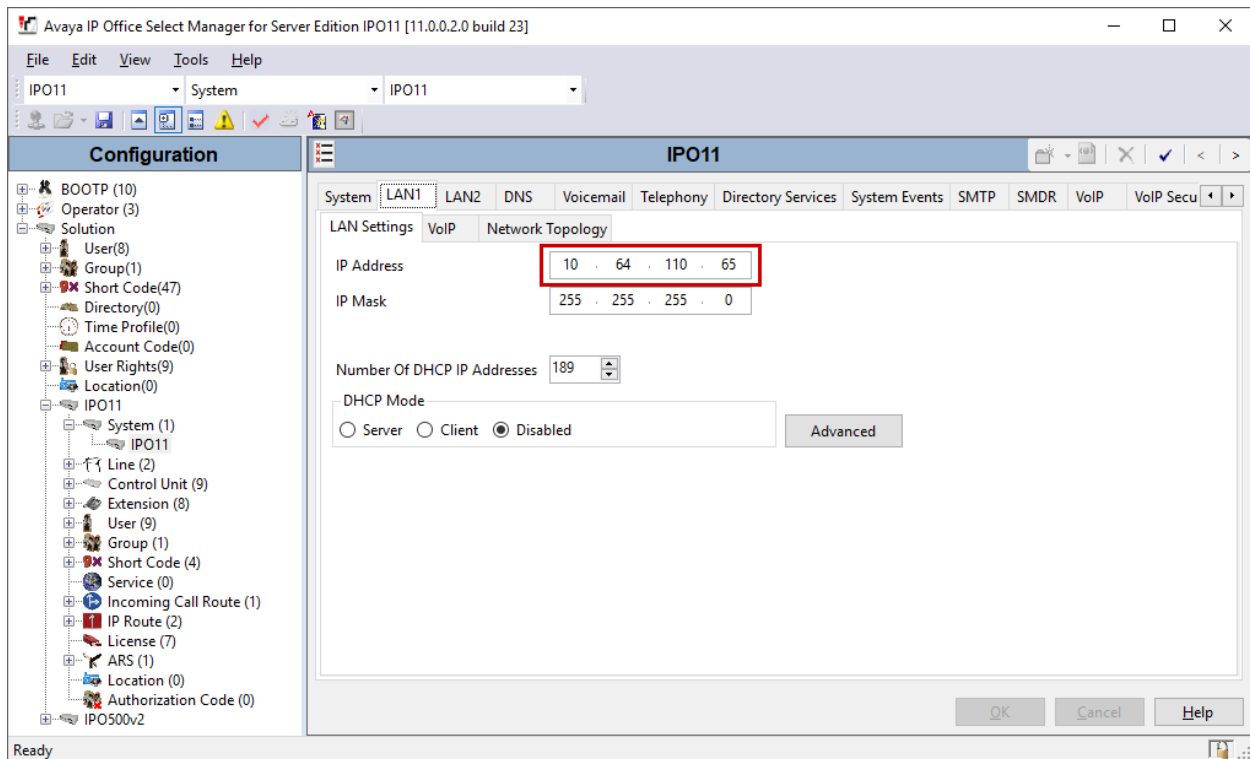


The screenshot shows the Avaya IP Office Select Manager for Server Edition IPO11 [11.0.0.2.0 build 23] window. The left pane displays the Configuration tree, and the right pane shows the License tab. The table in the License tab lists various features and their instances.

Feature	Instances	Status	Expiration Date	Source
Additional Voicemail Pro Ports	2	Valid	5/8/2019	WebLM
Power User	1	Valid	5/8/2019	WebLM
Avaya IP endpoints	8	Valid	5/8/2019	WebLM
<b>SIP Trunk Channels</b>	<b>100</b>	<b>Valid</b>	<b>5/8/2019</b>	<b>WebLM</b>
Server Edition	1	Valid	5/8/2019	WebLM
SM Trunk Channels	10	Valid	5/8/2019	WebLM
Avaya Contact Center Select	1	Valid	5/8/2019	WebLM

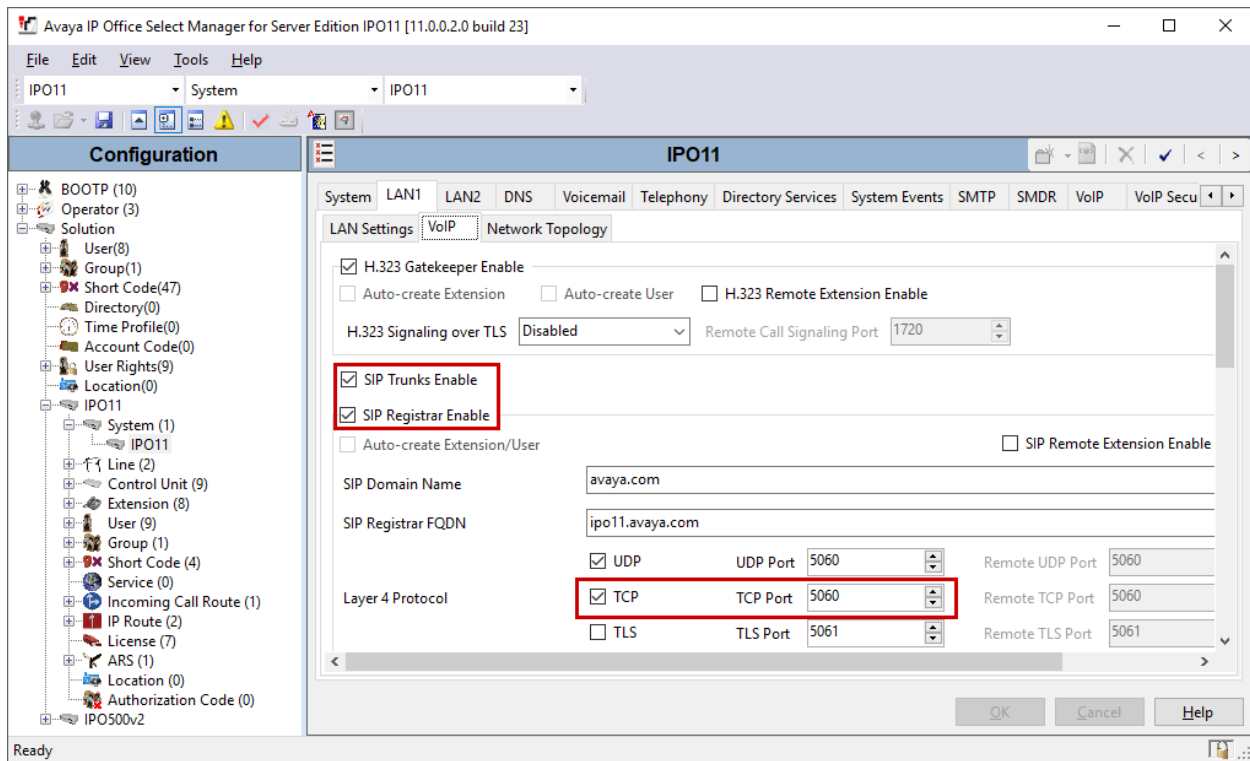
## 5.2. Configure System

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.

Avaya IP Office Select Manager for Server Edition IPO11 [11.0.0.2.0 build 23]

File Edit View Tools Help

IPO11 Line 1

**Configuration**

**SIP Line - Line 1**

SIP Line Transport Call Details VoIP SIP Credentials SIP Advanced Engineering

Line Number: 1

ITSP Domain Name:

Local Domain Name:

URI Type: SIP URI

Location: Cloud

Prefix:

National Prefix: 0

International Prefix: 00

Country Code:

Name Priority: System Default

Description:

In Service: ☒

Check OOS: ☒

Session Timers

Refresh Method: Auto

Timer (sec): On Demand

Redirect and Transfer

Incoming Supervised REFER: Never

Outgoing Supervised REFER: Never

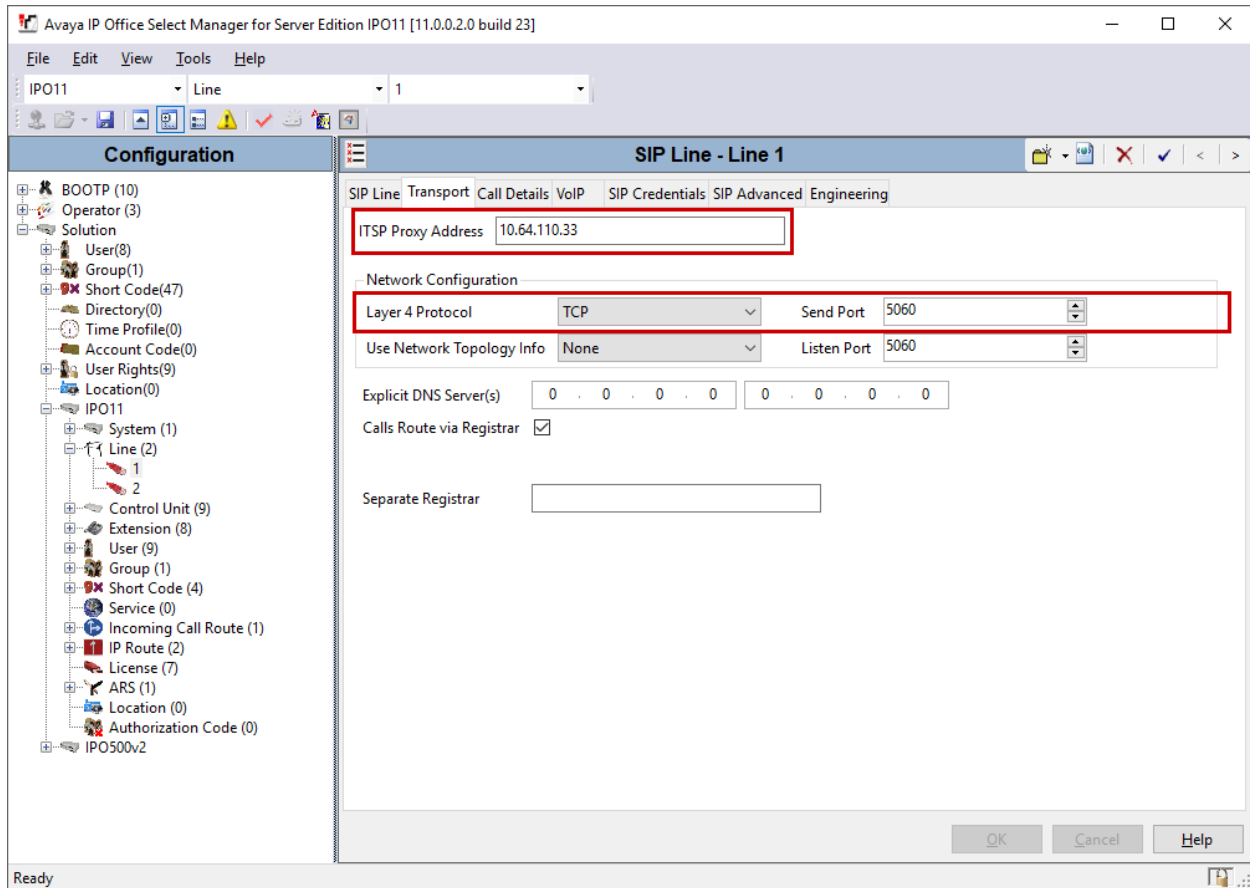
Send 302 Moved Temporarily: ☐

Outgoing Blind REFER: ☐

OK Cancel Help

### 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.

SIP Line - 1 | Call Details | SIP URI

New URI

Incoming Group: 1 Max Sessions: 100

Outgoing Group: 1

Credentials: 0: <None>

Display	Content	Field meaning
Local URI	Auto	Outgoing Calls: Caller, Forwarding/Twinning: Original Caller, Incoming Calls: Called
Contact	Auto	Outgoing Calls: Caller, Forwarding/Twinning: Original Caller, Incoming Calls: Called
P Asserted ID	Auto	Outgoing Calls: Caller, Forwarding/Twinning: Original Caller, Incoming Calls: Called
P Preferred ID	None	Outgoing Calls: None, Forwarding/Twinning: None, Incoming Calls: None
Diversion Header	None	Outgoing Calls: None, Forwarding/Twinning: None, Incoming Calls: None
Remote Party ID	None	Outgoing Calls: None, Forwarding/Twinning: None, Incoming Calls: None

OK Cancel Help

### 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.

Configuration SIP Line - Line 2

SIP Line: Transport: SIP URI VoIP SIP Credentials: SIP Advanced: Engineering

Codec Selection: System Default

Selected: G.711 ULAW 64K, G.711 ALAW 64K, G.729(a) 8K CS-ACELP

☒ Re-invite Supported

☐ Local Hold Music

☐ Codec Lockdown

☐ Allow Direct Media Path

☐ PRACK/100rel Supported

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

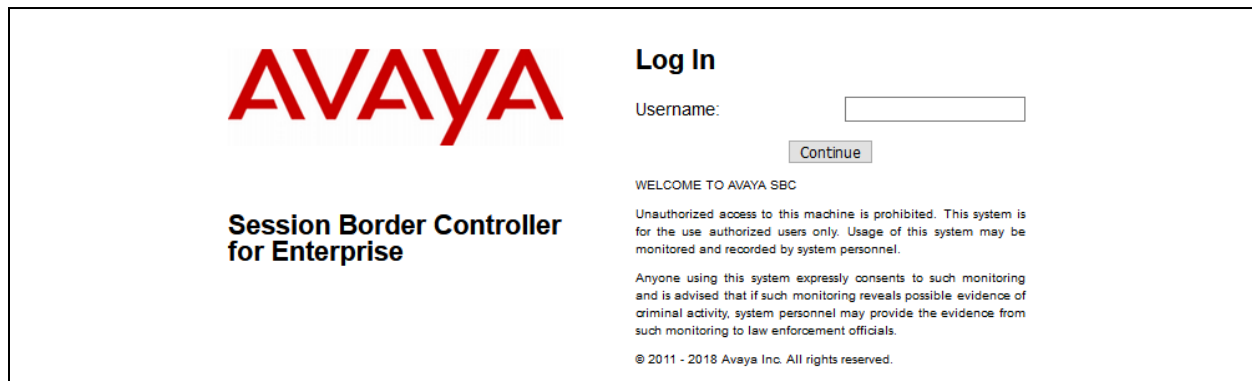
005056AB77B6 Line 2

Configuration

## 6. Configure Avaya Session Border Controller for Enterprise

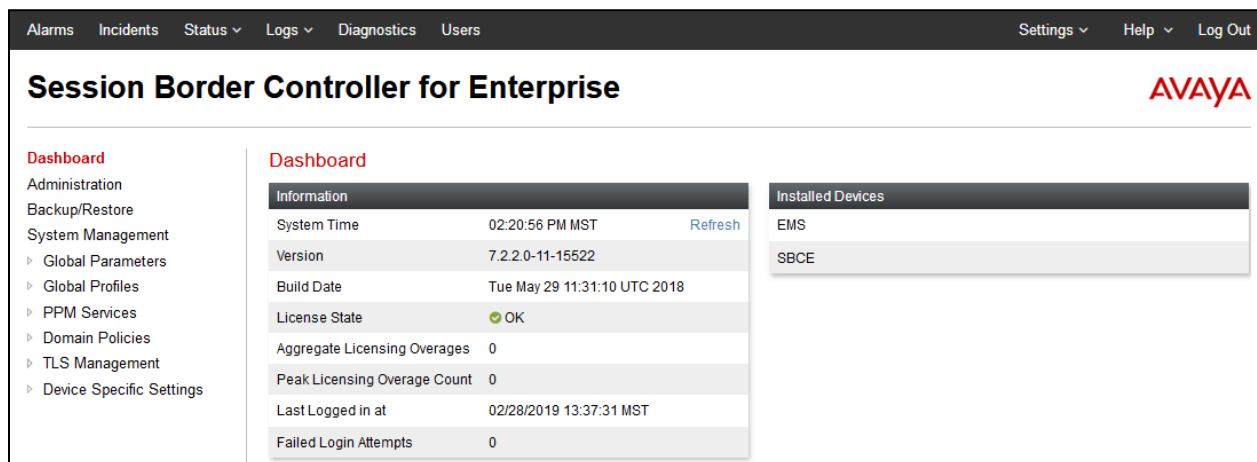
This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP trunk and IP Office Remote Workers. Avaya SBCE also provides the SIPREC interface that is used by MiaRec to record calls. Note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



The login page features the Avaya logo in red on the left. To the right, under the heading "Log In", is a "Username:" label followed by a text input field and a "Continue" button. Below the login fields, a "WELCOME TO AVAYA SBC" message is displayed, followed by a disclaimer: "Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel." A second paragraph states: "Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials." At the bottom, the copyright notice "© 2011 - 2018 Avaya Inc. All rights reserved." is shown.

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.



The dashboard has a dark navigation bar at the top with links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. On the right side of the bar are links for Settings, Help, and Log Out. The main content area is titled "Session Border Controller for Enterprise" and features the Avaya logo in the top right corner. On the left is a sidebar menu with "Dashboard" selected, listing options like Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, and Device Specific Settings. The main area displays a "Dashboard" section with an "Information" table and an "Installed Devices" list.

Information	
System Time	02:20:56 PM MST <a href="#">Refresh</a>
Version	7.2.2.0-11-15522
Build Date	Tue May 29 11:31:10 UTC 2018
License State	OK
Aggregate Licensing Overages	0
Peak Licensing Overage Count	0
Last Logged in at	02/28/2019 13:37:31 MST
Failed Login Attempts	0

Installed Devices
EMS
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

Devices		Interfaces	Networks		
SBCE					
Add					
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	10.207.80.3	255.255.255.128	B1	10.207.80.3 10.207.80.88	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**.

Devices		Interfaces	Networks		
SBCE					
Add VLAN					
Interface Name	VLAN Tag	Status			
A1		Enabled			
A2		Disabled			
B1		Enabled			
B2		Disabled			

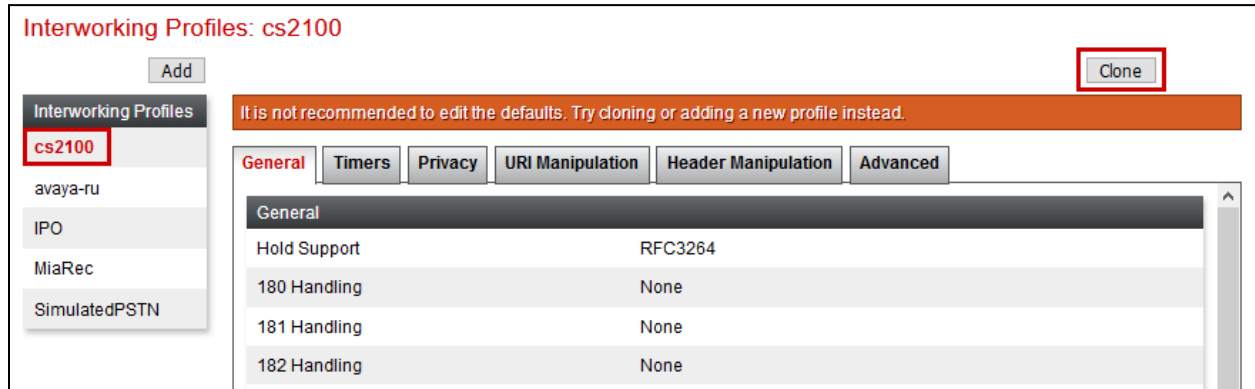
**Note:** to ensure that the Avaya SBCE uses the interfaces defined, the Application must be restarted.

- 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**.



General	
Hold Support	RFC3264
180 Handling	None
181 Handling	None
182 Handling	None

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



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

**Editing Profile: MiaRec**

**Record Routes**

- ☐ None
- ☐ Single Side
- ☒ Both Sides
- ☐ Dialog-Initiate Only (Single Side)
- ☐ Dialog-Initiate Only (Both Sides)

**Include End Point IP for Context Lookup** ☒

**Extensions** Avaya

**Diversion Manipulation** ☐

**Diversion Condition** None

**Diversion Header URI**

**Has Remote SBC** ☒

**Route Response on Via Port** ☐

**Relay INVITE Replace for SIPREC** ☐

**MOBX Re-INVITE Handling** ☐

**DTMF**

**DTMF Support**

- ☐ None
- ☐ SIP Notify
- ☒ RFC 2833 Relay & SIP Notify
- ☐ SIP Info
- ☐ RFC 2833 Relay & SIP Info
- ☐ Inband

**Finish**

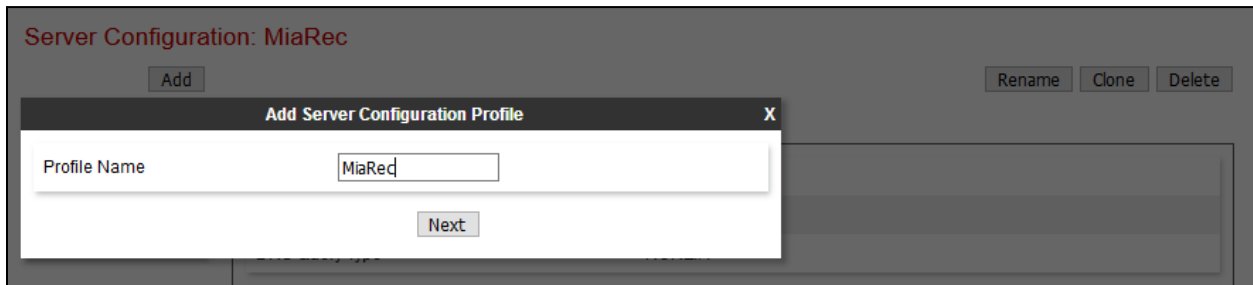
Similarly, create another Server Interworking profile for IP Office.



### 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.

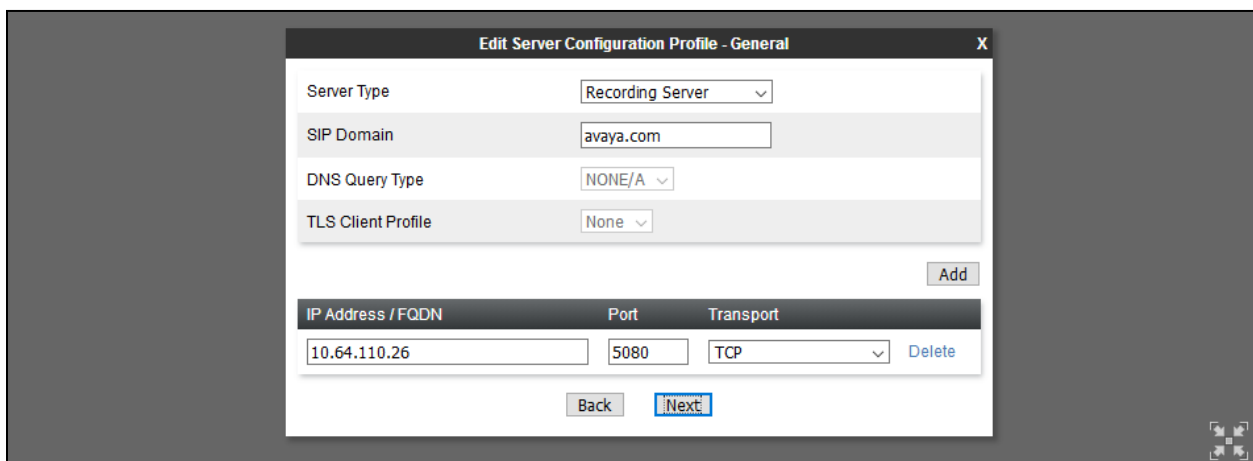
To define the MiaRec Recording Server, navigate to **Global Profiles → Server Configuration** in the main menu on the left hand side. Click on **Add** and enter an appropriate name in the pop-up menu.



The screenshot shows the 'Server Configuration: MiaRec' window. At the top, there are buttons for 'Add', 'Rename', 'Clone', and 'Delete'. The 'Add' button is highlighted. Below it, the 'Add Server Configuration Profile' dialog is open, showing a 'Profile Name' field with the value 'MiaRec' and a 'Next' button.

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**.

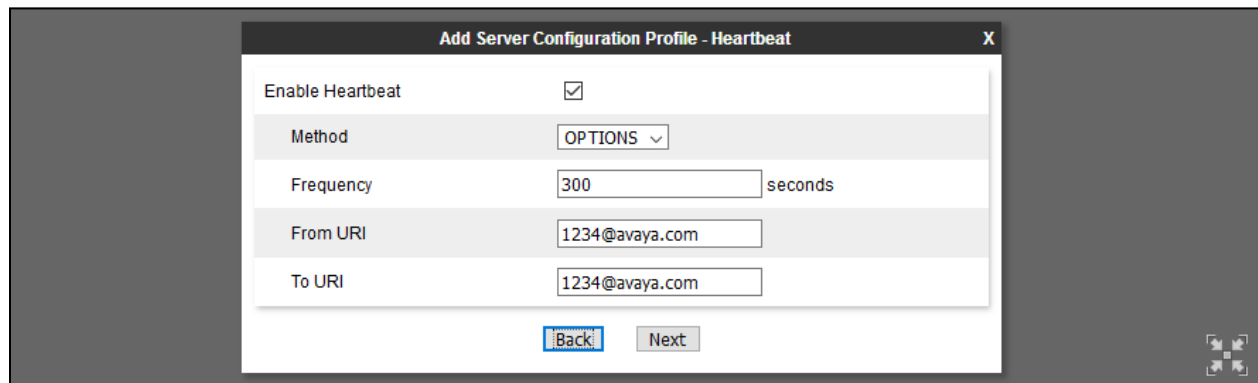


The screenshot shows the 'Edit Server Configuration Profile - General' dialog box. It contains the following fields and values:

Field	Value
Server Type	Recording Server
SIP Domain	avaya.com
DNS Query Type	NONE/A
TLS Client Profile	None
IP Address / FQDN	10.64.110.26
Port	5080
Transport	TCP

Buttons: Add, Back, Next (highlighted), Delete.

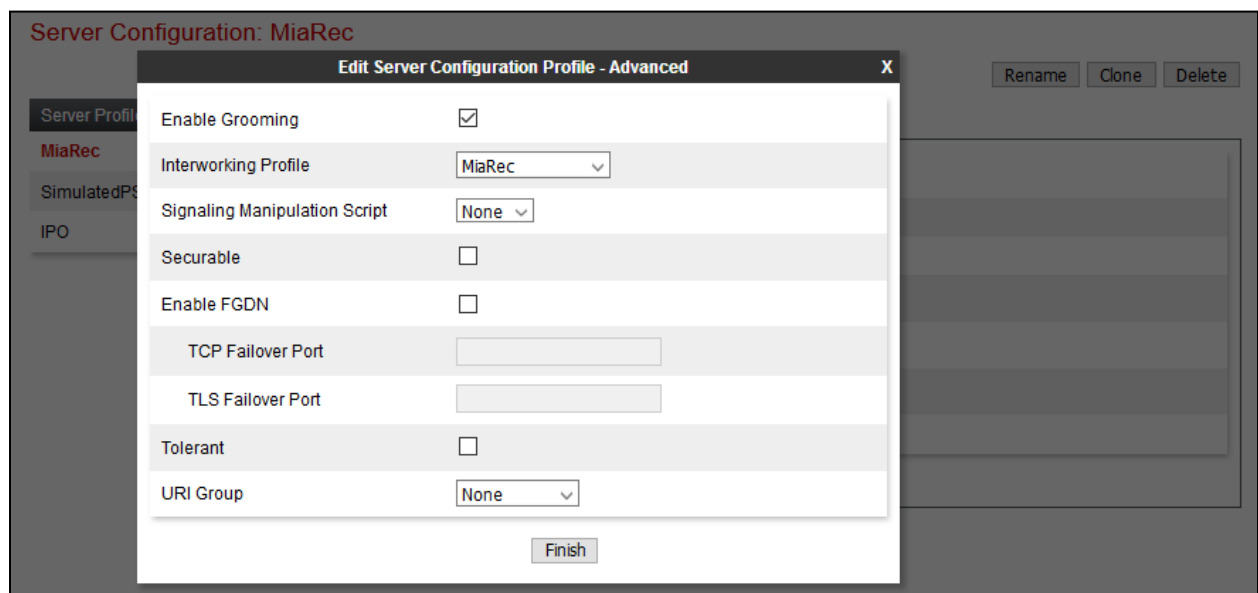
Click on **Next** and configure **From URI** and **To URI** as follows. Instead of a domain, an IP Address can also be used in the URI.



The screenshot shows a dialog box titled "Add Server Configuration Profile - Heartbeat". It contains the following fields and controls:

- Enable Heartbeat:** A checkbox that is checked.
- Method:** A dropdown menu showing "OPTIONS".
- Frequency:** A text input field containing "300", followed by the unit "seconds".
- From URI:** A text input field containing "1234@avaya.com".
- To URI:** A text input field containing "1234@avaya.com".
- Buttons:** "Back" and "Next" buttons at the bottom.

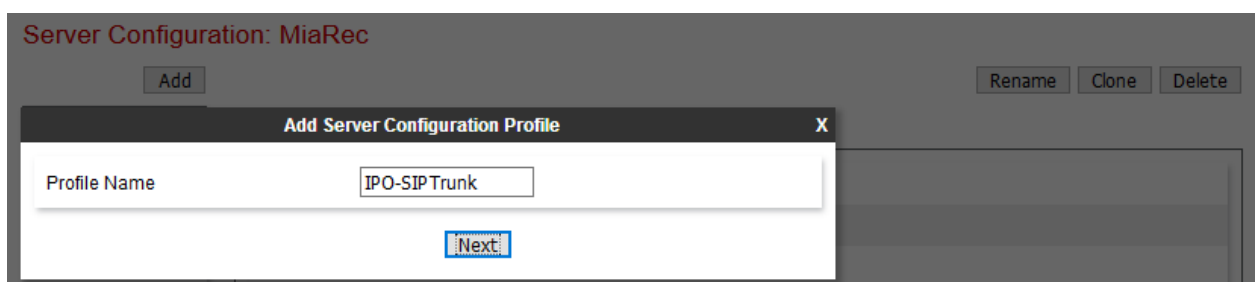
Select **Next** and select the **Interworking Profile** configured in previous section for MiaRec. Select **Finish** once done.



The screenshot shows a dialog box titled "Edit Server Configuration Profile - Advanced". It contains the following fields and controls:

- Enable Grooming:** A checkbox that is checked.
- Interworking Profile:** A dropdown menu showing "MiaRec".
- Signaling Manipulation Script:** A dropdown menu showing "None".
- Securable:** A checkbox that is unchecked.
- Enable FGDN:** A checkbox that is unchecked.
- TCP Failover Port:** A text input field.
- TLS Failover Port:** A text input field.
- Tolerant:** A checkbox that is unchecked.
- URI Group:** A dropdown menu showing "None".
- Buttons:** "Finish" at the bottom.

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



The screenshot shows a dialog box titled "Add Server Configuration Profile". It contains the following fields and controls:

- Profile Name:** A text input field containing "IPO-SIP Trunk".
- Buttons:** "Next" at the bottom.

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**.

**Edit Server Configuration Profile - General**

Server Type: Trunk Server

SIP Domain: avaya.com

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
10.64.110.65	5060	TCP

Delete

Back Next

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

**Add Server Configuration Profile - Advanced**

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: IPO-SIPTrunk

Signaling Manipulation Script: None

Securable: ☐

Enable FGDN: ☐

TCP Failover Port: 5060

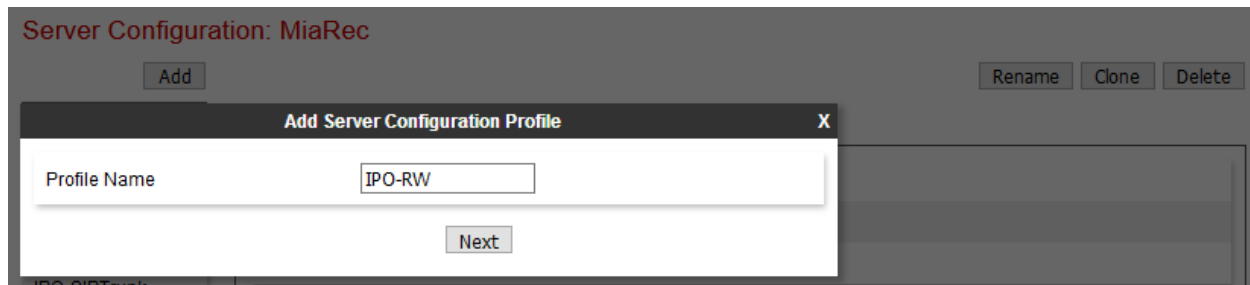
TLS Failover Port: 5061

Tolerant: ☐

URI Group: None

Back Finish

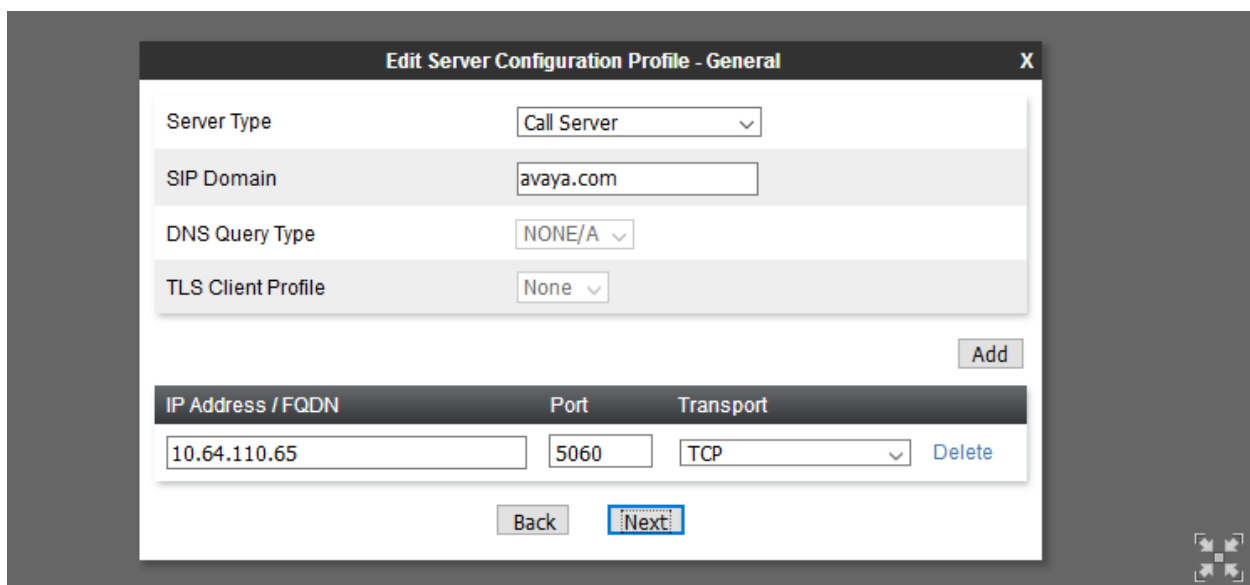
To define another Server for IP Office, click on **Add** and enter an appropriate name in the pop-up menu.



The screenshot shows a window titled "Server Configuration: MiaRec". In the top right corner, there are buttons for "Rename", "Clone", and "Delete". A modal dialog box titled "Add Server Configuration Profile" is open in the center. It has a close button "X" in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "IPO-RW". Below the input field is a "Next" button.

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**, 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**.

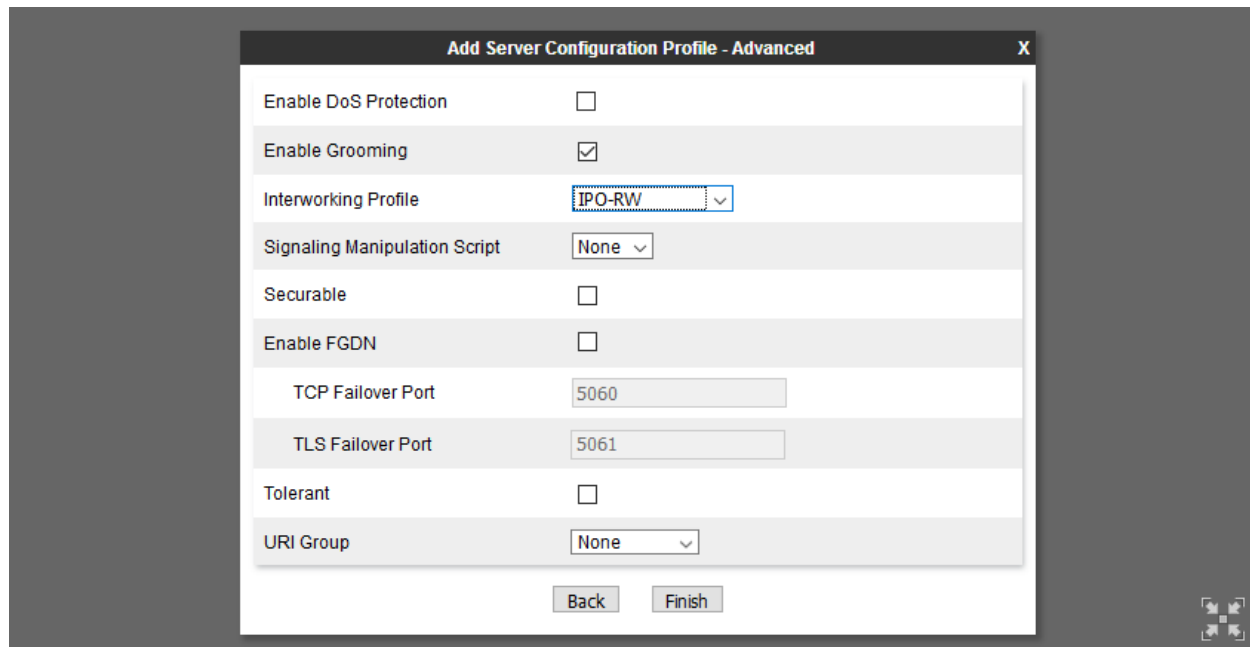


The screenshot shows a dialog box titled "Edit Server Configuration Profile - General" with a close button "X" in the top right corner. The dialog contains several fields and a table:

- Server Type**: A dropdown menu with "Call Server" selected.
- SIP Domain**: A text input field containing "avaya.com".
- DNS Query Type**: A dropdown menu with "NONE/A" selected.
- TLS Client Profile**: A dropdown menu with "None" selected.
- Add**: A button located to the right of the TLS Client Profile dropdown.
- Table**: A table with three columns: "IP Address / FQDN", "Port", and "Transport".

IP Address / FQDN	Port	Transport
10.64.110.65	5060	TCP
- Delete**: A blue text link located to the right of the table.
- Back**: A button at the bottom left.
- Next**: A button at the bottom center, which is highlighted with a blue border.

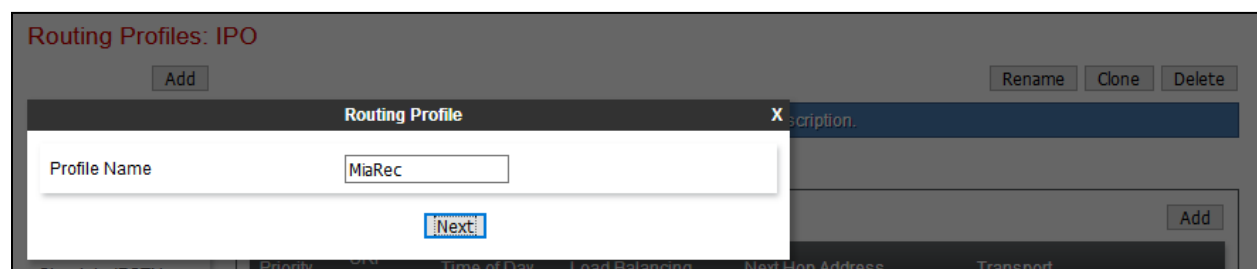
Select **Next** and configure the **Interworking Profile** configured in previous section for IP Office. Select **Finish** once done.



## 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**.

Profile : MiaRec - Edit Rule

URI Group: \* Time of Day: default

Load Balancing: Priority NAPTR:

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	MiaRec	10.64.110.26:5080 (TCP)	None

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.

Routing Profiles: IPO-RW

Add Rename Clone Delete

Routing Profile

Profile Name: IPO-SIPTrunk

Next

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**.

Profile : IPO-SIPTrunk - Edit Rule

URI Group: \* Time of Day: default

Load Balancing: Priority NAPTR: ☐

Transport: None Next Hop Priority: ☒

Next Hop In-Dialog: ☐ Ignore Route Header: ☐

ENUM: ☐ ENUM Suffix:

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IPO-SIPTrunk	10.64.110.65:5060 (TCP)	None

Delete

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.

Routing Profiles: IPO-RW

Add Rename Clone Delete

Routing Profile

Profile Name: IPO-RW

Next

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**.

Profile : IPO-RW - Edit Rule

URI Group: \* Time of Day: default

Load Balancing: Priority Transport: None

Next Hop In-Dialog: ☐ Next Hop Priority: ☒

ENUM: ☐ Ignore Route Header: ☐

ENUM Suffix:

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	IPO-RW	10.64.110.65:5060 (TCP)	None

Delete

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**.

Application Rules: MiaRec

Add Filter By Device... Rename Clone Delete

Application Rule

Rule Name: MiaRec

Next



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

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	100
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	<input checked="" type="radio"/> Off <input type="radio"/> RADIUS <input type="radio"/> CDR Adjunct
RADIUS Profile	None
Media Statistics Support	<input type="checkbox"/>
Call Duration	<input checked="" type="radio"/> Setup <input type="radio"/> Connect
RTCP Keep-Alive	<input type="checkbox"/>

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**.

Media Rules: MiaRec

Add Filter By Device... Rename Clone Delete

Media Rule

Rule Name: MiaRec

Next

Preferred Formats: SRTP, AES, CM, 128, HMAC, SHA1, 32

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

**Media Rule** X

**Audio Encryption**

Preferred Format #1

Preferred Format #2

Preferred Format #3

Encrypted RTCP ☒

MKI ☐

Lifetime  Leave blank to match any value.

Interworking ☐

**Video Encryption**

Preferred Format #1

Preferred Format #2

Preferred Format #3

Encrypted RTCP ☒

MKI ☐

Lifetime  Leave blank to match any value.

Interworking ☐

**Miscellaneous**

Capability Negotiation ☒

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).

The screenshot shows the 'Media Rule' configuration window. It is divided into two main sections: 'Audio Codec' and 'Video Codec'.

**Audio Codec Section:**

- Codec Prioritization:** ☒ (checked)
- Allow Preferred Codecs Only:** ☐ (unchecked)
- Transcode:** ☐ (unchecked)
- Transrating:** ☐ (unchecked)
- Preferred Codecs:**
  - Available:** G728 (15), DVI4 (16), DVI4 (17), G729AB (18) [T], G726-32 [DT], OPUS Constrained Narrow Band [T], OPUS Narrow Band [DT], OPUS Wide Band [DT].
  - P-Time (Optional):** 10, 20 (selected), 30, 60.
  - Selected:** PCMU (0) [T], G729 (18) [T], telephone-event [D].

**Video Codec Section:**

- Codec Prioritization:** ☐ (unchecked)
- Allow Preferred Codecs Only:** ☐ (unchecked)
- Transcode When Needed:** ☐ (unchecked)
- Transrating:** ☐ (unchecked)
- Preferred Codecs:**
  - Available:** CelB (25), JPEG (26), nv (28), H261 (31), MPV (32), MP2T (33), H263 (34).
  - Selected:** (empty)

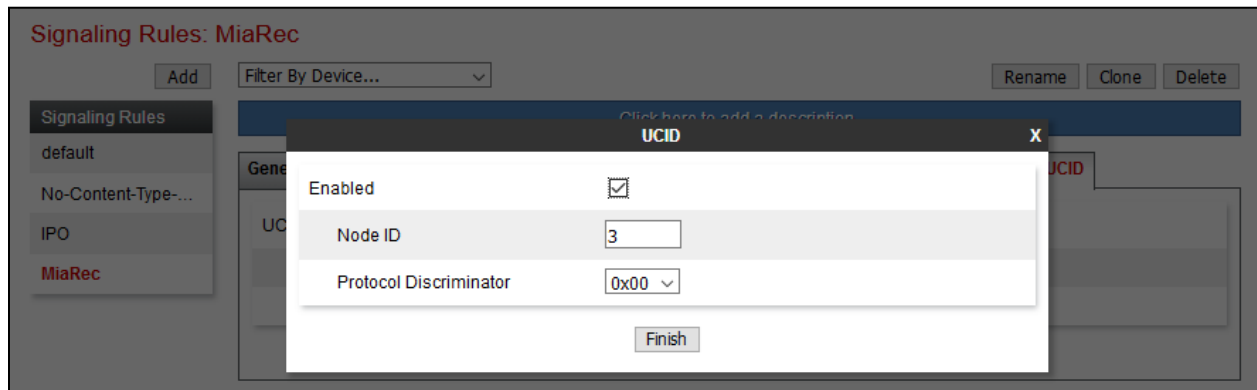
At the bottom of the window are 'Back' and 'Next' buttons.

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

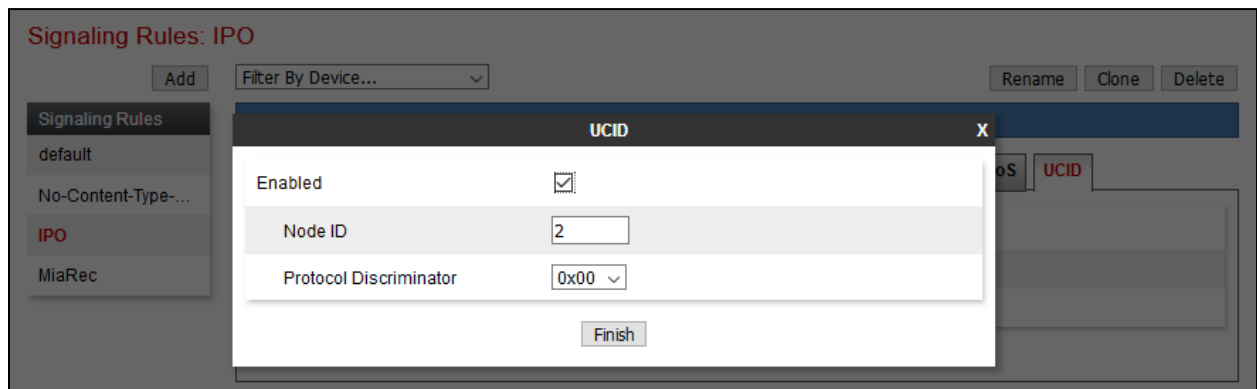
## 6.7. Configure UCID

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.

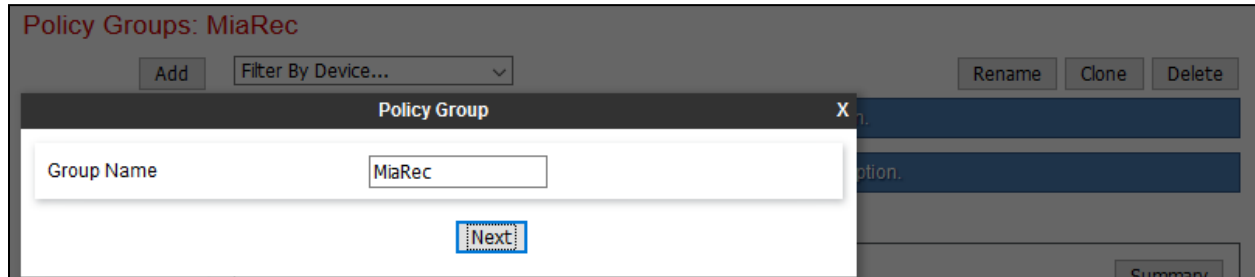


Perform similar steps for IP Office Signaling Rule.



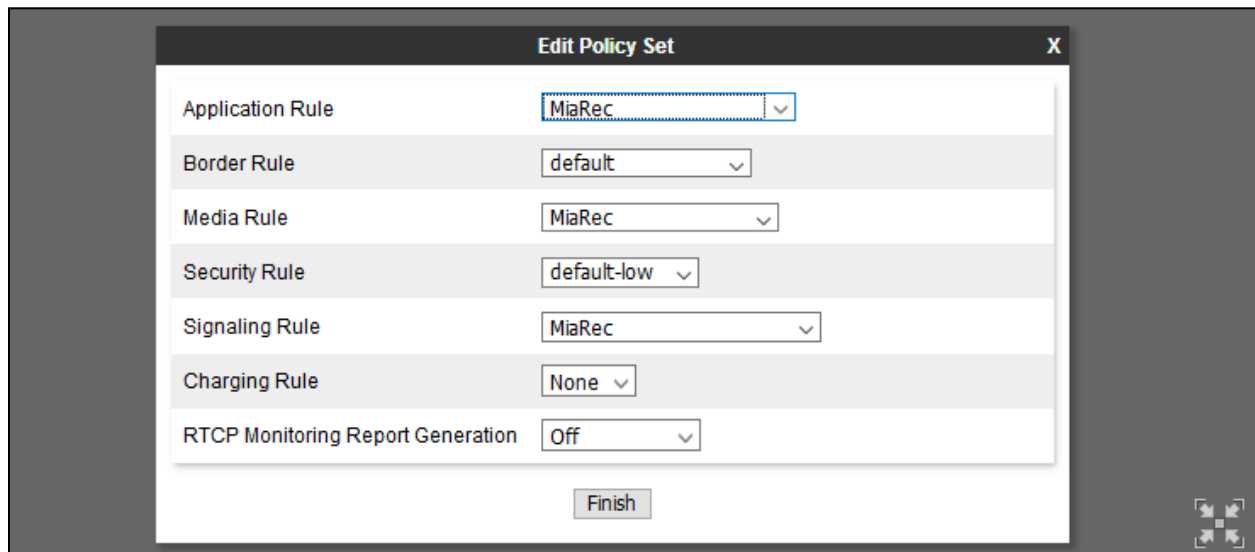
## 6.8. Define End Point Policy Group

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**.



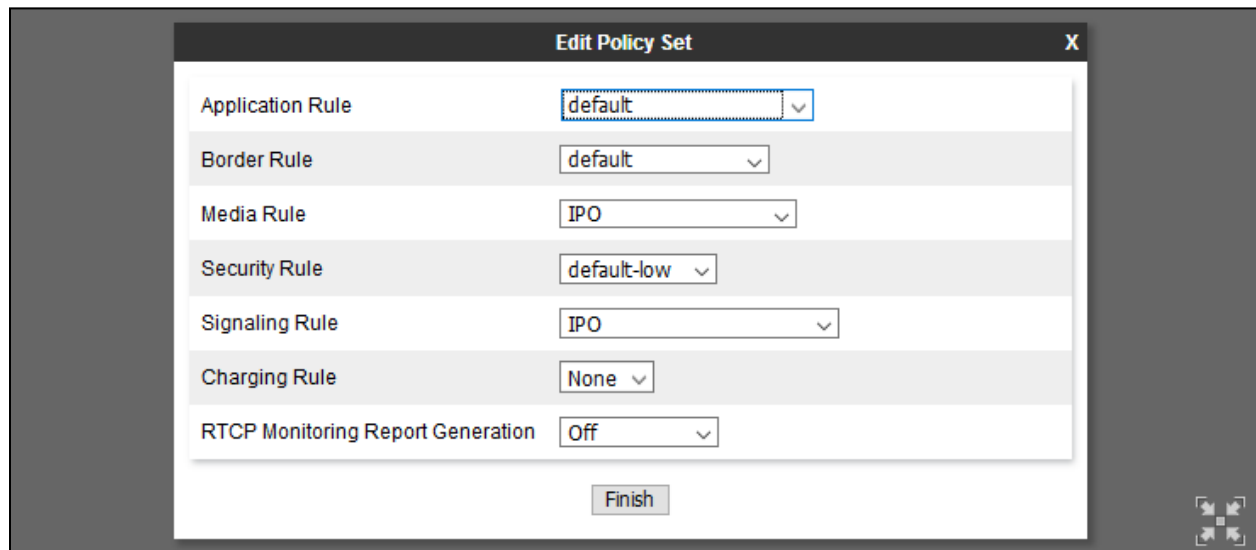
The screenshot shows a 'Policy Groups: MiaRec' window. At the top, there is an 'Add' button and a 'Filter By Device...' dropdown. Below this is a 'Policy Group' header with a close button 'X'. The main area contains a 'Group Name' field with the text 'MiaRec' and a 'Next' button at the bottom right. In the background, there are buttons for 'Rename', 'Clone', and 'Delete', and a 'Summary' button at the bottom right.

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.



The screenshot shows an 'Edit Policy Set' window with a close button 'X'. It contains several dropdown menus for configuring rules: 'Application Rule' (MiaRec), 'Border Rule' (default), 'Media Rule' (MiaRec), 'Security Rule' (default-low), 'Signaling Rule' (MiaRec), 'Charging Rule' (None), and 'RTCP Monitoring Report Generation' (Off). A 'Finish' button is located at the bottom center. A small icon with four arrows is in the bottom right corner.

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.



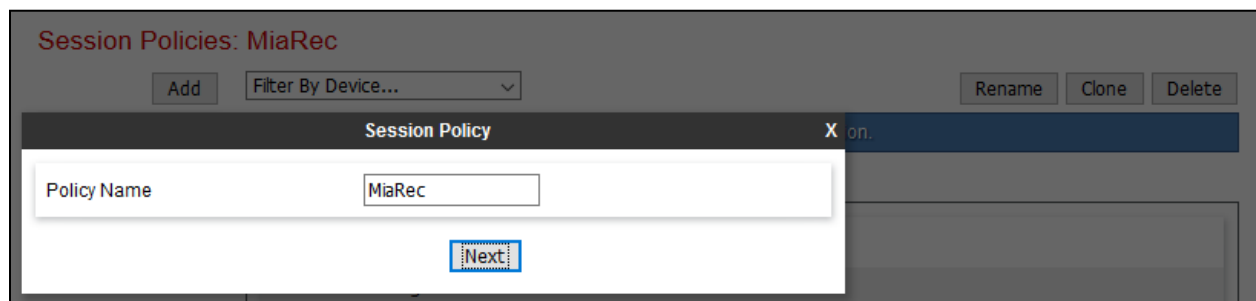
**Edit Policy Set** X

Application Rule	default
Border Rule	default
Media Rule	IPO
Security Rule	default-low
Signaling Rule	IPO
Charging Rule	None
RTCP Monitoring Report Generation	Off

Finish

## 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**.



**Session Policies: MiaRec**

Add Filter By Device... Rename Clone Delete

**Session Policy** X on.

Policy Name MiaRec

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**.

The screenshot shows a 'Media' configuration window with the following settings:

Setting	Value
Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input checked="" type="checkbox"/>
Recording Type	Full Time
Play Recording Tone	<input type="checkbox"/>
Call Termination on Recording Failure	<input type="checkbox"/>
Routing Profile	MiaRec
Media Server	<input type="checkbox"/>
Routing Profile	None
Call Type for Media Unanchoring	Media Tromboning Only

At the bottom of the window is a 'Finish' button.

## 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.

The screenshot shows a configuration window titled "Edit Flow: MiaRec". The window contains the following fields and controls:

- Flow Name:** A text input field containing "MiaRec".
- URI Group #1:** A dropdown menu with an asterisk (\*) as the selected option.
- URI Group #2:** A dropdown menu with an asterisk (\*) as the selected option.
- Subnet #1:** A text input field with an asterisk (\*) and an example "Ex: 192.168.0.1/24".
- SBC IP Address:** A dropdown menu with an asterisk (\*) as the selected option.
- Subnet #2:** A text input field with an asterisk (\*) and an example "Ex: 192.168.0.1/24".
- SBC IP Address:** A dropdown menu with an asterisk (\*) as the selected option.
- Session Policy:** A dropdown menu with "MiaRec" as the selected option.
- Has Remote SBC:** A checkbox that is currently unchecked.
- Finish:** A button at the bottom center of the window.



## 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.

### Signaling Interface: SBCE

Devices

SBCE

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
ExternalSig-SIPTrunk	[REDACTED] External (B1, VLAN 0)	5060	5060	---	None	Edit Delete
ExternalSig-RW	[REDACTED] External (B1, VLAN 0)	5060	5060	---	None	Edit Delete
InternalSig-RW	10.64.110.33 Internal (A1, VLAN 0)	5060	5060	---	None	Edit Delete
InternalSig-SIPTrunk	10.64.110.32 Internal (A1, VLAN 0)	5060	5060	---	None	Edit Delete

## 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.

### Media Interface: SBCE

Devices

SBCE

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from [System Management](#).

Add

Name	Media IP Network	Port Range	
ExternalMedia-RW	[REDACTED] External (B1, VLAN 0)	35000 - 40000	Edit Delete
ExternalMedia-SIPTrunk	[REDACTED] External (B1, VLAN 0)	35000 - 40000	Edit Delete
InternalMedia-SIPTrunk	10.64.110.32 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
InternalMedia-RW	10.64.110.33 Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

## 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.

End Point Flows: SBCE

Click here to add a row description.

**Server Configuration: IPO-RW**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	IPO-RW	*	ExternalSig-RW	InternalSig-RW	IPO	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Server Configuration: IPO-SIPTrunk**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	toIPOffice	*	ExternalSig-SIPTrunk	InternalSig-SIPTrunk	default-low	SimulatedPSTN	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Server Configuration: MiaRec**

[Update](#)

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	MiaRec_RW	*	InternalSig-RW	InternalSig-SIPTrunk	default-low	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
2	MiaRec_External	*	ExternalSig-SIPTrunk	InternalSig-SIPTrunk	default-low	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
3	MiaRec_Internal	*	InternalSig-SIPTrunk	InternalSig-SIPTrunk	default-low	default	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

**Server Configuration: SimulatedPSTN**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	fromIPOffice	*	InternalSig-SIPTrunk	ExternalSig-SIPTrunk	IPO	IPO-SIPTrunk	<a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

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.

The screenshot shows the 'Edit Flow: IPOffice\_Users' dialog box with the 'Criteria' tab selected. The dialog contains several input fields for defining flow criteria:

Criteria	
Flow Name	IPOffice_Users
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	ExternalSig-RW

A 'Next' button is located at the bottom right of the dialog.

The screenshot shows the 'Edit Flow: IPOffice\_Users' dialog box with the 'Profile' tab selected. The dialog contains settings for the flow profile:

Profile	
Source	<input checked="" type="radio"/> Subscriber <input type="radio"/> Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	ExternalMedia-RW
Secondary Media Interface	None
Received Interface	None
End Point Policy Group	IPO
Routing Profile	IPO-RW

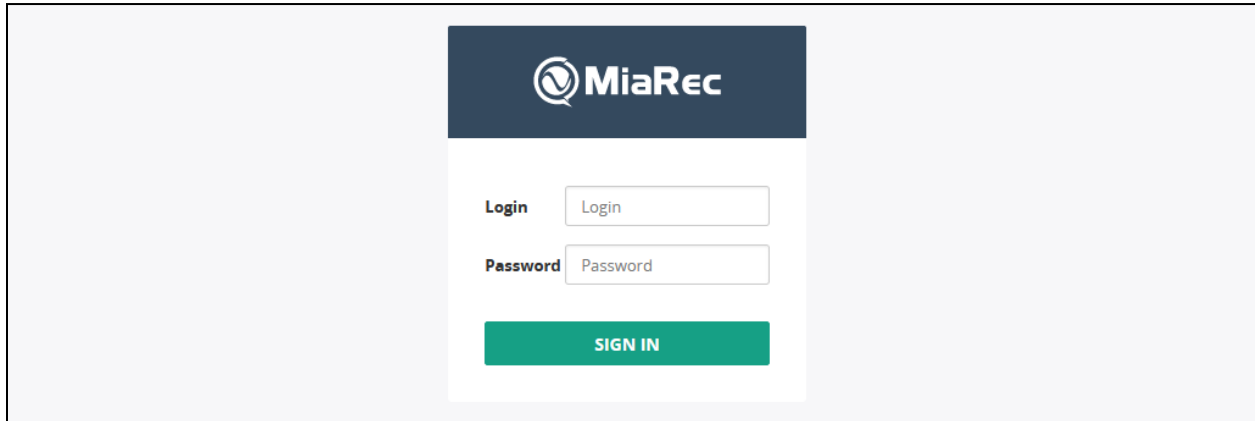
Below the profile settings is the 'Optional Settings' section:

Optional Settings	
TLS Client Profile	None
Signaling Manipulation Script	None
Presence Server Address Ex: domain.com, 192.168.0.101	

'Back' and 'Finish' buttons are located at the bottom of the dialog.

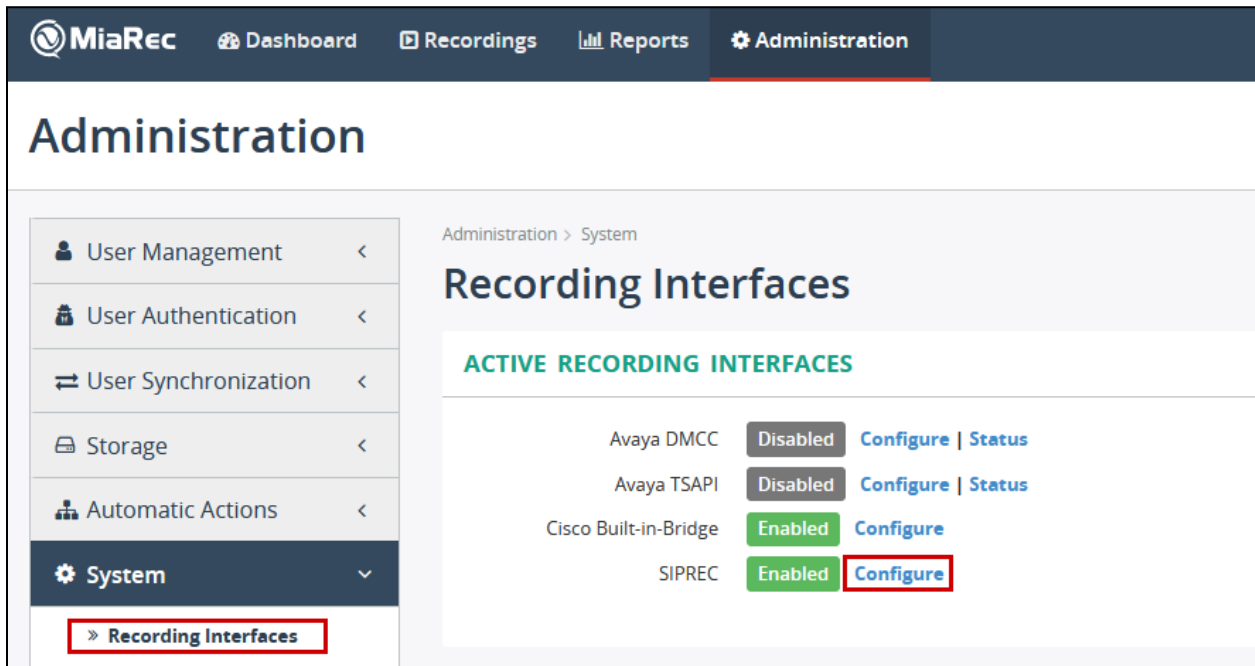
## 7. Configure the MiaRec

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.



The image shows the MiaRec login page. It features the MiaRec logo at the top. Below the logo, there are two input fields: 'Login' and 'Password'. A green 'SIGN IN' button is positioned below the password field.

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



The image shows the MiaRec Administration interface. The top navigation bar includes 'Dashboard', 'Recordings', 'Reports', and 'Administration'. The 'Administration' section is expanded, showing a sidebar with 'User Management', 'User Authentication', 'User Synchronization', 'Storage', 'Automatic Actions', 'System', and 'Recording Interfaces'. The 'System' section is selected, and the 'Recording Interfaces' page is displayed. The page title is 'Recording Interfaces'. Below the title, there is a section for 'ACTIVE RECORDING INTERFACES' with a table listing recording interfaces and their status.

Interface	Status	Action
Avaya DMCC	Disabled	<a href="#">Configure</a>   <a href="#">Status</a>
Avaya TSAPI	Disabled	<a href="#">Configure</a>   <a href="#">Status</a>
Cisco Built-in-Bridge	Enabled	<a href="#">Configure</a>
SIPREC	Enabled	<a href="#">Configure</a>

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).

## Configure Recording Interface

**Enable \***

☒ Enable SIPREC recording

No-Audio Begin Timeout

240

seconds

This timeout specifies how long to wait for the first RTP media packet before give up

No-Audio Normal Timeout

3600

seconds

In case of RTP transmission stopping, this timeout specifies how long to wait for RTP restoration before forcibly completing call recording

Signaling UDP port

5080

Listening UDP port for SIPREC signaling (use 0 to disable UDP)

Signaling TCP port

5080

Listening TCP port for SIPREC signaling (use 0 to disable TCP)

Signaling TLS port

0

Listening TLS port for encrypted SIP signaling (use 0 to disable TLS)

Begin RTP port range

22000

Begin UDP port range for RTP media

## 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**.

The screenshot shows the AVAYA IP Office System Status application. The left sidebar contains navigation links: System, Alarms (2), Extensions (2), Trunks (1), Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area is titled "IP Office System Status" and has tabs for Status, Utilization Summary, and Alarms. The "Status" tab is selected, showing the "SIP Trunk Summary" for "Line: 1".

**SIP Trunk Summary:**

- Line Service State: In Service
- Peer Domain Name: sip://10.64.110.33
- Resolved Address: 10.64.110.33
- Line Number: 1
- Number of Administered Channels: 100
- Number of Channels in Use: 0
- Administered Compression: G711 Mu, G711 A, G729 A
- Enable Faststart: Off
- Silence Suppression: Off
- Media Stream: RTP
- Layer 4 Protocol: TCP
- SIP Trunk Channel Licenses: 100
- SIP Trunk Channel Licenses in Use: 0 (0%)
- SIP Device Features: UPDATE (Incoming and Outgoing)

Below the summary is a table showing the current state of SIP channels:

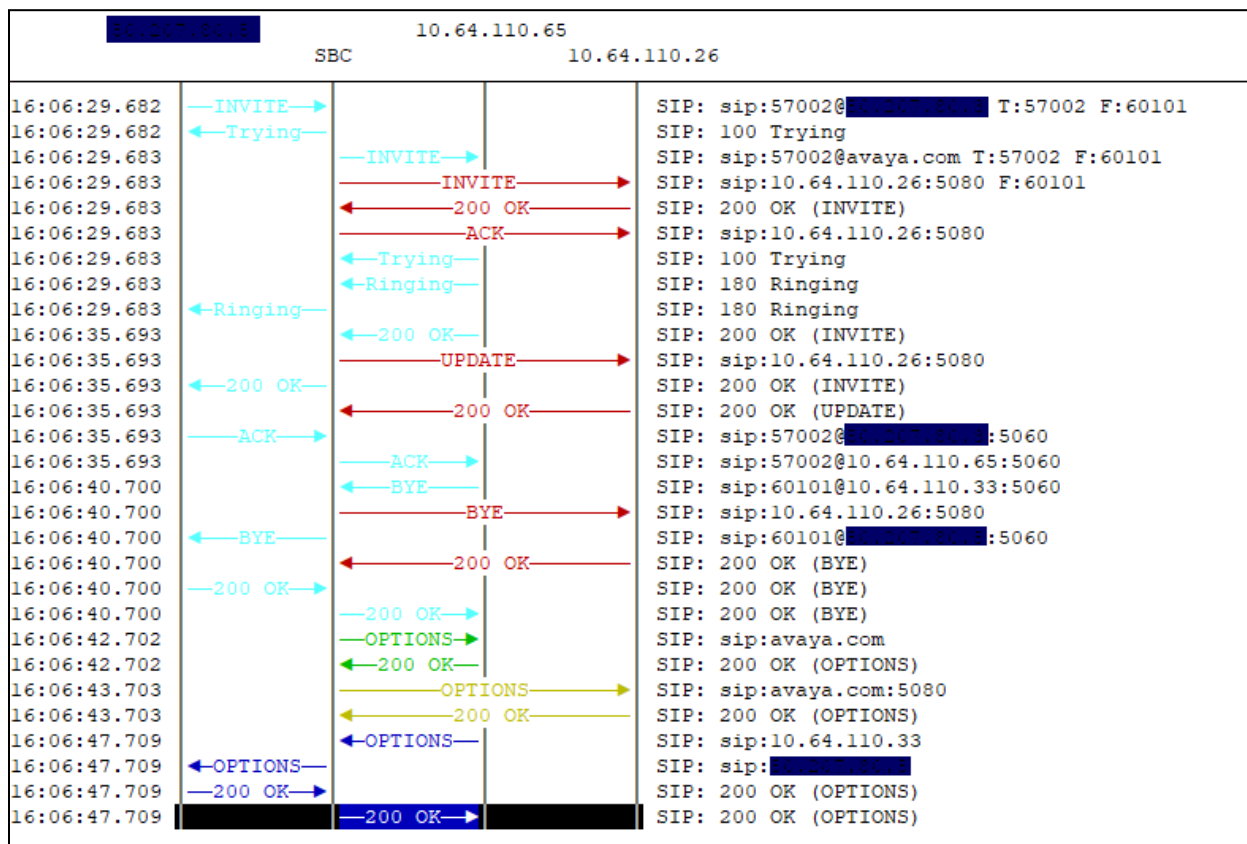
Channel Number	URI G...	Call Ref	Current State	Time in State	Remote Media Ad...	Codec	Connec...	Caller ID or Diale...	Other Party on Call	Direction of Call	Round Trip Delay	Receive Jitter	Receive Packet...	Transmit Jitter	Transmit Packe...
1			Idle	02:24:47											
2			Idle	02:24:47											
3			Idle	2 days 01:17:00											
4			Idle	2 days 01:17:00											
5			Idle	2 days 01:17:00											
6			Idle	2 days 01:17:00											
7			Idle	2 days 01:17:00											
8			Idle	2 days 01:17:00											
9			Idle	2 days 01:17:00											
10			Idle	2 days 01:17:00											

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**.

The screenshot shows the AVAYA Server Status application. The "Server Status" tab is selected, displaying a table of server profiles:

Server Profile	Server FQDN	Server IP	Server Port	Server Transport	Heartbeat Status	Registration Status	TimeStamp
MiaRec	10.64.110.26	10.64.110.26	5080	TCP	UP	UNKNOWN	02/28/2019 16:02:43 MST
SimulatedPSTN	10.255.255.5	10.255.255.5	5060	TCP	UP	UNKNOWN	02/28/2019 16:02:52 MST
IPO	10.64.110.65	10.64.110.65	5060	TCP	UP	UNKNOWN	02/28/2019 16:02:42 MST

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**.

The screenshot shows the MiaRec web interface with the 'Recordings' tab selected. The page displays a table of recorded calls with columns for User, Date, Time, Duration, From, To, and Categories. The table shows three calls recorded today.

USER	DATE	TIME	DURATION	FROM	TO	CATEGORIES
SIP Trunk User 2, Internal User 2	Today	6:15 PM	0:06	57002	61111	
SIP Trunk User 2, Internal User 2	Today	6:13 PM	0:05	57002	61111	
Internal User 2, SIP Trunk User 1	Today	6:13 PM	0:12	57002	60101	



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


## Call 57002 -> 61111

[Mark as confidential](#)[Delete Call](#)

Edit Categories ▾

### MEDIA PLAYER

Switch to basic player | Wide view ↗



[▶ Play](#)[x1](#)[x1.2](#)[x1.5](#)[x1.7](#)[x2](#)[⬇️ Save audio file](#)

#### INFO

Date: **Today**

Connect Time: **6:13:32 PM**

Disconnect Time: **6:13:37 PM**

Duration: **0:05**

Watermark: [View](#)

#### FROM

User: [Internal User 2](#)

Group: [Agents](#)

Phone Number: **57002**

Phone Name:

Phone Id: **sip:57002@10.64.110.65**

Ip-address: **10.64.110.32 (17391)**

[🔊 Live monitor phone 57002](#)

#### TO

User: [SIP Trunk User 2](#)

Group: [Agents](#)

Phone Number: **61111**

Phone Name:

Phone Id: **sip:61111@10.64.110.33**

Ip-address: **10.64.110.26 (5080)**

[🔊 Live monitor phone 61111](#)

## 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/>.

---

**©2019 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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