Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Fonolo In-Call Rescue with Avaya IP Office Server Edition using SIP Trunks – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue application to interoperate with Avaya IP Office Server Edition using SIP trunks. In-Call Rescue provides functionality to replace hold-time with a call-back.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue (ICR) to interoperate with Avaya IP Office Server Edition (IP Office) using SIP trunks. ICR provides functionality to replace hold-time with a call-back and during this compliance tesing was hosted on the cloud by Fonolo. The solution communicates via SIP/RTP. The ICR functionality was compliance tested utilizing SIP trunks to IP Office. The configuration allowed IP Office to use SIP trunking for calls to and from the ICR application. The ICR is a contact center solution where instead of a caller staying in the queue when agents are all busy, can request to get a call back when an agent becomes available.

When a caller encounters a scenario where no agents are available in a call center environment and IP Office is part of that environment, the caller is presented with options by the call center to either continue waiting in the queue or receive a call back from the call center. If the caller chose the latter, then the call center directs the caller to ICR via IP Office SIP trunks where ICR then provides a message to the caller to leave a call back number, so that ICR can call back the caller when an agent becomes available. Once ICR receives the confirmed call back number from the caller, ICR uses SIP trunk with IP Office to call back into the call center) and wait in the queue until an agent becomes available. When an agent becomes available, ICR informs the agent that there is a call waiting and if the agent would like to get connected to the caller. If the agent accepts to connect to the caller, ICR then calls the caller via SIP trunks to IP Office and connects the caller with the available agent. When ICR makes an outbound call to the caller and agent via IP Office, it makes two SIP INVITE requests. One to the available agent and one to the caller and then mixes the audio within the ICR server.

The IP Office Server Edition configuration consisted of two IP Office systems, a primary Linux server and an expansion IP500V2 that were connected via Small Community Network (SCN) trunks.

The SIP trunks connection from ICR can be with either the primary Linux server or the expansion IP500V2 IP Office system. The configuration shown in these Application Notes used the primary Linux server IP Office system for SIP trunks connectivity.

For security purposes public and Lab IP addresses have been altered in this document.

2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying inbound and outbound calls flows between IP Office and ICR. The feature test cases were performed manually. Calls were placed manually from users on the PSTN to a call center Control Directory Number (CDN). During compliance testing Avaya Contact Center Select (Contact Center Select) was used to eumulate a call center. Assumption was made during compliance testing in the Contact Center Select script to direct callers to ICR when no agents are available. When caller connected with ICR, ICR read the call back number of the caller or asked caller to input a new call back number. ICR recognized the Dual Tone Multi Frequency (DTMF) input provided by the caller confirming the call back number. For compliance testing purposes, agents were made available after the above call between caller and ICR is completed. ICR then called into the call center CDN and connected with an available agent. ICR provided a recording informing the agent of a call in waiting and if the agent wants to get connected to the PSTN caller. Agent accepted the call by using DTMF input. ICR then made the second outbound call to the PSTN caller via IP Office and if the PSTN caller answered the call he/she then get connected with the agent. During compliance testing agents were present on both primary and expansion IP Office systems.

The serviceability test cases were performed manually by disconnecting and reconnecting the SIP trunk connection to ICR.

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 this DevConnect Application Note 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 this Application Note, the interface between Avaya systems and Fonolo utilized enabled capabilities of TLS and SRTP.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The ICR application is hosted in a cloud environment by Fonolo. SIP trunks were used to connect the ICR application with IP Office. The following features and functionality were covered during compliance testing:

- Establishment of SIP trunks connectivity between ICR and IP Office including session refresh.
- Testing of G.711MU codec.
- Incoming calls to a CDN of Contact Center Select via IP Office can be redirected to the ICR application via the SIP trunks based on Contact Center Select scripting. Outgoing calls from ICR to the CDN via IP Office when callers decide on Call back. During this compliance testing Contact Center Select was used to simulate a call center environment and is not the scope of these Application Notes.
- The ICR application can make outbound call to the caller via IP Office who had selected the call back option and merge the call between the caller and and available agents (on both primary and expansion) . The outbound call is made via IP Office using SIP INVITE.
- DTMF transmission to ensure that options selected by the caller and agent is accepted correctly by ICR.

Serviceability testing focused on verifying the ability of ICR to recover from adverse conditions, such as the SIP trunks going down and reboot of IP Office.

2.2. Test Results

All test cases were executed and passed with the following exceptions/observations:

- ICR only supports G.711 codec variants.
- ICR only supports RFC2833 for DTMF transmission.

2.3. Support

Technical support on Fonolo ICR can be obtained through the following:

- **Phone:** 1-855-366-2500 (Toll-free)
- **Web:** https://fonolo.com/contact/
- **Email:** support@fonolo.com

3. Reference Configuration

A simulated enterprise site consisting of IP Office, Contact Center Select and Avaya telephones were used during compliance testing. As shown in **Figure 1**, SIP trunks were used to connect ICR with IP Office directly. IP Office is connected to an emulated PSTN using T1/PRI. A CDN and skillset is configured on Contact Center Select with a few agents belonging to the configured skillset. The configuration allowed the enterprise site to use SIP trunking for calls to and from ICR and IP Office.

During compliance testing inbound calls to Fonolo were sent to two of Fonolo's specific servers and outbound calls from Fonolo came from four of Fonolo's other servers. This architecture was implemented by Fonolo due to some PBX vendors cannot support inbound and outbound calls on the same SIP trunk. Due to this design intent of Fonolo, inbound and outbound calls to and from Fonolo were handled by different servers. All these servers were hosted on the cloud by Fonolo.

A CDN of 33000 was configured on Contact Center Select and agents from IP Office on both primary and expansion were logged into the pertinent skillset.

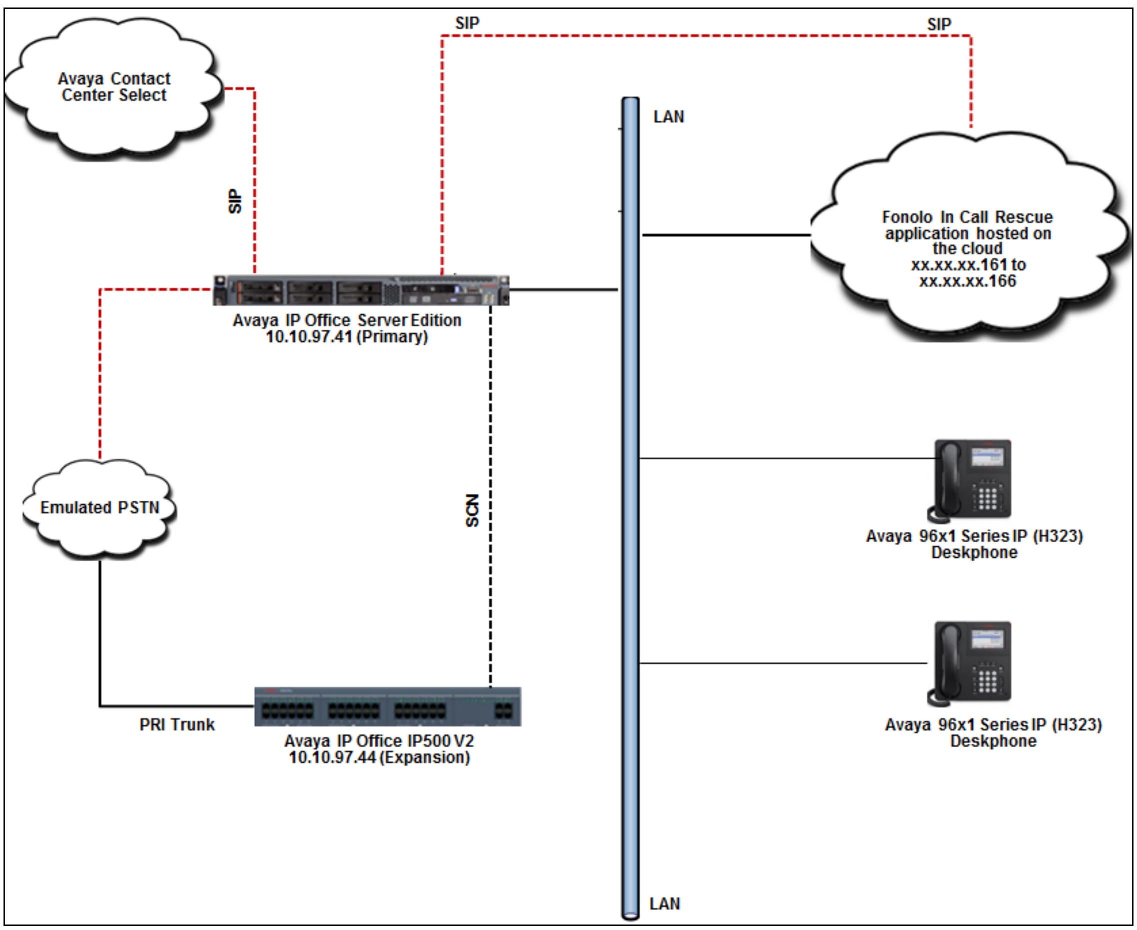


Figure 1: Avaya IP Office Network with Fonolo In-Call Rescue

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Linux (Primary)	10.1.0.0.0 build 237
Avaya IP Office IP500 V2 (Expansion)	10.1.0.0.0 build 237
Avaya Contact Center Select installed on VMware	7.0.1.1
Avaya Telephones: • 9650 IP (H323) Deskphone • 1140 IP (SIP) Deskphone • 9641 IP (H323) Deskphone	 3.270B 04.04.23.00 6.6401
Fonolo In-Call Rescue	3.0

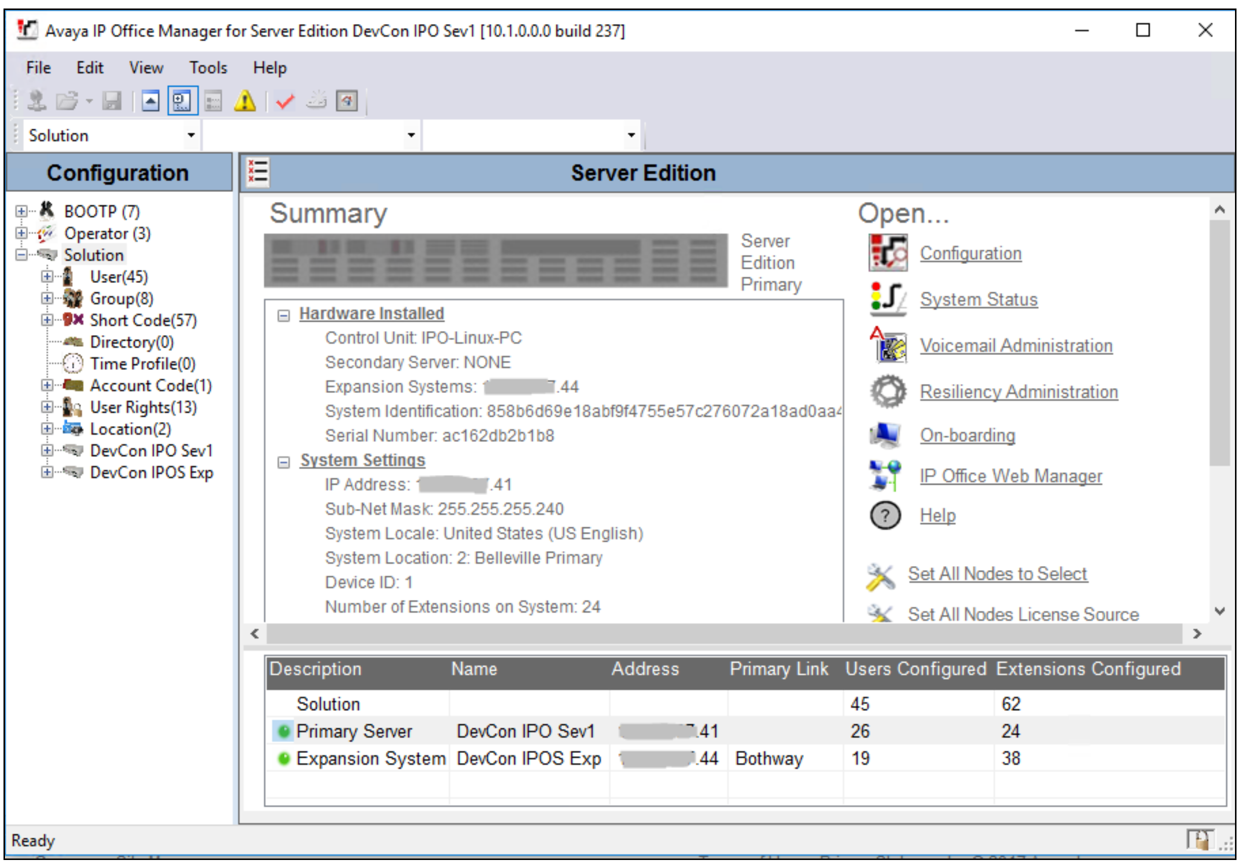
Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office IP500 V2 and also when deployed with IP Office Server Edition in all configurations.

5. Configure Avaya IP Office

Configuration and verification operations on the IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration done on the Primary (Linux server) system. It is implied a working system is already in place with the necessary licensing. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**. The configuration operations described in this section can be summarized as follows:

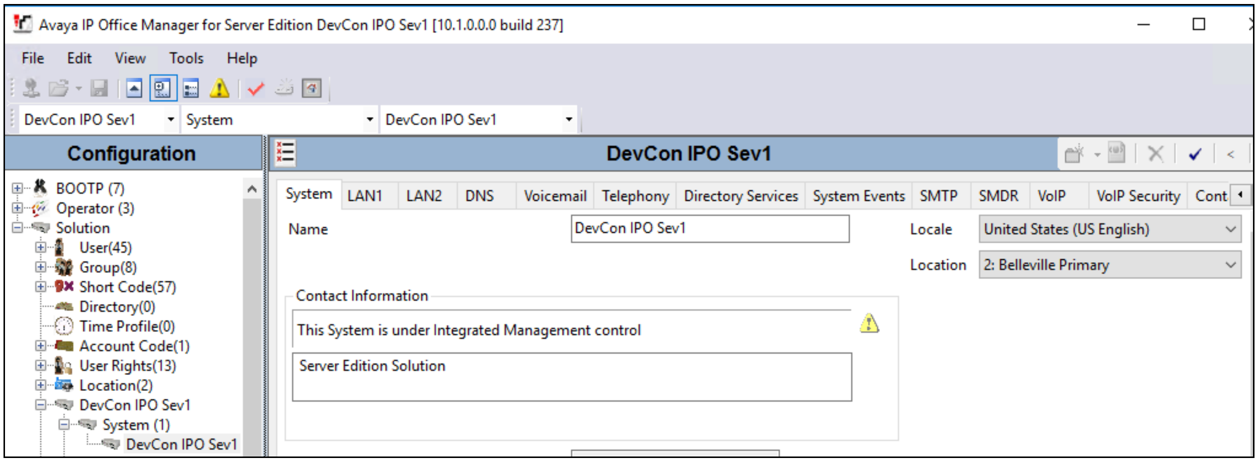
- Configure System Locale
- Configure System
- Create SIP Lines
- Configure Incoming Call Route
- Create Short Code (Route Calls)
- Save Configuration

From a PC running the IP Office Manager application, select **Start → Programs →IP Office → Manager** to launch the Manager application. Select the proper IP Office system. In this case the primary server and log in using the appropriate credentials. The **Avaya IP Office Manager for Server Edition** screen is displayed as shown below.



5.1. Configure System Locale

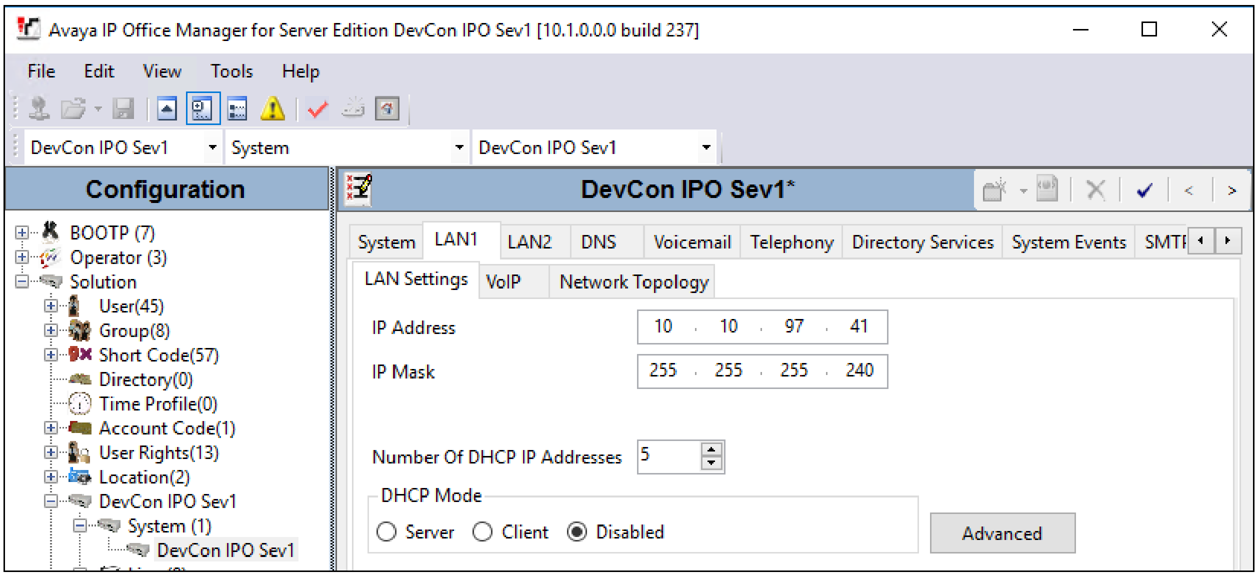
The Locale is usually the country where the IP Office is installed. By selecting the correct country a number of system defaults for that country will be used by the IP Office. To configure the Locale, select **DevCon IPO Sev1 → System →DevCon IPO Sev1**from the IP Office Configuration Tree. During compliance testing the System was called **DevCon IPO Sev1** for the Primary Server and **DevConIPOS Exp** for the Expansion IP500V2. In the right hand pane select the **System** tab, and from the **Locale** dropdown menu select the appropriate country (i.e. **United States (US English)**) as shown in the screen below. Click the **OK** button to save.



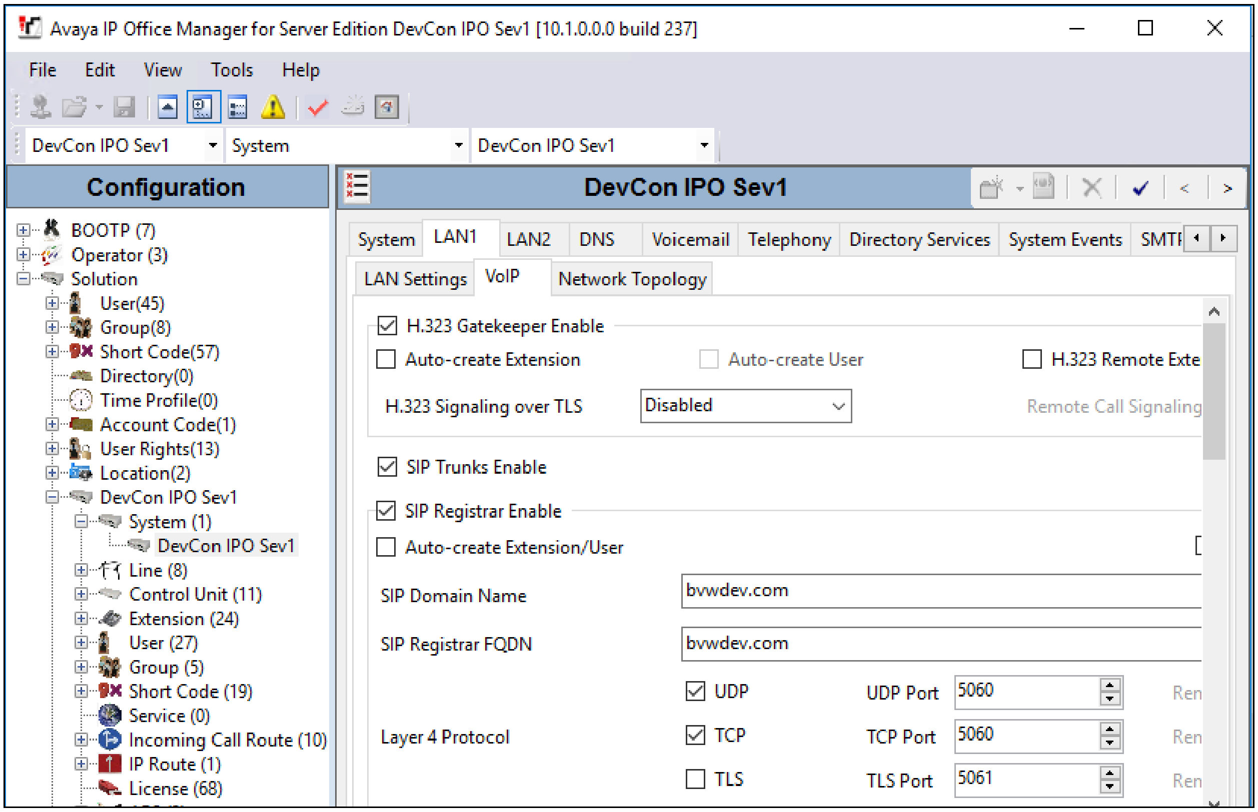
5.2. Configure System

From the configuration tree in the left pane, select **DevCon IPO Sev1 → System → DevCon IPO Sev1** to display the screen in the right pane, where **DevCon IPO Sev1** is the name of the IP Office system.

Select the **LAN1** tab, IP Office can support SIP on the LAN1 and/or LAN2 interfaces, however during compliance testing the LAN1 interface was used. From the **LAN Settings** sub-tab, note the **IP Address** configured, which is *10.10.97.41*. This IP address is required during ICR configuration.



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

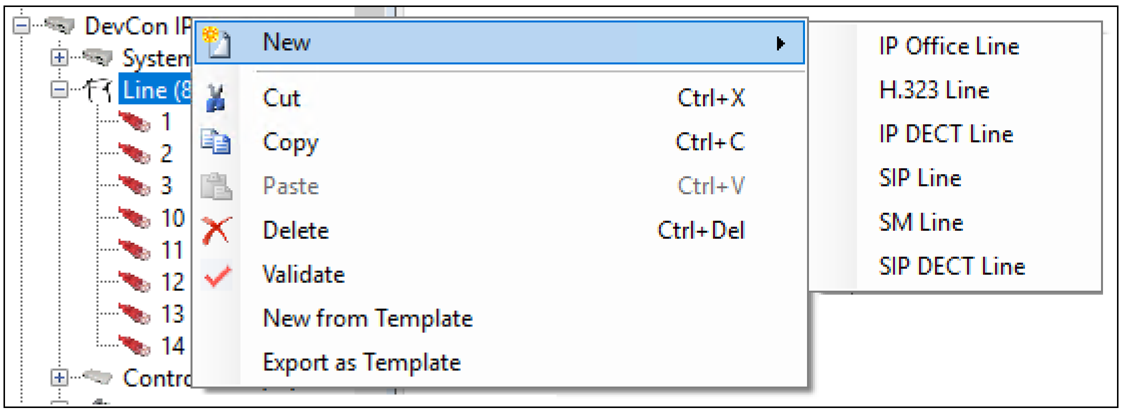


5.3. Create SIP Lines

During compliance testing two SIP lines were created since ICR used different servers for inbound and outbound calls. One line was for outgoing calls from IP Office to ICR, which is an inbound call for ICR and the other line was for incoming calls to IP Office from ICR, which is an outbound call for ICR.

5.3.1. Configure Outgoing SIP Line

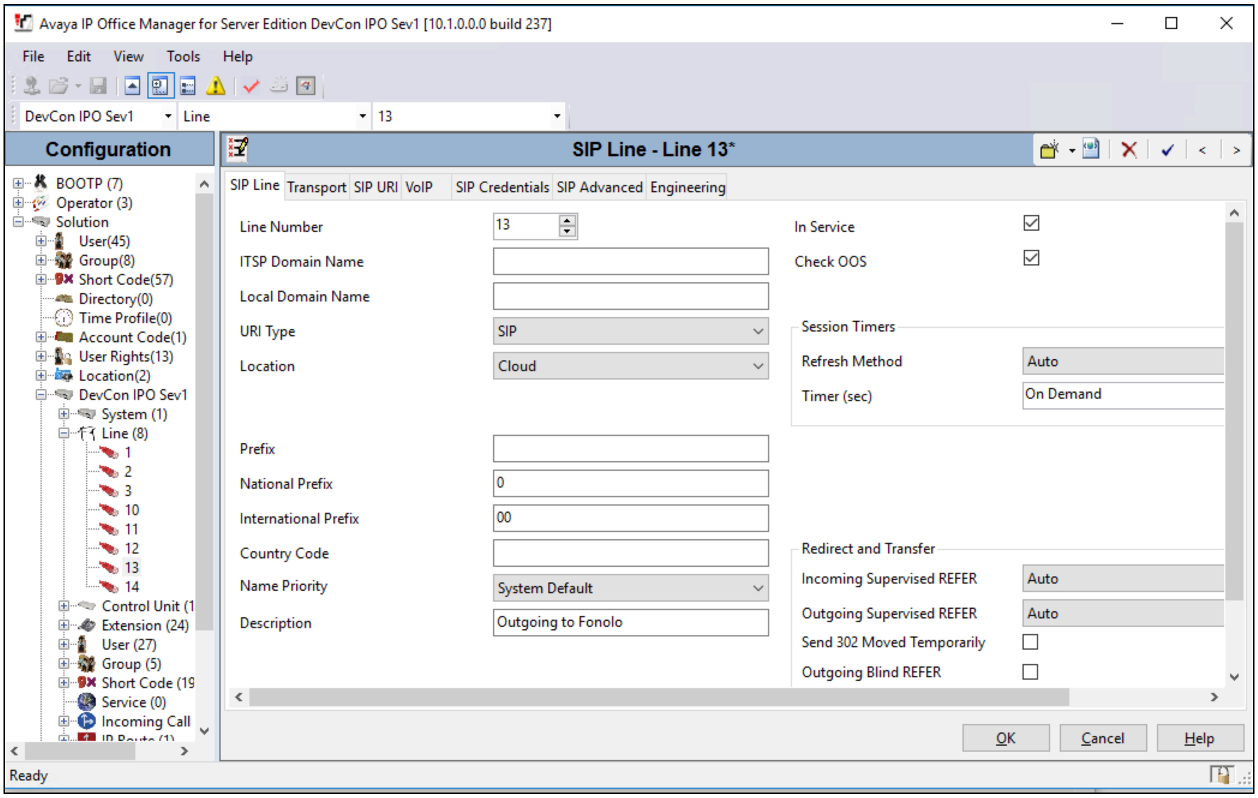
To create the SIP line from the IP Office for outgoing calls to ICR, navigate to **System → Line** and right click on **Line** followed by **New →SIP Line** as shown in the screen below. In this example, line **13** was created to connect to ICR. In terms of ICR, this is an inbound call coming to ICR from IP Office.



Screen below shows the configuration of the SIP Line in the subsequent **SIP Line** window; enter the following in the **SIP Line** tab.

- **Line Number:** Line number *13* was configured.
- **ITSP Domain Name:** Configure domain name of ICR or leave this field blank.
- **Description:** Provide a description for the SIP Line. This field is optional.

Retain default values for all remaining fields.



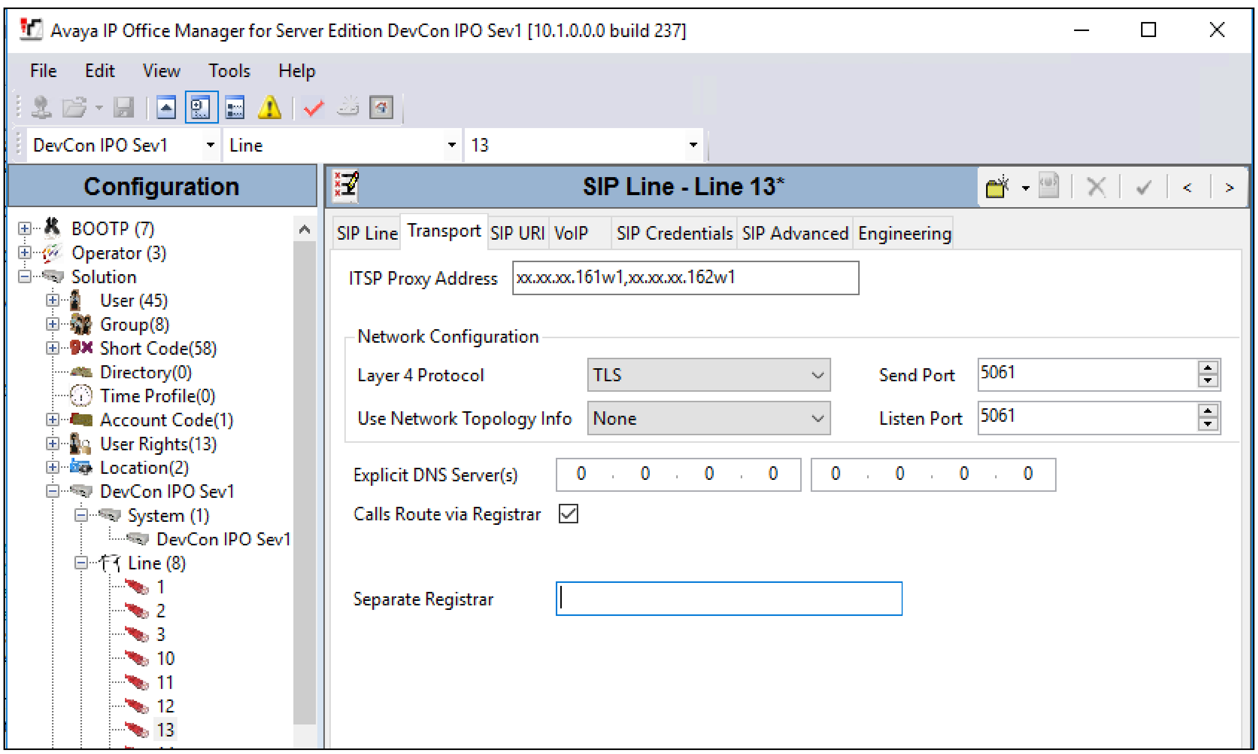
In the **Transport** tab enter IP address of ICR in the **ITSP Proxy Address** field. During compliance testing *xx.xx.xx.161w1,xx.xx.xx.162w1* was configured. ICR requested the use of two servers for outgoing calls.

In the **ITSP Proxy Address** field, a list of up to four IP addresses, with each address separated by a comma or space can be configured as per IP Office design. The addresses can include an indication of the relative call weighting of each address compared to the others. This is done by adding a *wN* suffix to the address where *N* is the weighting value.

For example during compliance testing for IP addresses *xx.xx.xx.161w1*, *xx.xx.xx.162w1*, the weighting values assign1 times the weight of calls to both addresses. The default weight if not specified is 1. A weight of 0 can be used to disable an address.

Under **Network Configuration**, in the **Layer 4 Protocol** field, select *TLS* from the drop down menu.

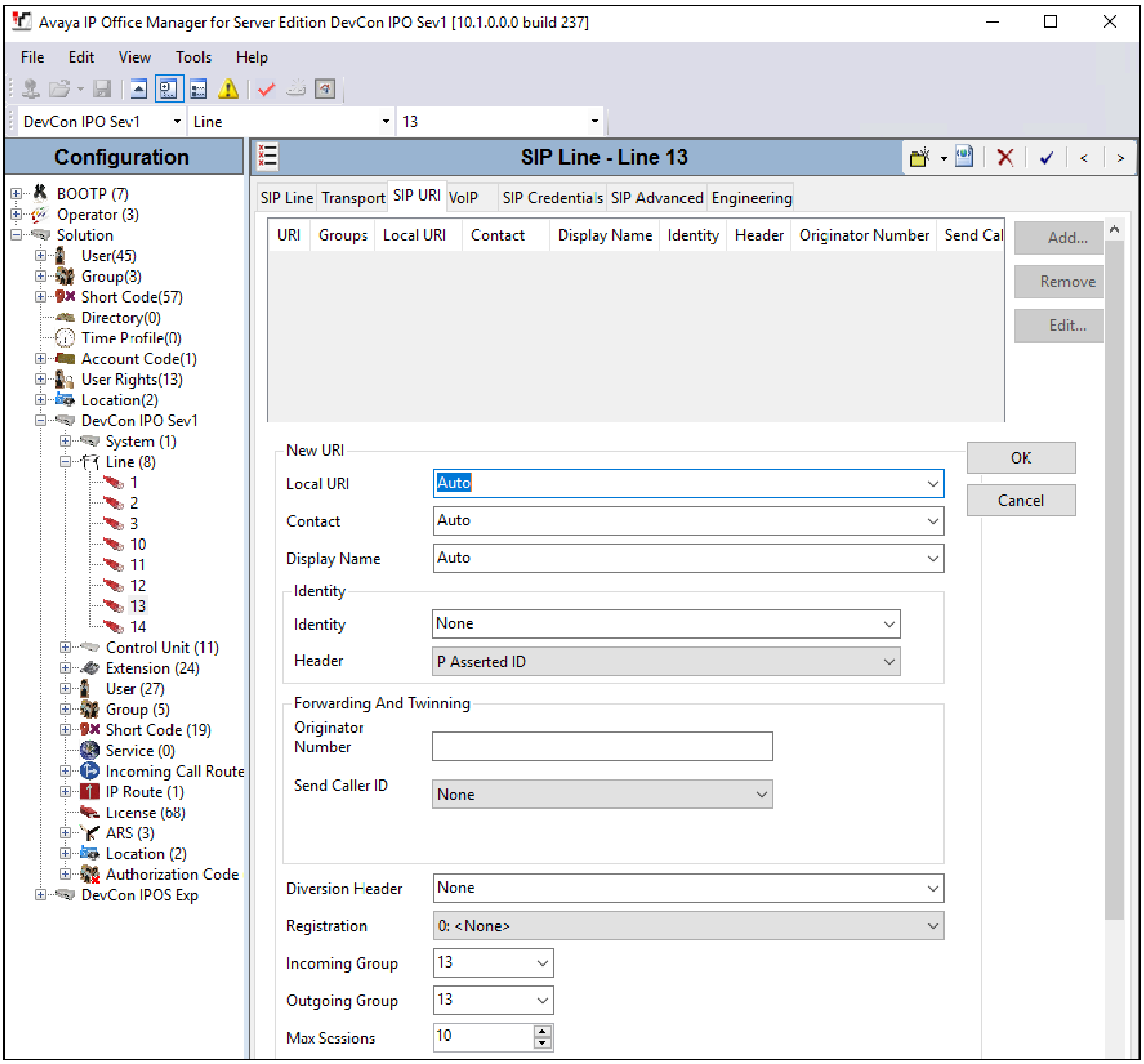
Retain default values for remaining fields. For compliance testing TLS protocol was tested.



In the **SIP URI** tab click on the **Add** button. In the subsequent window, enter the following:

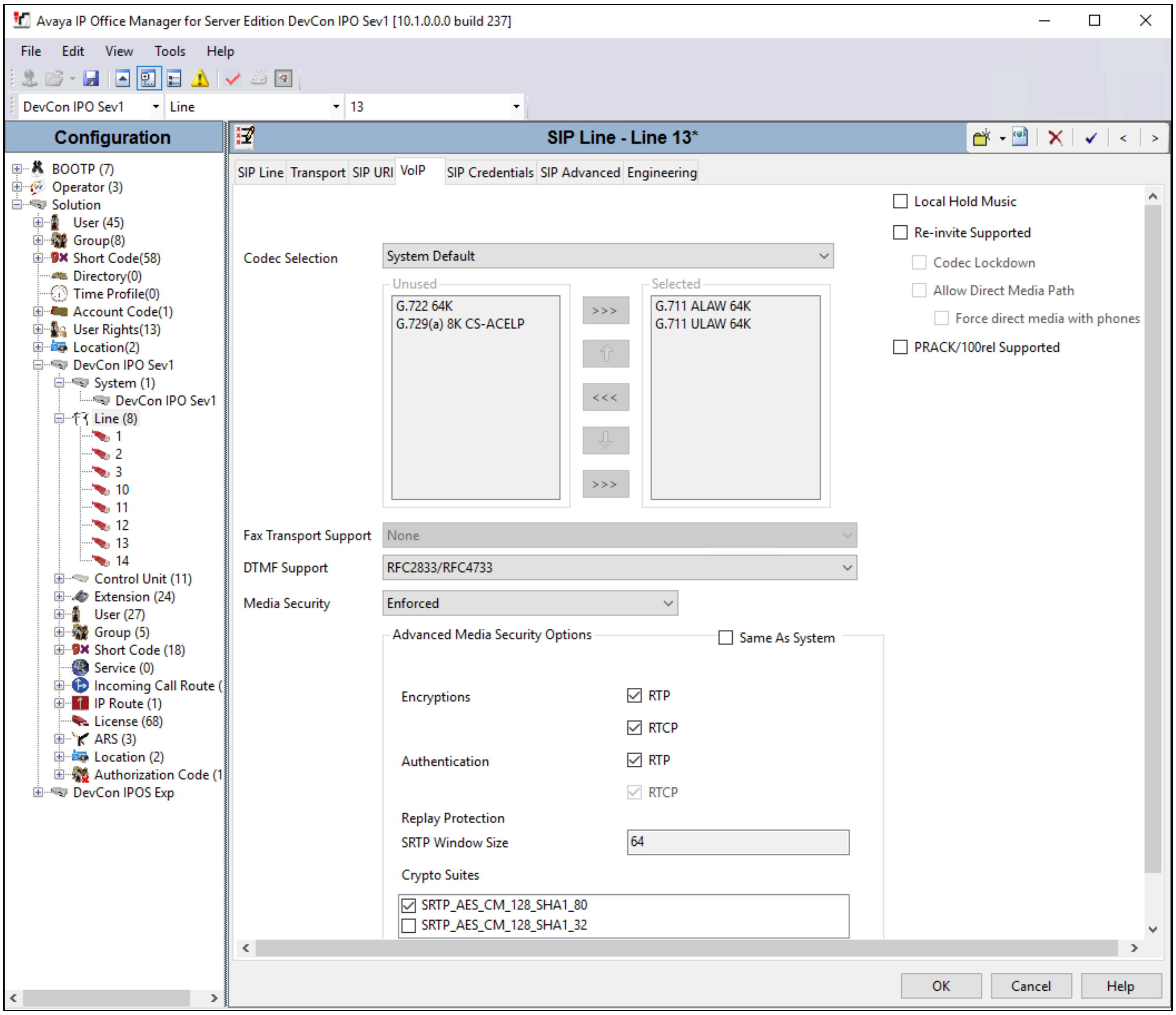
- **Local URI:** Select *Auto*.
- **Contact:** Select *Auto*.
- **Display Name:** Select *Auto*.
- **Incoming Group:** Select an available group number. During compliance testing *13* was selected.
- **Outgoing Group:** Select an available group number. During compliance testing *13* was selected.
- **Max Sessions:** During compliance testing *10* were configured.

Retain default values for all other remaining fields and click the **OK** button.

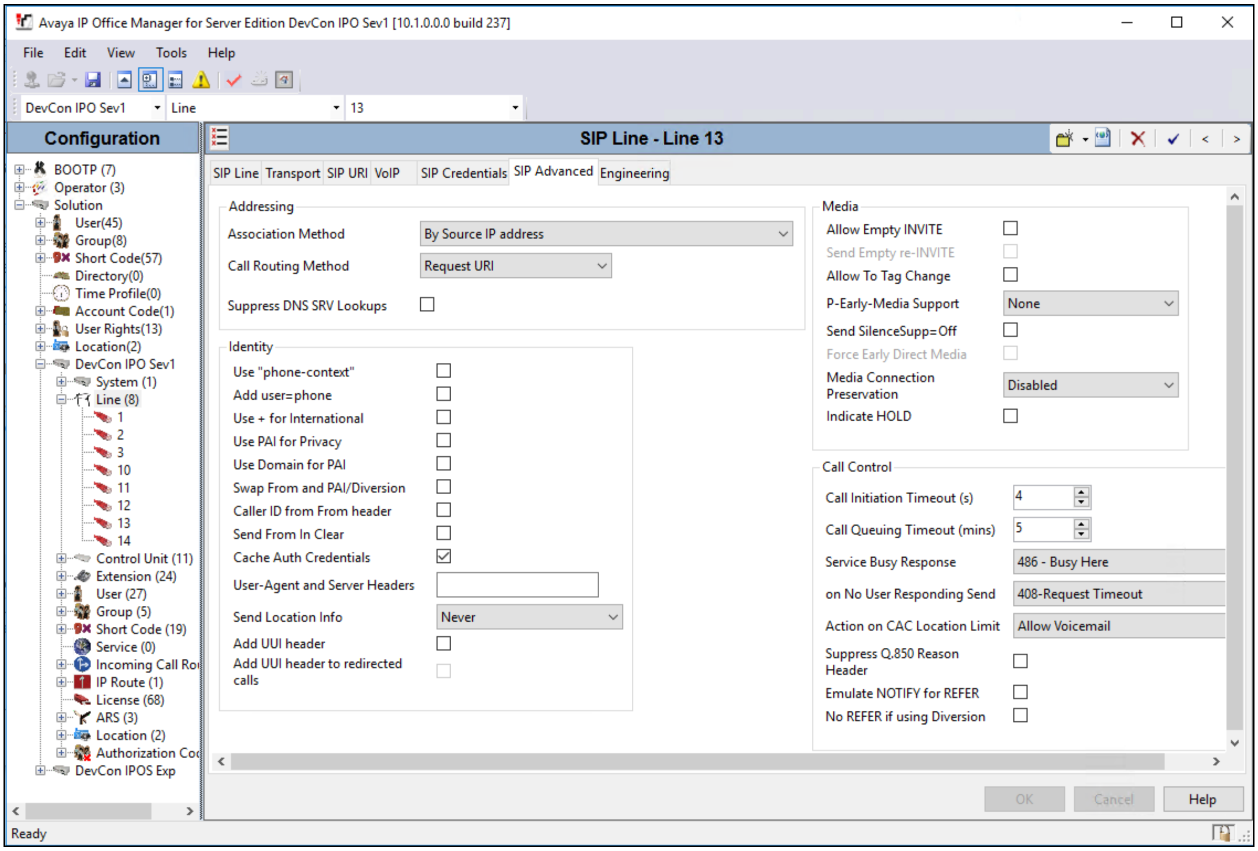


In the **VoIP** tab ensure that for **DTMF Support**, *RFC2833/RFC4733* is selected from the drop down menu. Select *Enforced* from the drop down menu for **Media Security**. Check all boxes for **Encryptions** and **Authentication** fields and under **Crypto Suites** check the box for *SRTP_AES_CM_128_SHA1_80*.

Retain default values for all remaining fields. During compliance testing only the **G.711 ULAW** codec was tested as shown in the screen below.

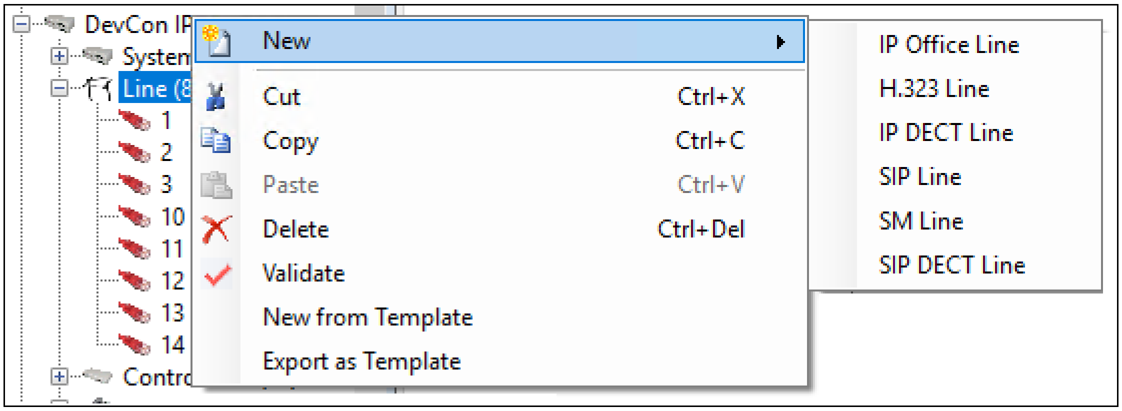


Default values were used for the remaining fields in the **SIP Credentials**, **SIP Advanced** and **Engineering** tabs. Screen below shows an example of the **SIP Advanced** tab with the default values. Click on the **OK** button to complete the configuration of the new SIP Line.



5.3.2. Configure Incoming SIP Line

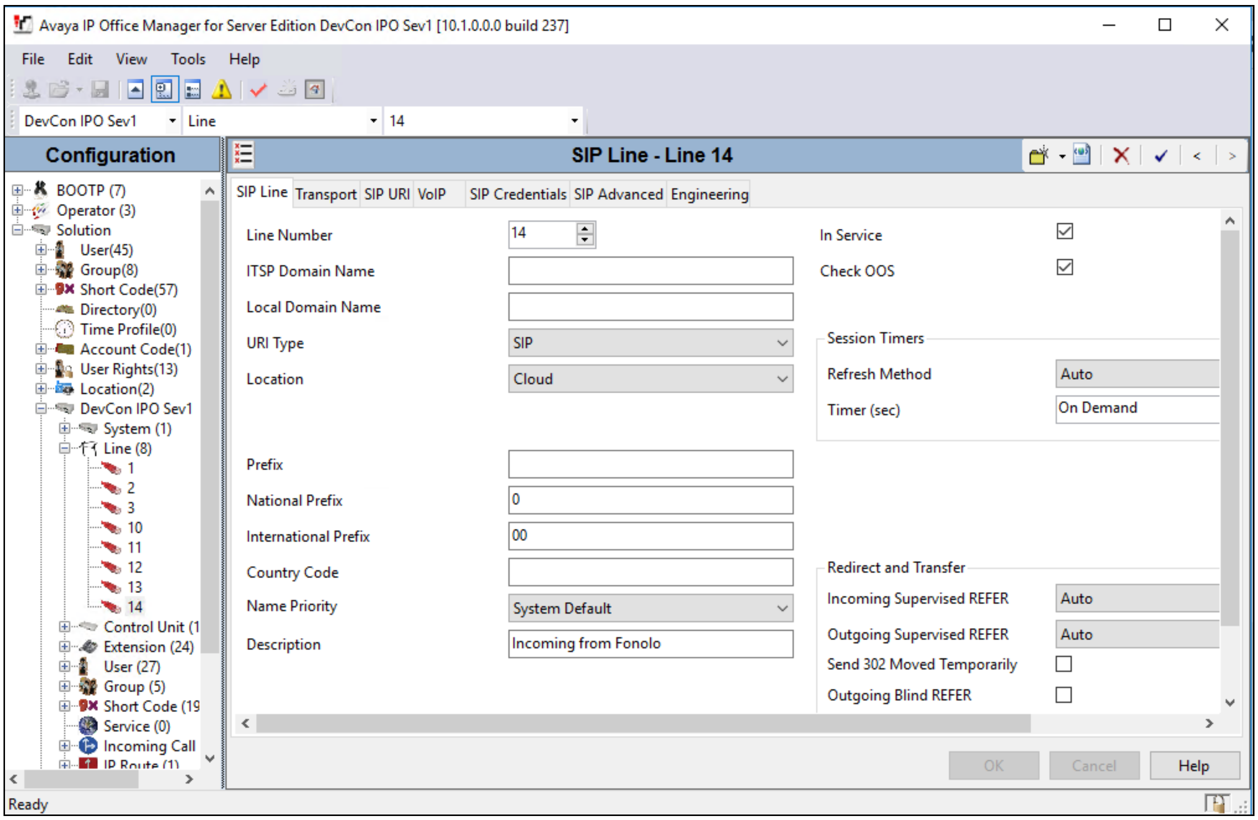
To create the SIP line from the IP Office for incoming calls from ICR, navigate to **System → Line** and right click on **Line** followed by **New →SIP Line** as shown in the screen below. In this example, line **14** was created to connect to ICR. In terms of ICR, this is an outbound that ICR makes to IP Office.



Screen below shows the configuration of the SIP Line in the subsequent **SIP Line** window; enter the following in the **SIP Line** tab.

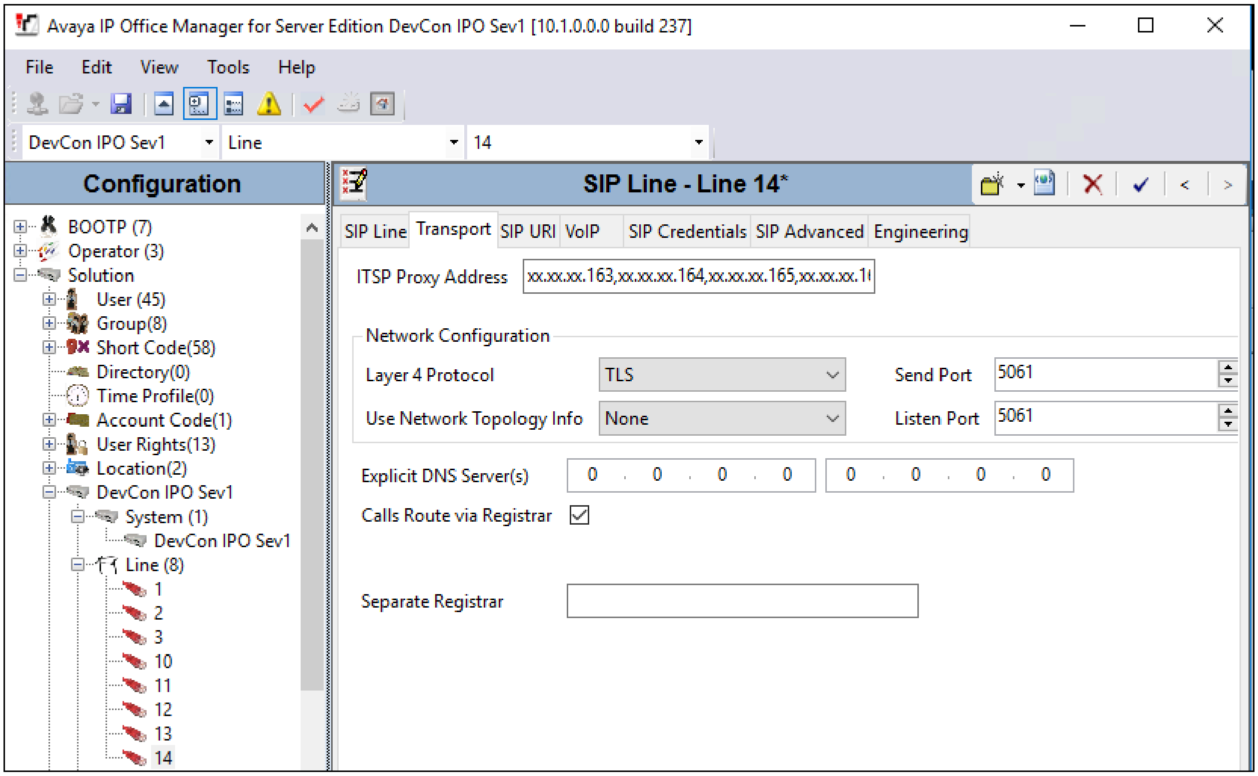
- **Line Number:** Line number *14* was configured.
- **ITSP Domain Name:** Configure domain name of ICR or leave this field blank.
- **Description:** Provide a description for the SIP Line. This field is optional.

Retain default values for all remaining fields.



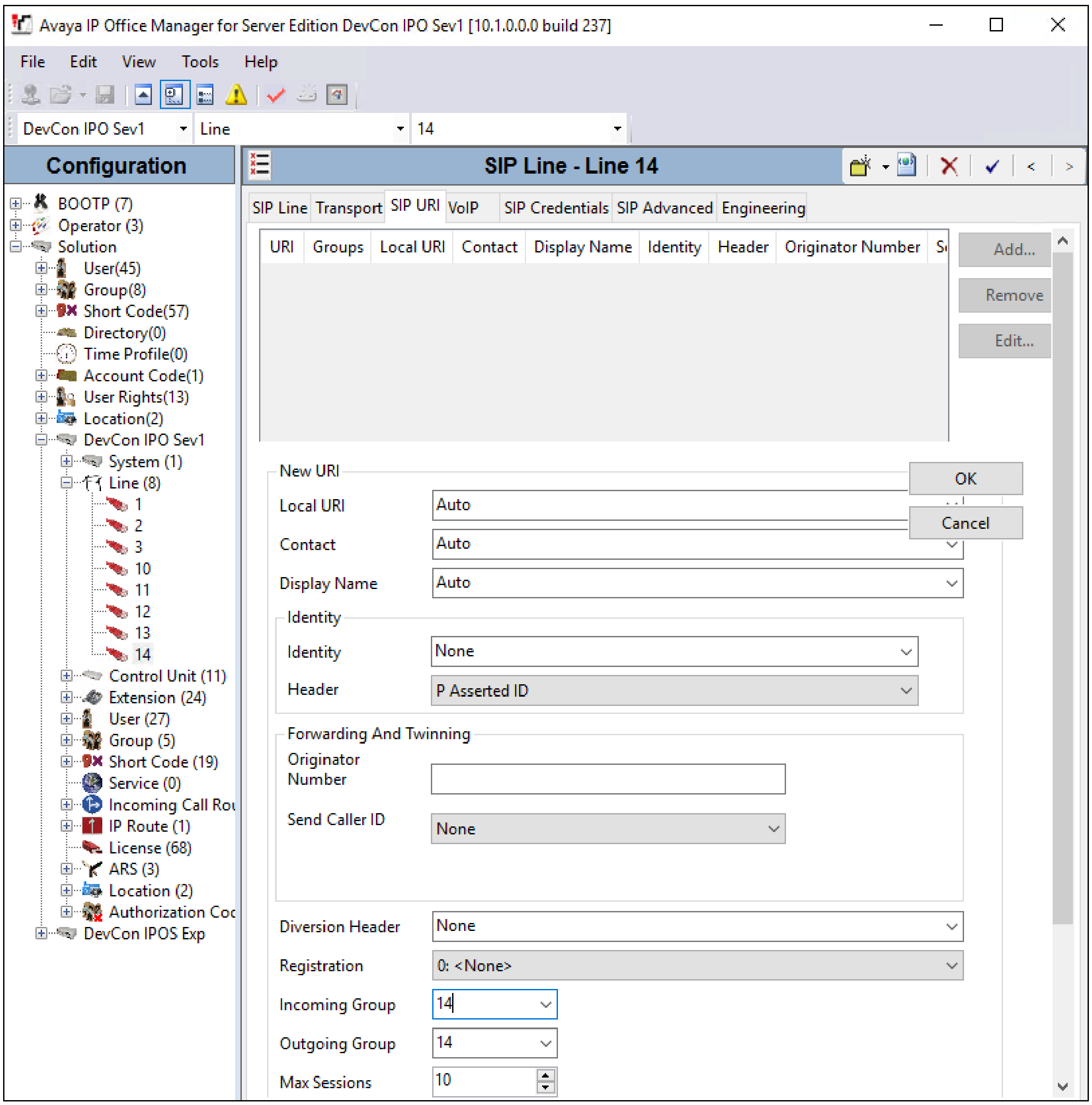
In the **Transport** tab enter IP address of ICR in the **ITSP Proxy Address** field. During compliance testing *xx.xx.xx.163,xx.xx.xx.164,xx.xx.xx.165,xx.xx.xx.166* was configured. ICR requested the use of four servers for incoming calls. In this field, a list of up to four IP addresses, with each address separated by a comma or space can be configured as per IP Office design. Under **Network Configuration**, in the **Layer 4 Protocol** field, select *TLS* from the drop down menu.

Retain default values for remaining fields. For compliance testing TLS protocol was tested.



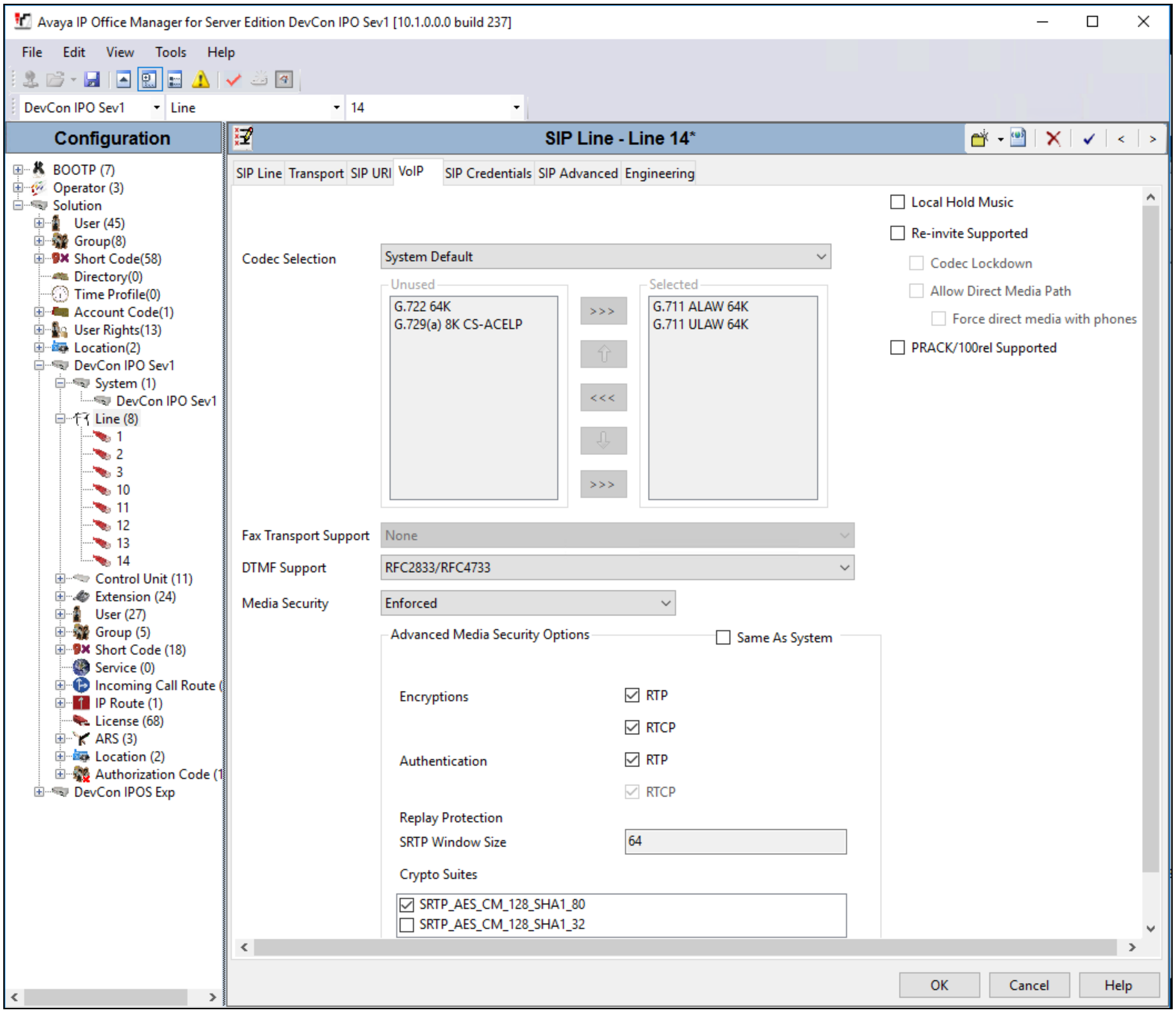
In the **SIP URI** tab click on the **Add** button. In the subsequent window, enter the following and retain default values for all other remaining fields and click the **OK** button.

- **Local URI:** Select *Auto*.
- **Contact:** Select *Auto*.
- **Display Name:** Select *Auto*.
- **Incoming Group:** Select an available group number. During compliance testing *14* was selected.
- **Outgoing Group:** Select an available group number. During compliance testing *14* was selected.
- **Maximum Sessions:** During compliance testing *10* were configured.

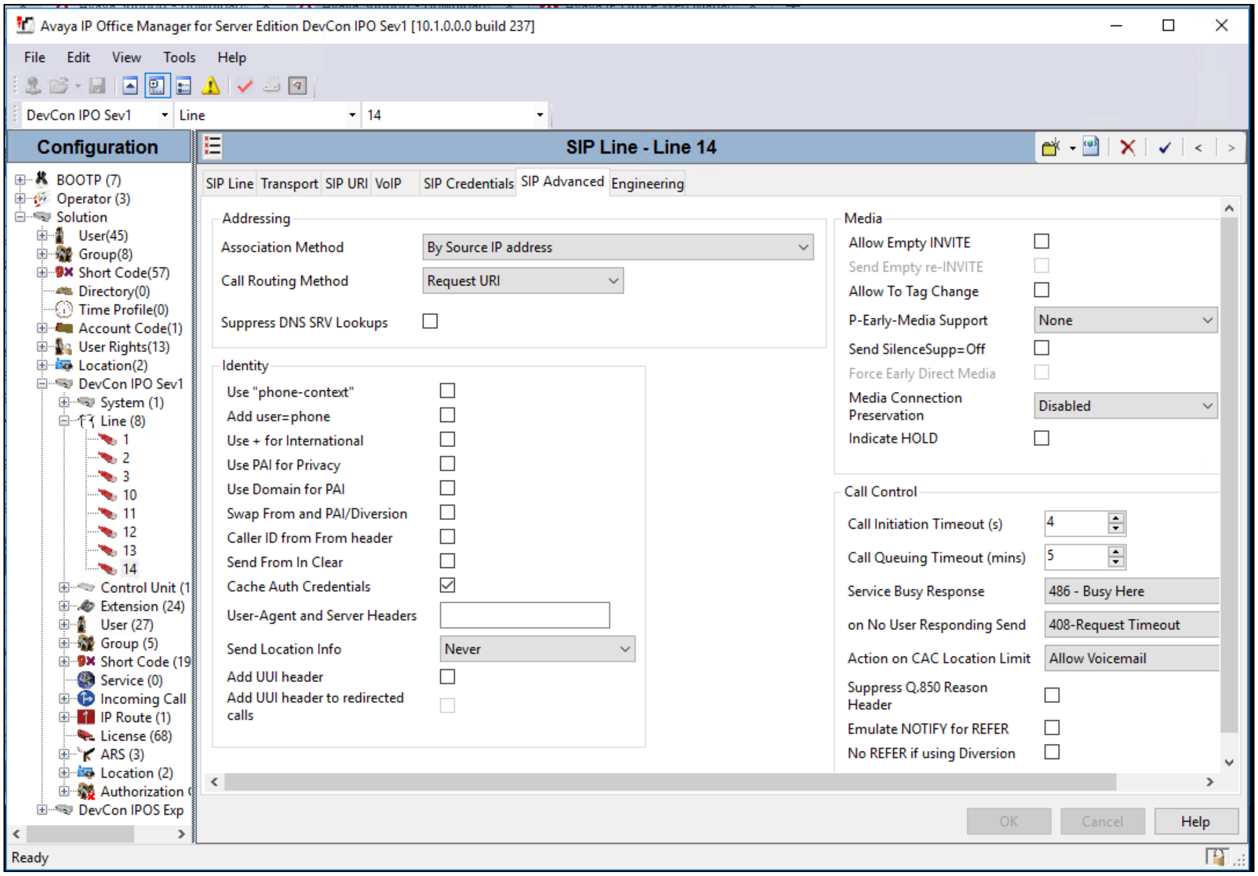


In the **VoIP** tab ensure that for **DTMF Support**, *RFC2833/RFC4733* is selected from the drop down menu. Select *Enforced* from the drop down menu for **Media Security**. Check all boxes for **Encryptions** and **Authentication** fields and under **Crypto Suites** check the box for *SRTP_AES_CM_128_SHA1_80*.

Retain default values for all remaining fields. During compliance testing only the **G.711 ULAW** codec was tested as shown in the screen below.



Default values were used for the remaining fields in the **SIP Credentials**, **SIP Advanced** and **Engineering** tabs. Screen below shows an example of the **SIP Advanced** tab with the default values. Click on the **OK** button to complete the configuration of the new SIP Line.

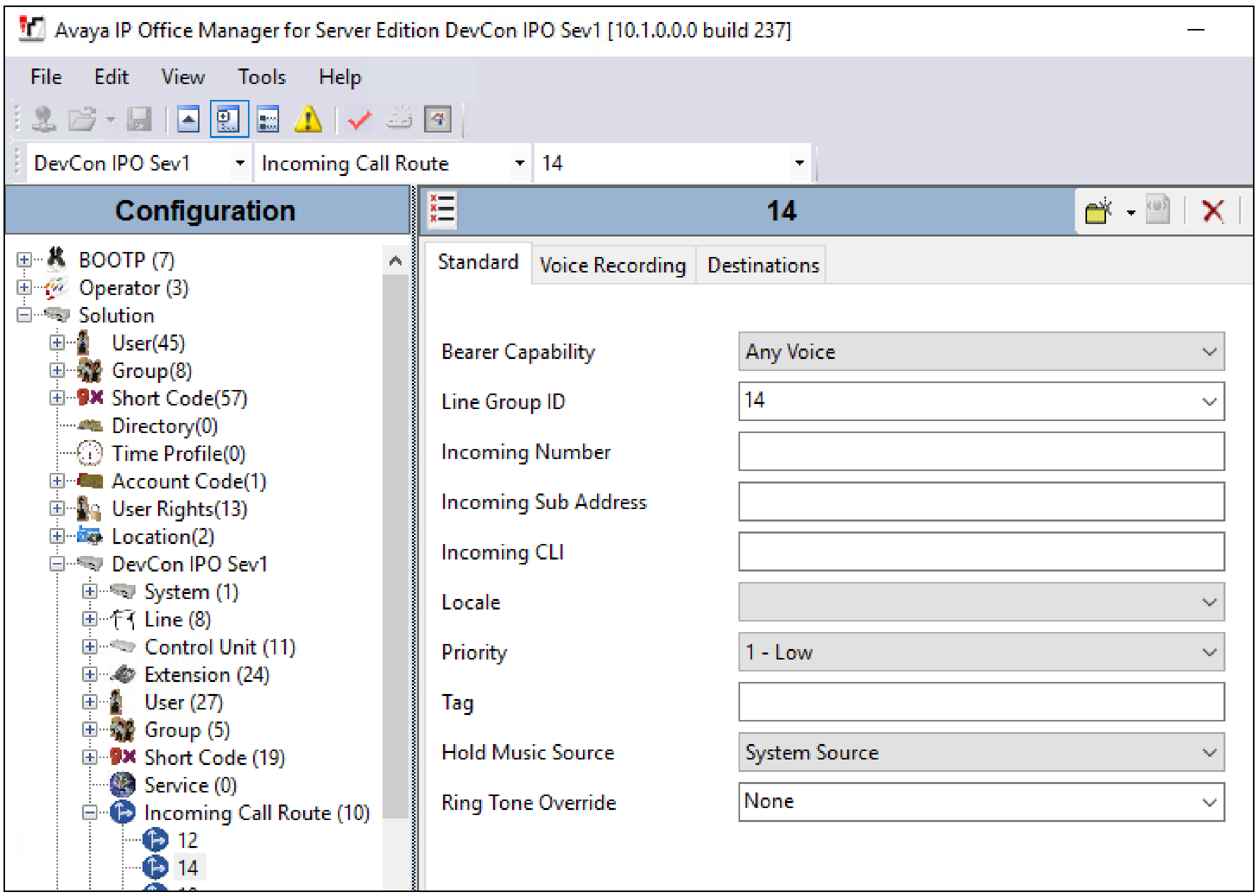


5.4. Configure Incoming Call Route

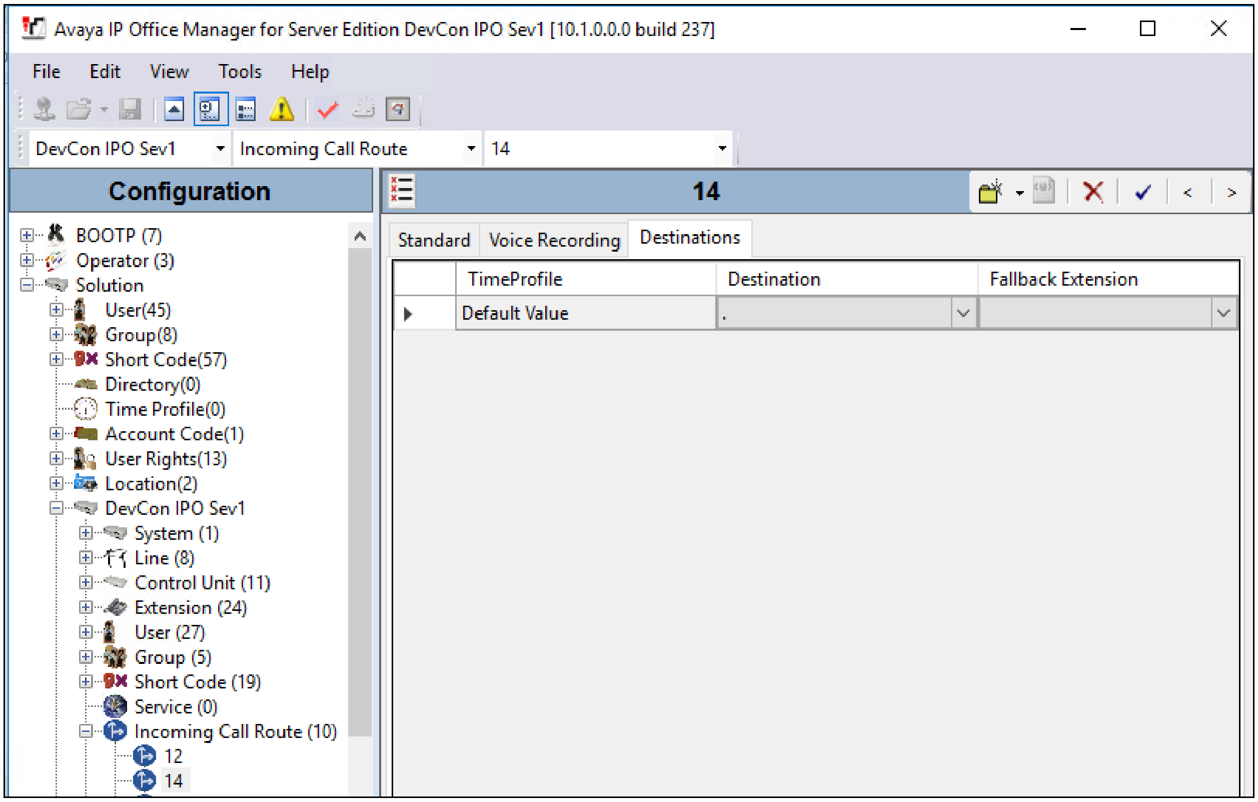
To configure an incoming call route for routing of incoming calls from ICR, navigate to **DevCon IPO Sev1 → Incoming Call Route** and right click on **Incoming Call Route** followed by **New** (not shown). In the subsequent window, enter the following in the **Standard** tab. This route is used by ICR to make an outbound call to IP Office.

- **Bearer Capability:** Select *Any Voice* from the drop down menu.
- **Line Group ID:** Select *14*, the incoming SIP Line as configured in **Section 5.3.2**.

Retain default values for all remaining values.

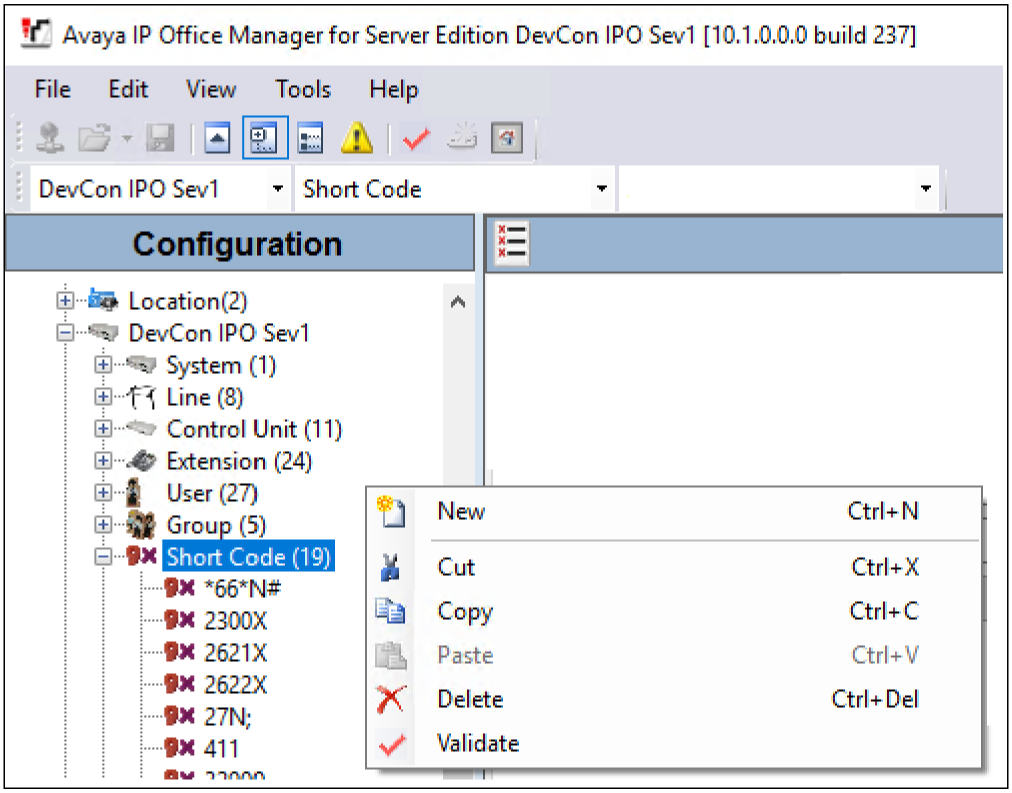


In the **Destinations** tab, under the **Destination** column enter ".". Retain default values for all remaining fields and click the **OK** (not shown) button.



5.5. Create Short Code (Route Calls)

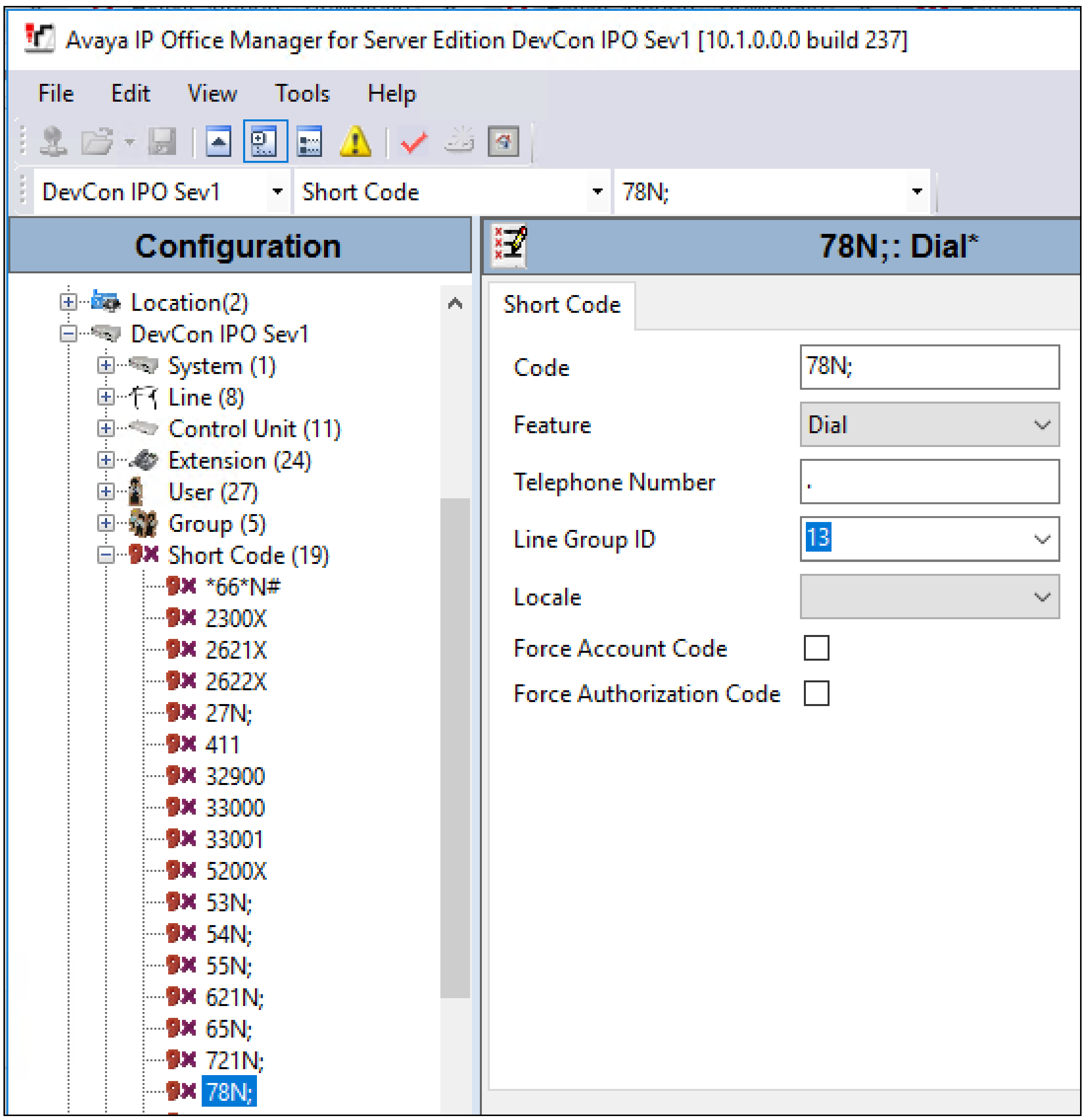
A Short Code needs to be configured on the IP Office to route calls to ICR. Navigate to **DevCon IPO Sev1 → Short Codes**, and then right click and select **New** as shown in the screen below.



In the subsequent window, enter the following:

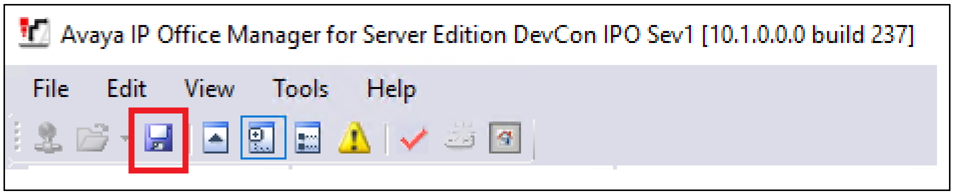
- **Code:** Enter the number range that will be routed to ICR (during compliance testing, all 78xxx numbers were sent to ICR, therefore *78N;* was entered).
- **Feature:** Select *Dial* from the drop down menu.
- **Telephone Number:** Enter ".".
- **Group Line ID:** Enter *13*, the outgoing SIP Line configured in **Section 5.3.1**.

Retain default values for all remaining fields and click the **OK** (not shown) button.



5.6. Save Configuration

Once all the configurations are complete, the changes need to be saved on the IP Office system. Click the Save icon as shown in the screen below to save the changes. A subsequent window will appear (not shown) asking the user to proceed with the changes made to the IP Office system/s or not. Click on the **OK** button to confirm.

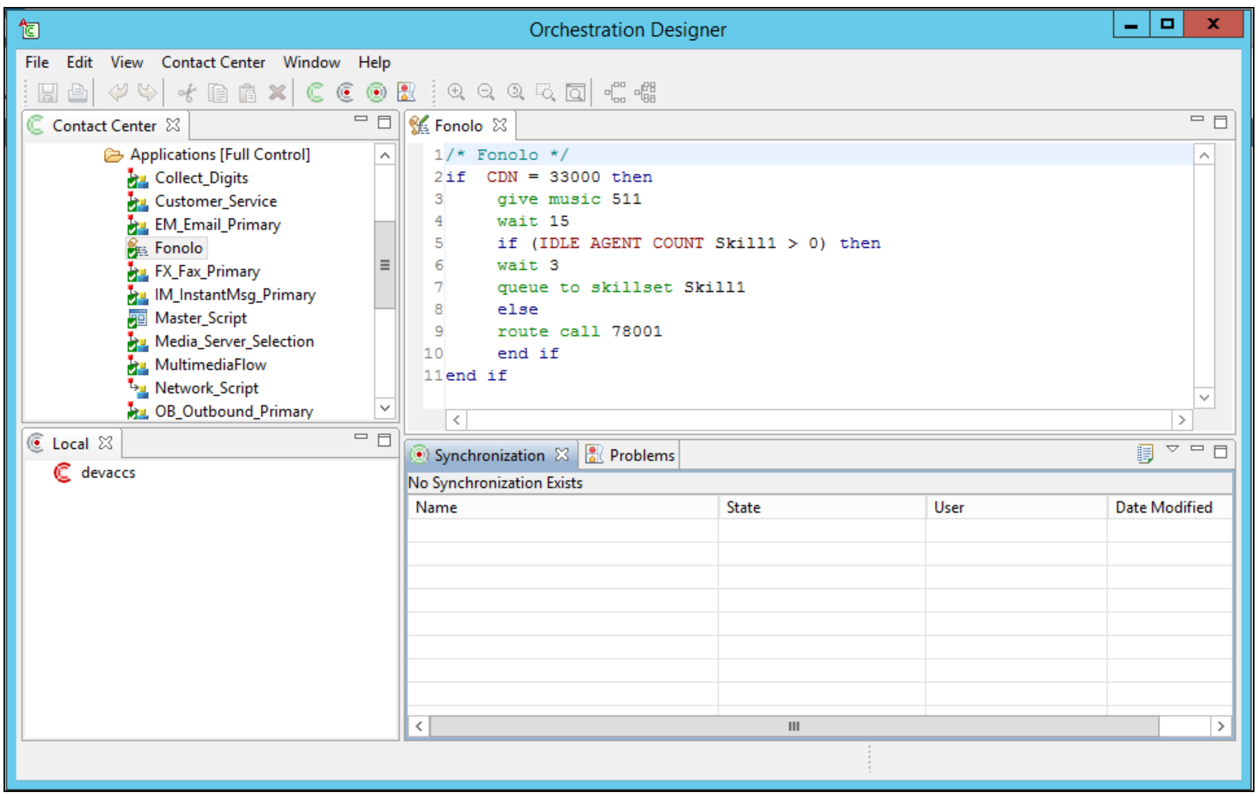


6. Configure Avaya Contact Center Select

The administration of the routing and basic connectivity between IP Office and Contact Center Select or the setting up of Skillset, CDN, Scripts, Agents for a contact center type environment are not the focus of these Application Notes; however, some details are provided only for informational purposes and completeness.

This section provides a sample script that was used during the compliance testing. When a call is directed to this script, caller is connected to ICR if there are no agents available in the Skillset.

From Contact Center Select Launchpad, navigate to **Scripting → Orchestration Designer → Launch Orchestration Designer** (not shown) to open the **Orchestration Designer** window as shown below. A basic script is configured in the example below. When a call reaches the CDN **33000** that was configured during compliance testing and if agents are not available, then the call is routed to **78001** which is the short code that was configured in **Section 5.5** to reach ICR.



7. Configure Fonolo In-Call Rescue

This section provides a “snapshot” of ICR configuration used during compliance testing. ICR is typically configured for customers by Fonolo. The screen shots and partial configuration shown below, supplied by Fonolo, are provided only for reference. These represent only an example of the configuration GUI of ICR, available through the Fonolo Customer Portal at https://portal.fonolo.com/. Other configurations are possible. Contact Fonolo for details on how to configure ICR. The configuration operations described in this section can be summarized as follows:

- Add a New SIP Trunk Group
- Adding the Agent Call-Back Endpoint
- Adding a New Call-Back Profile

7.1. Add a New SIP Trunk Group

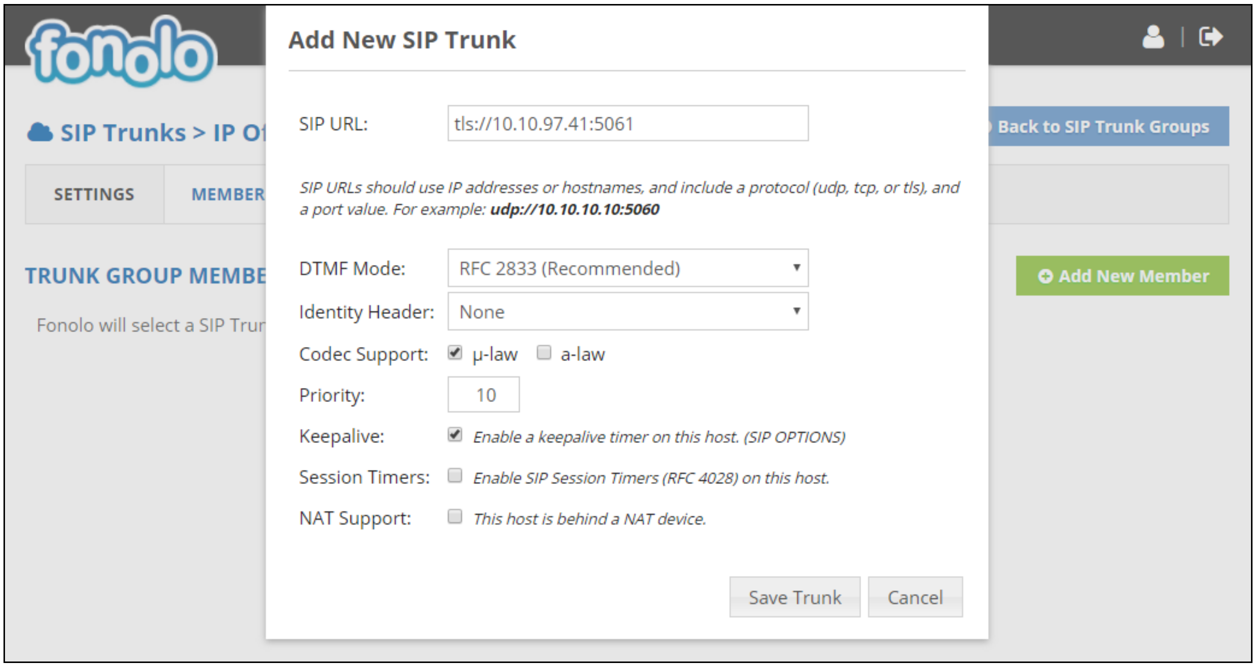
Navigate to **Telco → SIP Trunks** and click the **Add New SIP Trunk Group** button (not shown) at the top of the page. Define a new label to identify this SIP trunk group. During compliance testing **IP Office 10.1** was used as the label. Then select **Save Changes** (not shown).

Under the **Members** tab in this new SIP trunk group, click the **Add New Member** button (not shown), and the **Add New SIP Trunk** dialog will appear as shown below.

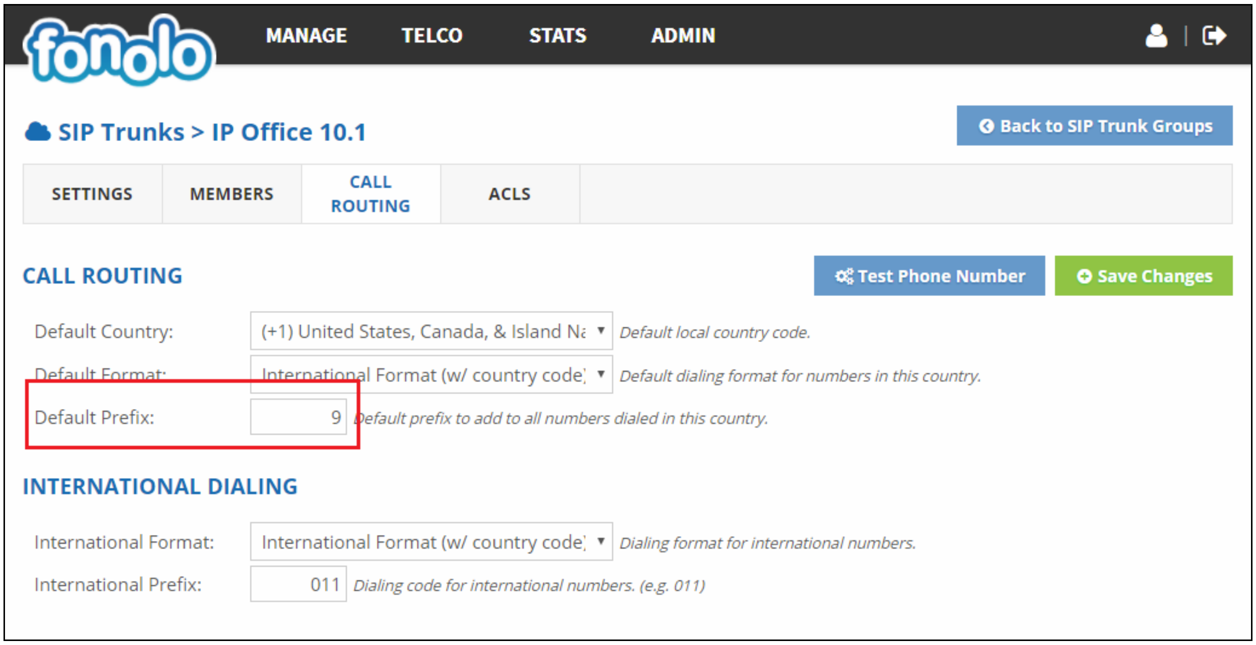
Under **Add New SIP Trunk**:

- **SIP URL**: The IP address of the IP Office formatted as a fully qualified URL, defining the protocol and SIP port.
- **DTMF Mode**: The mode to use for sending DTMF tones. Default is RFC 2833.
- **Identity Header**: Whether to include an identity header (either Remote-Party-ID or P-Asserted-Identity). Default is none.
- **Codec Support**: The list of audio codecs to use. Default is μ-law.
- **Priority**: A numeric value that can be used to determine failover or load balance groups when more than one SIP trunk group member is defined. Members with lower priority values are used first; members with a equal priority values are load balanced
- **Keepalive**: This instructs the Fonolo platform to perform regular keep-alive using SIP OPTIONS requests, based on the number of seconds defined. Default is disabled.
- **Session Timers**: If Fonolo should enable SIP Session Timers (RFC 4028). Default is disabled.
- **NAT Support**: If the SIP trunk group member specified is located behind a NAT (Network Address Translation) device. Fonolo can compensate for the un-reachable RTP data specified in the SDP body of the INVITE request, using symmetric RTP.

Add the IP address of IP Office, formatted as a fully qualified URL, defining the protocol and SIP port, then click the **Save Trunk** button. During compliance testing, the protocol **TLS** and port **5061** is used for the SIP service with IP Office, and the default values for the remaining SIP trunk group member settings.



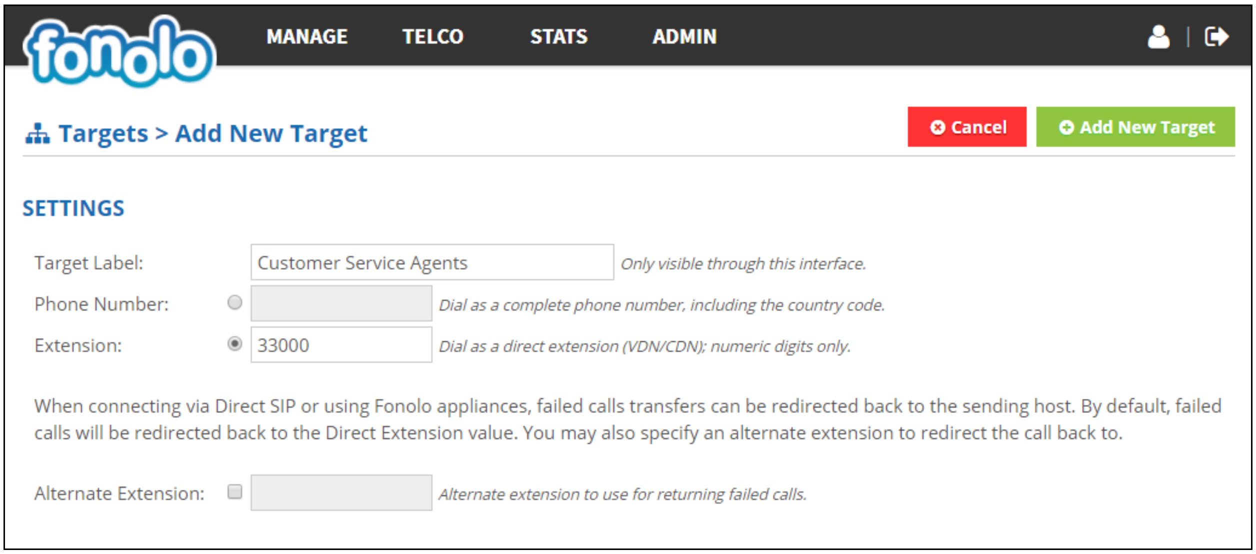
During compliance testing, the short code to dial outbound (to PSTN) from IP Office was "9N". Therefore, all outbound calls to customer call-back phone numbers via the IP Office needed to be prefixed with a "**9**". Under the **CALL ROUTING** tab in this new SIP trunk group, enter the digit "**9**" in the **Default Prefix** input field (shown below), and then click **Save Changes**.



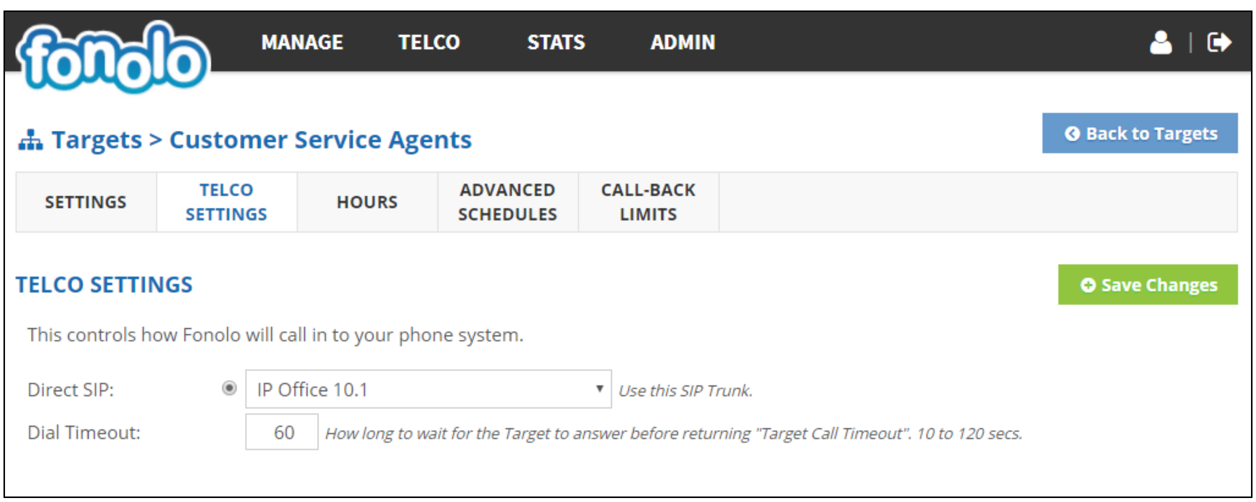
7.2. Adding the Agent Call-Back Endpoint

Navigate to **Manage → Targets** and click the **Add New Target** button (not shown). Define a new label to identify this new Target. During compliance testing **Customer Service Agents** was used as the label. Select the **Extension** option (shown below), and enter the CDN to reach the pertinent skillset via IP Office.

During compliance testing, CDN 33000 was pre-configured on Contact Center Select which was accessible via IP Office. Then click on the **Add New Target** button to save this Target.



From the **TELCO SETTINGS** section of the newly added Target, select the SIP trunk to use for this Target, from the **Direct SIP** drop down menu shown below. Select the **IP Office 10.1** SIP trunk, added in **Section 7.1**, and then click the **Save Changes** button.

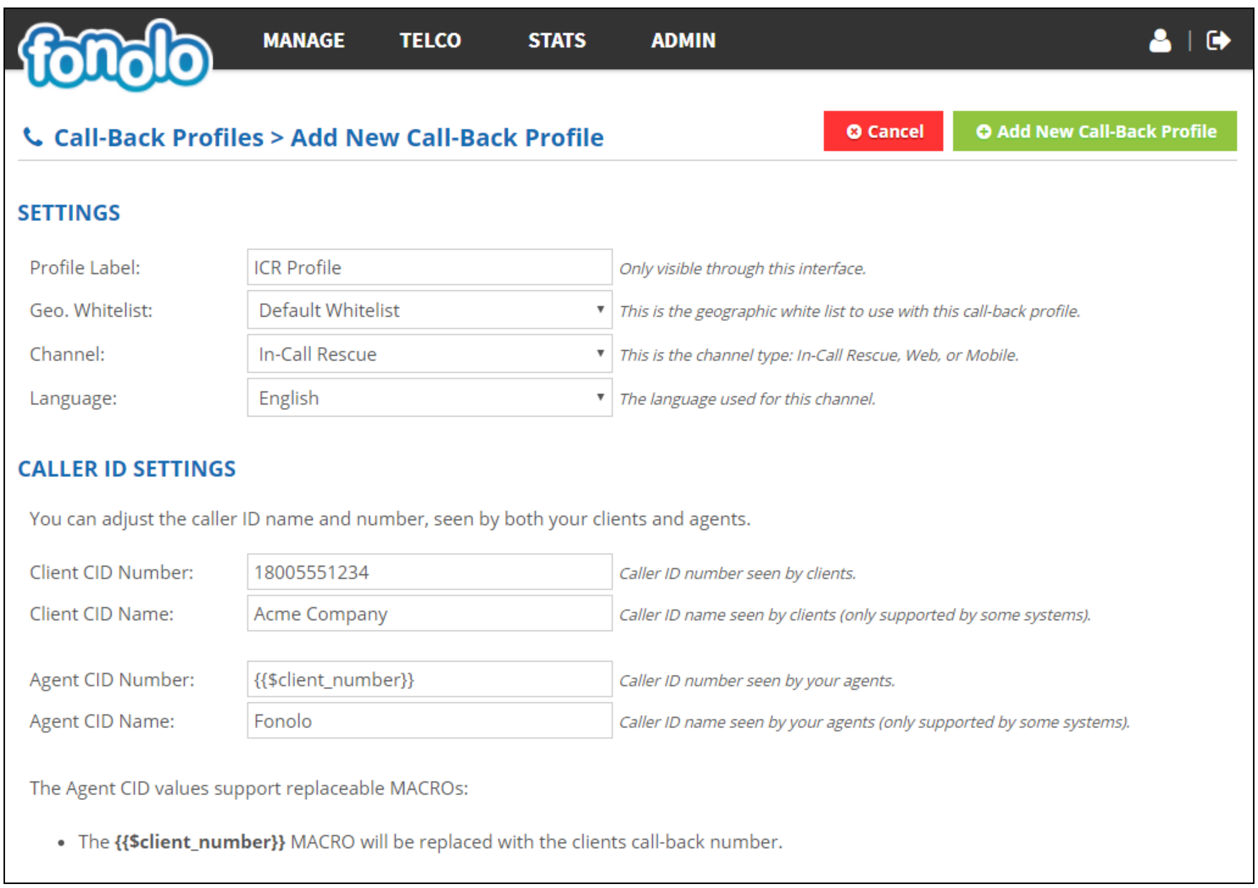


7.3. Adding a New Call-Back Profile

Navigate to **Manage → Call-Back Profiles** and click on the **Add New Profile** button, and configure the new profile:

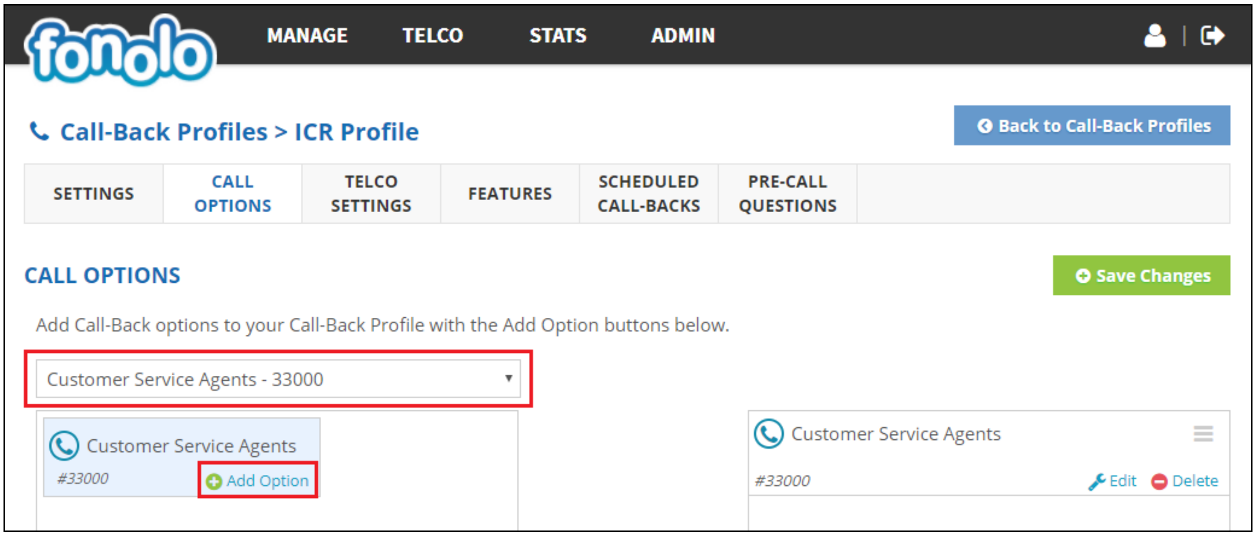
- **Profile Label:** A label to identify this new profile.
- **Geo Whitelist:** A geographic whitelist to use for this new profile.
- **Channel:** Select **In-Call Rescue**.
- **Language:** Select the appropriate language for this skill set queue.
- **Customer CID Number:** The Caller-ID number the customer will see.
- **Customer CID Name:** The Caller-ID name the customer will see.
- **Agent CID Number:** The Caller-ID number the agent will see.
- **Agent CID Name:** The Caller-ID name the agent will see.

Click the **Add New Call-Back Profile** button to add this new profile.

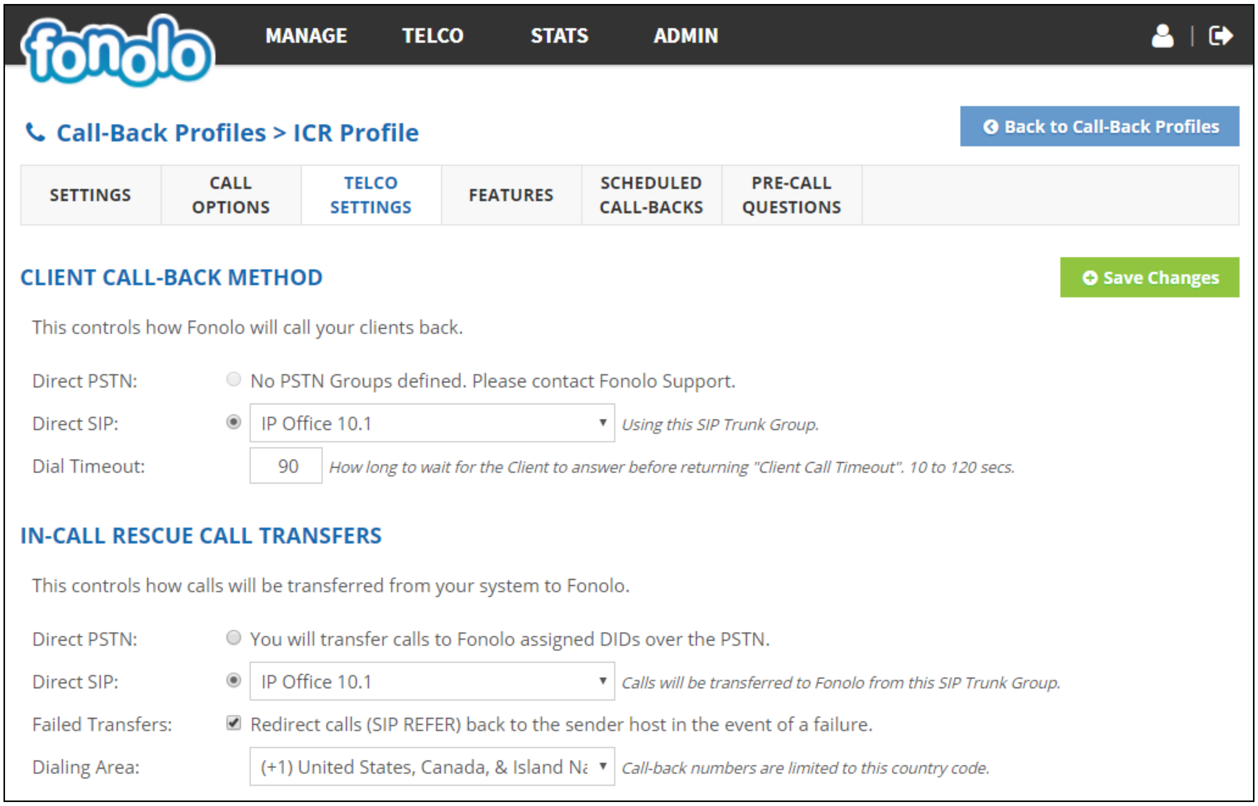


From the **CALL OPTIONS** section of the new **Call-Back Profile**, select the Target added in **Section 7.2** (from the drop-down menu highlighted below), and click the **Add Option** link to add the CDN value to the section on the right, as shown below, then click the **Save Changes** button.

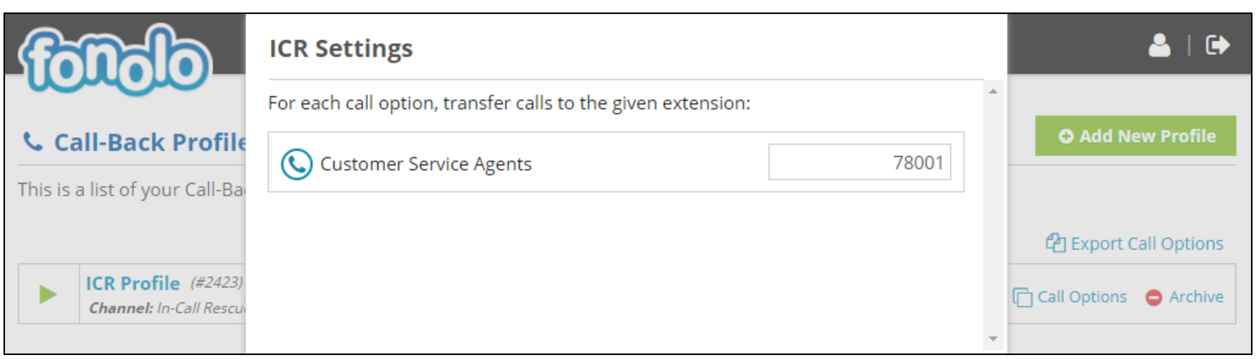
This associates the Target CDN with this new **Call-Back Profile**. Multiple call options can be associated with a single **Call-Back Profile**, one for each skill call-backs are being offered on.



From the **TELCO SETTINGS** section of the new **Call-Back Profile**, select the **IP Office 10.1** SIP trunk group created in **Section 7.1** as the **Direct SIP** value under both the **CLIENT CALL-BACK METHOD**, and the **IN-CALL RESCUE CALL TRANSFERS** section, as shown below, then click the **Save Changes** button.



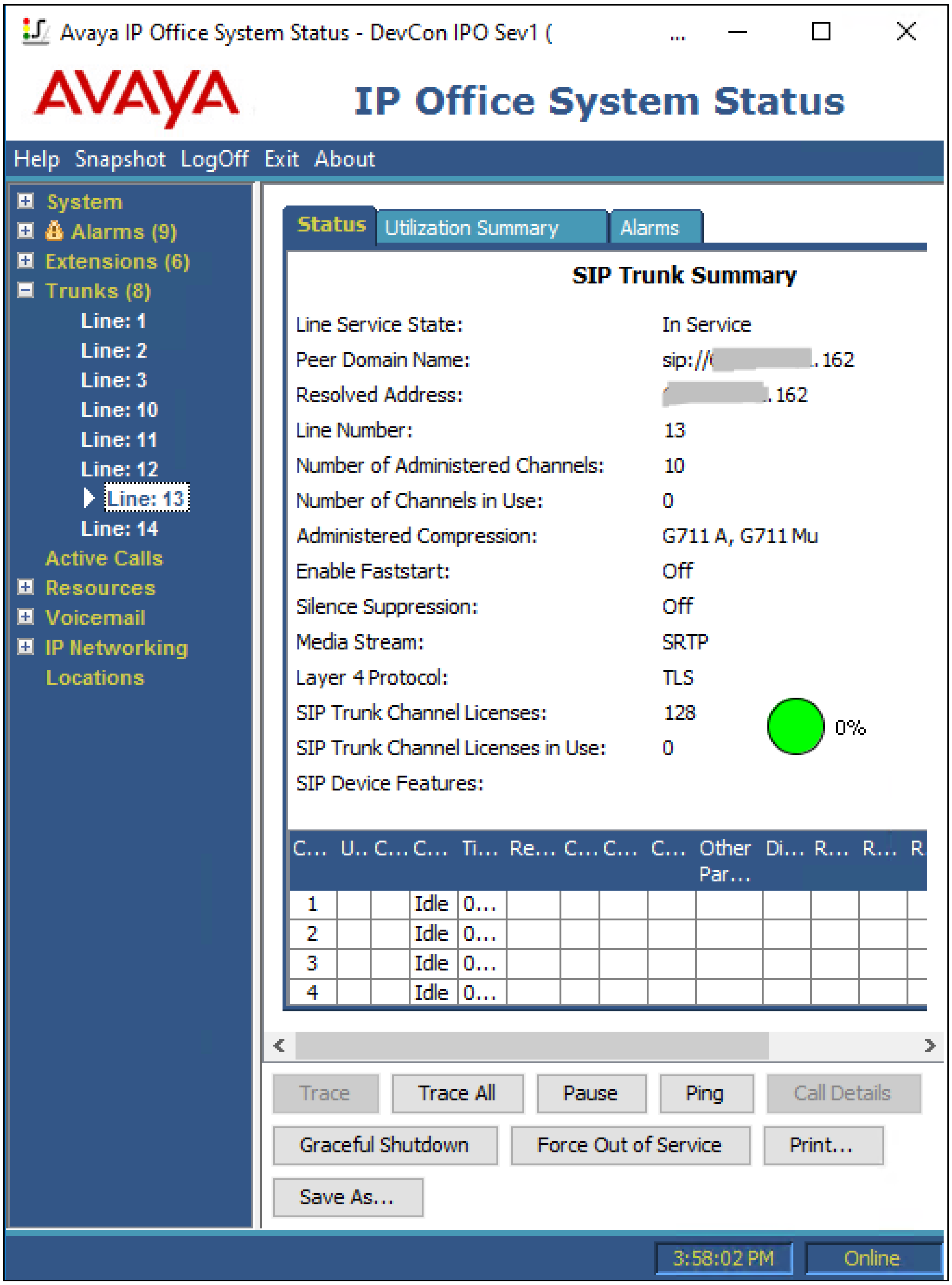
Navigate to **Manage → Call-Back Profiles** and click on the **In-Call Rescue** link on the newly created **Call-Back Profile** (not shown). The **ICR Settings** dialog will appear (shown below), and include the inbound extensions to use for each pertinent Contact Center Select CDN. These are the extensions to transfer calls to, on the ICR system, when a call opts-in for a call-back. During compliance testing, the extension *78001* is configured on the Fonolo system.

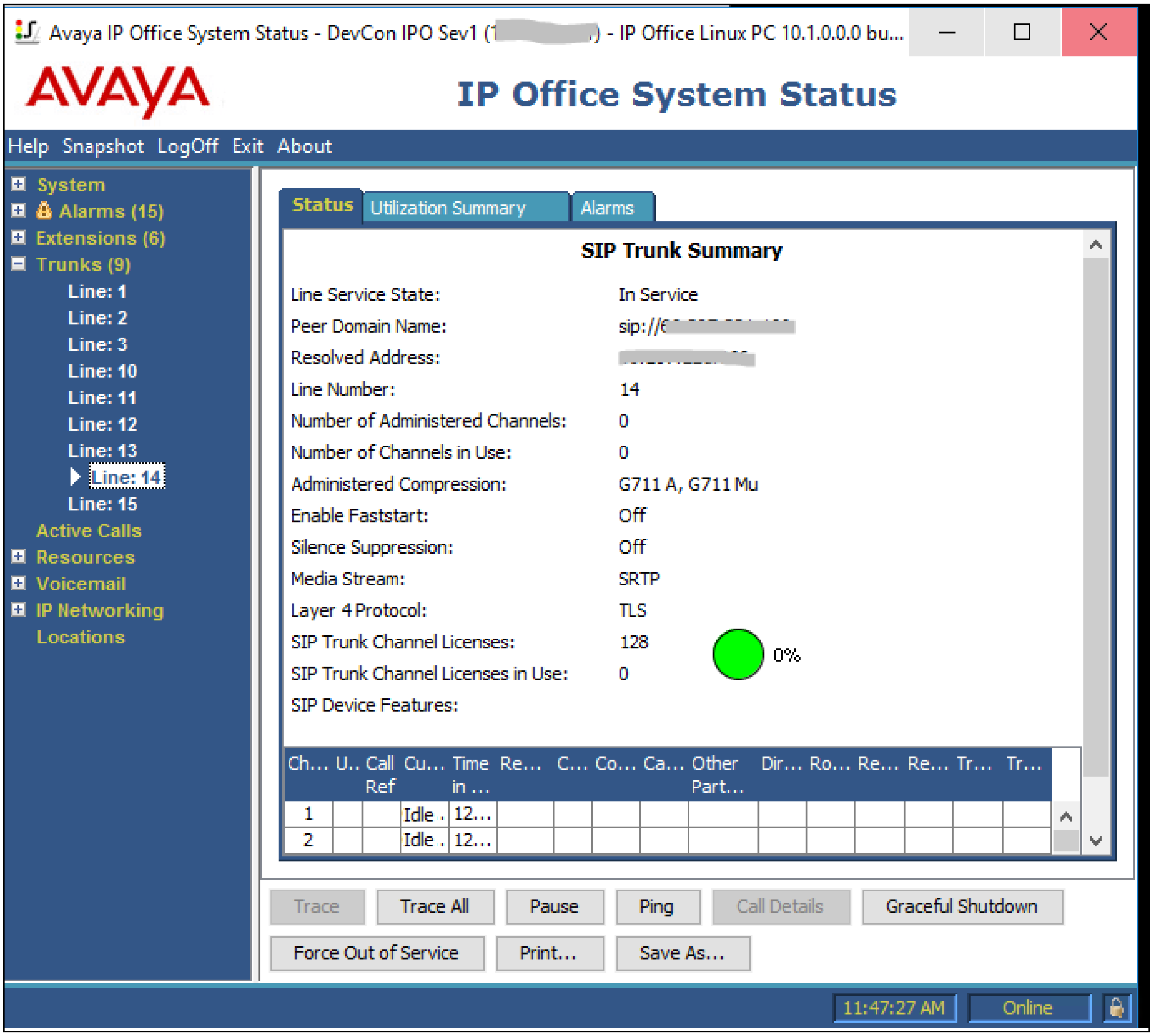


8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of IP Office, and ICR.

From the **Avaya IP Office System Status** window for the Primary server, verify that the **Trunks** configured are in service. Screen below shows the SIP Line trunks *13* and *14* have *In Service* under the **Line Service State** field.



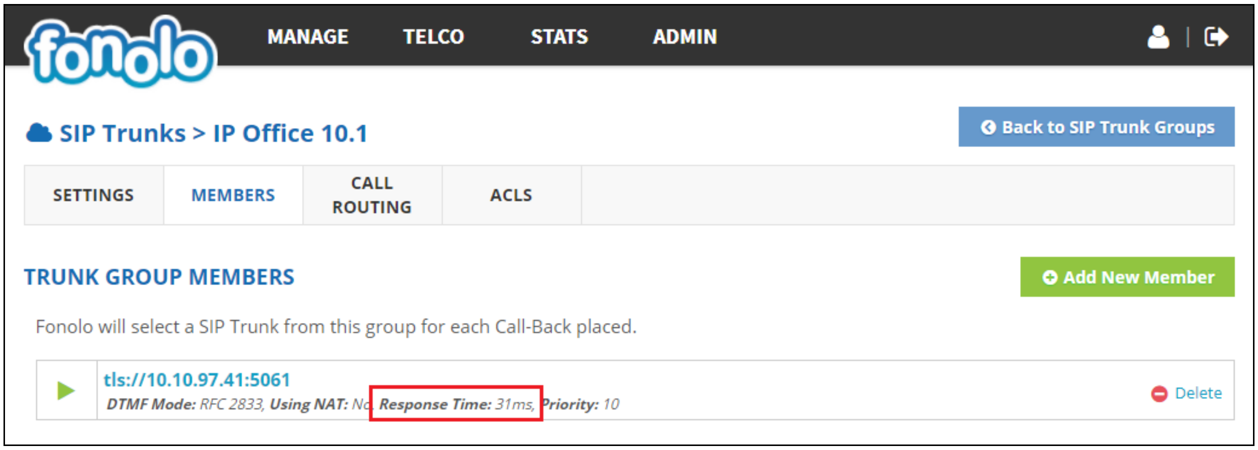


The following tests were also performed to verify proper configuration of ICR with IP Office.

- PSTN caller is able to select the call back option and get redirected to ICR via IP Office.
- PSTN caller is able to hear the ICR menu and make the required choices.
- ICR is able to recognize the choices made by the PSTN user.
- ICR is able to call the CDN and wait for an available agent.
- ICR is able to call out to the PSTN caller and connect them to an available agent.

8.1. Verify Fonolo In-Call Rescue

In the Fonolo customer portal, verify the link status of the SIP trunk group to IP Office, by navigating to **Telco → SIP Trunks**. Each SIP trunk group member will have a response time value, indicating the network latency (in milliseconds) between the Fonolo network, and IP Office. A positive **Response Time** value indicates a positive link status.



Additional information is available through the **Stats → Graphs** section of the Fonolo customer portal (not shown).

9. Conclusion

These Application Notes describe the configuration steps required for Fonolo In-Call Rescue to successfully interoperate with Avaya IP Office Server Edition. All feature and serviceability test cases were completed and passed with the exceptions/observations if any noted in **Section 2.2**.

10. Additional References

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

1. *Deploying IP Office ™ Platform Server Edition Solution,* Release 10.1, June 2017.
2. *Administering Avaya IP Office™ Platform with Manager,* Release 10.1, June 2017.
3. *Deploying Avaya IP Office™ Platform IP500 V2,* 15-601042 Issue 32f - (20 July 2017).

Fonolo provides their documentation upon delivery of their products/services.

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.