Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Komutel SIT2 SIP Console with Avaya IP Office Server Edition Release 11.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning the Komutel SIT2 SIP Console to interoperate with Avaya IP Office Server Edition Release 11.0.

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 steps required to integrate the Komutel SIT2 SIP Console (**S**olution for **I**ntegrated **T**elecommunications) with Avaya IP Office Server Edition. The SIT2 SIP Console provides a desktop communications center with enhanced control of call handling features. It provides the ability to handle a high volume of calls and offers tools designed to manage telephony functions. In the compliance test, the SIT2 SIP Console successfully registered with IP Office as a SIP endpoint, established calls with other telephones, and executed telephony features such as Hold, Transfer, and Conference.

In the compliance testing, Avaya IP Office Server Edition system consists of Avaya IP Office Primary Linux running on Virtualized Environment and a 500V2 Expansion.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between the SIT2 SIP Console and Avaya SIP, H.323, and digital stations and exercising common telephony features, such as hold, transfer, and conference.

The serviceability testing focused on verifying that the SIT2 SIP Console comes back into service after re-connecting the Ethernet connection or rebooting the PC on which the SIT2 SIP Console is running.

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 only (private network side). 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 the Komutel SIT2 did not include use of any specific encryption features as requested by Komutel.

2.1. Interoperability Compliance Testing

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

- Successful registration of the SIT2 SIP Console with IP Office.
- Calls between SIT2 IP Console and Avaya SIP, H.323, digital stations, and PSTN.
- G.711 codec support.
- Caller ID display on Avaya endpoints and SIT2 SIP Console.
- Proper recognition of DTMF tones.
- Basic telephony features including Hold, Mute, Transfer, and Conference.
- Proper system recovery after a restart of the SIT2 SIP Console and loss of IP connectivity.

2.2. Test Results

All test cases passed successfully with the following observation.

- Komutel SIT2 SIP Console supports codec G.711 only.
- Komutel SIT2 SIP Console does not support Call Forward, MWI and Call Park at the time of testing.

2.3. Support

For technical support on the SIT2 SIP Console, contact Komutel Support via phone, email, or website.

- **Phone:** (877) 225-9988
- **Email:** service@komutel.com
- **Web:** https://www.komutel.com/fr/a-propos-de-komutel/services/

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the test configuration used for the DevConnect compliance testing.

The Avaya components used to create the simulated enterprise customer site includes:

- IP Office Server Edition running in Virtualized environment.
  - Avaya IP Office Voicemail Pro.
- Avaya IP Office 500 V2 as expansion system.
- Avaya 96x1 Series IP Deskphones (H.323).
- Avaya 1100 Series IP Deskphones (SIP).
- Avaya J129 IP Deskphones (SIP).
- Avaya 1400 Series Digital Deskphones.
- Analog Deskphones.
- IP Office Primary has SIP trunk to PSTN

Komutel SIT2 SIP Console registers to IP Office Primary as SIP endpoint.

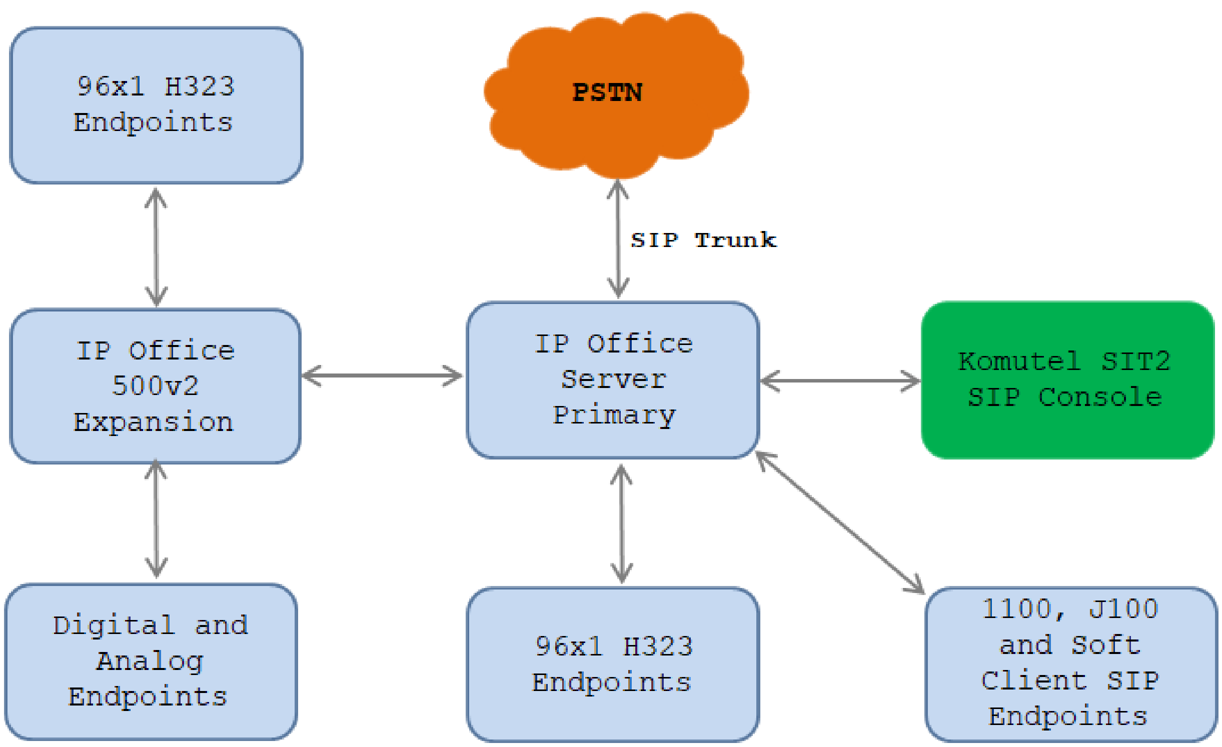


Figure 1: Avaya Interoperability Test Lab Configuration

4. Equipment and Software Validated

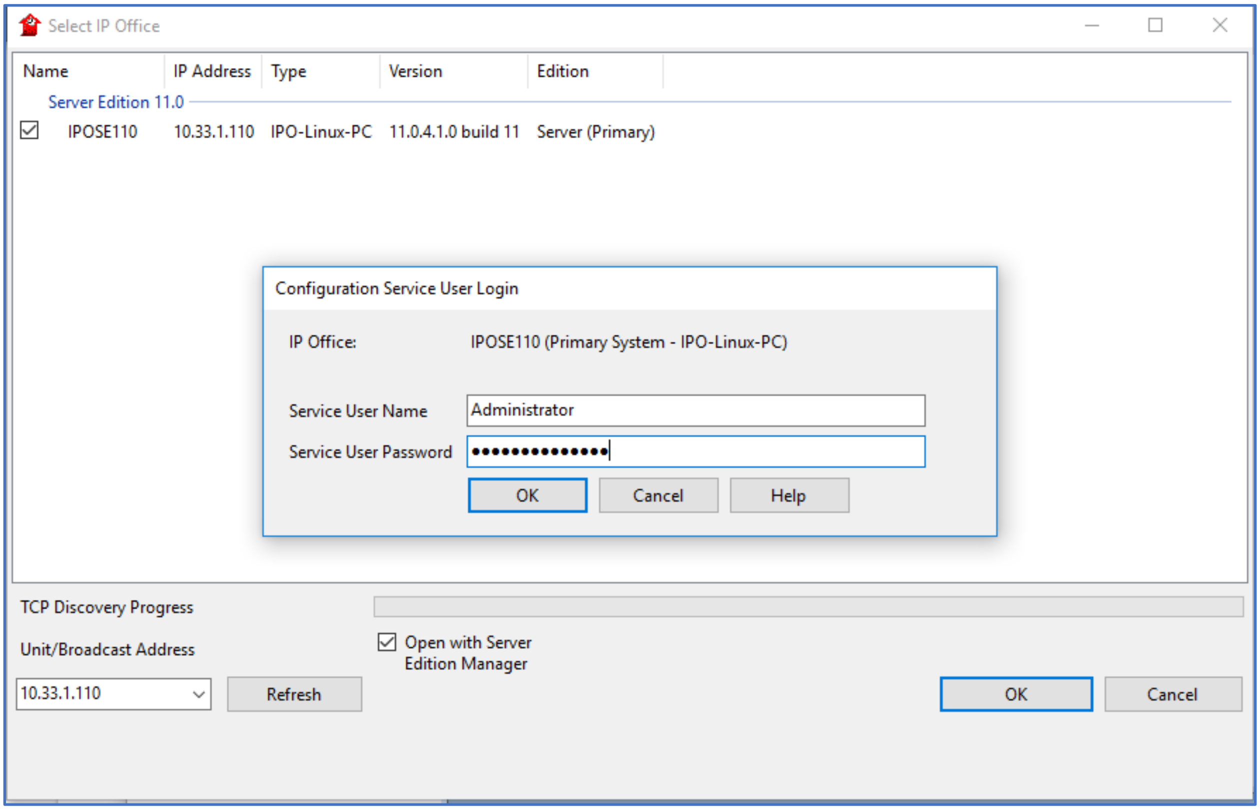
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition (Primary Server) • Avaya IP Office Voicemail Pro	11.0.4.1.0 Build 11 11.0.4.1.0 Build 2
Avaya IP Office IP500 V2 (Expansion Systems)	11.0.4.1.0 Build 11
Avaya IP Office Manager	11.0.4.1.0 Build 11
Avaya 96x1 Series IP Deskphones (H.323)	6.8002
Avaya 1140E IP Deskphones (SIP)	SIP1140e Ver. 04.04.23.00
Avaya J129 IP Deskphones (SIP)	4.0.0.0.21
Avaya 1408 Digital Telephone	48.02
Avaya Equinox™ for Windows (SIP)	3.6.0.153.36
Analog Telephone	---
Komutel	
Komutel SIT2 SIP Console	Version 2.5.8
Komutel SIP Telephone Plugin	2.1.0.48402

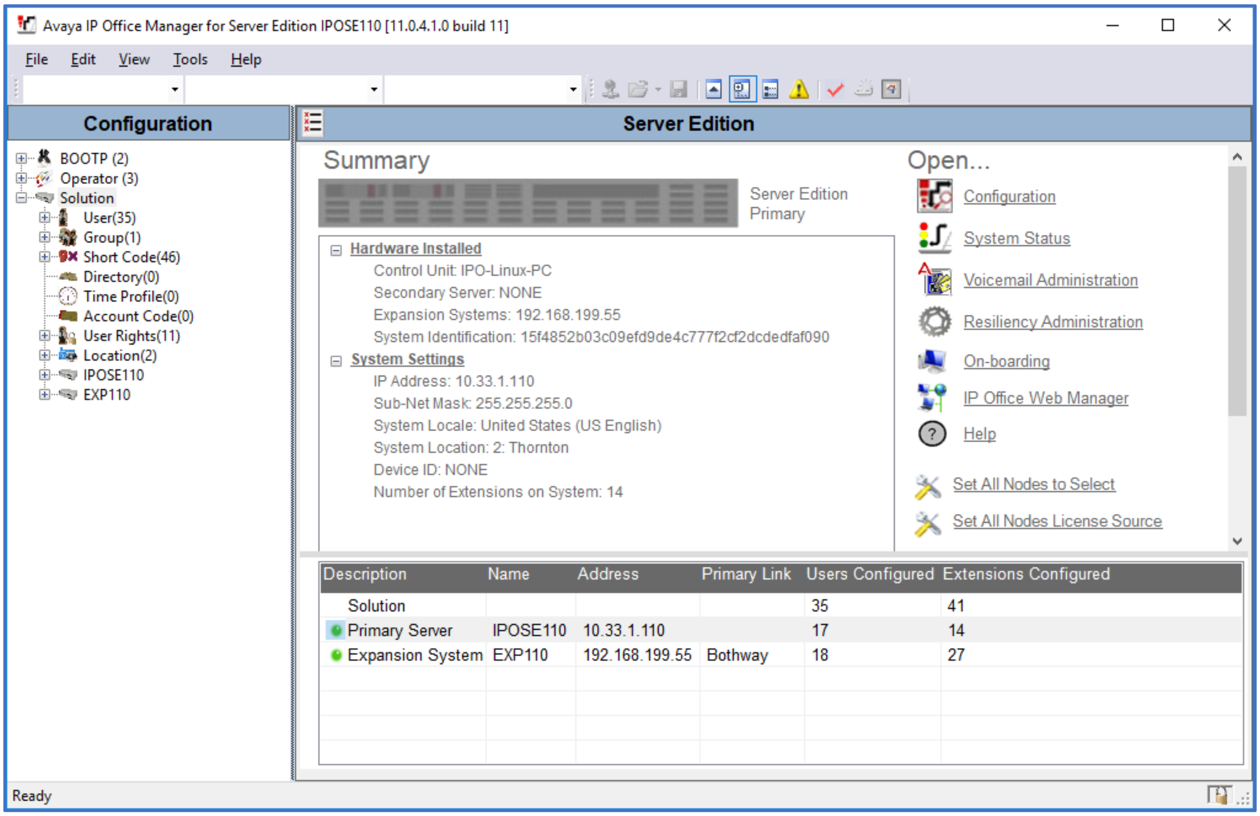
Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints.

5. Avaya IP Office Primary Server Configuration

Avaya IP Office is configured through the Avaya IP Office Manager application. From the PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in using the appropriate credentials.



On Server Edition systems, the Solution View screen will appear, similar to the one shown below. All the Avaya IP Office configurable components are shown in the left pane, known as the Navigation Pane. Clicking the "plus" sign next to the Primary server system name, e.g., **IPOSE110**, on the navigation pane will expand the menu on this server.



In the screens presented in the following sections, the View menu was configured to show the Navigation pane on the left side and the Details pane on the right side. These panes will be referenced throughout the rest of this document.

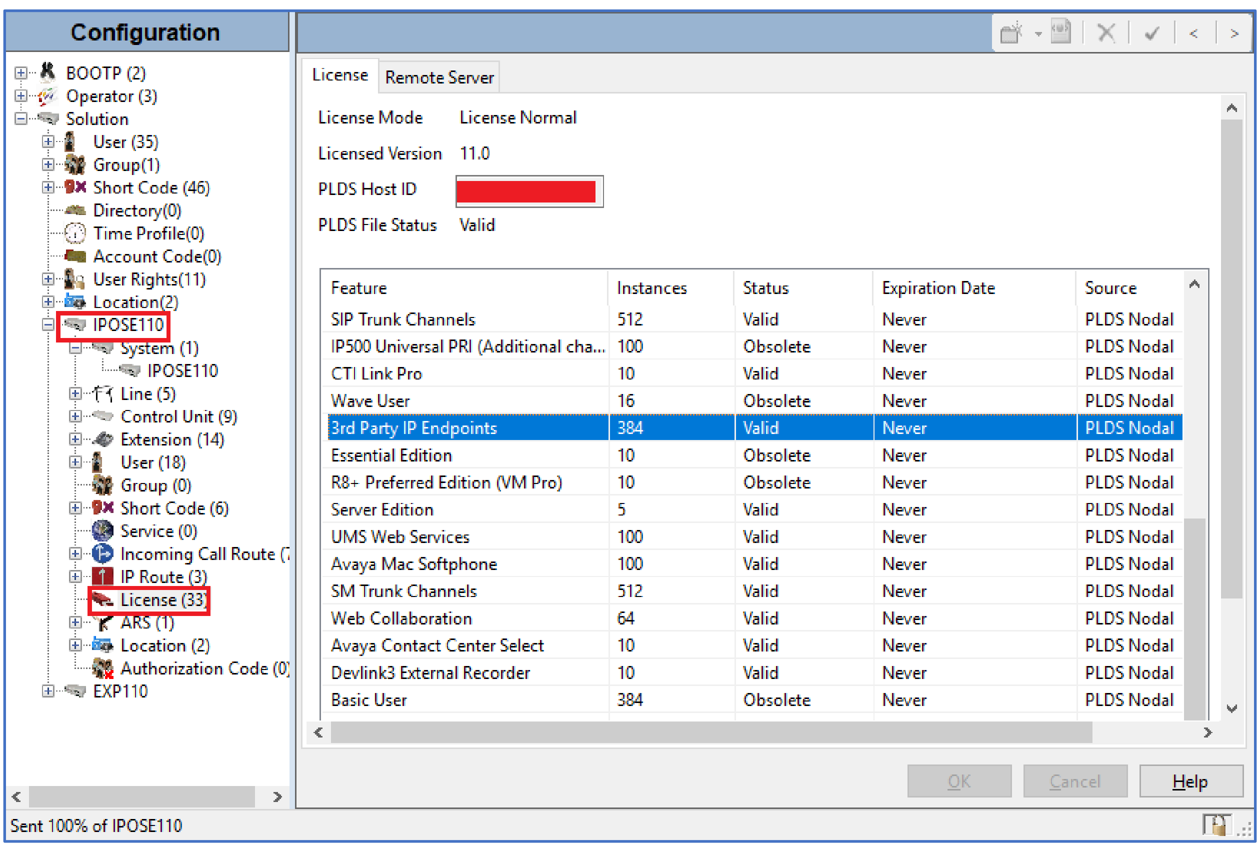
Standard feature configurations that are not directly related to the interfacing with the service provider are assumed to be already in place, and they are not part of these Application Notes.

5.1. Licensing

The configuration and features described in these Application Notes require the IP Office system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

In the reference configuration, **IPOSE110** was used as the system name of the Primary Server and **EXP110** was used as the system name of the Expansion System. All navigation described in the following sections (e.g., **License**) appears as submenus underneath the system name in the Navigation Pane.

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **3rd Party IP Endpoints** is Valid and that the number of **Instances** is sufficient to support the number of channels provisioned for the SIP trunk.



5.2. System Settings

Configure the necessary system settings. The LAN2 tab settings correspond to the IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side).

Note: In the compliance test, the LAN1 interface was used to connect the Avaya IP Office to the enterprise site IP network (private network). The LAN2 interface configuration is not directly relevant to the interface with the Komutel SIT2 SIP Console, and therefore is not described in these Application Notes.

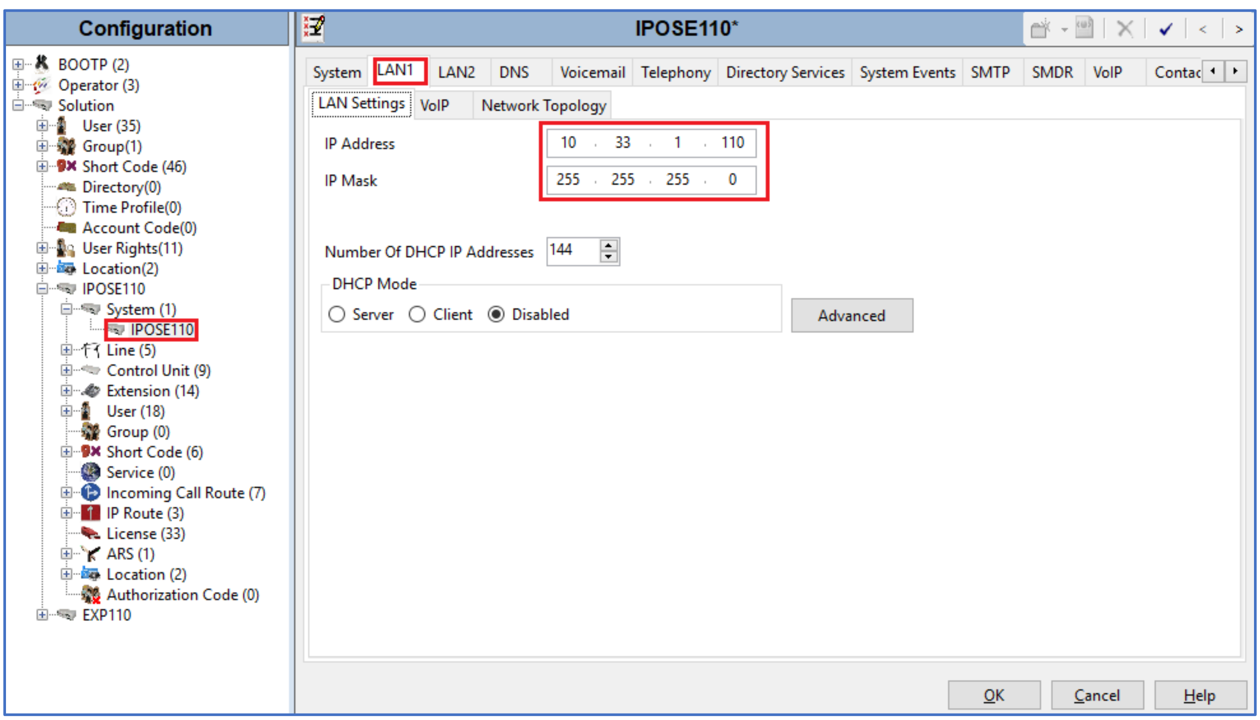
5.2.1. System – LAN1 Tab

In the sample configuration, the LAN1 interface is used for the SIP Registrar for SIP endpoint.

5.2.1.1 LAN1 - LAN Settings Tab

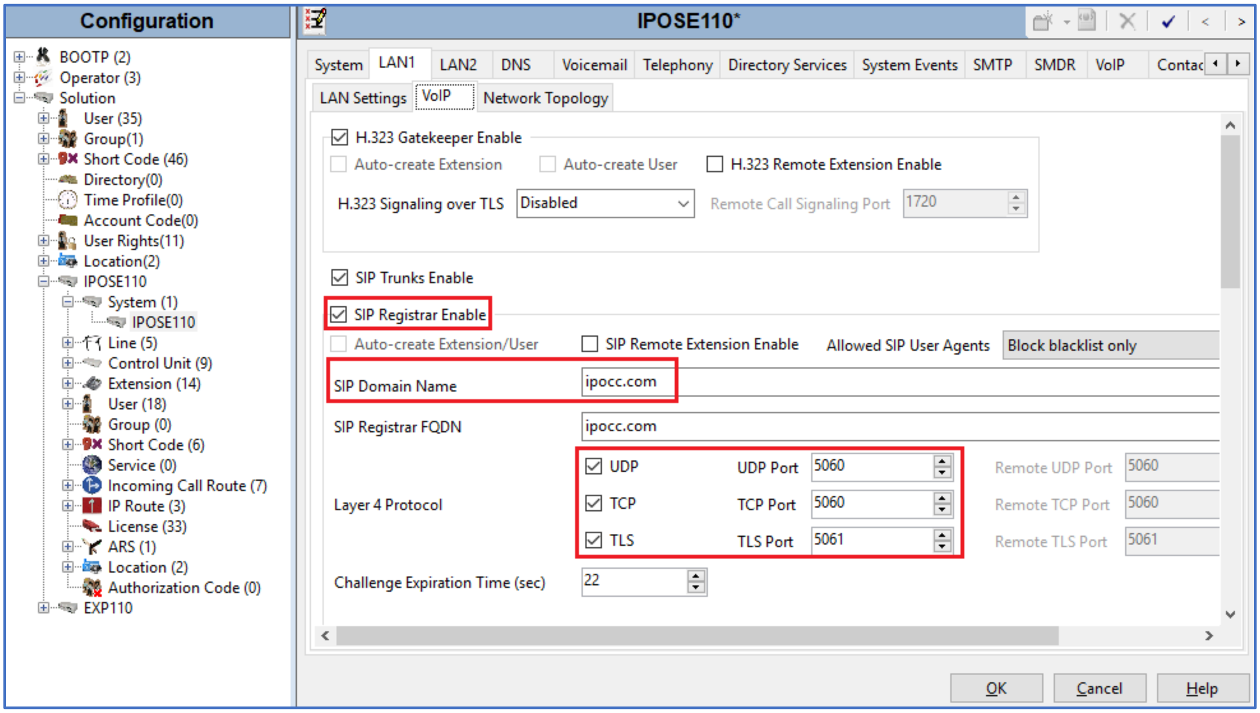
To view or configure the LAN1 IP address and subnet mask, select the **LAN1 → LAN Settings** tab, and enter the information as needed, according to the customer network requirements:

- **IP Address: 10.33.1.110** was used in the reference configuration, this is the public IP address assigned to IP Office.
- **IP Mask: 255.255.255.0** was used in the reference configuration.
- Other parameters on this screen are set to the defaults.



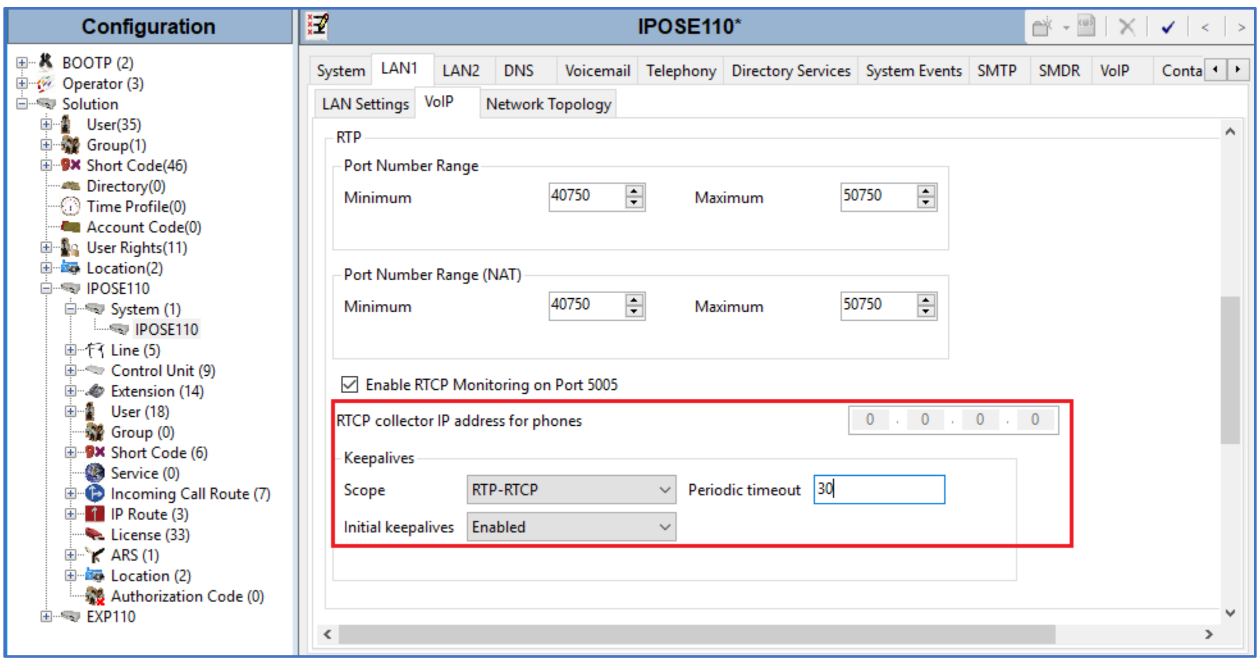
5.2.1.2 LAN1 VoIP Tab

- Select the **LAN1 → VoIP** tab in the Details Pane. Check the **SIP Registrar Enable** box to allow the configuration of SIP Registrar. Enter a SIP domain "***ipocc.com***" in the **SIP Domain Name** field and make sure all protocols and its port enabled and configured in the **Layer 4 Protocol** section. In the compliance test, Komutel SIT2 SIP endpoint registered to IP Office using UDP protocol.



Scroll down the page:

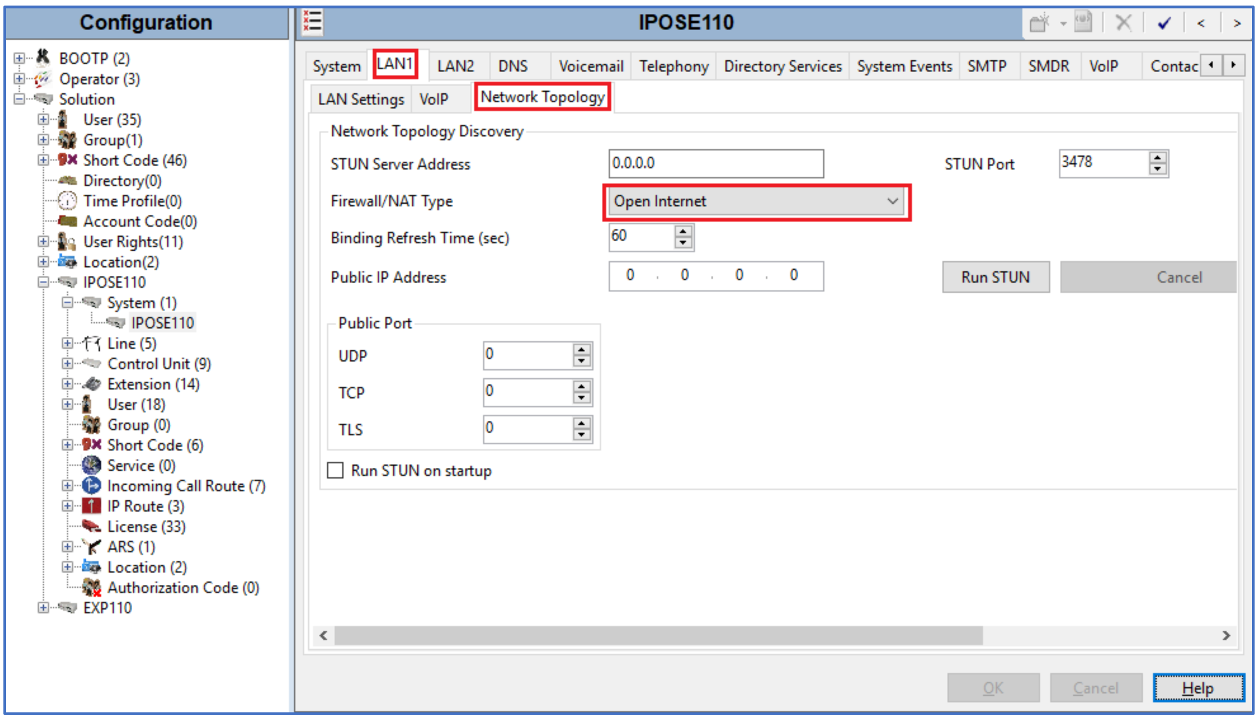
- Verify the **RTP Port Number Range**. Based on this setting, Avaya IP Office will request RTP media to be sent to a UDP port in the configurable range for calls using LAN1. The **Minimum** and **Maximum** port numbers were kept at their default values in the reference configuration.
- In the **Keepalives** section, set the **Scope** to **RTP-RTCP**. Set the **Periodic timeout** to **30** and the **Initial keepalives** parameter to **Enabled**. This is done to prevent possible issues with network firewalls closing idle RTP channels.
- In the **DiffServ Settings** section, IP Office can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services (QoS) policies for both signaling and media. The **DSCP** field is the value used for media, while the **SIG DSCP** is the value used for signaling. These settings should be set according to the customer's QoS policies in place. The default values used during the compliance test are shown.
- Click **OK** to commit (not shown).



5.2.1.3 LAN1 - Network Topology Tab

On the **LAN1 Network Topology** tab in the Details pane, set the following:

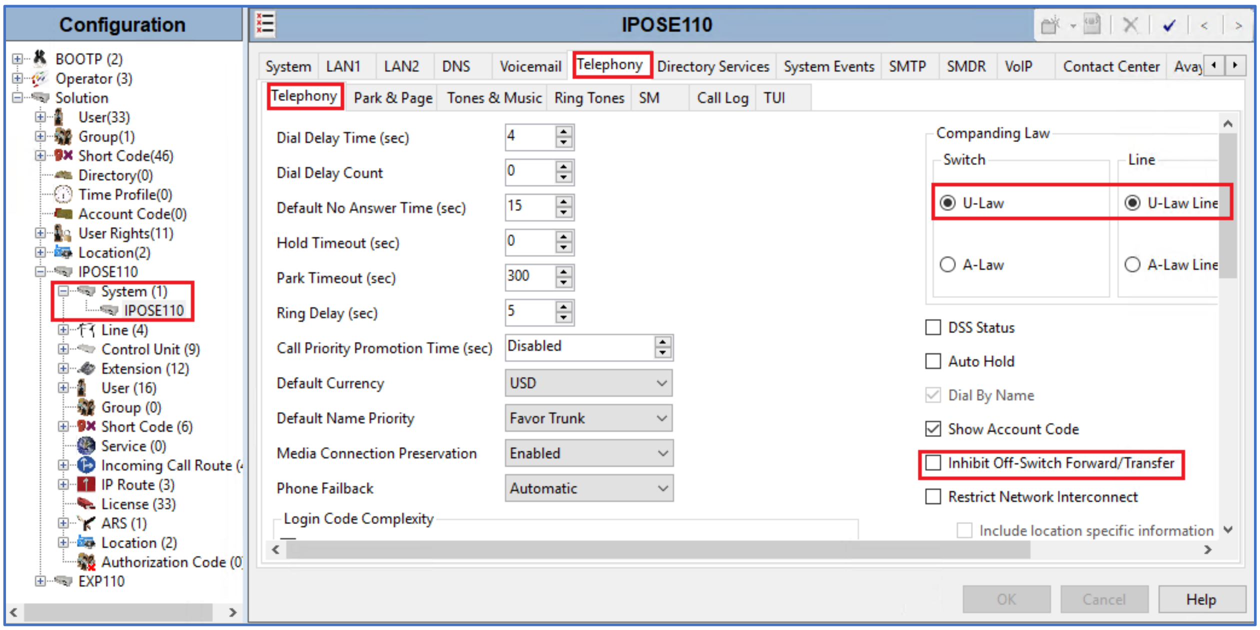
- Select the **Firewall/NAT Type** from the pull-down menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used.
- Set **Binding Refresh Time (seconds)** to **60.** This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to SIP endpoint and SIP trunk service on this LAN.
- Default values were used for all other parameters.
- Click the **OK** button (not shown).



5.2.2. Telephony Tab

To access the System Telephony settings, navigate to the **Telephony → Telephony** tab in the **Details** pane, configure the following parameters:

- Choose the **Companding Law** typical for the enterprise location; **U-Law** was used for the compliance test.
- Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN. If for security reasons incoming calls should not be allowed to transfer back to the PSTN then leave this setting checked.
- All other parameters should be set to default or according to customer requirements.
- Click **OK** to commit (not shown).



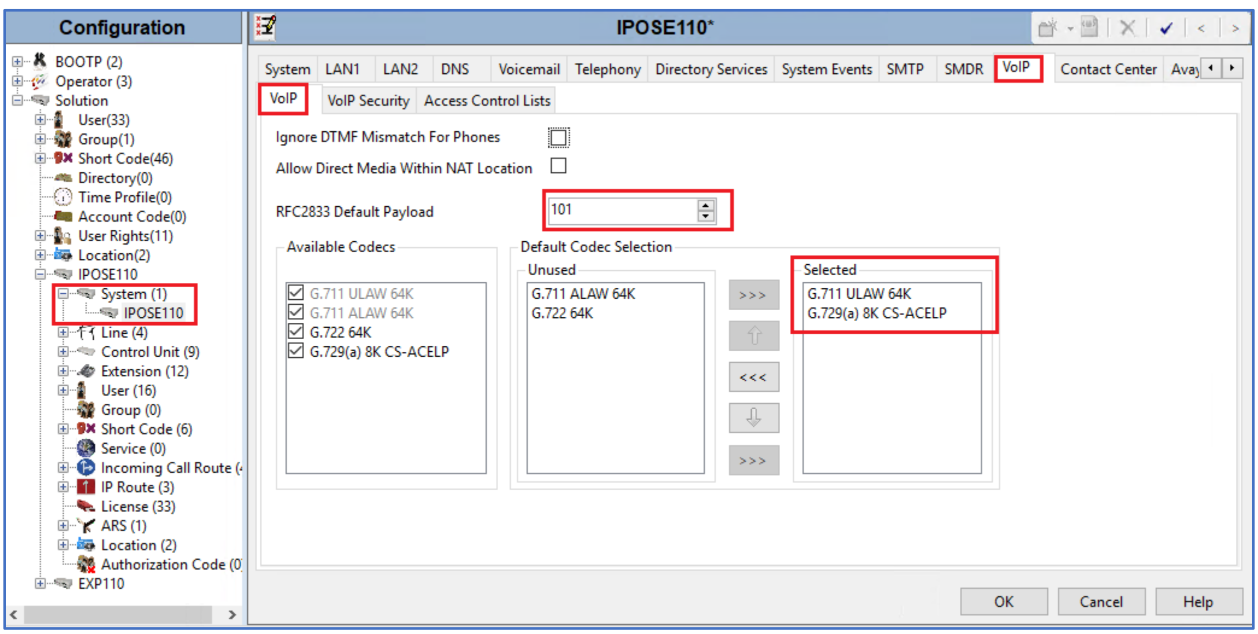
5.2.3. VoIP Tab

Navigate to the **VoIP** tab in the Details pane to view or change the system codecs and VoIP security settings.

5.2.3.1 VoIP - VoIP Tab

Select the **VoIP → VoIP** tab, configure the following parameters:

- The **RFC2833 Default Payload** field allows for the manual configuration of the payload type used on SIP calls that are initiated by the IP Office. The default value **101** was used.
- For codec selection, select the codecs and codec order of preference on the right, under the **Selected** column. The **Default Codec Selection** area enables the codec preference order to be configured on a system-wide basis. The buttons between the two lists can be used to move codecs between the **Unused** and **Selected** lists, and to change the order of the codecs in the **Selected** codecs list. By default, all IP lines and phones (SIP and H.323) will use the system default codec selection shown here, unless configured otherwise for a specific line or extension. The example below shows the codecs used for IP phones (SIP and H.323), the system's default codecs and order were used.
- Click **OK** to commit (not shown).



Note: The codec selections defined under this section (VoIP – VoIP Tab) are the codecs selected for the IP phones/extensions.

5.2.3.2 VoIP – VoIP Security Tab

Secure Real-Time Transport Protocol (SRTP) refers to the application of additional encryption and or authentication to VoIP calls (SIP and H.323). SRTP can be applied between telephones, between ends of an IP trunk or in various other combinations.

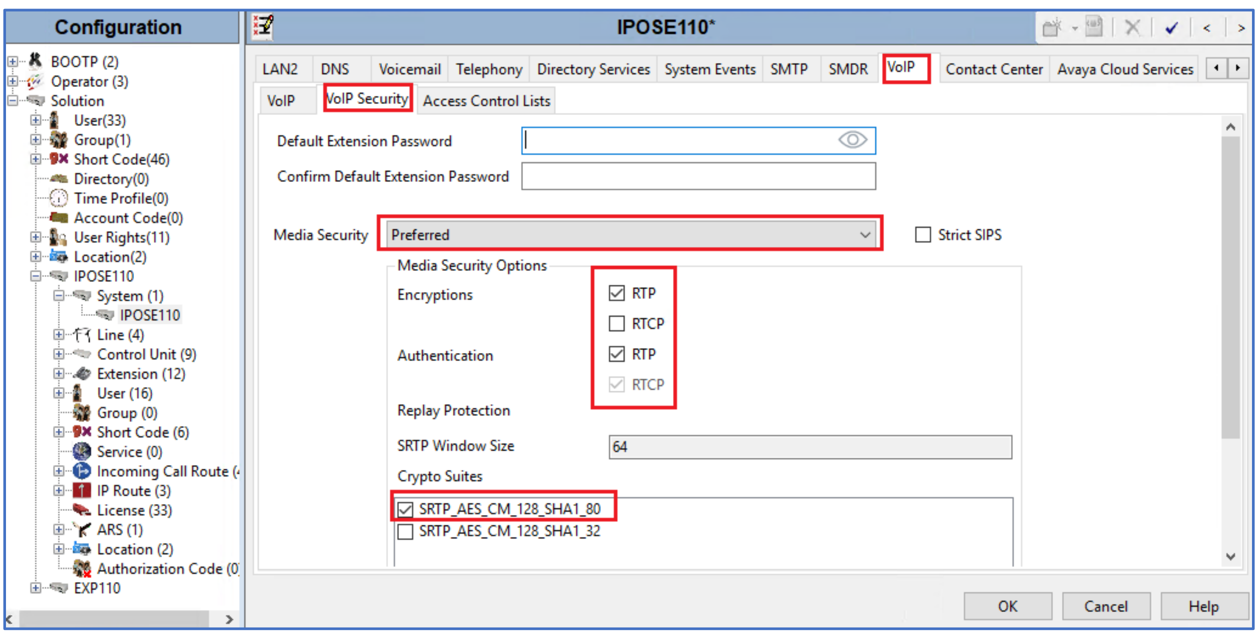
Configuring the use of SRTP at the system level is done on the **VoIP Security** tab using the Media Security setting. The options are:

- Disabled (default).
- Preferred.
- Enforced.

When enabling SRTP on the system, the recommended setting is **Preferred**. In this scenario, IP Office uses SRTP if supported by the far-end, otherwise uses RTP. If the **Enforced** setting is used, and SRTP is not supported by the far-end, the call is not established.

To configure the use of SRTP, select the **VoIP → VoIP Security** tab on the Details pane.

- Set the **Media Security** drop-down menu to **Preferred** to have IP Office attempt use encrypted RTP for devices that support it and fall back to RTP for devices that do not support encryption.
- Verify **Strict SIPS** is not checked.
- Under **Media Security Options**, select **RTP** for the **Encryptions** and **Authentication** fields.
- Under **Crypto Suites**, select **SRTP_AES_CM_128_SHA1_80**.
- Click **OK** to commit (not shown).

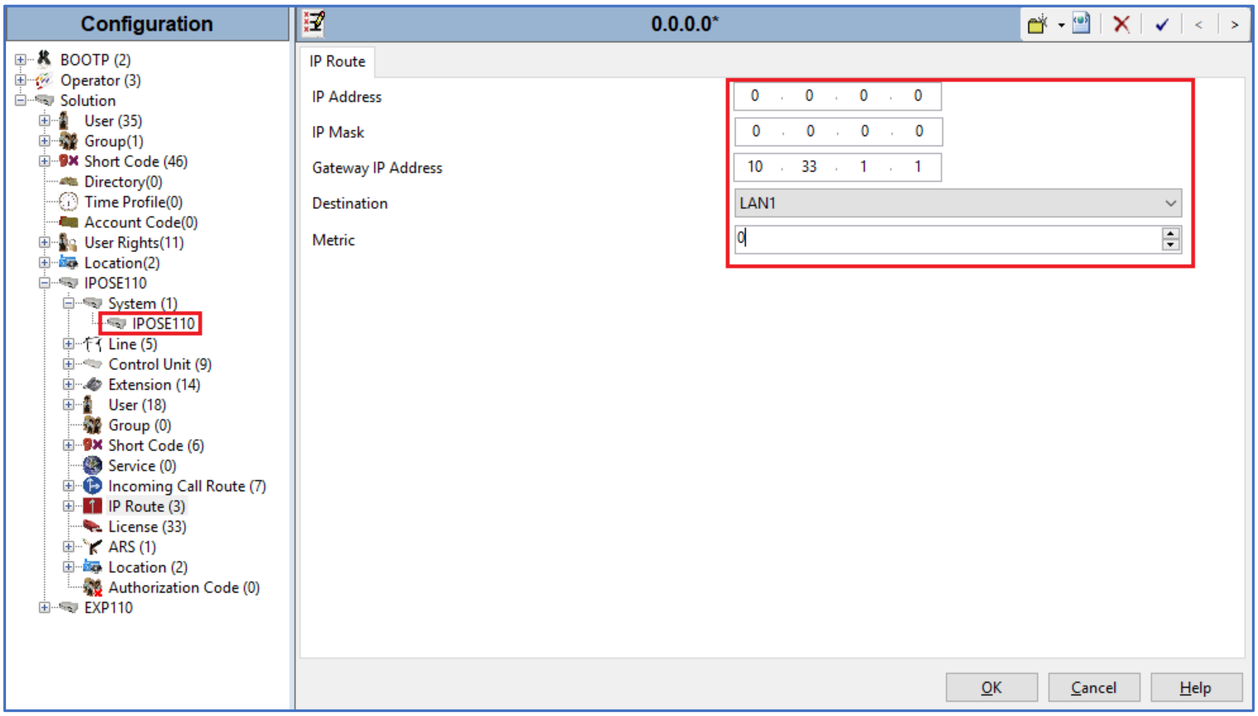


5.3. IP Route

Create an IP route to specify the IP address of the gateway or router where the IP Office needs to send the packets in order to communicate with endpoints.

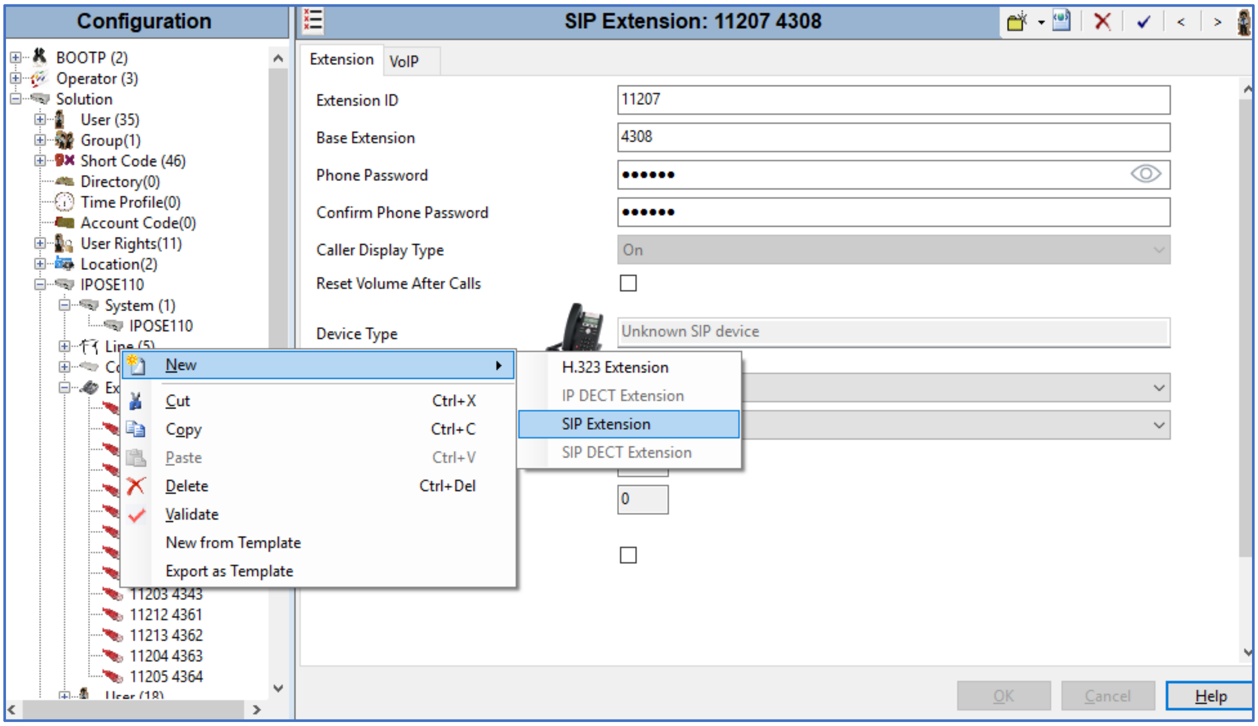
Navigate to **IP Route**, right-click on **IP Route** and select **New**. The values used during the compliance test are shown below:

- Set the **IP Address** and **IP Mask** to **0.0.0.0** to make this the default route.
- Set **Gateway IP Address** to the IP address of the gateway/router used to route calls to the network, e.g., **10.33.1.1**.
- Set **Destination** to **LAN1** from the pull-down menu.
- Click **OK** to commit (not shown).

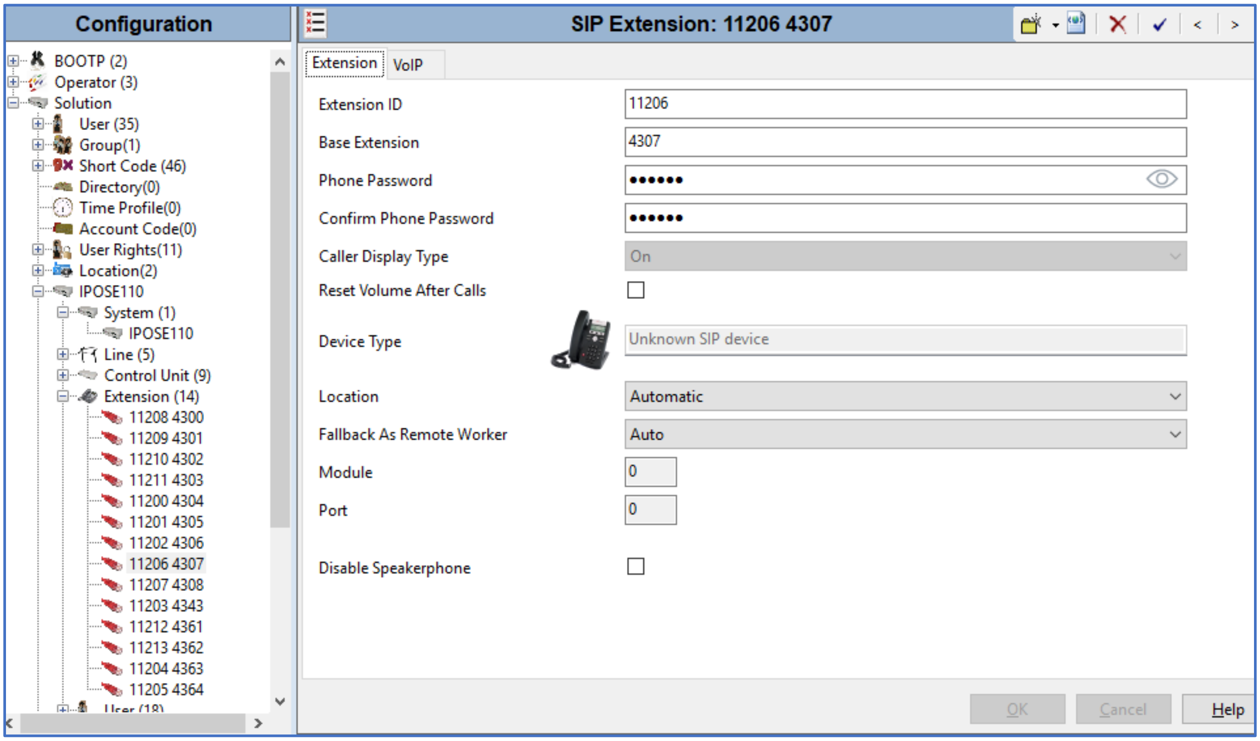


5.5. Administer SIP Extension

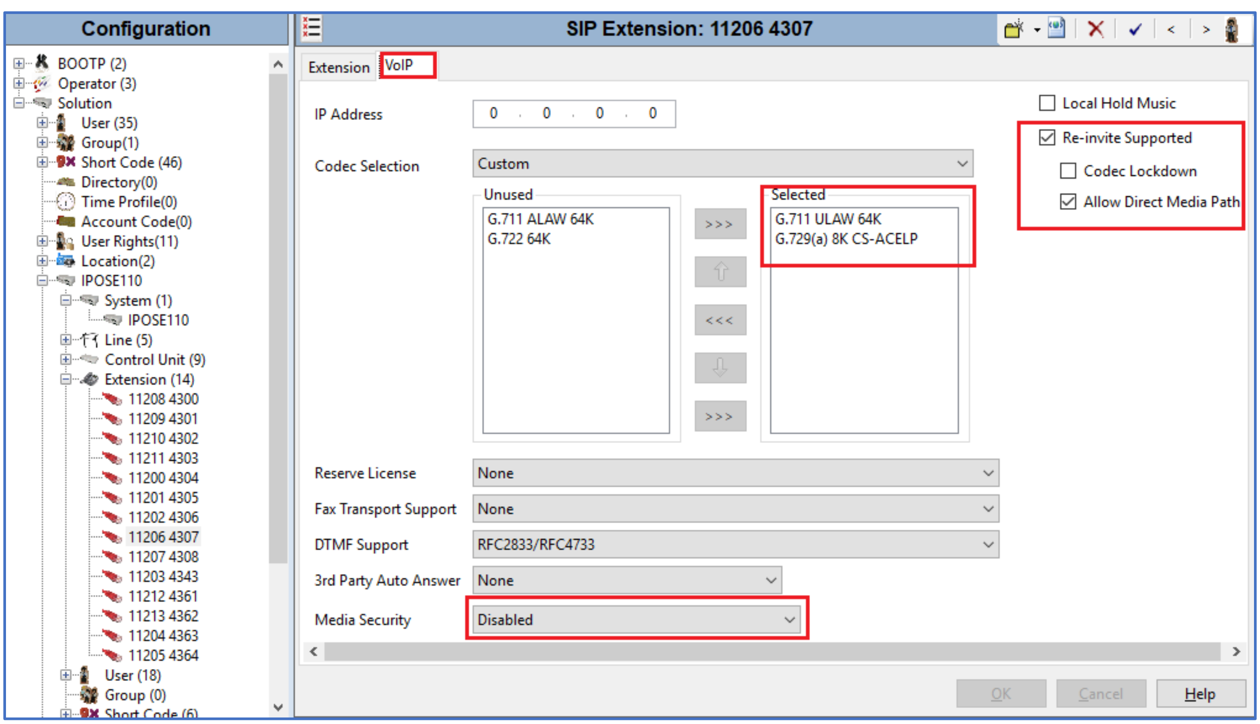
An extension needs to be created for every SIP endpoint that regiters to IP Office. To create a new extension, from the left navigate pane, right click on **Extension → New → SIP Extension**.



The screen below shows the pre-created extension **4307** that was used for the compliance test. Note that the password is set in the **Phone Password** field is later used for Komutel SIT2 registerting to IP Office.

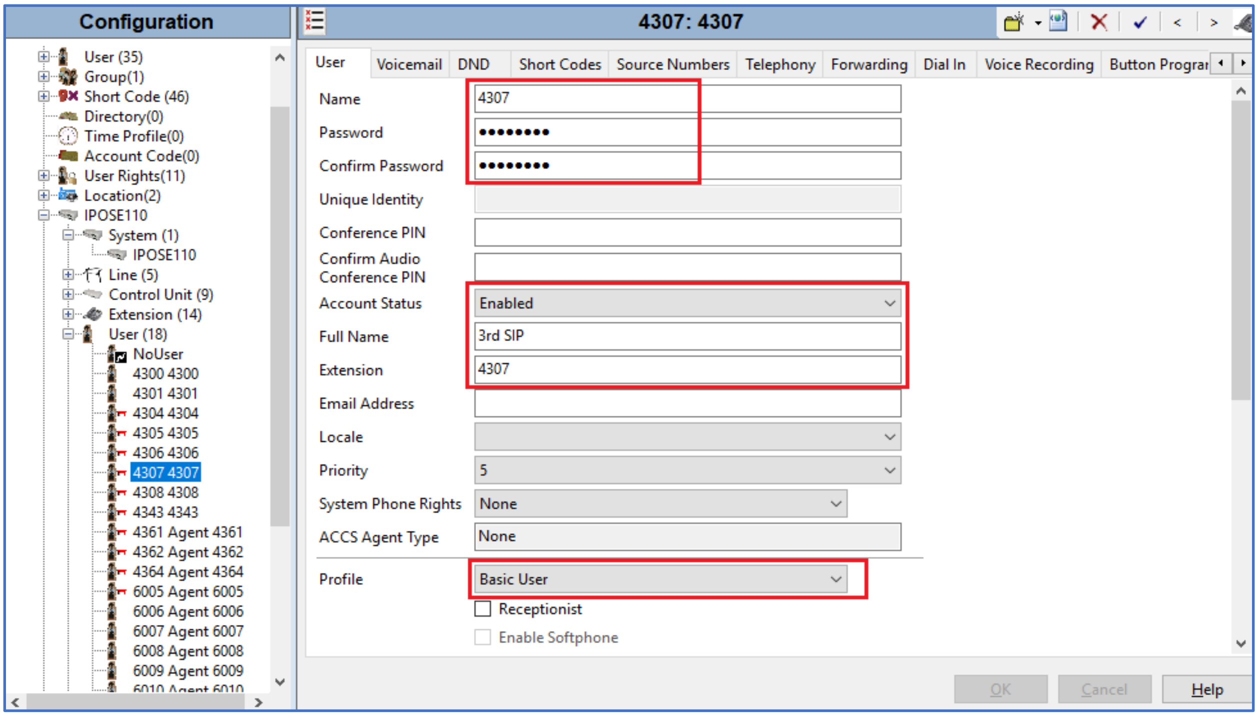


The screen below shows the **VoIP** tab of the extension 4307, make sure the **Media Security** is set to **Disabled** to avoid audio issue since the Komutel SIT2 did not support secure media SRTP for the testing.

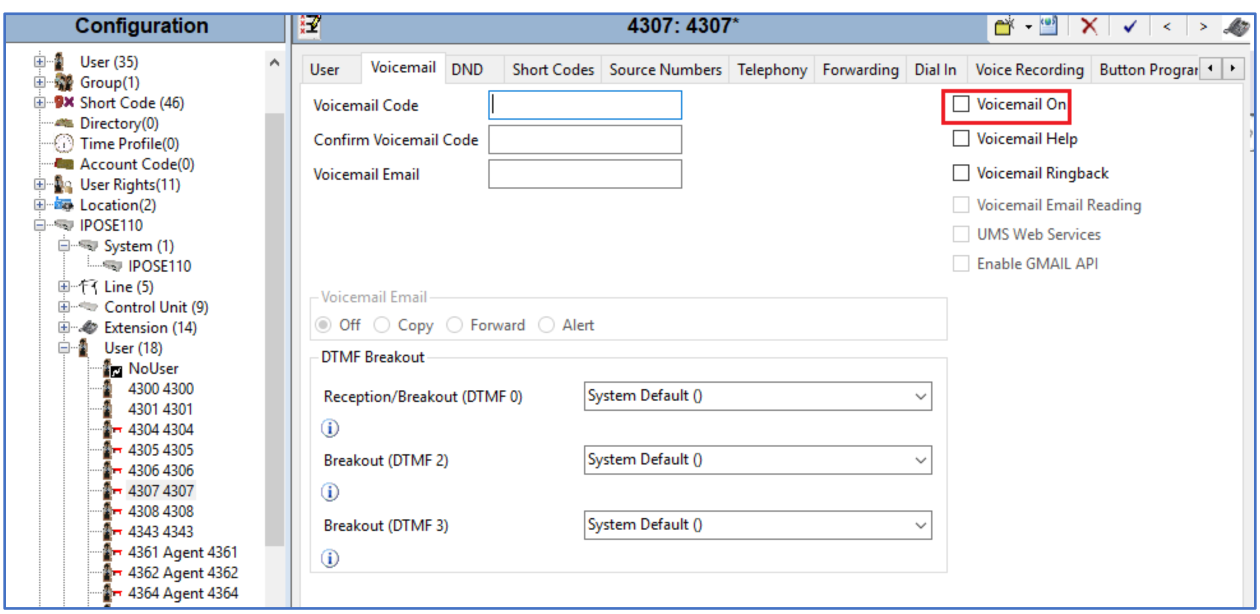


5.6. Administer SIP User

A user can be newly added as new or edit by selecting **User** in the left pane. The screen below shows the user 4307 that was created for the testing. The extension **4307** is entered in the **Extension** field, the name is entered in the Full Name field will be displayed in other endpoint as call established.



In the **Voicemail** tab, uncheck the Voicemail On checkbox because Komutel SIT2 does not support voicemail and MWI.

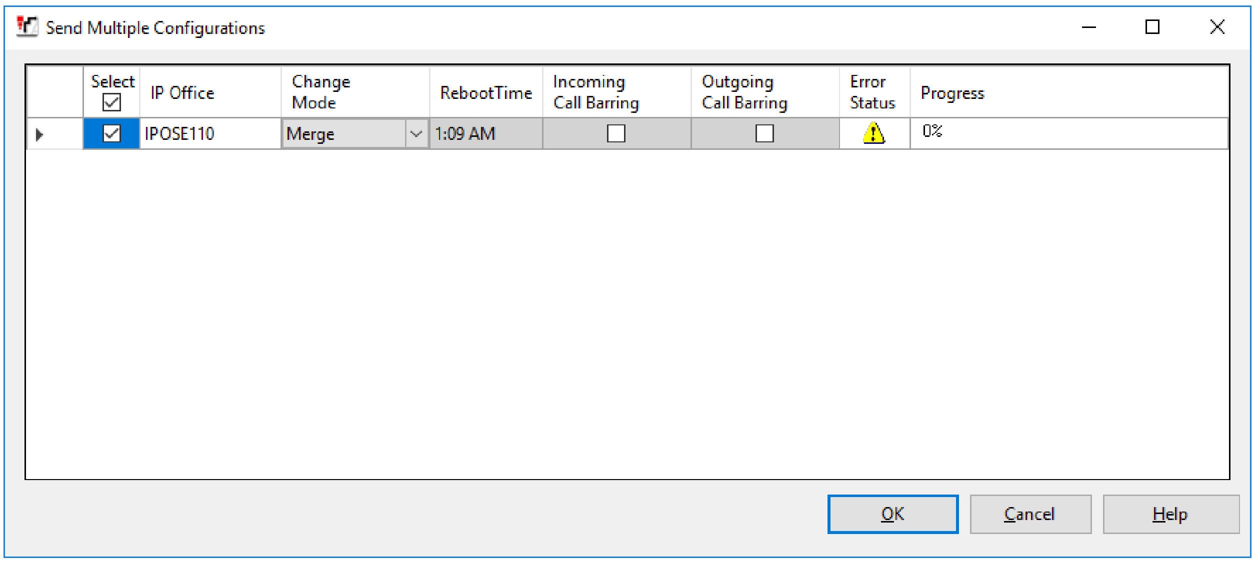


5.7. Save IP Office Primary Server Configuration

The provisioning changes made in Avaya IP Office Manager must be applied to the Avaya IP Office server in order for the changes to take effect. At the top of the Avaya IP Office Manager page, click **File → Save Configuration** (if that option is grayed out, no changes are pending).

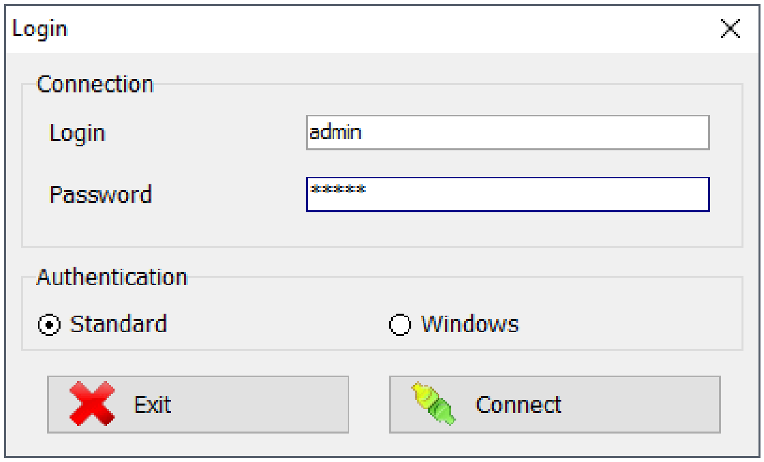
A screen similar to the one below will appear, with either **Merge** or **Reboot** automatically selected, based on the nature of the configuration changes. The **Merge** option will save the configuration change with no impact to the current system operation. The **Reboot** option will save the configuration and cause the Avaya IP Office server to reboot.

Click **OK** to execute the save.

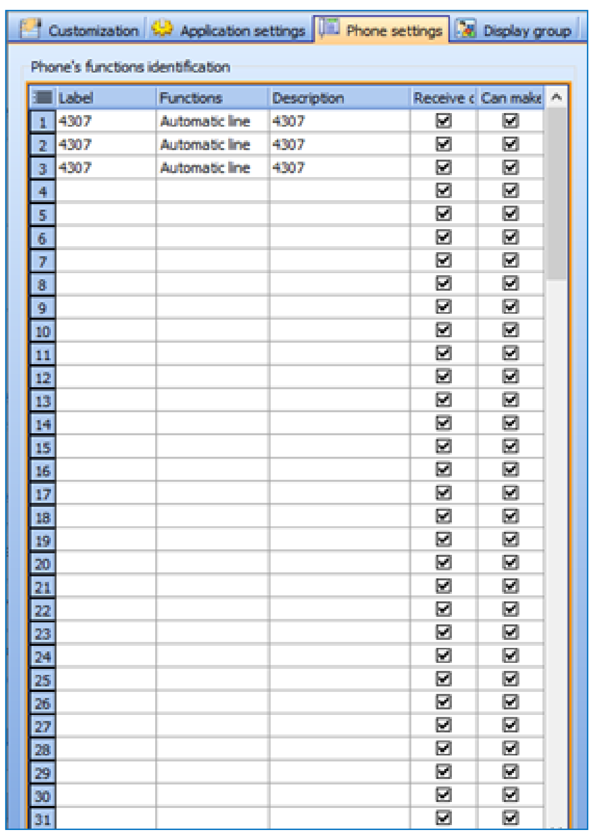


6. Configure Komutel SIT2 SIP Console

Launch the SIT2 SIP Console application and login in with the appropriate credentials.

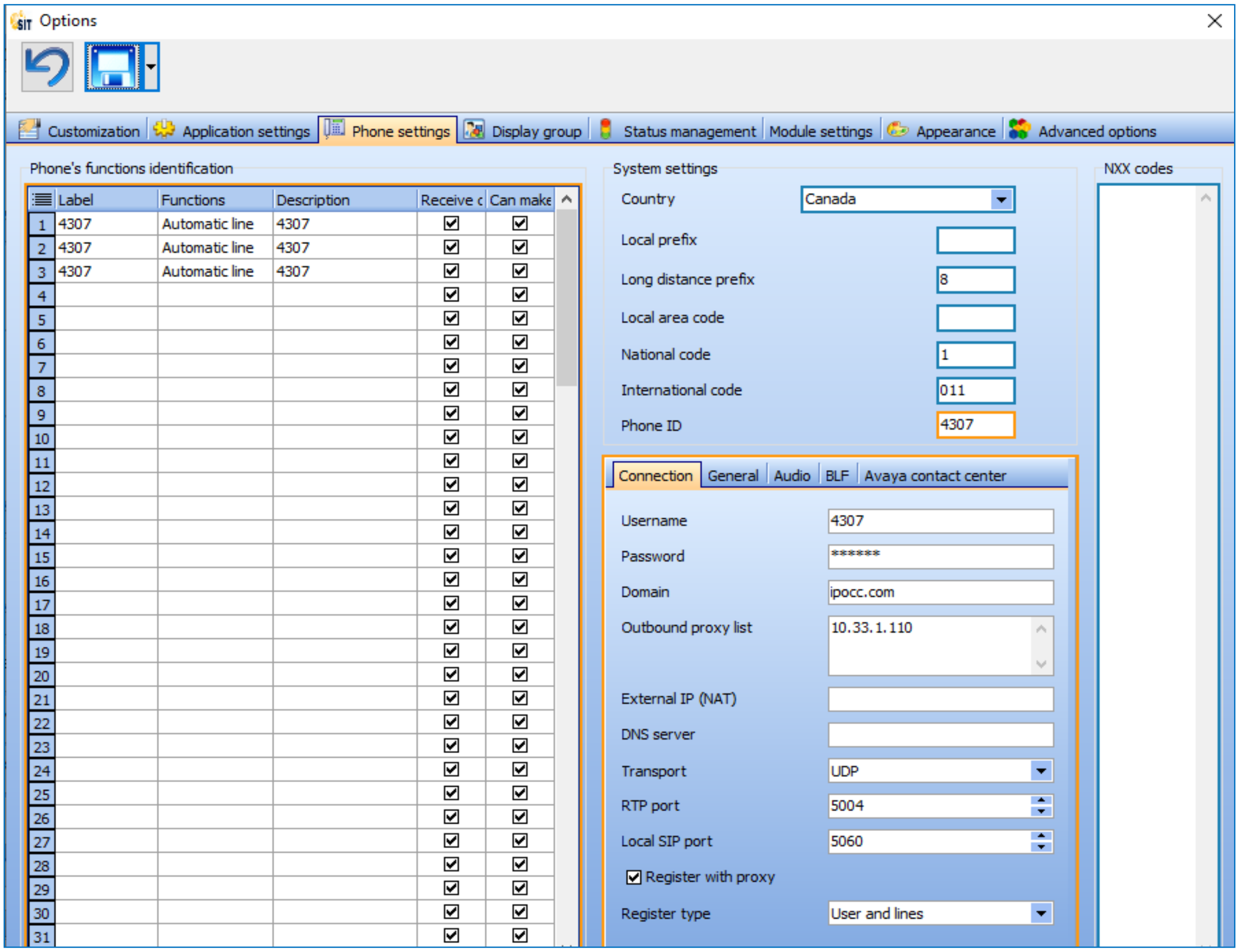


To configure the console's lines, navigate to the **Tools → Options → Phone Settings** tab. Depending on the number of lines that are available, choose *Automatic Line* in the **Functions** column, enter the **DN** in the **Description** column and type the text that will be displayed on the line's button in the **Label** column. As shown below, the console was configured with three line appearances with extension 4307.

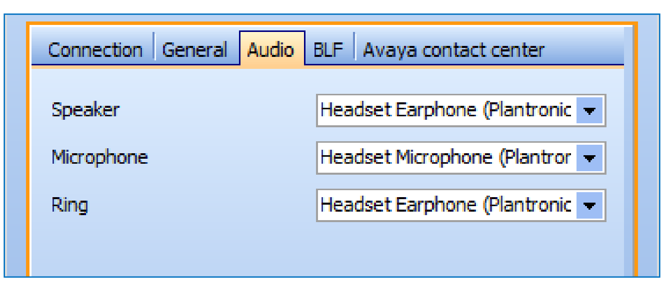


In the **Connection** tab, configure the SIP parameters, including:

- Enter **Username** and **Password** as configured in **Section 5.6** to register with IP Office.
- Enter the SIP domain ***ipocc.com*** in the **Domain** field.
- Enter the IP Office IP address of LAN1 in the **Outbound proxy list** field.



In the **Audio** tab, specify the audio device or headset that will be used with the console.



Click on the **Save** button  on the **Options** window to save the configuration.

7. Verification Steps

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

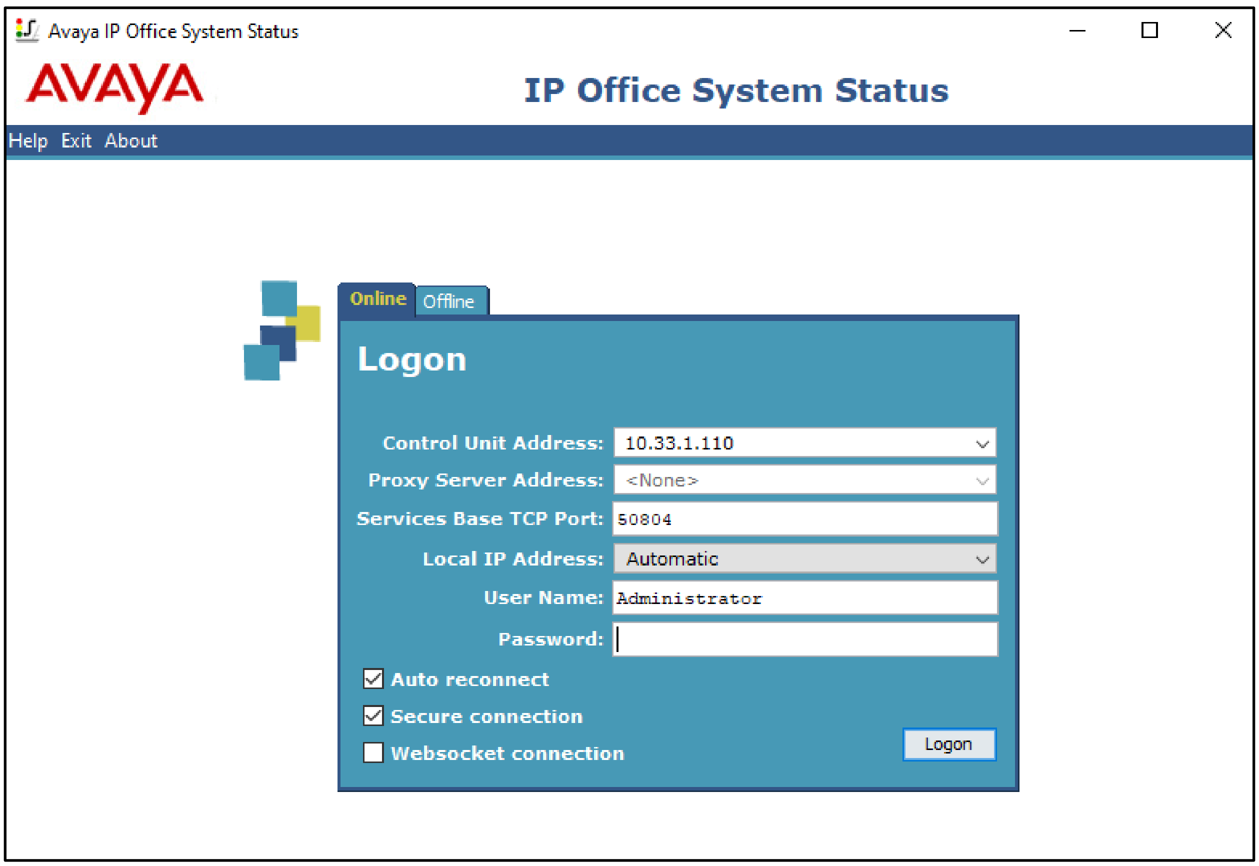
The following steps may be used to verify the configuration:

- Verify that Komutel SIT2 SIP can place calls to local extensions.
- Verify that Komutel SIT2 SIP can receive calls from local extensions.

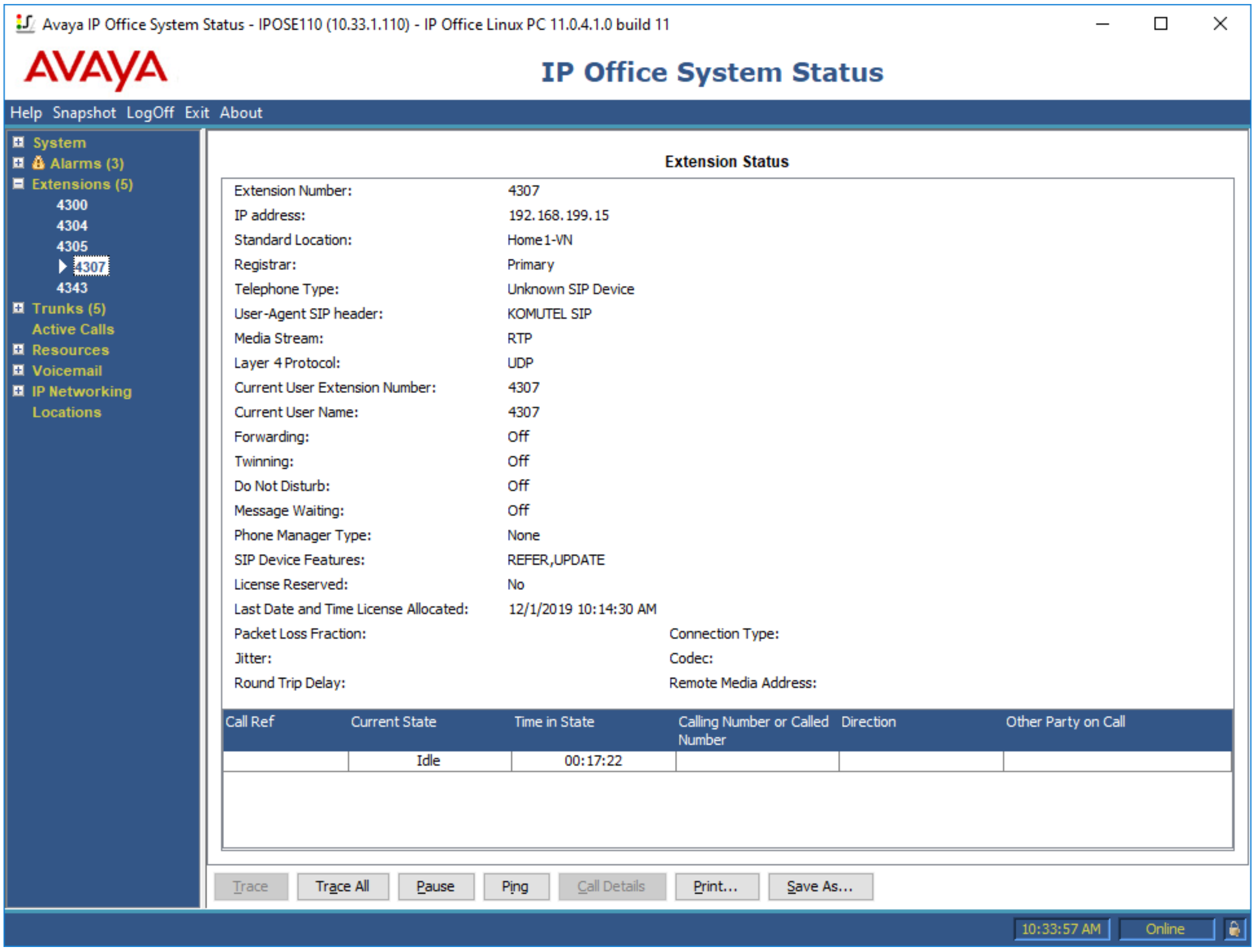
7.1. IP Office System Status

The following steps can also be used to verify the configuration.

Use the IP Office **System Status** application to verify the state of SIP connections. Launch the application from **Start → Programs → IP Office → System Status** on the PC where IP Office Manager is installed, log in with the proper credentials.

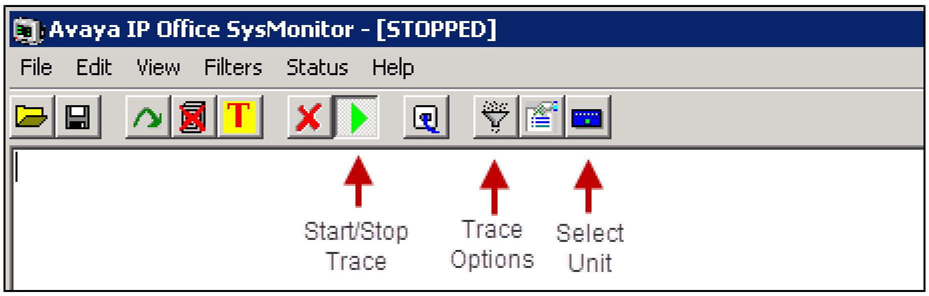


Expand the **Extensions** from the left pane and select the extension 4307, the **Extension Status** window displays in the right pane, verify the **Current State** is **Idle**.

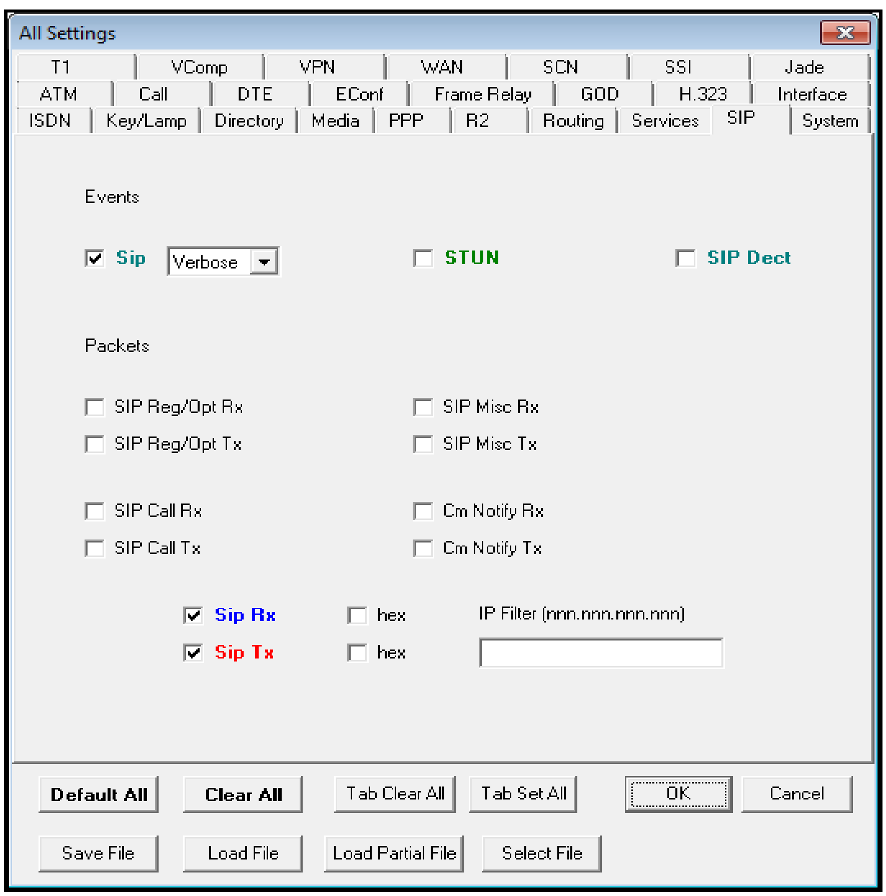


7.2. Monitor

The Avaya IP Office Monitor application can be used to monitor and troubleshoot signaling messaging on the SIP register. Launch the application from **Start → Programs → IP Office → Monitor** on the PC where IP Office Manager was installed. Click the **Select Unit** icon on the taskbar and Select the IP address of the IP Office system under verification.

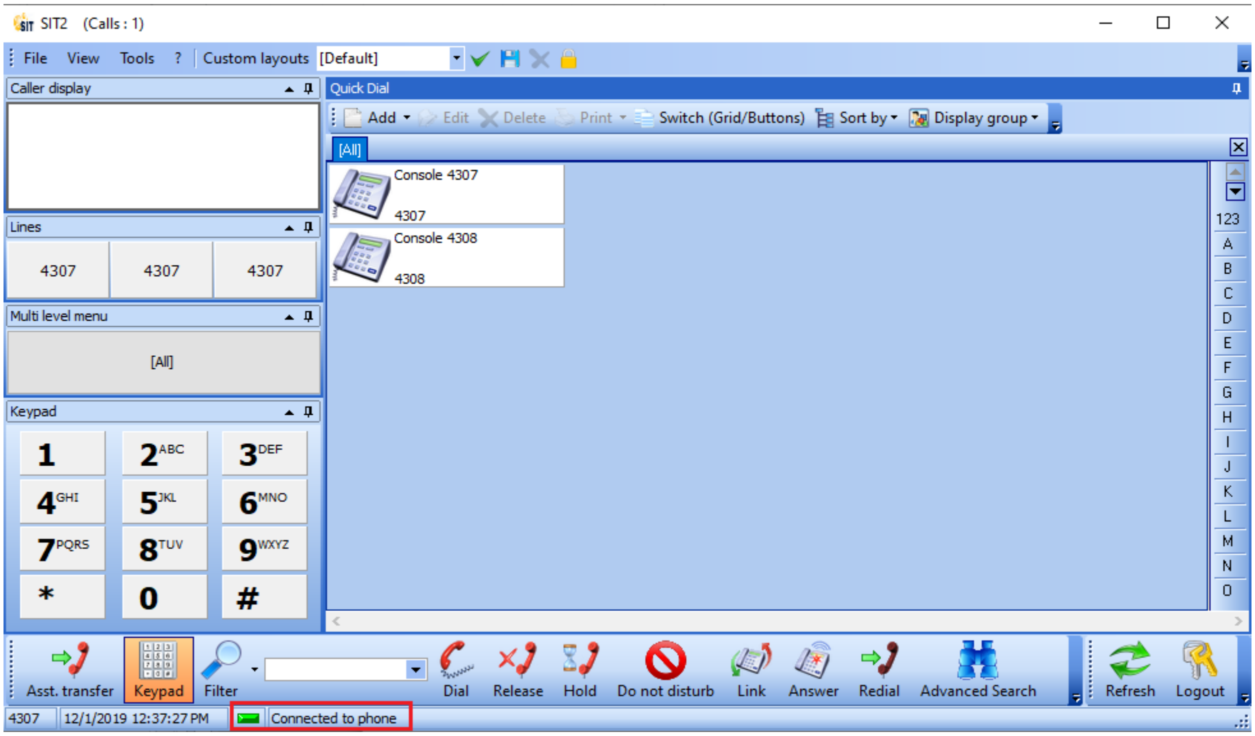


Clicking the **Trace Options** icon on the taskbar, selecting the **SIP** tab allows modifying the threshold used for capturing events, types of packets to be captured, filters, etc. Additionally, the color used to represent the packets in the trace can be customized by right clicking on the type of packet and selecting the desired color.

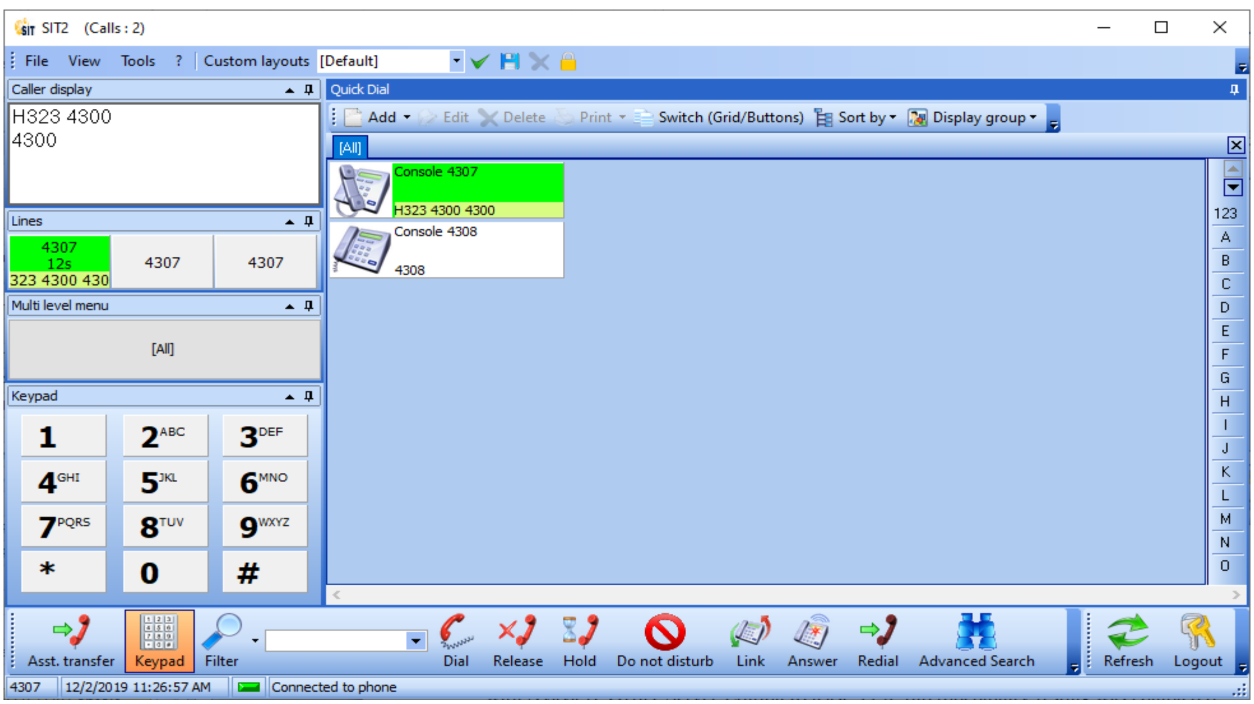


7.3. Verify Komutel SIT2 SIP Console

Verify the Komutel SIT2 SIP console is able to register successfully to IP Office, the status in the bottom should show the green icon and “Connected to phone”.



Verify the Komutel SIT2 SIP console is able to answer an incoming call with a clear voice.



8. Conclusion

These Application Notes describe the configuration necessary for Komutel SIT2 SIP Console with Avaya IP Office Server Edition Release 11.0. Interoperability testing was completed successfully with the observations/limitations outlined in the scope of testing in **Section 2.1** as well as under test results in **Section 2.2**.

9. Additional References

This section references the documentation relevant to these Application Notes. Product documentation for Avaya IP Office, including the following, is available at:
http://support.avaya.com/

[1] *Deploying IP Office Platform Server Edition Solution*, Release 11.0, May 2018

[2] *IP Office Platform 11.0, Deploying Avaya IP Office Servers as Virtual Machines*, January 2019

[3] *IP Office Platform 11.0, Deploying Avaya IP Office Essential Edition (IP500 V2)*, February 2019.

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

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

[6] *Planning for and Administering Avaya Equinox for Android, iOS, Mac and Windows, Release 3.4.8, November 2018*

[7] *Using Avaya Equinox for IP Office, Release 11.0 FP4*, February 2019

Additional Avaya IP Office documentation can be found at:
http://marketingtools.avaya.com/knowledgebase/

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.