



DevConnect Program

Application Notes for Configuring Avaya IP Office 12.0 with Keyyo SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Keyyo SIP Trunk and Avaya IP Office.

The Keyyo SIP Trunk Platform provides PSTN access via a SIP trunk connected to the Keyyo Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks.

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.

Keyyo is a member of the DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

1. Introduction

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between the Keyyo SIP Trunk and Avaya IP Office. Customers using this Avaya SIP-enabled enterprise solution with Keyyo SIP Trunk are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using Avaya IP Office R12.0 to connect to the Keyyo SIP Platform. This configuration (shown in **Figure 1**) was used to exercise the features and functionality listed in **Section 2.1**.

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.

2.1. Interoperability Compliance Testing

Avaya IP Office was connected to the Keyyo SIP Trunk via a direct connection over the internet. Keyyo use DNS/SRV to manage the connection.

To verify SIP trunking interoperability the following features and functionality were exercised during the interoperability compliance test:

- Incoming PSTN calls to various phone types including H.323, SIP, Digital and Analog telephones at the enterprise.
- All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, Digital, and Analog telephones at the enterprise.
- All outbound PSTN calls were routed from the enterprise across the SIP trunk to the Service Provider.
- Calls using the G.711A, G.729 and G.722 codecs.
- Inbound and outbound PSTN calls to/from Avaya Workplace for Windows Softphone client.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38-fallback fax transmissions.
- DTMF transmission using RFC 2833 with successful Voice Mail for inbound and outbound calls.
- Various call types including: local, long distance, international, toll free (outbound) and directory assistance.
- Caller ID presentation and Caller ID restriction.
- User features such as hold and resume, and conference.
- Blind and Consultative call transfer to PSTN.
- Off-net call forwarding and mobile twinning.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for the Keyyo SIP Trunk with the following observations:

- No inbound toll-free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked by the Service Provider with the Emergency Services Operator.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on Keyyo products please visit <https://www.keyyo.com/fr/support/contact-support-partenaire/>

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Keyyo SIP Trunk. Located at the enterprise site is an Avaya IP Office 500 v2. Endpoints include an Avaya 1600 Series IP Telephone (with H.323 firmware), Avaya 9600 Series IP Telephones (with H.323 firmware), an Avaya 1140e SIP Telephone, an Avaya Analogue Telephone and a fax machine. The site also has a Windows 7 PC running Avaya IP Office Manager to configure the Avaya IP Office as well as Avaya Communicator for Windows and Avaya Communicator for Web for mobility testing. For security purposes, public IP addresses have been changed and any PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

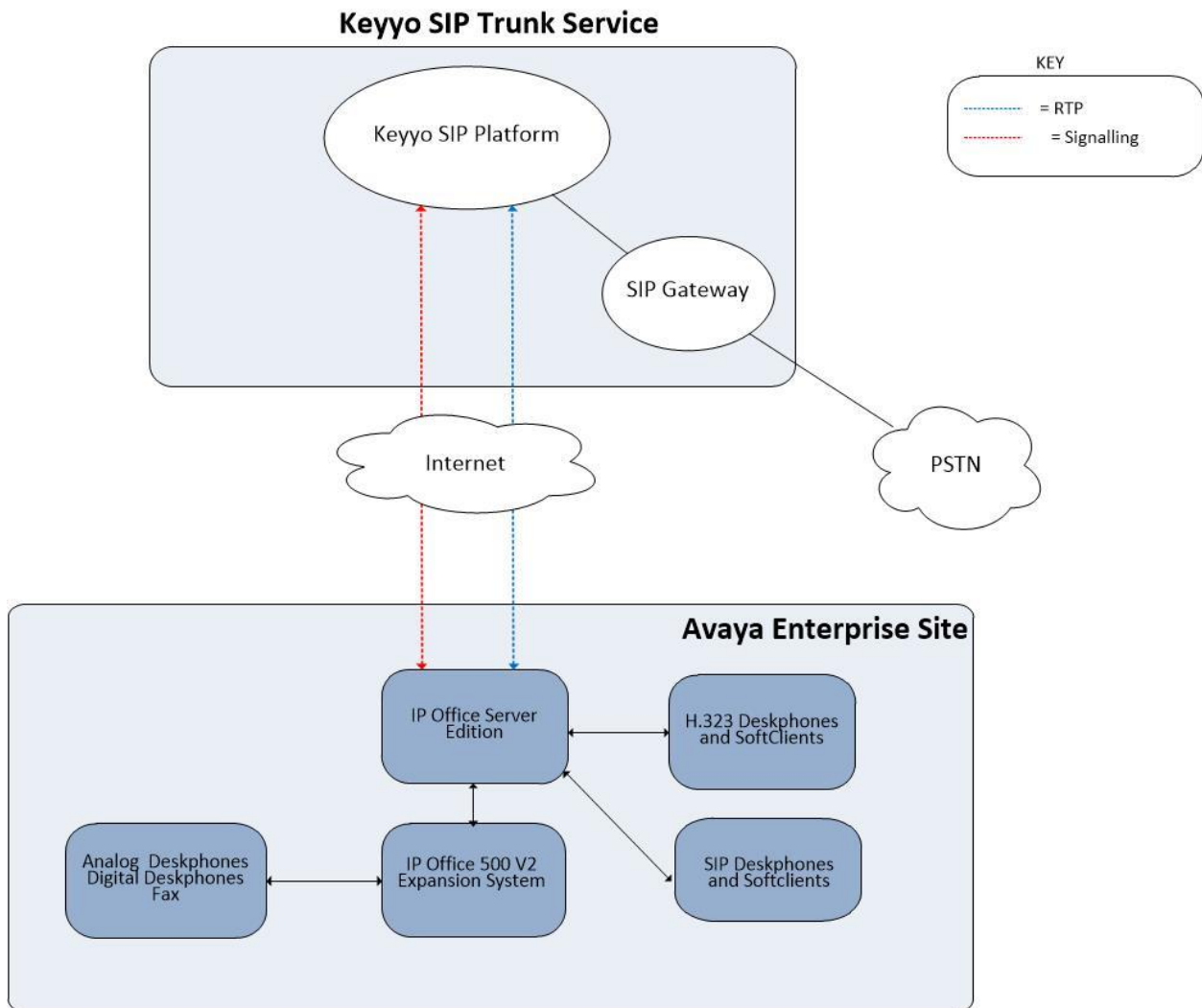


Figure 1: Keyyo SIP Trunk to Avaya IP Office Topology

4. Equipment and Software Validated

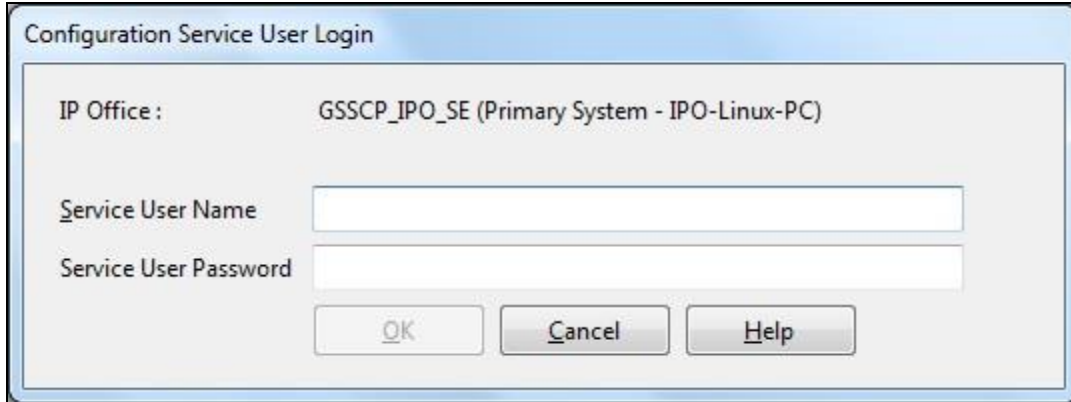
The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	Version 12.0.0.0.0 build 55
Avaya IP Office 500 V2	Version 12.0.0.0.0 build 55
Avaya Voicemail Pro Client	Version 12.0.0.26
Avaya IP Office Manager	Version 12.0.0.0.0 build 55
Avaya 1608 Phone (H.323)	1.3.12
Avaya 9611G Series Phone (H.323)	6.8.3
Avaya 9608 Series Phone (H.323)	6.8.3
Avaya J179 IP Phone (SIP)	4.0.10
Avaya Workplace for Windows (SIP)	3.36.0
Avaya 1140e (SIP)	FW: 04.04.30.00.bin
Avaya 1408 Digital Telephone	R48
Avaya 98390 Analogue Phone	N/A
Keyyo	
SIP Trunk	"Trunk SIP Libre" offer with 3 SDAs
SIP Platform	Proprietary

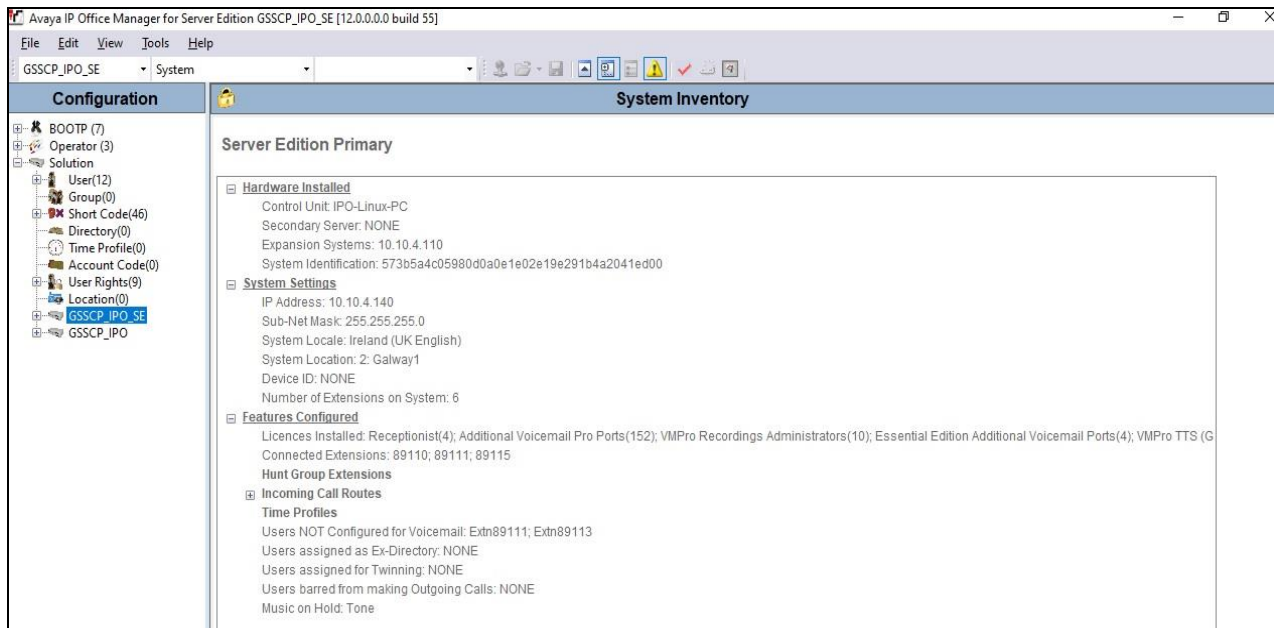
Note – Testing was performed with IP Office Server Edition with 500 V2 Expansion R12.0. Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with all configurations of IP Office Server Edition. **Note:** that IP Office Server Edition requires an Expansion IP Office 500 V2 to support analog or digital endpoints or trunks, this includes T.38 fax.

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Keyyo SIP platform. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Navigate to **File → Open Configuration**, select the appropriate Avaya IP Office system from the pop-up window and log in with the appropriate credentials.



A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration. All licensing and feature configuration that is not directly related to the interface with the Service Provider is assumed to already be in place.



5.1. Verify System Capacity

Navigate to **License** in the Navigation Pane. In the Details Pane verify that the **License Status** for **SIP Trunk Channels** is Valid and that the number of **Instances** is sufficient to support the number of SIP trunk channels provisioned by Keyyo.

Licence Remote Server					
Licence Mode		Licence Normal			
Licensed Version		12.0			
PLDS Host ID		338645006189			
PLDS File Status		Valid			
Feature	Instances	Status	Expiry Date	Source	
Receptionist	4	Valid	Never	PLDS Nodal	
Additional Voicemail Pro Ports	152	Valid	Never	PLDS Nodal	
VMPro Recordings Administrators	10	Valid	Never	PLDS Nodal	
Essential Edition Additional Voice...	4	Obsolete	Never	PLDS Nodal	
VMPro TTS (Generic)	40	Obsolete	Never	PLDS Nodal	
Teleworker	384	Obsolete	Never	PLDS Nodal	
Mobile Worker	384	Obsolete	Never	PLDS Nodal	
Office Worker	384	Valid	Never	PLDS Nodal	
Avaya Softphone Licence	100	Valid	Never	PLDS Nodal	
VMPro TTS (Scansoft)	40	Obsolete	Never	PLDS Nodal	
VMPro TTS Professional	40	Valid	Never	PLDS Nodal	
IPSec Tunnelling	10	Obsolete	Never	PLDS Nodal	
Power User	384	Valid	Never	PLDS Nodal	
Customer Service Agent	5	Dormant	Never	PLDS Nodal	
Customer Service Supervisor	5	Dormant	Never	PLDS Nodal	
Avaya IP endpoints	384	Valid	Never	PLDS Nodal	
IP500 Voice Networking Channels	32	Obsolete	Never	PLDS Nodal	
SIP Trunk Channels	300	Valid	Never	PLDS Nodal	
IP500 Universal PRI (Additional cha...	100	Obsolete	Never	PLDS Nodal	
CTI Link Pro	10	Valid	Never	PLDS Nodal	
Wave User	16	Obsolete	Never	PLDS Nodal	
3rd Party IP Endpoints	384	Valid	Never	PLDS Nodal	
Centralized Endpoints	10	Obsolete	Never	PLDS Nodal	

5.2. LAN2 Settings

In an Avaya IP Office, the LAN2 tab settings correspond to the Avaya IP Office WAN port (public network side) and the LAN1 tab settings correspond to the LAN port (private network side).

In the test configuration, the LAN2 port was used to connect the Avaya IP Office to the external internet. To access the LAN2 settings, first navigate to **System** → **GSSCP_IPO_SE** in the Navigation Pane where GSSCP_IPO_SE is the name of the IP Office. Navigate to the **LAN2** → **LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the public interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

The screenshot shows the configuration interface for the GSSCP_IPO_SE system. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, and VoIP. The LAN2 tab is selected, and the LAN Settings sub-tab is active. The IP Address field is set to 192 . 168 . 122 . 46, and the IP Mask field is set to 255 . 255 . 255 . 0. The Number Of DHCP IP Addresses is set to 200. The DHCP Mode is set to Disabled, with radio buttons for Server, Client, and Disabled. An Advanced button is visible at the bottom right.

On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If Avaya Communicator along with any other SIP endpoint is to be used, the **SIP Registrar Enable** box must also be checked. The **Domain Name** has been set to the customer premises equipment domain “**avaya.com**”. If the **Domain Name** is left at the default blank setting, SIP registrations may use the IP Office LAN2 IP Address. All other parameters shown are default values.

The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. Set **Scope** to **RTP-RTCP** and **Initial keepalives** to **Enabled** and **Periodic timeout** to **30**.

Avaya IP Office can also be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for both signalling and media. The **DSCP** field is the value used for media and the **SIG DSCP** is the value used for signalling. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).

The screenshot displays the configuration page for **GSSCP_IPO_SE*** in the Avaya IP Office management console. The interface is divided into several sections:

- System Navigation:** Includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The **VoIP** section is active, with sub-tabs for LAN Settings, VoIP, and Network Topology.
- H323 Gatekeeper Settings:**
 - H323 Gatekeeper Enable
 - Auto-create Extn Auto-create User H323 Remote Extn Enable
 - H.323 Signalling over TLS: Disabled
 - Remote Call Signalling Port: 1720
- SIP Trunks and Registrar Settings:**
 - SIP Trunks Enable
 - SIP Registrar Enable
 - Auto-create Extn/User SIP Remote Extn Enable
 - Allowed SIP User Agents: Block blacklist only
 - SIP Domain Name: avaya.com
 - SIP Registrar FQDN: avaya.com
- Layer 4 Protocol Settings:**
 - UDP: UDP Port 5060, Remote UDP Port 5060
 - TCP: TCP Port 5060, Remote TCP Port 5060
 - TLS: TLS Port 5061, Remote TLS Port 5061
- Challenge Expiry Time (secs):** 10
- RTP Settings:**
 - Port Number Range: Minimum 49152, Maximum 53246
 - Port Number Range (NAT): Minimum 49152, Maximum 53246
 - Enable RTCP Monitoring on Port 5005
 - RTCP collector IP address for phones: 0 . 0 . 0 . 0
 - Keepsalives:
 - Scope: RTP-RTCP
 - Periodic timeout: 30
 - Initial keepsalives: Enabled
- DiffServ Settings:**
 - DSCP (Hex): B8, Video DSCP (Hex): B8, DSCP Mask (Hex): FC, SIG DSCP (Hex): 88
 - DSCP: 46, Video DSCP: 46, DSCP Mask: 63, SIG DSCP: 34

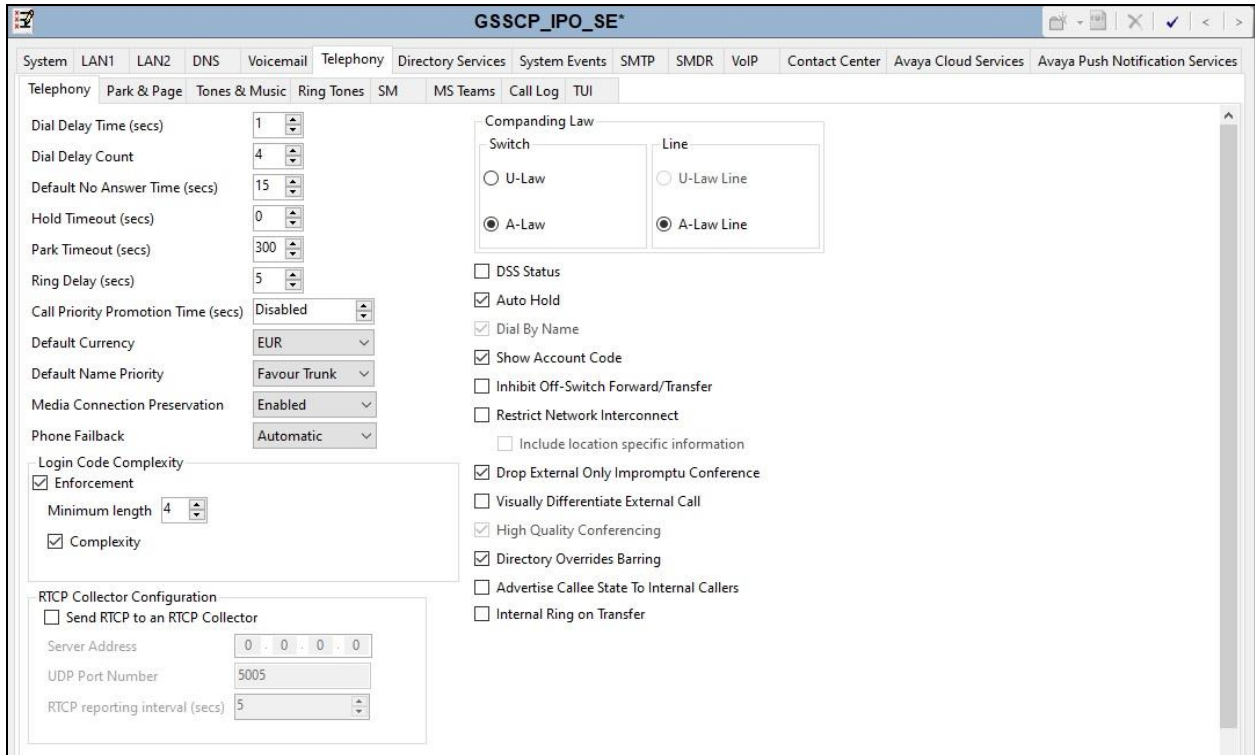
On the **Network Topology** tab, set the **Firewall/NAT Type** from the pulldown menu to **Open Internet**. With this configuration, the **STUN Server IP Address** and **STUN Port** are not used as NAT was not required for this configuration, therefore resulting in no requirement for a STUN server. The **Use Network Topology Info** in the **SIP Line** was set to **None** in **Section 5.5.2**. Set **Binding Refresh Time (seconds)** to **300**. This value is used to determine the frequency at which Avaya IP Office will send SIP OPTIONS messages to the service provider. Default values were used for all other parameters. On completion, click the **OK** button (not shown).

The screenshot shows the configuration window for GSSCP_IPO_SE*. The window has a title bar with the text "GSSCP_IPO_SE*" and a standard window icon. Below the title bar is a navigation menu with tabs for "System", "LAN1", "LAN2", "DNS", "Voicemail", "Telephony", "Directory Services", "System Events", "SMTP", "SMDR", "VoIP", "Contact Center", and "Avaya Cloud Services". The "VoIP" tab is selected, and within it, the "Network Topology" sub-tab is active. The main content area is titled "Network Topology Discovery" and contains the following fields and controls:

- STUN Server Address:** An empty text input field.
- STUN Port:** A numeric spinner set to 3478.
- Firewall/NAT Type:** A dropdown menu currently showing "Open Internet".
- Binding Refresh Time (seconds):** A numeric spinner set to 300.
- Public IP Address:** A field containing "0 . 0 . 0 . 0".
- Run STUN / Cancel:** Two buttons located to the right of the Public IP Address field.
- Public Port:** A section with three sub-fields: "UDP" (0), "TCP" (0), and "TLS" (0), each with a numeric spinner.
- Run STUN on startup:** A checkbox that is currently unchecked.

5.3. System Telephony Settings

Navigate to the **Telephony** → **Telephony** tab on the Details Pane. Choose the **Companding Law** typical for the enterprise location. For Europe, **ALAW** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfer to the PSTN via the Service Provider across the SIP trunk. On completion, click the **OK** button (not shown).



5.4. VoIP Settings

Navigate to the **VoIP** tab on the Details Pane. Check the available Codecs boxes as required. Note that **G.711 ULAW 64K** and **G.711 ALAW 64K** are greyed out and always available. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.711 ALAW 64K**, **G.729(a)8K CS-ACELP** and **G.722 64K** are the codecs's supported on the Keyyo SIP Trunk. The order of priority can be changed using the vertical arrows. On completion, click the **OK** button (not shown).

GSSCP_IPO_SE

System LAN1 LAN2 DNS Voicemail Telephony Directory Services System Events SMTP SMDR VoIP

VoIP VoIP Security Access Control Lists

Ignore DTMF Mismatch For Phones

Allow Direct Media Within NAT Location

Disable Direct Media For Simultaneous Clients

RFC2833 Default Payload 101

OPUS Default Payload 116

Available Codecs

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.722 64K
- G.729(a) 8K CS-AC
- OPUS

Default Codec Selection

Unused

- G.711 ULAW 64K

Selected

- G.711 ALAW 64K
- G.729(a) 8K CS-A
- G.722 64K

5.5. SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and the Keyyo SIP platform. The recommended method for configuring a SIP Line is to use the template associated with these Application Notes. The template is an .xml file that can be used by IP Office Manager to create a SIP Line. Follow the steps in **Section 5.5.1** to create the SIP Line from the template.

Some items relevant to a specific customer environment are not included in the template or may need to be updated after the SIP Line is created. Examples include the following:

- IP addresses
- SIP Credentials (if applicable)
- SIP URI entries
- Setting of the **Use Network Topology Info** field on the Transport tab

Therefore, it is important that the SIP Line configuration be reviewed and updated if necessary after the SIP Line is created via the template. The resulting SIP Line data can be verified against the manual configuration shown in **Section 5.5.2**.

Also, the following SIP Line settings are not supported on Basic Edition:

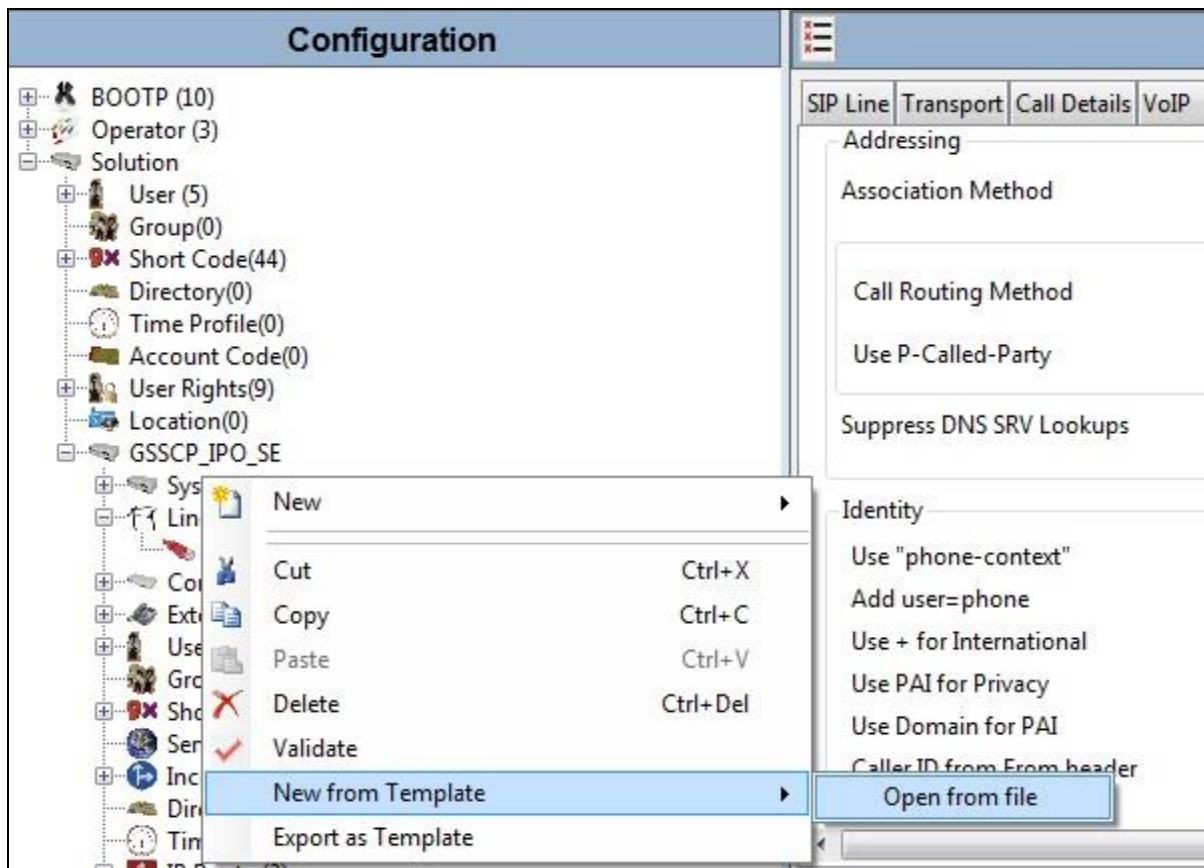
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

Alternatively, a SIP Line can be created manually. To do so, right-click **Line** in the Navigation Pane and select **New → SIP Line**. Then, follow the steps outlined in **Section 5.5.2**.

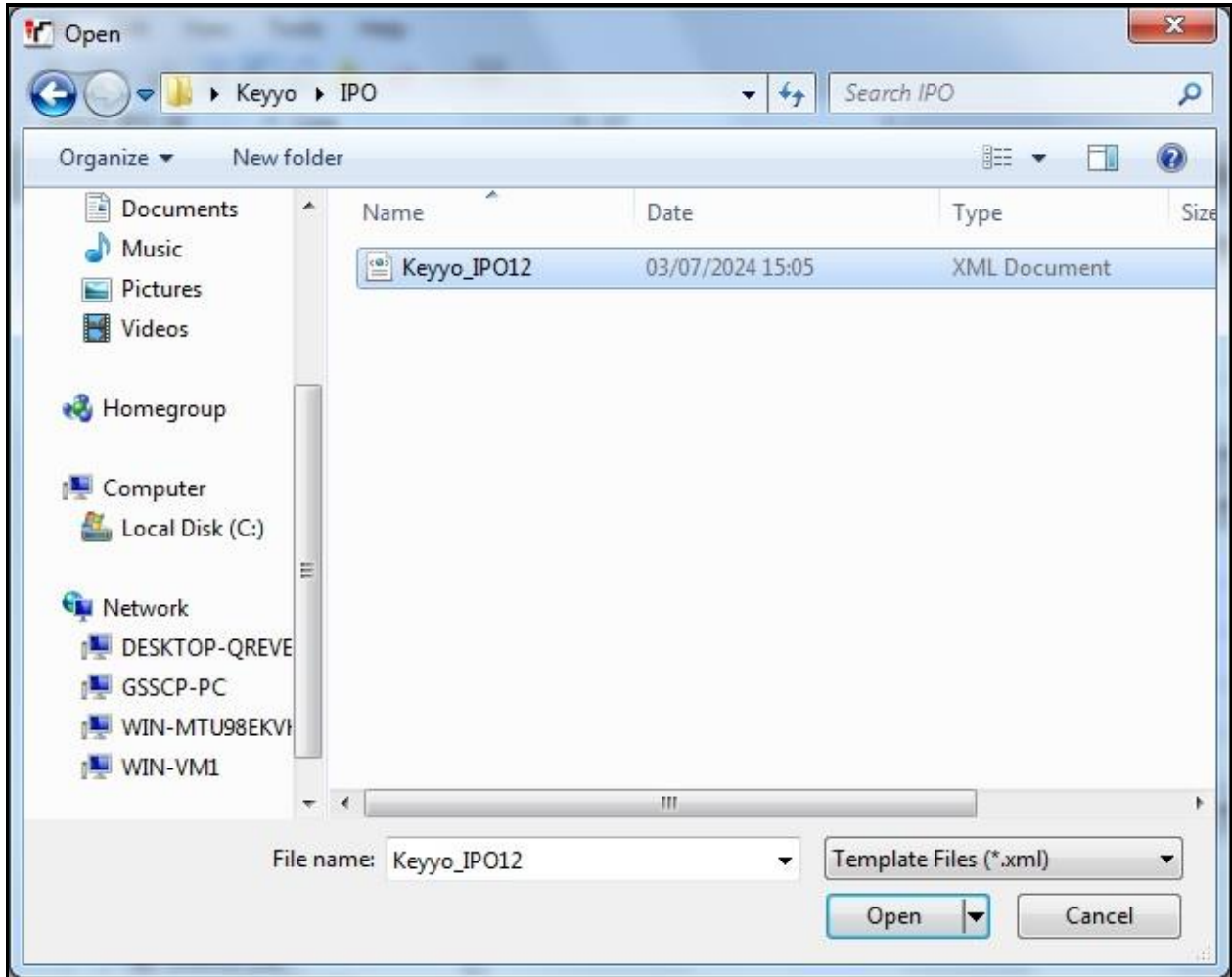
5.5.1. SIP Line From Template

DevConnect generated SIP Line templates are always exported in an XML format. These XML templates do not include sensitive customer specific information and are therefore suitable for distribution. The XML format templates can be used to create SIP trunks on both IP Office Standard Edition (500 V2) and IP Office Server Edition systems. Alternatively, binary templates may be generated. However, binary templates include all the configuration parameters of the Trunk, including sensitive customer specific information. Therefore, binary templates should only be used for cloning trunks within a specific customer's environment.

Copy a previously created template file to a location (e.g., *temp*) on the same computer where IP Office Manager is installed. To create the SIP Trunk from the template, right-click on **Line** in the Navigation Pane, then navigate to **New** → **New from Template**.



Navigate to the directory on the local machine where the template was copied and select the template as required.



The SIP Line is automatically created and can be verified and edited as required using the configuration described in **Section 5.5.2**.

5.5.2. Manual SIP Line Configuration

On the **SIP Line** tab in the Details Pane, configure the parameters below to connect to the SIP Trunking service.

- Set **ITSP Domain Name** to a domain name provider by the Service Provider if required, **keyyo.net** was used in this configuration.
- Set **National Prefix** to 0 and **International Prefix** to 00 so that national and international numbers can be correctly identified.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Leave the **Refresh Method** at the default value of **Auto** which results in re-INVITE being used for Session Refresh.
- Leave **Timer (seconds)** at the default value of **On Demand**. This value allows the Session Refresh interval to be set by the network.
- Set **Incoming Supervised REFER** and **Outgoing Supervise REFER** to **Auto**.
- Default values may be used for all other parameters.

On completion, click the **OK** button (not shown).

The screenshot shows the 'SIP Line - Line 17*' configuration window. The 'SIP Line' tab is selected, and the 'SIP Credentials' sub-tab is active. The configuration is as follows:

Field	Value	Field	Value
Line Number	17	In Service	<input checked="" type="checkbox"/>
ITSP Domain Name	keyyo.net	Check OOS	<input checked="" type="checkbox"/>
Local Domain Name			
URI Type	SIP URI	Session Timers	
Location	Cloud	Refresh Method	Auto
Prefix		Timer (seconds)	On Demand
National Prefix	0		
International Prefix	00		
Country Code		Redirect and Transfer	
Name Priority	System Default	Incoming Supervised REFER	Auto
Description		Outgoing Supervised REFER	Auto
		Send 302 Moved Temporarily	<input checked="" type="checkbox"/>
		Outgoing Blind REFER	<input checked="" type="checkbox"/>

Select the **Transport** tab and set the following:

- Leave **ITSP Proxy Address** blank.
- Set **Use Network Topology Info** to **None** as NAT is not used in this configuration and the Network Topology settings defined in **Section 5.2** are not required.
- Set **Layer 4 Protocol** to **UDP**.
- Set **Send Port** and **Listen Port** to **5060**.

On completion, click the OK button (not shown).

The screenshot shows the configuration window for 'SIP Line - Line 17*'. The 'Transport' tab is selected. The 'ITSP Proxy Address' field is empty. Under 'Network Configuration', 'Layer 4 Protocol' is set to 'UDP', 'Send Port' is 5060, 'Use Network Topology Info' is set to 'None', and 'Listen Port' is 5060. 'Explicit DNS Server(s)' are both set to '0 . 0 . 0 . 0'. 'Calls Route via Registrar' is checked. 'Separate Registrar' is empty.

After the SIP line parameters are defined, the SIP credentials used for registration and authorisation on this line must be created. To define SIP credentials, first select the **SIP Credentials** tab. Click the **Add** button and the **New SIP Credentials** area will appear at the bottom of the pane.

The screenshot shows the 'SIP Credentials' tab selected. A table with columns 'Index', 'UserName', 'Authentication Name', 'Contact', 'Expiry (mins)', and 'Register' is visible. To the right of the table are three buttons: 'Add...', 'Remove', and 'Edit...'.

Enter the registration credentials provided by Keyyo as shown below. Click the **OK** button.

SIP Line - Line 17*

SIP Line | Transport | Call Details | VoIP | **SIP Credentials** | SIP Advanced | Engineering

Edit...

Edit SIP Credentials

User name: 331xxxxc16

Authentication Name: 331xxxxd16

Contact: 331xxxxd16

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Expiry (mins): 60

Registration required:

OK

Cancel

After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, select the **Call Details** tab and click on **Add**.

SIP Line - Line 17*

SIP Line | Transport | **Call Details** | VoIP | SIP Credentials | SIP Advanced | Engineering

SIP URIs

URI	Groups	Credential	Local URI	Contact	P Asserted ID	P Preferred ID	Diversion Header	Remote Party ID
-----	--------	------------	-----------	---------	---------------	----------------	------------------	-----------------

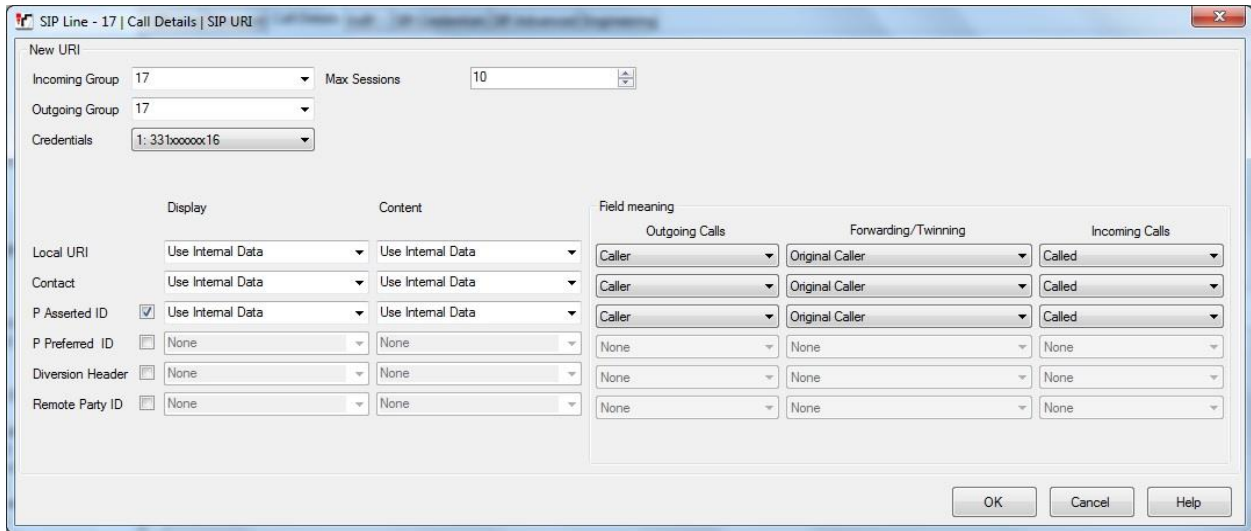
Add...

Remove

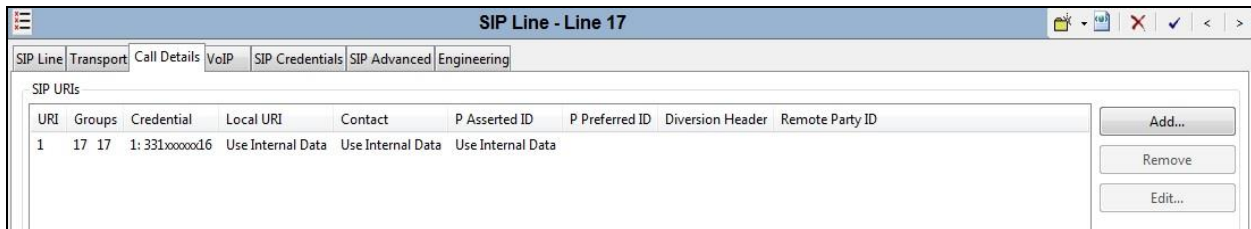
Edit...

For the compliance test, SIP URI entries were created that matched any number assigned to an Avaya IP Office user. The entry was created with the parameters shown below.

- Set **Incoming Group**. This is the value assigned for incoming calls that's analysed in the Incoming Call Route settings described in **Section 5.8**. In the test environment a value of **17** was used for the Keyyo SIP platform.
- Set **Outgoing Group**. This is the value assigned for outgoing calls that can be selected directly in the short code settings described in **Section 5.6**. In the test environment a value of **17** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- For **Credentials**, select **1: <033xxxxxx98>** from the pull-down menu since this configuration uses SIP registration
- Set **Local URI**, **Contact** and **P Asserted ID** to **Use Internal Data** for both the **Display** name and **Content**. On incoming calls, this will analyse the Request-Line sent by Keyyo and match to the SIP settings in the User profile as described in **Section 5.7**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Leave the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective default values of **Caller**, **Original Caller** and **Called** for the **Local URI**, **Contact** and **P Asserted ID** call details.



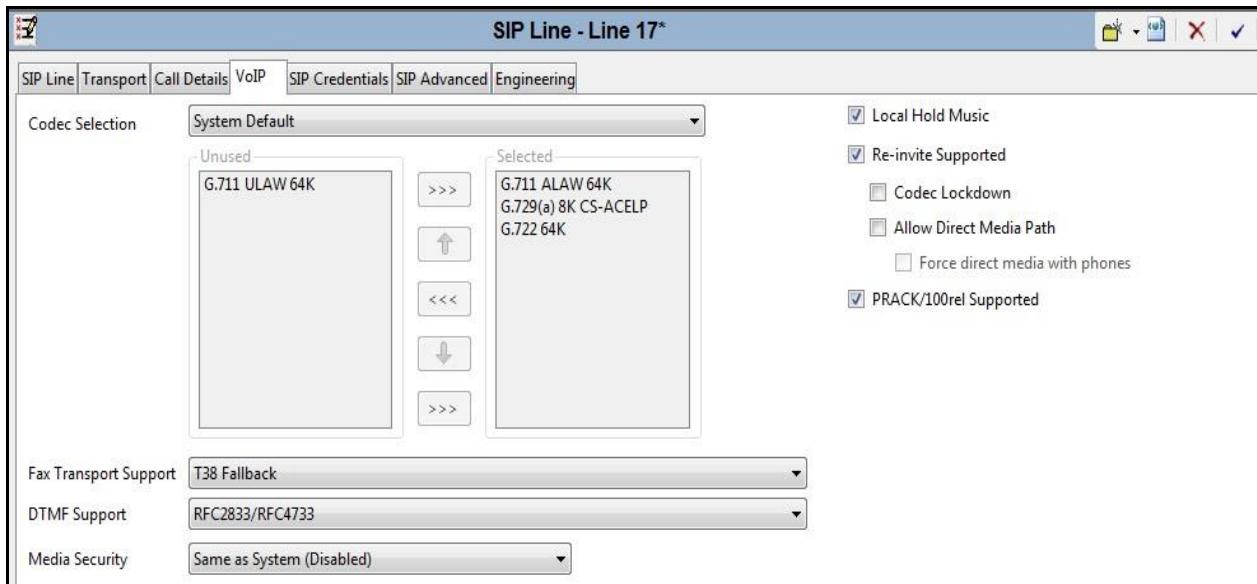
The following screenshot shows the completed configuration:



Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- Select **System Default** from the drop-down menu as system default codecs were already defined in **Section 5.4**.
- Set the **Fax Transport Support** box to **T38 Fallback** as this is the preferred method of fax transmission for Keyyo.
- Set the **DTMF Support** field to **RFC2833/RFC4733**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Set **Media Security** field to **Same as System (Disabled)**.
- Check the **Local Hold Music** box.
- Check the **Re-invite Supported** box to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated.
- Check the **PRACK/100rel Supported** box if early media is required. This was checked during compliance testing.
- On completion, click the **OK** button (not shown).

Default values may be used for all other parameters.



Select the **SIP Advanced** tab and set the following:

- Check the **Use + for International** as E.164 numbering is used on the SIP Trunk.
- Default values may be used for all other parameters.

The screenshot shows the configuration window for 'SIP Line - Line 17*'. The 'SIP Advanced' tab is selected. The configuration is organized into several sections:

- Addressing:** Association Method is set to 'By Source IP address'. Call Routing Method is 'Request URI'. 'Use P-Called-Party' and 'Suppress DNS SRV Lookups' are unchecked.
- Identity:** 'Use + for International' is checked. Other options like 'Use "phone-context"', 'Add user=phone', 'Use PAI for Privacy', 'Use Domain for PAI', 'Caller ID from From header', 'Send From In Clear', 'Cache Auth Credentials', 'User-Agent and Server Headers', 'Send Location Info', 'Add UUI header', and 'Add UUI header to redirected calls' are unchecked.
- Media:** 'Allow Empty INVITE', 'Send Empty re-INVITE', 'Allow To Tag Change', 'Send SilenceSupp=Off', 'Force Early Direct', 'Media Connection Preservation', 'Indicate HOLD', and 'Media Security' are unchecked. 'P-Early-Media Support' is set to 'None' and 'Media Connection Preservation' is set to 'Disabled'.
- Call Control:** 'Call Initiation Timeout (s)' is 4, 'Call Queuing Timeout (m)' is 5. 'Service Busy Response' is '503 - Service Unavailable', 'on No User Responding Send' is '408-Request Timeout', and 'Action on CAC Location Limit' is 'Allow Voicemail'. 'Suppress Q,850 Reason Header', 'Emulate NOTIFY for REFER', and 'No REFER if using Diversion' are unchecked.
- Other:** 'Calling Number Verification' is unchecked. 'Incoming Calls Handling' is set to 'System'.

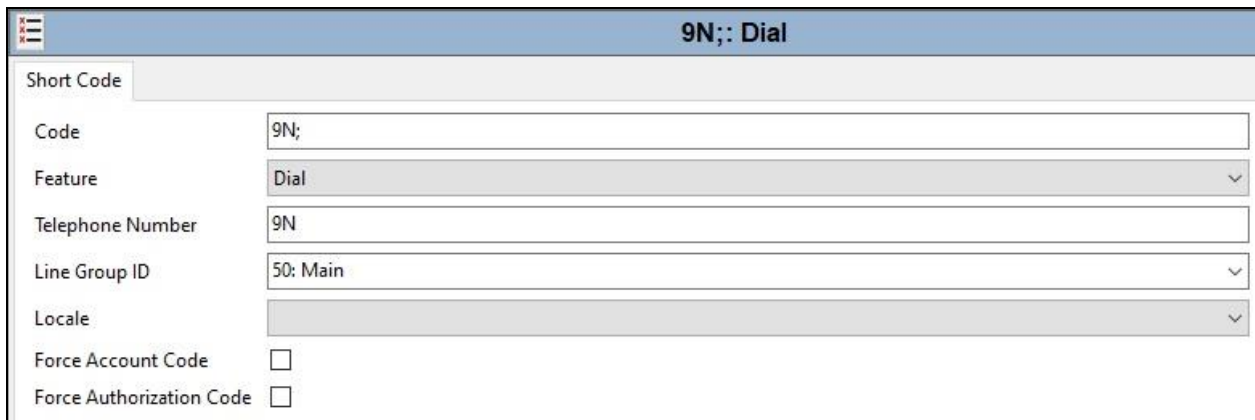
Note: It is advisable at this stage to save the configuration as described in **Section 5.11** to make the Line Group ID defined in **Section 5.5.2** available.

5.6. Short Codes

Define a short code to route outbound traffic to the SIP line. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as required. The example below shows the configuration used during testing for national numbers.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon.
- The example shows **9N**; which will be invoked when the user dials 9 followed by a public number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to **9N** so that the call is passed to the ARS function with the dialled number unchanged.
- Set the **Line Group Id** to the ARS route number described in **Section 5.9**.
- On completion, click the **OK** button (not shown).

On completion, click the **OK** button (not shown).



The screenshot displays a configuration window titled "9N;: Dial". The window contains a "Short Code" tab and several input fields:

Code	9N;
Feature	Dial
Telephone Number	9N
Line Group ID	50: Main
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

5.7. User

Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5.2**. To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

The following example shows the configuration required for a SIP Endpoint.

- Change the **Name** of the User if required.
- Set the **Password** and **Confirm Password**.
- Select the required profile from the **Profile** drop down menu. **Basic User** is commonly used; **Power User** can be selected for SIP softphone, WebRTC and Remote Worker endpoints.

The screenshot displays the configuration page for a user named 'Ext89110: 89110'. The page is divided into several tabs: User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, Voice Recording, and Button Programming. The 'User' tab is active, showing the following configuration fields:

- Name: Ext89110
- Password: [Redacted]
- Confirm Password: [Redacted]
- Unique Identity: [Empty]
- Audio Conference PIN: [Empty]
- Confirm Audio Conference PIN: [Empty]
- Account Status: Enabled
- Full Name: Ext89110
- Extension: 89110
- Email Address: [Empty]
- Locale: [Empty]
- Priority: 5
- System Phone Rights: None
- Profile: Basic User

Below the Profile dropdown, there are several checkboxes for additional features:

- Receptionist
- Enable Softphone
- Enable one-X Portal Services
- Enable one-X TeleCommuter
- Enable Remote Worker
- Enable Desktop/Tablet VoIP client
- Enable Mobile VoIP Client
- Enable MS Teams Client
- Send Mobility Email
- Web Collaboration

SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**.

Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right-hand side of the Details Pane until it becomes visible. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.5.2**). As such, these fields should be set to one of the DDI numbers assigned to the enterprise from Keyyo.

The screenshot shows the configuration for Ext89110: 89110. The SIP tab is selected. The fields are as follows:

SIP Name	33xxxxxx38
SIP Display Name (Alias)	33xxxxxx38
Contact	33xxxxxx38
Anonymous	<input type="checkbox"/>

Note: The **Anonymous** box can be used to restrict Calling Line Identity (CLIR).

The following screen shows the Mobility tab for user 89110. The **Mobility Features** and **Mobile Twinning** are checked. The **Twinned Mobile Number** field is configured with the number to dial to reach the twinned mobile telephone over the SIP Trunk. Other options can be set accordingly to customer requirements.

The screenshot shows the configuration for Ext89110: 89110. The Mobility tab is selected. The configuration is as follows:

- Simultaneous Coverage Delay (secs): 0
- MS Teams URI: (empty)
- Internal Twinning:
 - Twinned Handset: <None>
 - Maximum Number of Calls: 1
 - Twin Bridge Appearances:
 - Twin Coverage Appearances:
 - Twin Line Appearances:
- Mobility Features:
 - Mobile Twinning:
 - Twinned Mobile Number (including dial access code): 900353xxxxxx52
 - Twinning Time Profile: <None>
 - Mobile Dial Delay (secs): 3
 - Mobile Answer Guard (secs): 0
 - Hunt group calls eligible for mobile twinning:
 - Forwarded calls eligible for mobile twinning:
 - Twin When Logged Out:
 - Fallback Twinning:
 - one-X Mobile Client:
 - Mobile Call Control:
 - Mobile Callback:

5.8. Incoming Call Routing

An incoming call route maps an inbound DDI number on a specific line to an internal extension. To create an incoming call route, right-click **Incoming Call Routes** in the Navigation Pane and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capability** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.5.2**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.

The screenshot shows the configuration form for an incoming call route. The title bar displays '17 33xxxxxxxx38'. The 'Standard' tab is selected. The form contains the following fields:

Bearer Capability	Any Voice
Line Group ID	17
Incoming Number	33xxxxxxxx38
Incoming Sub Address	
Incoming CLI	
Locale	
Priority	1 - Low
Tag	
Hold Music Source	System Source
Ring Tone Override	None

On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DDI number **33xxxxxxxx38** on line 17 are routed to extension 89110.

The screenshot shows the 'Destinations' tab of the configuration form. The title bar displays '17 33xxxxxxxx38'. The 'Destinations' tab is selected. The form contains the following fields:

TimeProfile	Destination
Default Value	89110 Extn89110

5.9. ARS

The Main ARS route exists by default and requires editing. Select the ARS **Main** route and click on **Add**.

The screenshot shows the configuration for the 'Main' ARS route. The 'ARS Route Id' is 50, 'Route Name' is 'Main', and 'Dial Delay Time' is 'System Default (1)'. The 'Secondary Dial tone' checkbox is unchecked, and 'Check User Call Barring' is checked. The 'Out of Service Route' and 'Out of Hours Route' are both set to '<None>'. The table below lists the following entries:

Code	Telephone Number	Feature	Line Group ID
?	.	Dial	0
086756;	086756	Dial Emergency	17
9N;	N	Dial Emergency	17
90XXXXXXXX	0N	Dial	17
90035391XXXXXX	0035391N	Dial	17

The 'Alternate Route Priority Level' is set to 3, and the 'Alternate Route Wait Time' is 30. The 'Alternate Route' dropdown is set to '<None>'. Buttons for 'Add...', 'Remove', and 'Edit...' are visible on the right side of the table.

Define numbers as required. An example for national numbers is as follows:

- Define the **Short Code**, the example shows a 15 international number with country code and city code prefixed with **9** for an outside line. Note that **X** indicates any digit and **;** causes the system to wait for the full number to be dialled.
- Select **Dial** in the **Feature** drop down menu.
- Define the **Telephone Number** without the **9** which removes it and sends the number as dialled. All **X** characters can be replaced with a single **N**.
- Select the **Line Group ID** defined in the SIP Line URI described in **Section 5.5.2**. During testing this was **17** for the SIP Trunk. Click on **OK**

Edit Short Code

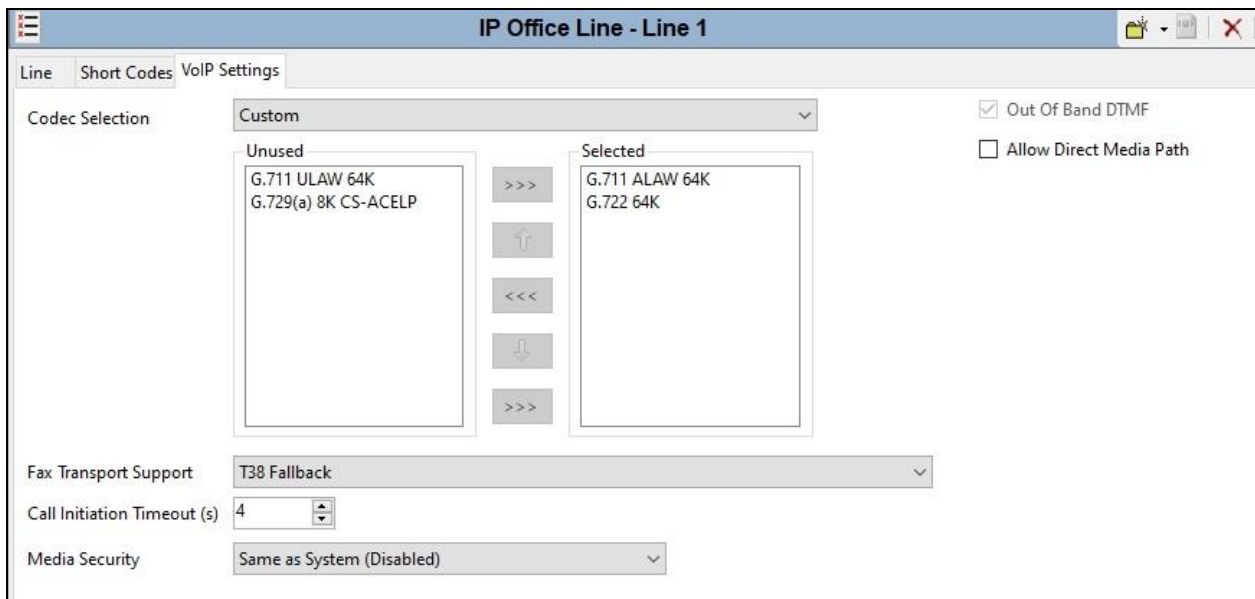
Code	<input type="text" value="90035391XXXXXX"/>	<input type="button" value="OK"/>
Feature	<input type="text" value="Dial"/>	<input type="button" value="Cancel"/>
Telephone Number	<input type="text" value="0035391N"/>	
Line Group ID	<input type="text" value="17"/>	
Locale	<input type="text"/>	
Force Account Code	<input type="checkbox"/>	
Force Authorization Code	<input type="checkbox"/>	

5.10. T38 Fallback Fax Settings

The T38 Fallback Fax settings are defined on the SIP Line between the Expansion and the Server. Note that the VoIP settings for T38 Fallback Fax are required in three places in this configuration:

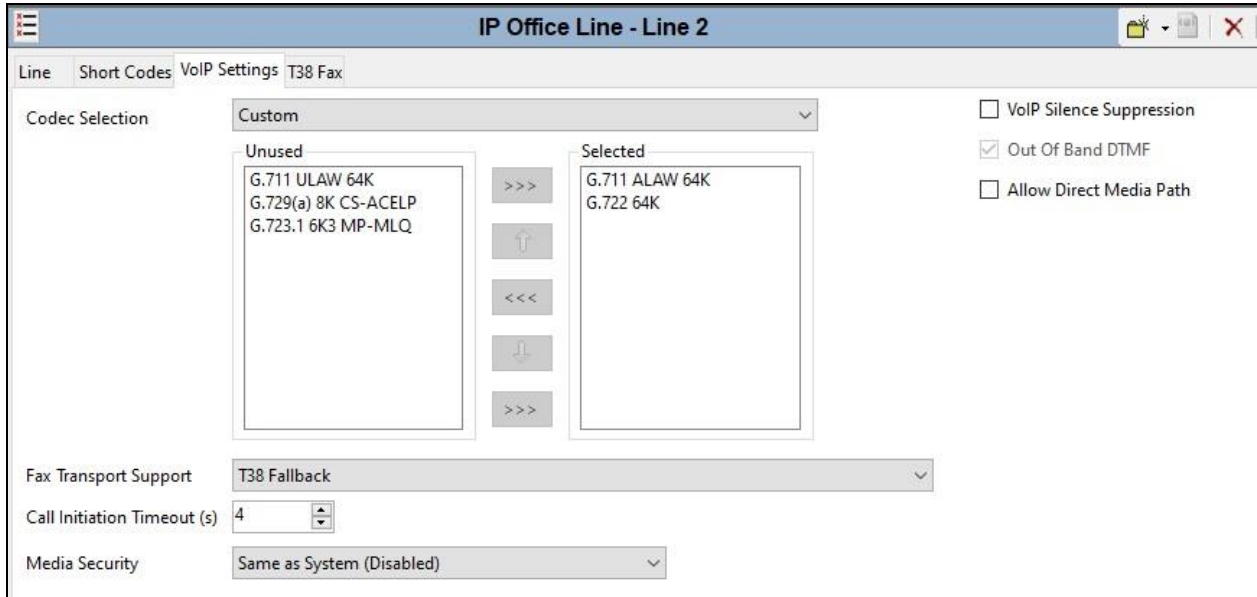
- The SIP Line for the Keyyo SIP Trunk as described in **Section 5.5.2**.
- The IP Office Line between the Server and the Expansion on the Expansion.
- The IP Office Line between the Server and the Expansion on the Server.

In all the above cases, the **Fax Transport Support** was set to **T38 Fallback**. The following screenshot shows the VoIP Settings for the IP Office Line between the Server and the Expansion on the Server configuration:

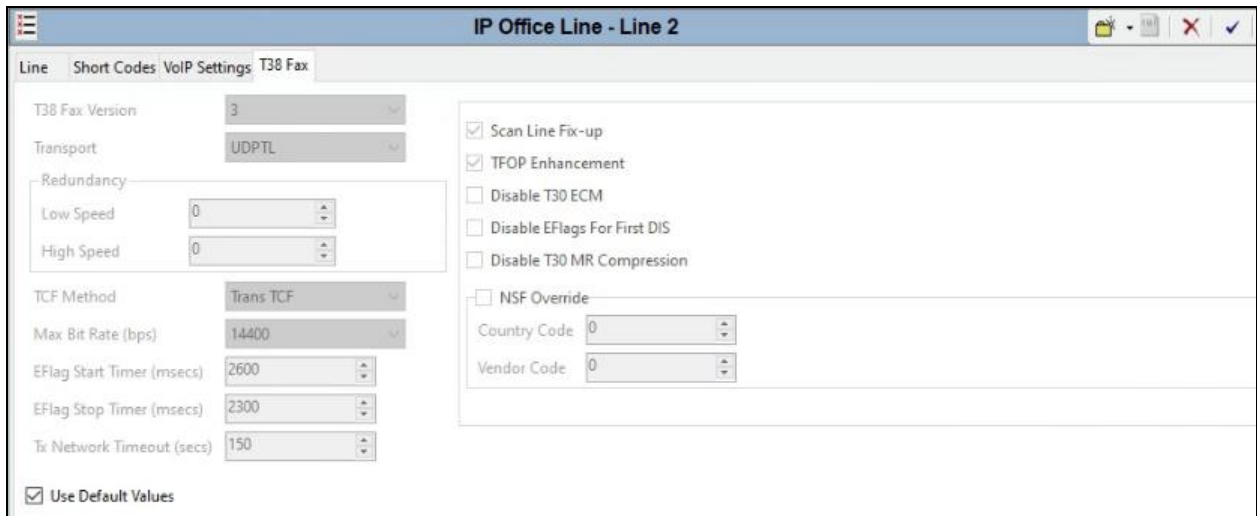


The screenshot displays the configuration interface for 'IP Office Line - Line 1'. The 'VoIP Settings' tab is active. Under 'Codec Selection', a 'Custom' dropdown is shown. Two lists are present: 'Unused' (G.711 ULAW 64K, G.729(a) 8K CS-ACELP) and 'Selected' (G.711 ALAW 64K, G.722 64K). Navigation buttons (>>>, <<<, <-, >+) are between the lists. 'Fax Transport Support' is set to 'T38 Fallback', 'Call Initiation Timeout (s)' is 4, and 'Media Security' is 'Same as System (Disabled)'. Checkboxes for 'Out Of Band DTMF' (checked) and 'Allow Direct Media Path' (unchecked) are on the right.

The following shows the **VoIP Settings** tab in the IP Office Line for the Server in the Expansion configuration:



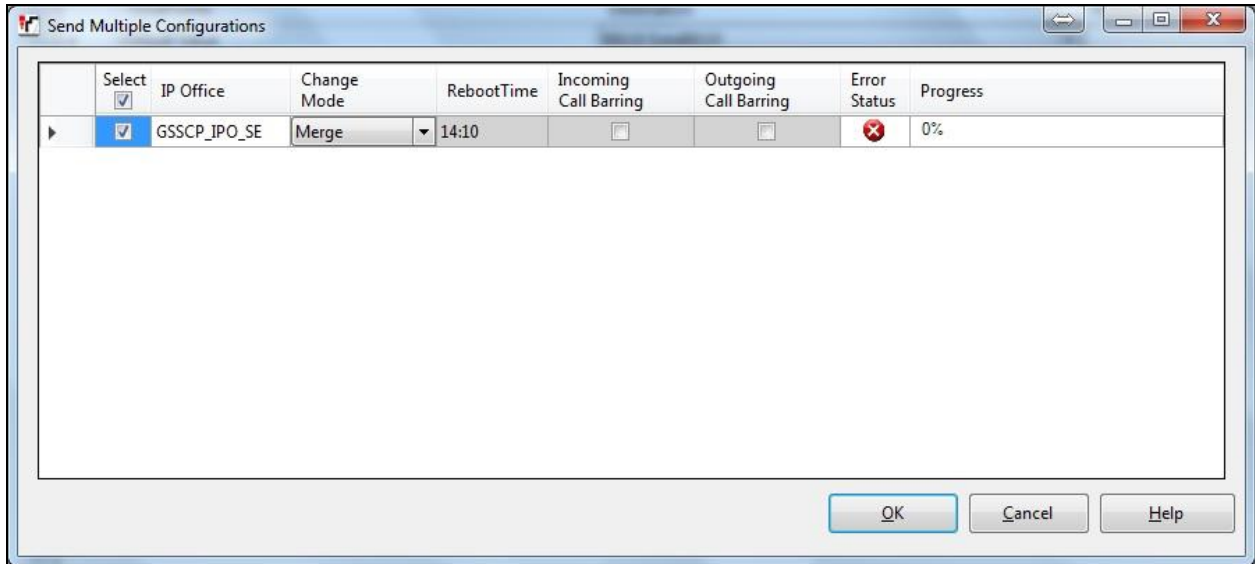
The following shows the T38 Fax tab in the IP Office Line for the Server in the Expansion configuration with **Use Default Values** enabled.



Refer to **Section 5.5.2** for the VoIP Settings on the SIP Line for the Keyyo Premium SIP Trunk

5.11. Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. A screen like the one shown below is displayed where the system configuration has been changed and needs to be saved on the system. **Merge, Reboot, Timed** or **RebootWhen Free** can be selected from the **Change Mode** drop-down menu based on the nature of the configuration changes made since the last save. Note that clicking **OK** may cause a service disruption. Click **OK** to save the configuration.



6. Keyyo SIP Trunk Configuration

The configuration of the Keyyo equipment used to support Keyyo's SIP platform is outside of the scope of these Application Notes and will not be covered. To obtain further information on Keyyo equipment and system configuration please contact an authorized Keyyo representative.

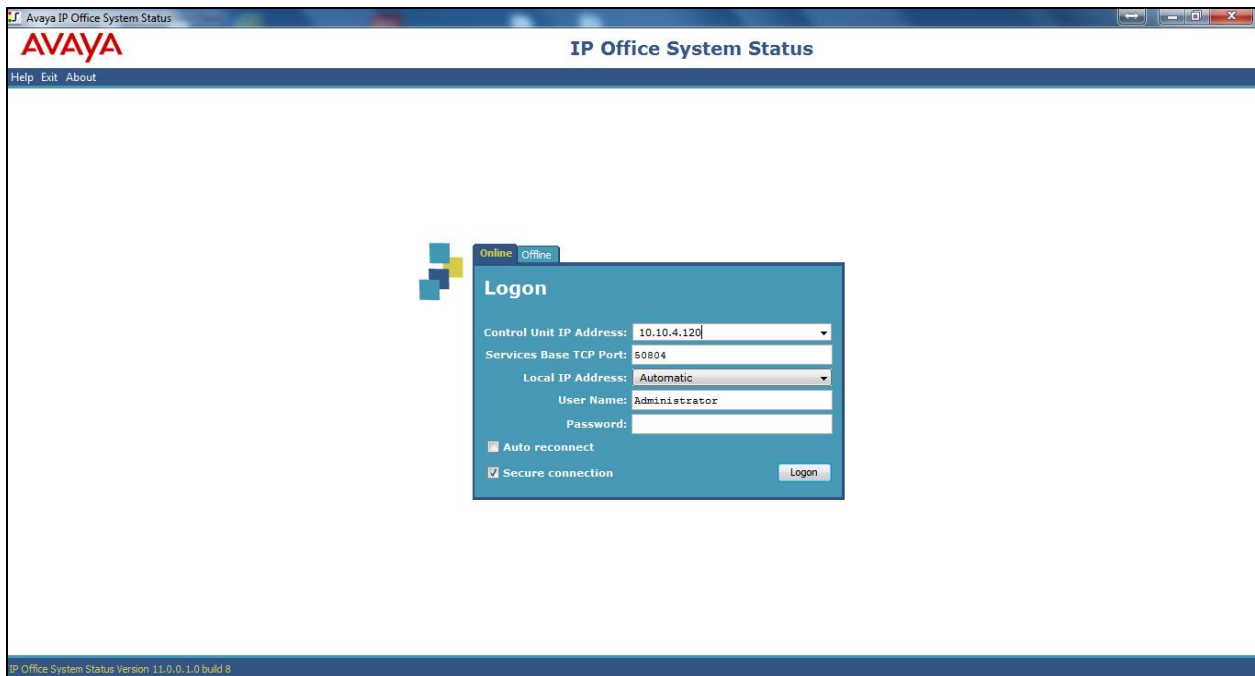
7. Verification Steps

This section includes steps that can be used to verify that the configuration has been done correctly.

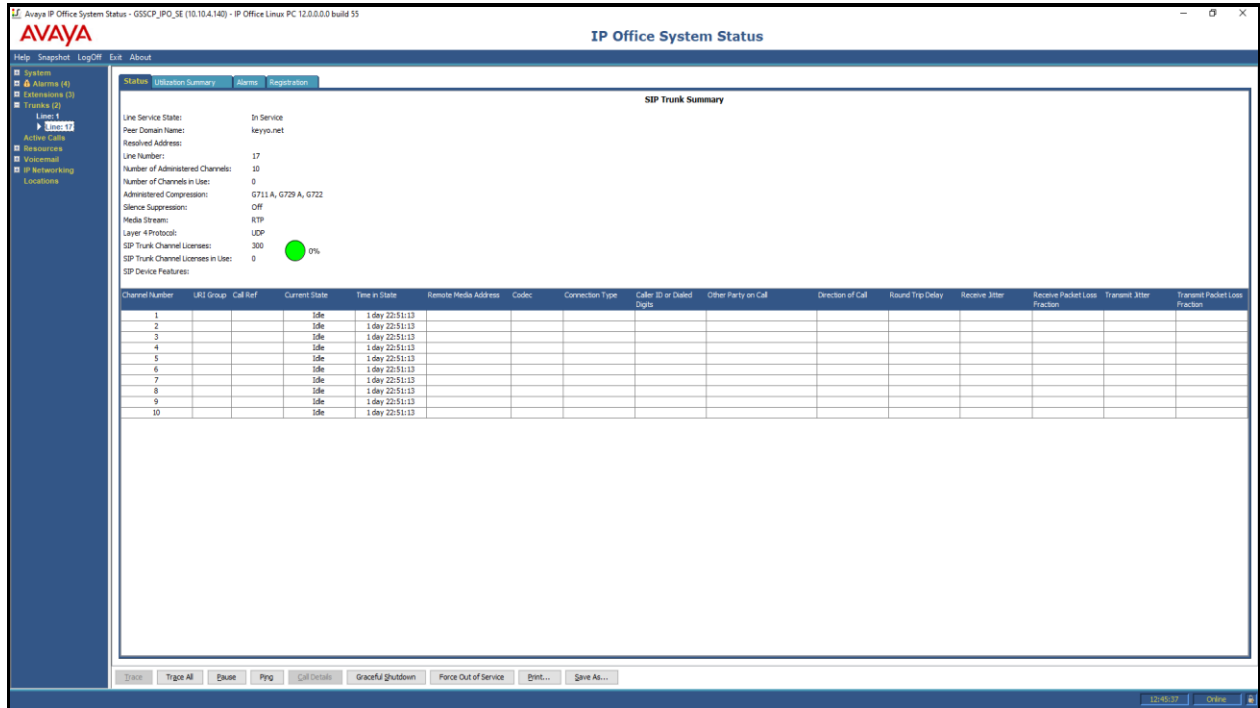
7.1. SIP Trunk status

The status of the SIP trunk can be verified by opening the System Status application. This is found on the PC where IP Office Manager is installed in PC programs under **Start → All Programs → IP Office → System Status** (not shown).

Log in to IP Office System Status at the prompt using the **Control Unit IP Address** for the IP Office. The **User Name** and **Password** are the same as those used for IP Office Manager.

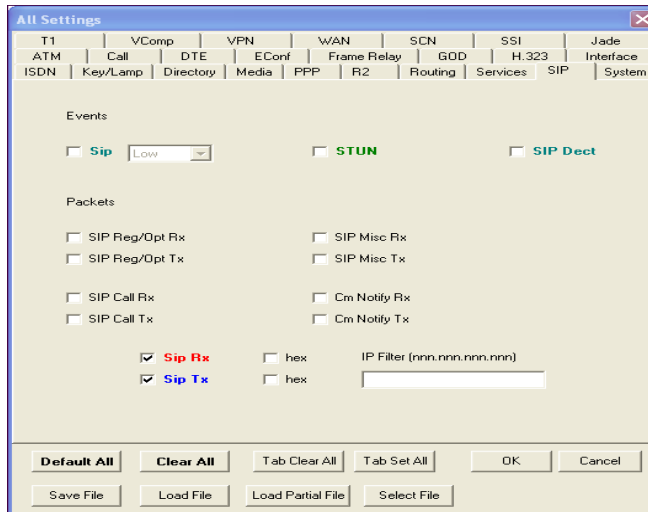


From the left-hand menu expand **Trunks** and choose the SIP trunk (**17** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational.



7.2. Monitor

The Monitor application can also be used to monitor and troubleshoot IP Office. Monitor can be accessed from **Start → Programs → IP Office → Monitor**. The application allows the monitored information to be customized. To customize, select the button that is third from the right in the screen below, or select **Filters → Trace Options**. The following screen shows the **SIP** tab, allowing configuration of SIP monitoring. In this example, the **SIP Rx** and **SIP Tx** boxes are checked. All SIP messages will appear in the trace with the color blue. To customize the color, right-click on **SIP Rx** or **SIP Tx** and select the desired color.



As an example, the following shows a portion of the monitoring window of an OPTIONS message being sent between IP Office and the Service Provider.

```

Avaya IP Office SysMonitor - trying to connect to 10.10.4.140
File Edit View Filters Status Help
13:14:42 170447988mS HTTP: Secure Tx Dest: 10.10.4.140(51284)-(8443)
HTTP/1.1 304 Not Modified
13:14:44 170449572mS Sip: SIP Line (17): Options timer expired
13:14:44 170449572mS Sip: SIP Line (17): OptionsNeededForKeepAlive refer_in_auto 1 refer_out_auto 1 update_auto 1
13:14:44 170449572mS Sip: SIP Line (17): Setting options timer 300 seconds
13:14:44 170449572mS Sip: SIPDialog 20045e50 created, dialogs 2 txn_keys 0 video 1 presentation 1 camera 1 un supp audio 0
13:14:44 170449572mS Sip: (20045e50) SetUnIntTransactionCondition to UnInt_None
13:14:44 170449572mS Sip: (20045e50) OPTIONS SENT TO 83.136.161.72 5060
13:14:44 170449572mS SIP Tx: UDP 86.47.122.56:5060 -> 83.136.161.72:5060
OPTIONS sip:keyyo.net SIP/2.0
Via: SIP/2.0/UDP 86.47.122.56:5060;rport;branch=z9hG4bKbla6a5b5360e710b8498186647b5d5cf
From: <sip:keyyo.net>;tag=6e34a812eab33fde
To: <sip:keyyo.net>
Call-ID: e021abe8d2a93cdd5a19ca49bf590225
CSeq: 926890584 OPTIONS
Contact: <sip:86.47.122.56:5060;transport=udp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer
User-Agent: IP Office 12.0.0.0 build 55
Content-Length: 0

13:14:44 170449604mS SIP Rx: UDP 83.136.161.72:5060 -> 86.47.122.56:5060
SIP/2.0 200 OK
Via: SIP/2.0/UDP 86.47.122.56:5060;received=86.47.122.56;rport=5060;branch=z9hG4bKbla6a5b5360e710b8498186647b5d5cf
From: <sip:keyyo.net>;tag=6e34a812eab33fde
To: <sip:keyyo.net>;tag=a448cb92ee847f7f00df9a03166dc078.ff20
Call-ID: e021abe8d2a93cdd5a19ca49bf590225
CSeq: 926890584 OPTIONS
Accept: */*
Accept-Language: en
Content-Length: 0

```

8. Conclusion

These Application Notes describe the procedures required to configure the connectivity between Avaya IP Office R12.0 and Keyyo SIP Trunk solution as shown in **Figure 1**.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and demonstrates Avaya IP Office R12.0 can be configured to interoperate successfully with Keyyo SIP Trunk. Keyyo SIP Trunk is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

9. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

- [1] *Deploying IP Office as Virtual Servers*, Release 12.0, Apr 2024.
- [2] *Deploying IP Office Server Edition Servers*, Release 12.0, Apr 2024.
- [3] *Deploying an IP500 V2 IP Office System*, Release 12.0, Apr 2024.
- [4] *Administering Avaya IP Office with IP Office Web Manager*, Release 12.0, May 2024.
- [5] *Administering Avaya IP Office with IP Office Manager*, Release 12.0, May 2024.
- [6] *Using Avaya IP Office System Status*, Apr 2024.
- [7] *Using IP Office System Monitor*, Apr 2024.
- [8] *Administrating Voicemail Pro*, Release 12.0, May 2024.
- [9] *Using Avaya Workplace Client for Windows*, Nov 2023.
- [10] *IP Office SIP Phone Installation Notes*, Apr 2024..
- [11] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

2024 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.