Avaya Solution & Interoperability Test Lab

Application Notes for OneAccess-Telstra Business SIP with Avaya IP Office Release 10.1 using SIP Trunking - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of OneAccess-Telstra Business SIP (Australia) with Avaya IP Office Release 10.1 using SIP trunks.

OneAccess-Telstra Business SIP provides PSTN access via a SIP trunk between the enterprise and the OneAccess-Telstra Business SIP as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

OneAccess-Telstra is a member of the Avaya 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 at the OneAccess test lab.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration for Avaya IP Office Release 10.1 with SIP trunks to OneAccess-Telstra Business SIP (Australia).

The enterprise SIP trunking service available from OneAccess-Telstra Business SIP is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. OneAccess-Telstra Business SIP allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

The general test approach was to make calls from/to the Avaya IP Office through the OneAccess NTU using OneAccess-Telstra Business SIP. The configuration (shown in **Figure 1**) was used to exercise the features and functionality tests 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.

For the testing associated with this Application Note, the interface between Avaya systems and OneAccess-Telstra did not include use of any specific encryption features as requested by OneAccess-Telstra.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya IP Office and the OneAccess-Telstra Business SIP.

The testing covered functionality required for compliance as a solution supported by OneAccess-Telstra Business SIP. Calls were made to and from the PSTN across OneAccess-Telstra Business SIP.

The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including H.323, SIP, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, SIP, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya Communicator for Windows.
- Dialing plans including local, long distance, international, outbound toll-free, emergency calls.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.729A, G.711A and G.711MU.
- Fax using pass-through mode.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- Mobile twinning.
- Response to OPTIONS heartbeat and Registration.
- Response to incomplete call attempts and trunk errors.

2.2 Test Results

Interoperability testing of OneAccess-Telstra Business SIP was completed with successful results for all test cases with the exception of the observations/limitations described below.

- **CLI restriction -** CLI restriction is not supported on outbound calls from OneAccess-Telstra Business SIP. It is possible to use the carrier short code of *67, in conjunction with the Avaya IP Office ARS form to achieve the feature. Please see **Section 5.8 Configure Caller Identity Restriction on Outbound Call** for the detailed configuration.
- **Faxing** – OneAccess-Telstra Business SIP service only supports FAX G.711 pass-through mode. G.711 fax pass-through was successfully tested during the compliance test.
- **Direct Media** – Direct Media must be turned off for SIP line on IP Office to Telstra; otherwise, one-way speech path may occur when changing media path mid call.
- **Blind transfer** – Telstra IP Telephone (TIPT) blind transfer Avaya IP Office phone to another Avaya IP Office phone results in no voice and call is disconnected. This issue needs to be investigated from carrier side.

2.3 Support

- For technical support for OneAccess-Telstra SIP Business service, contact Telstra Support at https://www.telstra.com.au/support or call 1800-199-458.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya IP Office Server Edition running on VMware ESXi.
- Avaya IP Office 500 V2.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running H.323 firmware, Avaya 1600 Series IP Telephones running H.323 software, and Avaya 1100 Series IP Telephones running SIP firmware.
- Avaya Communicator for Windows.
- Avaya 2400 Series Digital Telephones.
- OneAccess-Telstra Business SIP provided one trunk group and DID range for this testing is 0285xxx4xx (10 digits). Enterprise network is connected to Telstra network via OneAccess SIP Network Termination Unit (NTU).

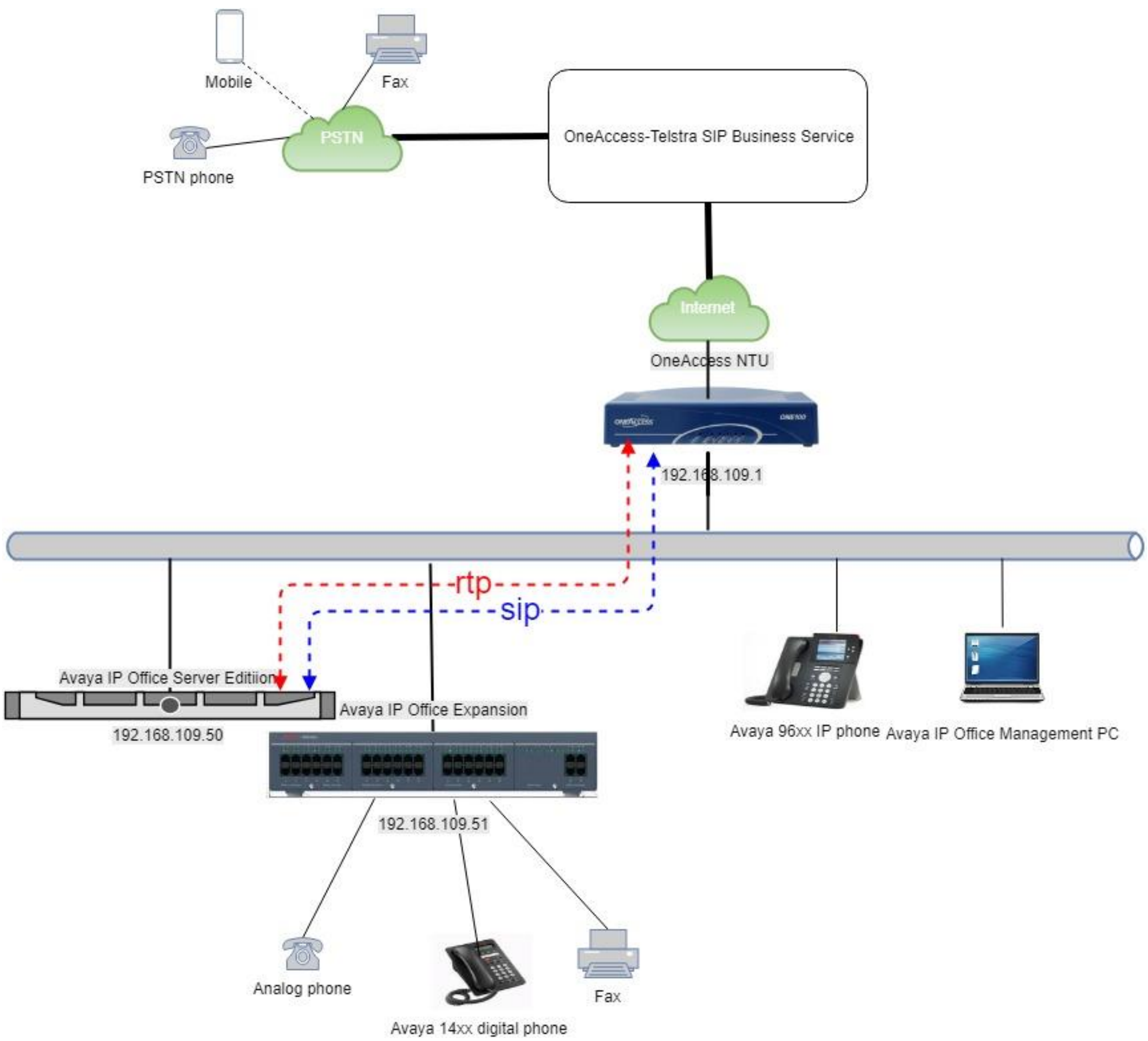


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

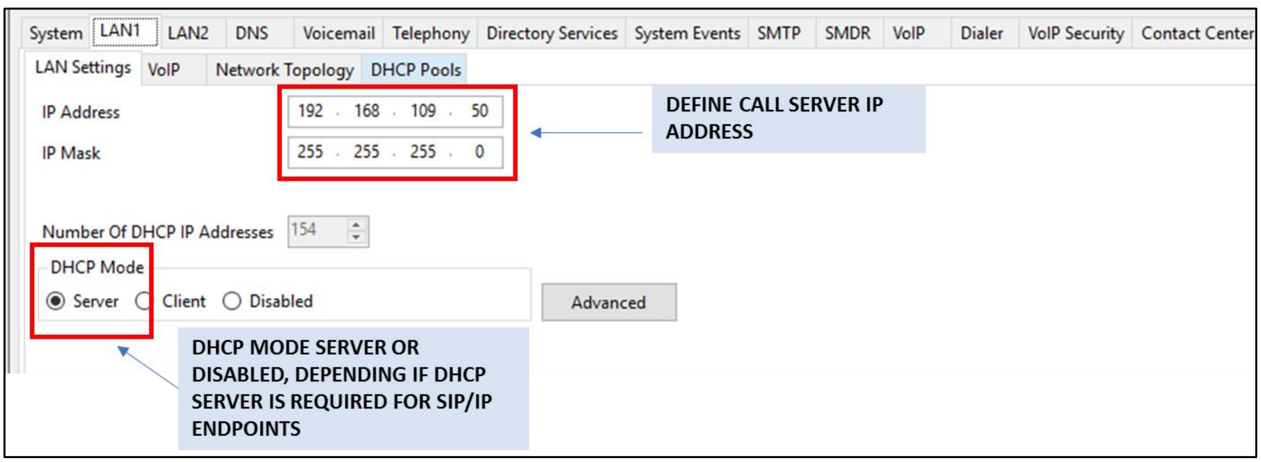
Equipment/Software	Release/Version
Avaya	
Avaya IP Office Server Edition	10.1.0.2.0 build 2
Avaya IP Office Expansion System	10.1.0.2.0 build 2
Avaya 9600 Series IP Deskphones – H.323	6.6.5
Avaya 2400 Series Digital phones	R6
Avaya 1600 Series IP Deskphones, H.323	1.3.11
Avaya 1100 Series IP Deskphones, SIP	4.4.8
Avaya Communicator for Windows	2.1.4.0
Analog Telephones	N/A
Fax Machine	N/A
Service Provider	
OneAccess-Telstra Business SIP	N/A

5. Configure Avaya IP Office

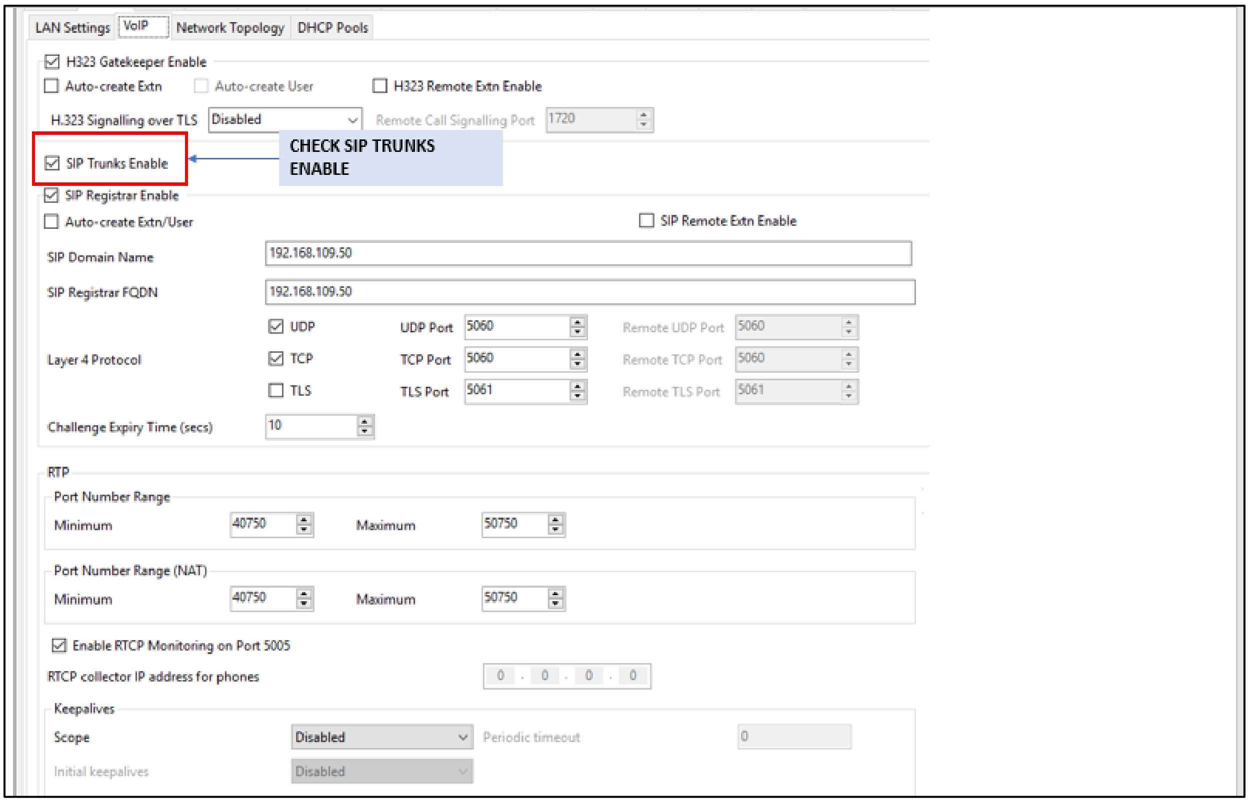
This section describes the Avaya IP Office configuration to support connectivity to OneAccess SIP NTU. Avaya IP Office is configured through the Avaya IP Office Manager PC application. From a PC running the Avaya IP Office Manager application, select **Start > Programs > IP Office > Manager** to launch the application. Navigate to **File > Open Configuration**, select the proper Avaya IP Office system from the pop-up window, and log in with the appropriate credentials (not shown).

5.1 LAN1 Settings

In the sample configuration, the LAN1 port was used to connect to OneAccess SIP NTU. To access the LAN1 settings, first navigate to **System (1) > 000C292B2458** in the **Navigation** and **Group** panes and then navigate to the **LAN1 > LAN Settings** tab in the **Details** pane. Set the **DHCP Mode** to **Server**, then set the **IP Address** field to the IP address assigned to the Avaya IP Office LAN port. Set the **IP Mask** field to the mask used on the network. Other parameters are set as default values.

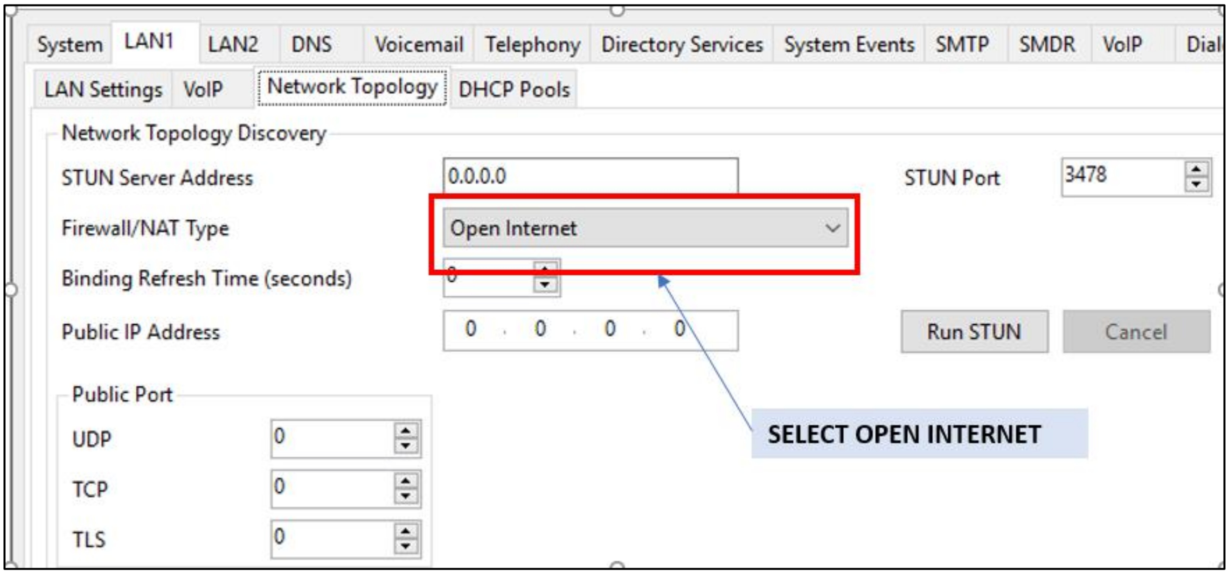


In the **VoIP** tab, as shown in the following screen, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol, such as the 9600-Series IP Telephones used in the sample configuration. The **SIP Trunks Enable** box must be checked to enable the configuration of SIP trunks to OneAccess SIP NTU. The **SIP Registrar Enable** box is checked to allow Avaya IP Office SIP phones usage. The **SIP Domain Name** is set to desired IP Office SIP domain or IP address. The **Layer 4 Protocol** use **UDP/TCP** with port **5060**. The **RTP Port Number Range** can be customized to a specific range of receive ports for the RTP media. The **Enable RTCP Monitoring on Port 5005** is checked. The specific values used for the compliance test are shown in the example below. All other parameters should be set according to customer requirements.



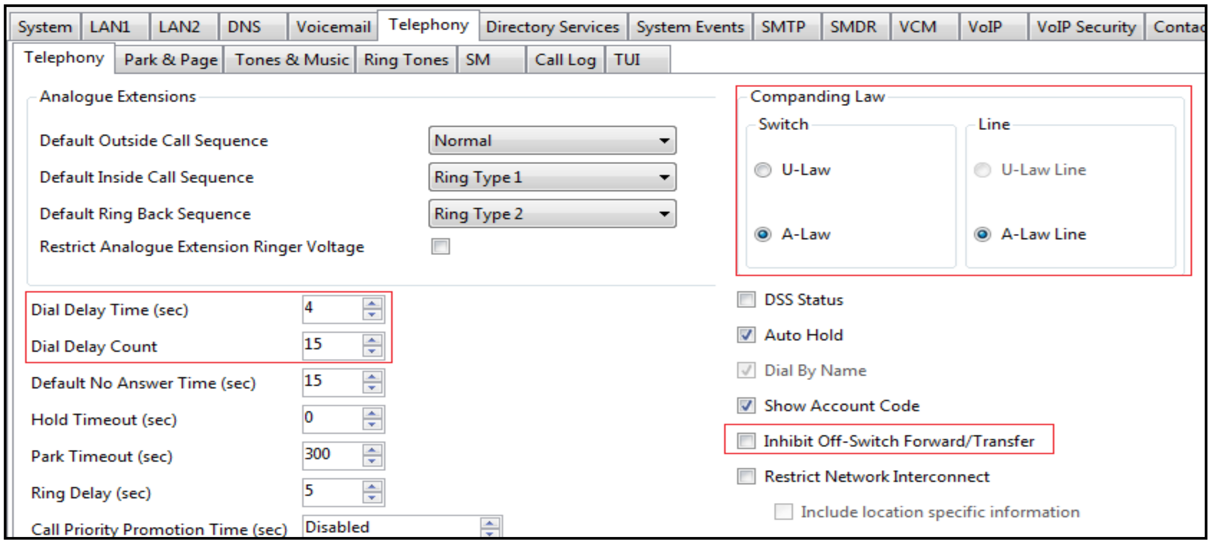
On the **Network Topology** tab in the **Details** Pane, configure the following parameters:

- Select the **Firewall/NAT Type** from the pull-down menu that matches the network configuration. The parameter was set to **Open Internet**. All other parameters should be set according to customer requirements.



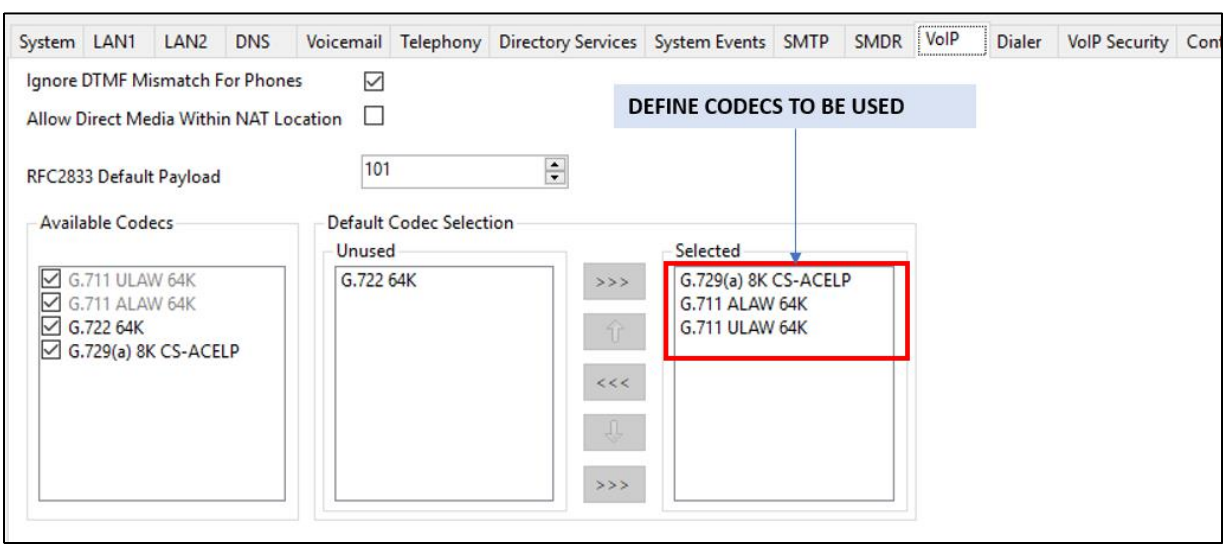
5.2 System Telephony Settings

Navigate to **System (1) > 000C292B2458** in the **Navigation** and **Group** panes and then navigate to the **Telephony > Telephony** tab in the **Details** pane. Choose the **Companding Law** typical for the enterprise location. For Australia, **A-Law** is used. Uncheck the **Inhibit Off-Switch Forward/Transfer** box to allow call forwarding and call transfers to the PSTN via the service provider across the SIP trunk. Set **Dial Delay Count** to **15** so IP Office will allow up to 15 digit dialing. Set **Dial Delay Time (sec)** to desired number.



5.3 System Codec Settings

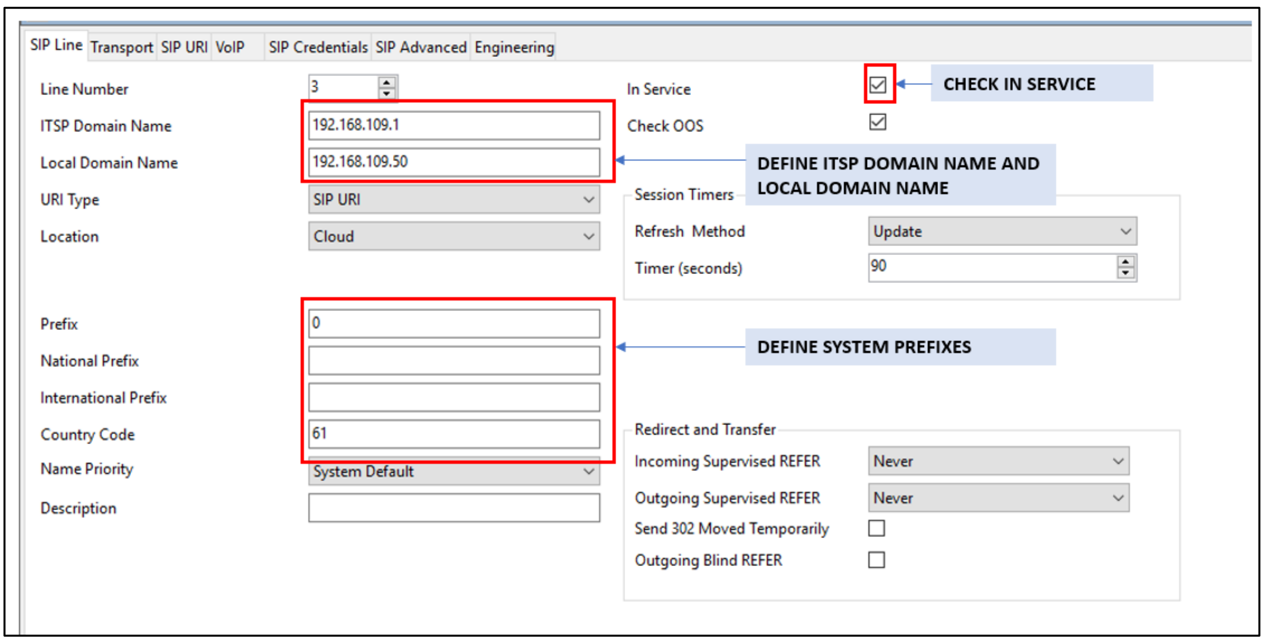
Navigate to **System (1) > 000C292B2458** in the **Navigation** and **Group** panes and then navigate to the **Codecs** tab in the **Details** pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.729(a) 8K CS-ACELP, G.711 ALAW 64K and G.711 ULAW 64K.**



5.4 Administer SIP Line

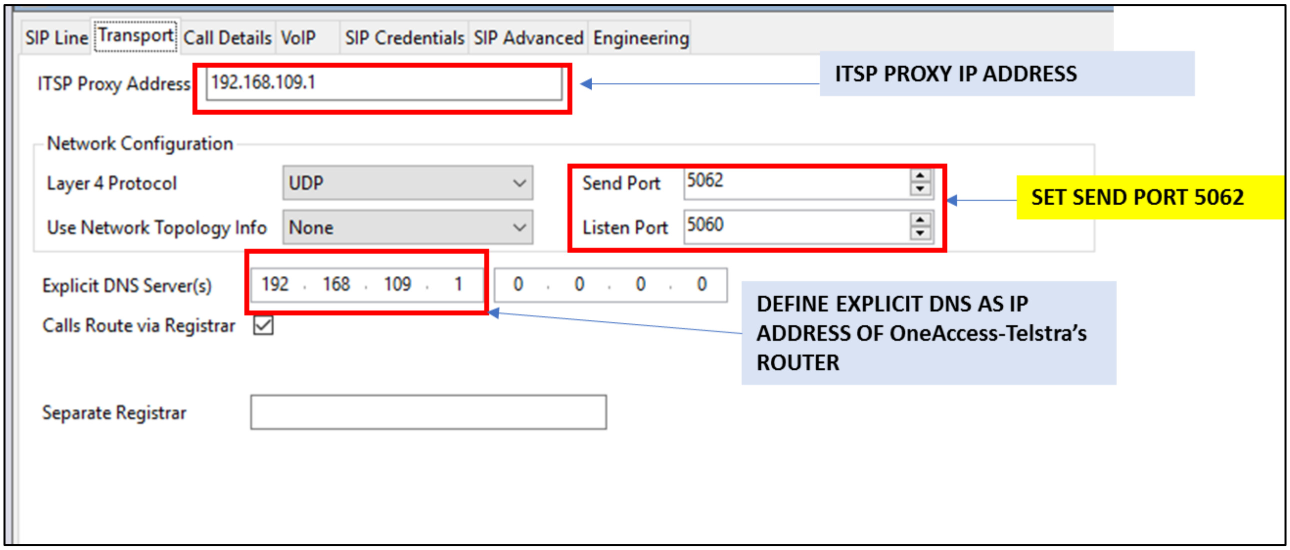
A SIP line is needed to establish the SIP connection between Avaya IP Office and OneAccess-Telstra Business SIP. To create a SIP line, begin by navigating to **Line** in the left **Navigation** pane, then right-click in the **Group** pane and select **New > SIP Line** (not shown) and enter the desired number for **Line number** (here **2** was chosen). On the **SIP Line** tab in the **Details** pane, configure the parameters as shown below:

- Set **ITSP Domain Name** to the enterprise domain (or IP address) so that IP Office uses this domain as the host portion of the SIP URI in SIP headers such as the From header.
- Set **Local Domain Name** to the same domain set in **LAN1**.
- Check the **In Service** box.
- Set **URI Type** to SIP.
- Check the **Check OOS** box. With this option selected, IP Office will use the SIP OPTIONS method to periodically check the SIP Line.
- Under **Session Timers**:
    - **Refresh Method**: Select **Update**.
    - **Timer (sec)**: Enter **90**.
- Set **Country Code** to **61** (Country Code of Australia).
- Set **National Prefix** to **0**.
- Set **Incoming Supervised REFER** to **Never**.
- Set **Outgoing Supervised REFER** to **Never**.



Select the **Transport** tab:

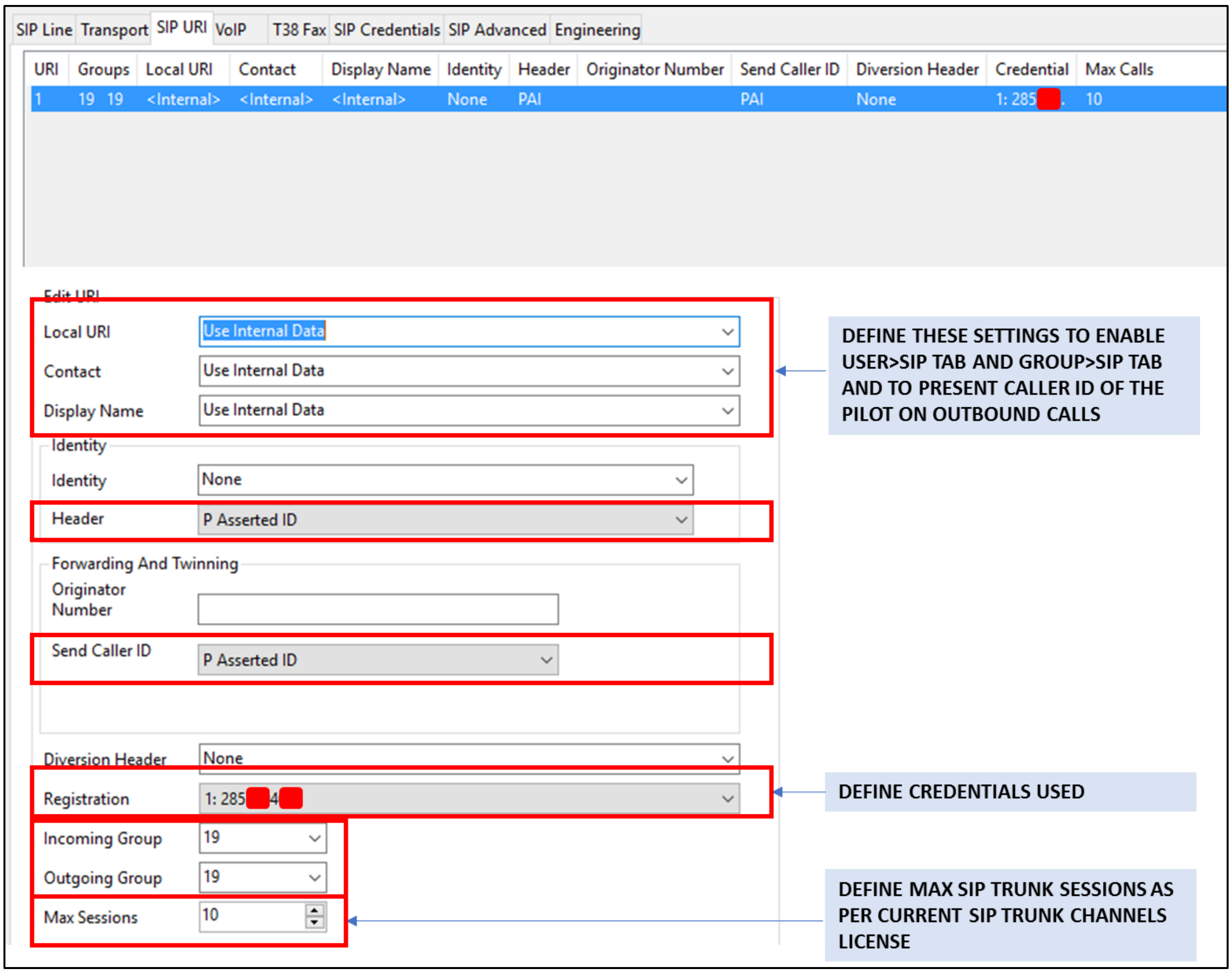
- The **ITSP Proxy Address** is set to the IP address of OneAccess SIP NTU. As shown in screenshot below, this IP address is 192.168.109.1.
- In the **Network Configuration** area, **UDP** is selected as the Layer 4 Protocol, and the **Send Port** is set to **5062**, Listen Port is set to **5060**. The **Use Network Topology Info** parameter is set to **None**. Other parameters retain default values in the screen below.
- **Define Explicit DNS Server** as IP address of OneAccess-Telstra's router**.** As shown in the screenshot below, this is 92.168.109.1



A SIP URI entry must be created to match each incoming number that Avaya IP Office will accept on this line. Select the **SIP URI** tab then click the **Add** button and the **New URI** area will appear at the bottom of the pane (not shown).

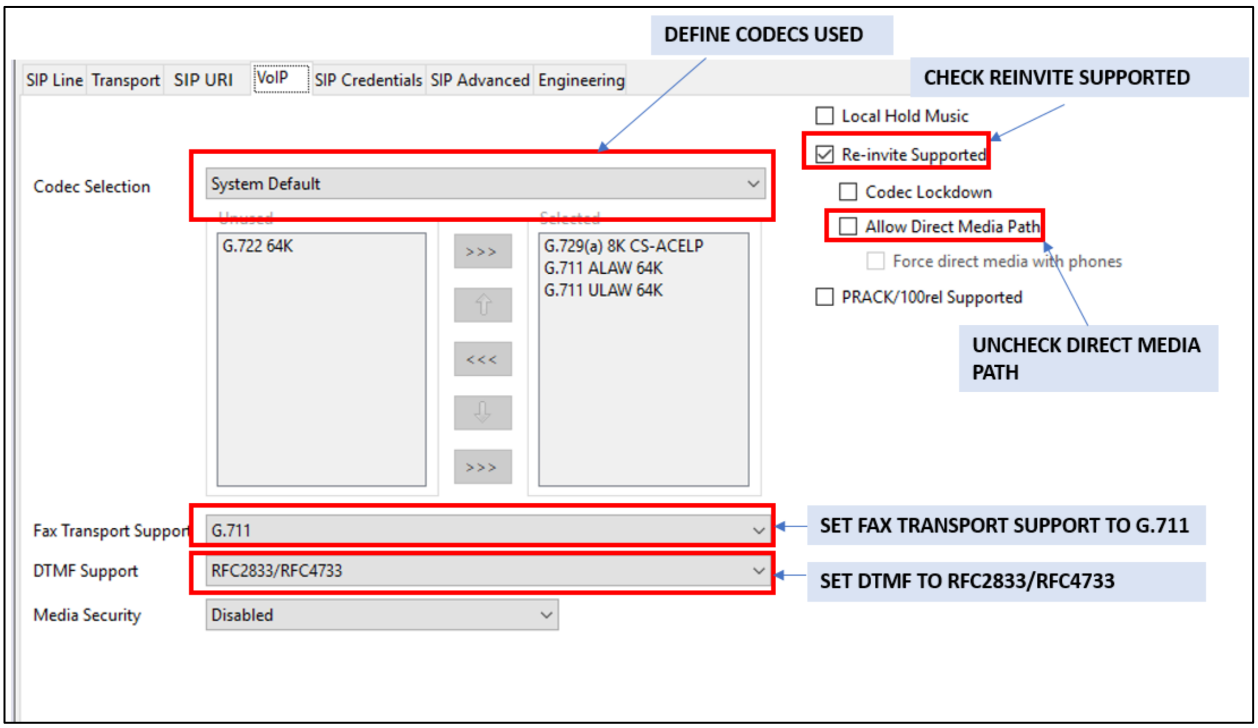
For the compliance test, a single SIP URI entry was created that matched any DID number assigned to an Avaya IP Office user. The entry was created with the parameters shown below:

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**.
- Under **Identity:** set **Identity** to **Use Internal Data** and set **Header** to **P Asserted ID**. With this setting IP Office will populate the SIP P-Asserted-Identity header on outgoing calls with the data set in the SIP tab of the call initiating User as shown in **Section 5.6**.
- Set **Caller** to **P Asserted ID** for **Forwarding and Twinning**.
- Associate this line with an incoming line group in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern, as per your license entitlement.



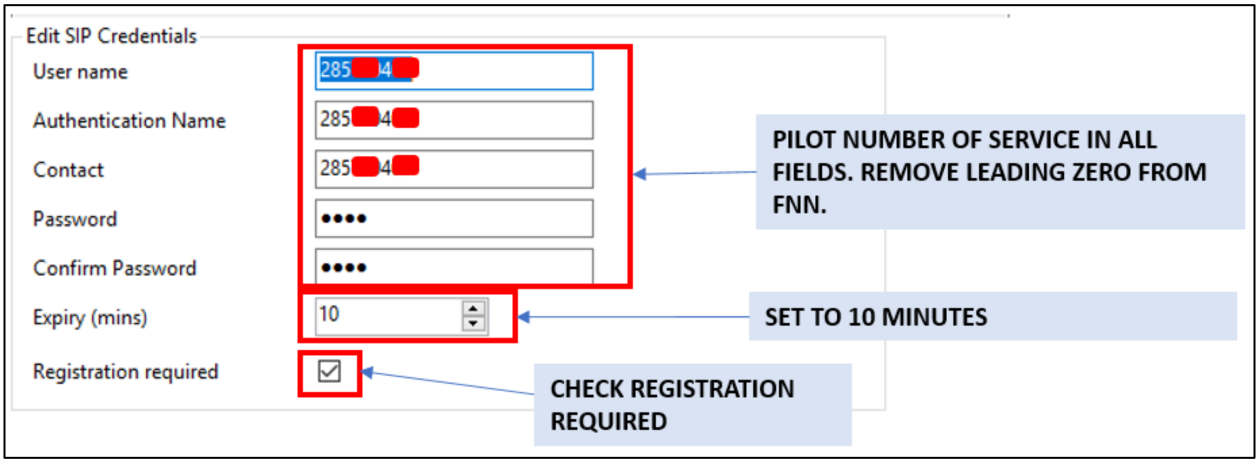
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- The Codec Selection can be selected by choosing **Custom** from the pull-down menu, allowing an explicit ordered list of codecs to be specified. Selecting **G.729(a) 8K CS-ACELP , G.711 ALAW 64K** and **G.711 ULAW 64K c**odecs causes Avaya IP Office to include these codecs.
- Check the **Re-invite Supported** box.
- Uncheck **Codec Lockdown** box.
- Uncheck **Allow Direct Media Path** box.
- Set **Fax Transport Support** to **G.711** from the pull-down menu.
- Set the **DTMF Support** to **RFC2833/RFC4733** from the pull-down menu.
- Default values may be used for all other parameters.



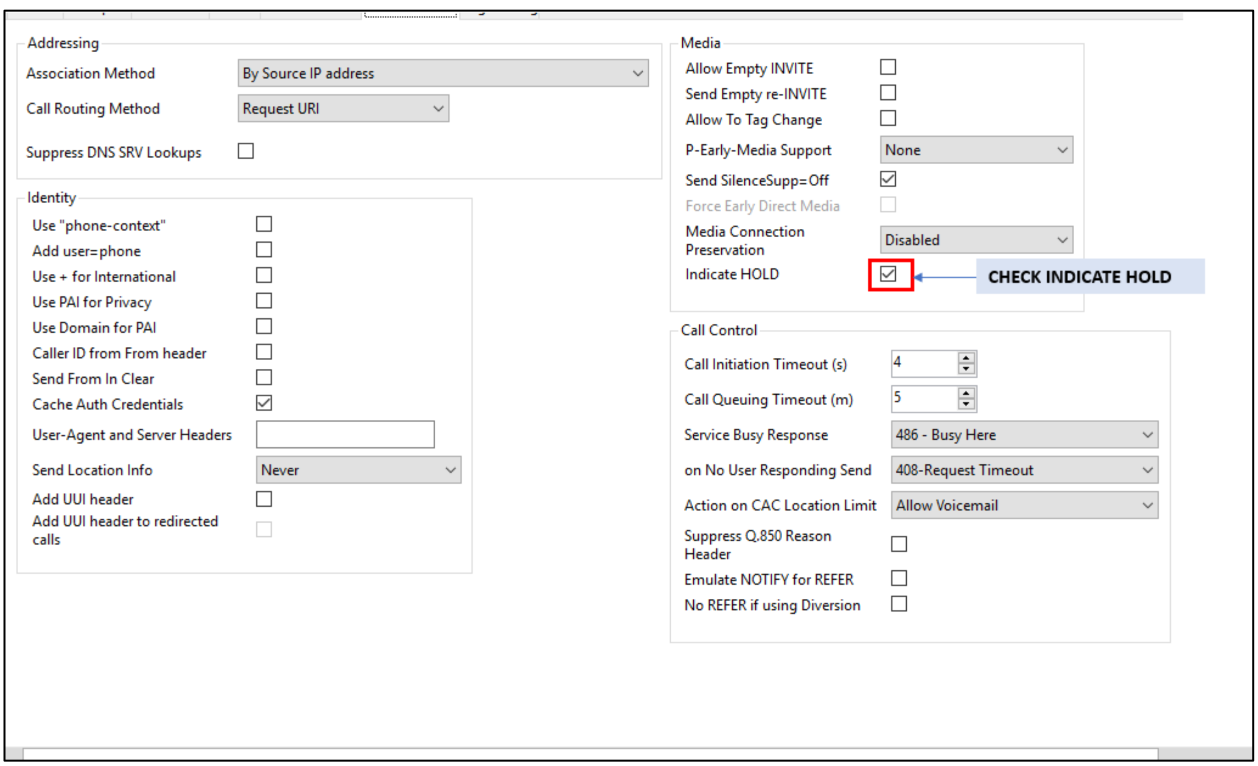
Select **SIP Credentials** tab, configure the credentials as provided by service provider.

- Enter the **User Name**, **Authentication Name** and **Contact** numbers and the associated password.
- Set **Expiry** time to **10** minutes
- Check the **Registration required**



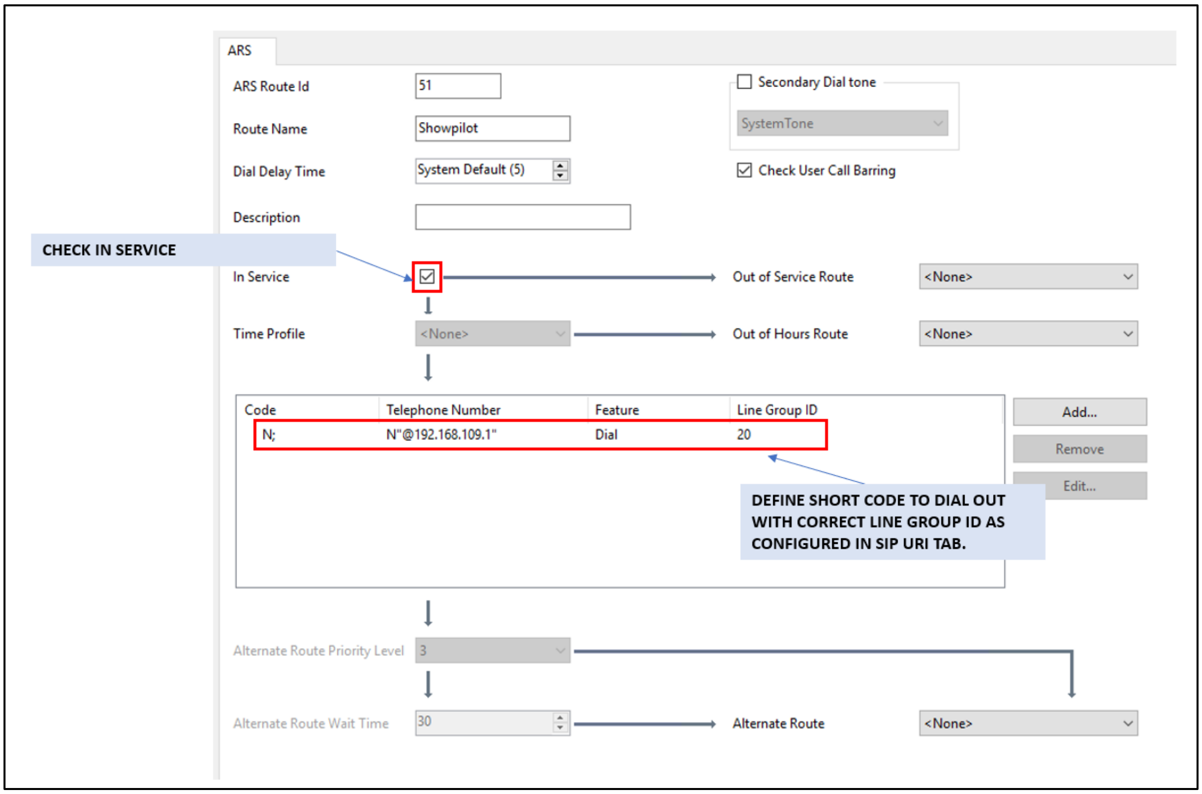
Select **SIP Advanced** tab:

- Check **Indicate HOLD** box.



5.5 ARS table

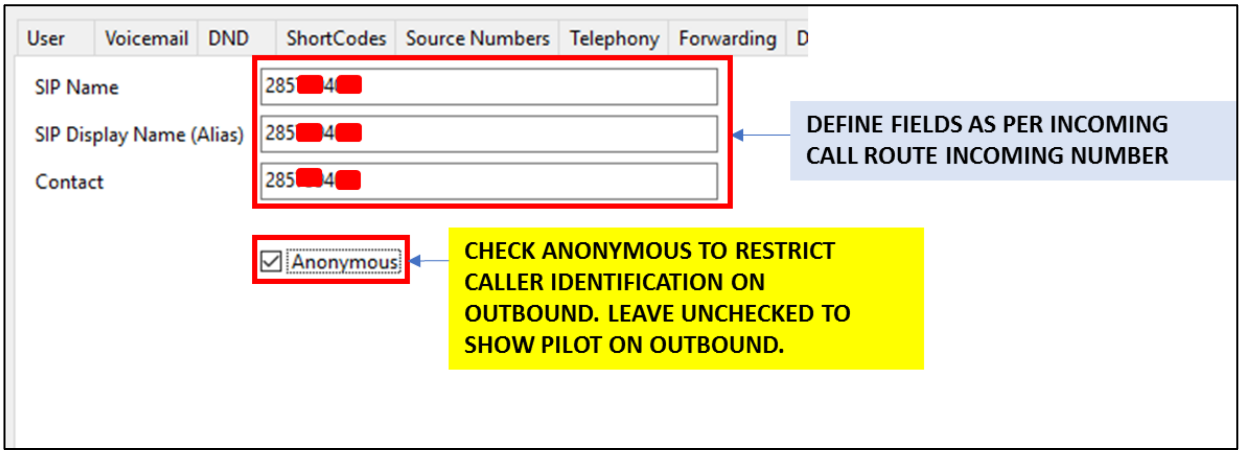
In the left **Navigation**, right-click on **ARS** and select **New** to create a new ARS form and place in service.



5.6 User

Any user that is used to make outbound calls to OneAccess-Telstra Business SIP must be configured with one of the DID numbers assigned. From the **User** in the left **Navigation**, select a user in the user list and navigate to **SIP** tab of that user

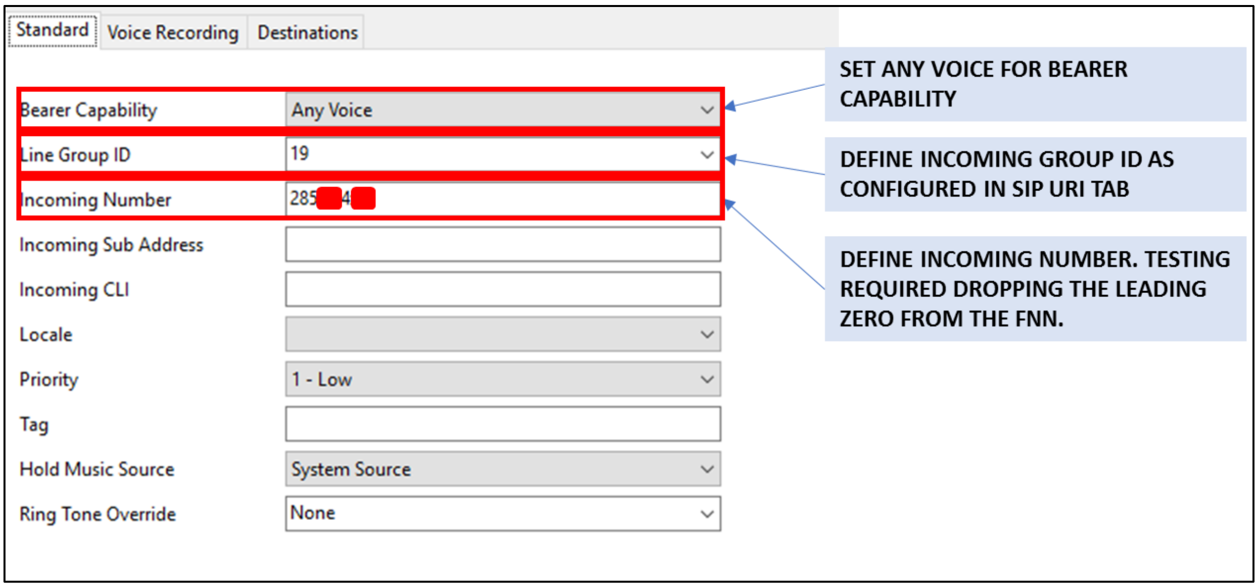
- Enter one of the DID numbers to **SIP Name**, **SIP Display Name (Alias)** and **Contac**t.
- Check **Anonymous** to restrict caller identification on outbound call



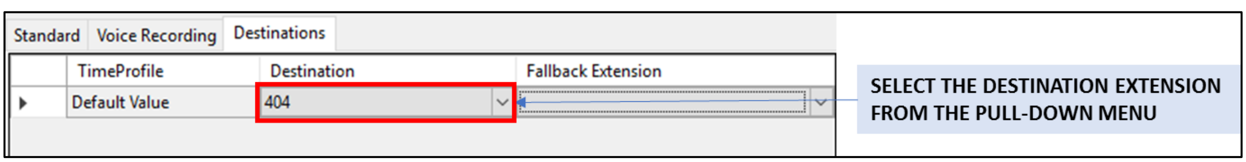
5.7 Incoming Call Route

An incoming call route maps an inbound DID 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:

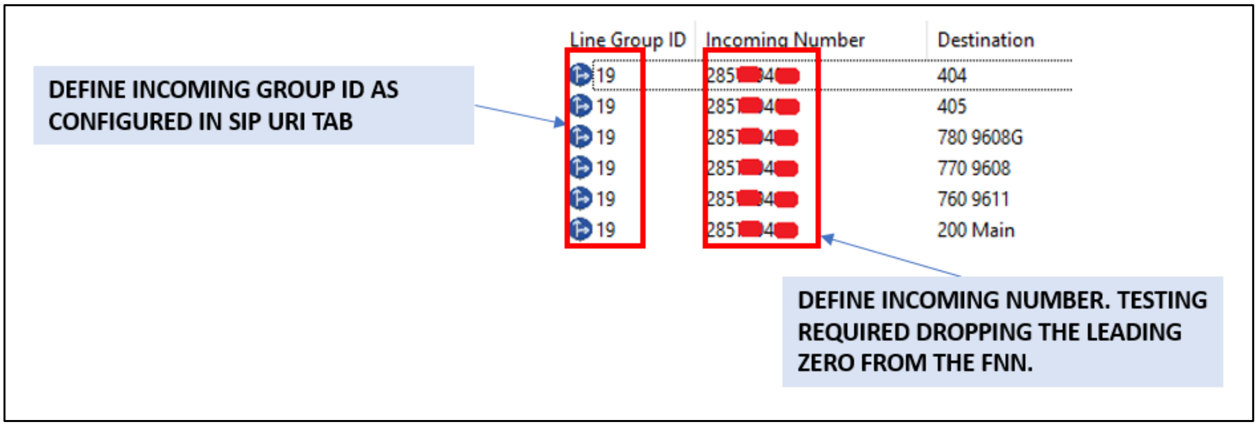
- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.4**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left. In this sample configuration, assigned DID numbers starting with 028 have been masked as 285xxx4xx due to security reasons.



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).



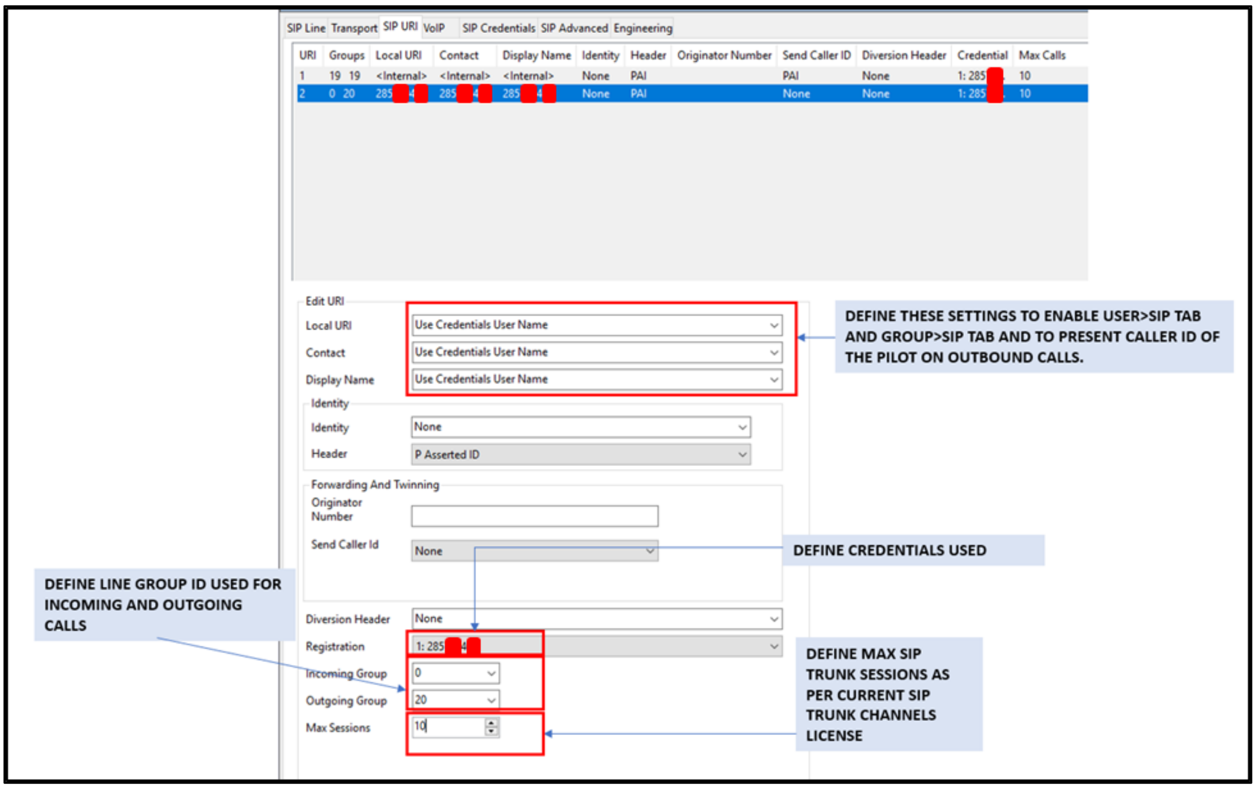
Repeat above steps to map multiple DID numbers to multiple users / extensions. As shown in below screenshot, multiple DID numbers are mapped to multiple users / extensions, and they are sharing same line group ID



5.8 Configure Caller Identity Restriction on Outbound Call

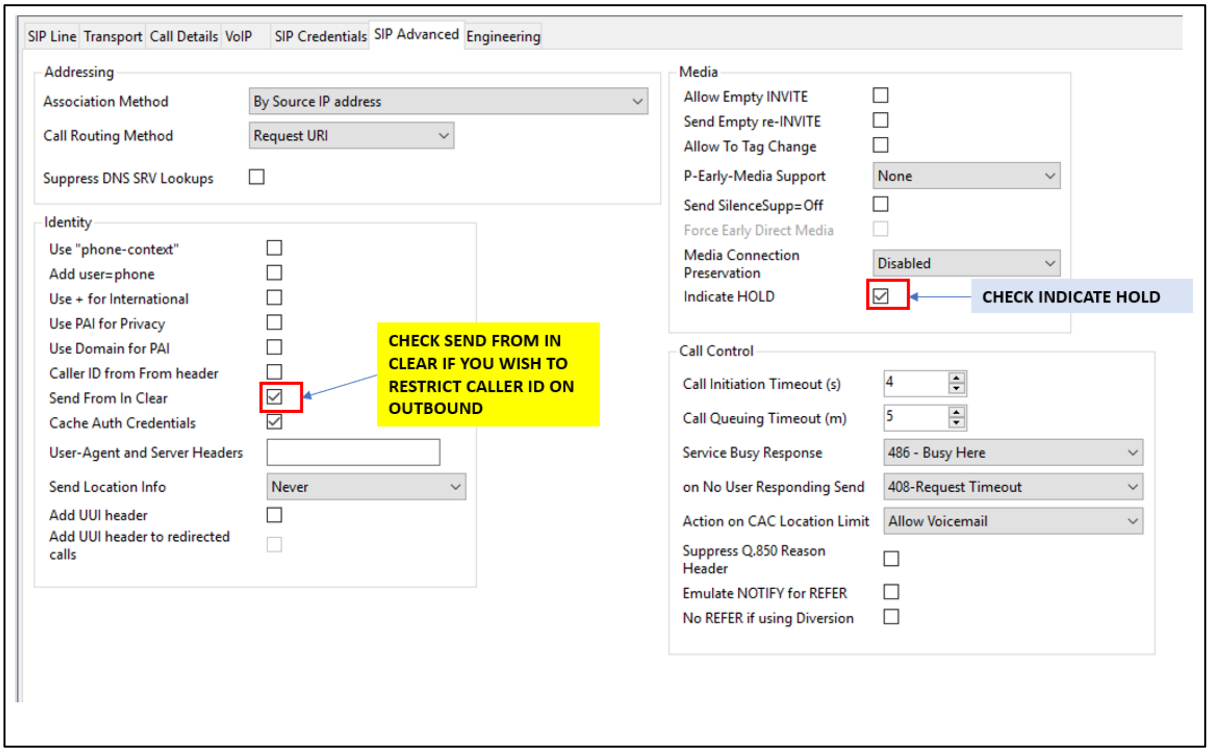
Create a new SIP URI in existing line.

- Set **Local URI**, **Contact**, and **Display Name** to **Use Internal Data**.
- Under **Identity,** set **Identity** to **None** and set **Header** to **P Asserted ID**. With this setting IP Office will populate the SIP P-Asserted-Identity header on outgoing calls with the data set in the SIP tab of the call initiating User as shown in **Section 5.6**.
- Associate this line with an outgoing line group using the **Outgoing Group** field.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern, as per your license entitlement.



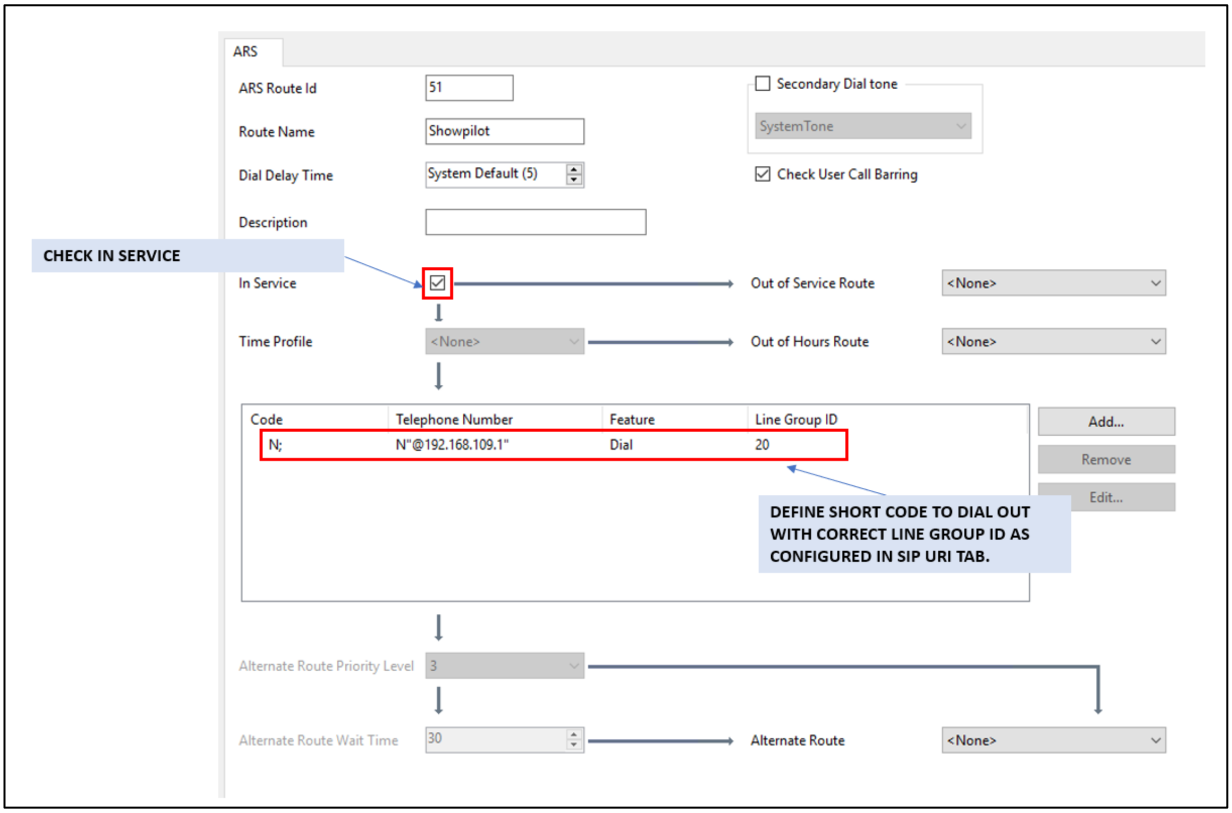
Select **SIP Advanced** tab and configure the following parameters as follows:

- Check **Send From In Clear.**
- Check **Indicate HOLD.**

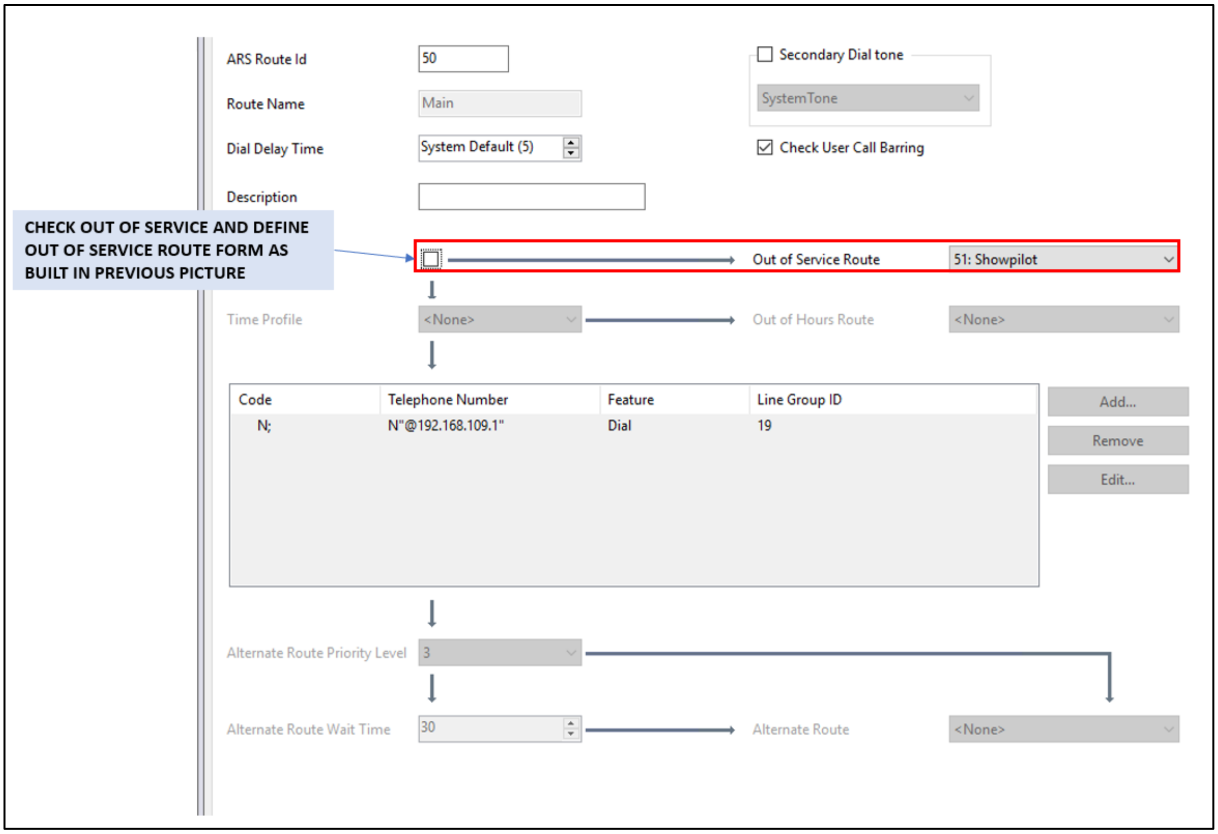


Go to the **ARS** form and perform the following steps:

- Create a new **ARS** form and place in service.
- Define a short code to dial out with the group id as configured in **SIP URI** tab.

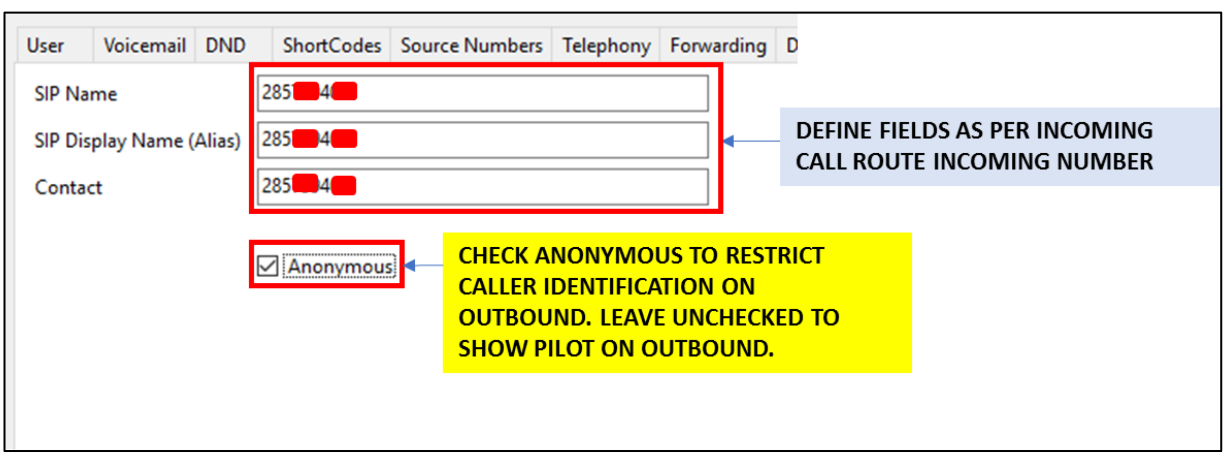


- Modify the main **ARS** form to be out of service.
- Define the out of service route to route to the second **ARS** form.



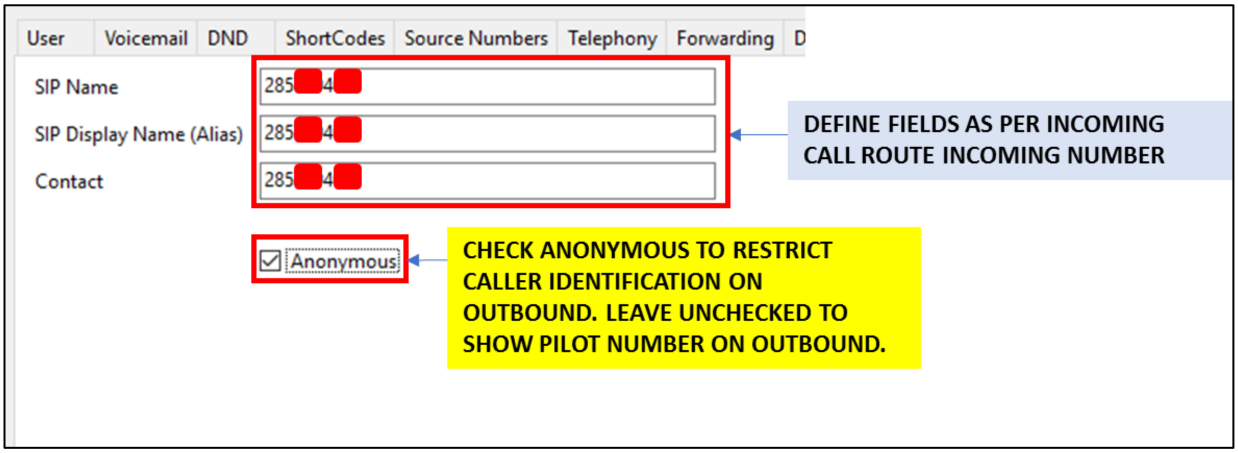
Go to **User** configuration, select **SIP** tab and configure the following fields:

- Define the **SIP Name**, **SIP Display Name (Alias)** and **Contact.**
- Check **Anonymous.**



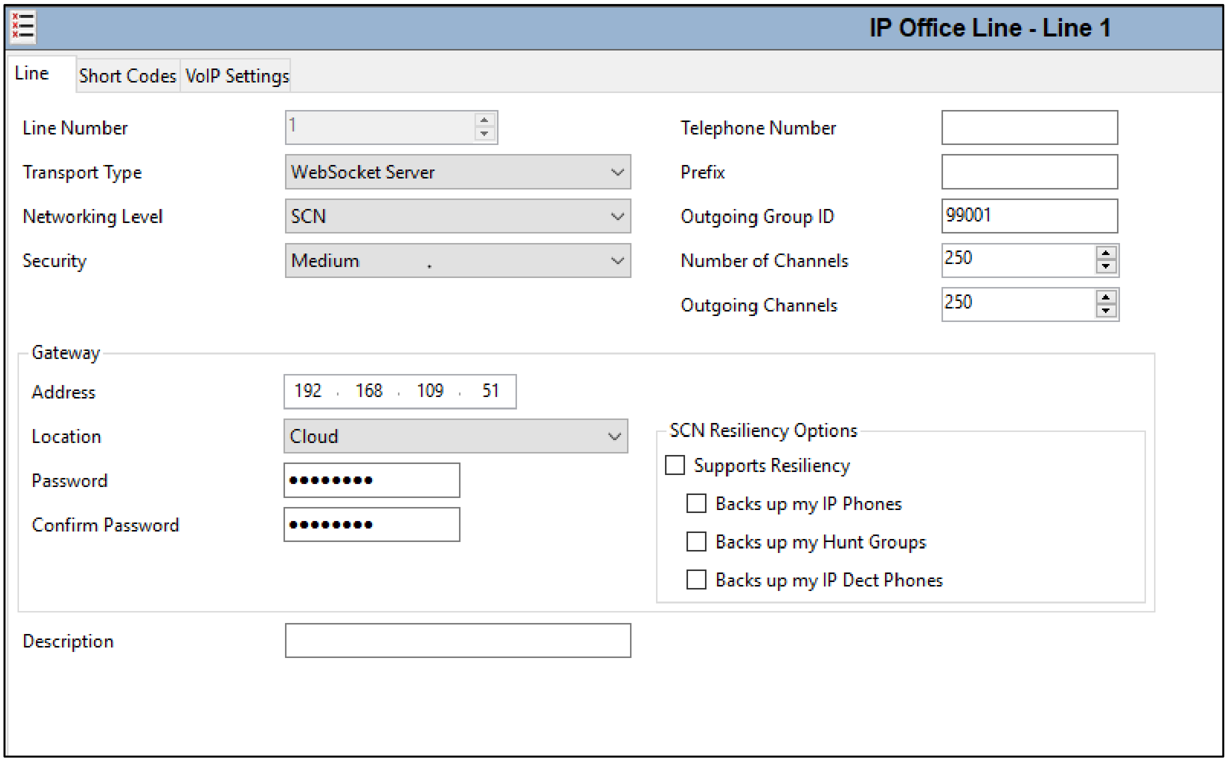
Go to **Group** configuration, select **SIP** tab and perform these steps:

- Define the **SIP Name**, **SIP Display Name (Alias)** and **Contact.**
- Check **Anonymous.**



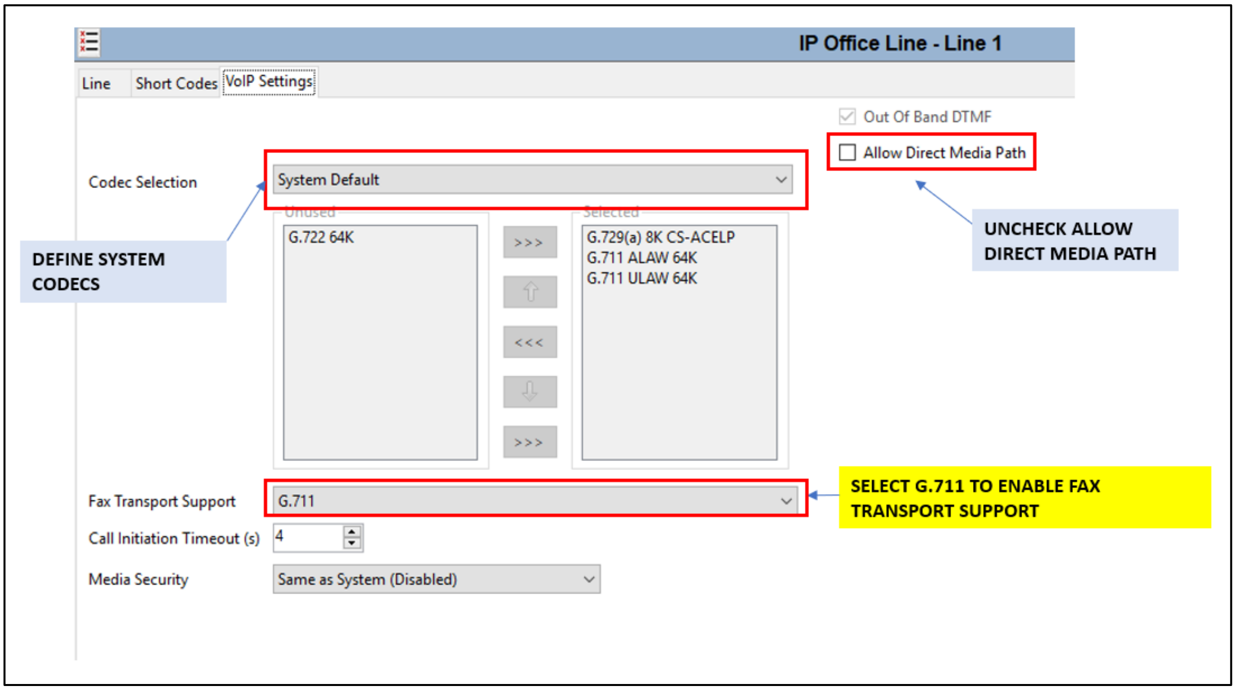
5.9 Configuring Expansion System to Allow Fax Support

In **Line** tab, configure the **IP Office Line** as in screenshot below on IP Office Server Edition.



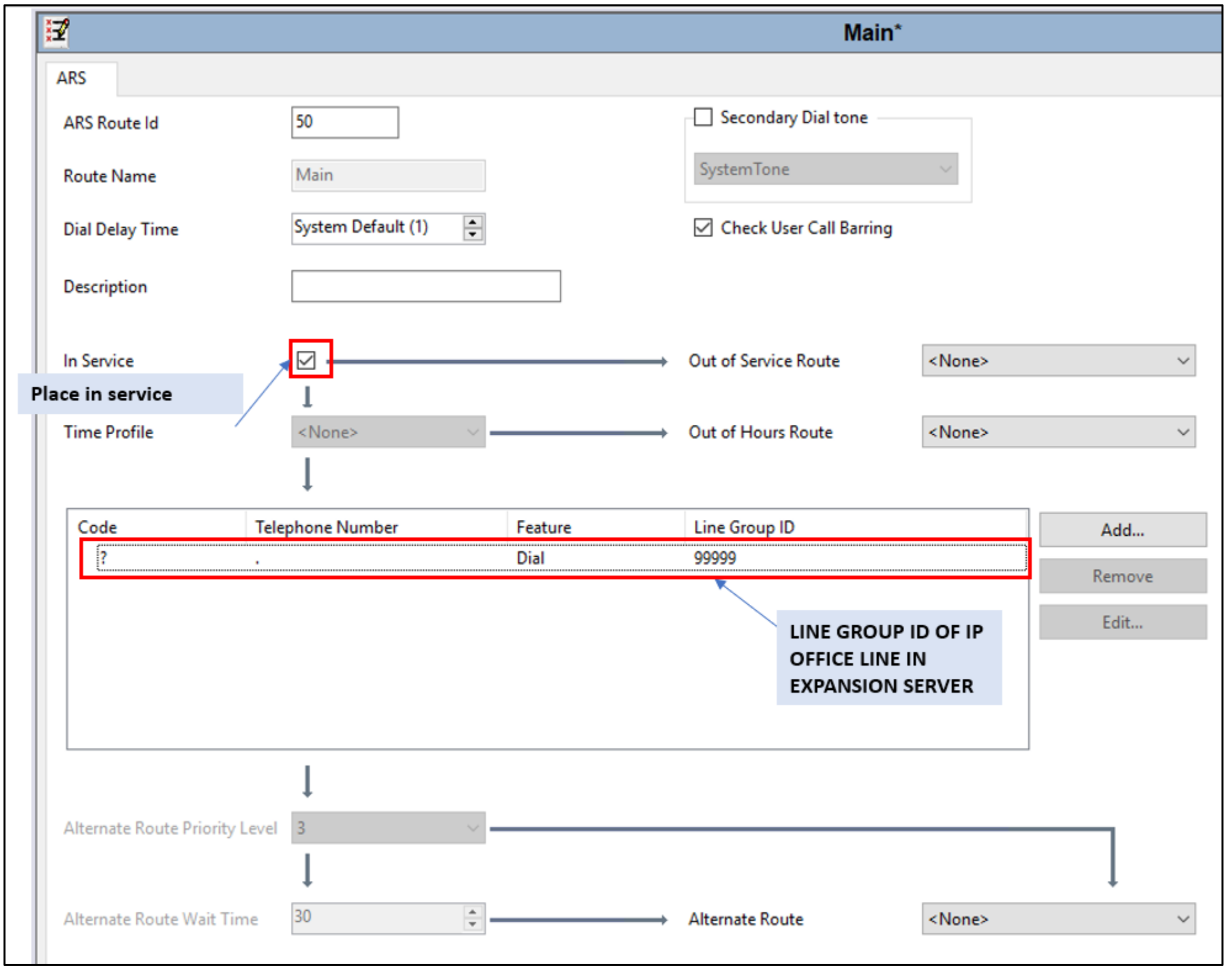
Select **VoIP Settings** tab, select Codec list and configure the following fields:

- Uncheck **Allow Direct Media Path.**
- Select **G.711** for **Fax Transport Support.**

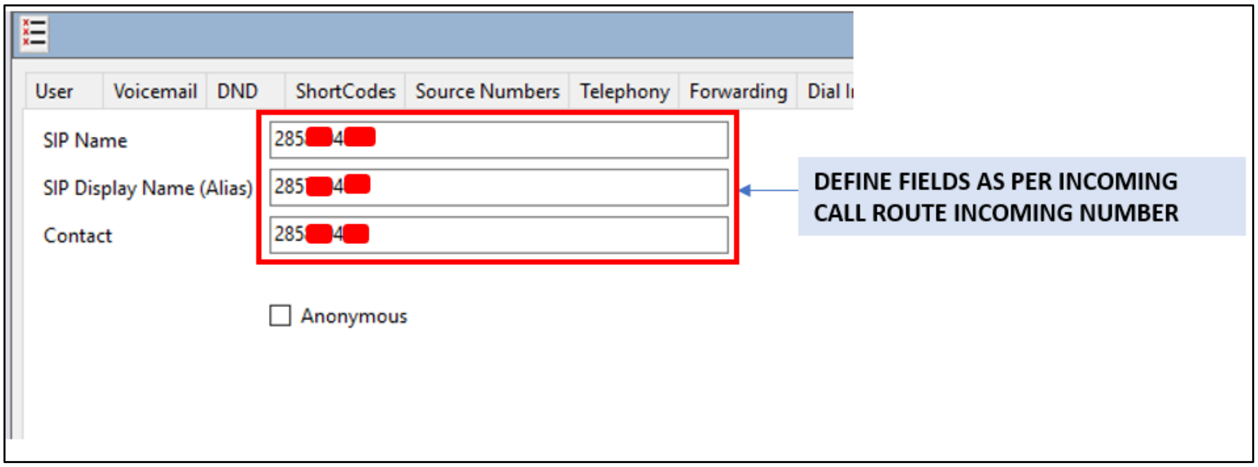


Create a new **ARS** form on IP Office Expansion System and perform the following steps:

- Check **In Service.**
- Add **Short Code** with **Line Group ID** of **99999** as shown in screenshot below.

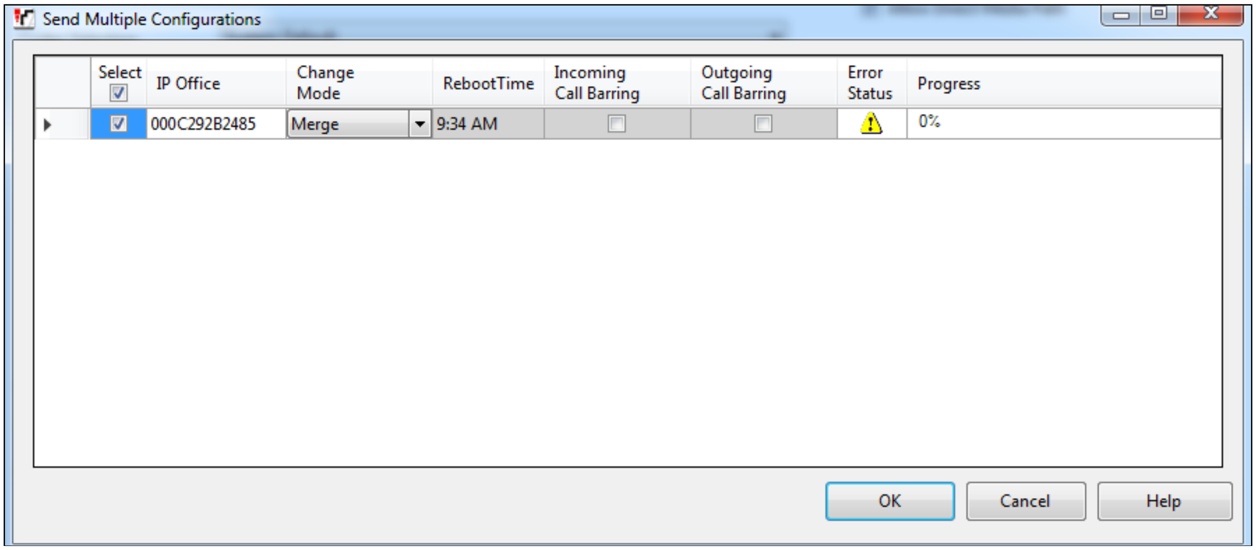


Configure user in IP Office Expansion, select **SIP** tab and enter one of the DID numbers to **SIP Name**, **SIP Display Name (Alias)** and **Contac**t.



5.10 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. The screen below is displayed indicating the system configuration has been changed and needs to be saved. **Merge**, **Immediate**, **When Free** or **Timed** is shown under the **Change Mode** column, 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.

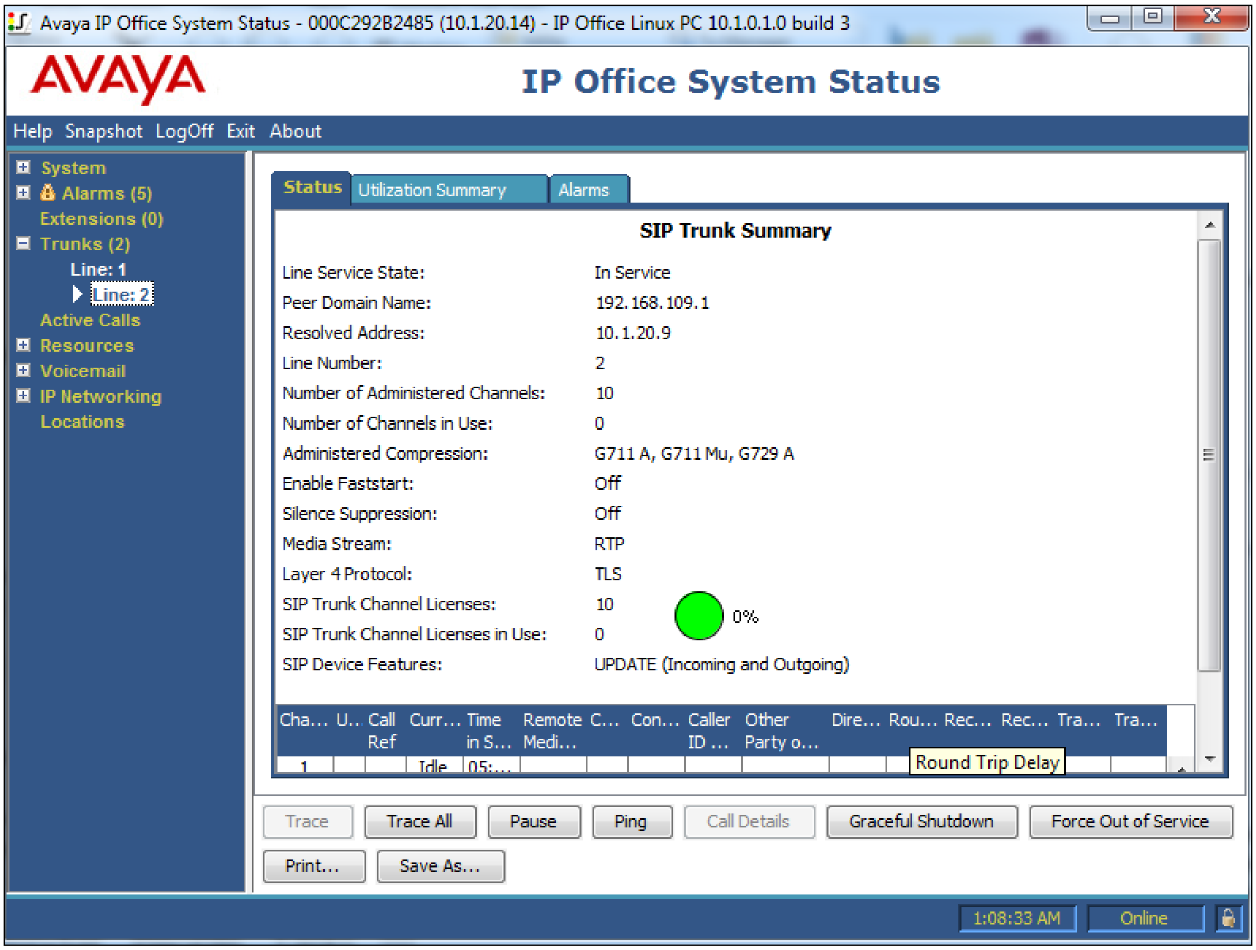


6. Verification Steps

The following steps may be used to verify the configuration on Avaya IP Office and OneAccess-Telstra Business SIP Trunk Service.

6.1 Avaya IP Office

On the PC that has IP Office Manager installed, navigate to **Start** > **All Programs** > **IP Office** > **System Status**. A login window appears, login with proper credentials. Click on **Trunks** > **Line: 2** (the SIP line configured on IP Office for SIP trunking) and verify that **Line Service State** is **In Service** with all settings as administered.



6.2 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling by placing call to some public Interactive Voice Response (IVR) system, and navigating the menu using phone keypad.

7. Conclusion

As illustrated in these Application Notes, Avaya IP Office Release 10.1 can be configured to interoperate successfully with OneAccess-Telstra Business SIP. This solution allows enterprise users access to the PSTN using the OneAccess-Telstra Business SIP. Please refer to **Section 2.2** for observations.

8. Additional References

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

[1] *Deploying IP Office Server Edition Solution,* Release 10.1.
[2] *Deploying IP Office IP500 V2,* Release 10.1.
[3] *Administering Avaya IP Office with Manager*, Release 10.1.

Product documentation for OneAccess-Telstra Business SIP is available from Telstra.

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.