



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.....	3
2.	General Test Approach and Test Results.....	3
2.1	Interoperability Compliance Testing.....	3
2.2	Test Results	4
2.3	Support	4
3.	Reference Configuration.....	5
4.	Equipment and Software Validated	6
5.	Configure Avaya IP Office	7
5.1	LAN1 Settings.....	7
5.2	System Telephony Settings	10
5.3	System Codec Settings	10
5.4	Administer SIP Line.....	11
5.5	ARS table	16
5.6	User	17
5.7	Incoming Call Route	18
5.8	Configure Caller Identity Restriction on Outbound Call	20
5.9	Configuring Expansion System to Allow Fax Support.....	25
5.10	Save Configuration	29
6.	Verification Steps.....	30
6.1	Avaya IP Office.....	30
6.2	Telephony Services	30
7.	Conclusion	31
8.	Additional References.....	31

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.

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.

The screenshot displays the 'LAN Settings' window for 'LAN1'. The 'IP Address' field is set to '192 . 168 . 109 . 50' and the 'IP Mask' field is set to '255 . 255 . 255 . 0'. Both fields are enclosed in a red rectangular box. A blue callout box with an arrow points to this red box, containing the text 'DEFINE CALL SERVER IP ADDRESS'. Below these fields, the 'Number Of DHCP IP Addresses' is set to '154'. The 'DHCP Mode' section shows three radio buttons: 'Server' (which is selected and also enclosed in a red rectangular box), 'Client', and 'Disabled'. A blue callout box with an arrow points to the 'Server' radio button, containing the text 'DHCP MODE SERVER OR DISABLED, DEPENDING IF DHCP SERVER IS REQUIRED FOR SIP/IP ENDPOINTS'. An 'Advanced' button is visible to the right of the DHCP Mode section.

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.

The screenshot displays the VoIP configuration page with the following settings:

- LAN Settings** tab is selected.
- H323 Gatekeeper Enable** is checked.
- Auto-create Extn**, **Auto-create User**, and **H323 Remote Extn Enable** are unchecked.
- H323 Signalling over TLS** is set to **Disabled**.
- Remote Call Signalling Port** is set to **1720**.
- SIP Trunks Enable** is checked and highlighted with a red box. A blue callout box points to it with the text "CHECK SIP TRUNKS ENABLE".
- SIP Registrar Enable** is checked.
- Auto-create Extn/User** and **SIP Remote Extn Enable** are unchecked.
- SIP Domain Name** is set to **192.168.109.50**.
- SIP Registrar FQDN** is set to **192.168.109.50**.
- Layer 4 Protocol** settings:
 - UDP** is checked, **UDP Port** is **5060**, **Remote UDP Port** is **5060**.
 - TCP** is checked, **TCP Port** is **5060**, **Remote TCP Port** is **5060**.
 - TLS** is unchecked, **TLS Port** is **5061**, **Remote TLS Port** is **5061**.
- Challenge Expiry Time (secs)** is set to **10**.
- RTP** section:
 - Port Number Range**: Minimum **40750**, Maximum **50750**.
 - Port Number Range (NAT)**: Minimum **40750**, Maximum **50750**.
 - Enable RTCP Monitoring on Port 5005** is checked.
 - RTCP collector IP address for phones** is set to **0 . 0 . 0 . 0**.
 - Keepalives** section:
 - Scope** is set to **Disabled**.
 - Periodic timeout** is set to **0**.
 - Initial keepalives** is set to **Disabled**.

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.

The screenshot shows a configuration window with multiple tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Dial. The 'Network Topology' tab is selected. Under the 'Network Topology Discovery' section, the 'Firewall/NAT Type' is set to 'Open Internet' in a dropdown menu, which is highlighted with a red rectangle. A blue arrow points from a text box labeled 'SELECT OPEN INTERNET' to this dropdown. Other visible fields include 'STUN Server Address' (0.0.0.0), 'STUN Port' (3478), 'Binding Refresh Time (seconds)' (0), 'Public IP Address' (0.0.0.0), and 'Public Port' (UDP, TCP, TLS, all set to 0). 'Run STUN' and 'Cancel' buttons are also present.

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.

The screenshot shows the 'Telephony' configuration page for a system. The 'Companding Law' section is highlighted with a red box, showing 'Switch' set to 'A-Law' and 'Line' set to 'A-Law Line'. The 'Dial Delay Time (sec)' is set to 4 and 'Dial Delay Count' is set to 15, both highlighted with red boxes. The 'Inhibit Off-Switch Forward/Transfer' checkbox is unchecked, also highlighted with a red box. Other settings include 'Default Outside Call Sequence' (Normal), 'Default Inside Call Sequence' (Ring Type 1), 'Default Ring Back Sequence' (Ring Type 2), 'Restrict Analogue Extension Ringer Voltage' (unchecked), 'DSS Status' (unchecked), 'Auto Hold' (checked), 'Dial By Name' (checked), 'Show Account Code' (checked), 'Restrict Network Interconnect' (unchecked), and 'Include location specific information' (unchecked).

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**.

The screenshot shows the 'Codecs' configuration page. The 'RFC2833 Default Payload' is set to 101. The 'Available Codecs' list includes G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-ACELP. The 'Default Codec Selection' section shows 'Unused' and 'Selected' lists. The 'Selected' list is highlighted with a red box and contains G.729(a) 8K CS-ACELP, G.711 ALAW 64K, and G.711 ULAW 64K. A blue box labeled 'DEFINE CODECS TO BE USED' points to the 'Selected' list.

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**.

The screenshot displays the 'SIP Line' configuration window with the following fields and settings:

- Line Number:** 3
- ITSP Domain Name:** 192.168.109.1
- Local Domain Name:** 192.168.109.50
- URI Type:** SIP URI
- Location:** Cloud
- Prefix:** 0
- National Prefix:** (empty)
- International Prefix:** (empty)
- Country Code:** 61
- Name Priority:** System Default
- Description:** (empty)
- In Service:** ☒ (labeled 'CHECK IN SERVICE')
- Check OOS:** ☒
- Session Timers:**
 - Refresh Method:** Update
 - Timer (seconds):** 90
- Redirect and Transfer:**
 - Incoming Supervised REFER:** Never
 - Outgoing Supervised REFER:** Never
 - Send 302 Moved Temporarily:** ☐
 - Outgoing Blind REFER:** ☐

Blue callout boxes highlight the following areas:

- CHECK IN SERVICE:** Points to the 'In Service' checkbox.
- DEFINE ITSP DOMAIN NAME AND LOCAL DOMAIN NAME:** Points to the 'ITSP Domain Name' and 'Local Domain Name' fields.
- DEFINE SYSTEM PREFIXES:** Points to the 'Prefix' and 'Country Code' fields.

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

The screenshot displays the 'SIP Line' configuration window with the 'Transport' tab selected. The 'ITSP Proxy Address' field is set to '192.168.109.1'. The 'Network Configuration' section shows 'Layer 4 Protocol' set to 'UDP', 'Use Network Topology Info' set to 'None', 'Send Port' set to '5062', and 'Listen Port' set to '5060'. The 'Explicit DNS Server(s)' field is set to '192.168.109.1'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

Annotations in the screenshot include:

- ITSP PROXY IP ADDRESS** pointing to the ITSP Proxy Address field.
- SET SEND PORT 5062** pointing to the Send Port field.
- DEFINE EXPLICIT DNS AS IP ADDRESS OF OneAccess-Telstra's ROUTER** pointing to the Explicit DNS Server(s) field.

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.

SIP Line	Transport	SIP URI	VoIP	T38 Fax	SIP Credentials	SIP Advanced	Engineering				
1	19	19	<Internal>	<Internal>	<Internal>	None	PAI	PAI	None	1: 285 4	10

Edit URI

Local URI: Use Internal Data

Contact: Use Internal Data

Display Name: Use Internal Data

Identity: None

Header: P Asserted ID

Forwarding And Twinning

Originator Number:

Send Caller ID: P Asserted ID

Diversion Header: None

Registration: 1: 285 4

Incoming Group: 19

Outgoing Group: 19

Max Sessions: 10

DEFINE THESE SETTINGS TO ENABLE USER>SIP TAB AND GROUP>SIP TAB AND TO PRESENT CALLER ID OF THE PILOT ON OUTBOUND CALLS

DEFINE CREDENTIALS USED

DEFINE MAX SIP TRUNK SESSIONS AS PER CURRENT SIP TRUNK CHANNELS LICENSE

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** codecs 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.

DEFINE CODECS USED

SIP Line Transport SIP URI **VoIP** SIP Credentials SIP Advanced Engineering **CHECK REINVITE SUPPORTED**

Codec Selection System Default

Unused Selected

G.722 64K >>> G.729(a) 8K CS-ACELP
G.711 ALAW 64K
G.711 ULAW 64K

<<< >>>

☐ Local Hold Music
☒ **Re-invite Supported**
☐ Codec Lockdown
☐ **Allow Direct Media Path**
☐ Force direct media with phones
☐ PRACK/100rel Supported

UNCHECK DIRECT MEDIA PATH

Fax Transport Support G.711 **SET FAX TRANSPORT SUPPORT TO G.711**

DTMF Support RFC2833/RFC4733 **SET DTMF TO RFC2833/RFC4733**

Media Security Disabled

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**

The screenshot shows the 'Edit SIP Credentials' form. A red box highlights the 'User name', 'Authentication Name', and 'Contact' fields, which all contain the value '285 4'. A blue callout box points to these fields with the text 'PILOT NUMBER OF SERVICE IN ALL FIELDS. REMOVE LEADING ZERO FROM FNN.'. Another blue callout box points to the 'Expiry (mins)' field, which is set to '10', with the text 'SET TO 10 MINUTES'. A third blue callout box points to the 'Registration required' checkbox, which is checked, with the text 'CHECK REGISTRATION REQUIRED'.

Select **SIP Advanced** tab:

- Check **Indicate HOLD** box.

The screenshot shows the 'SIP Advanced' configuration tab. In the 'Media' section, the 'Indicate HOLD' checkbox is checked, and a blue callout box points to it with the text 'CHECK INDICATE HOLD'. Other settings visible include 'Association Method' set to 'By Source IP address', 'Call Routing Method' set to 'Request URI', and 'Suppress DNS SRV Lookups' unchecked. The 'Identity' section has several options unchecked, including 'Use "phone-context"', 'Add user=phone', 'Use + for International', 'Use PAI for Privacy', 'Use Domain for PAI', 'Caller ID from From header', and 'Send From In Clear'. The 'Cache Auth Credentials' checkbox is checked. The 'Send Location Info' dropdown is set to 'Never'. The 'Call Control' section has 'Call Initiation Timeout (s)' set to 4, 'Call Queuing Timeout (m)' set to 5, 'Service Busy Response' set to '486 - Busy Here', 'on No User Responding Send' set to '408-Request Timeout', and 'Action on CAC Location Limit' set to 'Allow Voicemail'.

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.

The screenshot shows the ARS configuration form with the following fields and values:

- ARS Route Id: 51
- Route Name: Showpilot
- Dial Delay Time: System Default (5)
- Description: (empty)
- Secondary Dial tone: ☐ (unchecked)
- SystemTone: (dropdown menu)
- Check User Call Barring: ☒ (checked)
- In Service: ☒ (checked) - Annotated with "CHECK IN SERVICE"
- Out of Service Route: <None>
- Time Profile: <None>
- Out of Hours Route: <None>
- Table with 4 columns: Code, Telephone Number, Feature, Line Group ID. One row is highlighted with a red border: Code: N, Telephone Number: N"@192.168.109.1", Feature: Dial, Line Group ID: 20. Annotated with "DEFINE SHORT CODE TO DIAL OUT WITH CORRECT LINE GROUP ID AS CONFIGURED IN SIP URI TAB."
- Alternate Route Priority Level: 3
- Alternate Route Wait Time: 30
- Alternate Route: <None>

Buttons on the right: Add..., Remove, Edit...

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 **Contact**.
- Check **Anonymous** to restrict caller identification on outbound call

User Voicemail DND ShortCodes Source Numbers Telephony Forwarding D

SIP Name 285 4

SIP Display Name (Alias) 285 4

Contact 285 4

DEFINE FIELDS AS PER INCOMING CALL ROUTE INCOMING NUMBER

☒ Anonymous

CHECK ANONYMOUS TO RESTRICT CALLER IDENTIFICATION ON OUTBOUND. LEAVE UNCHECKED TO SHOW PILOT ON OUTBOUND.

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.

Standard		Voice Recording	Destinations
Bearer Capability	Any Voice		
Line Group ID	19		
Incoming Number	285xxx4xx		
Incoming Sub Address			
Incoming CLI			
Locale			
Priority	1 - Low		
Tag			
Hold Music Source	System Source		
Ring Tone Override	None		

SET ANY VOICE FOR BEARER CAPABILITY

DEFINE INCOMING GROUP ID AS CONFIGURED IN SIP URI TAB

DEFINE INCOMING NUMBER. TESTING REQUIRED DROPPING THE LEADING ZERO FROM THE FNN.

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).

Standard		Voice Recording	Destinations
TimeProfile	Destination	Fallback Extension	
Default Value	404		

SELECT THE DESTINATION EXTENSION FROM THE PULL-DOWN MENU

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

Line Group ID	Incoming Number	Destination
19	285 4	404
19	285 4	405
19	285 4	780 9608G
19	285 4	770 9608
19	285 4	760 9611
19	285 4	200 Main

DEFINE INCOMING GROUP ID AS CONFIGURED IN SIP URI TAB

DEFINE INCOMING NUMBER. TESTING REQUIRED DROPPING THE LEADING ZERO FROM THE FNN.

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.

The screenshot shows the 'SIP Line' configuration window. At the top, there is a table with columns: URI, Groups, Local URI, Contact, Display Name, Identity, Header, Originator Number, Send Caller ID, Diversion Header, Credential, and Max Calls. Two rows are visible, with the second row highlighted in blue. Below the table, the 'Edit URI' section contains several fields. Annotations with arrows point to specific fields and sections:

- DEFINE LINE GROUP ID USED FOR INCOMING AND OUTGOING CALLS**: Points to the 'Outgoing Group' dropdown menu, which is set to '20'.
- DEFINE THESE SETTINGS TO ENABLE USER>SIP TAB AND GROUP>SIP TAB AND TO PRESENT CALLER ID OF THE PILOT ON OUTBOUND CALLS.**: Points to a red box containing three dropdown menus: 'Local URI' (set to 'Use Credentials User Name'), 'Contact' (set to 'Use Credentials User Name'), and 'Display Name' (set to 'Use Credentials User Name').
- DEFINE CREDENTIALS USED**: Points to the 'Send Caller ID' dropdown menu, which is set to 'None'.
- DEFINE MAX SIP TRUNK SESSIONS AS PER CURRENT SIP TRUNK CHANNELS LICENSE**: Points to the 'Max Sessions' spinner box, which is set to '10'.

Other visible settings include: 'Identity' set to 'None', 'Header' set to 'P Asserted ID', 'Originator Number' and 'Diversion Header' set to 'None', and 'Registration' set to '1: 285'.

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

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

The screenshot displays the 'SIP Advanced' configuration tab. The 'Addressing' section includes 'Association Method' (By Source IP address) and 'Call Routing Method' (Request URI). The 'Identity' section lists various identity-related options, with 'Send From In Clear' checked and highlighted by a red box and a yellow callout box stating 'CHECK SEND FROM IN CLEAR IF YOU WISH TO RESTRICT CALLER ID ON OUTBOUND'. The 'Media' section includes options like 'Allow Empty INVITE', 'Send Empty re-INVITE', and 'Indicate HOLD', with 'Indicate HOLD' checked and highlighted by a red box and a blue callout box stating 'CHECK INDICATE HOLD'. The 'Call Control' section shows settings for call initiation and queuing timeouts, service busy response, and action on CAC location limit.

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.

The screenshot shows the ARS configuration form with the following fields and values:

- ARS Route Id: 51
- Route Name: Showpilot
- Dial Delay Time: System Default (5)
- Description: (empty)
- Secondary Dial tone: ☐ (unchecked)
- System Tone: (dropdown menu)
- Check User Call Barring: ☒ (checked)
- In Service: ☒ (checked, highlighted with a red box and a blue arrow pointing to a "CHECK IN SERVICE" callout)
- Out of Service Route: <None>
- Time Profile: <None>
- Out of Hours Route: <None>

A table is displayed below the In Service field:

Code	Telephone Number	Feature	Line Group ID
N;	N"@192.168.109.1"	Dial	20

The table row is highlighted with a red box, and a blue arrow points to it from a callout box that says: "DEFINE SHORT CODE TO DIAL OUT WITH CORRECT LINE GROUP ID AS CONFIGURED IN SIP URI TAB."

Below the table, there are two more fields:

- Alternate Route Priority Level: 3
- Alternate Route Wait Time: 30
- Alternate Route: <None>

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

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (5)

Description:

☐ Secondary Dial tone: SystemTone

☒ Check User Call Barring

CHECK OUT OF SERVICE AND DEFINE OUT OF SERVICE ROUTE FORM AS BUILT IN PREVIOUS PICTURE

Out of Service Route: 51: Showpilot

Time Profile: <None>

Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
N;	N"@192.168.109.1"	Dial	19

Buttons: Add..., Remove, Edit...

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: <None>

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

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

User | Voicemail | DND | ShortCodes | Source Numbers | Telephony | Forwarding | D

SIP Name: 285 4

SIP Display Name (Alias): 285 4

Contact: 285 4

☒ Anonymous

DEFINE FIELDS AS PER INCOMING CALL ROUTE INCOMING NUMBER

CHECK ANONYMOUS TO RESTRICT CALLER IDENTIFICATION ON OUTBOUND. LEAVE UNCHECKED TO SHOW PILOT ON OUTBOUND.

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

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

The screenshot shows a configuration window with tabs: User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, and D. The 'Telephony' tab is active. Below the tabs are three text input fields: 'SIP Name', 'SIP Display Name (Alias)', and 'Contact'. Each field contains the text '285' followed by a red square icon and the number '4'. A red rectangular box encloses these three fields. A blue arrow points from a light blue text box to the right side of the 'SIP Display Name (Alias)' field. Below the input fields is a checkbox labeled 'Anonymous', which is checked. A red rectangular box encloses the 'Anonymous' checkbox. A blue arrow points from a yellow text box to the right side of the 'Anonymous' checkbox.

DEFINE FIELDS AS PER INCOMING CALL ROUTE INCOMING NUMBER

CHECK ANONYMOUS TO RESTRICT CALLER IDENTIFICATION ON OUTBOUND. LEAVE UNCHECKED TO SHOW PILOT NUMBER ON OUTBOUND.

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.

The screenshot shows the 'IP Office Line - Line 1' configuration window. It has tabs for 'Line', 'Short Codes', and 'VoIP Settings'. The 'Line' tab is active. The configuration is divided into several sections:

- Line Settings:**
 - Line Number: 1
 - Transport Type: WebSocket Server
 - Networking Level: SCN
 - Security: Medium
 - Telephone Number: (empty)
 - Prefix: (empty)
 - Outgoing Group ID: 99001
 - Number of Channels: 250
 - Outgoing Channels: 250
- Gateway:**
 - Address: 192 . 168 . 109 . 51
 - Location: Cloud
 - Password: (masked with dots)
 - Confirm Password: (masked with dots)
- SCN Resiliency Options:**
 - ☐ Supports Resiliency
 - ☐ Backs up my IP Phones
 - ☐ Backs up my Hunt Groups
 - ☐ Backs up my IP Dect Phones
- Description:** (empty text box)

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

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

The screenshot displays the 'IP Office Line - Line 1' configuration interface, specifically the 'VoIP Settings' tab. The interface includes a 'Codec Selection' section with 'Unused' and 'Selected' lists. The 'Fax Transport Support' dropdown is set to 'G.711'. The 'Allow Direct Media Path' checkbox is unchecked. A yellow callout points to the 'G.711' selection, and a blue callout points to the 'Allow Direct Media Path' checkbox.

IP Office Line - Line 1

Line Short Codes **VoIP Settings**

Codec Selection

System Default

Unused

G.722 64K

Selected

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

Out Of Band DTMF ☒

Allow Direct Media Path ☐

DEFINE SYSTEM CODECS

UNCHECK ALLOW DIRECT MEDIA PATH

Fax Transport Support G.711

SELECT G.711 TO ENABLE FAX TRANSPORT SUPPORT

Call Initiation Timeout (s) 4

Media Security Same as System (Disabled)

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.

ARS

ARS Route Id: 50

Route Name: Main

Dial Delay Time: System Default (1)

Description:

In Service: ☒ **Place in service**

Out of Service Route: <None>

Out of Hours Route: <None>

Code	Telephone Number	Feature	Line Group ID
?	.	Dial	99999

LINE GROUP ID OF IP OFFICE LINE IN EXPANSION SERVER

Alternate Route Priority Level: 3

Alternate Route Wait Time: 30

Alternate Route: <None>

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

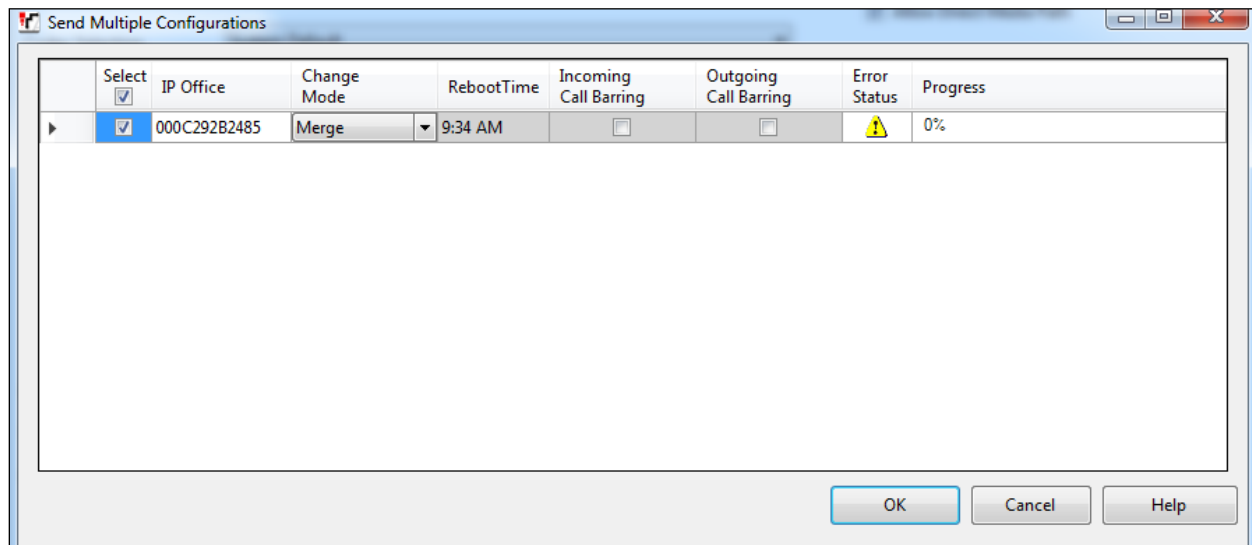
The screenshot shows the configuration interface for a user in IP Office Expansion. The 'SIP' tab is selected. The fields for 'SIP Name', 'SIP Display Name (Alias)', and 'Contact' are highlighted with a red box and contain the number 285-4. A blue callout box points to these fields with the text 'DEFINE FIELDS AS PER INCOMING CALL ROUTE INCOMING NUMBER'.

User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In
SIP Name							
SIP Display Name (Alias)							
Contact							

☐ Anonymous

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.

The screenshot shows the Avaya IP Office System Status application window. The title bar reads "Avaya IP Office System Status - 000C292B2485 (10.1.20.14) - IP Office Linux PC 10.1.0.1.0 build 3". The main window has a menu bar with "Help", "Snapshot", "LogOff", "Exit", and "About". A left-hand navigation pane lists various system components: System, Alarms (5), Extensions (0), Trunks (2), Line: 1, Line: 2 (selected), Active Calls, Resources, Voicemail, IP Networking, and Locations. The main content area is titled "IP Office System Status" and contains tabs for "Status", "Utilization Summary", and "Alarms". The "Status" tab is active, displaying the "SIP Trunk Summary" for Line 2. The summary shows the Line Service State as "In Service", Peer Domain Name as "192.168.109.1", Resolved Address as "10.1.20.9", Line Number as "2", Number of Administered Channels as "10", Number of Channels in Use as "0", Administered Compression as "G711 A, G711 Mu, G729 A", Enable Faststart as "Off", Silence Suppression as "Off", Media Stream as "RTP", Layer 4 Protocol as "TLS", SIP Trunk Channel Licenses as "10", SIP Trunk Channel Licenses in Use as "0", and SIP Device Features as "UPDATE (Incoming and Outgoing)". A green circle indicates 0% utilization. Below the summary is a table with columns for Channel, U., Call Ref, Curr... Time, Remote C..., Con..., Caller ID, Other Party o..., Dire..., Rou..., Rec..., Rec..., Tra..., and Tra... The table shows one entry with a "Round Trip Delay". At the bottom of the window, there are buttons for "Trace", "Trace All", "Pause", "Ping", "Call Details", "Graceful Shutdown", "Force Out of Service", "Print...", and "Save As...". The status bar at the bottom right shows the time "1:08:33 AM" and the status "Online".

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.

©2018 Avaya Inc. All Rights Reserved.

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

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