



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya IP Office 11 and Avaya Session Border Controller for Enterprise 8.0 with Optus Evolve Voice SIP Trunking Service - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Session Initiation Protocol (SIP) trunking between Avaya IP Office 11 and Avaya Session Border Controller (Avaya SBCE) 8.0 with Optus Evolve Voice.

The Optus Evolve Voice provides PSTN access via a SIP trunk connected to the Optus Voice over Internet Protocol (VoIP) network as an alternative to legacy analogue or digital trunks. Optus is a member of the Avaya DevConnect Service Provider program.

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.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	5
2.2	Test Results	6
2.3	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	8
5.	Configure Avaya IP Office	9
5.1	Verify System Capacity	10
5.2	LAN1 Settings.....	10
5.3	System Telephony Settings	12
5.4	VoIP Settings.....	13
5.5	SIP Line.....	13
5.5.1	SIP Line From Template.....	14
5.5.2	Manual SIP Line Configuration.....	15
5.6	Short Codes	19
5.7	ARS table	20
5.8	User	21
5.9	Incoming Call Route	23
5.10	Digital, Analog and T.38 Fax Extensions	24
5.11	Save Configuration.....	27
6.	Configure Avaya Session Border Controller for Enterprise	28
6.1	Device Management – Status	29
6.2	Server Interworking Profiles	31
6.2.1	Server Interworking – IP Office	31
6.2.2	Server Interworking – Optus EV	34
6.3	SIP Server Profiles	37
6.3.1	SIP Server – IP Office.....	37
6.3.2	SIP Server – Optus EV	39
6.4	Routing Profiles.....	41
6.4.1	Routing – To IP Office	41
6.4.2	Routing – To Optus EV	42
6.5	Topology Hiding	43
6.5.1	Topology Hiding – IP Office	43
6.5.2	Topology Hiding – Optus	43
6.6	Domain Policies	44
6.6.1	Application Rules.....	44
6.6.2	Border Rules	44
6.6.3	Media Rules	45
6.6.4	Signaling Rules	45
6.6.5	Endpoint Policy Groups	46
6.7	Network & Flows	46

6.7.1	Network Management.....	46
6.7.2	Media Interfaces.....	47
6.7.3	Signaling Interface	48
6.7.4	Endpoint Flows – For IP Office.....	49
6.7.5	Endpoint Flows – For Optus EV.....	50
7.	Verification Steps.....	51
7.1	IP Office Verification.....	51
7.2	Avaya Session Border Controller for Enterprise Verification	52
8.	Conclusion	55
9.	Additional References.....	56

1. Introduction

These Application Notes describe the procedures for configuring Avaya IP Office and Avaya Session Border Controller for Enterprise with Optus Evolve Voice SIP Trunking service. Customers using this Avaya SIP-enabled enterprise solution with Optus Evolve Voice 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 R11.0 and Avaya Session Border Controller for Enterprise 8.0 to connect to the Optus Evolve Voice. 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 this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Optus Evolve Voice do not include use of any specific encryption features.

2.1 Interoperability Compliance Testing

The compliance testing was based on the standard Avaya GSSCP test plan. The testing covered functionality required for compliance as a solution supported on the Optus Evolve Voice network. Calls were made to and from the PSTN across the Optus Evolve Voice network. The following standard features were tested as part of this effort:

- PSTN incoming and outgoing calls to/from various phone types supported by Avaya IP Office including H.323, SIP, analog and digital stations; and Avaya Equinox Softphone.
- Passing of DTMF events and their recognition by navigating Interactive Voice Response menus.
- PBX features such as hold, resume, conference and transfer.
- G.711A and G.729A audio codecs.
- Network Call Redirection.
- Dialing plan including local 8-digit number and 10-digit Full Nation Number (FNN), international number.
- Caller ID presentation and restriction.
- Faxing (T.38 fallback to G.711).
- Mobility: forwarding and mobile twining.

2.2 Test Results

Interoperability testing of Optus Evolve Voice SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Faxing** – Optus Evolve Voice supports Fax t.38 fallback to G.711 mode. At the time of compliance testing, there are circumstances t.38 was successfully negotiated between Optus Evolve Voice and Avaya Aura, but there is no t.38 fax data transmitted toward Avaya IP Office. Optus should continue investigating the issue from Optus Evolve Voice network to understand the issue.
- **Calling Party Number Restriction** – the Privacy header is not included in the outbound SIP INVITE when IP Office user uses WITHHOLD feature (or *67 short code) to make outbound call via SIP trunk. This results in pilot number is displayed on PSTN phone. In order to hide calling party number for outbound call via SIP trunk, Anonymous option should be checked under SIP tab of IP Office user configuration.
- **Off-net call forwarding** does not present original calling party number on the forward target. The pilot number is presented.
- **Transfer** – Original caller ID is not presented to transfer target in blind transfer scenario. While REFER is disabled, IP Office does not include the Diversion header in the outbound INVITE to transfer target, thus there is no original caller ID presented to transfer target.
- **Emergency ‘000’ Services Limitations and Restrictions** – Although Optus provides Emergency Services dialing on ‘000’, Optus does not warrant or represent that the equipment and software (e.g., IP PBX) reviewed in this customer configuration guide will properly operate with Optus Evolve SIP Trunking Service to complete ‘000’ calls; therefore, it is the customer’s responsibility to ensure proper operation with its equipment/software vendor.
While the Optus Evolve SIP Trunking Service does support ‘000’ calling capabilities under certain Calling Plans, there are circumstances when that ‘000’ service may not be available. Such circumstances include, but are not limited to, relocation of the end user’s CPE, use of a non-native or virtual telephone number, failure in the broadband connection, loss of electrical power, and delays that may occur in updating the customer’s location in the automatic location information database.
- **REFER must be disabled** on the Avaya IP Office SIP trunk to the Optus Evolve Voice Service as Optus Evolve Voice does not support REFER.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>
- **Optus:** Customers should contact their Optus Business representative or follow the support links available on <http://www.optus.com.au>

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 Application Server running on VMware ESXi 6.0.
- Avaya IP Office 500 V2.
- Avaya IP phones are represented with Avaya 9600 Series IP Telephones running SIP / H.323 software, Avaya 1600 Series IP Telephones running H.323 software
- Avaya Communicator for Windows 3.5.
- Avaya 1400 Series Digital Telephones.
- The Avaya SBCE 8.0 provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Optus Evolve Voice Service and the enterprise internal network.
- Optus Evolve Voice Service provided one trunk group. DID range assigned by Optus for this testing: 02xxxxx3xx (10 digits).

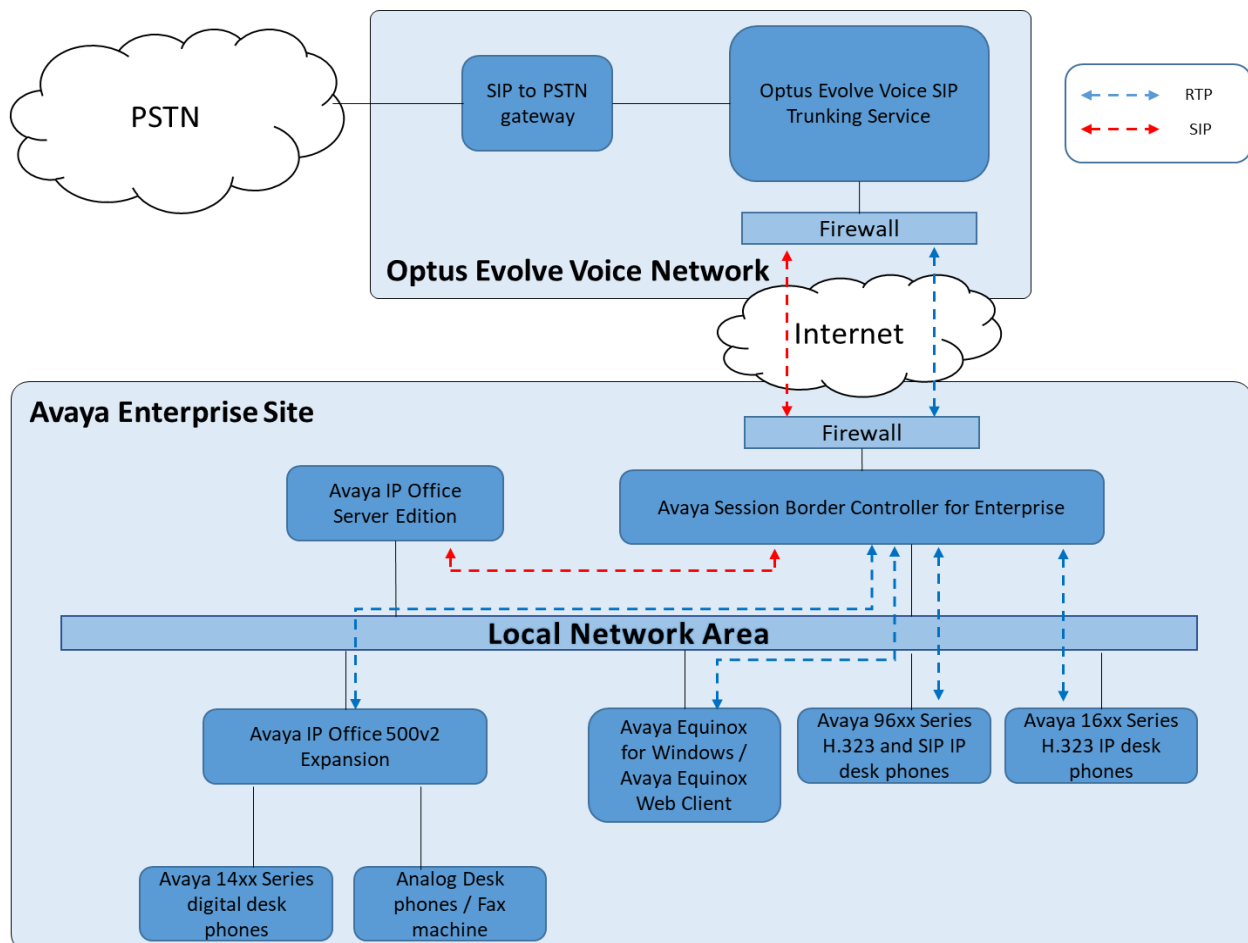


Figure 1: Test Setup Optus Evolve Voice to Avaya Enterprise

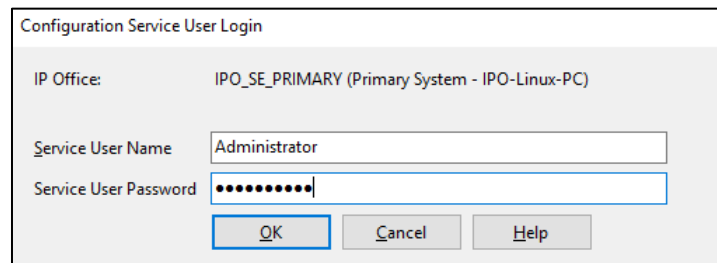
4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya IP Office Server Edition 11	11.0.4.0.74
Avaya IP Office 500 v2	11.0.4.0.74
Avaya Session Border Controller for Enterprise 8.0	8.0 - 8.0.0.0-19-16991
Avaya Equinox for Windows 3.5	3.5.7.30.1
Avaya 96x1 series – SIP phone	7.1.5
Avaya 96xx series – H.323 phone	3.2.8
Avaya 16xx series – H.323 phone	1.3.12
Service Provider – Optus Evolve Voice	
Genband CS2000	Release 18
Acme Packet SBC	SCZ7.2.0 MR-2 GA (Build 252)

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to Avaya SBCE. 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.



Configuration Service User Login

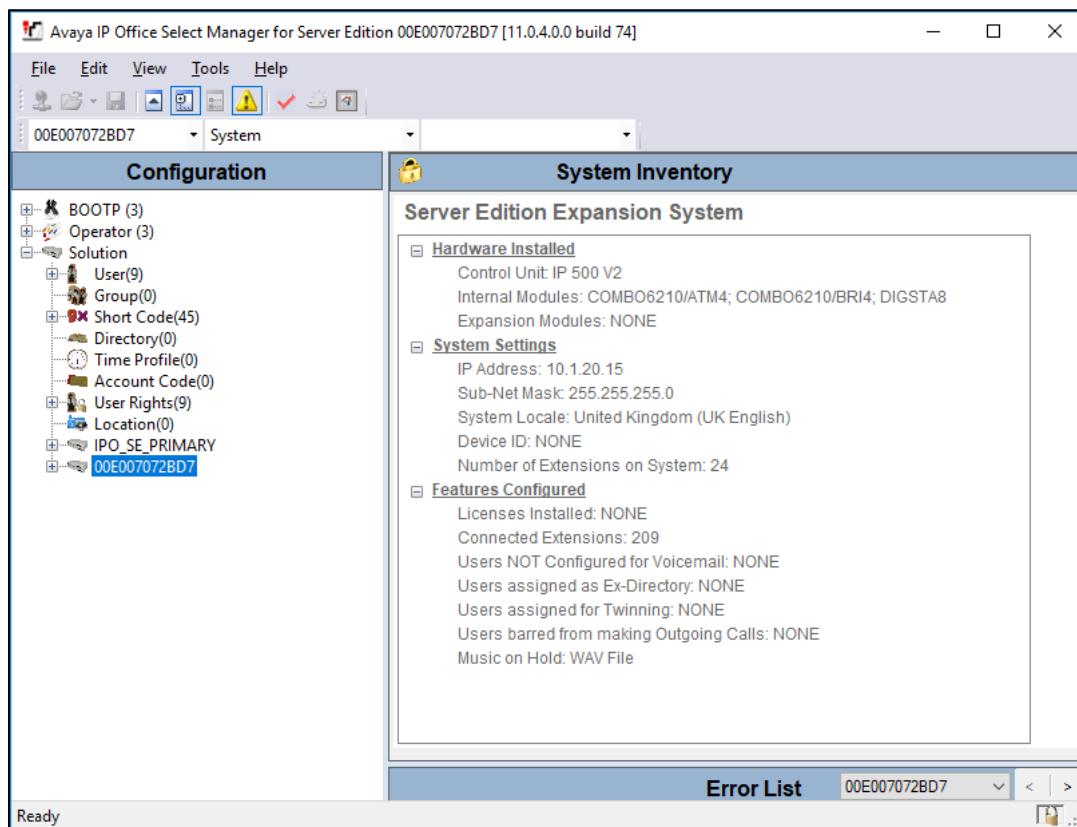
IP Office: IPO_SE_PRIMARY (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password:

Buttons: OK, Cancel, Help

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 Optus Evolve Voice Services.

The screenshot shows the Avaya IP Office Select Manager for Server Edition [11.0.4.0.0 build 74]. The interface is divided into three main panes: Configuration, License, and Error List. The License pane is active, displaying a table of licenses.

Feature	Instances	Status	Expiration Date
Power User	1000	Valid	Never
Avaya IP endpoints	1000	Valid	Never
SIP Trunk Channels	256	Valid	Never
CTI Link Pro	1	Valid	Never
3rd Party IP Endpoints	1000	Valid	Never
Server Edition	150	Valid	Never
UMS Web Services	1000	Valid	Never
Avaya Mac Softphone	1000	Valid	Never
Avaya Softphone Licence	1000	Valid	Never
SM Trunk Channels	128	Valid	Never
Web Collaboration	64	Valid	Never
Avaya Contact Center Select	1	Valid	Never
Allow Virtualization	10	Valid	Never
Devlink3 External Recorder	1	Valid	Never
Call Analytics	1000	Valid	Never
SP Soft Branding	1000	Valid	Never

5.2 LAN1 Settings

In the sample configuration, the LAN1 port was used to connect to Avaya SBCE. To access the LAN1 settings, first navigate to **System (1) > IPO_SE_PRIMARY** in the **Navigation** and **Group** panes and then navigate to the **LAN1 > LAN Settings** tab in the **Details** pane. Set the **DHCP Mode** to **Disabled**, then set the **IP Address** field to the IP address of 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 shows the Avaya IP Office Select Manager for Server Edition [11.0.4.0.0 build 74]. The interface is divided into three main panes: Configuration, System, and IPO_SE_PRIMARY. The IPO_SE_PRIMARY pane is active, displaying the LAN Settings tab.

System: LAN1

LAN Settings

IP Address: 10 . 1 . 20 . 14

IP Mask: 255 . 255 . 255 . 0

Number Of DHCP IP Addresses: 200

DHCP Mode: ☐ Server ☐ Client ☒ Disabled

Advanced

Select 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 Avaya SBCE. 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. The **Layer 4 Protocol** use **UDP/TCP** with port **5060** and **TLS** with port **5061**. 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 Avaya IP Office configuration interface, specifically the **VoIP** tab. The interface is divided into several sections:

- System Settings:** Includes tabs for LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The **VoIP** tab is selected.
- LAN Settings:** Includes sub-tabs for LAN Settings, VoIP, and Network Topology. The **VoIP** sub-tab is selected.
- H.323 Gatekeeper Enable:**
 - ☒ H.323 Gatekeeper Enable
 - ☐ Auto-create Extension
 - ☐ Auto-create User
 - ☐ H.323 Remote Extension Enable
 - H.323 Signaling over TLS: **Preferred** (dropdown)
 - Remote Call Signaling Port: **1720** (spin box)
- SIP Trunks Enable:**
 - ☒ SIP Trunks Enable
- SIP Registrar Enable:**
 - ☒ SIP Registrar Enable
 - ☐ Auto-create Extension/User
 - ☐ SIP Remote Extension Enable
 - Allowed SIP User Agents: **Block blacklist only** (dropdown)
 - SIP Domain Name: **sipinterop.net** (text box)
 - SIP Registrar FQDN: **sipinterop.net** (text box)
- Layer 4 Protocol:**
 - ☒ UDP: UDP Port **5060** (spin box), Remote UDP Port **5060** (spin box)
 - ☒ TCP: TCP Port **5060** (spin box), Remote TCP Port **5060** (spin box)
 - ☒ TLS: TLS Port **5058** (spin box), Remote TLS Port **5061** (spin box)
- Challenge Expiration Time (sec):** **10** (spin box)
- RTP:**
 - Port Number Range:**
 - Minimum: **40750** (spin box)
 - Maximum: **50750** (spin box)
 - Port Number Range (NAT):**
 - Minimum: **40750** (spin box)
 - Maximum: **50750** (spin box)
 - ☒ Enable RTCP Monitoring on Port 5005
 - RTCP collector IP address for phones: **0 . 0 . 0 . 0** (text box)
 - Keepalives:**
 - Scope: **Disabled** (dropdown)
 - Periodic timeout: **0** (spin box)
 - Initial keepalives: **Enabled** (dropdown)

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 **Unknown**. All other parameters should be set according to customer requirements.

The screenshot shows the 'Network Topology' configuration page. The 'Firewall/NAT Type' is set to 'Unknown'. Other fields include STUN Server Address, STUN Port (3478), Binding Refresh Time (0), Public IP Address (0.0.0.0), and Public Port (UDP, TCP, TLS all set to 0). There are 'Run STUN' and 'Cancel' buttons, and a checkbox for 'Run STUN on startup'.

5.3 System Telephony Settings

Navigate to **System (1) > IPO_SE_PRIMARY** 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 Time (sec)** to desired number.

The screenshot shows the 'System Telephony Settings' page. The 'Companding Law' is set to 'A-Law'. Other settings include Dial Delay Time (4), Dial Delay Count (0), Default No Answer Time (15), Hold Timeout (0), Park Timeout (300), Ring Delay (5), Call Priority Promotion Time (Disabled), Default Currency (AUD), Default Name Priority (Favor Trunk), Media Connection Preservation (Enabled), Phone Failback (Automatic), Login Code Complexity (Enforcement checked, Minimum length 6, Complexity checked), RTCP Collector Configuration (Send RTCP to an RTCP Collector unchecked, Server Address 0.0.0.0, UDP Port Number 5005, RTCP reporting interval 5), and various other checkboxes like DSS Status, Auto Hold, Dial By Name, Show Account Code, Inhibit Off-Switch Forward/Transfer, Restrict Network Interconnect, Include location specific information, Drop External Only Impromptu Conference, Visually Differentiate External Call, High Quality Conferencing, Directory Overrides Barring, Advertise Callee State To Internal Callers, and Internal Ring on Transfer.

5.4 VoIP Settings

Navigate to **System (1) > IPO_SE_PRIMARY** in the **Navigation** and **Group** panes and then navigate to the **VoIP** tab in the **Details** pane. Choose the **RFC2833 Default Payload** as IP Office default of **101**. Select codecs **G.711 ALAW 64K**, **G.11 ULAW 64K** and **G.729(a) 8K CS-ACELP** that Optus Evolve Voice supports.

The screenshot displays the VoIP configuration page within a web application. At the top, there is a navigation bar with tabs: System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, Contact Center, and Avaya Cloud Services. The 'VoIP' tab is active. Below the navigation bar, there are sub-tabs: VoIP, VoIP Security, and Access Control Lists. The 'VoIP' sub-tab is selected. The main configuration area includes several settings: 'Ignore DTMF Mismatch For Phones' is checked, 'Allow Direct Media Within NAT Location' is unchecked, and 'RFC2833 Default Payload' is set to '101'. Below these, there is a section for codec selection. It features three columns: 'Available Codecs', 'Default Codec Selection' (with 'Unused' and 'Selected' sub-sections), and 'Selected'. In the 'Available Codecs' column, four codecs are listed with checkboxes: G.711 ULAW 64K, G.711 ALAW 64K, G.722 64K, and G.729(a) 8K CS-ACELP. In the 'Unused' sub-section of the 'Default Codec Selection' column, 'G.722 64K' is listed. In the 'Selected' column, three codecs are listed: G.711 ALAW 64K, G.711 ULAW 64K, and G.729(a) 8K CS-ACELP. Navigation buttons (left arrow, right arrow, up arrow, down arrow) are located between the columns.

5.5 SIP Line

A SIP line is needed to establish the SIP connection between Avaya IP Office and Optus Evolve Voice Service. 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:

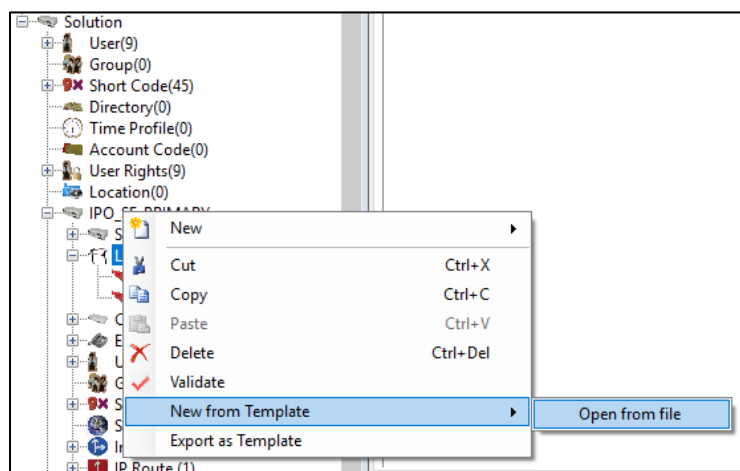
- SIP Line – Originator number for forwarded and twinning calls
- Transport – Second Explicit DNS Server
- SIP Credentials – Registration Required

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 → Open from file**



Navigate to the directory on the local machine where the template was copied and select the template (Not Shown). 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

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 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.
- Set **Location** to **Cloud**.
- Set **Country Code** to **61** (Country Code of Australia).
- Set **International Prefix** to **0011**.
- Set **National Prefix** to **0**.
- Set **Incoming Supervised REFER** to **Never**.
- Set **Outgoing Supervised REFER** to **Never**.

SIP Line		Transport	Call Details	VoIP	SIP Credentials	SIP Advanced	Engineering
Line Number	2	In Service		<input checked="" type="checkbox"/>			
ITSP Domain Name	sipinterop.net	Check OOS		<input checked="" type="checkbox"/>			
Local Domain Name	sipinterop.net						
URI Type	SIP URI						
Location	Cloud						
Prefix							
National Prefix	0						
International Prefix	0011						
Country Code	61						
Name Priority	System Default						
Description	SBCE-Optus-EV-Trunk						
		Session Timers					
		Refresh Method		Update			
		Timer (sec)		90			
		Redirect and Transfer					
		Incoming Supervised REFER		Never			
		Outgoing Supervised REFER		Never			
		Send 302 Moved Temporarily		<input type="checkbox"/>			
		Outgoing Blind REFER		<input type="checkbox"/>			

Select the **Transport** tab:

- The **ITSP Proxy Address** is set to the IP address of Avaya SBCE A1 Interface. As shown in **Figure 1**, this IP address is 10.1.20.9.
- In the **Network Configuration** area, **TCP** is selected as the Layer 4 Protocol, and the **Send Port** is set to **5060**. The **Use Network Topology Info** parameter is set to **None**. Other parameters retain default values in the screen below.
- Check **Calls Route via Registrar**.

The screenshot shows the 'Transport' tab of the SIP Line configuration interface. The 'ITSP Proxy Address' is set to '10.1.20.9'. Under the 'Network Configuration' section, 'Layer 4 Protocol' is set to 'TCP', 'Send Port' is '5060', 'Use Network Topology Info' is 'None', and 'Listen Port' is '5060'. The 'Explicit DNS Server(s)' are set to '0 . 0 . 0 . 0' and '0 . 0 . 0 . 0'. The 'Calls Route via Registrar' checkbox is checked. The 'Separate Registrar' field is empty.

SIP Line	Transport	Call Details	VoIP	SIP Credentials	SIP Advanced	Engineering
ITSP Proxy Address: 10.1.20.9						
Network Configuration						
Layer 4 Protocol		TCP		Send Port		5060
Use Network Topology Info		None		Listen Port		5060
Explicit DNS Server(s)		0 . 0 . 0 . 0		0 . 0 . 0 . 0		
Calls Route via Registrar		<input checked="" type="checkbox"/>				
Separate Registrar						

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 **Incoming Group**. This is the value assigned for incoming calls that is analyzed in the **Incoming Call Route** settings described in **Section 5.9**. In the test environment a value of **2** was used for the Optus Evolve Voice Service.
- 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 **2** was used.
- Set **Max Sessions** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.
- Set **Local URI**, **Contact**, **P Asserted ID** and **Diversion Header** to **Use Internal Data** for both the **Display name** and **Content**. On incoming calls, this will analyze the Request-Line sent by Optus Evolve Voice Service and match to the SIP settings in the User profile as described in **Section 5.8**. On outgoing calls this will insert the SIP settings in the User profile into the relevant headers in the SIP messages.
- Set the **Outgoing Calls**, **Forwarding/Twinning** and **Incoming Calls** at their respective values of **Caller**, **Original Caller** and **Called** for the **Local URI**, **Contact** and **P Asserted ID** call details. This ensures that the original called party number is sent for forwarded calls.

SIP Line - 2 | Call Details | SIP URI

New URI

Incoming Group: 2 Max Sessions: 10

Outgoing Group: 2

Credentials: 0: <None>

	Display	Content
Local URI	Use Internal Data	Use Internal Data
Contact	Use Internal Data	Use Internal Data
P Asserted ID	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data
P Preferred ID	<input type="checkbox"/> None	None
Diversion Header	<input checked="" type="checkbox"/> Use Internal Data	Use Internal Data
Remote Party ID	<input type="checkbox"/> None	None

Field meaning	
Outgoing Calls	Forwarding/Twinning
Caller	Original Caller
Caller	Original Caller
Caller	Original Caller
None	None
Caller	Original Caller
None	None

Incoming Calls
Called
Called
Called
None
None

OK Cancel Help

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.711 ALAW 64K**, **G.711 ULAW 64K** and **G.729(a) 8K CS-ACELP** codecs causes Avaya IP Office to include these codecs, which are supported by Optus Evolve Voice Service.
- Check the **Re-invite Supported** box.
- Check **Codec Lockdown** box.
- Uncheck **Allow Direct Media Path** box.
- Set **Fax Transport Support** to **T38 Fallback** from the pull-down menu as Optus Evolve Voice Service support T.38 fallback to G.711 pass-thru. At the time this testing happens, T.38 Fax is unsuccessful, the root cause is still unknown.
- Set the **DTMF Support** to **RFC2833/RFC4733** from the pull-down menu.
- Default values may be used for all other parameters.

The screenshot shows the 'VoIP' configuration tab for a SIP Line. The 'Codec Selection' section features a 'System Default' dropdown menu. Below it, there are two lists: 'Unused' containing 'G.722 64K' and 'Selected' containing 'G.711 ALAW 64K', 'G.711 ULAW 64K', and 'G.729(a) 8K CS-ACELP'. Between these lists are buttons for moving items: '>>>', '<<<', and '<<<' (for moving to unused) and '>>>' (for moving to selected). To the right of the codec lists are checkboxes for 'Local Hold Music' (unchecked), 'Re-invite Supported' (checked), 'Codec Lockdown' (checked), 'Allow Direct Media Path' (unchecked), 'Force direct media with phones' (unchecked), and 'PRACK/100rel Supported' (unchecked). Below the codec lists are three dropdown menus: 'Fax Transport Support' set to 'T38 Fallback', 'DTMF Support' set to 'RFC2833/RFC4733', and 'Media Security' set to 'Disabled'.

Select **SIP Advanced** tab:

- Check **Indicate HOLD** box.
- Default values may be used for all other parameters.

The screenshot shows the 'SIP Advanced' configuration tab. It includes sections for Addressing, Identity, Media, and Call Control. Key settings include 'Indicate HOLD' checked in the Media section and 'Cache Auth Credentials' checked in the Identity section.

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** (not shown). On the **Short Code** tab in the **Details** pane, configure the parameters as shown below:

- In the **Code** field, enter the dial string which will trigger this short code. The example shows “xxxxxxxx” which will be invoked when the user dials any 8-digit number.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to “N”.
- Set the **Line Group Id** to **51: Optus-EV**.
- Set **Locale** to **Australia (UK English)**.

The screenshot shows the 'Short Code' configuration form with the following values: Code: xxxxxxxx, Feature: Dial, Telephone Number: N, Line Group ID: 51: Optus-EV, and Locale: Australia (UK English).

5.7 ARS table

ARS Route ID 51 was selected to route outbound calls as defined in the Short Code in **Section 5.6**. That Short Code and the SIP Line created in **Section 5.5** must be added to this ARS Route ID as shown below.

The screenshot displays the configuration interface for an ARS (Automatic Route Selection) table. The main configuration area includes the following fields and options:

- ARS Route ID:** 51
- Route Name:** Optus-EV
- Dial Delay Time:** System Default (4)
- Description:** SBCE-Trunk-Optus-EV
- Secondary Dial tone:** ☒ (checked), SystemTone (dropdown)
- Check User Call Barring:** ☒ (checked)
- In Service:** ☒ (checked), Out of Service Route: <None> (dropdown)
- Time Profile:** <None> (dropdown), Out of Hours Route: <None> (dropdown)

Below these fields is a table for adding or managing routes:

Code	Telephone Number	Feature	Line Group ID
xxxxxxxx	N	Dial	2

Buttons for **Add...**, **Remove**, and **Edit...** are located to the right of the table.

Below the table, there are additional configuration options:

- Alternate Route Priority Level:** 3 (dropdown)
- Alternate Route Wait Time:** 30 (dropdown)
- Alternate Route:** <None> (dropdown)

5.8 User

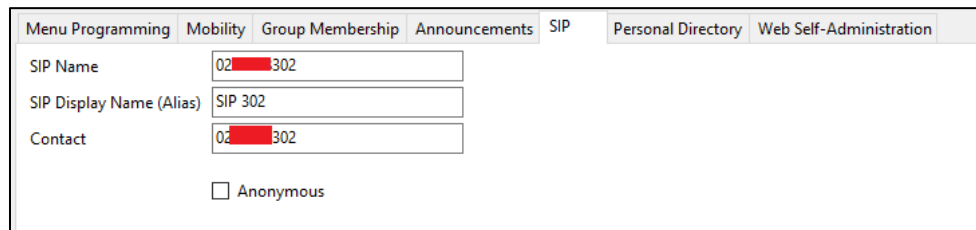
Configure the SIP parameters for each user that will be placing and receiving calls via the SIP line defined in **Section 5.5**. To configure these settings, first navigate to **User** in the Navigation Pane. Select the **User** tab if any changes are required.

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.

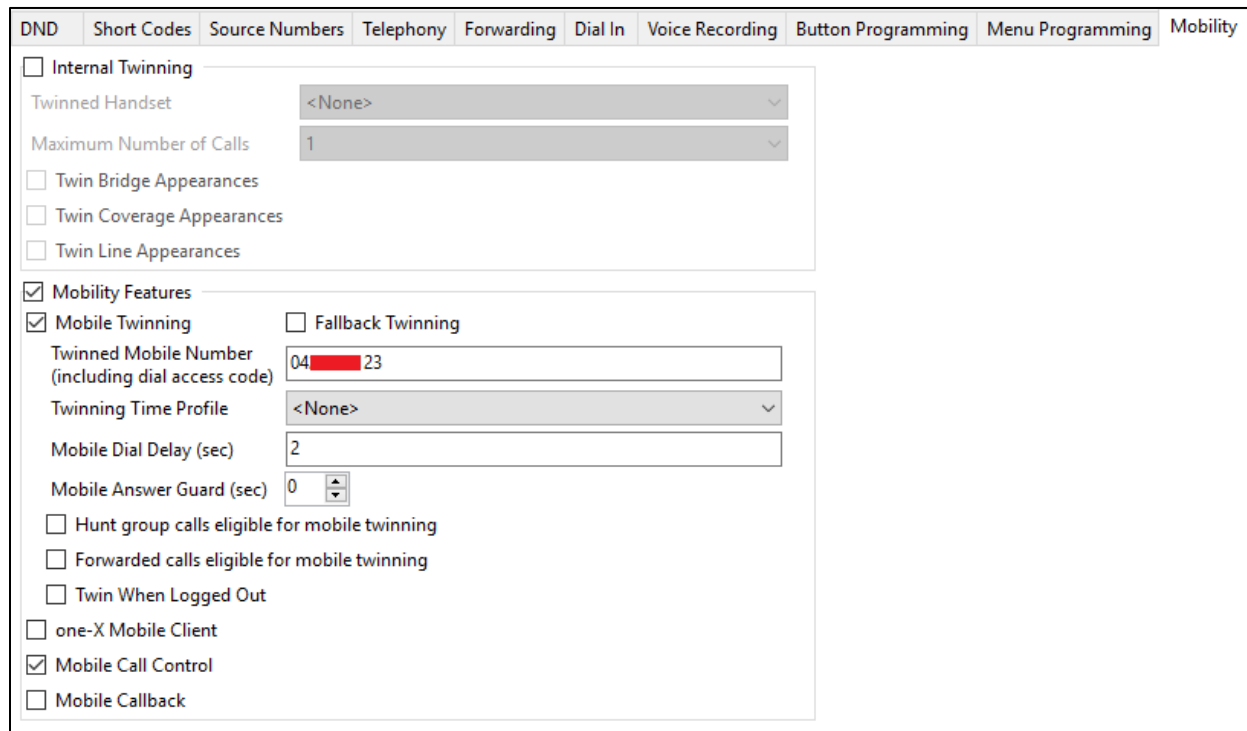
User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	<input type="text" value="H323 301"/>								
Password	<input type="password" value="•••••"/>								
Confirm Password	<input type="password" value="•••••"/>								
Unique Identity	<input type="text" value="h323.301@sipinterop.net"/>								
Conference PIN	<input type="password" value="•••••"/>								
Confirm Audio Conference PIN	<input type="password" value="•••••"/>								
Account Status	<input type="text" value="Enabled"/>								
Full Name	<input type="text" value="H323 301"/>								
Extension	<input type="text" value="301"/>								
Email Address	<input type="text"/>								
Locale	<input type="text" value="Australia (UK English)"/>								
Priority	<input type="text" value="5"/>								
System Phone Rights	<input type="text" value="None"/>								
Profile	<input type="text" value="Power User"/>								
	<input type="checkbox"/> Receptionist								
	<input checked="" type="checkbox"/> Enable Softphone								
	<input checked="" type="checkbox"/> Enable one-X Portal Services								
	<input checked="" type="checkbox"/> Enable one-X TeleCommuter								
	<input checked="" type="checkbox"/> Enable Remote Worker								
	<input checked="" type="checkbox"/> Enable Desktop/Tablet VoIP client								
	<input checked="" type="checkbox"/> Enable Mobile VoIP Client								
	<input type="checkbox"/> Send Mobility Email								

SIP endpoints require setting of the **SIP Registrar Enable** as described in **Section 5.2**. 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/P-Asserted-Identity/Contact** 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 Optus Evolve Voice.



Menu Programming	Mobility	Group Membership	Announcements	SIP	Personal Directory	Web Self-Administration
SIP Name		02 302				
SIP Display Name (Alias)		SIP 302				
Contact		02 302				
<input type="checkbox"/> Anonymous						

Optional: The following screen shows the **Mobility** tab for user 302. 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.



DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Programming	Mobility
<input type="checkbox"/> Internal Twinning									
Twinned Handset		<None>							
Maximum Number of Calls		1							
<input type="checkbox"/> Twin Bridge Appearances <input type="checkbox"/> Twin Coverage Appearances <input type="checkbox"/> Twin Line Appearances									
<input checked="" type="checkbox"/> Mobility Features									
<input checked="" type="checkbox"/> Mobile Twinning		<input type="checkbox"/> Fallback Twinning							
Twinned Mobile Number (including dial access code)		04 23							
Twinning Time Profile		<None>							
Mobile Dial Delay (sec)		2							
Mobile Answer Guard (sec)		0							
<input type="checkbox"/> Hunt group calls eligible for mobile twinning <input type="checkbox"/> Forwarded calls eligible for mobile twinning <input type="checkbox"/> Twin When Logged Out									
<input type="checkbox"/> one-X Mobile Client <input checked="" type="checkbox"/> Mobile Call Control <input type="checkbox"/> Mobile Callback									

5.9 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** (not shown). 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 5.5**.
- 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 02 have been masked due to security reasons.

Standard	Voice Recording	Destinations
Bearer Capability	Any Voice	
Line Group ID	2	
Incoming Number	02 301	
Incoming Sub Address		
Incoming CLI		
Locale		
Priority	1 - Low	
Tag		
Hold Music Source	System Source	
Ring Tone Override	None	

Select 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 DID number 02xxxxx301 on line 2 are routed to extension 301

Standard	Voice Recording	Destinations
	TimeProfile	Destination
▶	Default Value	301 H323 301

The following screen shows all the administered **Incoming Call Route** entries those are used in the compliance test

Configuration		Incoming Call Route		
		Line Group ID	Incoming Number	Destination
<ul style="list-style-type: none"> BOOTP (3) Operator (3) Solution <ul style="list-style-type: none"> User(9) Group(0) Short Code(45) Directory(0) Time Profile(0) Account Code(0) User Rights(9) Location(0) IPO_SE_PRIMARY <ul style="list-style-type: none"> System (1) Line (2) Control Unit (9) Extension (5) User (6) Group (0) Short Code (5) Service (0) Incoming Call Route (11) 		2	025 300	300 SIP 300
		2	025 301	301 H323 301
		2	025 302	302 SIP 302
		2	025 303	303 H323 303
		2	025 304	304 SIP 304
		2	025 305	305
		2	025 306	306
		2	025 307	307
		2	025 308	308
		2	025 398	FNE00
		2	025 399	VoiceMail

5.10 Digital, Analog and T.38 Fax Extensions

The compliance test with Optus Evolve Voice testing was also carried out with digital extensions and analog extensions including Fax machine on the IP Office Expansion. An IP Office line must be administered between IP Office Server Edition and IP Office Expansion (IP Office 500v2) with **T.38 Fallback** is configured as the fax transport

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

Configuration	Server Edition			
<ul style="list-style-type: none"> Solution <ul style="list-style-type: none"> User(9) Group(0) Short Code(45) Directory(0) Time Profile(0) Account Code(0) User Rights(9) Location(0) IPO_SE_PRIMARY <ul style="list-style-type: none"> System (1) Line (2) Control Unit (9) Extension (5) User (6) Group (0) Short Code (5) Service (0) Incoming Call Route (11) IP Route (1) License (28) 	<div>Line Short Codes VoIP Settings</div>			
	Line Number	1	Telephone Number	
	Transport Type	WebSocket Server	Prefix	
	Networking Level	SCN	Outgoing Group ID	99001
	Security	Medium	Number of Channels	250
			Outgoing Channels	250
	<div>Gateway</div>			
	Address	10 . 1 . 20 . 15		
	Location	Cloud		
	Password		
Confirm Password			
<div>SCN Resiliency Options</div> <div> <input type="checkbox"/> Supports Resiliency <div> <input type="checkbox"/> Backs up my IP phones <input type="checkbox"/> Backs up my hunt groups <input type="checkbox"/> Backs up my IP DECT phones </div> </div>				

In the **VoIP Settings** tab, select **T38 Fallback** from the **Fax Transport Support** drop down menu.

The screenshot shows the 'VoIP Settings' tab for a specific line. The 'Codec Selection' section has a 'System Default' dropdown. Below it are two lists: 'Unused' containing 'G.722 64K' and 'Selected' containing 'G.711 ALAW 64K', 'G.711 ULAW 64K', and 'G.729(a) 8K CS-ACELP'. Navigation arrows are between the lists. The 'Fax Transport Support' dropdown is set to 'T38 Fallback'. Other settings include 'Out Of Band DTMF' (checked), 'Allow Direct Media Path' (unchecked), 'Call Initiation Timeout (s)' set to 4, and 'Media Security' set to 'Same as System (Disabled)'.

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

The screenshot shows the 'IP Office Line - Line 17' configuration window. The 'Line' tab is active. Fields include: 'Line Number' (17), 'Transport Type' (WebSocket Client), 'Networking Level' (SCN), 'Security' (Medium), 'Telephone Number' (empty), 'Prefix' (empty), 'Outgoing Group ID' (99999), 'Number of Channels' (250), and 'Outgoing Channels' (250). The 'Gateway' section shows 'Address' (10.1.20.14), 'Port' (443), 'Location' (Cloud), 'Password' (masked), and 'Confirm Password' (masked). The 'SCN Resiliency Options' section has 'Supports Resiliency' (unchecked) and three sub-options: 'Backs up my IP phones', 'Backs up my hunt groups', and 'Backs up my IP DECT phones', all unchecked. A tree view on the left shows the system hierarchy with 'Line 17' selected.

In the **VoIP Settings** tab, select **T38 Fallback** from the **Fax Transport Support** drop down menu.

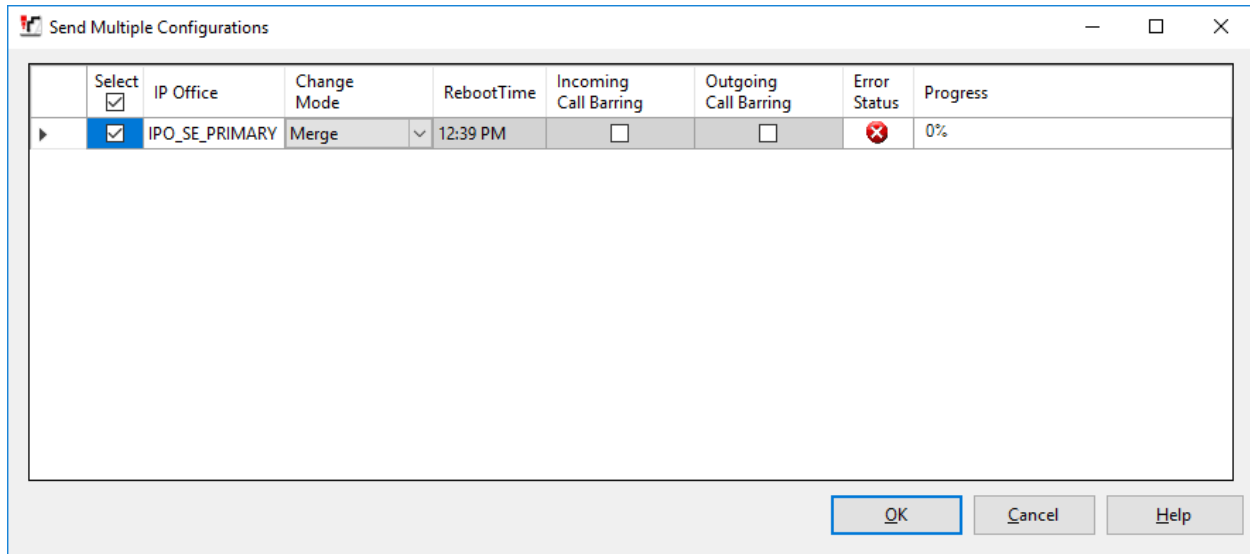
The screenshot shows the 'VoIP Settings' tab with the 'T38 Fax' sub-tab selected. The 'Codec Selection' section features a dropdown menu set to 'System Default'. Below this are two lists: 'Unused' containing 'G.722 64K' and 'G.723.1 6K3 MP-MLQ', and 'Selected' containing 'G.711 ALAW 64K', 'G.711 ULAW 64K', and 'G.729(a) 8K CS-ACELP'. Navigation buttons (left arrow, right arrow, up arrow, down arrow) are positioned between the lists. On the right side, there are three checkboxes: 'VoIP Silence Suppression' (unchecked), 'Out Of Band DTMF' (checked), and 'Allow Direct Media Path' (unchecked). At the bottom, the 'Fax Transport Support' dropdown is set to 'T38 Fallback', 'Call Initiation Timeout (s)' is set to '4', and 'Media Security' is set to 'Same as System (Disabled)'.

In the **T38 Fax** tab, check **Use Default Values**.


The screenshot shows the 'T38 Fax' tab with various configuration options. 'T38 Fax Version' is set to '3' and 'Transport' is set to 'UDPTL'. Under the 'Redundancy' section, 'Low Speed' and 'High Speed' are both set to '0'. 'TCF Method' is set to 'Trans TCF', 'Max Bit Rate (bps)' is '14400', 'EFlag Start Timer (ms)' is '2600', 'EFlag Stop Timer (ms)' is '2300', and 'Tx Network Timeout (sec)' is '150'. On the right, several checkboxes are present: 'Scan Line Fix-up' (checked), 'TFOP Enhancement' (checked), 'Disable T30 ECM' (unchecked), 'Disable EFlags For First DIS' (unchecked), 'Disable T30 MR Compression' (unchecked), and 'NSF Override' (unchecked). Below these, 'Country Code' and 'Vendor Code' are both set to '0'. At the bottom left, the 'Use Default Values' checkbox is checked.

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, Immediate, When Free** or **Timed** is shown under the **Configuration Reboot 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.



The image shows a Windows-style dialog box titled "Send Multiple Configurations". It contains a table with the following columns: "Select", "IP Office", "Change Mode", "RebootTime", "Incoming Call Barring", "Outgoing Call Barring", "Error Status", and "Progress". The first row of data is selected, showing "IPO_SE_PRIMARY" under "IP Office", "Merge" under "Change Mode", "12:39 PM" under "RebootTime", and "0%" under "Progress". The "Error Status" column shows a red "X" icon. At the bottom right of the dialog are three buttons: "OK", "Cancel", and "Help".

Select	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
<input checked="" type="checkbox"/>	IPO_SE_PRIMARY	Merge	12:39 PM	<input type="checkbox"/>	<input type="checkbox"/>		0%

6. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition resolved.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the Common site, (10.1.20.9), with access to the **Optus** site. The connection to Optus uses the Avaya SBCE public interface B1 (IP address 192.168.1.2). The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.



The screenshot shows the Avaya Session Border Controller for Enterprise login interface. On the left is the Avaya logo and the text "Session Border Controller for Enterprise". On the right, under the heading "Log In", there is a "Username:" label followed by a text input field containing "username". Below the input field is a "Continue" button. Further down, there is a "WELCOME TO AVAYA SBC" message, a disclaimer about unauthorized access, a consent statement, and a copyright notice: "© 2011 - 2019 Avaya Inc. All rights reserved."

3. Enter the password and click on **Log In**.



This screenshot shows the same Avaya Session Border Controller for Enterprise login interface as the previous one, but at the step where the password is entered. The "Username:" field now contains "username" and is highlighted. Below it, the "Password:" label is followed by a password input field containing eight dots. A "Log In" button is now visible below the password field. The rest of the page content, including the Avaya logo, disclaimer, and copyright notice, remains the same.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Session Border Controller for Enterprise AVAYA

Device: sbce | Alarms | Incidents | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

EMS Dashboard

- Device Management
- Backup/Restore
- System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
- Configuration Profiles
- Services
- Domain Policies
- TLS Management
- Network & Flows
- DMZ Services
- Monitoring & Logging

Dashboard

Information

System Time	08:21:01 PM AEST	Refresh
Version	8.0.0.0-19-16991	
Build Date	Sat Jan 26 21:58:11 UTC 2019	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	06/25/2019 19:47:08 AEST	
Failed Login Attempts	0	

Installed Devices

Device
sbce

Active Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

sbce: Heartbeat Successful, Server is UP
sbce: Heartbeat Successful, Server is UP
sbce: Heartbeat Successful, Server is UP
sbce: Heartbeat Successful, Server is UP

6.1 Device Management – Status

1. Select **Device Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.

Session Border Controller for Enterprise AVAYA

Device: sbce | Alarms | Incidents | Status | Logs | Diagnostics | Users | Settings | Help | Log Out

Device Management

EMS Dashboard | **Device Management** | Backup/Restore

- System Parameters
 - DoS / DDoS
 - Scrubber
 - User Agents
- Configuration Profiles

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status	
sbce	10.1.20.8	8.0.0.0-19-16991	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

- Click on **View** (shown above) to display the **System Information** screen. Note that DNS servers are Optus DNS servers and DNS client must be B1 IP address that is used for SIP trunk with Optus

System Information: sbce

General Configuration

Appliance Name

sbce

Box Type

SIP

Deployment Mode

Proxy

Device Configuration

HA Mode

No

Two Bypass Mode

No

License Allocation

Standard Sessions

Requested: 100

100

Advanced Sessions

Requested: 100

100

Scopia Video Sessions

Requested: 0

0

CES Sessions

Requested: 0

0

Transcoding Sessions

Requested: 0

0

CLID

Encryption

Available: Yes

☒

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.1.20.9	10.1.20.9	255.255.255.0	10.1.20.1	A1
10.1.20.19	10.1.20.19	255.255.255.0	10.1.20.1	A1
192.168.1.2	192.168.1.2	255.255.255.0	192.168.1.1	B1
192.168.1.3	192.168.1.3	255.255.255.0	192.168.1.1	B1
135.27.78.6	135.27.78.6	255.255.255.248	135.27.78.1	A2

DNS Configuration

Primary DNS

10.1.20.3

Secondary DNS

DNS Location

DMZ

DNS Client IP

192.168.1.2

Management IP(s)

IP #1 (IPv4)

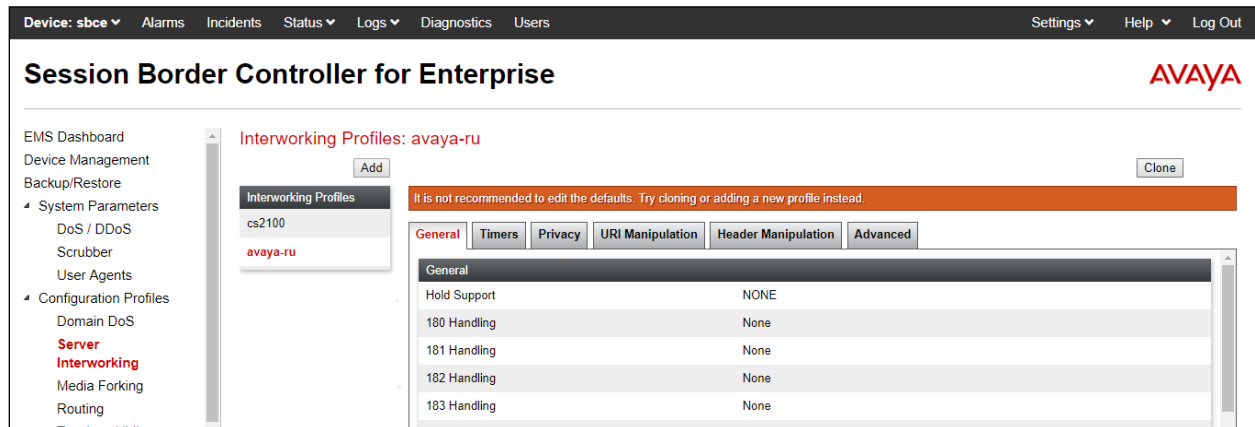
10.1.20.8

6.2 Server Interworking Profiles

6.2.1 Server Interworking – IP Office

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to IP Office.

1. Select **Configuration Profiles → Server Interworking** from the left-hand menu.
2. Select the pre-defined **avaya-ru** profile and click the **Clone** button.



3. Enter profile name: (e.g., **IP Office**), and click **Finish**.

The 'Clone Profile' dialog box is shown. It has a title bar 'Clone Profile' with a close button 'X'. Inside, there are two input fields: 'Profile Name' with the value 'avaya-ru' and 'Clone Name' with the value 'IP Office'. A 'Finish' button is located at the bottom center.

- The new **IP Office** profile will be listed. Select it, scroll to the bottom of the Profile screen, and click on **Edit**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right.

On the left, a sidebar menu lists various configuration options, including "Server Interworking" which is highlighted. The main content area is titled "Interworking Profiles: IP Office" and features a list of profiles on the left: "cs2100", "avaya-ru", "Session Manager", "Optus EV New", "Optus EV", and "IP Office" (which is selected and highlighted in red). An "Add" button is located above this list.

To the right of the profile list, there are buttons for "Rename", "Clone", and "Delete". Below these is a link that says "Click here to add a description." The main configuration area is divided into tabs: "General", "Timers", "Privacy", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is currently active.

Under the "General" tab, a table lists various configuration parameters and their values:

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

5. The **General** screen will open.

- Check **T.38 Support**.
- All other options can be left with default values, and click **Finish**.

Editing Profile: IP Office X

General

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None ▼
Send Hold	<input type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Finish

6. Leave settings in **Timer**, **Privacy**, **URI Manipulation**, **Header Manipulation** windows as default.
7. On the **Advanced** window, configure;
 - **Record Routes**: choose **Both Sides**.
 - **Has Remote SBC**: choose **Yes**.

The screenshot shows the 'Editing Profile: IP Office' window. The 'Record Routes' section has radio buttons for 'None', 'Single Side', 'Both Sides' (selected), 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'. The 'Include End Point IP for Context Lookup' checkbox is unchecked. The 'Extensions' dropdown is set to 'Avaya'. The 'Diversion Manipulation' checkbox is unchecked, and the 'Diversion Condition' dropdown is set to 'None'. The 'Diversion Header URI' field is empty. The 'Has Remote SBC' checkbox is checked. The 'Route Response on Via Port' checkbox is unchecked. The 'Relay INVITE Replace for SIPREC' checkbox is unchecked. The 'MOBX Re-INVITE Handling' checkbox is unchecked. The 'DTMF' section has radio buttons for 'None' (selected), 'SIP Notify', 'RFC 2833 Relay & SIP Notify', 'SIP Info', 'RFC 2833 Relay & SIP Info', and 'Inband'. A 'Finish' button is at the bottom.

6.2.2 Server Interworking – Optus EV

Repeat the steps shown in **Section 6.2.1** to add an Interworking Profile for the connection to Optus via the public network, with the following changes:

1. Click **Add** to add a new profile, enter **Optus EV** then click **Next** (not shown).
2. The **General** screen will open:
 - Check **T.38 Support**.
 - All other options can be left as default.
 - Click **Next**.
 - The **Privacy/DTMF**, **SIP Timers/Transport Timers** screens will open (not shown), accept default values for all the screens by clicking **Next**.

Editing Profile: Optus EV

X

General

Hold Support

☐ None
☐ RFC2543 - c=0.0.0.0
☒ RFC3264 - a=sendonly

180 Handling

☒ None ☐ SDP ☐ No SDP

181 Handling

☒ None ☐ SDP ☐ No SDP

182 Handling

☒ None ☐ SDP ☐ No SDP

183 Handling

☐ None ☒ SDP ☐ No SDP

Refer Handling

☐

URI Group

None

Send Hold

☐

Delayed Offer

☒

3xx Handling

☐

Diversion Header Support

☐

Delayed SDP Handling

☐

Re-Invite Handling

☐

Prack Handling

☐

Allow 18X SDP

☐

T.38 Support

☒

URI Scheme

☒ SIP ☐ TEL ☐ ANY

Via Header Format

☒ RFC3261
☐ RFC2543

Finish

The **Advanced** window is configured as below, click **Finish** to save the profile:

Editing Profile: Optus EV

Record Routes

☒ None

☐ Single Side

☐ Both Sides

☐ Dialog-Initiate Only (Single Side)

☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup

☐

Extensions

Nortel

Diversion Manipulation

☐

Diversion Condition

None

Diversion Header URI

Has Remote SBC

☒

Route Response on Via Port

☐

Relay INVITE Replace for SIPREC

☐

MOBX Re-INVITE Handling

☐

DTMF

DTMF Support

☒ None

☐ SIP Notify

☐ RFC 2833 Relay & SIP Notify

☐ SIP Info

☐ RFC 2833 Relay & SIP Info

☐ Inband

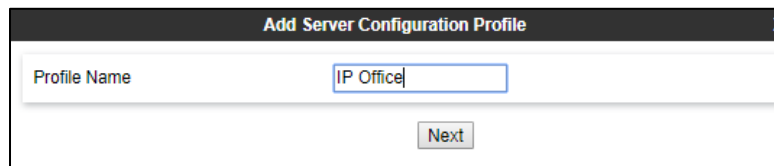
Finish

6.3 SIP Server Profiles

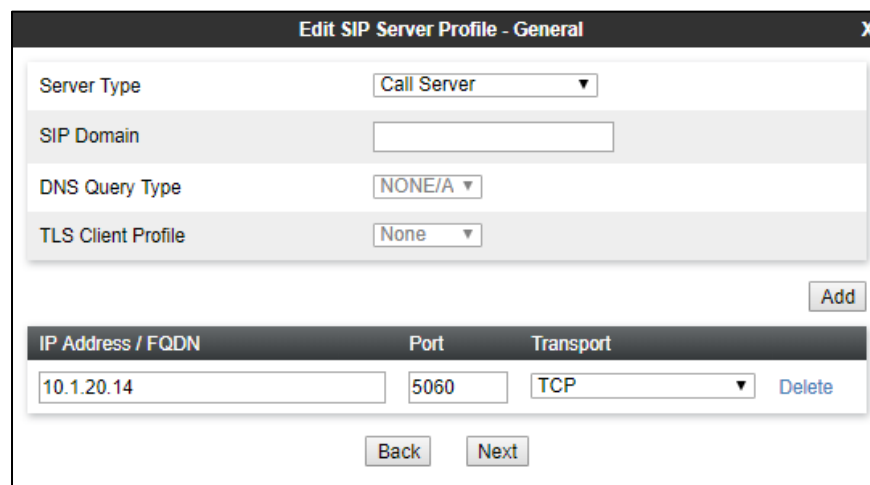
6.3.1 SIP Server – IP Office

This section defines the SIP Server Profile for the Avaya SBCE connection to IP Office.

1. Select **Services** → **SIP Server** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **IP Office**) and click **Next**.



3. The **Add SIP Server Profile** window will open.
 - Select **Server Type: Call Server**.
 - **IP Address / FQDN: 10.1.20.14** (IP Office Server LAN1 IP Address)
 - **Transport:** Select **TCP**.
 - **Port: 5060**.
 - Select **Next**.



4. The **Authentication** and **Heartbeat** windows will open (not shown).
 - Select **Next** to accept default values.

5. The **Advanced** window will open.
- For **Interworking Profile**, select the profile created for IP Office in **Section 6.2.1**.
 - Check **Enable Grooming**.
 - Select **Finish**.

Edit SIP Server Profile - Advanced [X]

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	IP Office ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

6.3.2 SIP Server – Optus EV

Repeat the steps in **Section 6.3.1**, with the following changes, to create a SIP Server Profile for the Avaya SBCE connection to Optus EV Trunk Group.

1. Select **Add Profile** and enter a Profile Name (e.g., **Optus EV**) and select **Next**.
2. On the **General** window (not shown), enter the following.
 - Select Server Type: **Trunk Server**.
 - **IP Address / FQDN**: **x.x.x.x** (outbound proxy of Optus).
 - **Transport**: Select **UDP**.
 - **Port**: **5060**.
 - Select **Next**.

Edit SIP Server Profile - General

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
x.x.x.x	5060	UDP

Delete

Back Next

3. Under **Heartbeat** window:
 - Select **Enable Heartbeat**.
 - **Method**: choose **OPTIONS**.
 - **Frequency**: enter **60**.
 - **From URI** and **To URI**: enter **sbc@sipinterop.net**.

Edit SIP Server Profile - Heartbeat

Enable Heartbeat: ☒

Method: OPTIONS

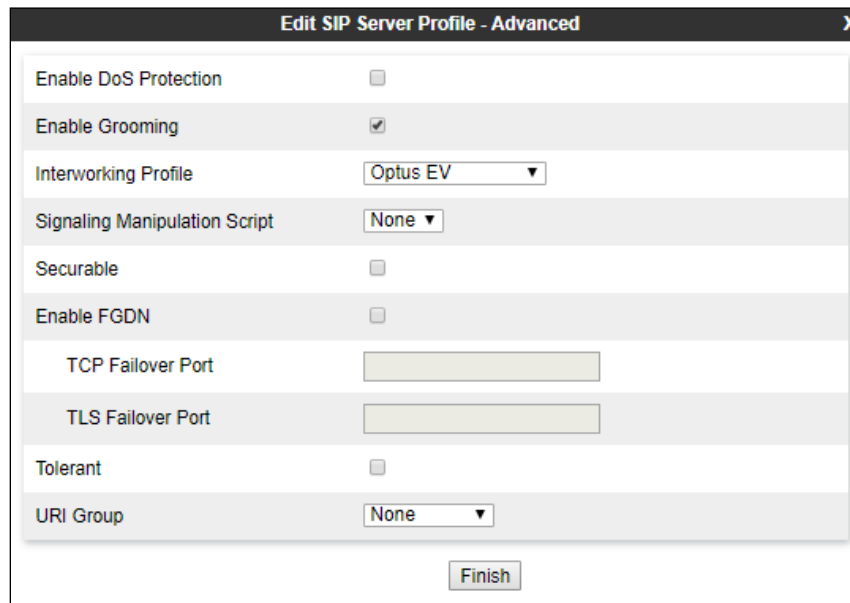
Frequency: 60 seconds

From URI: sbc@sipinterop.net

To URI: sbc@sipinterop.net

Finish

4. Under Advanced window:
- Check **Enable Grooming**.
 - Select **Optus EV** for Interworking Profile.



The screenshot shows a window titled "Edit SIP Server Profile - Advanced" with a close button (X) in the top right corner. The window contains a list of configuration options, each with a label and a control element (checkbox or dropdown menu). The options are: "Enable DoS Protection" (checkbox, unchecked), "Enable Grooming" (checkbox, checked), "Interworking Profile" (dropdown menu, set to "Optus EV"), "Signaling Manipulation Script" (dropdown menu, set to "None"), "Securable" (checkbox, unchecked), "Enable FGDN" (checkbox, unchecked), "TCP Failover Port" (text input field, empty), "TLS Failover Port" (text input field, empty), "Tolerant" (checkbox, unchecked), and "URI Group" (dropdown menu, set to "None"). A "Finish" button is located at the bottom right of the window.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Optus EV ▼
Signaling Manipulation Script	None ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	<input type="text"/>
TLS Failover Port	<input type="text"/>
Tolerant	<input type="checkbox"/>
URI Group	None ▼

Finish

6.4 Routing Profiles

6.4.1 Routing – To IP Office

This provisioning defines the Routing Profile for the connection to IP Office.

1. Select **Configuration Profiles** → **Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **IP Office**) and click **Next**.
3. The Routing Profile window will open. Using the default values shown, click on **Add**.
4. The Next-Hop Address window will open. Populate the following fields:
 - **Priority/Weight** = 1.
 - **SIP Server Profile** = **IP Office**.
 - **Next Hop Address**: Verify that the **10.1.20.14:5060 (TCP)** entry from the drop down menu is selected (IP Office Server LAN1 IP address). Also note that the **Transport** field is grayed out.
 - Click on **Finish**.

Profile : IP Office - Edit Rule

URI Group: *
Load Balancing: Priority
Transport: None
LDAP Server Profile: None
Matched Attribute Priority: ☐
Next Hop Priority: ☒
Ignore Route Header: ☐
ENUM: ☐
ENUM Suffix:
Time of Day: default
NAPTR: ☐
LDAP Routing: ☐
LDAP Base DN (Search): None
Alternate Routing: ☐
Next Hop In-Dialog: ☒
Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				IP Office	10.1.20.14:5060 ()	None

Finish

6.4.2 Routing – To Optus EV

Repeat the steps in **Section 6.4.1**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Optus.

1. On the **Configuration Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Optus EV**).
2. Load Balancing: select **Priority**.
3. On the **Next-Hop Address** window (not shown), populate the following fields:
 - **SIP Server Profile = Optus EV**.
 - **Next Hop Address**: Verify that the **x.x.x.x:5060** entry from the drop down menu is selected. Also note that the **Transport** field is grayed out.
 - Use default values for the rest of the parameters.
4. Click **Finish**.

Profile : Optus EV - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				Optus EV	x.x.x.x:5060	None

Delete

Finish

6.5 Topology Hiding

6.5.1 Topology Hiding – IP Office

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

1. Select **Configuration Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name:** (e.g., **IP Office**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly for all the headers.
4. Populate the fields as shown below, and click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand side menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The main area displays 'Topology Hiding Profiles: IP Office'. A table lists the configured headers and their replacement values.

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Overwrite	sipinterop.net
Referred-By	IP/Domain	Overwrite	sipinterop.net
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipinterop.net
SDP	IP/Domain	Overwrite	sipinterop.net
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sipinterop.net
Request-Line	IP/Domain	Overwrite	sipinterop.net

6.5.2 Topology Hiding – Optus

Repeat the steps in **Section 6.5.1**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Optus.

1. Enter a **Profile Name:** (e.g., **Optus EV**).
2. Click on the **Add Header** button repeatedly until all headers are added.
3. Populate the fields as shown below, and click **Finish**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand side menu is expanded to 'Configuration Profiles', and 'Topology Hiding' is selected. The main area displays 'Topology Hiding Profiles: Optus EV'. A table lists the configured headers and their replacement values.

Header	Criteria	Replace Action	Overwrite Value
Refer-To	IP/Domain	Overwrite	sip201.ippbx.optus.com.au
Referred-By	IP/Domain	Overwrite	sip201.ippbx.optus.com.au
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sip201.ippbx.optus.com.au
SDP	IP/Domain	Overwrite	sip201.ippbx.optus.com.au
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sip201.ippbx.optus.com.au
Request-Line	IP/Domain	Overwrite	sip201.ippbx.optus.com.au

6.6 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. Avaya SBCE has pre-defined / default Rules and Policies under Domain Policies. Although the default Rules and Policies are editable, it is highly recommended to clone the Rules and/or Policies before modification as needed. The compliance test was commenced using the default rules and policies without any modification.

6.6.1 Application Rules

Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 200 Voice sessions, and the default rule was amended accordingly. Other Application Rules could be utilized on an as needed basis.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Domain Policies" expanded to show "Application Rules". The main content area is titled "Application Rules: default" and features an "Add" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, a table lists application rules. The "default" rule is selected, showing details for Audio and Video sessions. The "Miscellaneous" section includes "CDR Support" (Off) and "RTCP Keep-Alive" (No).

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	5
Video	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous	
CDR Support	Off
RTCP Keep-Alive	No

6.6.2 Border Rules

The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface, specifically the "Border Rules" configuration page. The top navigation bar and header are consistent with the previous screenshot. The sidebar menu shows "Domain Policies" expanded to "Border Rules". The main content area is titled "Border Rules: default" and includes an "Add" button. A warning message states: "It is not recommended to edit the defaults. Try cloning or adding a new rule instead." Below this, a table lists border rules. The "default" rule is selected, showing details for "NAT Traversal". The "NAT Traversal" section includes "Enable Natting" (checked), "Use SIP Published IP" (checked), and "Use SDP Published IP" (checked).

NAT Traversal	
Enable Natting	<input checked="" type="checkbox"/>
Use SIP Published IP	<input checked="" type="checkbox"/>
Use SDP Published IP	<input checked="" type="checkbox"/>

6.6.3 Media Rules

This Media Rule will be applied to both directions and therefore, only one rule is needed. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

The screenshot shows the 'Media Rules: default-low-med' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules (selected), Security Rules, Signaling Rules, Charging Rules, End Point Policy, Groups, and Session Policies. The main content area has a header 'Media Rules: default-low-med' with an 'Add' button and a 'Clone' button. Below this is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration is divided into four tabs: Encryption, Codec Prioritization, Advanced, and QoS. The 'Encryption' tab is active, showing 'Audio Encryption' and 'Video Encryption' sections. Under 'Audio Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. Under 'Video Encryption', 'Preferred Formats' is set to 'RTP' and 'Interworking' is checked. A 'Miscellaneous' section at the bottom shows 'Capability Negotiation' is unchecked.

6.6.4 Signaling Rules

The default Signaling Rule was utilized. No customization was required.

The screenshot shows the 'Signaling Rules: default' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with options like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules (selected), Charging Rules, End Point Policy, Groups, and Session Policies. The main content area has a header 'Signaling Rules: default' with an 'Add' button and a 'Clone' button. Below this is a warning message: 'It is not recommended to edit the defaults. Try cloning or adding a new rule instead.' The configuration is divided into seven tabs: General, Requests, Responses, Request Headers, Response Headers, Signaling QoS, and UCID. The 'General' tab is active, showing 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. The 'Outbound' section shows 'Requests' set to 'Allow', 'Non-2XX Final Responses' set to 'Allow', 'Optional Request Headers' set to 'Allow', and 'Optional Response Headers' set to 'Allow'. The 'Content-Type Policy' section shows 'Enable Content-Type Checks' checked, 'Action' set to 'Allow', 'Multipart Action' set to 'Allow', and an 'Exception List'.

6.6.5 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was utilized. This rule incorporated the media and Signaling Rules specified above, as well as other policies.

Device: sbce Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

Policy Groups: default-low

It is not recommended to edit the defaults. Try cloning or adding a new group instead.

Click here to add a row description.

Order	Application	Border	Media	Security	Signaling	Charging	RTP Mon Gen
1	default	default	default-low-med	default-low	default	None	Off

6.7 Network & Flows

The **Network & Flows** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

6.7.1 Network Management

1. Select **Network & Flows** → **Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**. However, some of these values may not be changed if associated provisioning is in use.

Note: B1 has two IP Addresses configured for each interface. One is used for SIP trunking, another one is used for Remote worker. Configuration for Remote worker is out of scope of this document.

Device: sbce Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

Network Management

Interfaces Networks

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address
A1	10.1.20.1	255.255.255.0	A1	10.1.20.9, 10.1.20.19
B1-Optus	192.168.1.1	255.255.255.0	B1	192.168.1.2, 192.168.1.3

6.7.2 Media Interfaces

1. Select **Network & Flows** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Media_A1.
 - **IP Address:** 10.1.20.9 (Avaya SBCE A1 address).
 - **Port Range:** 35000-40000.
4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Optus media.
 - **IP Address:** 192.168.1.2 (Avaya SBCE B1 address).
 - **Port Range:** 35000-40000.
6. Click **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes 'Device: sbce', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar menu lists various management options, with 'Network & Flows' expanded to show 'Media Interface' as the selected option. The main content area, titled 'Media Interface', contains a table listing configured media interfaces. Each row includes the Name, Media IP Network, Port Range, and Edit/Delete actions. An 'Add' button is located in the top right corner of the table area.

Name	Media IP Network	Port Range	
Media_A1	10.1.20.9 A1(A1, VLAN 0)	35000 - 40000	Edit Delete
Optus media	192.168.1.2 B1-Optus (B1, VLAN 0)	35000 - 40000	Edit Delete
remote worker	192.168.1.3 B1-Optus (B1, VLAN 0)	35000 - 40000	Edit Delete
remote access	135.27.78.6 A2(A2, VLAN 0)	35000 - 40000	Edit Delete
Media_A1_RW	10.1.20.19 A1(A1, VLAN 0)	35000 - 40000	Edit Delete

6.7.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
 - **Name: Signaling_A1.**
 - **IP Address: 10.1.20.9** (Avaya SBCE A1 address).
 - **TCP Port: 5060.**
 - **UDP Port: 5060.**
 - **TLS Port: 5060.**
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
 - **Name: Optus Signaling.**
 - **IP Address: 192.168.1.2** (Avaya SBCE B1 address).
 - **TCP Port: 5060.**
 - **UDP Port: 5060.**
6. Click **Finish** (not shown). Note that changes to these values require an application restart.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar contains a menu with categories like EMS Dashboard, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, and Network & Flows. The 'Signaling Interface' page is active, showing a table of configured interfaces. An 'Add' button is visible in the top right of the table area.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Optus Signaling	192.168.1.2 B1-Optus (B1, VLAN 0)	5060	5060	---	None	Edit Delete
remote worker	192.168.1.3 B1-Optus (B1, VLAN 0)	5060	5060	5061	ServerB1	Edit Delete
Signaling_A1	10.1.20.9 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit Delete
Signaling_A1_RW	10.1.20.19 A1 (A1, VLAN 0)	5060	5060	5061	ServerA1	Edit Delete
remote access	135.27.78.6 A2 (A2, VLAN 0)	5060	5060	5061	ServerA1	Edit Delete

6.7.4 Endpoint Flows – For IP Office

1. Select **Device Specific Settings** → **Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
 - **Name:** IP Office.
 - **SIP Server Profile:** IP Office.
 - **URI Group:** *.
 - **Transport:** *.
 - **Remote Subnet:** *.
 - **Received Interface:** Optus Signaling.
 - **Signaling Interface:** Signaling_A1.
 - **Media Interface:** Media_A1.
 - **End Point Policy Group:** default-low.
 - **Routing Profile:** Optus EV.
 - **Topology Hiding Profile:** IP Office.
 - Let other values default.
4. Click **Finish**.

Edit Flow: IP Office	
Flow Name	IP Office
SIP Server Profile	IP Office
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Optus Signaling
Signaling Interface	Signaling_A1
Media Interface	Media_A1
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Optus EV
Topology Hiding Profile	IP Office
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

6.7.5 Endpoint Flows – For Optus EV

Repeat step **1** through **4** from **Section 6.7.4**, with the following changes:

- **Name: Optus EV.**
- **SIP Server Profile: Optus EV.**
- **URI Group: *.**
- **Transport: *.**
- **Remote Subnet: *.**
- **Received Interface: Signaling_A1.**
- **Signaling Interface: Optus Signaling.**
- **Media Interface: Optus media.**
- **End Point Policy Group: default-low.**
- **Routing Profile: IP Office.**
- **Topology Hiding Profile: Optus EV.**

Edit Flow: Optus EV	
Flow Name	Optus EV
SIP Server Profile	Optus EV
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Signaling_A1
Signaling Interface	Optus Signaling
Media Interface	Optus media
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	Session Manager
Topology Hiding Profile	Optus EV
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
Finish	

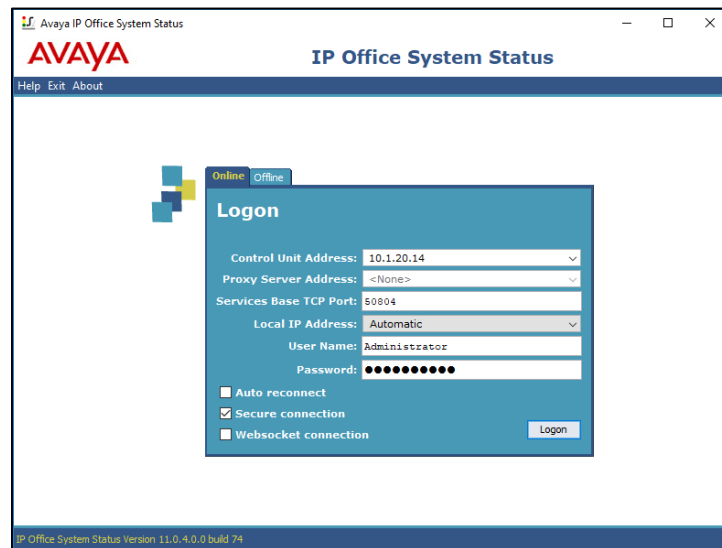
7. Verification Steps

The following steps may be used to verify the configuration.

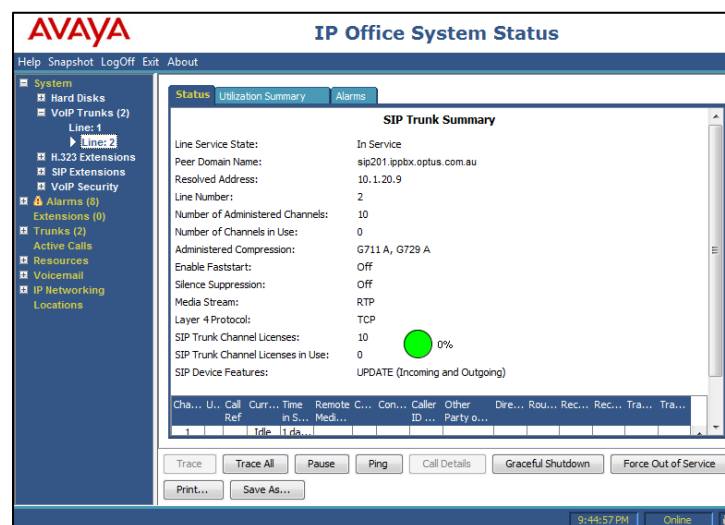
7.1 IP Office Verification

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

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



Select the **SIP Line** under **Trunks** from the left pane. On the **Status** tab in the right pane, verify the **Current State** is **Idle** for each channel.



7.2 Avaya Session Border Controller for Enterprise Verification

Log into the Avaya SBCE as shown in **Section 6**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Monitoring & Logging** → **Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **B1**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **10000**).
 - Specify a **Capture Filename** (e.g., **test.pcap**).
 - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
 - Click **Start Capture** to begin the trace.

The screenshot displays the Avaya SBCE web interface. At the top, a navigation bar includes links for Device: sbce, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads "Session Border Controller for Enterprise" with the Avaya logo on the right. A left-hand sidebar lists various management options, with "Monitoring & Logging" and "Trace" highlighted. The main content area, titled "Trace: sbce", contains two tabs: "Packet Capture" (active) and "Captures". Below the tabs is the "Packet Capture Configuration" form. This form includes fields for Status (Ready), Interface (B1), Local Address (192.168.1.2), Remote Address (*), Protocol (All), Maximum Number of Packets to Capture (10000), and Capture Filename (test.pcap). A note below the filename field states: "Using the name of an existing capture will overwrite it." At the bottom of the form are "Start Capture" and "Clear" buttons.

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address <small>(IP Port)</small>	192.168.1.2
Remote Address <small>(IP Port)</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test.pcap
<div>Start Capture Clear</div>	

The capture process will initialize and then display the following **In Progress** status window:

Device: sbceAlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & LoggingSNMPSyslog ManagementDebuggingTraceLog CollectionDoS LearningCDR Adjunct

Trace: sbce

Packet CaptureCaptures

A packet capture is currently in progress. This page will automatically refresh until the capture completes.

Packet Capture Configuration

StatusIn Progress

InterfaceB1

Local Address192.168.1.2Port

Remote AddressPort in IP Port

ProtocolAll

Maximum Number of Packets to Capture10000

Capture Filenametest.pcapUsing the name of an existing capture will overwrite it.

Stop Capture

3. Run the test.

4. When the test is completed, select the **Stop Capture** button shown above.

5. Click on the **Captures** tab and the packet capture is listed as a .pcap file with the date and time added to filename specified in **Step 2**.

6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

Device: sbceAlarmsIncidentsStatusLogsDiagnosticsUsersSettingsHelpLog Out

Session Border Controller for EnterpriseAVAYA

EMS DashboardDevice ManagementBackup/RestoreSystem ParametersConfiguration ProfilesServicesDomain PoliciesTLS ManagementNetwork & FlowsDMZ ServicesMonitoring & LoggingSNMPSyslog ManagementDebuggingTraceLog CollectionDoS LearningCDR Adjunct

Trace: sbce

Packet CaptureCaptures

Last ModifiedDescendingSortResetRefresh

File Name	File Size (bytes)	Last Modified	
long_call_20190703182356.pcap	952,560	July 3, 2019 6:24:11 PM AEST	Delete
long_call_20190703171957.pcap	2,373,471	July 3, 2019 5:20:42 PM AEST	Delete
incoming_fax_from_Awaya_20190703110033.pcap	2,335,680	July 3, 2019 11:02:05 AM AEST	Delete
7_4_6_20190703103026.pcap	1,945,600	July 3, 2019 10:31:03 AM AEST	Delete
7_4_5_20190703102932.pcap	2,224,128	July 3, 2019 10:30:21 AM AEST	Delete
7_4_2_20190703100118.pcap	1,851,392	July 3, 2019 10:02:09 AM AEST	Delete
7_11_10_directMedia_networking_20190703093937.pcap	1,404,928	July 3, 2019 9:40:07 AM AEST	Delete
7_11_10_directMedia_networking_20190703093832.pcap	1,019,904	July 3, 2019 9:38:57 AM AEST	Delete
7_11_10_fail_20190702191328.pcap	2,256,896	July 2, 2019 7:14:10 PM AEST	Delete
7_11_6_20190702191004.pcap	274,432	July 2, 2019 7:10:15 PM AEST	Delete

The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the Optus Evolve Voice Service and the customer SIP PABX is the customer SBC.

On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

Ping from the SBC to the Optus network gateway.

Ping from the SBC to the IP Office.

DNA; Reviewed:
SPOC 8/31/2019

Solution & Interoperability Test Lab Application Notes
©2019 Avaya Inc. All Rights Reserved.

53 of 57
OptusASBCEipo11

- Ping from the Optus network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Device: sbce
Help

Diagnostics

Full Diagnostic
Ping Test

Outgoing pings from this device can only be sent via the primary IP (determined by the OS) of each respective interface or VLAN.

Stop Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A2	A2 is operating within normal parameters with a full duplex connection at 1Gb/s.
⌛ SBC Link Check: B1	Running...
✗ Ping: SBC (A1) to Gateway (10.1.20.1)	
✗ Ping: SBC (A1) to Primary DNS (10.1.20.3)	
✗ Ping: SBC (B1) to Gateway (192.168.1.1)	
✗ Ping: SBC (B1) to Primary DNS (10.1.20.3)	
✗ Ping: SBC (A2) to Gateway (135.27.78.1)	
✗ Ping: SBC (A2) to Primary DNS (10.1.20.3)	

Help

Incident Viewer

Device: sbce
Category: All
Clear Filters
Refresh
Generate Report

Displaying results 466 to 480 out of 2001.

ID	Device	Date & Time	Category	Type	Cause
781109652777372	sbce	Jul 4, 2019 3:48:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109502774320	sbce	Jul 4, 2019 3:43:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109352774351	sbce	Jul 4, 2019 3:38:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109202773624	sbce	Jul 4, 2019 3:33:25 PM	Policy	Message Dropped	No Subscriber Flow Matched
781109148109554	sbce	Jul 4, 2019 3:31:36 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109148080928	sbce	Jul 4, 2019 3:31:36 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109084011121	sbce	Jul 4, 2019 3:29:28 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP
781109084006174	sbce	Jul 4, 2019 3:29:28 PM	Policy	Server Heartbeat	Heartbeat Successful, Server is UP

8. Conclusion

As illustrated in these Application Notes, Avaya IP Office 11 and Avaya Session Border Control for Enterprise 8.0 can be configured to interoperate successfully with Optus Evolve Voice SIP Trunking service. This solution allows enterprise users access to the PSTN using the Optus Evolve Voice SIP Trunking service connection. Please refer to **Section 2.2** for exceptions.

9. Additional References

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

- [1] *Avaya IP Office™ Platform Start Here First*, Release 11.0, May 2018.
- [2] *Avaya IP Office™ Platform Server Edition Reference Configuration*, Release 11.0, May 2018.
- [3] *Deploying IP Office™ Platform Server Edition Solution*, Release 11.0, May 2018.
- [4] *IP Office™ Platform 11.0, Deploying IP Office Essential Edition (IP500 V2)*, Document number 15- 601042, Feb 2019.
- [5] *IP Office™ Platform 11.0, Installing and Maintaining the Avaya IP Office™ Platform Application Server*, Document number 15-601011, Apr 2019.
- [6] *Administering Avaya IP Office™ Platform with Web Manager*, Release 11.0, May 2018.
- [7] *Administering Avaya IP Office™ Platform with Manager*, Release 11.0, May 2018.
- [8] *IP Office™ Platform 11.0, Using Avaya IP Office™ Platform System Status*, Document number 15-601758, Apr 2018.
- [9] *IP Office™ Platform 11.0, Using IP Office System Monitor*, Document number 15-601019, May 2018.
- [10] *Using Avaya Equinox for Windows on IP Office*, Release 11.0, Jun 2018.
- [11] *IP Office™ Platform 11.0 - Third-Party SIP Extension Installation Notes*, Apr 2018.
- [12] *Avaya IP Office Knowledgebase*, <http://marketingtools.avaya.com/knowledgebase>

©2019 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.