Avaya Solution & Interoperability Test Lab

Application Notes for Uecomm/Optus Evolve SIP Trunking Service with Avaya IP Office 9.1.6 and Avaya Session Border Controller for Enterprise 7.0 - Issue 1.0

Abstract

Uecomm UEConnect is a fully managed Communications as a Service (CaaS) solution, built on Avaya's well established IP Office application. UEConnect has been designed with SIP Trunks between Avaya Session Border Controllers for Enterprise and Optus Evolve SIP Trunking Service to secure and route all trunk-side SIP traffic to Optus. These Application Notes illustrate a sample configuration of Avaya IP Office in Uecomm UEConnect network with SIP Trunks to the Avaya Session Border Controller for Enterprise (Avaya SBCE) when used to connect to Optus Evolve SIP Trunking Service available from Optus (Australia).

Purely as an example, the lab setup is configured in a non-redundant configuration. Additional resiliency could be built in as per the standard supported configurations documented in other Avaya publications.

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

These Application Notes illustrate a sample configuration of Avaya IP Office Release 9.1.6 in Uecomm UEConnect network with SIP Trunks to the Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 when used to connect to Optus Evolve SIP Trunking Service available from Optus (Australia).

The Avaya SBCE is the point of connection between Avaya IP Office and Optus Evolve SIP Trunking Service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

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

2. General Test Approach and Test Results

The general test approach was to make calls through the Avaya SBCE while DoS policies are in place using various codec settings and exercising common and advanced PBX features.

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.

2.1 Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya IP Office, Avaya SBCE, and Optus Evolve SIP Trunking Service.

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

- SIP trunking (incoming and outgoing calls) with both Direct Media on and off.
- Passing of DTMF events and their recognition by navigating automated menus (interacting with IP Office Voicemail Pro)
- PBX features such as hold, resume, conference and transfer
- Mobile twinning – call extending to mobile
- G.711A and G.729A audio
- Basic IP Office Contact Center scenarios

- Remote Worker scenarios

2.2 Test Results

Interoperability testing of Uecomm/Optus Evolve SIP Trunking Service was completed with successful results for all test cases.

2.3 Support

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

3. Reference Configuration

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

- Avaya IP Office Server Edition running on VMware ESXi.
- Avaya IP Office Contact Center.
- Avaya IP phones are represented with Avaya 9600 Series and Avaya 1600 Series IP Telephones running H.323 software, and Avaya B179 SIP conference phone.
- Avaya Communicator for Windows 2.0
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Optus Evolve SIP Trunking Service and the enterprise internal network.
- Outbound calls were originated from a phone provisioned on Avaya IP Office. Signaling passed from Avaya IP Office to the Avaya SBCE, before being sent to the Telecom network for termination.
- Inbound calls were sent from Optus, through the Avaya SBCE to the Avaya IP Office. Avaya IP Office terminated the call to the appropriate phone extension.

All IP addresses shown in the diagram are private IP addresses.

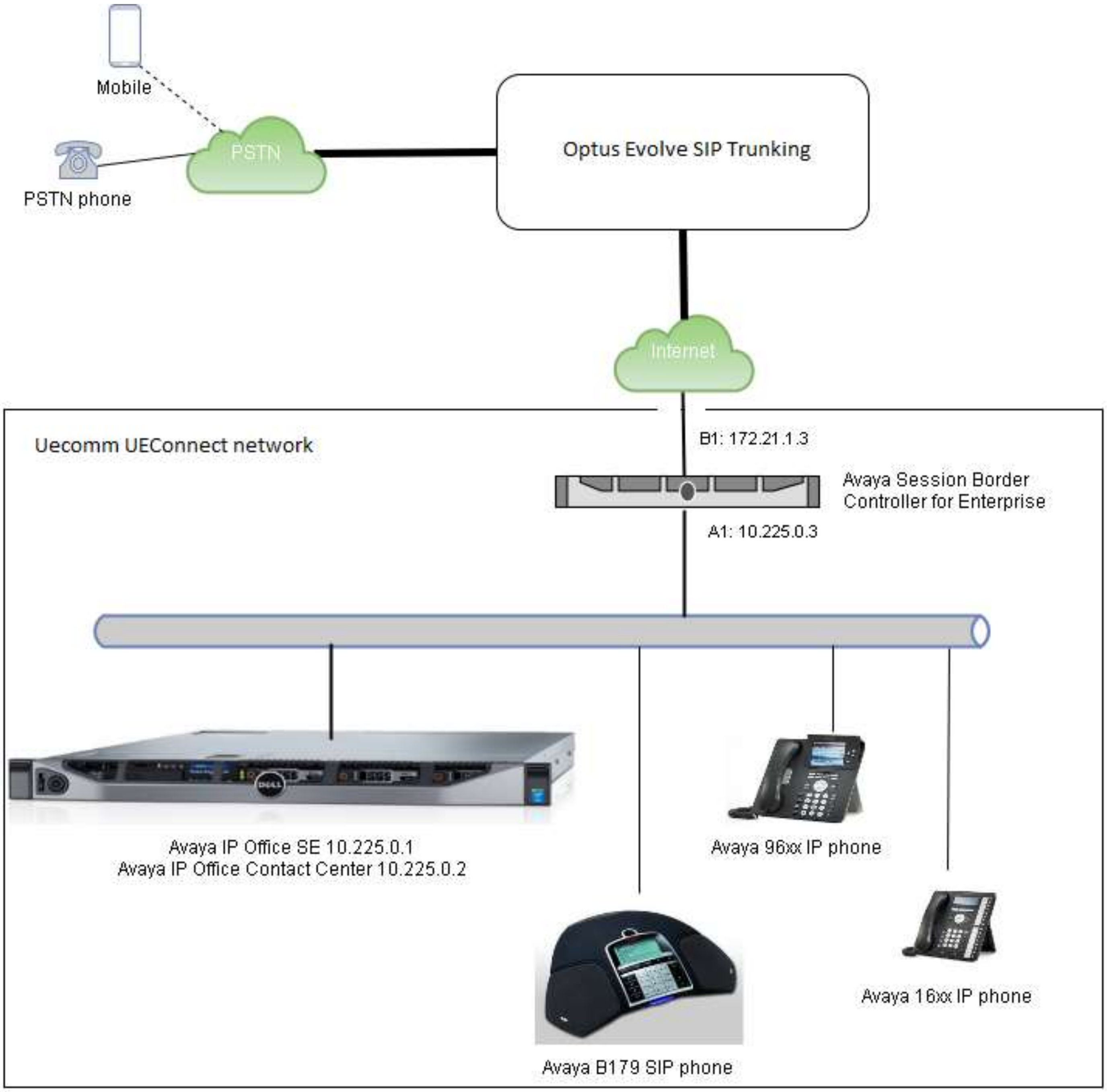


Figure 1: Network Components as Tested

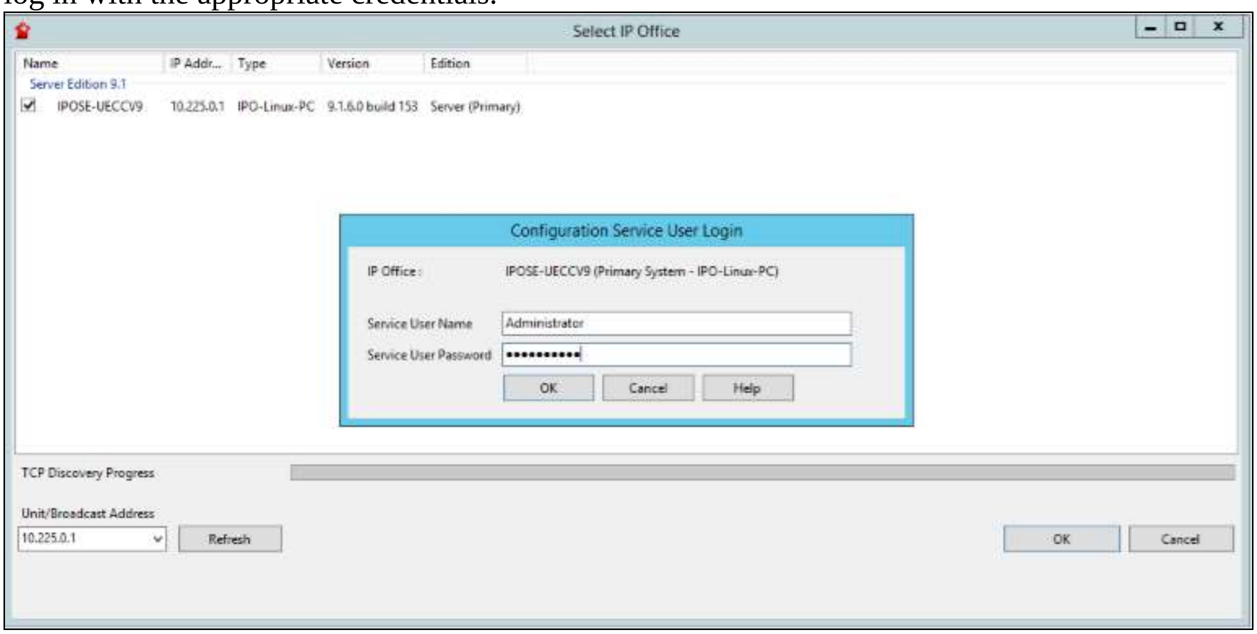
4. Equipment and Software Validated

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

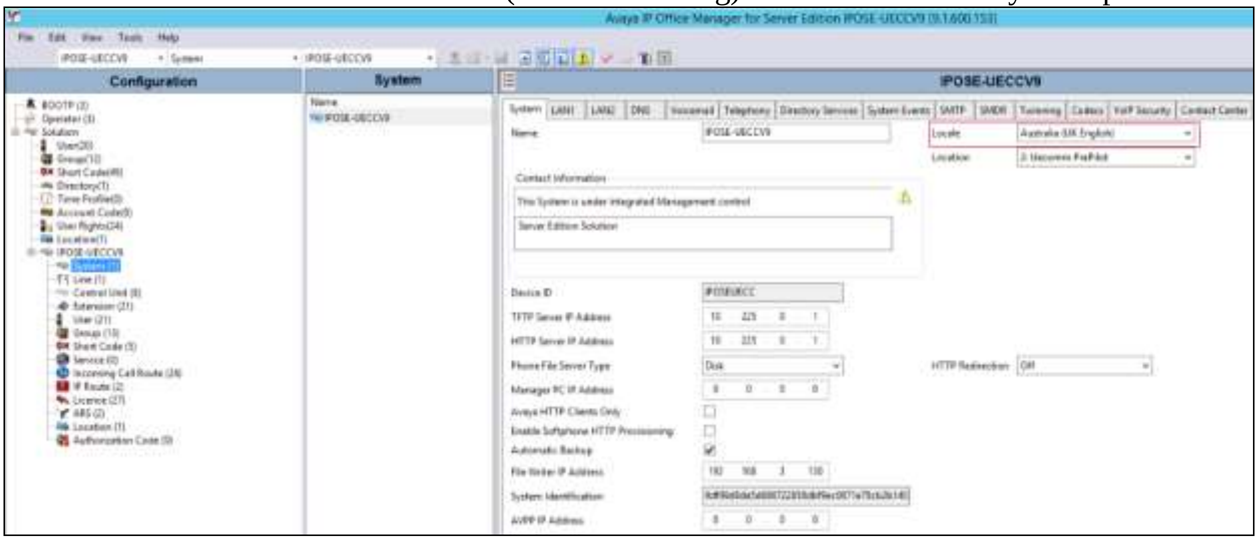
Component	Version
Avaya	
Avaya IP Office 9.1.6	9.1.600.153
Avaya IP Office Contact Center	9.1.2200.1448
Avaya Session Border Controller for Enterprise 7.0	7.0.0-21-6602
Avaya Communicator for Windows 2.0	2.0.3.40
Avaya B179 SIP	2.5.58020.0
Avaya 16xx Series Deskphone – H323 phone	1.3.8
Avaya 96xx Series Deskphone – H.323 phone	6.6.1.15
Service Provider	
Uecomm/Optus	Genband Q20 V8.3.8.2

5. Configure Avaya IP Office

This section describes the Avaya IP Office configuration to support connectivity to the Optus Evolve SIP Trunk via 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.

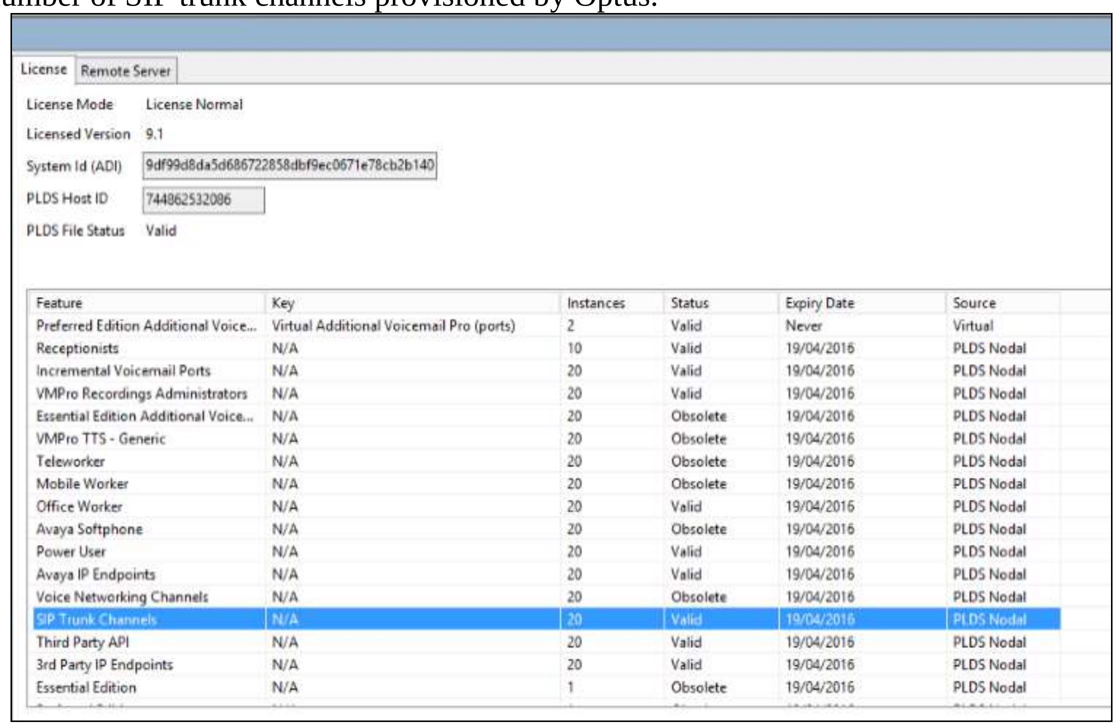


A management window will appear similar to the one in the next section. All the Avaya IP Office configurable components are shown in the left pane known as the Navigation Pane. The pane on the right is the Details Pane. These panes will be referenced throughout the Avaya IP Office configuration section.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



5.1 Verify System Capacity

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



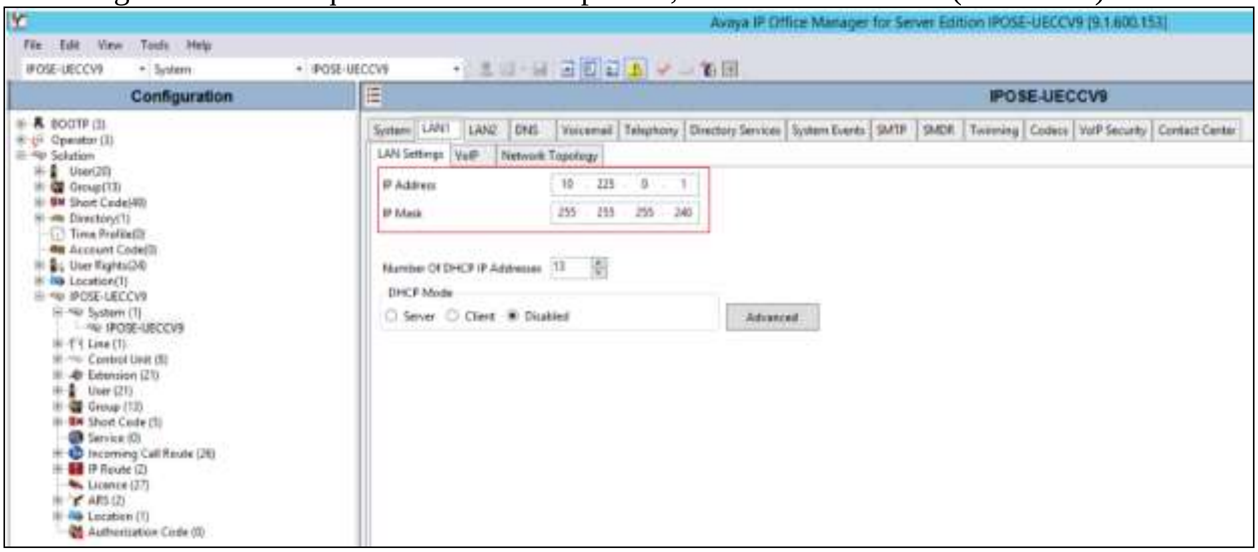
License | Remote Server

License Mode: License Normal
Licensed Version: 9.1
System Id (ADI): 9df99d8da5d686722858dbf9ec0671e78cb2b140
PLDS Host ID: 744862532086
PLDS File Status: Valid

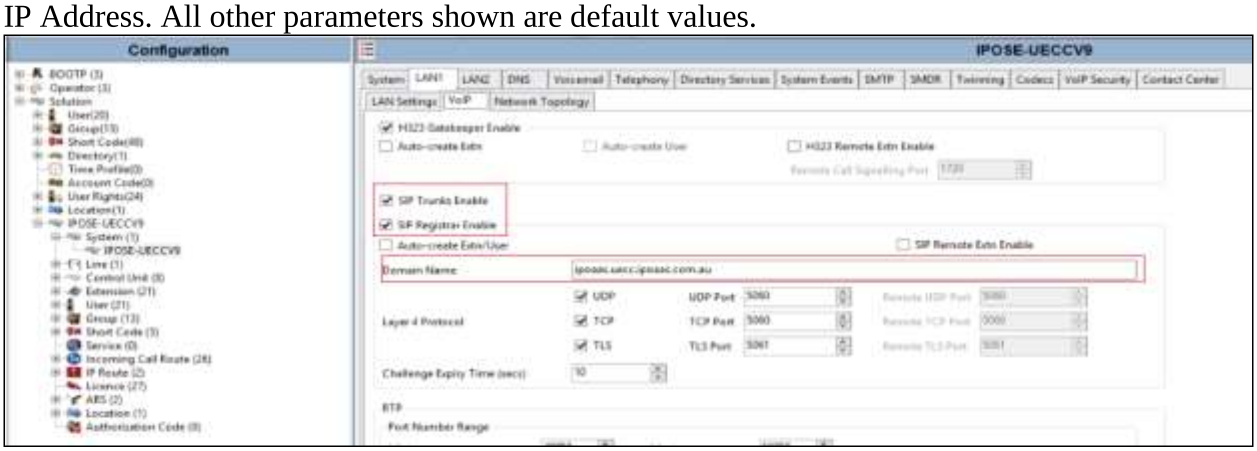
Feature	Key	Instances	Status	Expiry Date	Source
Preferred Edition Additional Voice...	Virtual Additional Voicemail Pro (ports)	2	Valid	Never	Virtual
Receptionists	N/A	10	Valid	19/04/2016	PLDS Nodal
Incremental Voicemail Ports	N/A	20	Valid	19/04/2016	PLDS Nodal
VMPro Recordings Administrators	N/A	20	Valid	19/04/2016	PLDS Nodal
Essential Edition Additional Voice...	N/A	20	Obsolete	19/04/2016	PLDS Nodal
VMPro TTS - Generic	N/A	20	Obsolete	19/04/2016	PLDS Nodal
Teleworker	N/A	20	Obsolete	19/04/2016	PLDS Nodal
Mobile Worker	N/A	20	Obsolete	19/04/2016	PLDS Nodal
Office Worker	N/A	20	Valid	19/04/2016	PLDS Nodal
Avaya Softphone	N/A	20	Obsolete	19/04/2016	PLDS Nodal
Power User	N/A	20	Valid	19/04/2016	PLDS Nodal
Avaya IP Endpoints	N/A	20	Valid	19/04/2016	PLDS Nodal
Voice Networking Channels	N/A	20	Obsolete	19/04/2016	PLDS Nodal
SIP Trunk Channels	N/A	20	Valid	19/04/2016	PLDS Nodal
Third Party API	N/A	20	Valid	19/04/2016	PLDS Nodal
3rd Party IP Endpoints	N/A	20	Valid	19/04/2016	PLDS Nodal
Essential Edition	N/A	1	Obsolete	19/04/2016	PLDS Nodal

5.2 LAN1 Settings

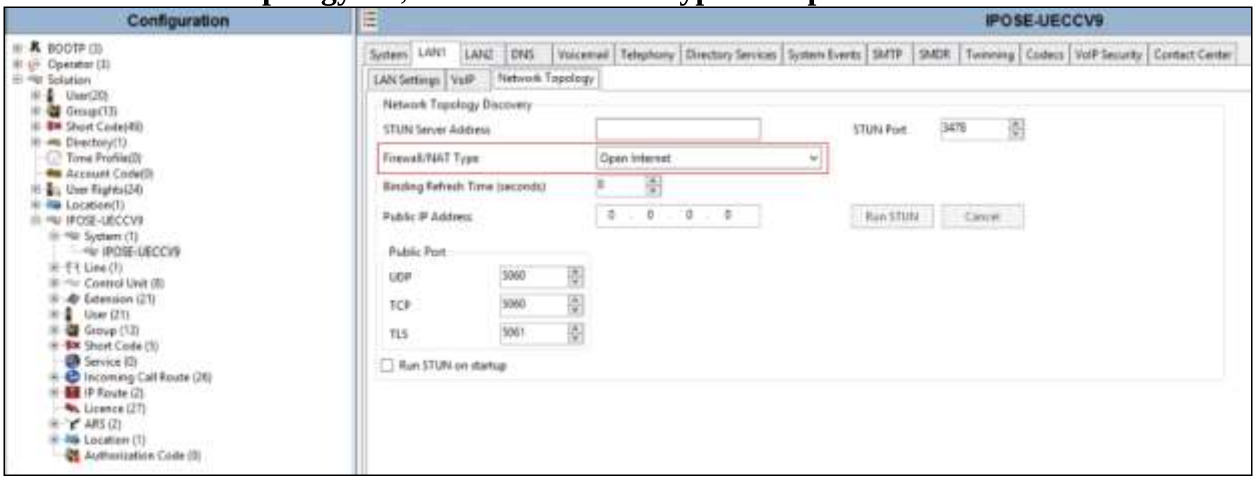
In the test configuration, the LAN1 port is used to configure the behavior of the services provided by the systems first LAN interface. To access the LAN1 settings, first navigate to **System → IPOSE-UECCV9** in the Navigation Pane where IPOSE-UECCV9 is the name of the IP Office. Navigate to the **LAN1 → LAN Settings** tab in the Details Pane. The **IP Address** and **IP Mask** fields are the private interface of the IP Office. All other parameters should be set according to customer requirements. On completion, click the **OK** button (not shown).



On the **VoIP** tab in the Details Pane, the **H323 Gatekeeper Enable** box is checked to allow the use of Avaya IP Telephones using the H.323 protocol. Check the **SIP Trunks Enable** box to enable the configuration of SIP trunks. If Avaya Communicator along with any other SIP endpoint is to be used, the **SIP Registrar Enable** box must also be checked. The Domain Name has been set to the customer premises equipment domain "**ipoaas.uecc.ipoaas.com.au**". If the Domain Name is left at the default blank setting, SIP registrations may use the IP Office LAN1 IP Address. All other parameters shown are default values.

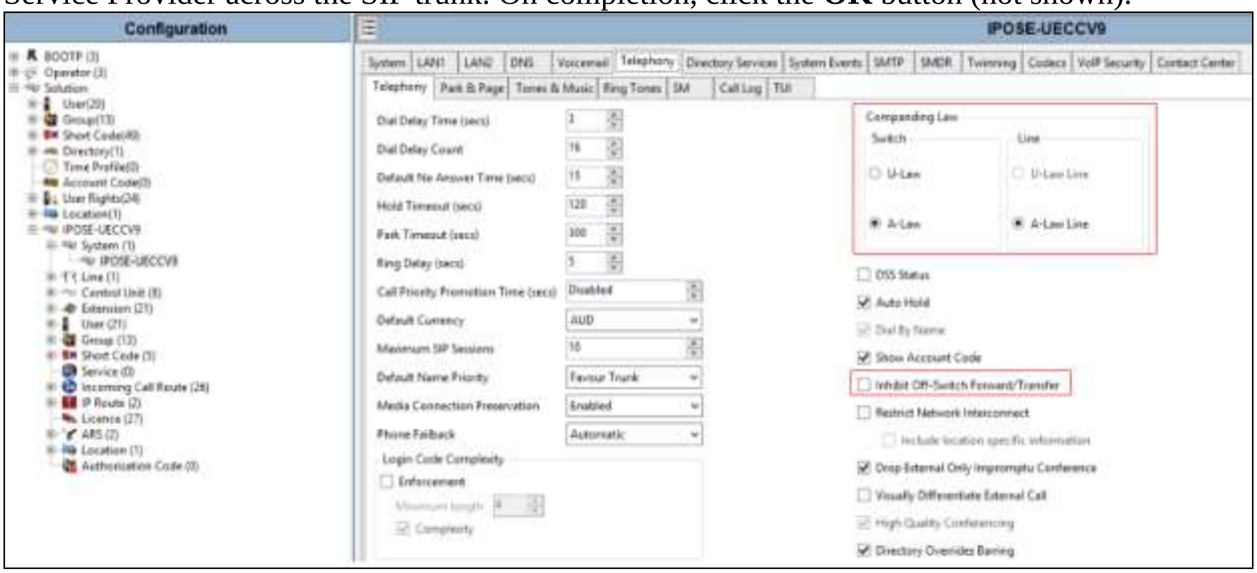


On the **Network Topology** tab, set **Firewall/NAT Type** to "**Open Internet**".



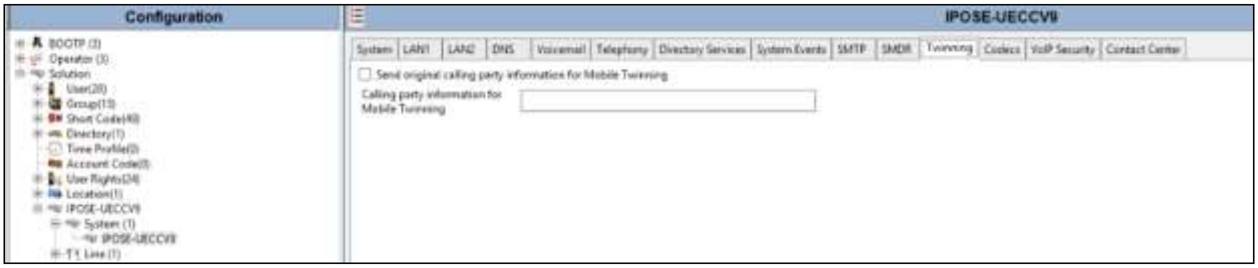
5.3 System Telephony Settings

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



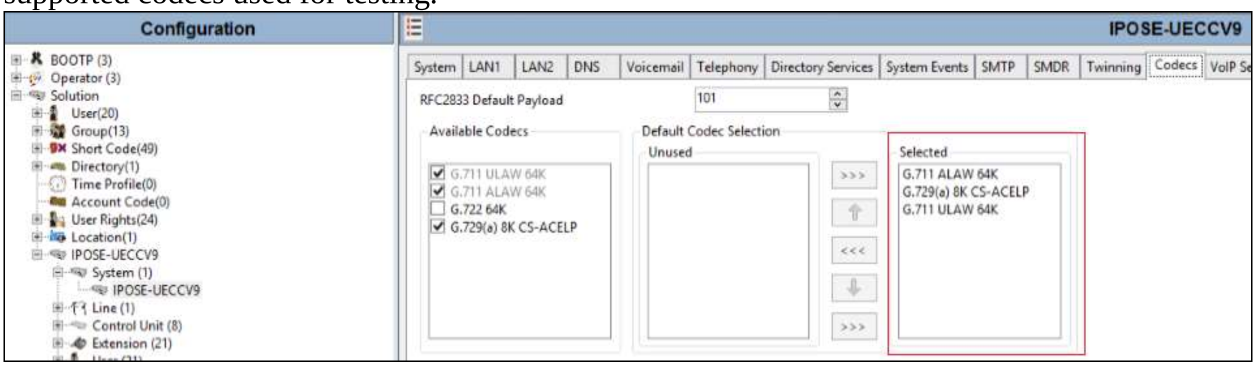
5.4 System Twinning Settings

To view or change Twinning settings, select the **Twinning** tab as shown in the following screen. The **Send original calling party information for Mobile Twinning** box is not checked, and the **Calling party information for Mobile Twinning** is left blank in the reference configuration. With this configuration, the true identity of a PSTN caller can be presented to the twinning destination (e.g., a user's mobile phone) when a call is twinned out via the Optus Evolve SIP Trunk.



5.5 Codec Settings

Navigate to the **Codecs** tab on the Details Pane. Check the available Codecs boxes as required. Once available codecs are selected, they can be used or unused by using the horizontal arrows as required. Note that in test, **G.711 ALAW 64K**, **G.711 ULAW 64K and G.729 (a) 8K** were the supported codecs used for testing.



5.6 SIP Line

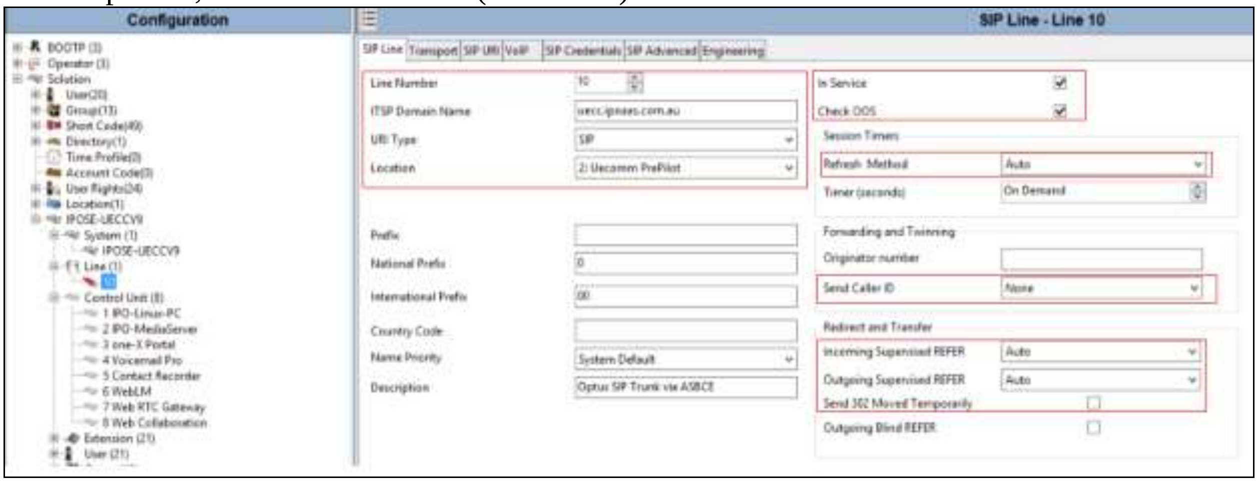
A SIP line is needed to establish the SIP connection between Avaya IP Office and Avaya SBCE for connection to the Optus Evolve SIP Trunk.

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

- Set **ITSP Domain Name** to a domain name provider by the Service Provider if required, however no ITSP Domain Name was used in this configuration.
- Ensure the **In Service** box is checked.
- Ensure the **Check OSS** box is checked.
- Set **Refresh Method** to **Auto**.
- Set **Send Caller ID** to **None**.
- Set **Incoming Supervised REFER** and **Outgoing Supervised REFER** to **Auto**.

- Ensure **Send 302 Moved Temporarily** is unchecked.
- Default values may be used for all other parameters.

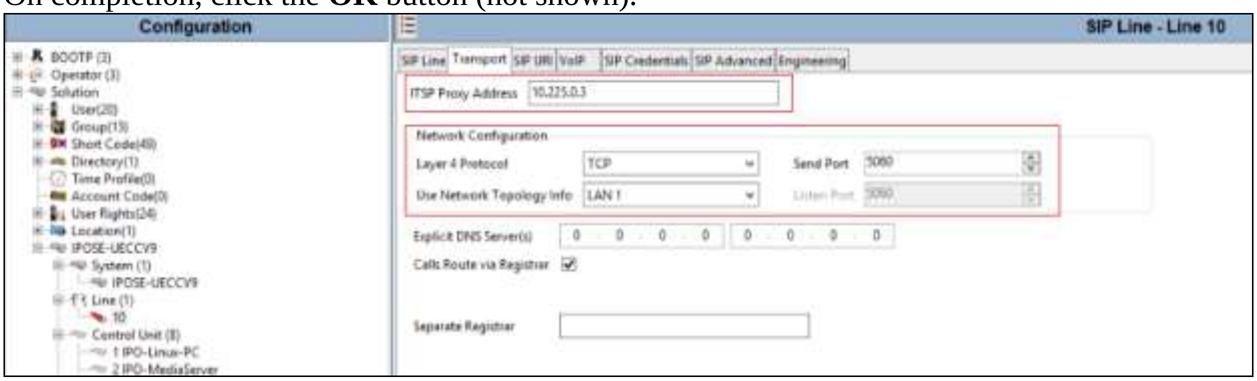
On completion, click the **OK** button (not shown).



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

- Set **ITSP Proxy Address** to the inside interface IP address of the Avaya SBCE as shown in **Figure 1**.
- Set **Layer 4 Protocol** to **TCP**.
- Set **Send Port** to **5060** and **Listen Port** to **5060**.
- Set **Use Network Topology Info** to **LAN1**.

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



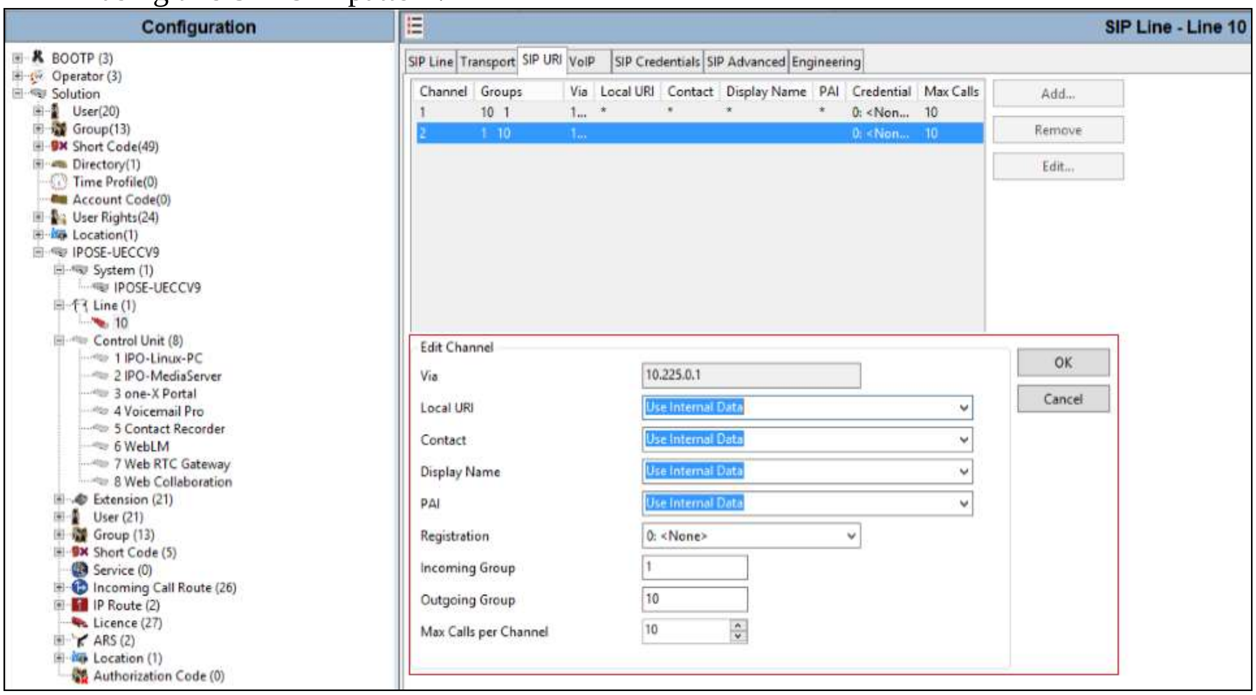
After the SIP line parameters are defined, the SIP URIs that Avaya IP Office will accept on this line must be created. To create a SIP URI entry, first select the **SIP URI** tab. Click the **Add** button and the **New Channel** area will appear at the bottom of the pane.

For the compliance test, two SIP URI entries were created that matched any number assigned to an Avaya IP Office user.

The first entry was created with the parameters shown below.

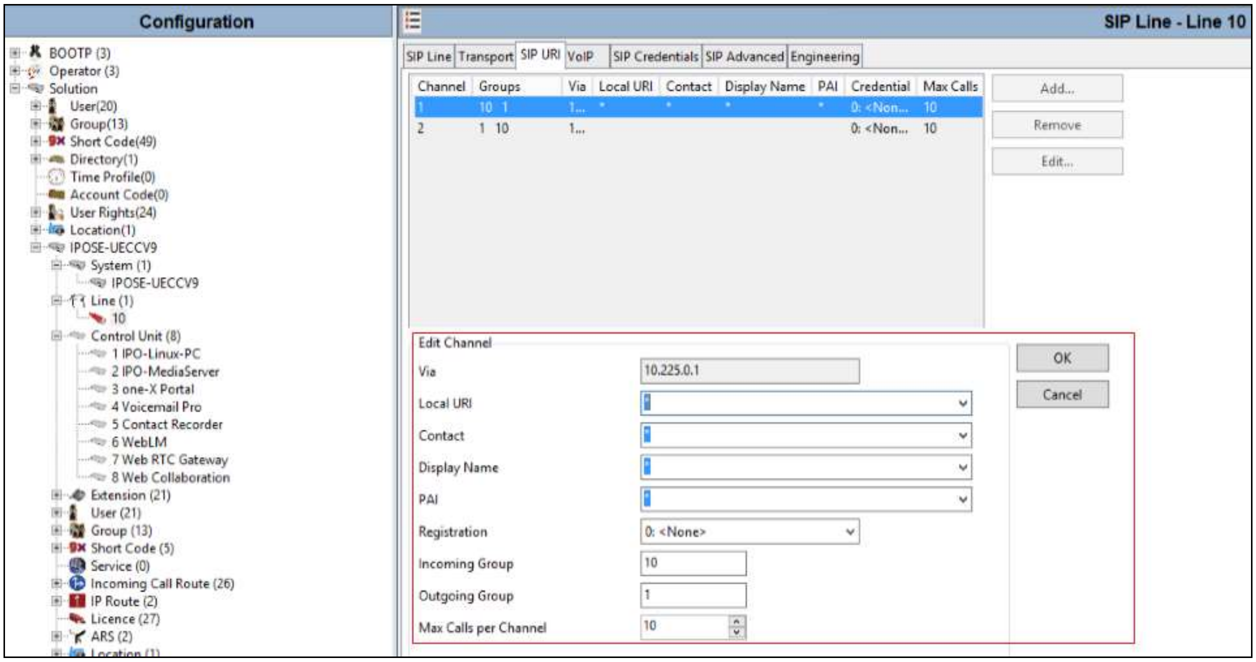
- Set **Local URI, Contact, Display Name** and **PAI** parameters to **Use Internal Data**. This setting allows calls on this line whose SIP URI matches the number set in the **SIP** tab of any **User** as shown in **Section 5.8**.

- For **Registration**, select **0: <None>** from the pull-down menu.
- Associate this line with an incoming line group by entering line group **1** in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line to an outgoing line group using the **Outgoing Group** field. The outgoing line group number is used in defining short codes for routing outbound traffic to this line. For the compliance test, a new outgoing group **10** was defined.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



The second entry was created with the parameters shown below.

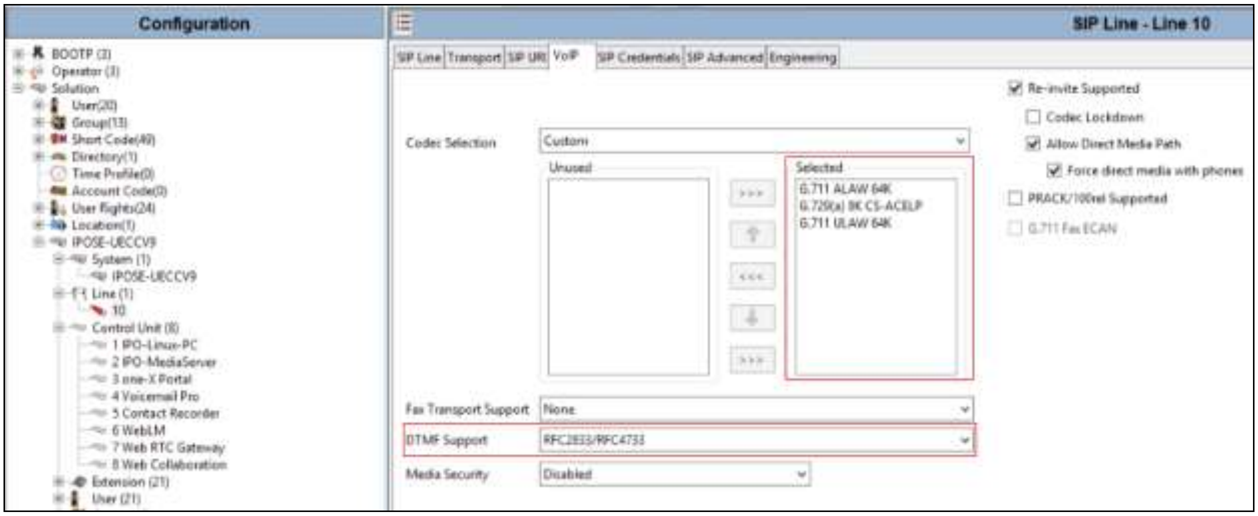
- Set **Local URI, Contact, Display Name** and **PAI** parameters to *****. This setting allows any calls on this line.
- For **Registration**, select **0: <None>** from the pull-down menu.
- Associate this line with an incoming line group by entering line group **10** in the **Incoming Group** field. This line group number will be used in defining incoming call routes for this line. Similarly, associate the line **1** to an outgoing line group using the **Outgoing Group** field.
- Set **Max Calls per Channel** to the number of simultaneous SIP calls that are allowed using this SIP URI pattern.



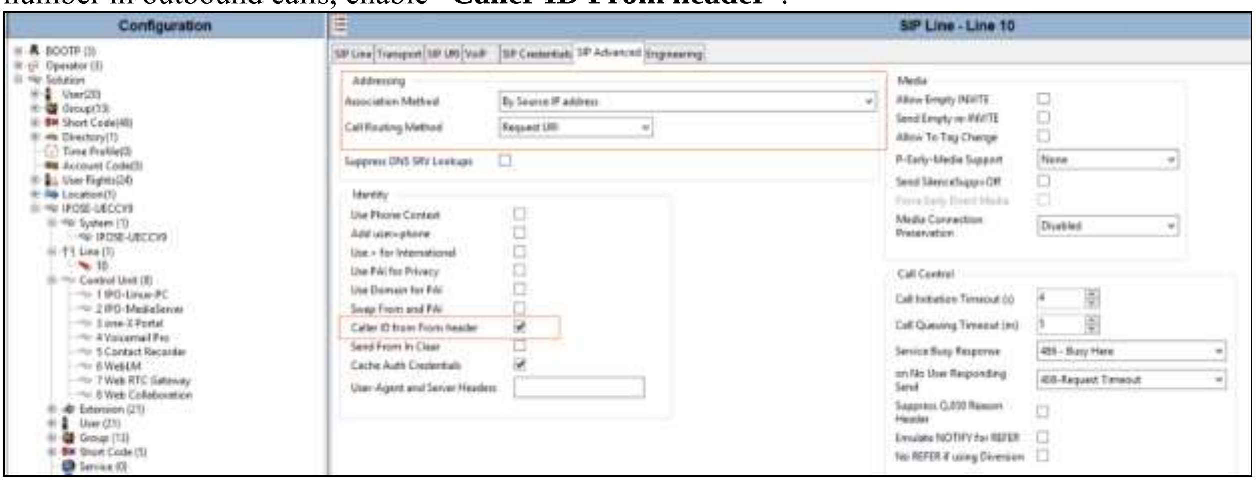
Select the **VoIP** tab to set the Voice over Internet Protocol parameters of the SIP line. Set the parameters as shown below:

- Select **Custom** from the drop-down menu.
- Select **G.711 ALAW 64K**, **G.729 (a) 8K** and **G.711 ULAW 64K** codecs.
- Set the **DTMF Support** field to **RFC2833**. This directs Avaya IP Office to send DTMF tones using RTP events messages as defined in RFC2833.
- Uncheck the **VoIP Silence Suppression** box.
- Check the **Re-invite Supported** box, to allow for codec re-negotiation in cases where the target of the incoming call or transfer does not support the codec originally negotiated on the trunk.
- Uncheck **PRACK/100rel Supported**.

Default values may be used for all other parameters.



Select the **SIP Advanced** tab. In order to remove "Anonymous" displayed along with called number in outbound calls, enable "**Caller ID From header**".

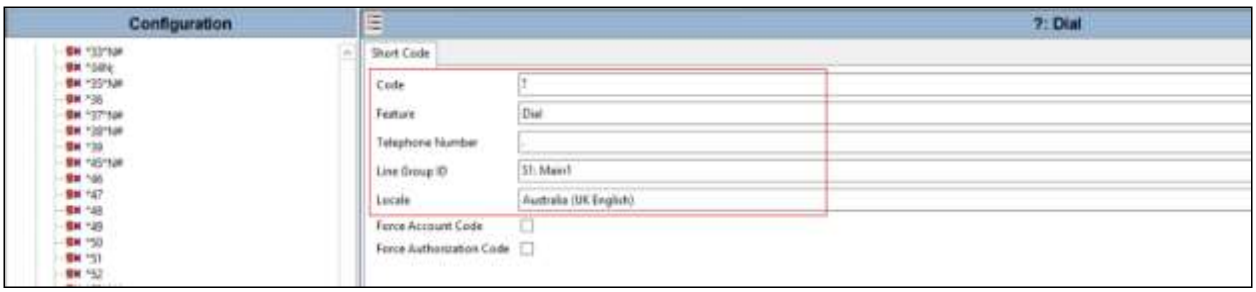


5.7 Short Codes

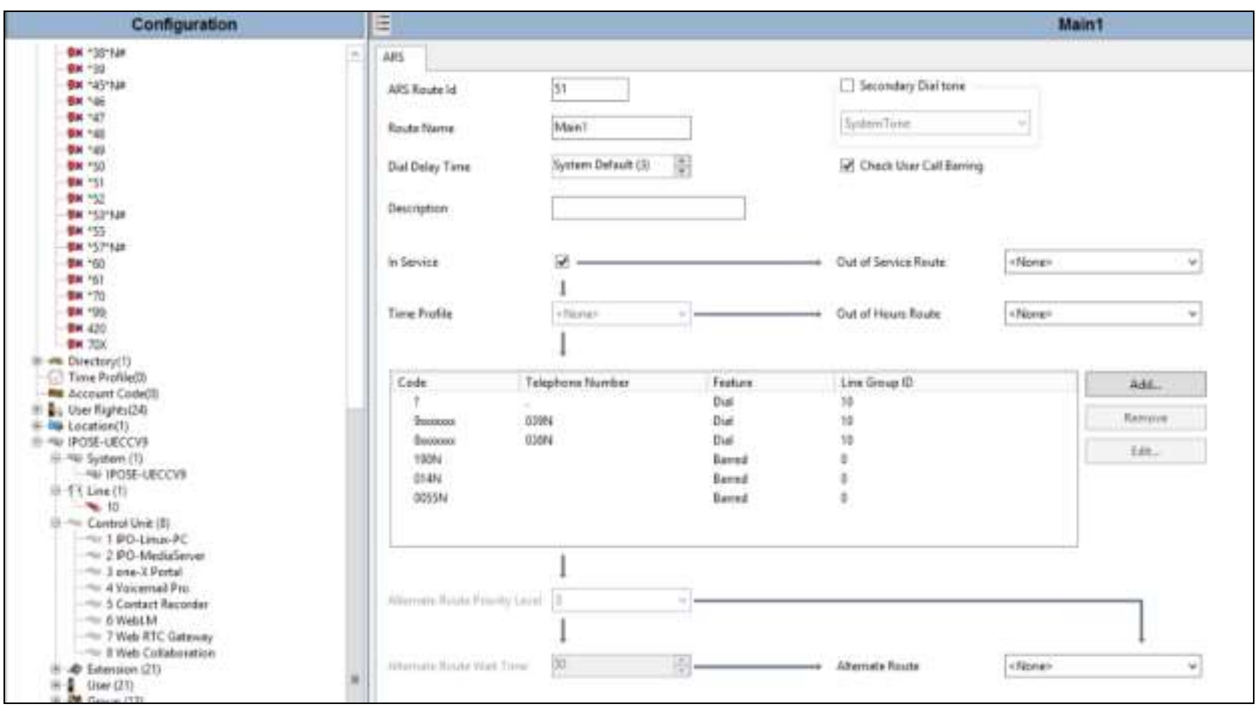
Define a short code to route outbound traffic to the SIP line and route incoming calls from mobility extensions to access Feature Name Extensions (FNE) hosted on IP Office. To create a short code, right-click **Short Code** in the Navigation Pane and select **New**. On the **Short Code** tab in the Details Pane, configure the parameters as shown below.

- In the **Code** field, enter the dial string which will trigger this short code, followed by a semi-colon. The example shows "**?**" which will be invoked when the user dials any numbers.
- Set **Feature** to **Dial**. This is the action that the short code will perform.
- Set **Telephone Number** to "**.**". The **Telephone Number** field is used to construct the Request URI and To Header in the outgoing SIP INVITE message.
- Set the **Line Group Id** to "**51:Main1**".

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



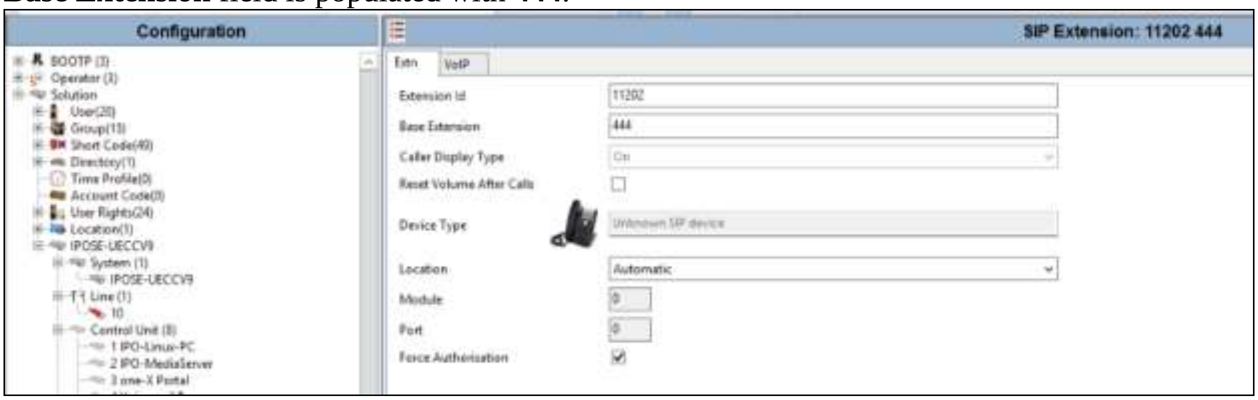
Under **ARS**, define rules as shown below.



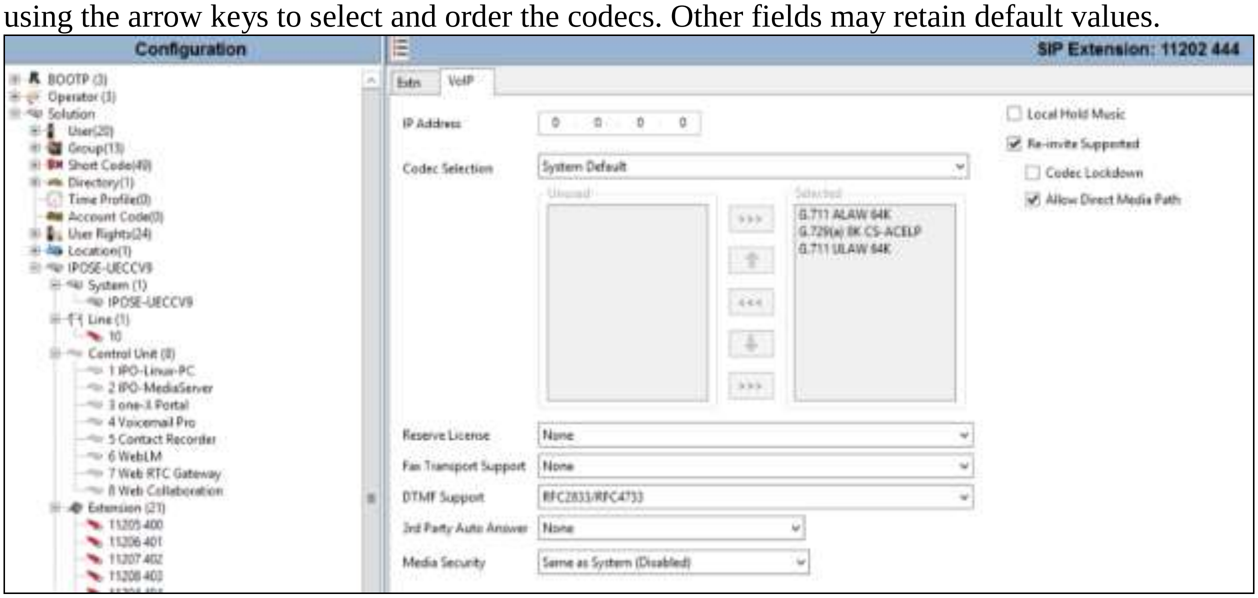
5.8 User and Extension

In this section, examples of IP Office Users and Extensions will be illustrated. In the interest of brevity, not all users and extensions will be presented, since the configuration can be easily extrapolated to other users.

A new SIP extension may be added by right-clicking on **Extension** (not shown) in the Navigation pane and selecting **New SIP Extension**. Alternatively, an existing SIP extension may be selected in the group pane. The following screen shows the **Extn** tab for a SIP extension. The **Base Extension** field is populated with **444**.

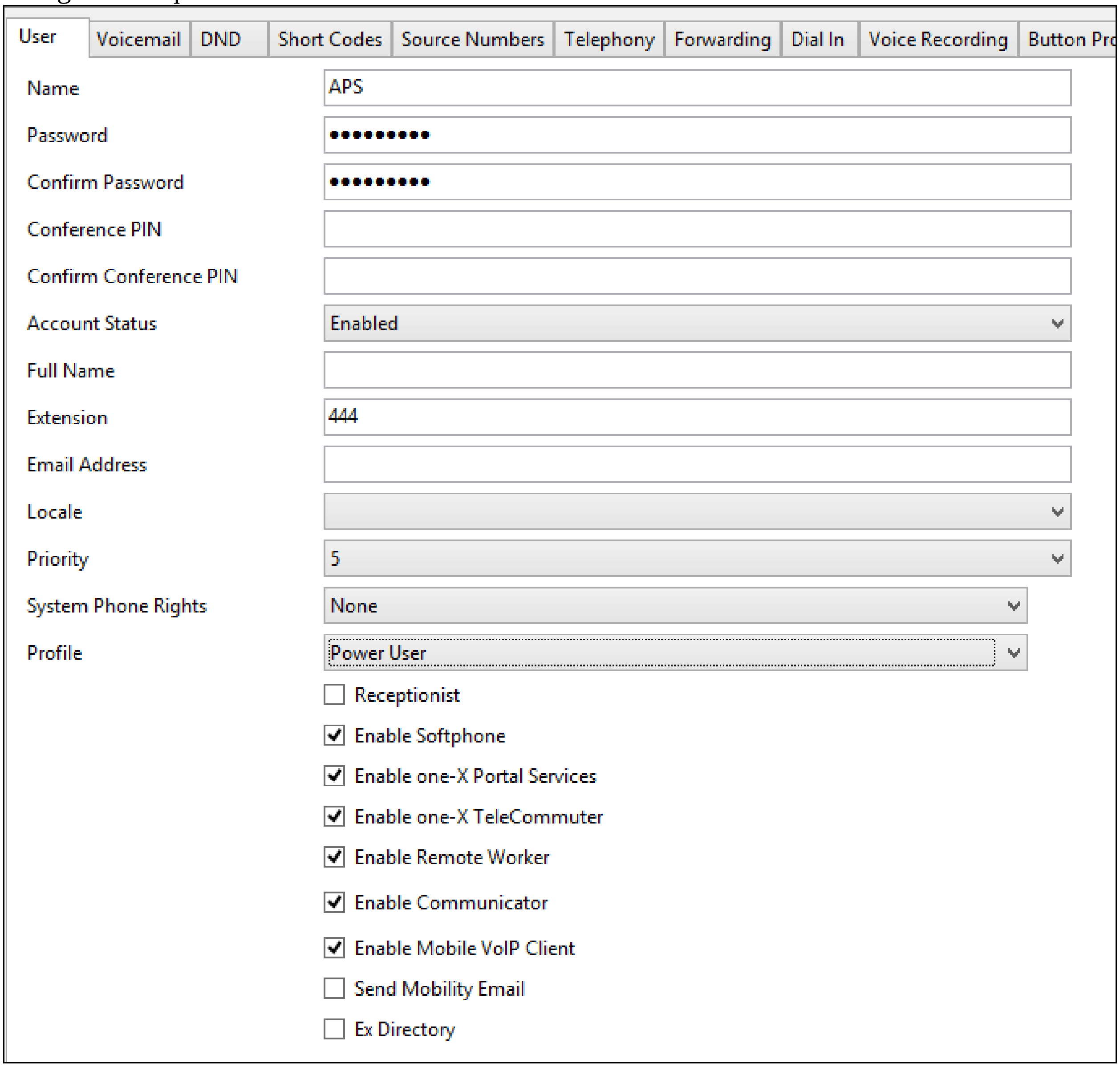


The following screen shows the **VoIP** tab for the extension. The **IP Address** field may be left blank or populated with a static IP address. The new **Codec Selection** parameter may retain the default setting **System Default** to follow the system configuration shown in **Section 5.5**. Alternatively, **Custom** may be selected to allow the codecs to be configured for this extension, using the arrow keys to select and order the codecs. Other fields may retain default values.

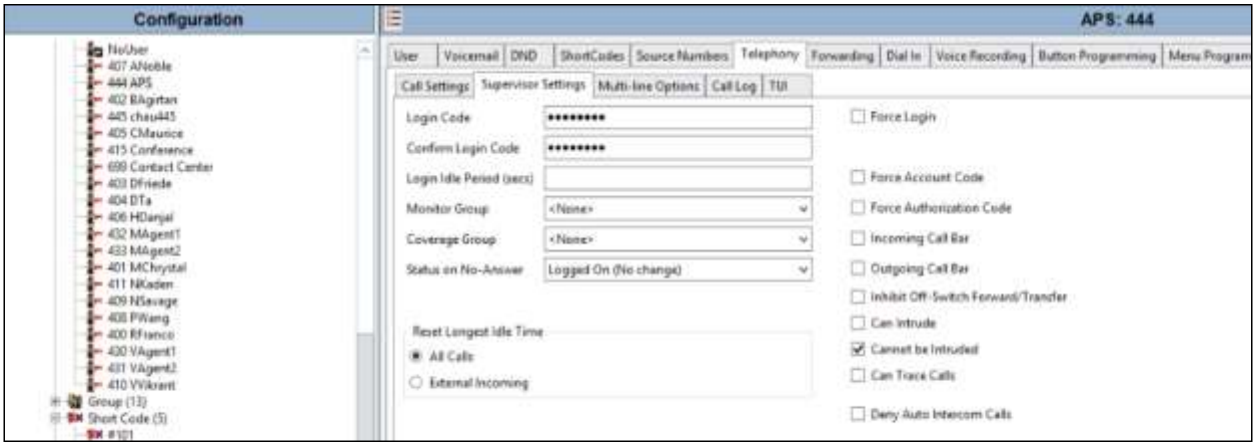


To add a User, right-click on **User** in the Navigation pane, and select **New**. To edit an existing User, select **User** in the Navigation pane, and select the appropriate user to be configured in the

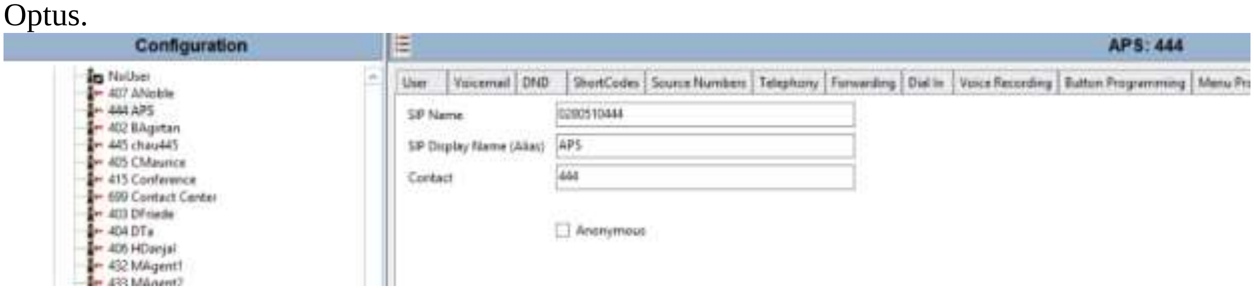
Group pane. Configure the SIP parameters for each User that will be placing and receiving calls via the SIP line defined in **Section 5.6**. To configure these settings, select the **User** tab if any changes are required.



Select the **Telephony** tab. Then select the **Supervisor Settings** tab as shown below. The **Login Code** will be used by the Avaya SIP telephone user as the login password.



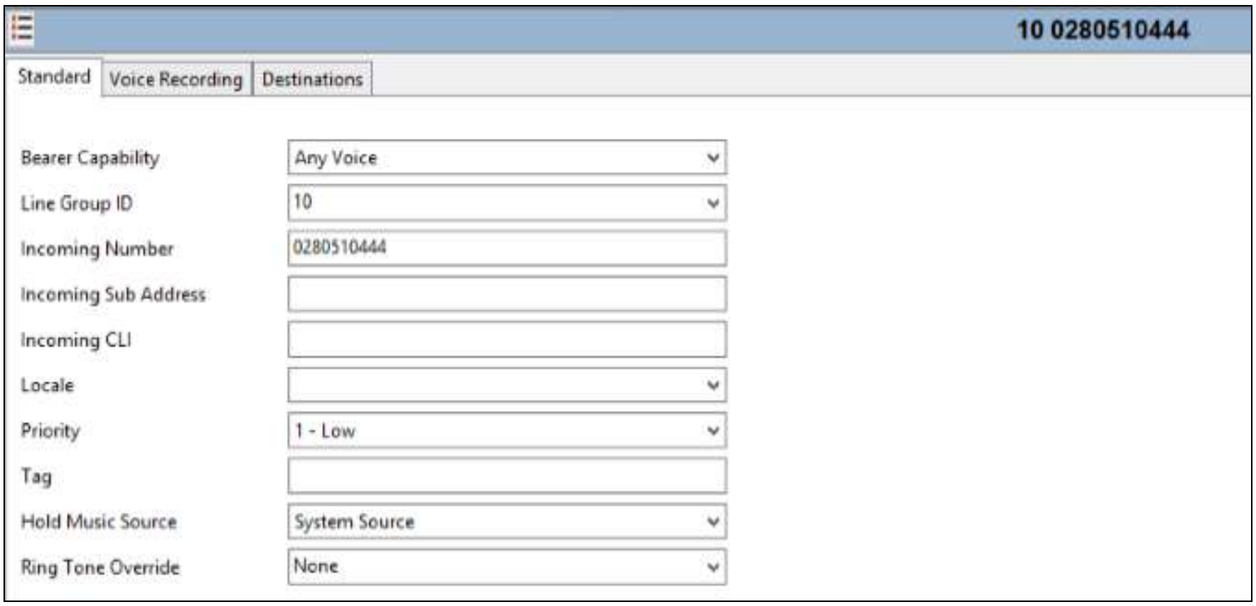
Next, select the **SIP** tab in the Details Pane. To reach the **SIP** tab click the right arrow on the right hand side of the Details Pane until it becomes visible. The values entered for the **SIP Name** and **Contact** fields are used as the user part of the SIP URI in the From header for outgoing SIP trunk calls. These allow matching of the SIP URI for incoming calls without having to enter this number as an explicit SIP URI for the SIP line (**Section 5.6**). As such, these fields should be set to one of the DID numbers assigned to the enterprise from Optus.



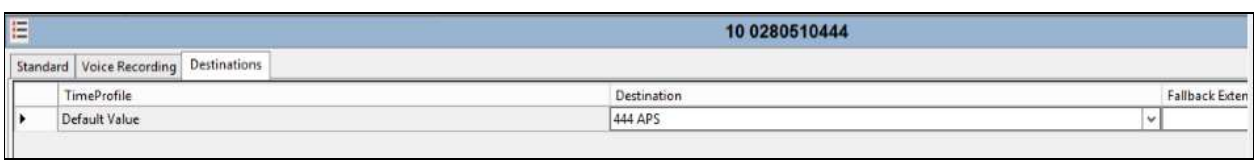
5.9 Incoming Call Routing

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 (not shown) and select **New**. On the **Standard** tab of the Details Pane, enter the parameters as shown below:

- Set the **Bearer Capacity** to **Any Voice**.
- Set the **Line Group Id** to the incoming line group of the SIP line defined in **Section 5.6**.
- Set the **Incoming Number** to the incoming number that this route should match on. Matching is right to left.
- Default values can be used for all other fields.



On the **Destinations** tab, select the destination extension from the pull-down menu of the **Destination** field. On completion, click the **OK** button (not shown). In this example, incoming calls to the test DID number **0280510444** on line 10 are routed to extension 444.



5.10 Save Configuration

Navigate to **File → Save Configuration** in the menu bar at the top of the screen to save the configuration performed in the preceding sections. 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.

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.

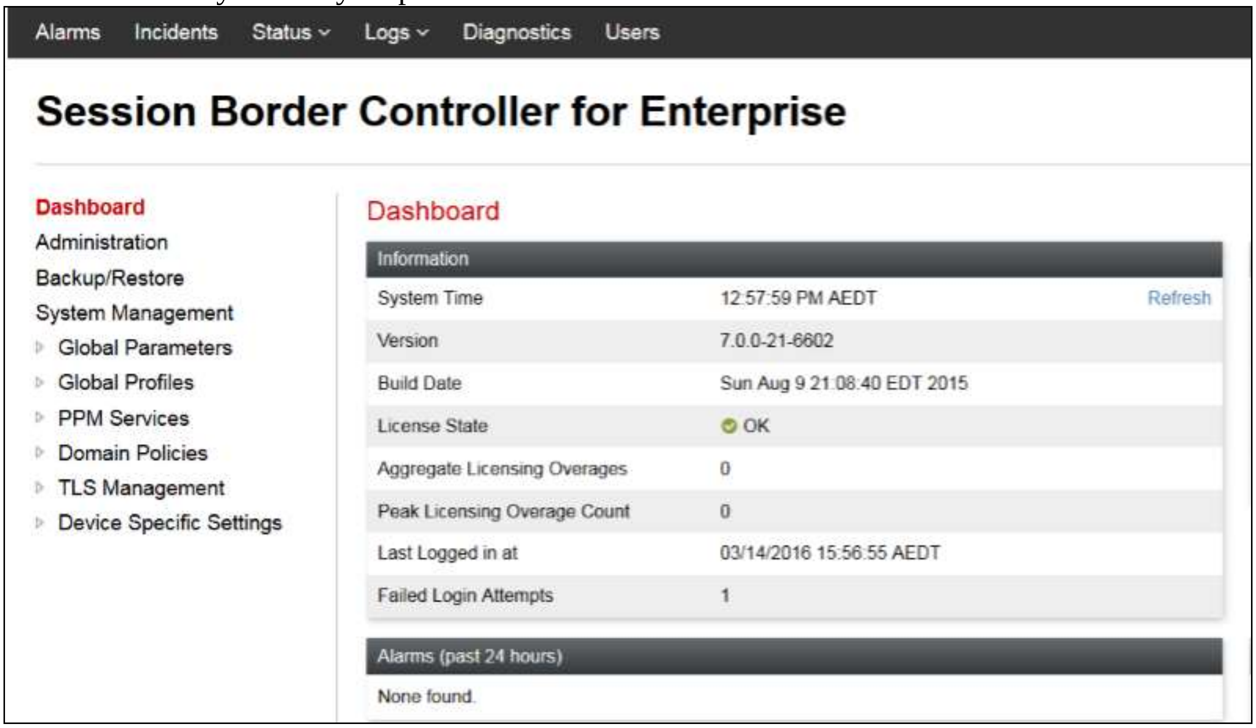
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1). If this is not the case, contact your Avaya representative to get this condition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

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the common site (IP address 10.225.0.3). The connection to Optus Evolve uses the Avaya SBCE public interface B1 (IP address 172.21.2.3). 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**.

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

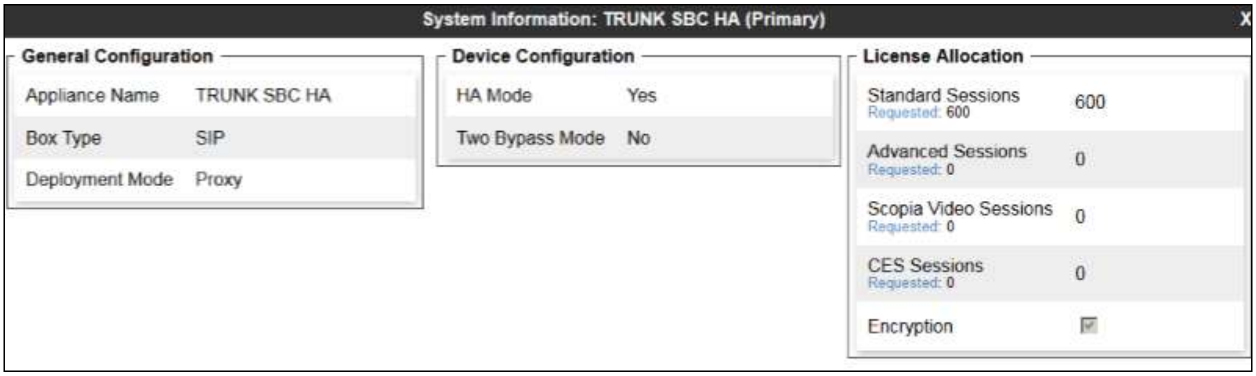
The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.



6.1 System Management – Status

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

2. Click on **View** (shown above) to display the **System Information** screen.



6.2 Global Profiles

6.2.1 Uniform Resource Identifier (URI) Groups

URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

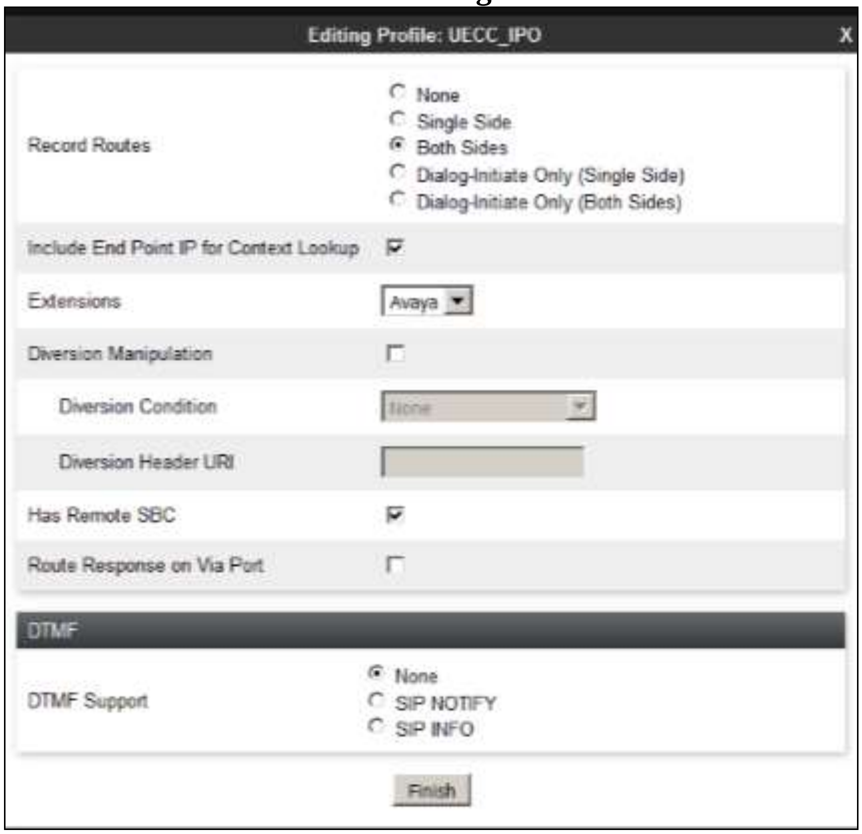
For this configuration testing, "*****" is used for all incoming and outgoing traffic.

6.2.2 Server Interworking – Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold. From the left-hand menu select **Global Profiles →** **Server Interworking** (not shown) and click on **Add**.

- Enter profile name such as UECC-IPO and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.

Default values can be used for the **Advanced Settings** window. Click **Finish**



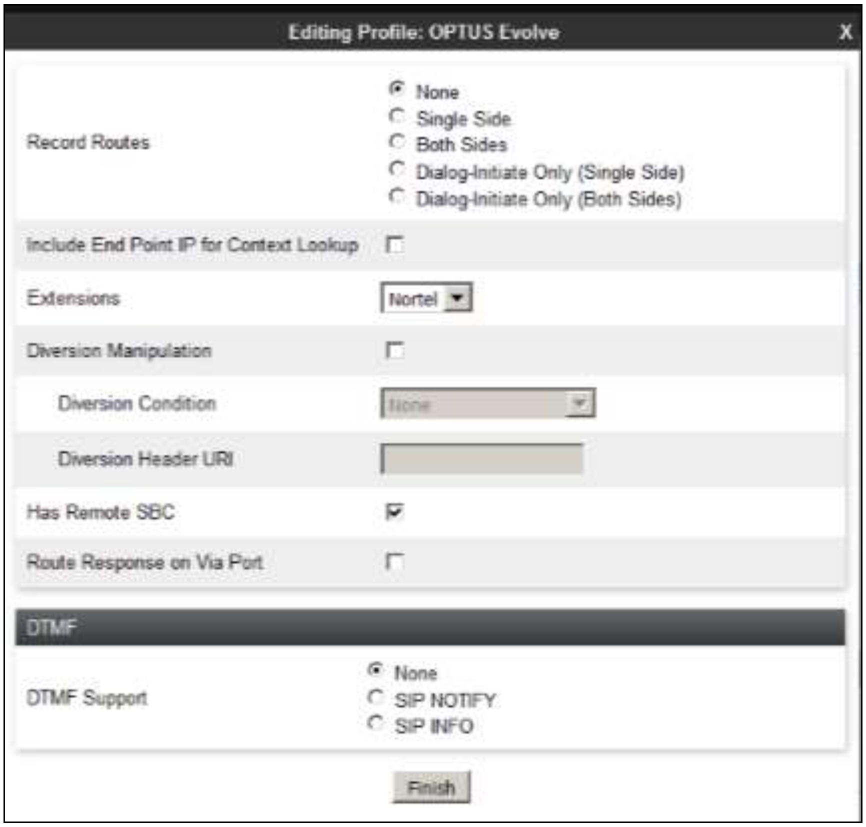
6.2.3 Server Interworking – Optus

Repeat the same steps as described in **Section 6.2.2** with changes as below.

- Enter profile name such as OPTUS Evolve and click **Next** (Not Shown).
- Check **Hold Support = None**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

Select **Nortel** for **Extension,** default values can be used for the others in **Advanced Settings** window. Click **Finish**.



6.2.4 Server Configuration – Avaya IP Office

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.225.0.1** (IP Office LAN1 IP Address).
- For **Port**, enter **5060**.
- For **Transport,** select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

On the **Advanced** tab:

- Select **UECC_IPO** for **Interworking Profile**.
- Click **Finish**.

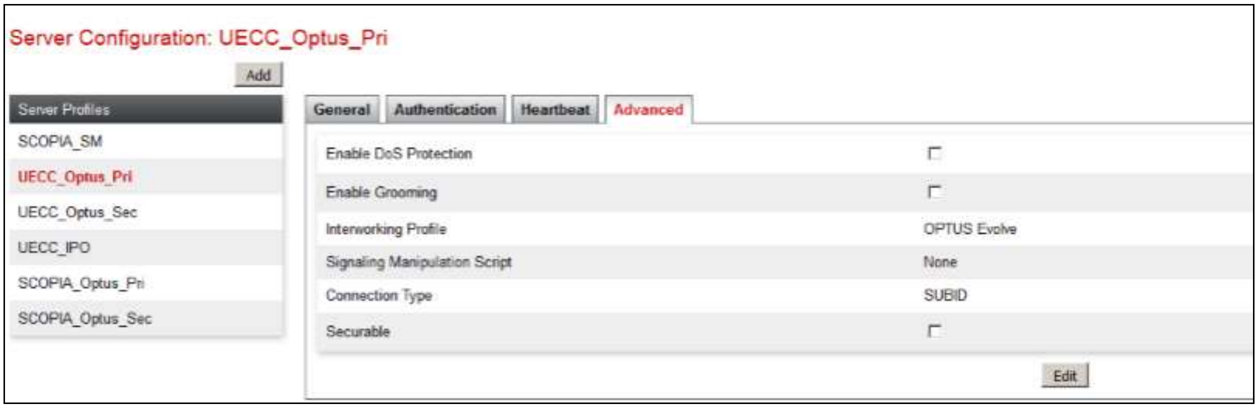
6.2.5 Server Configuration – Optus

Repeat the steps in **Section 6.2.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Optus Evolve.

1. Select **Add Profile** and enter a Profile Name (e.g., **UECC_Optus_Pri**) and select **Next**.
2. On the **General** window (not shown), enter the following.
   - Select Server Type to be **Trunk Server**.
   - Enter **IP Address / FQDN** to **123.102.x.x (**because of security reason, the real IP address is not shown here)
   - For **Port,** enter **5060**.
   - For **Transport**, select **UDP**.
   - Click on **Next (**not shown).

3. On the **Advanced** window, enter the following.
   - For **Interworking Profile**, select the profile created for Optus in **Section 6.2.3**.

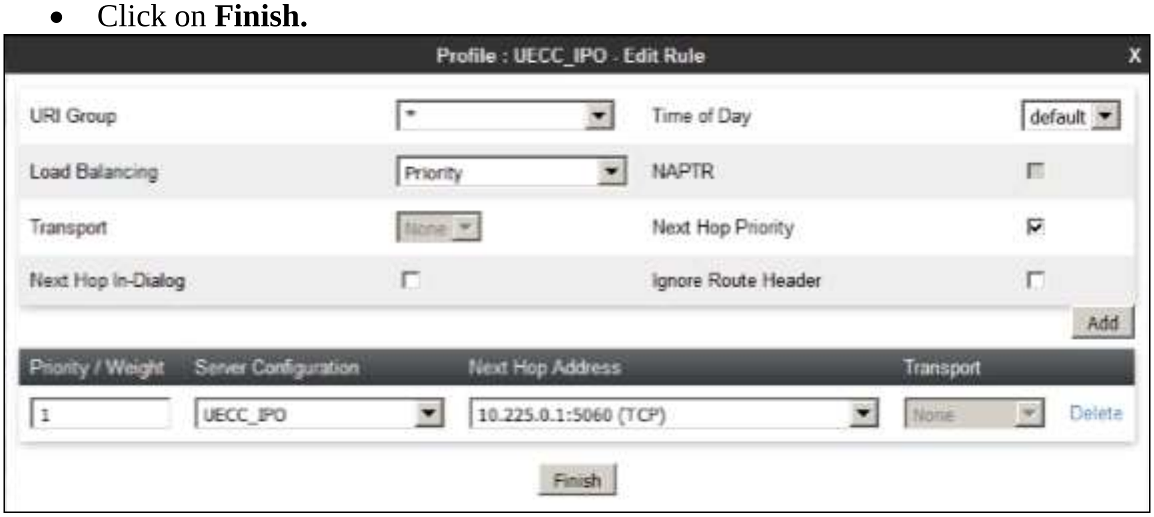
- Select **Finish**.



6.2.6 Routing – To Avaya IP Office

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

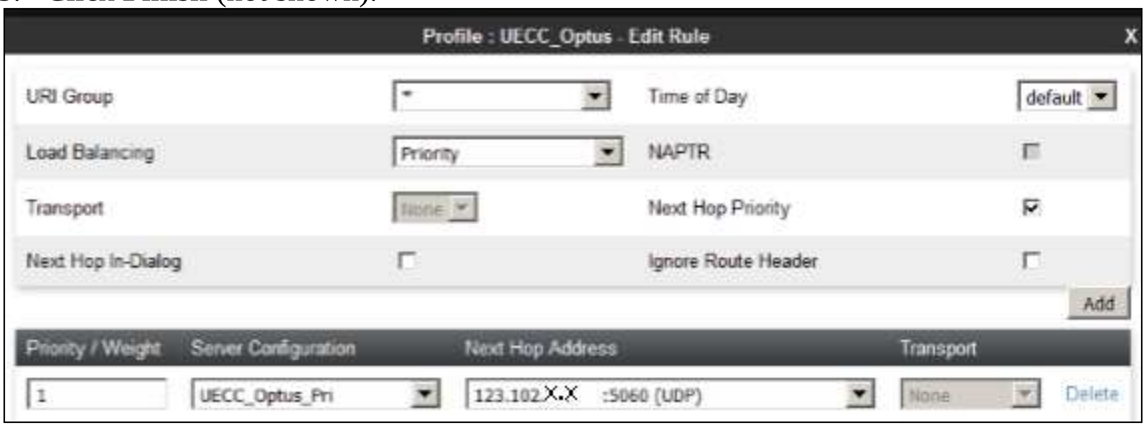
1. Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **UECC_IPO)** and click **Next**.
3. The Routing Profile window will open. Using the default values shown, click on **Add.**
4. The Next-Hop Address window will open. Populate the following fields:
   - **Priority/Weight** = **1**
   - **Server Configuration** = **UECC_IPO**.
   - **Next Hop Address** = Verify that the **10.225.0.1:5060 (TCP)** entry from the drop down menu is selected (IP Office IP address). Also note that the **Transport** field is grayed out.
   - Click on **Finish.**



6.2.7 Routing – To Optus

Repeat the steps in **Section 6.2.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Optus.

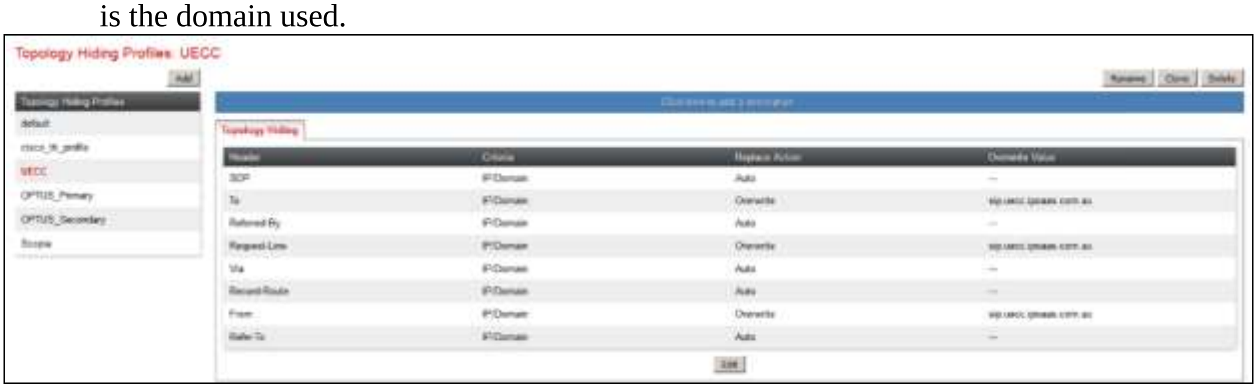
1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **UECC_Optus)**.
2. On the **Next-Hop Address** window (not shown), populate the following fields:
   - **Priority/Weight** = **1**
   - **Server Configuration** = **UECC_Optus_Pri**.
   - **Next Hop Address:** Verify that the **123.102.x.x:5060** entry from the drop down menu is selected.
   - Use default values for the rest of the parameters.
3. Click **Finish** (not shown).



6.2.8 Topology Hiding – Avaya

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 **Global Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name**: (e.g., **UECC**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly until **To** header is added.
4. Populate the fields as shown below, and click **Finish**. Note that **sip.uecc.ipoaas.com.au** is the domain used.



6.2.9 Topology Hiding –Optus

Repeat the steps in **Section 6.2.8,** with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Optus Evolve.

1. Enter a **Profile Name**: (e.g., **OPTUS_Primary**).
2. Use **Overwrite** under **Replace Action** and **sip4111.ippbx.optus.com.au** under **Overwrite Value** for header **To, Request-Line** and **From**. For other fields, use the default value and click **Finish** (not shown).

6.2.10 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.

6.2.11 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.

6.2.12 Border Rules

The default Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

6.2.13 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.

6.2.14 Signaling Rules

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

6.2.15 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.

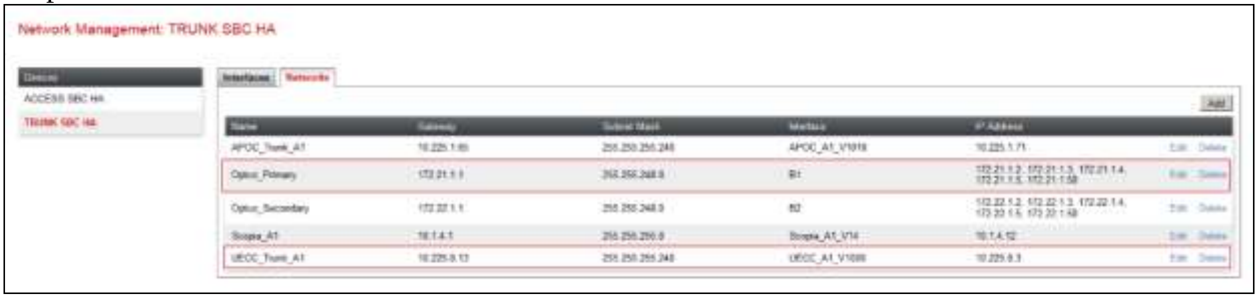
6.3 Device Specific Settings

The **Device Specific Settings** feature for SIP allows administrators 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, administrators 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.

6.3.1 Network Management

1. Select **Device Specific Settings → 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: A1 and B1 have 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.



6.3.2 Media Interfaces

1. Select **Device Specific Settings** 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**: **UECC_Media_A1**.
   - **IP Address**: **10.225.0.3** (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**: **UECC_Media_B1**.
   - **IP Address**: **172.21.2.3** (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.

6.3.3 Signaling Interface

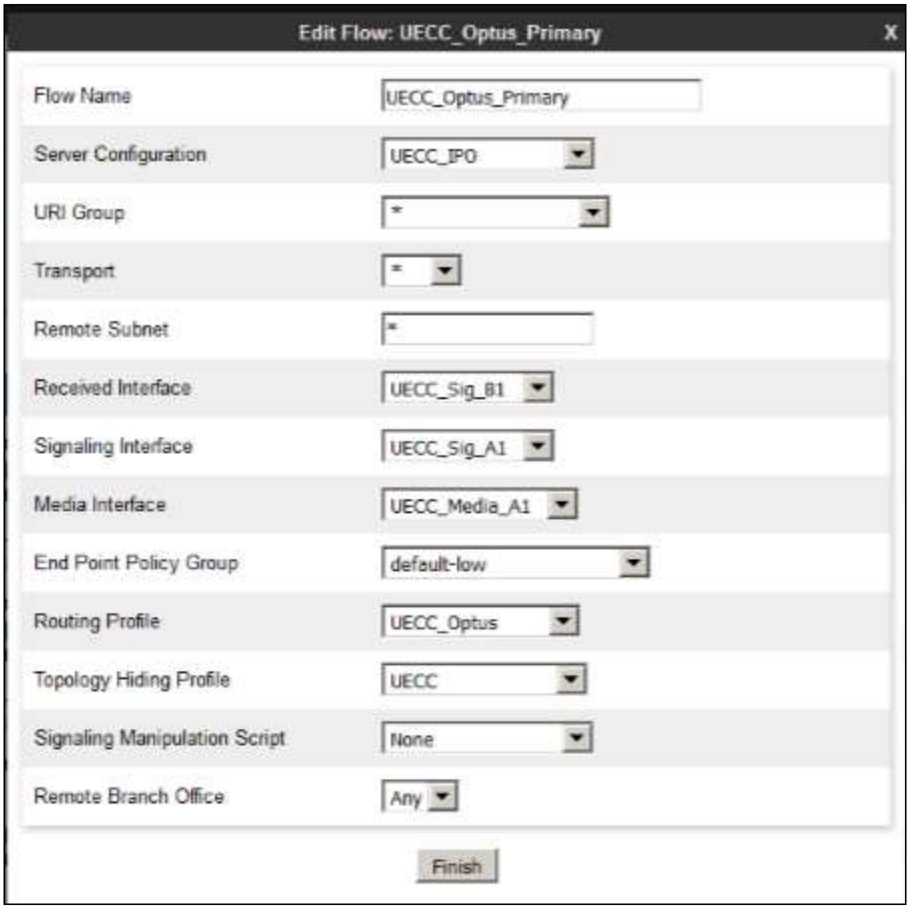
1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
   - **Name**: **UECC_Sig_A1**.
   - **IP Address**: **10.225.0.3** (Avaya SBCE A1 address).
   - **TCP Port**: **5060**.
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   - **Name**: **UECC_Sig_B1**.
   - **IP Address**: **172.21.1.3** (Avaya SBCE B1 address).
   - **UDP Port**: **5060**.
6. Click **Finish** (not shown). Note that changes to these values require an application restart.

6.3.4 Endpoint Flows – For Avaya 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**: **UECC_Optus_Primary**
   - **Server Configuration**: **UECC_IPO**
   - **URI Group**: *****
   - **Transport**: *****
   - **Remote Subnet**: *****
   - **Received Interface**: **UECC_Sig_B1**
   - **Signaling Interface**: **UECC_Sig_A1**
   - **Media Interface**: **UECC_Media_A1**
   - **End Point Policy Group**: **default-low**.
   - **Routing Profile**: **UECC_Optus**

- **Topology Hiding Profile**: **UECC**
- Let other values default.

4. Click **Finish** .



6.3.5 Endpoint Flows – For Optus

Repeat step **1** through **4** from **Section 6.3.4**, with the following changes:

- **Name**: **OPTUS_Primary_UECC**
- **Server Configuration**: **UECC_Optus_Pri**
- **URI Group**: *****
- **Transport**: **UDP**
- **Remote Subnet**: *****
- **Received Interface**: **UECC_Sig_A1**
- **Signaling Interface**: **UECC_Sig_B1**
- **Media Interface**: **UECC_Media_B1**
- **End Point Policy Group**: **default_low**.
- **Routing Profile**: **UECC_IPO**
- **Topology Hiding Profile**: **OPTUS_Primary**.

7. Verification Steps

The following steps may be used to verify the configuration.

7.1 Avaya Session Border Controller for Enterprise

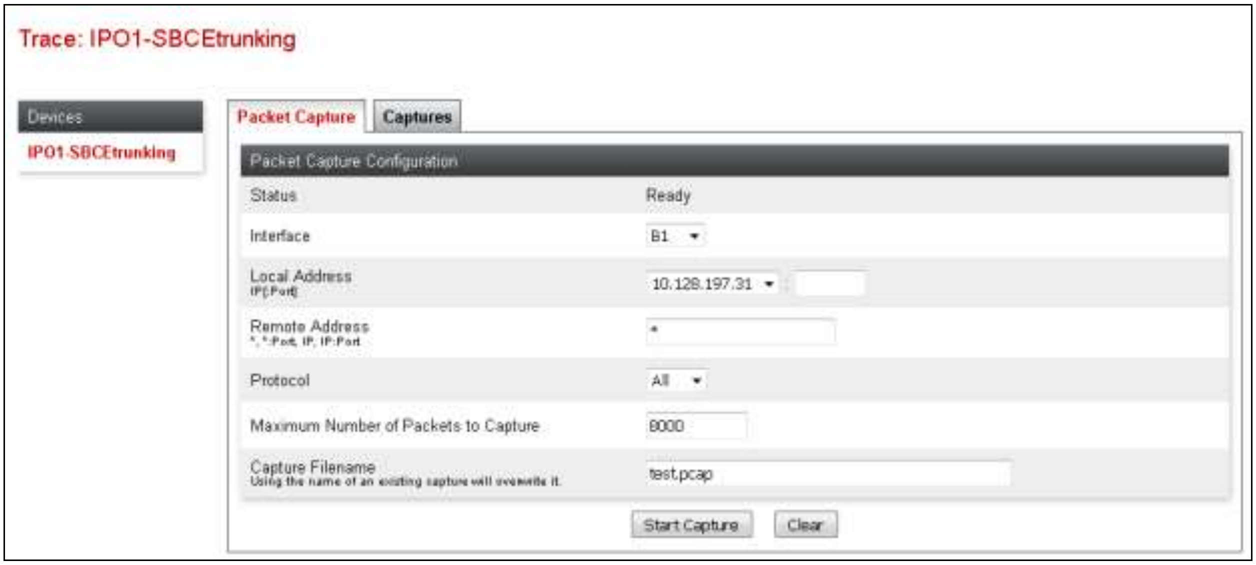
Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

Protocol Traces

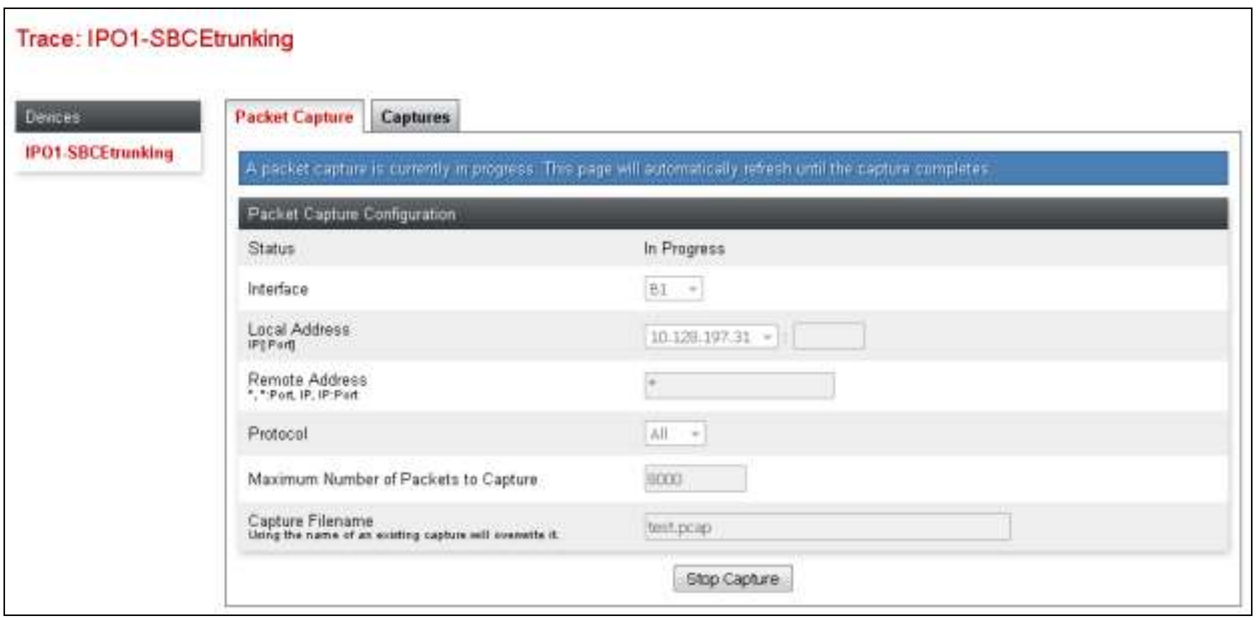
The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
   - Select the desired **Interface** from the drop down menu (e.g., **All**).
   - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
   - 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.

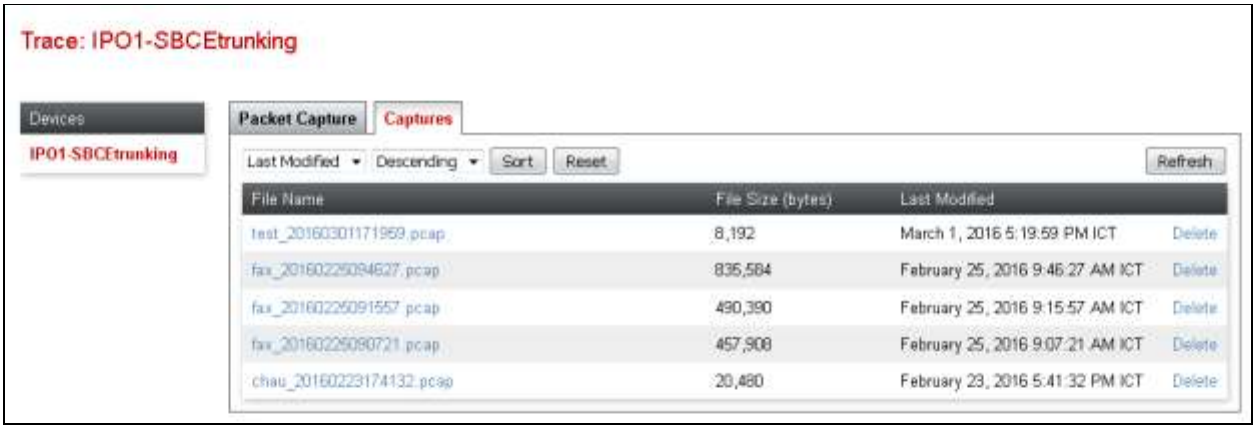
- Click **Start Capture** to begin the trace.



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

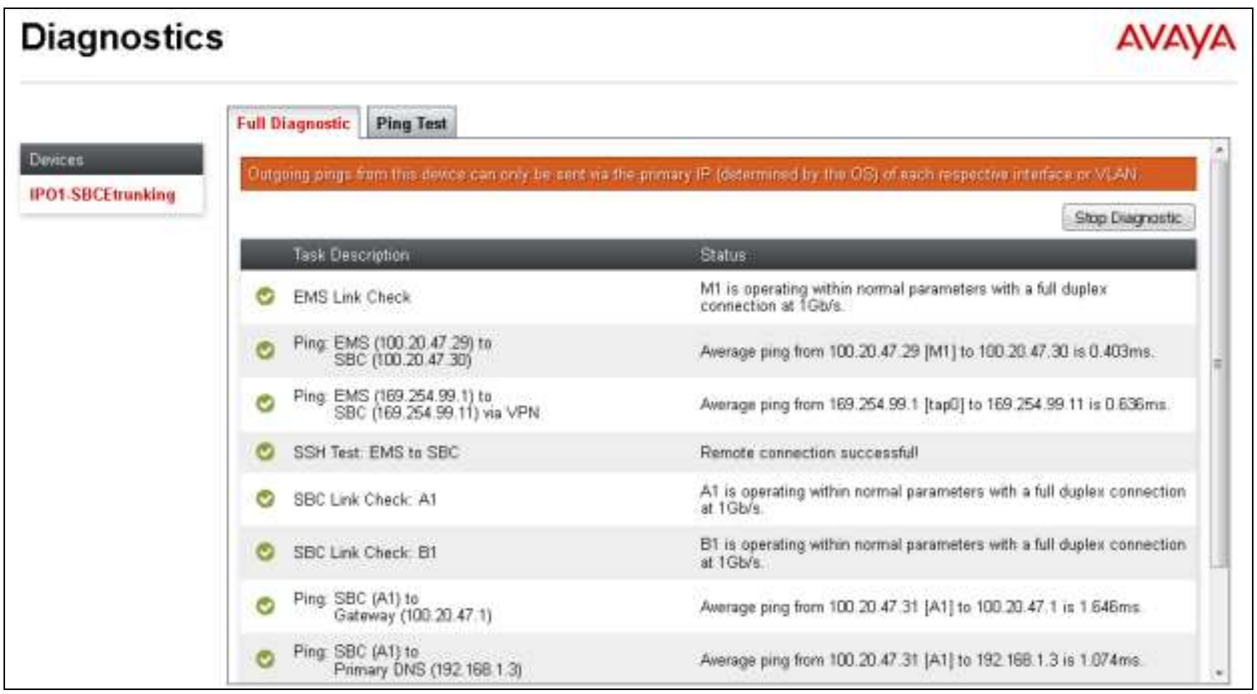


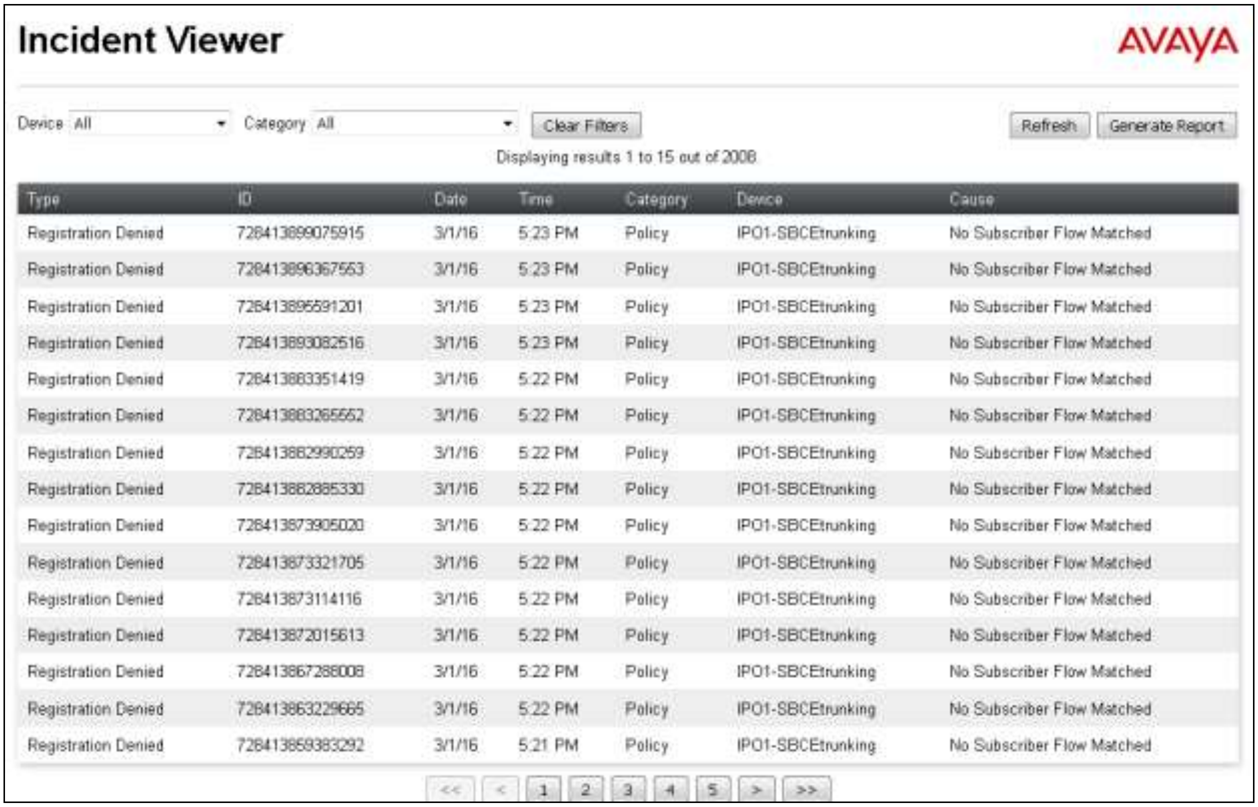
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.



The following section details various methods and procedures to help diagnose call failure or service interruptions.
On either side of the Avaya SBCE, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the Avaya SBCE to the B1 network gateway.
- Ping from the Avaya SBCE to the Avaya IPO.
- Ping from the B1 network towards the SIP trunking service.
- Note any Incidents or Alarms on the Dashboard screen of the Avaya SBCE.



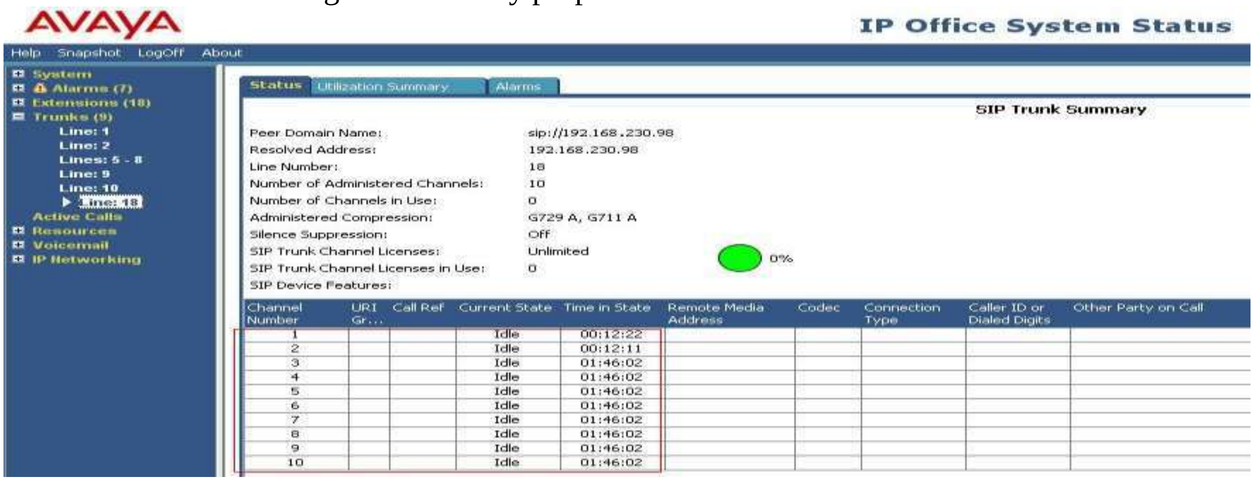


7.2 Avaya IP Office

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

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

From the left hand menu expand **Trunks** and choose the SIP trunk (**18** in this instance). The status window will show the status as being idle and time in state if the Trunk is operational. The IP address has been changed for security purposes.



7.3 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

8. Conclusion

As illustrated in these Application Notes, Avaya IP Office Server Edition 9.1.6 and Avaya Session Border Control for Enterprise 7.0 can be configured to interoperate successfully with Optus Evolve SIP Trunking service. This solution allows enterprise users in Uecomm UEConnect network access to the PSTN using the Optus Evolve SIP Trunking service connection.

9. Additional References

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

[1] *Administering Avaya IP Office with Manager*, February 2016.
[2] *Avaya Session Border Controller for Enterprise Overview and Specification,* Release 7.0, Issue1, August 2015.
[3] *Deploying Avaya Session Border Controller for Enterprise,* Release 7.0, Issue 1, August 2015.
[4] *Deploying Avaya Session Border Controller in Virtualized Environment,* Release 7.0, Issue 1, August 2015.
[5] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015.
[6] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/
[7] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, http://www.ietf.org/

Product documentation for Uecomm/Optus Evolve SIP Trunking Solution is available from Uecomm/Optus.

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.