Avaya Solution & Interoperability Test Lab

Application Notes for Computer Instruments 7.0 with Avaya IP Office Server Edition 11.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Computer Instruments eONE 7.0 to interoperate with Avaya IP Office Server Edition 11.1. Computer Instruments eONE is an IVR development platform that provides self-service IVR and Web applications.

In the compliance testing, Computer Instruments eONE used SIP trunk with Avaya IP Office Server Edition to support inbound and outbound IVR applications.

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.

1. Introduction

These Application Notes describe the configuration steps required for the Computer Instruments eONE 7.0 to interoperate with Avaya IP Office Server Edition 11.1. eONE is an IVR development platform that provides self-service IVR and Web applications.

In the compliance testing, eONE used SIP trunk with IP Office to support inbound and outbound IVR applications.

The IP Office Server Edition configuration consisted of two IP Office systems, a primary Linux server and an expansion IP500V2 that were connected via Small Community Network (SCN) trunk.

The eONE solution consisted of distributed components across multiple servers. The eONE solution used in the compliance testing utilized two servers – an eONE server and a Media server. The eONE server is responsible for eONE configuration via a web-based interface and included the CIMedia MRCP Connector for support of text-to-speech (TTS). The Media server is responsible for SIP trunk connection with IP Office and included the CIMedia ARC SIP Telecom Services for support of SIP protocol and the CIMedia ARC VXML Services for support of VXML.

eONE supports both on-premise and cloud deployments, and the compliance testing used the on-premise deployment method with eONE residing in the DevConnect test lab.

To facilitate testing, two custom applications were developed by Computer Instruments for testing of inbound and outbound applications that included greetings, menu option selection via DTMF, announcements, and transfer to internal and external destinations.

2. General Test Approach and Test Results

The feature test cases were performed manually. The eONE inbound application was tested by manually placing calls from users on the PSTN and on both IP Office systems to the eONE inbound application. The eONE inbound application played greeting and collected DTMF input from the caller to decide on the feature to provide, such as announcement playback and transfer to internal or external destinations.

The eONE outbound application was tested by manually requesting callbacks to users on the PSTN and on both IP Office systems. The callback requests were initiated from the Web page associated with the eONE outbound application.

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to eONE.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

For the testing associated with these Application Notes, the SIP trunk interface between IP Office and eONE did not include use of any specific encryption features as requested by Computer Instruments.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g. jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g. session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing included OPTIONS, G.711MU, media shuffling, session refresh, REFER, hold/reconnect, inbound DTMF, dial ahead, outgoing call screening, multiple calls, call forwarding, inbound, outbound, and supervised transfer via REFER to internal and external destinations.

The serviceability testing focused on verifying the ability of eONE to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to eONE.

2.2. Test Results

All test cases were executed and verified.

2.3. Support

Technical support on eONE can be obtained through the following:

- **Phone:** (888) 451-0851
- **Web:** http://instruments.com/tech_support.html
- **Email:** support@instruments.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. Each IP Office system has connectivity to the PSTN for testing of cross systems PSTN scenarios.

The detailed administration of IP Office resources is not the focus of these Application Notes and will not be described. As shown in **Figure 1** below, SIP trunk was used between the primary IP Office system and eONE.

A five-digit dial plan was used to facilitate routing with eONE. Unique extension ranges were assigned to users on the primary IP Office system (210xx), to users on the expansion IP Office system (220xx), and to eONE (21880).

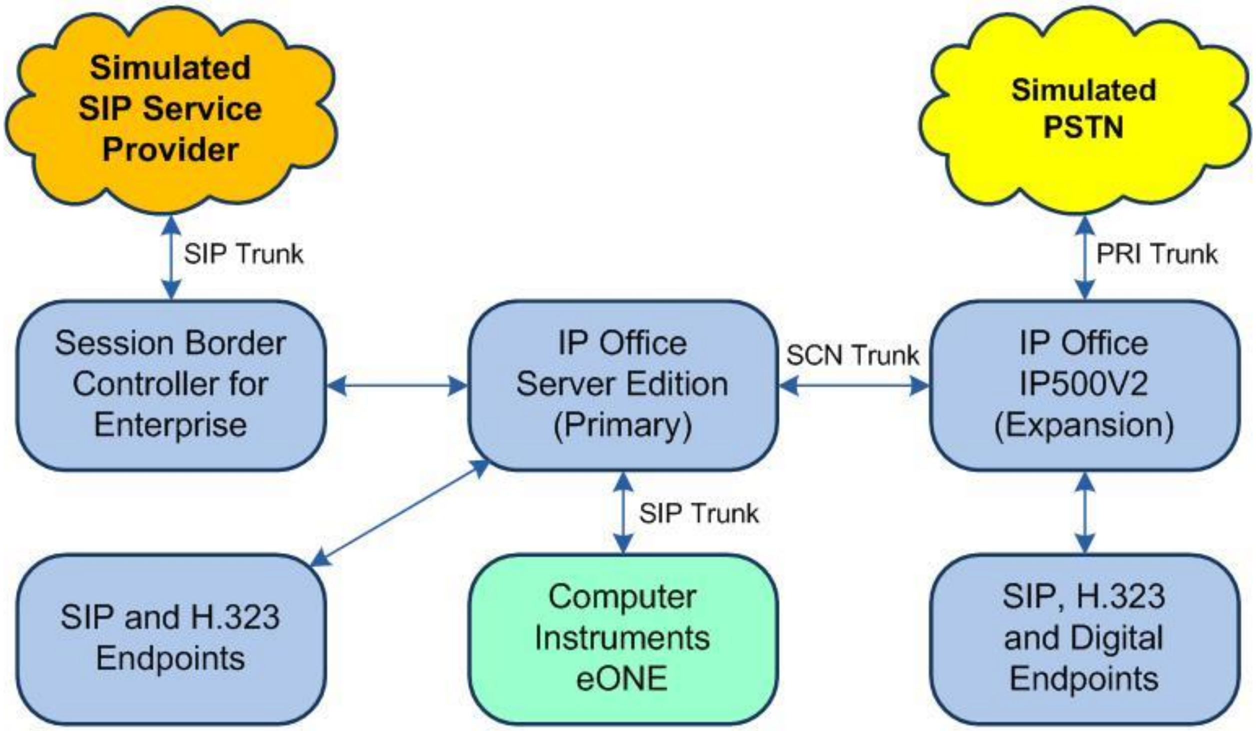


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition (Primary) in Virtual Environment	11.1.0.0.0
Avaya IP Office on IP500 V2 (Expansion)	11.1.0.0.0
Avaya 1120E IP Deskphone (SIP)	4.4.23.0
Avaya J129 IP Deskphone (SIP)	4.0.4.0.10
Avaya 1608-I IP Deskphone (H.323)	1.3120
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya 1408 Digital Deskphone	48.02
Computer Instruments eONE • CIMedia ARC SIP Telecom Services on Linux • CIMedia arcVXML3.6 Services • CIMedia Arc MRCP Connector	7.0 3.6 Build 12 3.6 Build 11 4.0 Build 24

Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

5. Configure Avaya IP Office

This section provides the procedures for configuring the IP Office systems. The procedures include the following area:

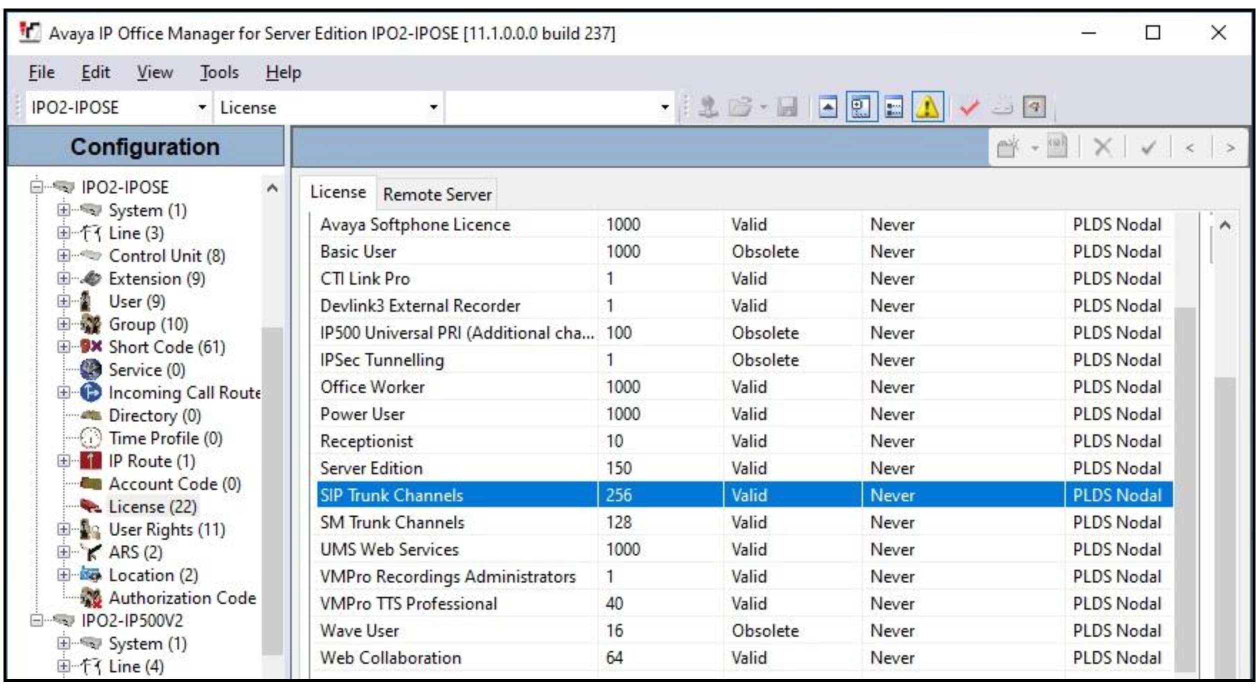
- Verify license
- Administer system
- Administer line
- Administer incoming call route
- Administer short code

5.1. Verify License

From a PC running the IP Office Manager application, select **Start → Programs → IP Office → Manager** to launch the application. Select the proper primary IP Office system, and log in using the appropriate credentials.

The **Avaya IP Office Manager for Server Edition IPO2-IPOSE** screen is displayed, where **IPO2-IPOSE** is the name of the primary IP Office system.

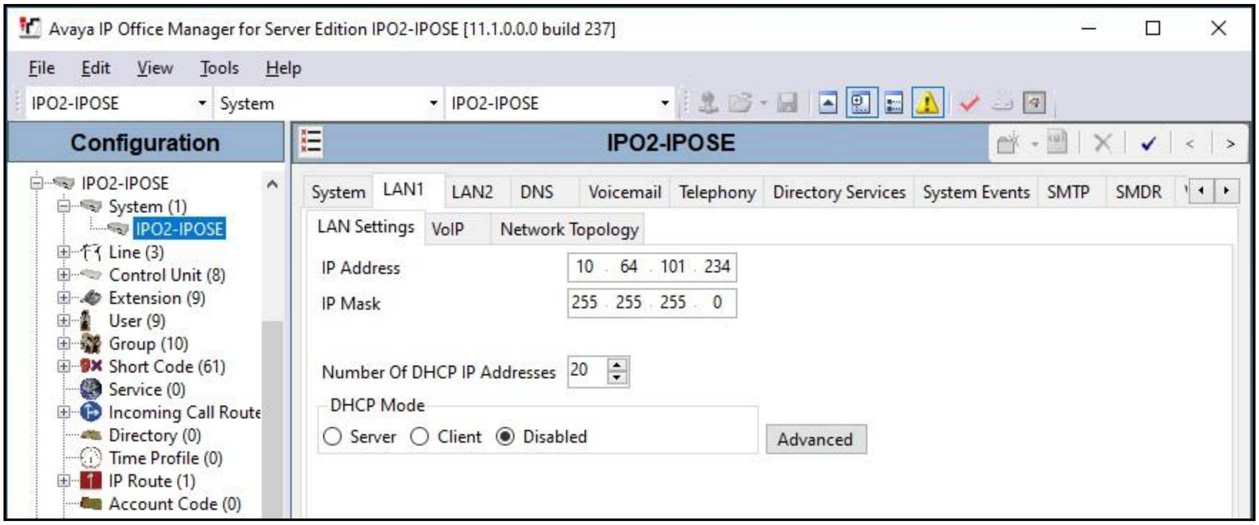
From the configuration tree in the left pane, select **License** under the primary IP Office system, in this case "IPO2-IPOSE", and a list of licenses is displayed in the right pane. Verify that there is a license for **SIP Trunk Channels** and that the **Status** is "Valid", as shown below.



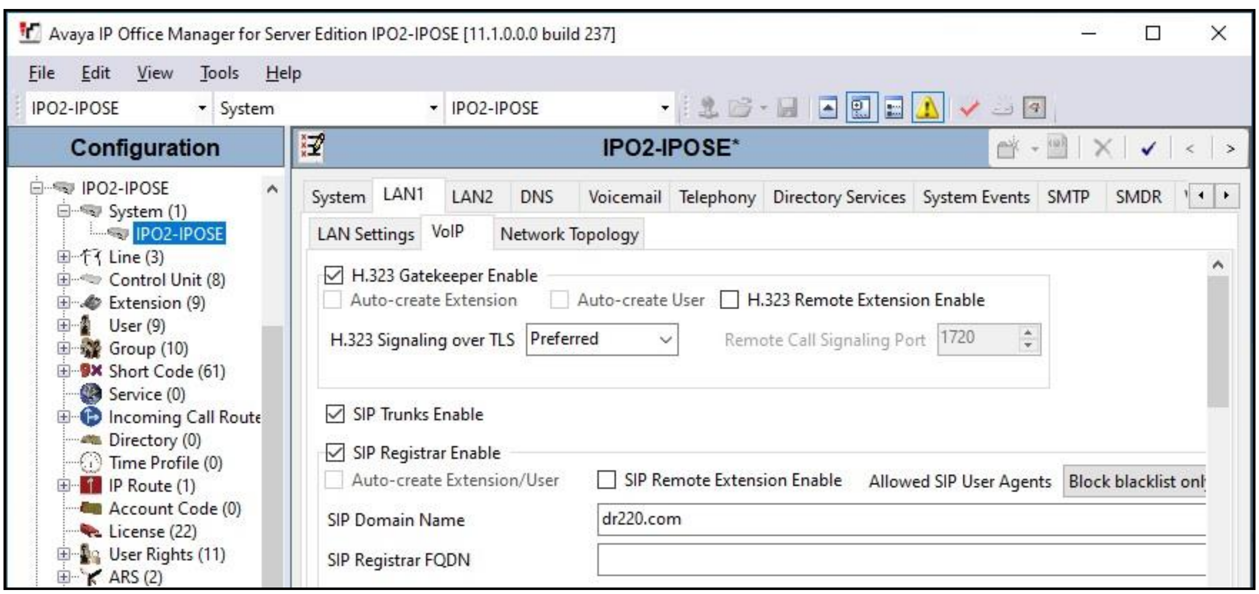
5.2. Administer System

From the configuration tree in the left pane, select **System** under the IP Office system used for SIP trunk connection with eONE, to display the system screen in the right pane.

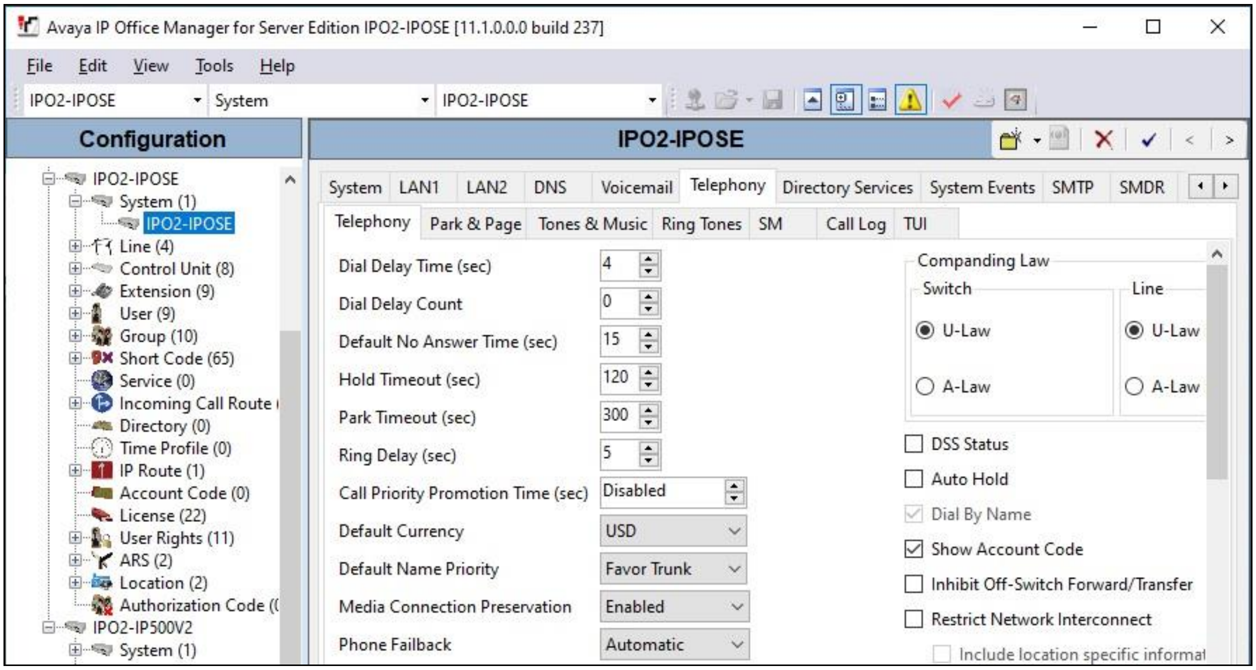
Select the **LAN1** tab, followed by the **LAN Settings** sub-tab in the right pane. Make a note of the **IP Address**, which will be used later to configure eONE. Note that IP Office can support SIP trunk on the LAN1 and/or LAN2 interfaces, and the compliance testing used the LAN1 interface.



Select the **VoIP** sub-tab. Make certain that **SIP Trunks Enable** is checked, as shown below. Retain the default values in the remaining fields.



Select the **Telephony** tab, followed by the **Telephony** sub-tab in the right pane. Uncheck **Inhibit Off-Switch Forward/Transfer** if transfer from eONE to PSTN destinations is desired. In the compliance testing, this parameter was disabled.



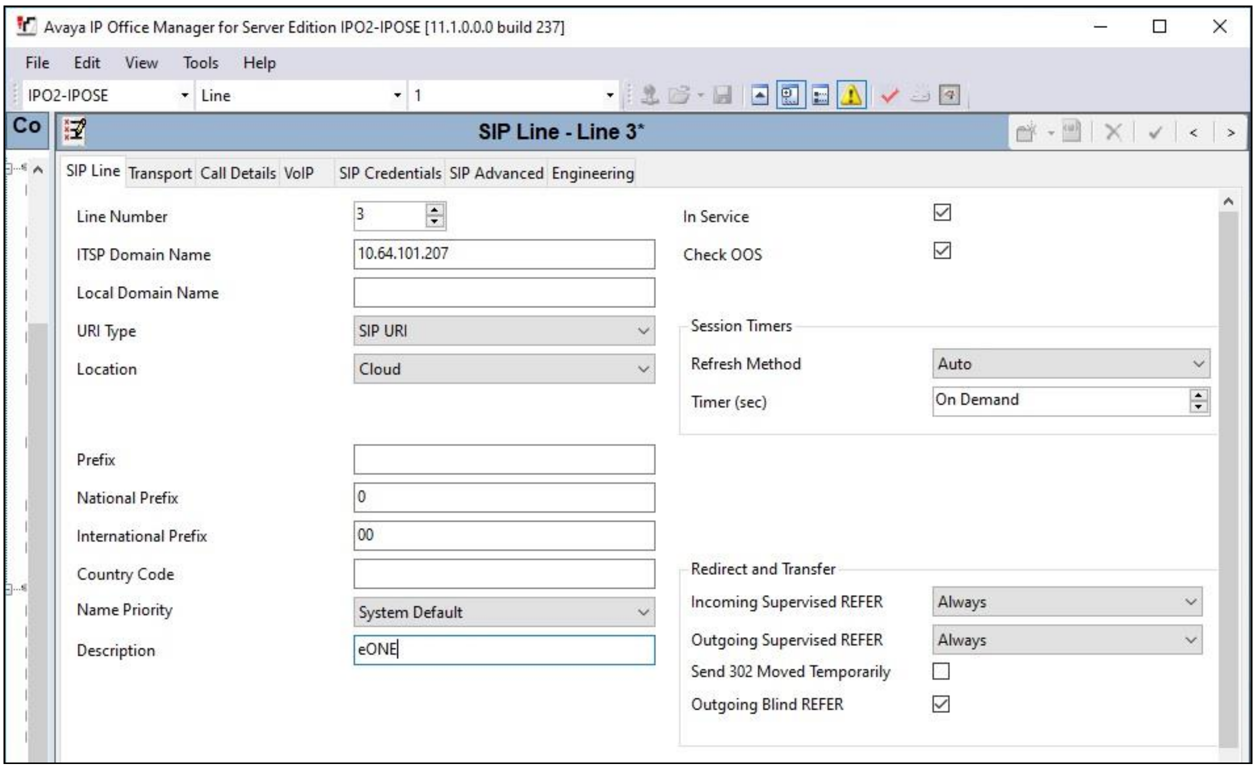
5.3. Administer Line

From the configuration tree in the left pane, right-click on **Line** under the IP Office system used for SIP trunk connection with eONE, and select **New → SIP Line** from the pop-up list to add a new SIP line (not shown).

Select the **SIP Line** tab. For **ITSP Domain Name**, enter the IP address of the eONE Media server with the CIMedia ARC SIP Telecom Services component.

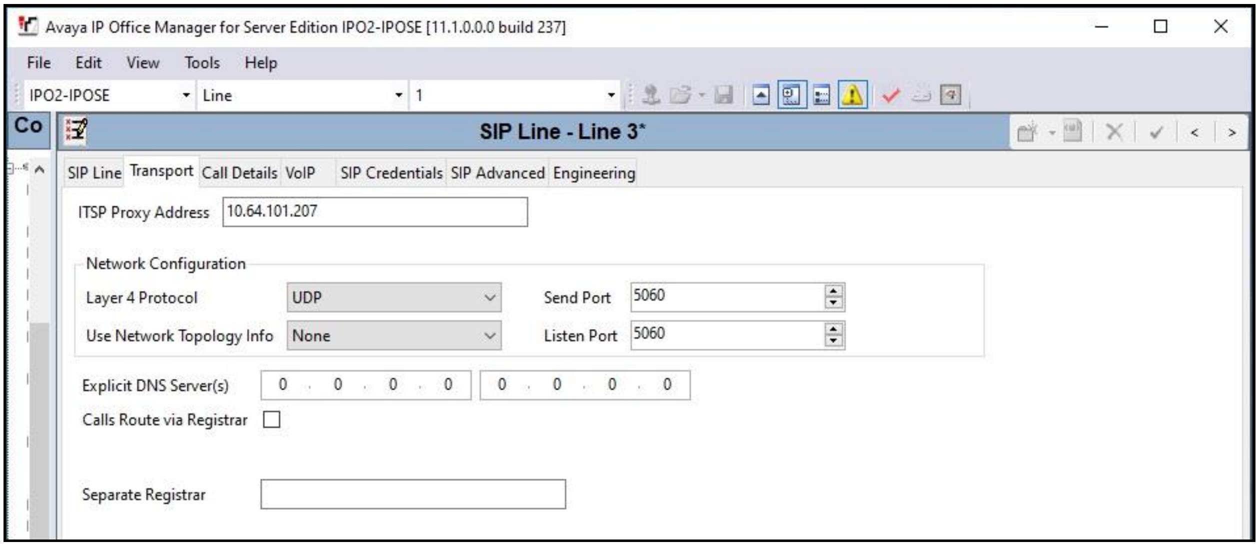
For **Incoming Supervised REFER** and **Outgoing Supervised REFER**, select "Always" as shown below.

Retain the defaults in the remaining fields.

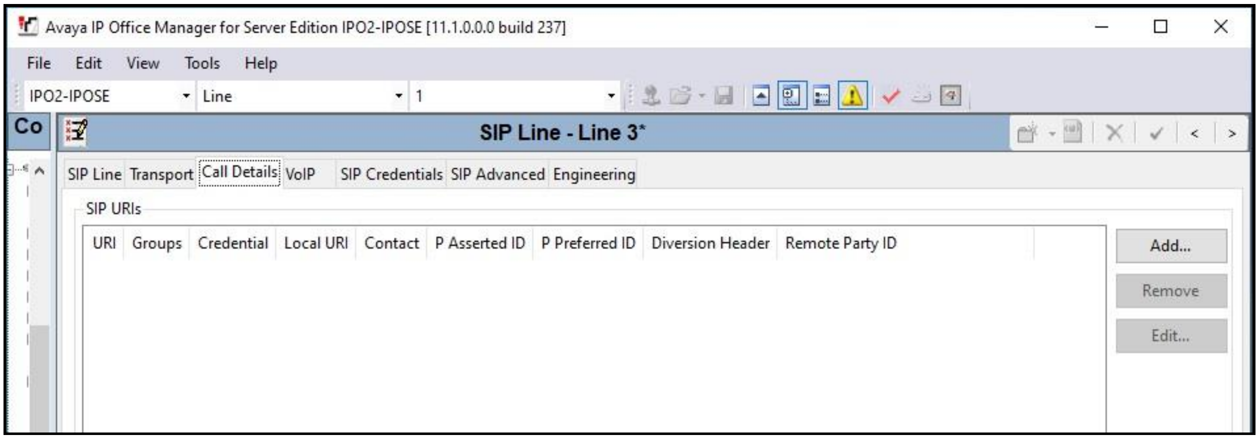


Select the **Transport** tab. For **ITSP Proxy Address**, enter the IP address of the eONE Media server with the CIMedia ARC SIP Telecom Services component. Uncheck **Calls Route via Registrar** as shown below and retain the default values in the remaining fields.

Note that eONE can support TLS, UDP and TCP, and the compliance testing used the UDP protocol.

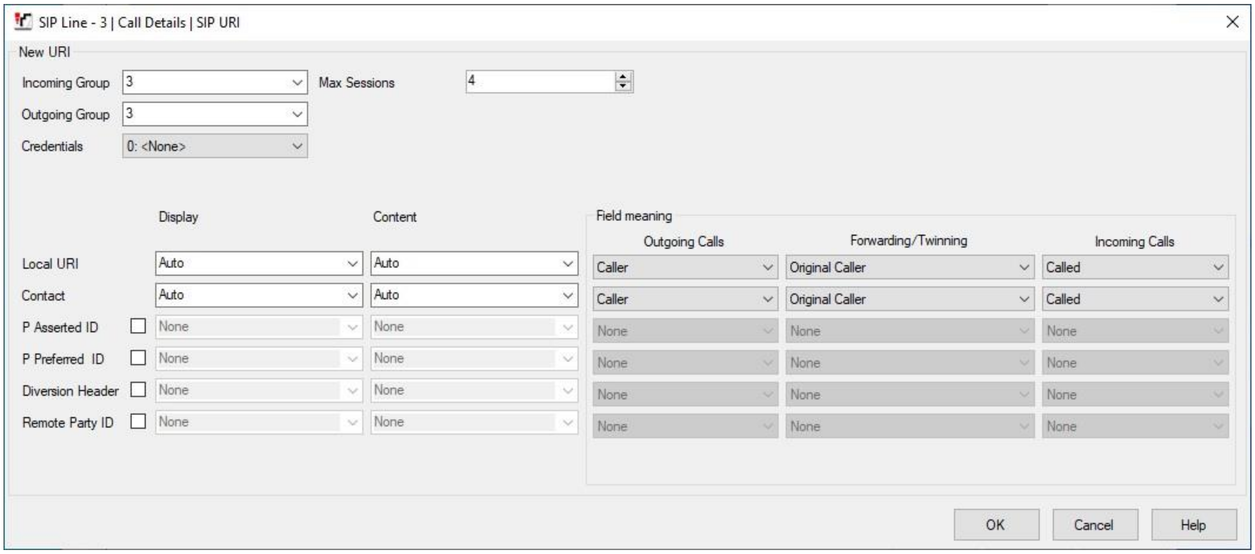


Select the **Call Details** tab, followed by **Add** in the **SIP URIs** sub-section.



The screen below is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

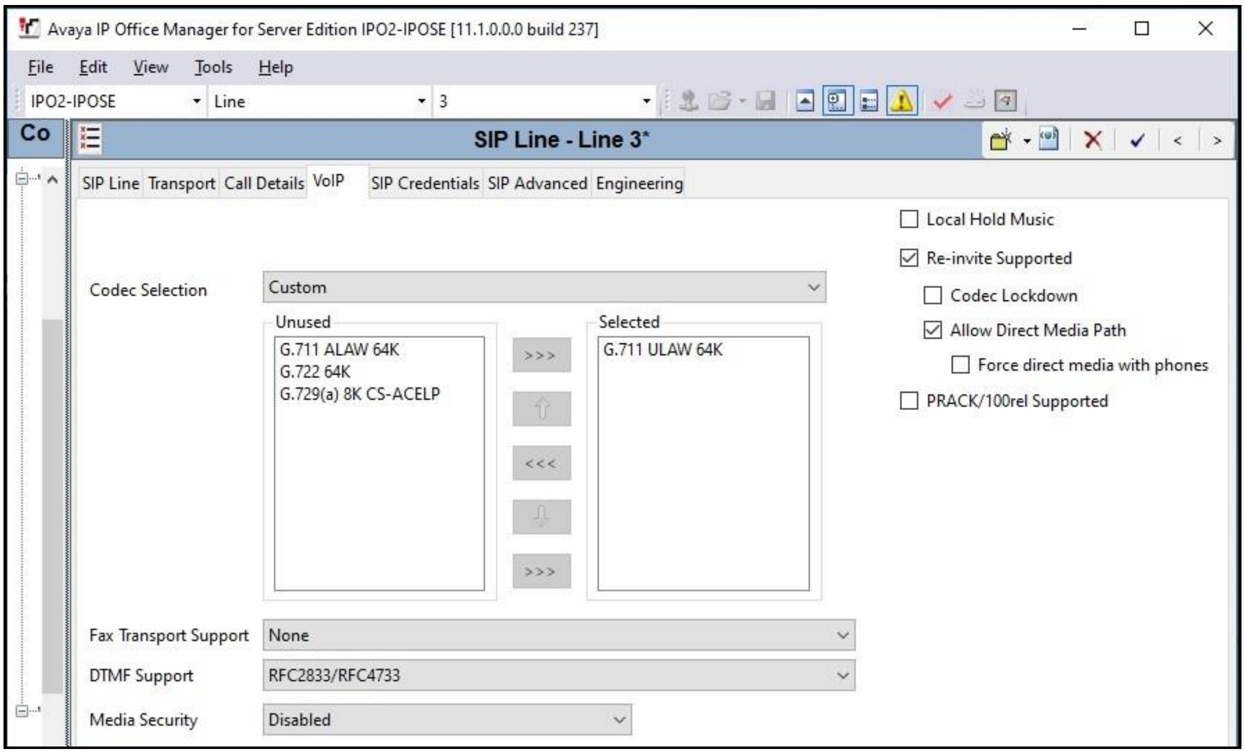
- **Incoming Group:** An available incoming group number.
- **Outgoing Group:** An available outgoing group number.
- **Max Sessions:** The maximum number of simultaneous calls.



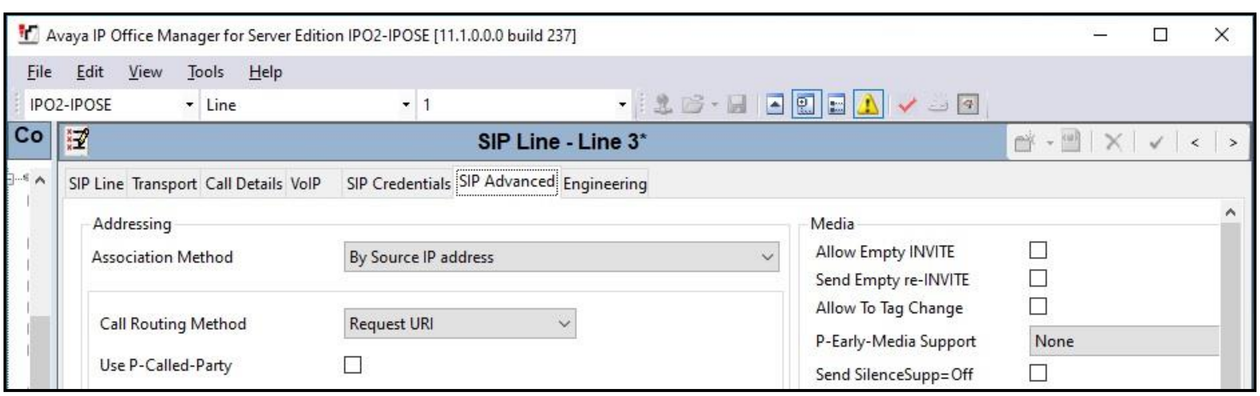
Select the **VoIP** tab. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Codec Selection:** "Custom"
- **Selected:** Retain the relevant G.711 codec variant.
- **Media Security:** "Disabled"
- **Re-invite Supported:** Check this parameter.
- **Allow Direct Media Path:** Check this parameter.

Note that eONE only supports the G.711 codec variant.



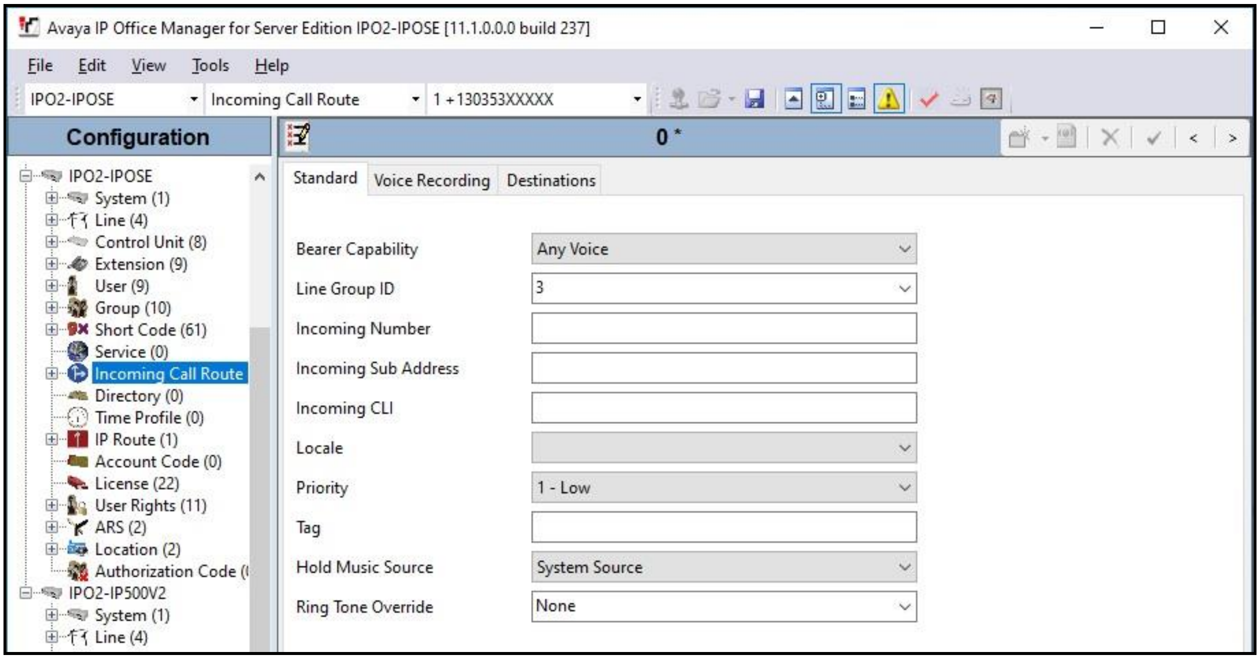
Select the **SIP Advanced** tab. For **Call Routing Method**, select "Request URI" as shown below. Retain the default values in the remaining fields.



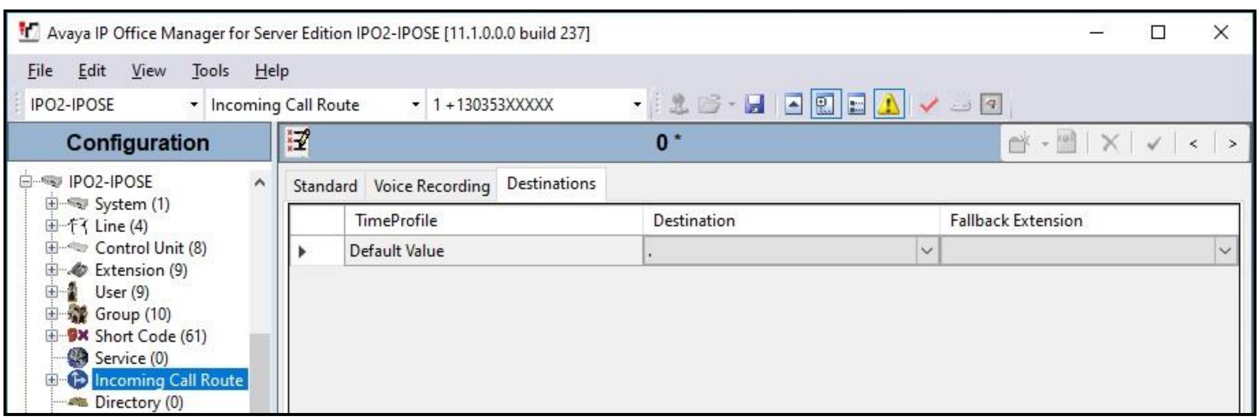
5.4. Administer Incoming Call Route

From the configuration tree in the left pane, right-click on **Incoming Call Route** under the IP Office system used for SIP trunk connection with eONE and select **New** from the pop-up list to add a new route for incoming calls from eONE.

For **Line Group Id**, select the incoming group number from **Section 5.3**, in this case "3". Retain the default value in the remaining fields.



Select the **Destinations** tab. For **Destination**, enter "." to match any dialed number from eONE.



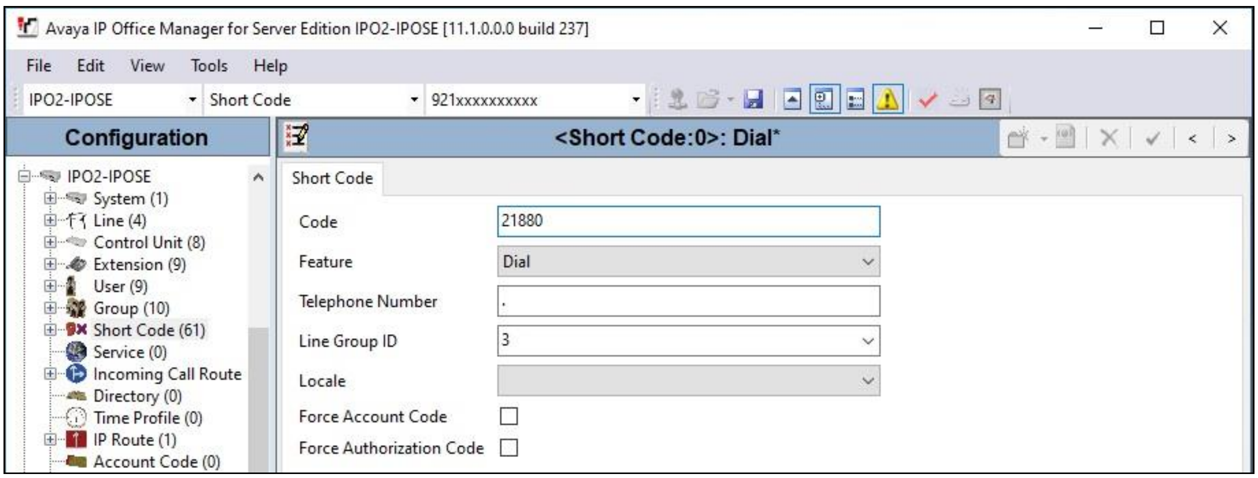
5.5. Administer Short Code

Configure a set of short codes for routing of outgoing calls to eONE and for routing of incoming calls from eONE to the PSTN.

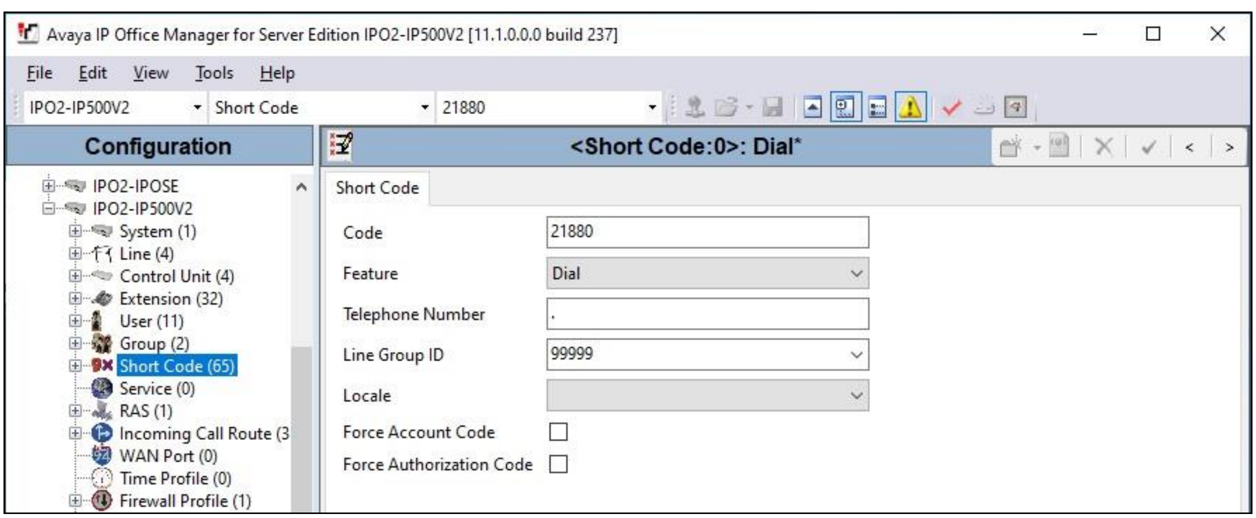
5.5.1. Short Code for Outgoing Calls to eONE

From the configuration tree in the left pane, right-click on **Short Code** under the primary IP Office system and select **New** from the pop-up list to add a new short code for outgoing calls to eONE. In the compliance testing, all calls to 21880 are routed over the SIP trunk to eONE.

For **Code**, enter the appropriate value, in this case "21880". For **Telephone Number**, enter "." to match the dialed number. For **Line Group ID**, select the outgoing group number from **Section 5.3**. Retain the default values in the remaining fields.



Repeat this section to add similar short code for the expansion IP Office system, which is named **IPO2-IP500V2** in this case. For **Line Group ID**, select the applicable outgoing group ID for the SCN trunk that connects to the primary IP Office system, in this case "99999" as shown below.



5.5.2. Short Code for Incoming Calls from eONE to PSTN

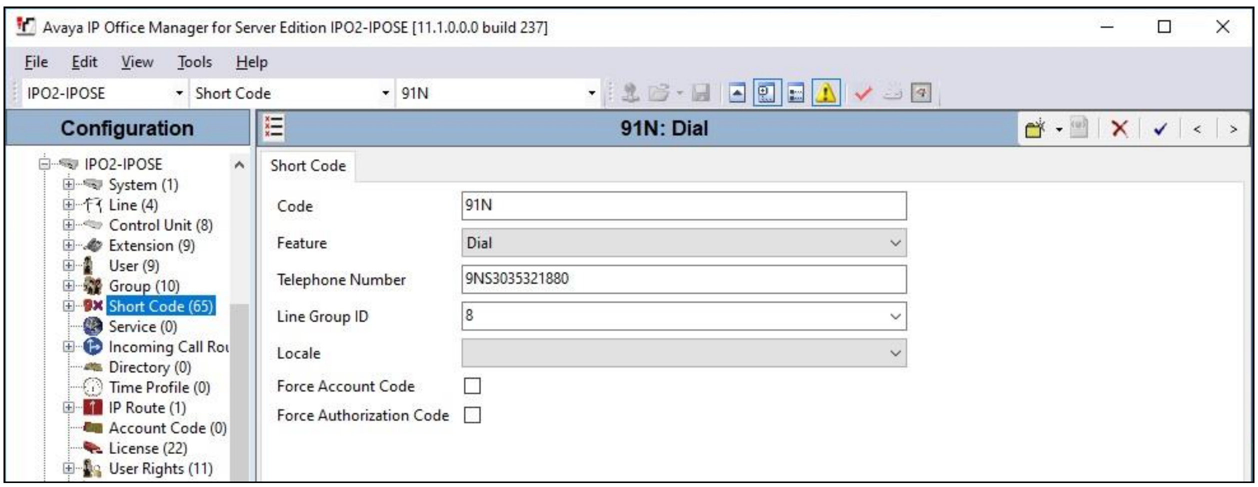
From the configuration tree in the left pane, right-click on **Short Code** under the primary IP Office system and select **New** from the pop-up list to add a new short code for incoming calls from eONE to the PSTN. In the compliance testing, eONE will add the prefix "91" for outbound call to the PSTN, and therefore a new short code is created for routing of such call.

For **Code**, enter the appropriate value, in this case "91N".

For **Telephone Number**, enter pertinent value with desired manipulation of called and calling numbers. In the compliance testing, "9NS3035321880" was used to strip "1" from the called number prefix sent by eONE and to use "3035321880" as the calling number, as shown below.

For **Line Group ID**, enter the outgoing group number for the PSTN line, in this case "8".

Retain the default values in the remaining fields.



6. Configure Computer Instruments eONE

This section provides the procedures for configuring eONE. The procedures include the following areas:

- Launch web interface
- Administer company management
- Administer system configuration
- Administer collect and store
- Administer extension manager
- Administer menu manager
- Administer VXML file

The configuration of eONE is typically performed by Computer Instruments deployment engineers, and the procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Web Interface

Access the eONE web interface by using the URL **http://ip-address/eci/voiceadmin/ LoginPage.aspx** in a browser window, where "ip-address" is the IP address of the eONE server with the web-based interface.

The **Login** screen below is displayed. Log in using the appropriate credentials.

The **Welcome to Computer Instruments** screen is displayed next.

Note that the relevant tenant in this case is "SIPIPO (43)" as shown below, which was pre-configured.

6.2. Administer Company Management

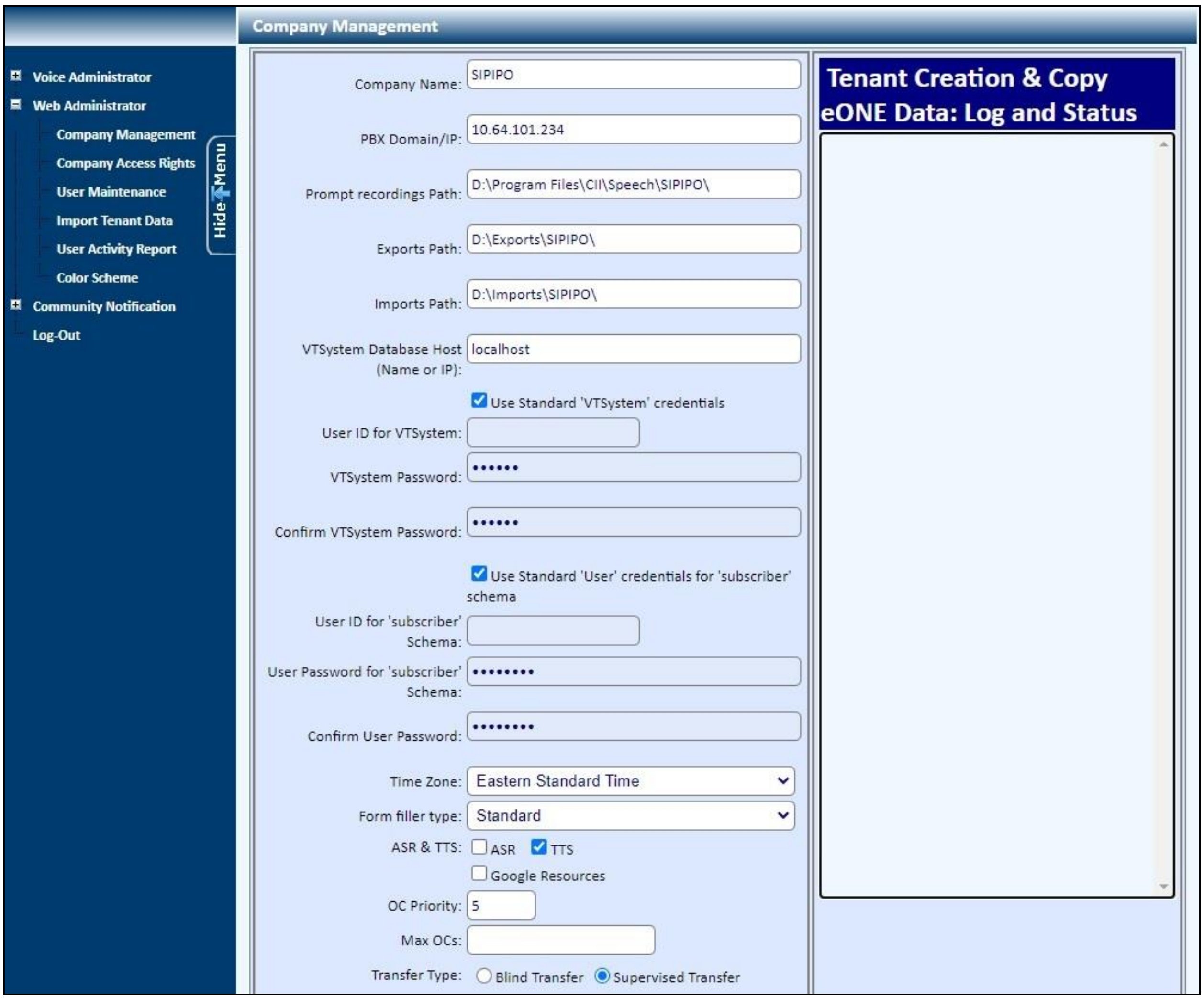
Expand and select **Web Administrator → Company Management** from the left pane to display the **Company Management** screen. Scroll down to the bottom of the screen to select the pertinent company entry and click **Edit** (not shown).

For **PBX Domain/IP**, enter the IP address of the primary IP Office system from **Section 5.2**.

For **Time Zone**, select the appropriate zone. For **ASR & TTS**, uncheck resources that are not used. In the compliance testing, only **TTS** was used.

For **Transfer Type**, select **Supervised Transfer**.

Retain the pre-configured values in the remaining fields.



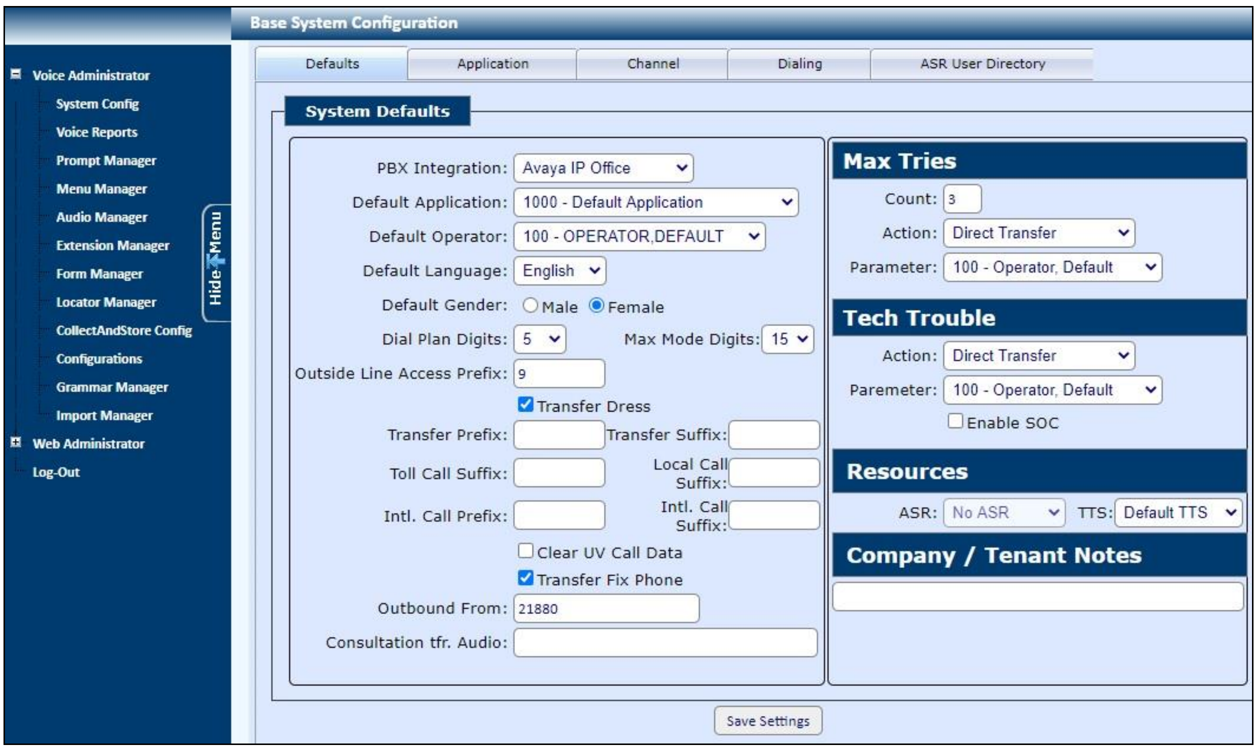
6.3. Administer System Configuration

Expand and select **Voice Administrator → System Config** from the left pane to display the **Base System Defaults** screen.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **PBX Integration:** "Avaya IP Office"
- **Dial Plan Digits:** The maximum length of internal extensions, in this case "5".
- **Outside Line Access Prefix:** The applicable prefix for calls to the PSTN, in this case "9".
- **Outbound From:** The eONE extension from **Section** 3.

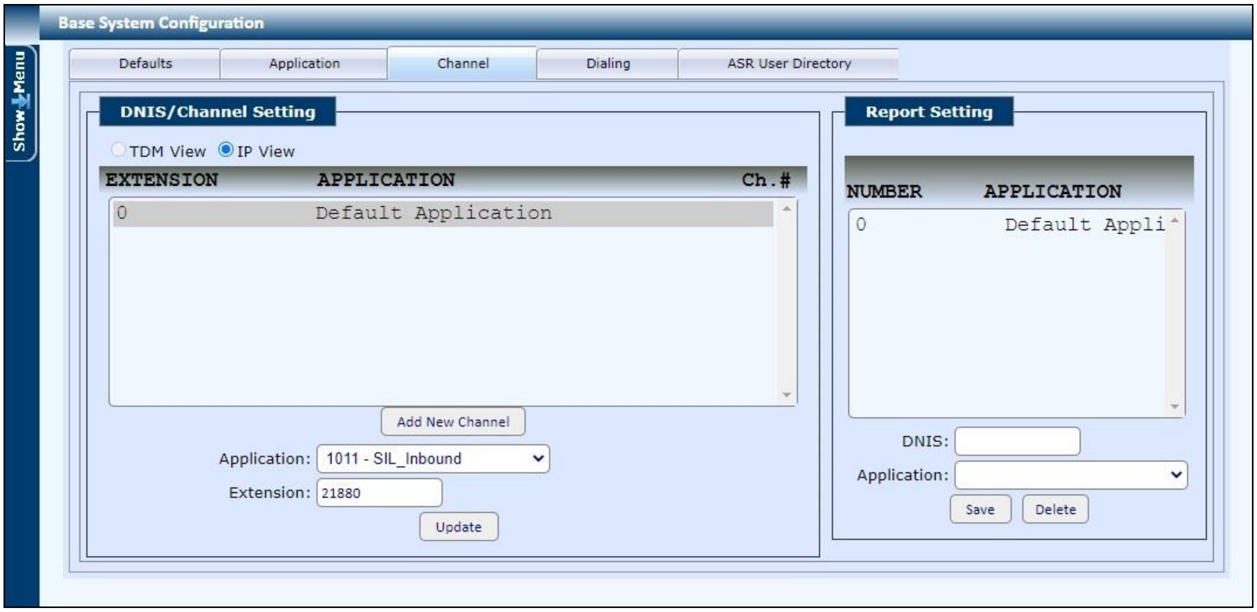
Note that for outbound calls from eONE to the PSTN, eONE will insert the value of the **Outside Line Access Prefix** plus the digit "1" as the called number.



Select the **Channel** tab. In the **DNIS/Channel Settings** sub-section, select the default entry. For **Application**, select the applicable pre-configured inbound application, in this case "1011 – SIL_Inbound".

For **Extension**, enter the eONE extension from **Section** 3.

Retain the default values in the remaining fields.

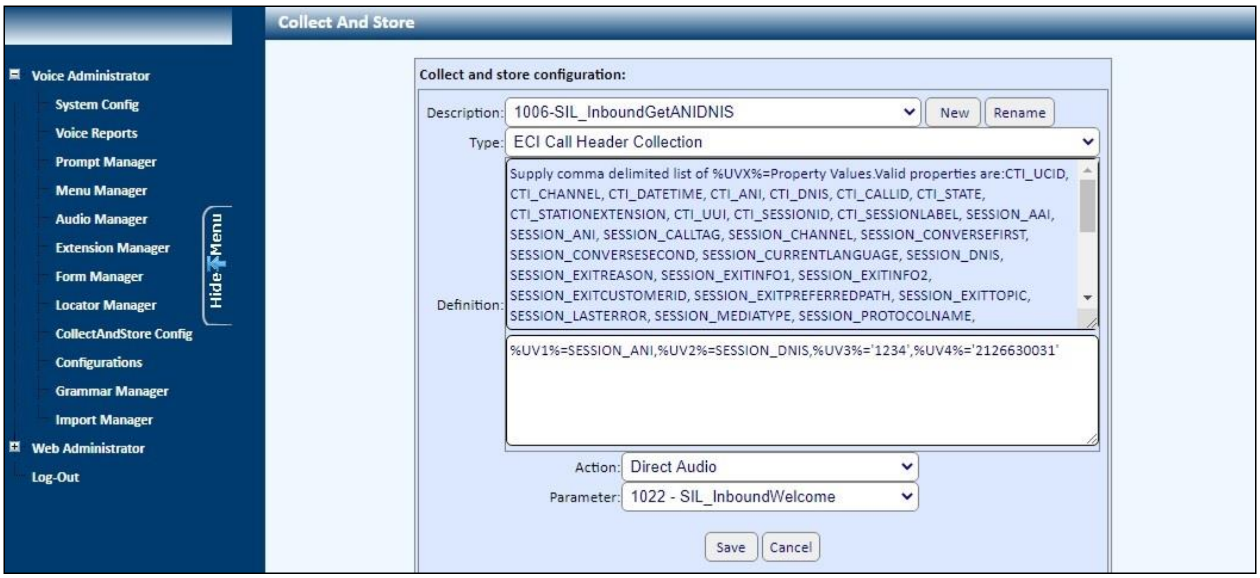


6.4. Administer Collect and Store

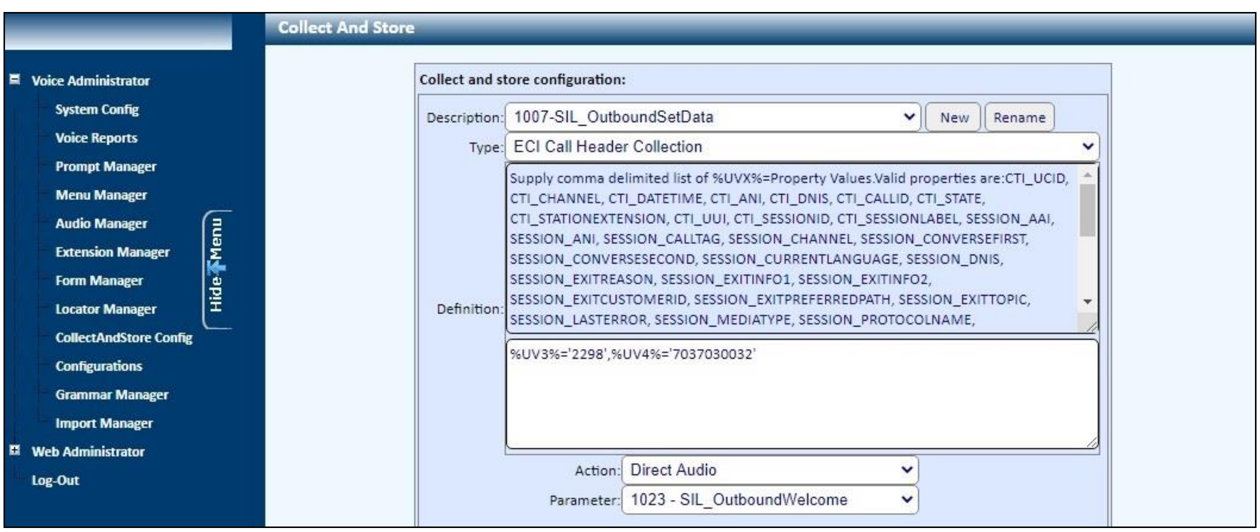
Expand and select **Voice Administrator → CollectAndStore Config** from the left pane to display the **Collect And Store** screen.

For **Description**, select the pertinent pre-configured entry associated with the inbound application, in this case "1006-SIL_InboundGetANIDNIS".

In the custom inbound application, parameter **UV4** stores the external transfer-to destination. Update content of **UV4** to the desired external destination as shown below. Retain the default values in the remaining fields.



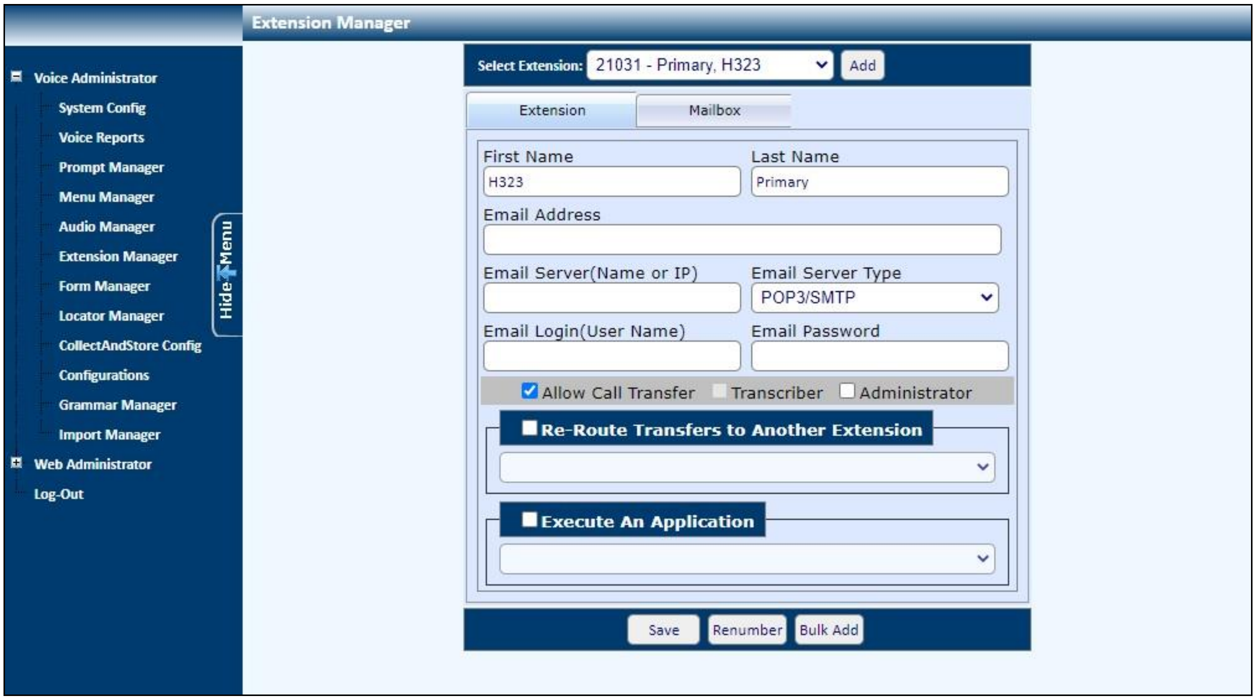
Repeat the procedures in this section to update the external transfer-to destination associated with the outbound application, as shown below.



6.5. Administer Extension Manager

Expand and select **Voice Administrator → Extension Manager** from the left pane to display the **Extension Manager** screen.

Follow reference **[3]** to create an entry for every internal extension that can be used by eONE as transfer destination. In the compliance testing, a total of five entries were created and shown below is one of the entries.



6.6. Administer Menu Manager

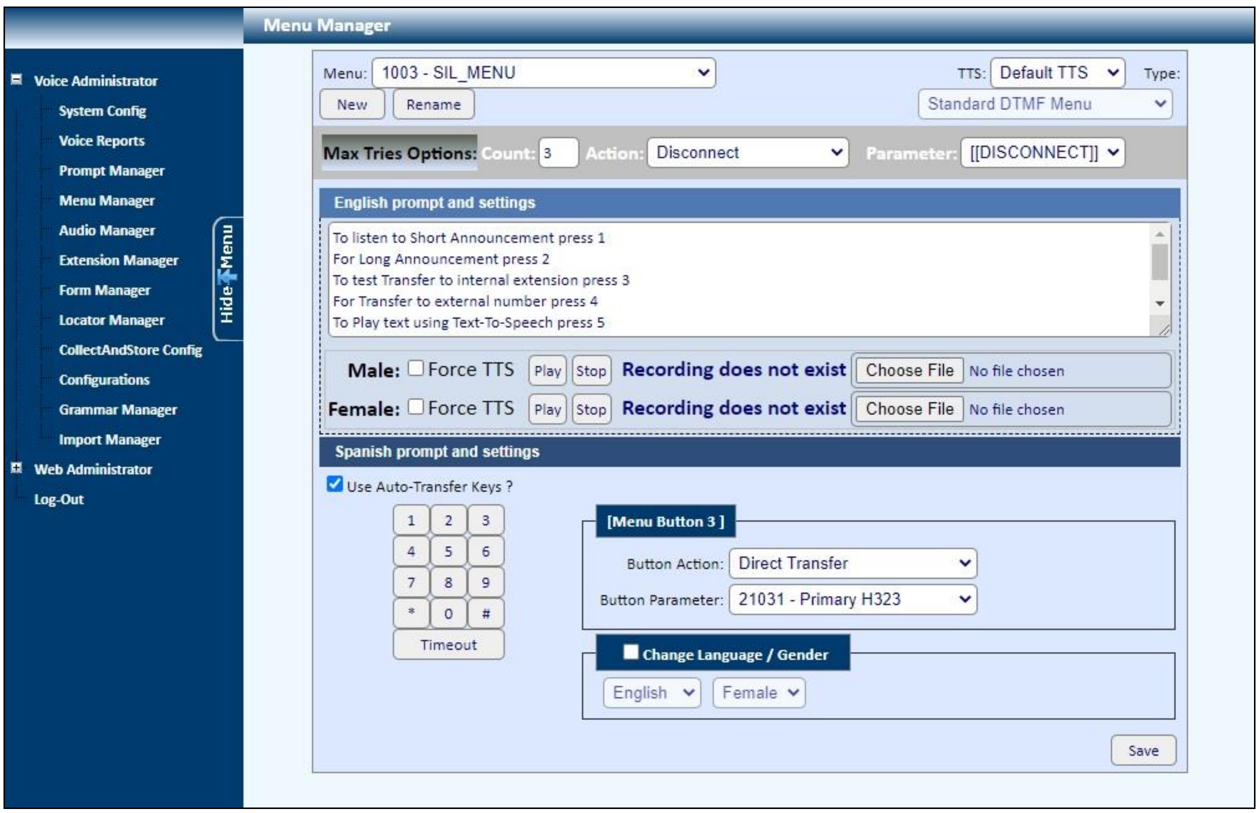
Select **Voice Administrator → Menu Manager** from the left pane to display the **Menu Manager** screen.

For **Menu**, select the pertinent pre-configured menu entry associated with the inbound application, in this case "1003 - SIL_MENU".

Under **Spanish prompt and settings**, press the keypad associated with the menu option for transfer to internal destination, in this case "3".

For **Button Parameter**, select the desired internal destination as shown below.

Repeat the procedures in this section to administer the transfer internal destination for the outbound application where applicable. In the compliance testing, the same menu entry was used for both the inbound and outbound applications.



6.7. Administer VXML File

Log into the Linux shell of the eONE Media server containing the CIMedia ARC VXML Services component.

Navigate to the **/home/arc/.ISP/Telecom/Exec/vxi** directory and use the copy command to create a new VXML configuration file as shown below, where "arcVXML2.vxml.cfg" is the existing default configuration file for ARC VXML 2.0 application and "21880" is the eONE extension from **Section** 3. Note that the eONE extension must be used as part of the name of the new configuration file.

Retain all default values in the newly created VXML configuration file.

```
[xxx@CI-TESTMS ~]# cd /home/arc/.ISP/Telecom/Exec/vxi
[xxx@CI-TESTMS vxi]#
[xxx@CI-TESTMS vxi]# cp arcVXML2.vxml.cfg arcVXML2.21880.vxml.cfg
```

Open the newly created file, in this case "arcVXML2.21880.vxml.cfg". Scroll down to the bottom of the file.

For **APP_NAME**, enter any descriptive name. For **SCRIPT**, enter the URL shown below where "10.64.101.206" is the IP address of the eONE server.

Retain the default values in the remaining fields.

```
#APP_NAME=arcVXML2
CACHE_DIR=/tmp/VXML2
KEEP_CACHE_DIR=1
SPEECH_REC=0
RESERVE_SPEECH_RESOURCE=0
VALIDATE_SCRIPTS=0
DEFAULT_COMPRESSION=COMP_WAV
#TRANSFER_MODE=BLIND
TRANSFER_MODE=LISTEN_ALL
#TRANSFER_FORMAT=IP
TRANSFER_FORMAT=NONE
#TTS_SERVER=LOQUENDO,MSS
TTS_SERVER=MSS
TTS_LANGUAGE=ENGLISH_AMERICAN
SR_LANGUAGE=ENGLISH_AMERICAN
#HTTP_VERSION=1.0
MRCP_ASR=MSS
NETWORK_ANNOUNCEMENT=0
#SKIP_TIME_IN_SECONDS=2
SCRIPT_MAXAGE=0
SCRIPT_MAXSTALE=0
APP_NAME=SIL_Inbound
SCRIPT=http://10.64.101.206/eCI/VXML/eONEMS_Inbound.vxml
```

7. Verification Steps

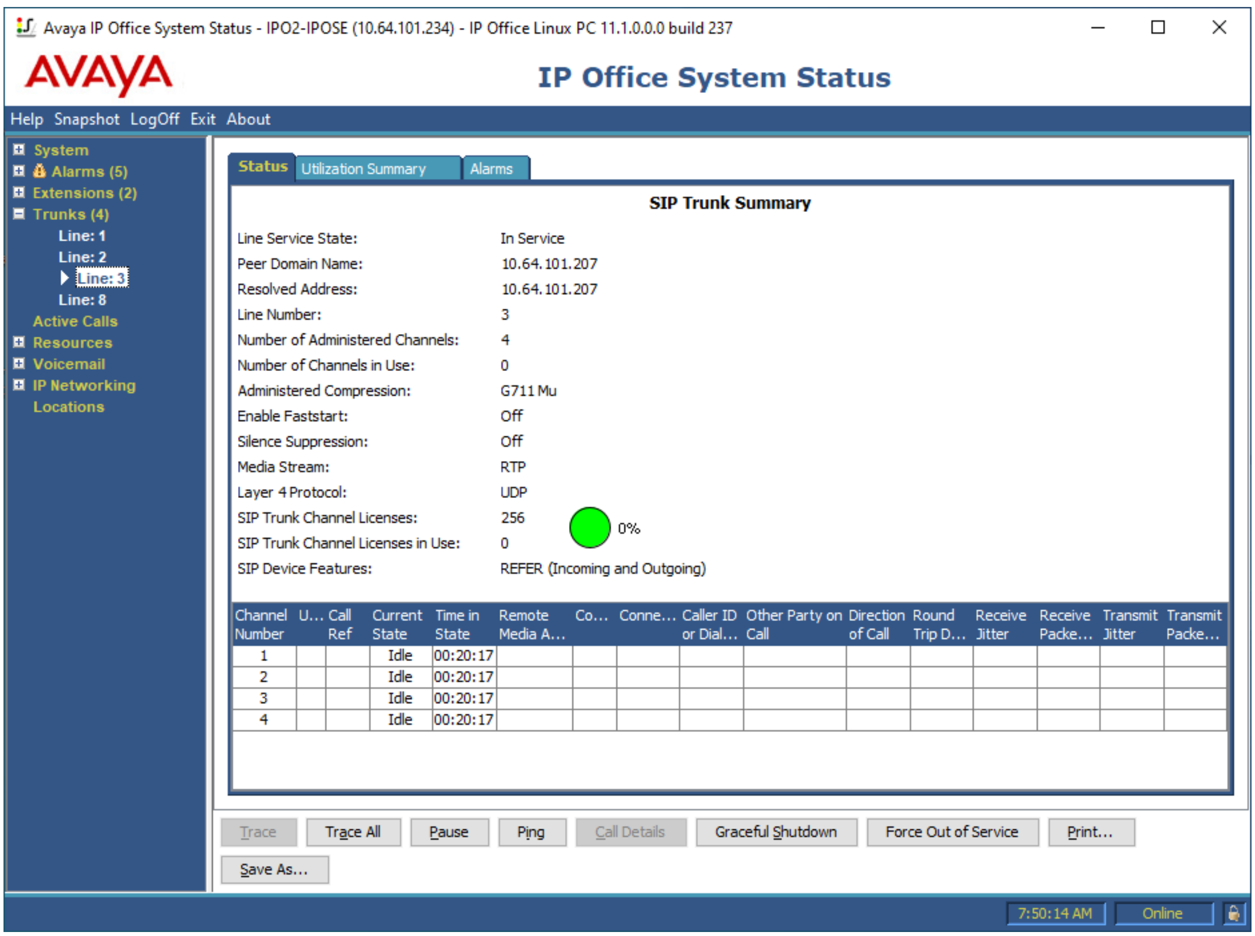
This section provides the tests that can be performed to verify proper configuration of IP Office and eONE.

7.1. Verify Avaya IP Office

From the **Avaya IP Office Manager for Server Edition IPO2-IPOSE** screen shown in **Section 5.1**, select **File → Advanced → System Status** to launch the System Status application, and log in using the appropriate credentials.

The **Avaya IP Office System Status – IPO2-IPOSE** screen is displayed. Expand **Trunks** in the left pane and select the SIP line from **Section 5.3**, in this case "3".

Verify that the **SIP Trunk Summary** screen shows all channels with **Current State** of "Idle", as shown below.



7.2. Verify Computer Instruments eONE

This section provides the tests that can be performed to verify the eONE inbound and outbound applications.

7.2.1. Inbound Application

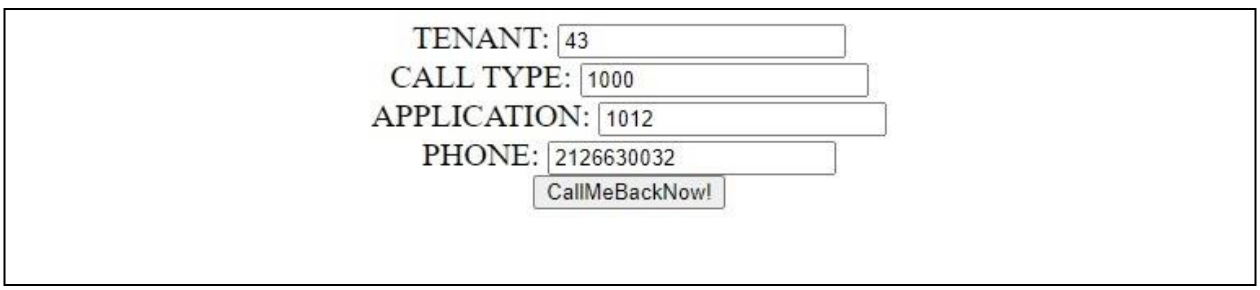
Establish an incoming trunk call from PSTN with eONE. Verify that the calling party hears the appropriate greeting associated with the inbound application.

7.2.2. Outbound Application

In a browser window, enter the URL associated with the eONE outbound application, in this case **http://10.64.101.206/MakeACallIPO.html** where "10.64.101.206" is the eONE server with the web-based interface.

The screen below is displayed. For **PHONE**, enter the phone number associated with an external destination on the PSTN. Retain the default values in the remaining fields and click **CallMeBackNow!**

Verify that an outbound call is initiated from eONE to the external destination. Answer the call at the external destination and verify that the called party hears the appropriate greeting associated with the outbound application.



8. Conclusion

These Application Notes describe the configuration steps required for Computer Instruments 7.0 to successfully interoperate with Avaya IP Office Server Edition 11.1.

9. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya IP Office™ Platform with Manager*, Release 11.1, Issue 1, April 2020, available at http://support.avaya.com.

2. *eONE User's Manual*, Version 7.0, 2020, available at http://instruments.com.

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.