



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring WinExpress 3.0 with Avaya IP Office Server Edition R10 – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for WinExpress 3.0 to interoperate with Avaya IP Office Server Edition Release 10. WinExpress is a universal system which offers a real-time, multi-tasking, seamless interface between the hotel exchange and the hotel front office system. It comprises of two main components, i.e., Phoenix voicemail, and Unicorn which includes calls billing and interface solution. In the compliance testing, WinExpress used SIP Users, Short Codes, SMDR, and Configuration Web Service interfaces from Avaya IP Office Server to provide voicemail, wake-up call, room status, mini-bar posting, call billing, as well as name and user profile template change, and do not disturb features.

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 WinExpress 3.0 to interoperate with Avaya IP Office Server Edition R10. WinExpress is a Windows-based hospitality system that provides a seamless interface with a hotel's Front Office System and Avaya IP Office Server. It comprises of two main components, i.e., Phoenix voicemail, and Unicorn which includes calls billing and interface solution. In the compliance testing, WinExpress used SIP Users, Short Codes, SMDR, and Configuration Web Service interfaces from Avaya IP Office Server to provide voicemail, message waiting lamp control, wake-up call, room status and mini-bar posting, call billing, name and user profile template change, and do not disturb features.

In the compliance testing, Phoenix voicemail lines registers as SIP users on Avaya IP Office Server for voice mail and wakeup services and posting of mini-bar and room status through the phones. The voicemail lines were configured as members of a hospitality hunt group. Guest room phones were forwarded to these voicemail lines when busy or did not answer within the specified time. Each voicemail line will forward to another in a round robin fashion till one is available.

For the voicemail coverage scenarios, voicemail messages were recorded and saved on WinExpress. Short Codes were used to activate/deactivate the Message Waiting Indicator (MWI).

The Unicorn component was used in the compliance testing to initiate the room Check-In, Check-Out, and Move requests on WinExpress. In the compliance testing, multiple rights templates were set up on Avaya IP Office Server for use with Check-In and Check-Out guests. Unicorn used the Configuration Web Service to send updates to Avaya IP Office Server on the guest name and user rights template as part of the Check-In, Check-Out, and Move process.

The Station Message Detail Reporting (SMDR) interface was used by WinExpress to capture calls made from room phones for the purpose of call billing.

2. General Test Approach and Test Results

The feature test cases were performed manually. Calls were made from the PSTN, and from local users, to the hospitality hunt group by dialing the different extensions for voice message recording/retrieval, mini-bar and room status posting and setting of wake-up call. Unicorn (with the aid of a PMS Simulator) was used to manually initiate Check-In/Check-Out/Move requests, update guest info, and to set Do Not Disturb. For SMDR testing, outgoing calls were made to the PSTN (simulated) and the WinExpress call billing reports were verified. The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to WinExpress, and rebooting the Avaya IP Office server and WinExpress server.

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 WinExpress utilized enabled capabilities of TLS, specifically for Web Configuration Service.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on WinExpress:

- Registration of SIP users
- Handling of voicemail and text messages including message waiting lamp control
- Voicemail recording and retrieval, with proper message waiting lamp activation/deactivation for users with analog, digital and IP telephones
- Scheduling and delivering of wake-up call requests, including retried attempts and escalation to Operator
- Turning on/off of MWI for both voice using short codes
- Posting of room status and mini-bar consumption from the room phones (with corresponding results shown in Unicorn)

- Use of Configuration Web Services to update guest name and user rights template associated with Check-In, Check-Out, Do Not Disturb and Move requests from Unicorn
- Capture calls made from room phones for the purpose of call billing

The serviceability testing focused on verifying the ability of WinExpress to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet cables to WinExpress server and rebooting of IP Office server and WinExpress server.

2.2. Test Results

All test cases were executed and passed. The following were observed:

- Voice Mail was not working after IP Office Server restart. A patch OS-9913 was required for Phoenix HMP driver. This patch will be incorporated in next driver update and WinExpress setup.

2.3. Support

Technical support on WinExpress can be obtained through the following:

- **Website:** <http://www.fcscs.com/>

3. Reference Configuration

The configuration used for the compliance testing is shown below. In the compliance testing, WinExpress was installed on a single server. Unicorn initiates room Check-In/Check-Out and room move via a PMS Simulator, capture SMDR, and to set Do Not Disturb. Phoenix handles the voicemail reception, recording and playback, message waiting lamps, wake-up calls as well as room and mini-bar status posting and reporting. In this compliance testing, Avaya IP Office Server Edition comprises of a Primary Server and an Expansion Module (IP500 V2). Avaya IP Deskphones (H.323) 96x1, 96x0, 16xx, Avaya Digital Deskphones 14xx as well as Analog Deskphone are deployed as guest room, front desk, operator and admin phones.

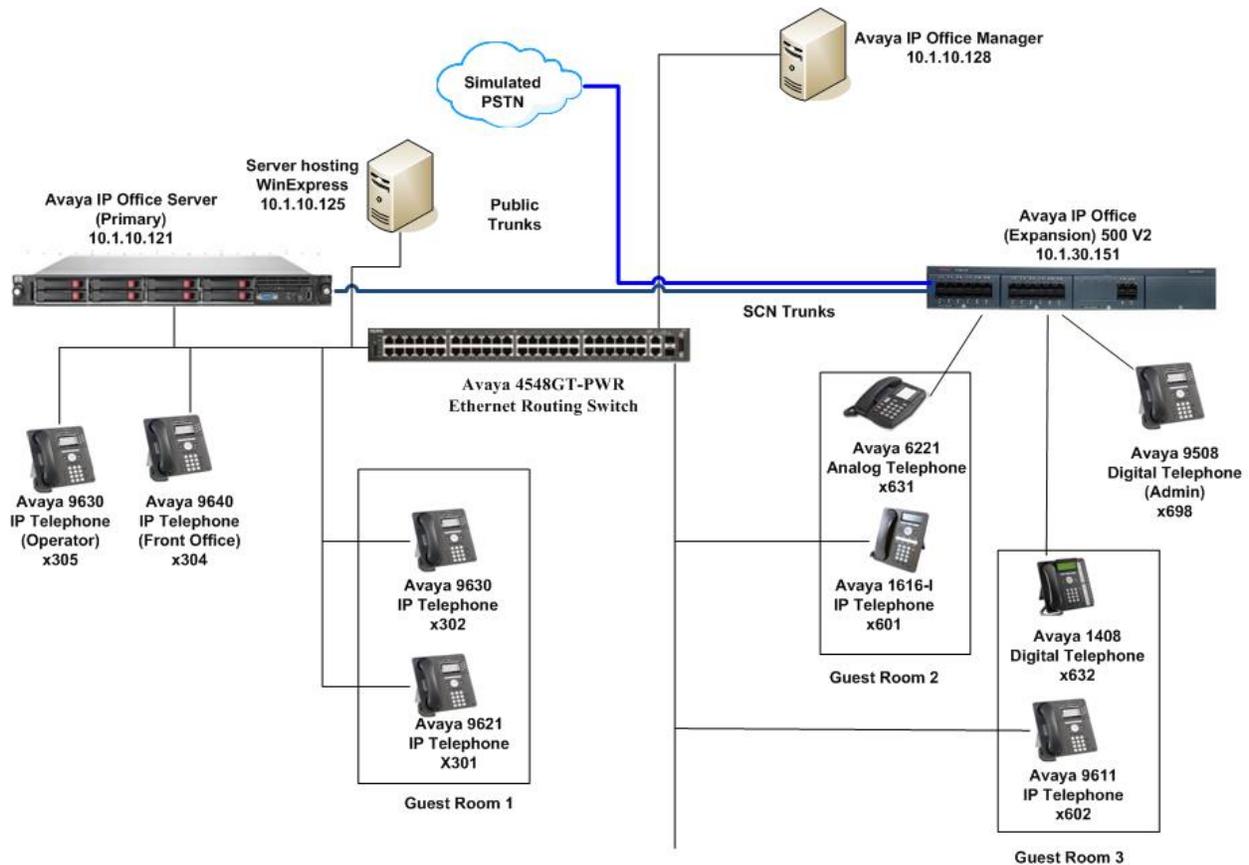


Figure 1: Test Configuration of WinExpress 3.0 and Avaya IP Office Server R10

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)	10.0.0.2.0 build 10
Avaya IP Office 500 V2 (Expansion)	10.0.0.2.0 build 10
Avaya IP Office Manager	10.0.0.2.0 build 10
Avaya 96x1 H323 IP Deskphone	6.6401
Avaya 96x0 H323 IP Deskphone	3.270B
Avaya 950x Digital Deskphone	R55
Avaya 16xx H323 IP Deskphone	1.3100
Avaya 14xx Digital Deskphone	R47
Avaya 6221 Analog Deskphone	-
WinExpress Server - FCS Phoenix and Unicorn running on Microsoft Windows 2012 R2 SP1 hosted on VMware 5.x platform	*2.2 (Phoenix) with patch OS-9913 1.3 (Unicorn)

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.

* Patch for HMP driver on issue observed in **Section 2.2**.

5. Configure Avaya IP Office

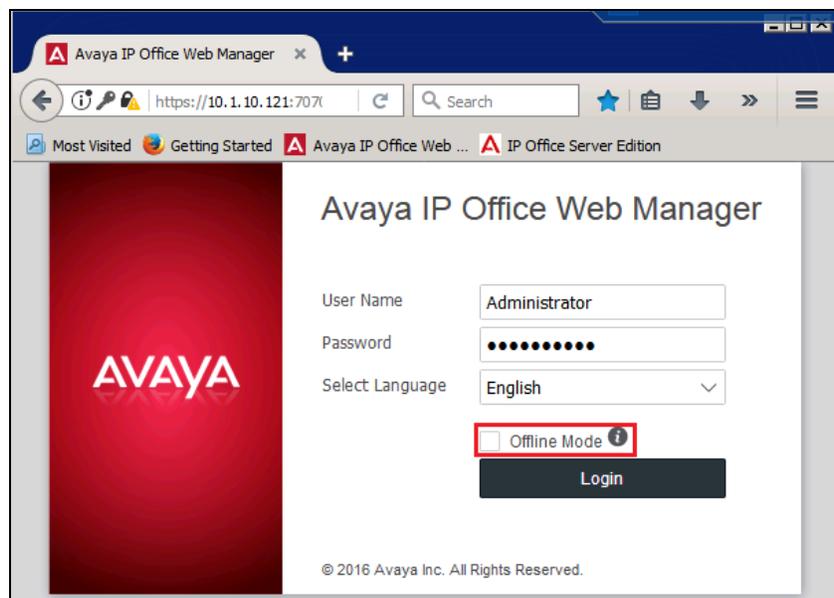
This section provides the procedures for configuring Avaya IP Office. The procedures include the following:

- Launch Avaya IP Office Web Manager
- Verify Avaya IP Office Server license
- Obtain LAN IP address
- Administer SIP Registrar
- Administer SIP Extensions
- Administer SIP Users
- Administer Hospitality Hunt Group
- Administer Voicemail Users
- Administer Short Codes for MWI ON/OFF
- Administer Analog User MWI
- Administer User Rights
- Administer System Password
- Administer SMDR
- Administer Security Settings

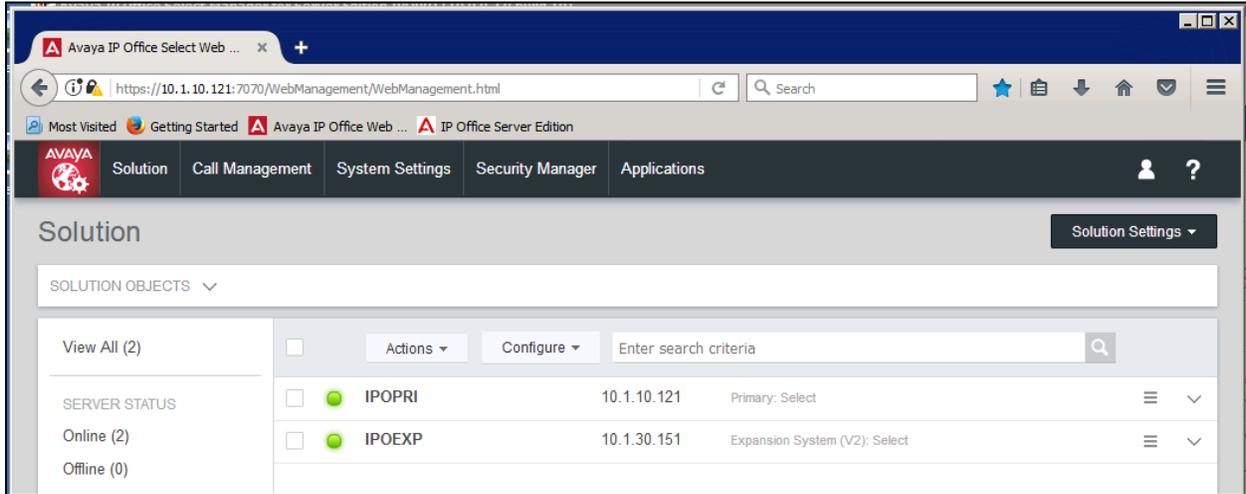
5.1. Launch Avaya IP Office Web Manager

Access the Avaya IP Office Web Manager by using the URL “https://ip-address:7070” in an Internet browser window, where “ip-address” is the IP address of the IP Office Primary Server.

The login screen is displayed. Notice that there is **Offline Mode** checkbox which is required if administering system parameters. Log in using the appropriate credentials.



The home screen is shown below.



5.2. Verify Avaya IP Office Server License

From the home screen, select **System Settings** → **Licenses**. Select the **Primary Server (IPOPRI)** where the SIP user will be administered.



Scroll down to display the **3rd Party IP Endpoints**. Verify that there is sufficient license, **Expiry Date** and the **Status** is “Valid”. This license is required for Phoenix to register to IP Office as SIP Users.

The screenshot shows the Avaya IPOPRI License Management interface. The top navigation bar includes Solution, Call Management, System Settings, Security Manager, and Applications. The main header is 'License | IPOPRI'. On the left, there are two menu items: 'Manage Licenses' (Manage Solution-Wide Licenses) and 'Remote Server' (Configure License Server). The main content area displays license details: License Mode (License Normal), Licensed Version (10.0), PLDS Host ID (479675452799), PLDS File Status (Valid), and Select Licensing (Valid). Below this is a search bar and a 'PLDS License' dropdown. A table lists various license features with columns for Feature, Instances, Status, Expiry Date, and Source. The '3rd Party IP Endpoints' row is highlighted with a red box, showing 1000 instances, a status of 'Valid', and an expiry date of 'Never'. Other features include Receptionist (10), SIP Trunk Channels (256), Office Worker (1000), Server Edition R.10 (150), Avaya Mac Softphone (1000), Additional Voicemail Pro (252), Devlink3 External Recorder (1), Allow Virtualization (10), and UMS Web Services (1000). The bottom right corner indicates 'Displaying 1 - 19 of 19'.

Feature	Instances	Status	Expiry Date	Source
Receptionist	10	Valid	Never	PLDS Nodal
SIP Trunk Channels	256	Valid	Never	PLDS Nodal
Office Worker	1000	Valid	Never	PLDS Nodal
Server Edition R.10	150	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal
Additional Voicemail Pro (p...	252	Valid	Never	PLDS Nodal
Devlink3 External Recorder	1	Valid	Never	PLDS Nodal
Allow Virtualization	10	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal

5.2.1. Obtain LAN IP Address

From the home screen, select **System Settings** → **System** → **IPOPRI** → **LAN1**. Make a note of the **IP Address**, which will be used later to configure WinExpress. Note that IP Office Server can support SIP on the LAN1 and/or LAN2 interfaces; in this compliance testing LAN1 interface is used.

The screenshot shows the Avaya IPOPRI System Configuration interface. The top navigation bar includes Solution, Call Management, System Settings, Security Manager, and Applications. The main header is 'System Configuration | IPOPRI'. On the left, there is a sidebar menu with options: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), and LAN2. The main content area is titled 'LAN Settings' and includes tabs for 'VoIP' and 'Network Topology'. A red banner at the top of the settings area states: 'These settings can only be changed in Offline mode.' Below this, the 'IP Address' field is highlighted with a red box and contains the value '10 . 1 . 10 . 121'. Other fields include 'IP Subnet Mask' (255 . 255 . 255 . 0) and 'Number Of DHCP IP Addresses' (133). The 'DHCP Mode' is set to 'Disabled' and the 'Advanced' section has a 'NO' button.

Similarly for Expansion server, select **System Settings** → **System** → **IPOEXP** → **LAN1**. Note the same for the Expansion Server **IPOEXP**.

The screenshot shows the Avaya System Configuration interface for the IPOEXP system. The navigation menu on the left includes System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), and LAN2. The main content area is titled 'System Configuration | IPOEXP' and has tabs for LAN Settings, VoIP, and Network Topology. A red banner at the top of the settings area states: 'These settings can only be changed in Offline mode.' The IP Address field is highlighted with a red box and contains the value '10 . 1 . 30 . 151'. Other settings include IP Subnet Mask (255 . 255 . 255 . 0), Primary Transfer IP Address (0 . 0 . 0 . 0), RIP Mode (None), Enable NAT (NO), DHCP Mode (Client), and Number Of DHCP IP Addresses (1).

5.3. Administer SIP Registrar

This portion of the administration required login in Offline mode as mentioned in **Section 5.1**. Select **System Settings** → **System** → **IPOPRI** → **LAN1** → **VOIP**. Ensure that **SIP Registrar Enable** is set to **YES**. Enter a valid **SIP Domain Name** for SIP endpoints to use for registration with IP Office. In this compliance testing, the **SIP Domain Name** is left **blank** so that the LAN IP address is used for registration. Ensure the **UDP** and **TCP** are set to **YES** for Layer 4 Protocol with **UDP Port 5060**. In this compliance testing, the UDP port is used for SIP registration by Phoenix. Leave the rest as default. Click **Update** at bottom of screen (not shown) to save.

The screenshot shows the Avaya System Configuration interface for IPOPRI. The left sidebar lists various system settings, with LAN1 selected. The main content area is divided into tabs: LAN Settings, VoIP, and Network Topology. The VoIP tab is active, showing H.323 GATEKEEPER and SIP REGISTRAR settings. The SIP REGISTRAR section includes: SIP Trunks Enable (YES), SIP Registrar Enable (YES), Auto-create Extension/User (NO), SIP Remote Extension Enable (NO), and SIP Domain Name (blank). The LAYER 4 PROTOCOL section includes: UDP (YES) with UDP Port 5060, and TCP (YES) with TCP Port 5060. Red boxes highlight the SIP Registrar Enable, SIP Domain Name, UDP, and TCP settings.

Section	Setting	Value
H.323 GATEKEEPER	H.323 Gatekeeper Enable	YES
	H.323 Signaling Over TLS	Disabled
	Auto-create Extension	NO
SIP REGISTRAR	SIP Trunks Enable	YES
	SIP Registrar Enable	YES
	Auto-create Extension/User	NO
	SIP Domain Name	
LAYER 4 PROTOCOL	UDP	YES
	UDP Port	5060
	TCP	YES
	TCP Port	5060

5.4. Administer SIP Extensions

In the compliance testing, the following SIP extensions with base extensions of **311-313** and **315-317** were created. Phoenix used the called-party number **311-313** for various hospitality features. Phoenix registered as extensions **315-317** to function as Voice Mail ports.

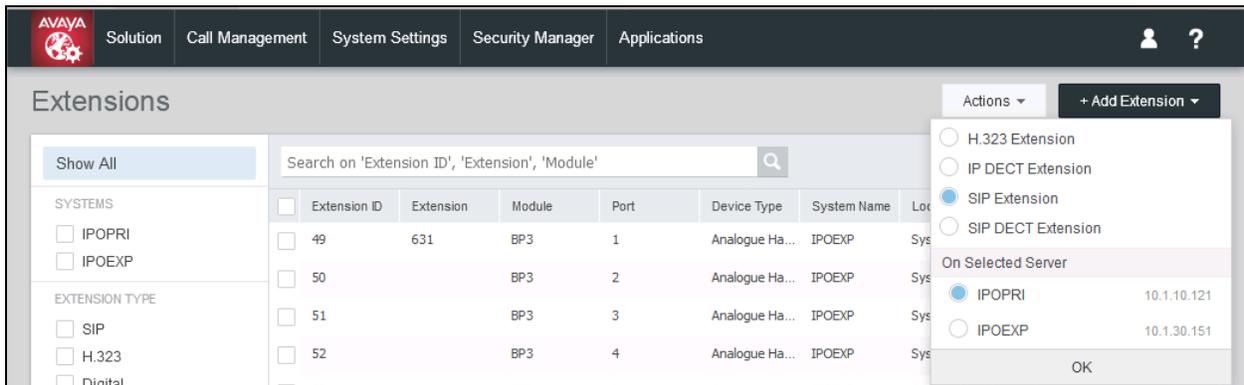
Note: Customer needs to purchase sufficient SIP ports to provide for the voicemail lines and services.

Phoenix can detect whether the call is routed from another phone or is an incoming direct call based upon the called-party number in the SIP INVITE to extensions 315-317. If it is direct hospitality hunt group, the caller is retrieving a voice message. But if it is indirect, where the called-party is user, the caller is leaving a voice message.

SIP Extension	Usage
315, 316 and 317	Phoenix registers to these extension for receiving voicemail calls
311	Post mini-bar/room status
312	Express leave voice message
313	Set wakeup call

Note: The above services tied to the numbers (311-313) are merely a sample configuration

From the home screen, select **Call Management** → **Extensions**. Click on **+Add Extension** and check **SIP Extension**, **IPOPRI**, and click **OK** to add a new SIP extension.



Enter the desired digits for **Base Extension** and set **Force Authorization** to **YES**, as shown below.

The screenshot shows the Avaya SIP Extension configuration interface for extension 315 (11200). The left sidebar has 'Common' selected. The main area shows the following settings:

Field	Value
Extension ID	11200
Base Extension	315
Device Type	Unknown SIP device
Caller Display Type	On
Reset Volume After Calls	NO
Location	Automatic
Fallback As Remote Worker	Auto
Force Authorization	YES

Click **VoIP** on the left pane and select **RFC2833/RFC4733** from the drop-down menu for the **DTMF Support** and click **Create** (not shown).

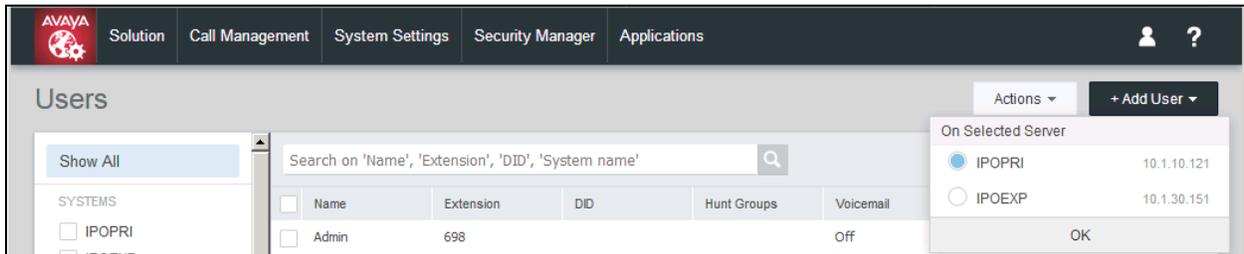
The screenshot shows the Avaya SIP Extension configuration interface for extension 315 (11200) with the 'VoIP' settings pane selected. The settings are as follows:

Field	Value
IP Address	0 . 0 . 0 . 0
Reserve License	None
Fax Transport	None
DTMF Transport	RFC2833/RFC4733
Requires DTMF	NO
Local Hold Music	NO
Allow Direct Media Path	YES
Re-INVITE Supported	YES

Repeat this section to add other SIP extensions.

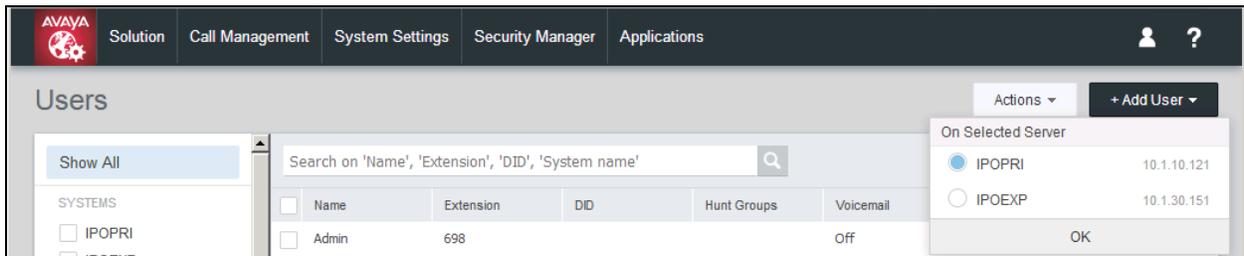
5.5. Administer SIP Users

From the home screen, select **Call Management** → **Users**. The primary SIP users **315**, **316** and **317** are for receiving calls and the secondary SIP users **311**, **312** and **313** are to forward calls to primary SIP users.

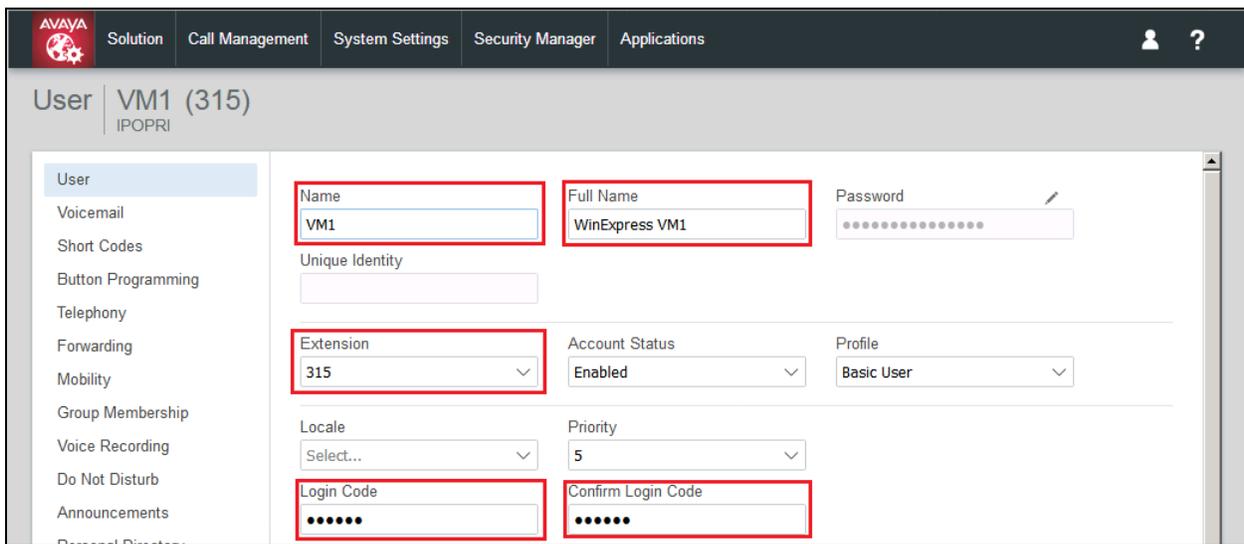


5.5.1. Administer Primary SIP Users

Click on **+Add User**, check **IPOPRI**, and click **OK** to add a new User.



Enter the desired values for **Name** and **Full Name**. For **Extension**, select the Base Extension from **Section 5.4**. Specify the **Login Code** and **Confirm Login Code** field, which will be used by Phoenix to log in as the SIP User. Phoenix registers using this primary SIP User to receive calls.



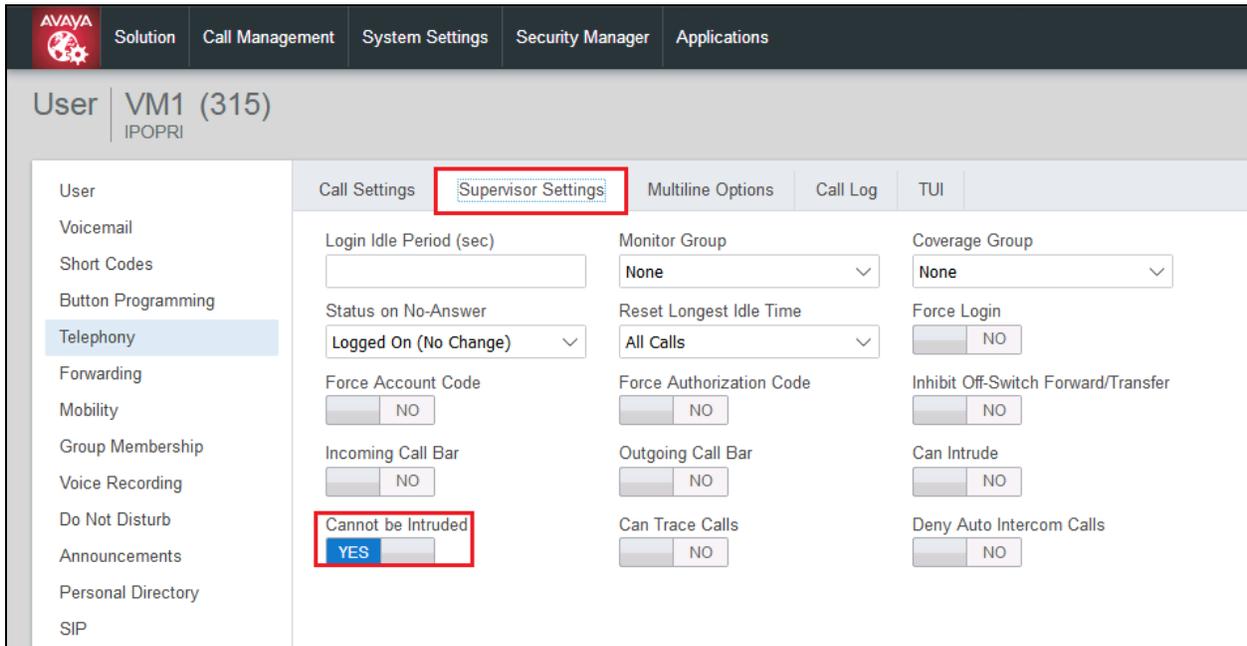
Select the **Voicemail** tab and set the **Voicemail On** to **NO** as shown below because the default Voicemail services available on IPO Server Edition will not be used.

The screenshot shows the Avaya user settings interface for user VM1 (315). The 'Voicemail' tab is selected in the left-hand menu. The 'Voicemail On' checkbox is highlighted with a red box and is currently set to 'NO'. Other settings visible include Voicemail Code (*****), Confirm Voicemail Code (*****), Voicemail Email (empty), Voicemail Email Mode (Off), Voicemail Ringback (NO), Voicemail Email Reading (NO), Voicemail Help (NO), and UMS Web Services (NO).

Select the **Telephony** → **Call Settings**. Set **Call Waiting** to **YES**, as shown below.

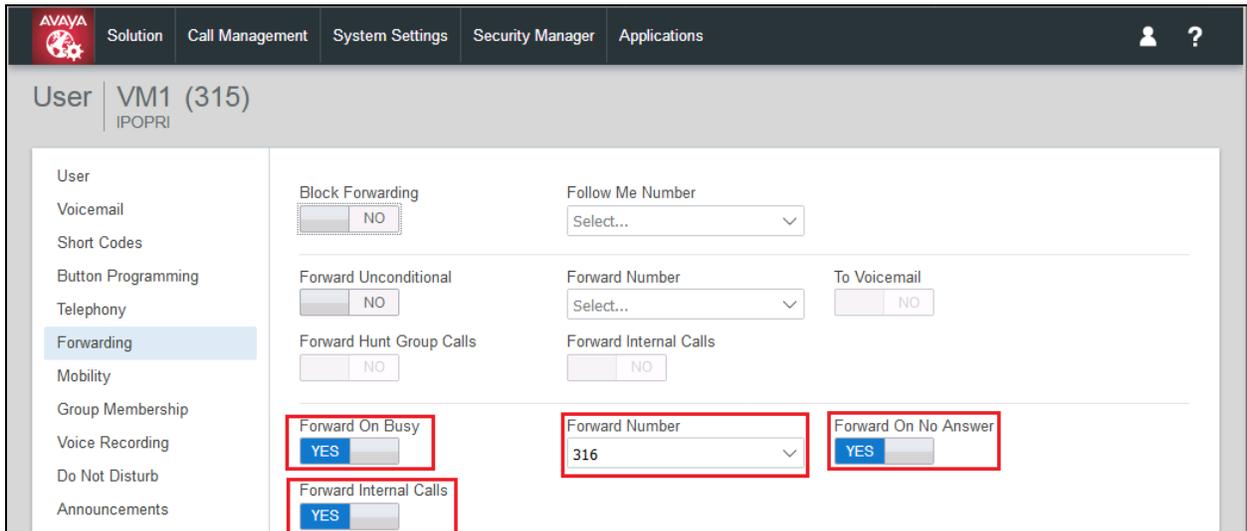
The screenshot shows the Avaya user settings interface for user VM1 (315). The 'Telephony' tab is selected in the left-hand menu, and the 'Call Settings' sub-tab is active. The 'Call Waiting' checkbox is highlighted with a red box and is currently set to 'YES'. Other settings visible include Outside Call Sequence (Default Ring), Inside Call Sequence (Default Ring), Ringback Sequence (Default Ring), No Answer Time (15), Transfer Return Time (Off), Wrap-up Time (2), Call Cost Mark-up (100), Advertise Callee State To Internal Callers (Same as System), Busy On Held (NO), Off Hook Station (NO), and Answer Call Waiting On Hold (YES).

Select **Telephony** → **Supervisor Settings**. Check the **Cannot be Intruded** field is set to **YES**, as shown below.



The screenshot shows the Avaya User Settings interface for user VM1 (315). The 'Supervisor Settings' tab is selected and highlighted with a red box. Within this tab, the 'Cannot be Intruded' checkbox is checked, with 'YES' displayed in a blue box and highlighted with a red box. Other settings include 'Login Idle Period (sec)', 'Monitor Group' (None), 'Coverage Group' (None), 'Status on No-Answer' (Logged On (No Change)), 'Reset Longest Idle Time' (All Calls), 'Force Login' (NO), 'Force Account Code' (NO), 'Force Authorization Code' (NO), 'Inhibit Off-Switch Forward/Transfer' (NO), 'Incoming Call Bar' (NO), 'Outgoing Call Bar' (NO), 'Can Intrude' (NO), and 'Can Trace Calls' (NO).

Select **Forwarding** and check **Forward on Busy**, **Forward On No Answer** and **Forward Internal Calls** are set to **YES** with the forwarding number as the next Voicemail Hunt group member, i.e. 316. The last primary SIP User will forward back to the first Voicemail Hunt Group member i.e. 315. Click **Create** to save (not shown).



The screenshot shows the Avaya User Settings interface for user VM1 (315) with the 'Forwarding' tab selected and highlighted with a blue box. Three settings are highlighted with red boxes: 'Forward On Busy' is checked (YES), 'Forward Internal Calls' is checked (YES), and 'Forward On No Answer' is checked (YES). The 'Forward Number' dropdown menu is set to 316. Other settings include 'Block Forwarding' (NO), 'Follow Me Number' (Select...), 'Forward Unconditional' (NO), 'Forward Number' (Select...), 'To Voicemail' (NO), and 'Forward Hunt Group Calls' (NO).

Repeat this section to add another two primary SIP Users associated with the last two primary SIP Extensions from **Section 5.4**.

5.5.2. Administer Secondary SIP Users

From the same screen in **Section 5.5.1**, enter the desired values for **Name** and **Full Name**. For **Extension**, enter the secondary SIP users Base Extension configured in **Section 5.4**, in this case starting from “311”.

The screenshot shows the Avaya User Management interface for a user named VMF1 (311). The left sidebar contains a list of configuration categories: User, Voicemail, Short Codes, Button Programming, Telephony, Forwarding, Mobility, Group Membership, Voice Recording, Do Not Disturb, and Announcements. The main content area displays the configuration form for the selected user. The following fields are highlighted with red boxes:

- Name:** VMF1
- Full Name:** MiniBar and Room Status
- Extension:** 311
- Account Status:** Enabled
- Profile:** Basic User
- Locale:** Select...
- Priority:** 5
- Login Code:** (masked with dots)
- Confirm Login Code:** (masked with dots)

Select the **Forwarding** on the left pane. Set **Forward Unconditional** to **YES** and set the **Forward Number** to the primary SIP Users hunt group, in this case “310” (created in the next **Section 5.6**), as shown below. Set also the **Forward Internal Calls** to **YES** and click **Create** (not shown).

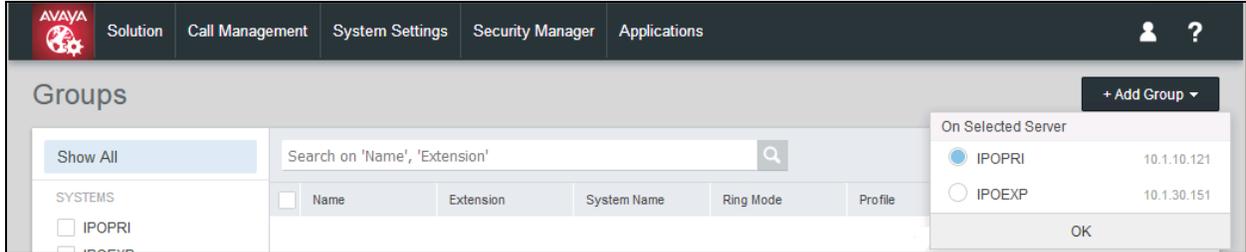
The screenshot shows the Avaya User Management interface for a user named VMF1 (311). The left sidebar contains a list of configuration categories: User, Voicemail, Short Codes, Button Programming, Telephony, Forwarding, Mobility, Group Membership, Voice Recording, Do Not Disturb, Announcements, and Personal Directory. The main content area displays the configuration form for the selected user. The following fields are highlighted with red boxes:

- Forward Unconditional:** YES
- Forward Number:** 310
- Forward Internal Calls:** YES

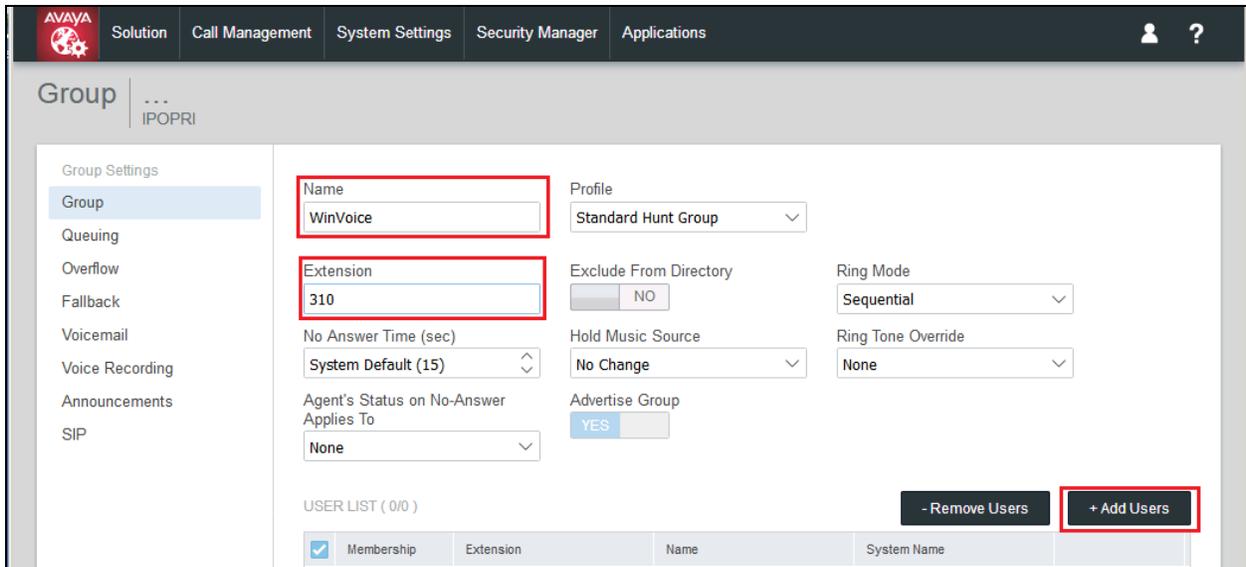
Repeat this section to add another two secondary SIP Users associated with the last two SIP Extensions from **Section 5.4**. In this compliance testing, SIP Users 311-313 were created.

5.6. Administer Hospitality Hunt Group

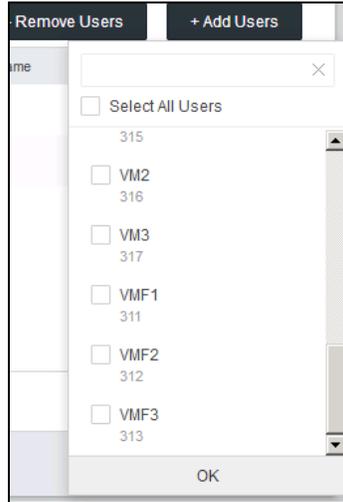
From the home screen, select **Call Management** → **Groups**. Click on **+Add Group** and check **IPOPRI** and click **OK** to add a new hunt group.



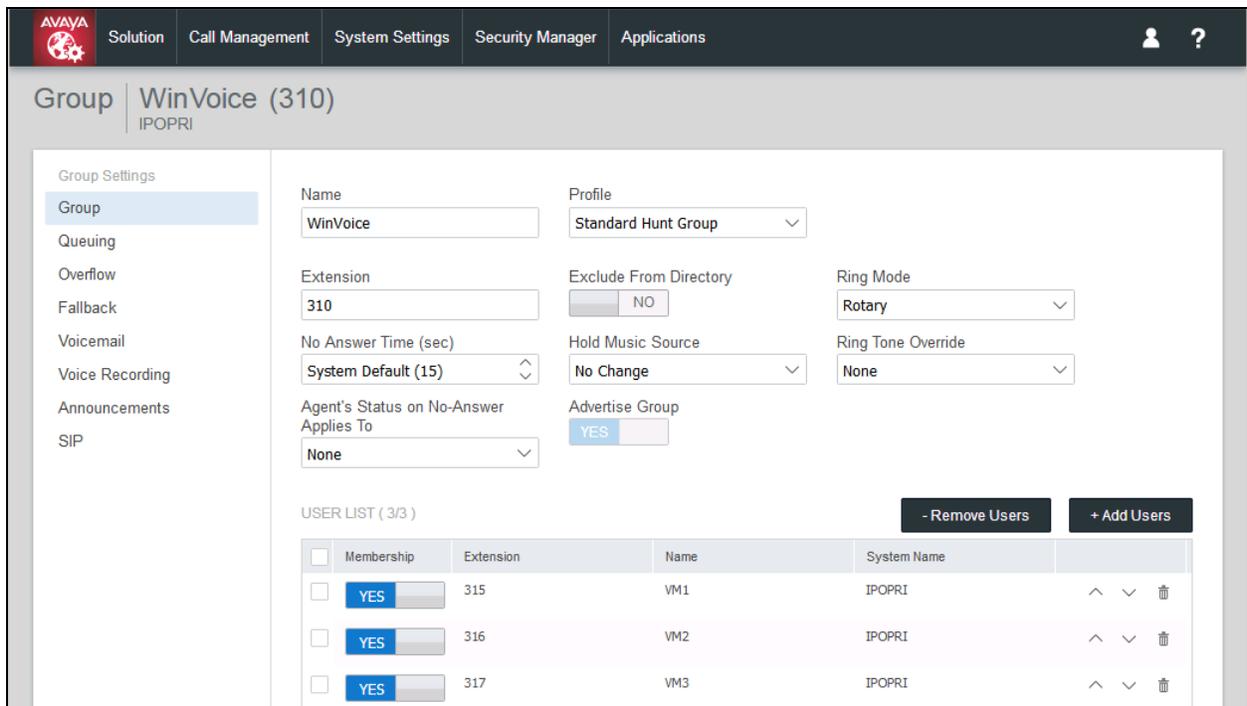
This hunt group will be used to deliver calls to Phoenix for the hospitality features and voicemail. Enter desired values for the **Name** and **Extension** fields and select **Ring Mode** as **Rotary** and retain the default values for the remaining fields. Rotary will allow the last selected member to be remembered and not necessary from the first member unlike sequential. Click on **+Add Users** in the USER LIST section below the page to add members.



The **Select Members** screen is displayed. Select the SIP primary users from **Section 0**.



Click **OK** and the **Group** screen is displayed again and updated with the selected member.



Select the **Voicemail** on the left pane and ensure **Voicemail On** is set to **NO**, as shown below.

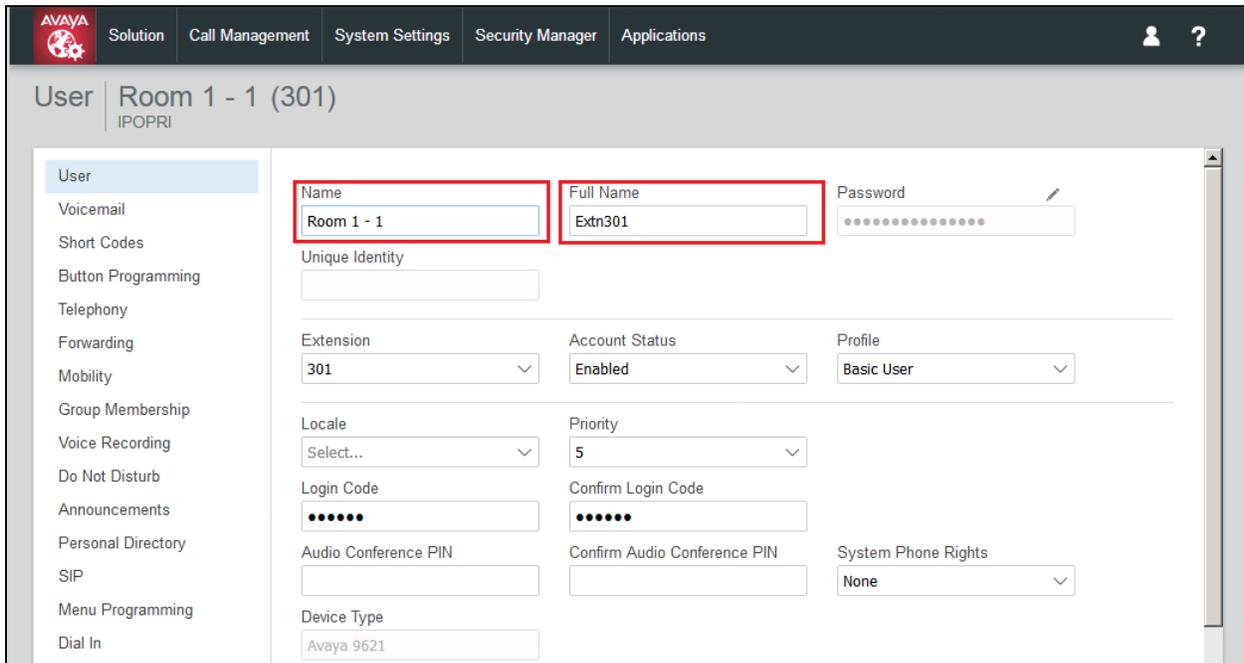
The screenshot shows the Avaya WinVoice (310) configuration interface. The left sidebar lists various settings, with 'Voicemail' selected. The main area displays the 'Voicemail On' toggle, which is highlighted with a red box and set to 'NO'. Other settings include 'Voicemail Answer Time (sec)' set to 45, 'Voicemail Code' and 'Confirm Voicemail Code' fields, 'Voicemail Email' field, 'Voicemail Email Mode' set to 'Off', 'Voicemail Help' set to 'NO', 'Broadcast' set to 'NO', and 'UMS Web Services' set to 'NO'.

Select the **Queuing** on the left pane and ensure that **Queuing** is set to **NO**, as shown below and click **Create** (not shown) below to save.

The screenshot shows the Avaya WinVoice (310) configuration interface. The left sidebar lists various settings, with 'Queuing' selected. The main area displays the 'Queuing On' toggle, which is highlighted with a red box and set to 'NO'. Other settings include 'Queue Type' set to 'Assign Call On Agent Answer', 'Queue Length' set to 'No Limit', 'Normalize Queue Length' set to 'YES', 'Calls In Queue Threshold' set to 1, and 'Analog Extension to Notify' set to 'None'.

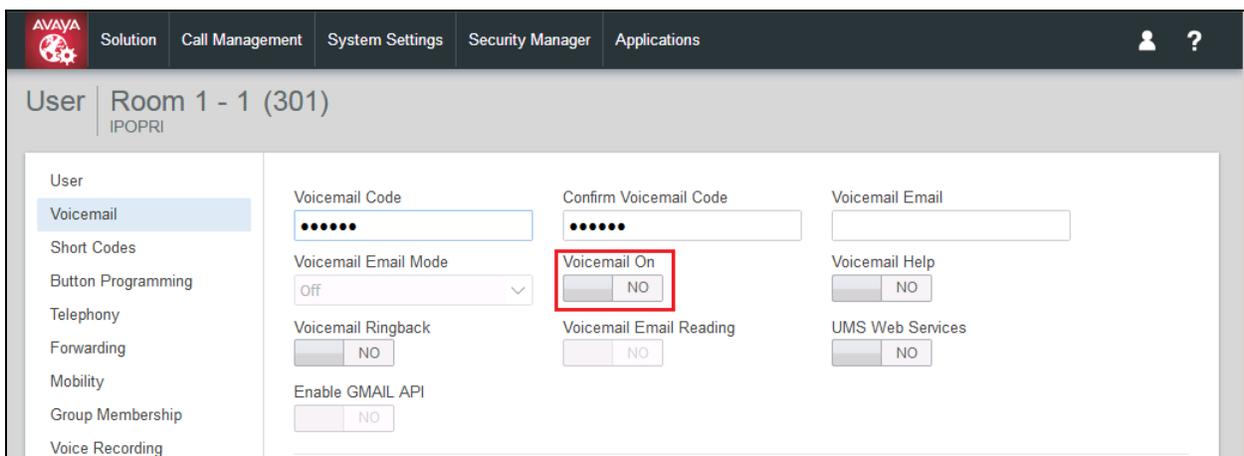
5.7. Administer Voicemail Users

From the home menu, select **Call Management** → **Users**, select the first user that will be using WinExpress for voicemail – these can be Guests and/or Admin staff. In this case, the user “301” is shown. Enter a descriptive **Name**. The **Full Name** can be completed as a template for identification or leave it as blank as Unicorn will update the guest name through IP Office Configuration Web Services regardless.



The screenshot shows the Avaya user configuration interface for 'Room 1 - 1 (301)'. The 'Name' field is set to 'Room 1 - 1' and the 'Full Name' field is set to 'Extn301'. Both fields are highlighted with red boxes. The 'Password' field is masked with dots. Other fields include 'Unique Identity', 'Extension' (301), 'Account Status' (Enabled), 'Profile' (Basic User), 'Locale' (Select...), 'Priority' (5), 'Login Code' (*****), 'Confirm Login Code' (*****), 'Audio Conference PIN', 'Confirm Audio Conference PIN', 'System Phone Rights' (None), and 'Device Type' (Avaya 9621).

Select the **Voicemail** on the left pane. Check that the **Voicemail On** is set to **NO**, as shown below because the default system Voicemail will not be used.



The screenshot shows the Avaya user configuration interface for 'Room 1 - 1 (301)' with the 'Voicemail' settings pane selected. The 'Voicemail On' checkbox is checked and highlighted with a red box. Other settings include 'Voicemail Code' (*****), 'Confirm Voicemail Code' (*****), 'Voicemail Email', 'Voicemail Email Mode' (Off), 'Voicemail Ringback' (NO), 'Voicemail Email Reading' (NO), 'UMS Web Services' (NO), and 'Enable GMAIL API' (NO).

Select the **Forwarding** on the left pane. Set the **Forward On Busy**, **Forward On No Answer** and **Forward Internal Calls** with the **Forward Number** as the first Voicemail Hunt group member in **Section 5.6**, as shown below and click **Update** below (not shown).

The screenshot shows the Avaya user configuration interface for 'User Room 1 - 1 (301) IPOPRI'. The left sidebar has 'Forwarding' selected. The main configuration area includes the following settings:

- Block Forwarding:** NO
- Follow Me Number:** Select...
- Forward Unconditional:** NO
- Forward Number:** Select...
- To Voicemail:** NO
- Forward Hunt Group Calls:** NO
- Forward Internal Calls:** NO
- Forward On Busy:** YES (highlighted with a red box)
- Forward Number:** 315 (highlighted with a red box)
- Forward On No Answer:** YES (highlighted with a red box)
- Forward Internal Calls (bottom):** YES (highlighted with a red box)

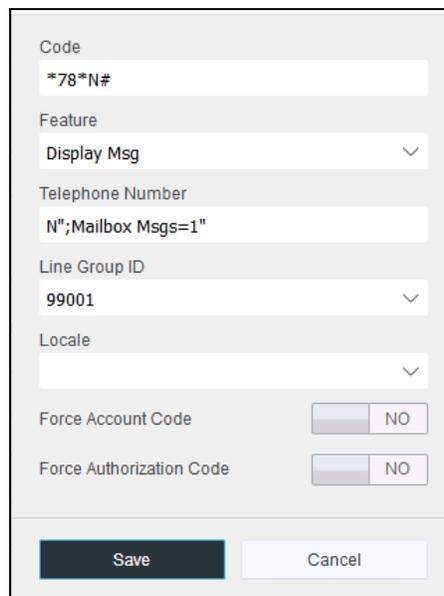
Repeat this section for all users using Phoenix for voicemail, including all guest rooms, front desk, and administrative staff. In the compliance testing, the voicemail users consisted of one front desk with extension “304”, admin phone with extension “698” and guest rooms with extensions “301, 302, 601, 631, 602 and 632”, as shown in **Figure 1**.

5.8. Administer Short Codes for MWI ON/OFF

From the home screen, select **System Settings** → **Short Code**. Click **+Add Short Code**, select **As Common Object** (for both Primary and Expansion Server) and click **OK**. Enter the parameters as below for turning message waiting lamp **ON** and leave the rest as default.

- **Code** *78*N# where 78 is a free number randomly assigned and N represents user station
- **Feature** Select **Display Msg** from drop down menu
- **Telephone Number** Enter the format **N";Mailbox Msgs=1"**

Leave the rest as default and click **Save**.



The screenshot shows a configuration form for a short code. The fields are as follows:

Code	*78*N#
Feature	Display Msg
Telephone Number	N";Mailbox Msgs=1"
Line Group ID	99001
Locale	
Force Account Code	<input type="checkbox"/> NO
Force Authorization Code	<input type="checkbox"/> NO
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Similarly, create a new **Short Code** and enter the parameters as below for turning message waiting lamp **OFF** and leave the rest as default.

- **Code** *79*N# where 79 is a free number randomly assigned and N represents user station
- **Feature** Select **Display Msg** from drop down menu
- **Telephone Number** Enter the format N";Mailbox Msgs=0"

Leave the rest as default and click **Save**.

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

- Code:** *79*N#
- Feature:** Display Msg
- Telephone Number:** N";Mailbox Msgs=0"
- Line Group ID:** 99001
- Locale:** (empty)
- Force Account Code:** NO
- Force Authorization Code:** NO

Buttons: Save, Cancel

5.9. Administer Analog User MWI

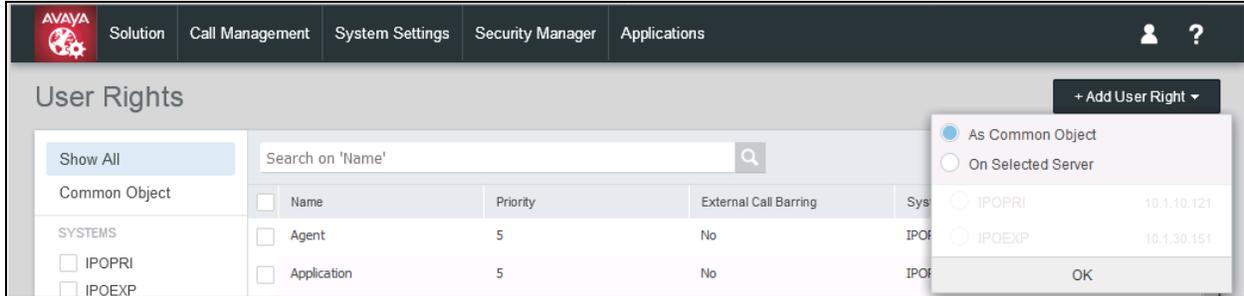
For voicemail users with analog telephones, the MWI setting on the analog extension may need modification depending on the type of analog telephone. Please refer to **Section 9** of these Application Notes for information on the specific analog telephone types requiring the MWI setting.

From the home menu, select **Call Management** → **Extensions**. Select the extension corresponding to the analog user. In this case, the extension is “631”. Click on **ANALOGUE** in the left pane, select from the drop-down list under **Message Waiting Lamp Indication Type** to, “51V Stepped” as shown below. Click **Update** below (not shown).

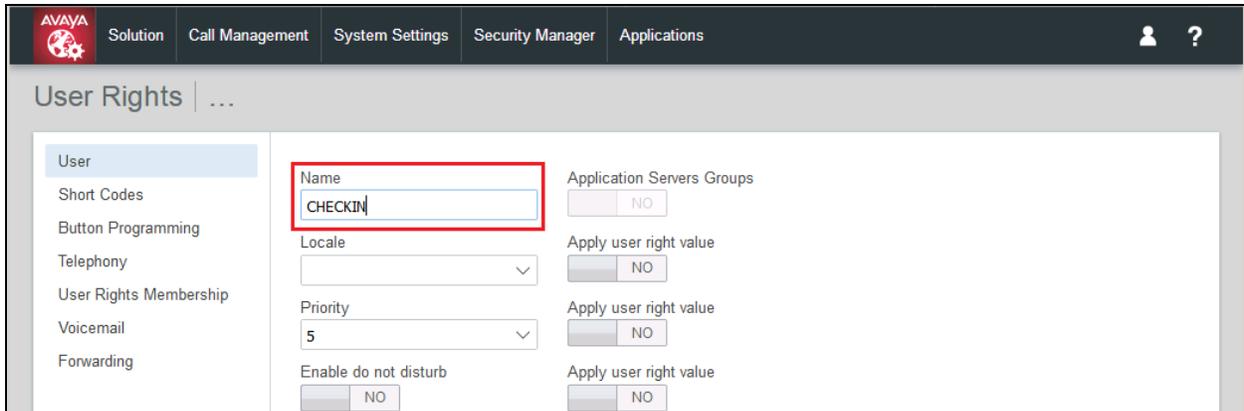
The screenshot displays the Avaya Call Management interface for configuring an analogue extension. The breadcrumb trail is Solution > Call Management > System Settings > Security Manager > Applications. The page title is 'Extension Analogue Extension 631 (49) IPOEXP'. On the left, under 'SETTING GROUPS', the 'ANALOGUE' group is selected. The main configuration area is divided into 'ANALOGUE' settings and 'Flash Hook Pulse Width' settings. The 'Message Waiting Lamp Indication Type' dropdown is highlighted with a red box and set to '51V Stepped'. Other settings include 'Equipment Classification' (Standard Telephone), 'Hook Persistency (ms)' (100), and 'Flash Hook Pulse Width' (Use System Defaults, YES, Minimum Width 20ms, Maximum Width 500ms).

5.10. Administer User Rights

From the home menu, select **System Settings** → **User Rights**. Click **+Add User Right**, check **As Common Object** (for both Primary and Expansion Server) and click **OK**.



Enter a desired **Name** to designate user rights for guests in the Check-In state. In the compliance testing, the name was set to **CHECKIN** as shown below. Note that there are differences in name if lower or upper case letters are used and these should be communicated to FCS service engineer.



Select the **Telephony** on the left pane and then the **Supervisor Settings** tab on the right pane. Set **Enable outgoing call bar** to **NO** and set **Apply user right value** to **YES**, as shown below. Click **Create** to save (not shown).

The screenshot shows the Avaya User Rights configuration interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security Manager', and 'Applications'. The main content area is titled 'User Rights | ...' and has a left sidebar with options: 'User', 'Short Codes', 'Button Programming', 'Telephony' (highlighted), 'User Rights Membership', 'Voicemail', and 'Forwarding'. The 'Supervisor Settings' tab is active, displaying a list of settings. The 'Enable outgoing call bar' setting is highlighted with a red box, showing a 'NO' radio button selected. The 'Apply user right value' setting for this option is also highlighted with a red box, showing a 'YES' radio button selected. Other settings include 'Can Intrude', 'Can not be intruded', 'Deny Auto Intercom Calls', 'Enable force login', 'Enable force account code', 'Inhibit Off-Switch Forward/Transfer', and 'Coverage Group'.

Setting	Value	Apply user right value
Can Intrude	NO	NO
Can not be intruded	NO	NO
Deny Auto Intercom Calls	NO	NO
Enable force login	NO	NO
Enable force account code	NO	NO
Inhibit Off-Switch Forward/Transfer	NO	NO
Enable outgoing call bar	NO	YES
Coverage Group	None	NO

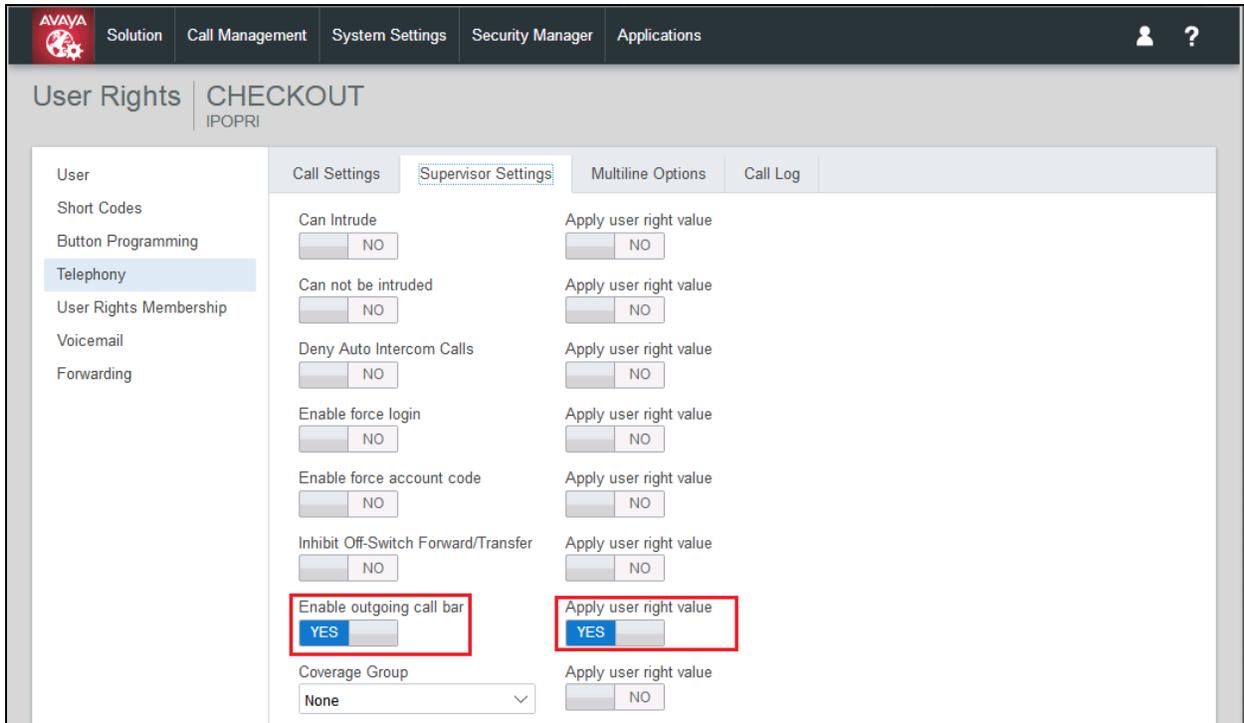
In this compliance testing, the same 2 sets of user rights templates were created with names as highlighted in the red box below for Primary and Expansion Server.

The screenshot shows the 'User Rights' configuration page in the Avaya system. The search filter is set to 'CHECK'. The interface is divided into a left sidebar for 'Common Object' and a main table area. The 'Common Object' sidebar shows 'IPOPRI' and 'IPOEXP' selected. The main table lists 20 user rights templates, grouped by system name. Two groups of 10 templates each are highlighted with red boxes: one for 'IPOPRI' and one for 'IPOEXP'. Each template has a priority of 5 and various external call barring settings.

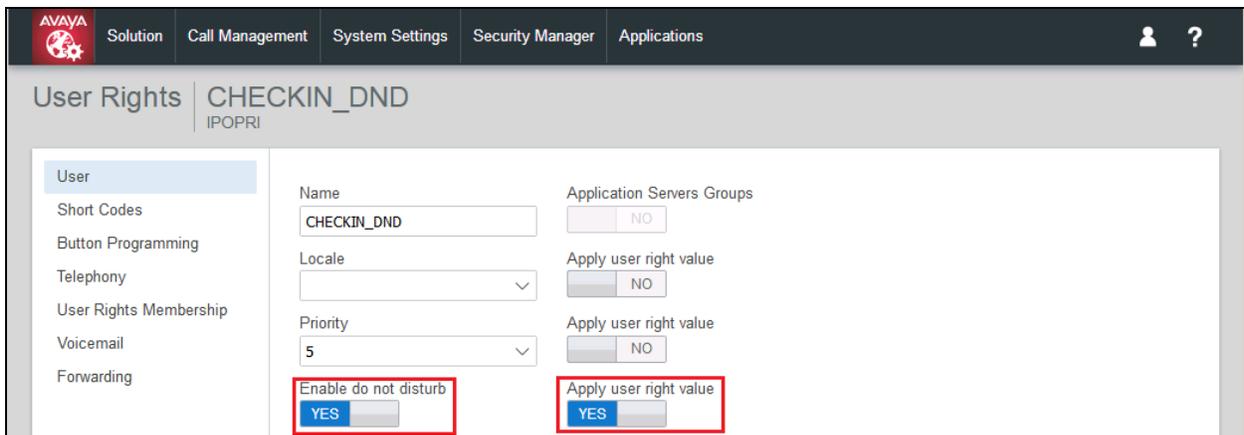
Name	Priority	External Call Barring	System Name
<input type="checkbox"/> CHECKIN	5	No	IPOPRI
<input type="checkbox"/> CHECKIN_BAR	5	Yes	IPOPRI
<input type="checkbox"/> CHECKIN_BAR_DND	5	Yes	IPOPRI
<input type="checkbox"/> CHECKIN_DND	5	No	IPOPRI
<input type="checkbox"/> CHECKIN_DOM	5	No	IPOPRI
<input type="checkbox"/> CHECKIN_DOM_DND	5	No	IPOPRI
<input type="checkbox"/> CHECKIN_LOC	5	No	IPOPRI
<input type="checkbox"/> CHECKIN_LOC_DND	5	No	IPOPRI
<input type="checkbox"/> CHECKOUT	5	Yes	IPOPRI
<input type="checkbox"/> CHECKIN	5	No	IPOEXP
<input type="checkbox"/> CHECKIN_BAR	5	Yes	IPOEXP
<input type="checkbox"/> CHECKIN_BAR_DND	5	Yes	IPOEXP
<input type="checkbox"/> CHECKIN_DND	5	No	IPOEXP
<input type="checkbox"/> CHECKIN_DOM	5	No	IPOEXP
<input type="checkbox"/> CHECKIN_DOM_DND	5	No	IPOEXP
<input type="checkbox"/> CHECKIN_LOC	5	No	IPOEXP
<input type="checkbox"/> CHECKIN_LOC_DND	5	No	IPOEXP
<input type="checkbox"/> CHECKOUT	5	Yes	IPOEXP

Displaying 1 - 18 of 18

During this compliance testing, the **Enable outgoing call bar** field was checked for the user rights **CHECKOUT** to prevent the guest room users from making calls out to the PSTN when either of these user rights is applied.



User rights **CHECKIN_DND** was set with **Enable do not disturb** and **Apply user right value** set to **YES**. With this user right applied, Guest user will not be disturbed upon Check-In to hotel room.



User rights **CHECKIN_LOC** means that guest will only be able to make local calls. User rights **CHECKIN_DOM** means that guest user will be able to call up to domestic (long distance) but not international. Short Codes will be used in this case to restrict domestic or international calls by the digits dialed. These will be applied to both Primary and Secondary Servers.

Avaya Solution Call Management System Settings Security Manager Applications

User Rights | CHECKIN_LOC
IPOPRI

User

Short Codes YES

Button Programming

Telephony

User Rights Membership

VoiceMail

Forwarding

+ Add

Code	Telephone Number	Feature	Line Group ID	Force Account C...	Force Authorizati...		
902	902N=902N	Barred	2	No	No	/	🗑️
9001	9001N=9001N	Barred	2	No	No	/	🗑️

Avaya Solution Call Management System Settings Security Manager Applications

User Rights | CHECKIN_DOM
IPOPRI

User

Short Codes NO

Button Programming

Telephony

User Rights Membership

VoiceMail

Forwarding

+ Add

Code	Telephone Number	Feature	Line Group ID	Force Account C...	Force Authorizati...		
9001	9001N=9001N	Barred	2	No	No	/	🗑️

The rest of the user rights will be a combination of the above.

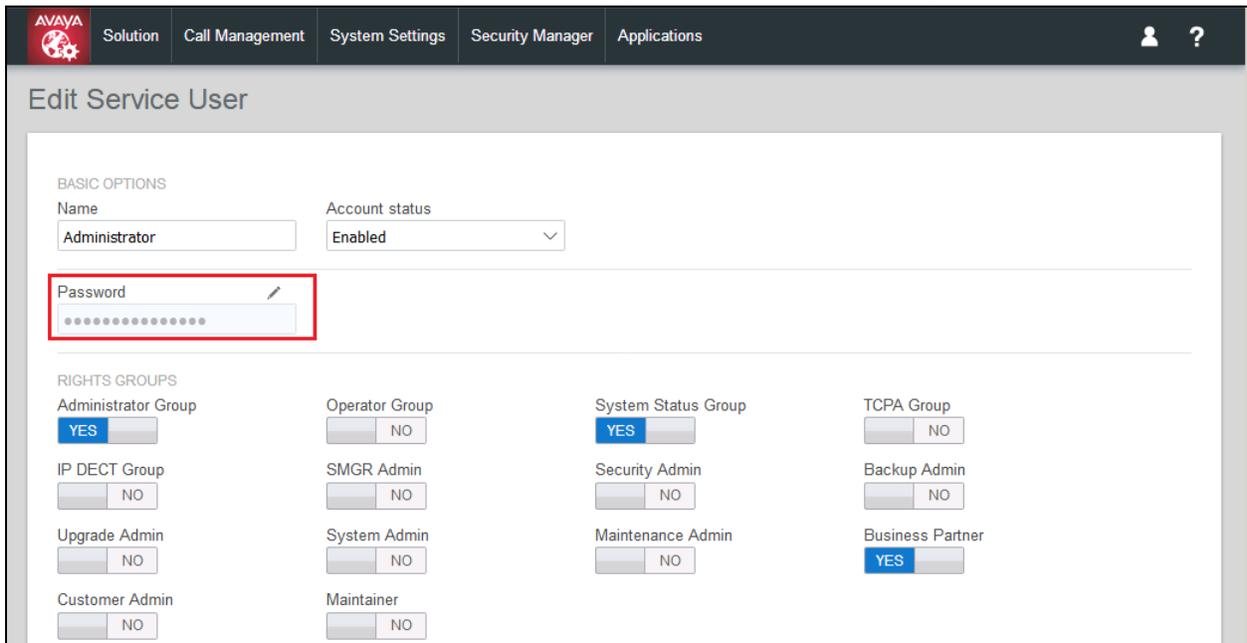
5.11. Administer System Password

From the home menu, select **Security Manager** → **Service Users**. Click on the pencil icon to edit the **Administrator**.



Name	Access Rights		
Administrator	Administrator Group, System Status Group, Business Partner	User Preferences	 
EnhTcpaService	TCPA Group, TCPA Group	User Preferences	 
IPDECTService	IPDECT Group, IPDECT Group	User Preferences	 
BranchAdmin	SMGR Admin	User Preferences	 
BusinessPartner	Business Partner	User Preferences	 
Maintainer	Maintainer	User Preferences	 

On the **Edit Service User** screen below, click the pen beside the **Password** and set the new password. Click **Update** to save (not shown). The password is used in **Section 6.2** for Configuration Web Services.



Basic Options

Name: Account status:

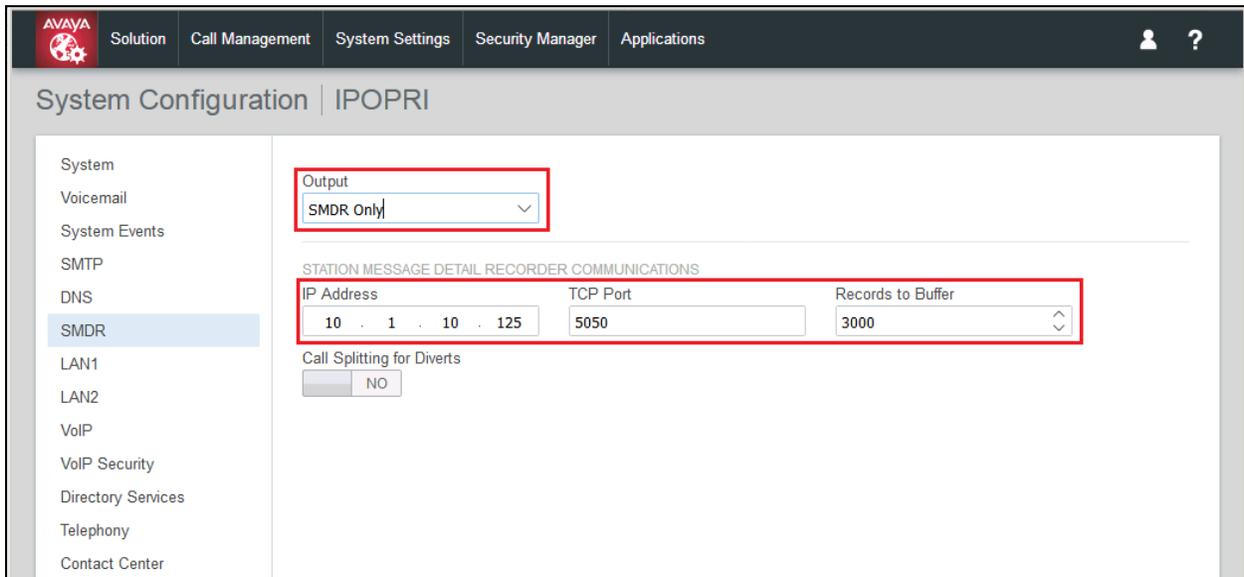
Password: 

Rights Groups

Administrator Group: <input checked="" type="checkbox"/>	Operator Group: <input type="checkbox"/>	System Status Group: <input checked="" type="checkbox"/>	TCPA Group: <input type="checkbox"/>
IP DECT Group: <input type="checkbox"/>	SMGR Admin: <input type="checkbox"/>	Security Admin: <input type="checkbox"/>	Backup Admin: <input type="checkbox"/>
Upgrade Admin: <input type="checkbox"/>	System Admin: <input type="checkbox"/>	Maintenance Admin: <input type="checkbox"/>	Business Partner: <input checked="" type="checkbox"/>
Customer Admin: <input type="checkbox"/>	Maintainer: <input type="checkbox"/>		

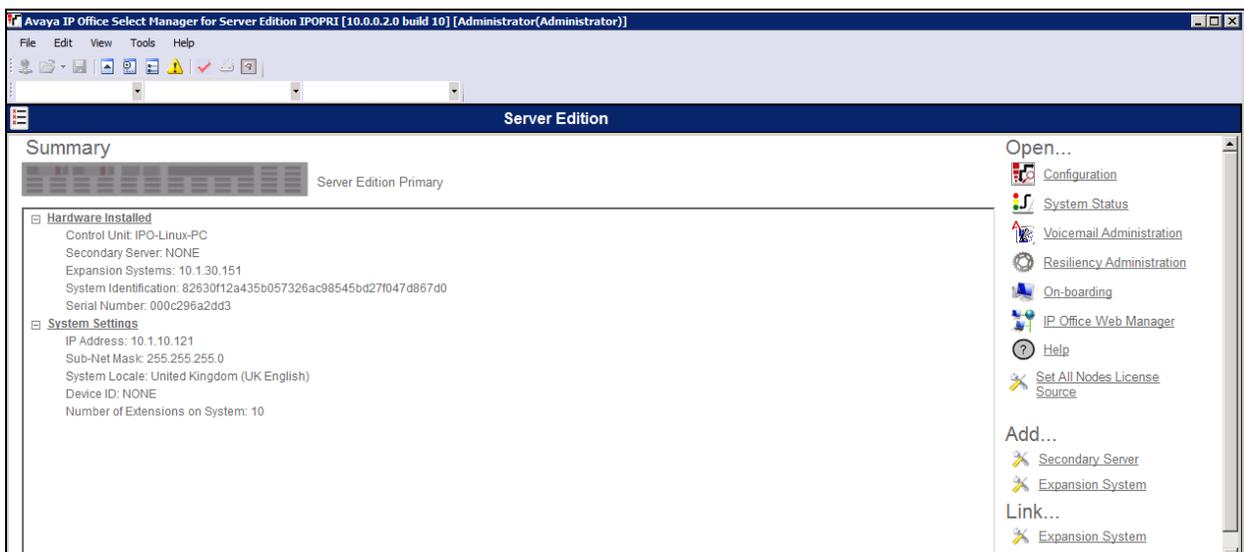
5.12. Administer SMDR

From the home menu, select **System Settings** → **System** → **IPOPRI** → **SMDR**. For the Output field, select “**SMDR Only**” from the drop-down box. Set **IP Address** to the WinExpress server IP address, and set the **TCP Port** to **5050**. Optionally, you can increase the **Records to Buffer** field from default **500** to **3000** to provide more buffer for call records in case the SMDR link is broken. Click **Update** to save (not shown).

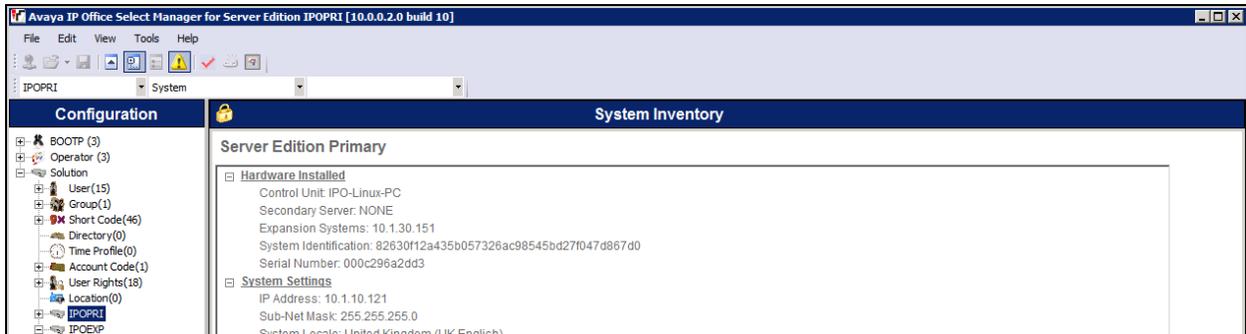


5.13. Administer Security Settings

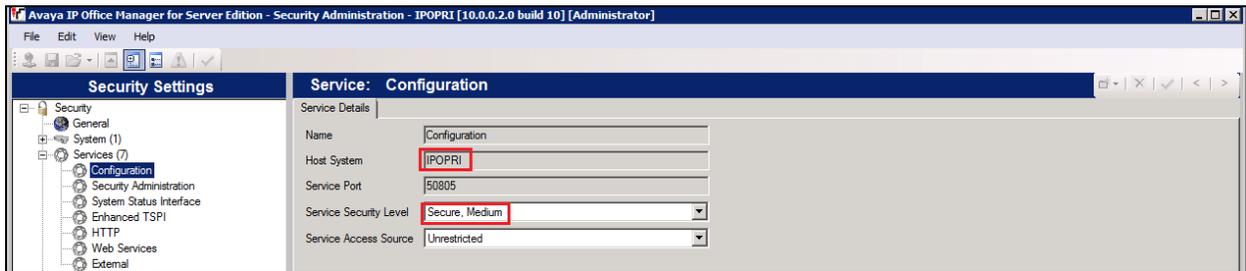
From the home screen, select **Applications** → **IP Office Manager**. Click on **Configuration** on the right pane.



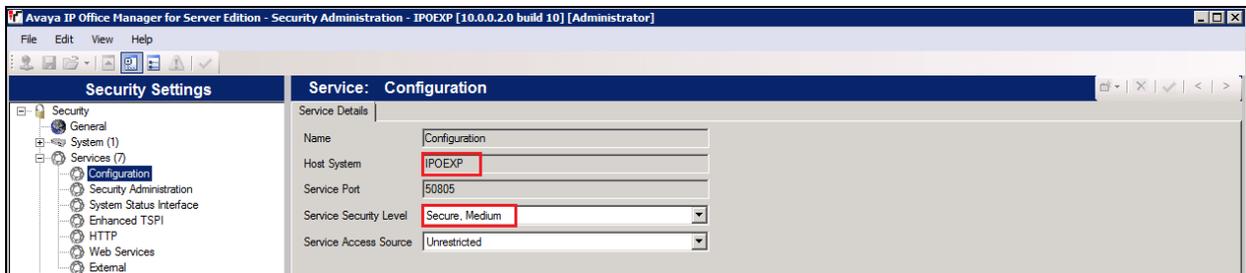
The **Configuration** screen is shown. Click on **Solution** → **IPOPRI** and then select **File** → **Advanced** → **Security Settings** (not shown) from the top menu.



The **Avaya IP Office Manager for Server Edition - Security Administration – IPOPRI** screen is displayed. From the configuration tree in the left pane, select **Security** → **Services** → **Configuration** to display the **Service: Configuration** screen in the right pane. For **Service Security Level**, select “**Secure, Medium**” as shown below. In this compliance testing, Unicorn used the “Secure” level for the Configuration Web Service interface. **Select File** → **Save Security Settings** and enter the appropriate **Service User Name/Password** (not shown) to complete.



Repeat the whole process for the security settings of the expansion module **IPOEXP** as shown in the screen above.



6. Configure WinExpress

This section provides the procedures for configuring WinExpress. WinExpress comprises of two main components, i.e., Phoenix voicemail and Unicorn call billing package and interface solution. The procedures include the following:

- Obtaining IP Office Configuration Web Service SDK
- Configuring Unicorn
- Configuring Phoenix

6.1. Obtaining Avaya IP Office Configuration Web Service SDK

Avaya provides the IP Office Configuration Web Service SDK for DevConnect members to incorporate IP Office configuration changes in their solutions. The latest Configuration Web Service SDK can be obtained from the DevConnect Program Portal at <http://www.devconnectprogram.com/> using a web browser and log in using a valid DevConnect member account. Then click **Downloads** → **IP Office™**. Select from the **Choose Interface** → **Configuration Web Services**. Locate and download the latest Configuration Web Service SDK. Member implementation engineer will then deploy the files from the Configuration Web Service SDK onto the WinExpress server.

6.2. Configuring Unicorn

Unicorn is a Windows-based integrated billing and interface solution. This section details the essential portion of the Unicorn configuration to interoperate with IP Office. These Application Notes assume that the Unicorn application has already been properly installed by FCS service Engineer.

1. To enable Unicorn Interface configuration for **Phoenix.VMS**, **AvayaIPOPMS**, **AvayaIPOPMS2** and **AvayaIPO.CDR**, use **Unicorn.xml** located in the "C:\Program Files(x86)\FCS\Unicorn\Control\" directory.

In the <Child> section of the xml file, the configuration highlighted in bold below indicates what needs to be added.

```
<Child Id="VMS1">
  <PropertyId>MY99</PropertyId>
  <EXENAME>Phoenix.VMS.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidel
  <LogFilePattern>VMS\VMS1-</LogFilePattern>
  <Description>Phoenix.VMS</Description>
  <XMLFile>Phoenix-VMS.xml</XMLFile>
  <IntfInQueueName>.\Private$\VMS1In</IntfInQueueName>
  <!--can be a remote MSMQ queue-->
  <IntfOutQueueName>.\Private$\VMS1Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <!-- interface will filter the packet if it's more than this value (in hour) as
  <!--during startup, the child has to initial a dialog with mother via tcp/ip bef
  <UnicornMotherIPPort>4017</UnicornMotherIPPort>
  <MemoryPage>7</MemoryPage>
</Child>

<Child Id="PBX1">
  <PropertyId>MY99</PropertyId>
  <EXENAME>AvayaIPOPMSSE.PBX.exe</EXENAME>
  <LogFilePattern>PBX\PBX1-</LogFilePattern>
  <Description>AvayaIPOPMS</Description>
  <XMLFile>AvayaIPOPMS-PBX.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX1In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX1Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>4018</UnicornMotherIPPort>
  <MemoryPage>10</MemoryPage>
</Child>

<Child Id="PBX2">
  <PropertyId>MY99</PropertyId>
  <EXENAME>AvayaIPOPMSSE2.PBX.exe</EXENAME>
  <LogFilePattern>PBX\PBX2-</LogFilePattern>
  <Description>AvayaIPOPMS2</Description>
  <XMLFile>AvayaIPOPMS-PBX2.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX2In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX2Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>4019</UnicornMotherIPPort>
  <MemoryPage>11</MemoryPage>
</Child>
```

```

<Child Id="CDR1">
  <PropertyId>MY99</PropertyId>
  <LogFilePattern>CDR\CDR1-</LogFilePattern>
  <EXENAME>AvayaIPO.CDR.exe</EXENAME>
  <Description>AvayaIPO CDR Interface </Description>
  <XMLFile>AvayaIPO-CDR.xml</XMLFile>
  <IntfInQueueName>.\Private$\SMDRIn</IntfInQueueName>
  <IntfOutQueueName>.\Private$\SMDROut</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>4001</UnicornMotherIPPort>
  <MemoryPage>9</MemoryPage>
</Child>

```

2. Unicorn provides a web interface for configuration of guest rooms, posting like DND and MWI on/off updates and operations reporting. An administrator can log in with the appropriate credentials from <http://<server name or ip address>/Unicorn.Web/Login.aspx> as shown below by substituting the appropriate server IP address. Select the **Property** and log in with the appropriate credentials.

Unicorn

Property: MY99-Castel Primus

Language: English

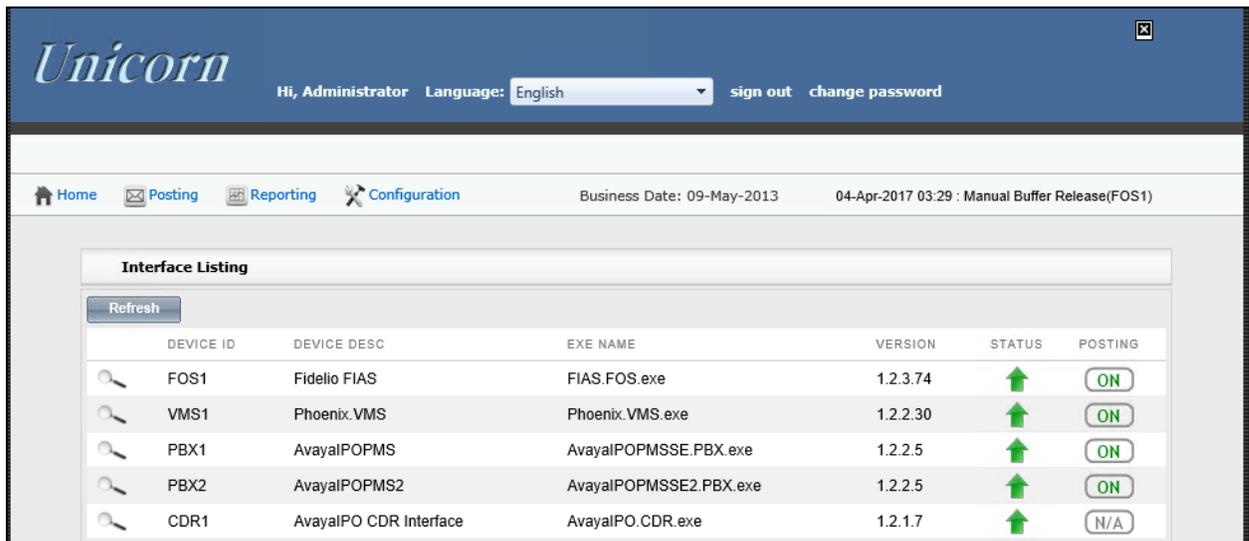
User ID: admin

Password: ●●●

Login [Change Password](#)

© 2012 FCS Computer Systems | www.fcscs.com

3. Click **Home** → **System** → **Interface Listing** to show the integrated interfaces and their status which should show up as . The list below shows the **Device ID** list and their purpose.
 - a. **FOS1** – Front Office System
 - b. **VMS1**- Phoenix Voicemail
 - c. **PBX1** – IP Office Primary Server PMS
 - d. **PBX2** – IP Office Expansion Module PMS
 - e. **CDR1** – IP Office SMDR



The screenshot shows the Unicorn web application interface. At the top, there is a navigation bar with the Unicorn logo, user information 'Hi, Administrator', language selection 'English', and links for 'sign out' and 'change password'. Below this is a secondary navigation bar with icons for 'Home', 'Posting', 'Reporting', and 'Configuration', along with 'Business Date: 09-May-2013' and '04-Apr-2017 03:29 : Manual Buffer Release(FOS1)'. The main content area is titled 'Interface Listing' and contains a table with the following data:

DEVICE ID	DEVICE DESC	EXE NAME	VERSION	STATUS	POSTING
FOS1	Fidello FIAS	FIAS.FOS.exe	1.2.3.74		ON
VMS1	Phoenix.VMS	Phoenix.VMS.exe	1.2.2.30		ON
PBX1	AvayaPOPMS	AvayaPOPMSSE.PBX.exe	1.2.2.5		ON
PBX2	AvayaPOPMS2	AvayaPOPMSSE2.PBX.exe	1.2.2.5		ON
CDR1	AvayaPO CDR Interface	AvayaPO.CDR.exe	1.2.1.7		N/A

- The Unicorn Avaya PMS interface module port and data configuration is defined in the **AvayaIPOPMS-PBX.xml** and **AvayaIPOPMS-PBX2.xml** located in the “C:\Program Files(x86)\FCS\Unicorn\Control\” directory. **Webservice** is configured for interfacing with Configuration Web Services of IP Office Servers.

```

      8 = Webservice
      (<InterfaceSetting>URL string</InterfaceSetting>)
-->
<!--
Examples:
<InterfaceType>1</InterfaceType>
<InterfaceSetting>1,9600,n,8,1</InterfaceSetting>
<InterfaceType>2</InterfaceType>
<InterfaceSetting>C,127.0.0.1:9600</InterfaceSetting>
<InterfaceType>2</InterfaceType>
<InterfaceSetting>C,10.8.2.127:5006</InterfaceSetting>
<InterfaceType>2</InterfaceType>
<InterfaceSetting>C,127.0.0.1:9600</InterfaceSetting>

<InterfaceType>2</InterfaceType>
<InterfaceSetting>C,127.0.0.1:9600</InterfaceSetting> -->
<!-- <InterfaceSetting>1,9600,n,8,1</InterfaceSetting> if you change to TCP/IP please restart interface -->
<InterfaceType>8</InterfaceType>
<!--<InterfaceSetting>http://10.10.10.1</InterfaceSetting>-->
<!--InterfaceSetting>http://10.161.190.178:8085/IPOConfigurationService</InterfaceSetting-->
<InterfaceSetting>http://127.0.0.1:8085/IPOConfigurationService</InterfaceSetting>

```

In both configuration xml files, the host is set as the **IPAddress** of IP Office server (or Expansion Module) listening to port **50805** which corresponds with the IP Office port at **Section 5.13** and the **AccountName** and **Password** administered in **Section 5.11**. The password is not revealed for security reasons.

```

-->
<InterPacketDelay>1000</InterPacketDelay>
<!--
Specify delay to allow for sufficient time to collected fragmented data
-->
<CheckRTSSignal>No</CheckRTSSignal>
<!--needed for RS232 Setting only-->
<CheckDTRSignal>No</CheckDTRSignal>
<!--needed for RS232 Setting only-->
<CheckCTSSignal>No</CheckCTSSignal>
<!--needed for RS232 Setting only-->
<SendCheckSum>Yes</SendCheckSum>
<MultiPosting>1</MultiPosting>
<InterStringDelay>5000</InterStringDelay>
<!--in second-->
<SendRetry>3</SendRetry>
<AccountName>Administrator</AccountName>
<PassWord>      </PassWord>
<IPAddress>10.1.10.121</IPAddress>
<PortNumber>50805</PortNumber>
<SendDelay>2000</SendDelay>
</CommunicationSetting>

```

5. The Unicorn Avaya CDR interface module port & data configuration is defined in the **AvayaIPO-CDR.xml** located in the "C:\Program Files (x86)\FCS\Unicorn\Control\" directory. The host is set as **tcp.ip** type listening to port **5050**. This corresponds with the setup of IP Office SMDR port at **Section 5.12**.

```
<PBX ID="CDR1">
  <!-- need to match with the XML filename -->
  <CommunicationSetting>
    <Name>Avaya IPO</Name>

    <ProtocolFormat>2</ProtocolFormat>
    <!--1 =[STX]xxxxx[ETX], 2=xxxxxxx[13][10] 3=[13][10]xxxxxxx, 4=Fixed Length-->
    <InterfaceType>2</InterfaceType>
    <!--1 = RS232, 2=tcp.ip 3=udp, 4=telnet,5=bisync 6=file sharing-->
    <InterfaceSetting>H,10.1.10.125:5050</InterfaceSetting>
    <!-- if tcp.ip, interfaceSetting could be "X,192.168.1.12:5600" , where X = H = host, C=client-->
    <!-- 3,9600,n,8,1 - com. port 3, baud rate 9600,n,8,1 -->
    <UDPSvrInterfaceSetting></UDPSvrInterfaceSetting>
    <InterPacketDelay>100</InterPacketDelay>
  </CommunicationSetting>
</PBX ID="CDR1">
```

6. The **Posting** tab below shows the various features such as Check In/Out and Edit Guest Profile that can be performed from the web interface. The screenshot below shows the **Check In/Out** page for checking a guest with name, date, room number and check in/out date etc.

The screenshot displays the Unicorn web interface for the 'Check In/Out' function. The header shows the user is logged in as 'Administrator' in 'English' with options to 'sign out' or 'change password'. The navigation bar includes 'Home', 'Posting', 'Reporting', and 'Configuration'. The 'Posting' menu is expanded, showing options for 'Guest', 'Room', 'Charges', 'Check In/Out', 'Edit Profile', 'Room Change', 'Check In', and 'Check Out'. The main form area contains the following fields:

- Extn. No. : (Mandatory) Extn. No. e.g: 2000 or 1000,2000,3000
- Room No. : (Mandatory) Room No. Share Room
- Guest Name : (Mandatory) Guest Name Title
- First Name : (Mandatory) First Name Last Name : (Mandatory) Last Name
- Check In : 04 Apr 2017, Tuesday 00 : 00
- Check Out : 05 Apr 2017, Wednesday 12 : 00
- Folio No. : Folio No. Group No. : Group No.
- VIP No. : VIP No. Password : Password
- Language : EN-English
- COS : UA-Unbar all (IDD/Intl and STD/Domestic and local call)

- Click **Configuration** → **Extensions** and select **Primary Extension Numbering** or **Slave Extension** to view the extensions configured with each room.

The screenshot shows the Unicorn system interface. At the top, the user is logged in as 'Hi, Administrator' with the language set to 'English'. The main navigation bar includes 'Home', 'Posting', 'Reporting', and 'Configuration'. The 'Configuration' menu is open, showing options like 'Company Hierarchy', 'Extensions', 'Computation', 'Code Mapping', 'Telephone Tariff', 'Printing', 'Others', and 'Read Only'. The 'Extensions' option is selected, and a sub-menu is displayed with 'Primary Extension Numbering' and 'Slave Extension' highlighted in red. Below the menu, there is a table titled 'Primary Extension Numbering' with columns for 'ExtnNo', 'ExtnName', and 'Proper'. The table contains three rows of data. Below the table is the 'Primary Extension Numbering Information' form, which includes fields for 'Extension Number From', 'Extension Name', 'Section (Dept)', 'Cost Center', 'Budget Charge', 'Budget Duration', 'Designation', 'Service Charge Code', 'Voucher Code', 'Log Code', 'Device Id', 'Post To FOS', 'Guest', and 'Extension Type'.

The screenshot below shows the **Slave Extension** page which also lists the primary extension number on the left column.

The screenshot shows the Unicorn system interface for the 'Slave Extension' page. The user is logged in as 'Hi, Administrator' with the language set to 'English'. The main navigation bar includes 'Home', 'Posting', 'Reporting', and 'Configuration'. The 'Configuration' menu is open, and the 'Slave Extension' option is selected. Below the menu, there is a table titled 'Slave Extension List' with columns for 'ExtensionNumber', 'PropertyID', 'SlaveExtension', 'Edit', and 'Delete'. The table contains three rows of data. Below the table is the 'Slave Extension Information' form, which includes fields for 'Extension Number' and 'Slave Extension'. The 'Extension Number' field is set to '301' and the 'Slave Extension' field is empty. Below the form are buttons for 'Add', 'Update', and 'Reset'. A red note at the bottom states: 'Fields marked with an asterisk * are required.'

6.3. Configure Phoenix

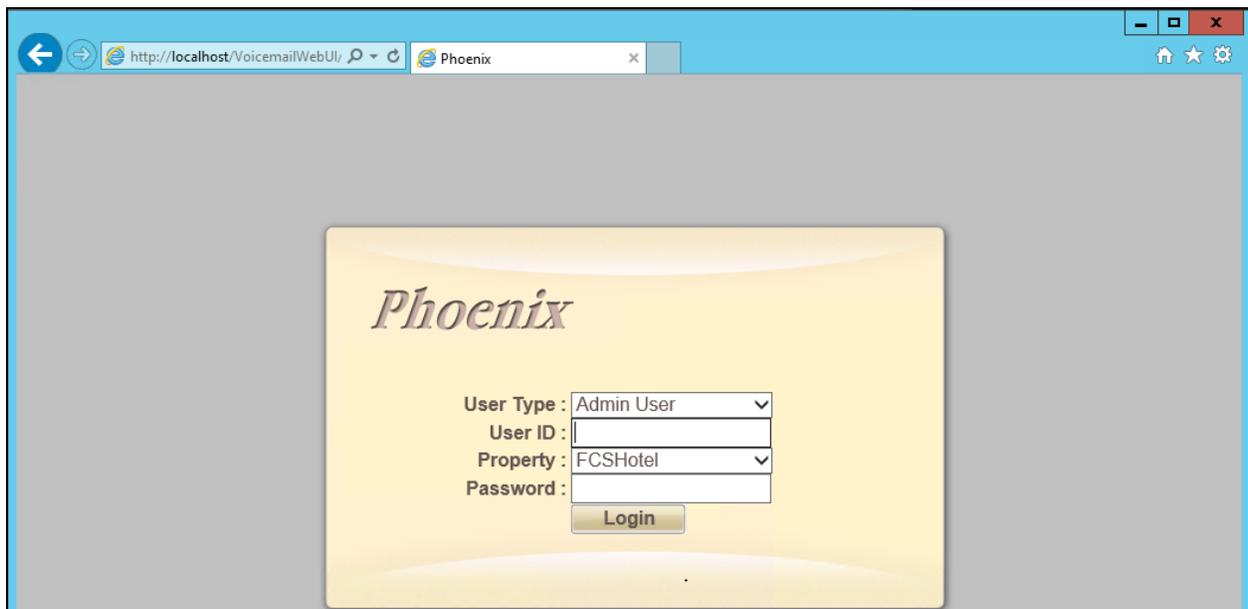
This section details the essential portion of the Phoenix configuration to interoperate with IP Office. These Application Notes assume that the Phoenix application has already been properly installed by FCS services engineer.

The following settings will be verified:

- License Verification
- PBX setting
- Server setting
- Service Numbers (Entry Points)

6.3.1. License Verification

To log into the Phoenix System, launch any browser and type in the Phoenix Configuration URL; in this case <http://<localhost, server name or ip address>/PhoenixWebUI/Login.aspx> as shown below by substituting the appropriate server IP Address. At the login screen, enter an account with administrative privileges.



Select **License** → **Active Licenses**. Ensure that the License has not expired.

The screenshot shows the Phoenix web interface. At the top, there are dropdown menus for 'Property' (set to 'FCSHotel') and 'Language' (set to 'English'). Below this is a navigation bar with tabs for 'System Configuration', 'Hotel Operation', 'Administration', 'Utilities', 'Reports', 'Fax', and 'License'. The 'License' tab is selected, and a sub-tab 'Active Licenses' is also selected. Below the navigation, there is a 'Please Select Organization' dropdown set to 'FCSHotel'. A table titled 'Property' lists license details:

Organization Code	Property Name	Property Code	Expiry Date	License Type	Action
EV0001	FCSHotel	001	2017-06-20	Temporary	

Click on the pen icon under **Action** as shown in the screen above and view the details. Ensure that the appropriate license parameters are enabled.

The screenshot shows the 'License Details' page. It is divided into two main sections: 'License Details' on the left and 'Modules' on the right.

License Details:

- License Type: Temporary
- Expiry Date: 2017-06-20
- MAC Address*: 00:50:56:8E:49:D2
- Organization: Evaluation
- Organization Code: EV0001
- Property: FCSHotel
- External Code: 1
- Address:
- Number Of Rooms: Unlimited
- Number Of Mailboxes: 10000
- Number Of Concurrent Super Users Session: Unlimited
- Number of Concurrent Users Session: Unlimited
- Number Of SIP Ports: MAX
- Number Of Analog Ports: 0
- Number Of E1 Ports: 0

Modules:

- Room Status
- Auto WakeUp
- Auto Attendant
- VPIM
- ConsoleXML
- MiniBar
- Voicemail
- Fax
- Agent-Assisted VIP Wakeup Call
- Voicemail to Email
- Check Out Reminder

Languages:

- English

WebUI Languages:

- English

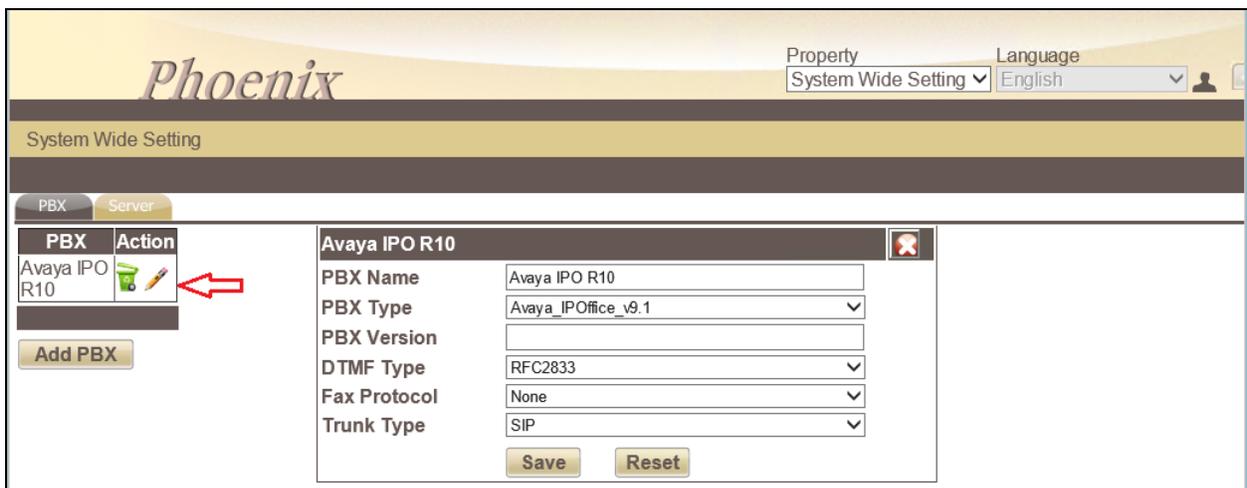
6.3.2. PBX Setting

From the home screen, select **System Wide Setting** from the drop-down menu.



Select the **PBX** tab below. Click on the pen icon and view the PBX settings. Ensure that the following settings are configured:

- **PBX Name:** Enter the appropriate name
- **PBX Type:** Select **Avaya_IPOffice_v9.1** from the drop-down menu
- **PBX Version** Optional field for information
- **DTMF Type:** Select **RFC2833** from the drop-down menu as configured in **Section 5.4** for Primary SIP Extensions
- **FAX Protocol:** Select **None** as fax feature is not offered
- **Trunk Type:** Enter **SIP** for SIP type of signaling with IP Office
- Click **Save**



6.3.3. Server Setting

Select the **Server** tab below and click on the pen icon next to the **Server** name **Phoenix**. Check the box next to “Avaya IPO R10” under **PBX Assigned** and select the appropriate property from the drop down **Property** list. Then click on the **Pencil** icon to edit the settings.

Phoenix

Please restart application for the changes to take effect

App Server Name: Phoenix

IP: 127.0.0.1 Port: 18888

Channel Monitor IP 1

Channel Monitor IP 2

Channel Monitor IP 3

System Trace: Debug Info Log Warning

Info Log Level: NORMAL

E-connect IVR Host Port: 11003

Enable SMTP: IMAP:

Server: [] Port No.: [] SMTP SSL Port No.: [] IMAP use SSL

Email Address: [] SMTP Username: [] SMTP Password: []

PBX Assigned	Interoperability	Property
<input checked="" type="checkbox"/> Avaya IPO R10		FCSHotel

A pop-up form appears, and the SIP User settings are configured as follows:

- **SIP Registration Name:** Provide an appropriate name
- **PBX IP:** Enter Avaya IP Office Server IP address
- **Local IP:** Enter WinExpress Server IP address
- **Transport protocol:** Select **UDP**
- **Client Extension:** Enter the SIP User in a URL form: “[315@10.1.10.121](#)”
- **Contact:** Enter the SIP contact as: “[315@10.1.10.125](#)”
- **Time Alive:** Enter a time less than 180 seconds (default expiry time for SIP registration)
- **Authentication:** Select **Yes**
- **Identity:** Enter the SIP Identity as in **Client Extension** above
- **Realm:** Leave it as default, i.e., **ipoffice**
- **User Name:** User name in **Section 5.5.1**
- **Password:** Login Code in **Section 5.5.1**

Edit SIP Register record

SIP Registration Name: AvayaPOL2

PBX IP: 10.1.10.121 PortNo: []

Local IP: 10.1.10.125 x PortNo: []

Transport protocol: TCP UDP

Client Extension: 315@10.1.10.121

Contact: 315@10.1.10.125

Time Alive: 120

Authentication: Yes No

Identity: 315@10.1.10.121

Realm: ipoffice

User Name: 315

Password: ●●●●●●

6.3.4. Service Numbers (Entry Points)

Select **System Configuration** → **Hardware Settings** → **Channels** → **Entry Point** from the home screen. Check that the Service Numbers tally with the Secondary SIP users created in **Section 5.5.2**. Create an entry with “W_W” mapped to **BUSY/NOANSWER** Call Flow, “315_W” mapped to **DIRECT** Entry Point for Voice Mail Pilot Number **310** and **DIRECT** Entry Point for the rest of the Voice Mail SIP lines **316-317**. The Entry Points configured as shown at the bottom of the home screen.

Phoenix

System Configuration Hotel Operation Administration Utilities Reports Fax L

System Configuration → Hardware Settings → Channels → Entry Point

Entry Point

Entry Point Format : _ Advanced Setting

Call Flow : ▼

Normal Operation : W = This wild card represents any number of whatever lengths

Special Circumstances (Advanced Setting) : C = This character represents the Calling Party and is used for call flows that require such information. For instance, can be used with Direct & SetAWU (when setup for Guests' usage) flows

X = This character is used to specifically ignore the Calling Party information. Typically used for TUI, AA, Minibar/Room Status, Xpress Messaging, and SetAWU (when setup for Operators' usage) call flows

Note: When utilized, both C or X must correspond exactly to the number of digits of the Calling Party it represents

	Entry Point	CPI Format	Description
	1	310_W	DIRECT
	2	311_W	MINIBAR/ROOMSTATUS
	3	312_W	XPRESS MESSAGE LEAVE
	4	313_W	SETAWU
	5	W_W	BUSY/NOANSWER
	6	315_W	DIRECT
	7	316_W	DIRECT
	8	317_W	DIRECT

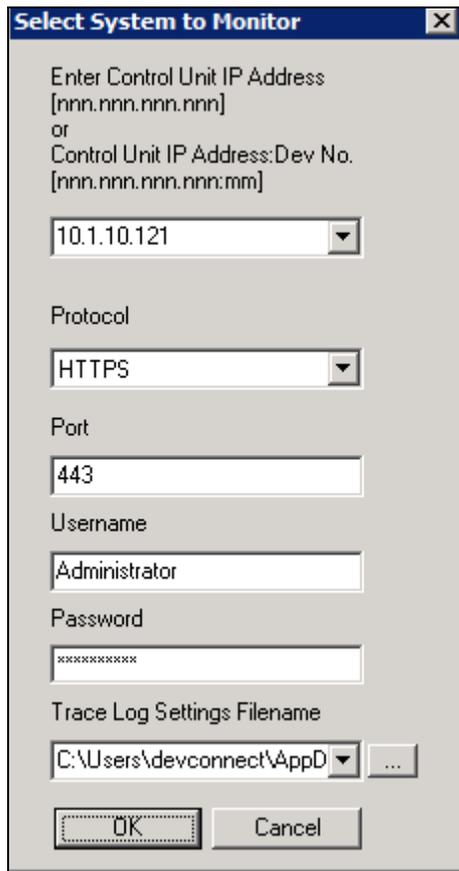
1

7. Verification Steps

This section provides the tests that can be performed to verify the correct configuration of Avaya IP Office and WinExpress.

7.1. Verify SIP User Integration

From a PC running the Avaya IP Office Monitor application, select **Start → All Programs → IP Office → Monitor** to launch the application. Click **File → Select Unit...** and select the Primary Server for the **Control Unit IP Address**. Enter the appropriate **Username** and **Password**. Leave the rest as default.



The screenshot shows a dialog box titled "Select System to Monitor" with the following fields and values:

- Control Unit IP Address: 10.1.10.121
- Protocol: HTTPS
- Port: 443
- Username: Administrator
- Password: [Redacted]
- Trace Log Settings Filename: C:\Users\devconnect\AppData

Buttons: OK, Cancel

Select **Status** → **SIP Phone Status** from the top menu and the **SIPPhoneStatus** screen is displayed. Verify that there are entries for the three Primary SIP Extensions 315, 316 and 317 configured in **Section 5.4** and the **Status** shown is “SIP: Registered” for each, as shown below.

The screenshot shows the SIPPhoneStatus application window. At the top, it indicates 'Total Configured: 6' and 'Total Registered: 3'. A progress bar shows the registration status. Below this is a table with columns: Extn Num, User Num, Security, Behind NAT, IP Address, Private Address, Transport, User Agent, Licensed, SIP Options, SIP Events, SIP Subs..., Status, and LastAv... L. The table lists three SIP phones (315, 316, 317) with their respective configurations and a status of 'SIP: Registered'. The status column for these three rows is highlighted with a red box. At the bottom, there are 'Display Options' (Show All, Registered, UnRegistered), 'Page 1', and buttons for 'Save Page', 'Reset Phones', 'Reregister Phones', and 'Cancel'.

Extn Num	User Num	Security	Behind NAT	IP Address	Private Address	Transport	User Agent	Licensed	SIP Options	SIP Events	SIP Subs...	Status	LastAv... L
311	311	disable		0.0.0.0			UA?	No Licence		0	0	SIP: Unregistered	
312	312	disable		0.0.0.0			UA?	No Licence		0	0	SIP: Unregistered	
313	313	disable		0.0.0.0			UA?	No Licence		0	0	SIP: Unregistered	
315	315	disable		10.1.10.125		UDP	Synway/5.4.0.0	3rd Party IP	R	0	0	SIP: Registered	3
316	316	disable		10.1.10.125		UDP	Synway/5.4.0.0	3rd Party IP	R	0	0	SIP: Registered	3
317	317	disable		10.1.10.125		UDP	Synway/5.4.0.0	3rd Party IP	R	0	0	SIP: Registered	3

7.2. Verify Message Waiting Lamp

Check-In a guest and leave a message for the room. Verify physically or from IP Office System Status application as below that the message waiting lamp is on. Retrieve the message and verify that the message waiting lamp is turned off on the phone.

Avaya IP Office System Status - IPOPRI (10.1.10.121) - IP Office Linux PC 10.0.0.2.0 build 10

AVAYA IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (5)
- Extensions (7)
 - 301
 - 302
 - 304
 - 305
 - 315
 - 316
 - 317
- Trunks (3)
 - Line: 1
 - Line: 2
 - Line: 3
- Active Calls
- Resources
- Voicemail
- IP Networking
 - Locations

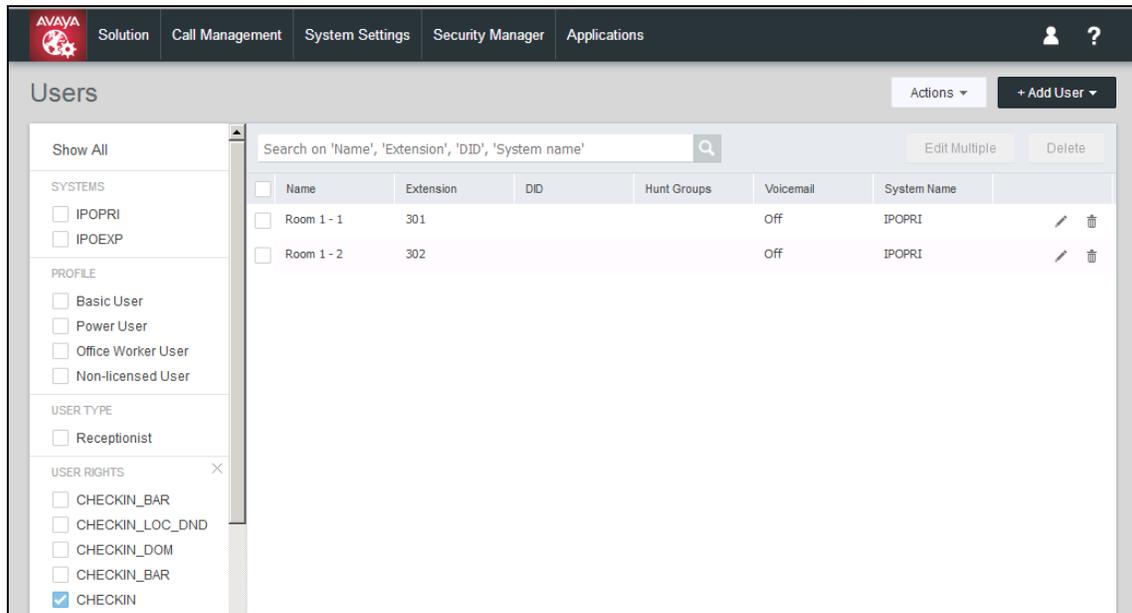
Extension Status

Extension Number: 301
 IP address: 10.1.10.174
 MAC address: B4-B0-17-8B-7C-12
 Standard Location: None
 Gatekeeper: Primary
 Telephone Type: 9621
 Firmware Version: 6.6401
 Media Stream: RTP
 Layer 4 Protocol: TCP
 Current User Extension Number: 301
 Current User Name: Room 1 - 1
 Forwarding: Forward On No Answer 315
 Forward On Busy 315
 Twinning: Off
 Do Not Disturb: Off
Message Waiting: On
 Phone Manager Type: None
 Licensed: Yes
 License Reserved: No
 Last Date and Time License Allocated: 3/31/2017 4:37:56 PM
 DTMF Required: No
 Packet Loss Fraction: Connection Type:
 Jitter: Codec:
 Round Trip Delay: Remote Media Address:

Button Number	Button Type	Call Ref	Current State	Time in State	Calling Number or Called Direct Number
1	CA		Idle	00:03:25	
2	CA		Idle		
3	CA		Idle		

7.3. Verify Configuration Web Service Integration

Use a simulator to perform a guest Check-In request. From the home menu of the IP Office Web Manager, select **Call Management** → **Users** and check the **CHECKIN** box under **USER RIGHTS** on the left pane. Verify on the right pane that the appropriate rooms are Check-In and that physically the guest name is updated on the phone display (depending on phone type) or from the next screen.



Click on the pen icon for **Room 1-1** as seen in the screen above and verify the **Full Name** is correctly reflected.

AVAYA Solution Call Management System Settings Security Manager Applications

User Room 1 - 1 (301)
IPOPRI

User

Voicemail

Short Codes

Button Programming

Telephony

Forwarding

Mobility

Group Membership

Voice Recording

Do Not Disturb

Announcements

Personal Directory

SIP

Menu Programming

Dial In

Source Numbers

Name

Room 1 - 1

Full Name

Patrick Eng

Password

Unique Identity

Extension

301

Account Status

Enabled

Profile

Basic User

Locale

Select...

Priority

5

Login Code

Confirm Login Code

Audio Conference PIN

Confirm Audio Conference PIN

System Phone Rights

None

Device Type

Avaya 9621

7.4. Verify SMDR

On the Unicorn web interface, click **Home** → **System** → **Billing**. Place a few outbound calls to an internal, local, mobile, toll free and international location. Verify that the calls are all processed correctly as shown below:

Hi, Administrator Language: English sign out change password

Home Posting Reporting Configuration Business Date: 04-May-2013 30-Mar-2017 16:52 : Invalid or no cal

Billing

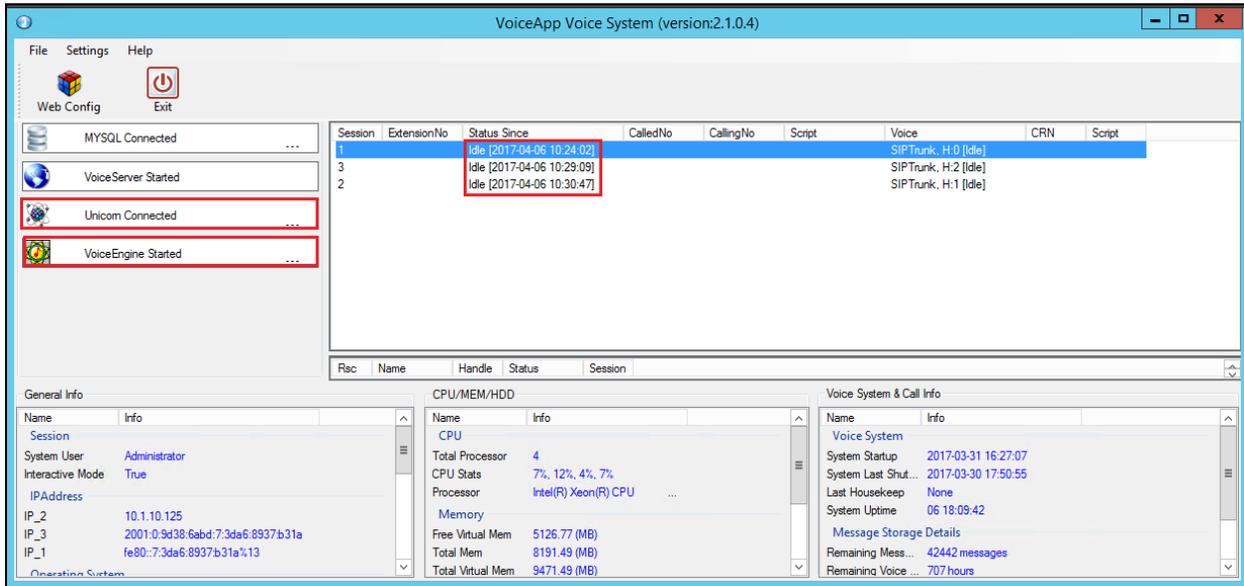
Data last refreshed: 5:18:42 PM Data will be refreshed every 30 sec

Auto refresh Refresh Error PO FP NP

SENDER	DATE	EXTNNO	ROOM	TRUNK	TELEPHONE	DESTINATION	DURATION	COST	BASIC	SURCHARGE	PROFIT	TAX	SERVICE
CDR1	2017/03/30 17:17:24	301	301		020388810XXX	Kuala Lumpur	12s	0.10	0.10	0.00	0.00	0.00	0.00
CDR1	2017/03/30 17:17:07	301	301		68728XXX	Singapore	2s	0.20	0.20	0.00	0.00	0.00	0.00

7.5. Verify Phoenix Voicemail Integration

From the server, launch **Phoenix** from the desktop shortcut  to run the main program. Verify on the left pane that the Voice Engine status shows '**VoiceEngine Started**' and the voice channels under **Status Since** column are **Idle** or **Reserved**. Once the Unicorn communication has been successfully established, the Unicorn status will show up as **Connected**.



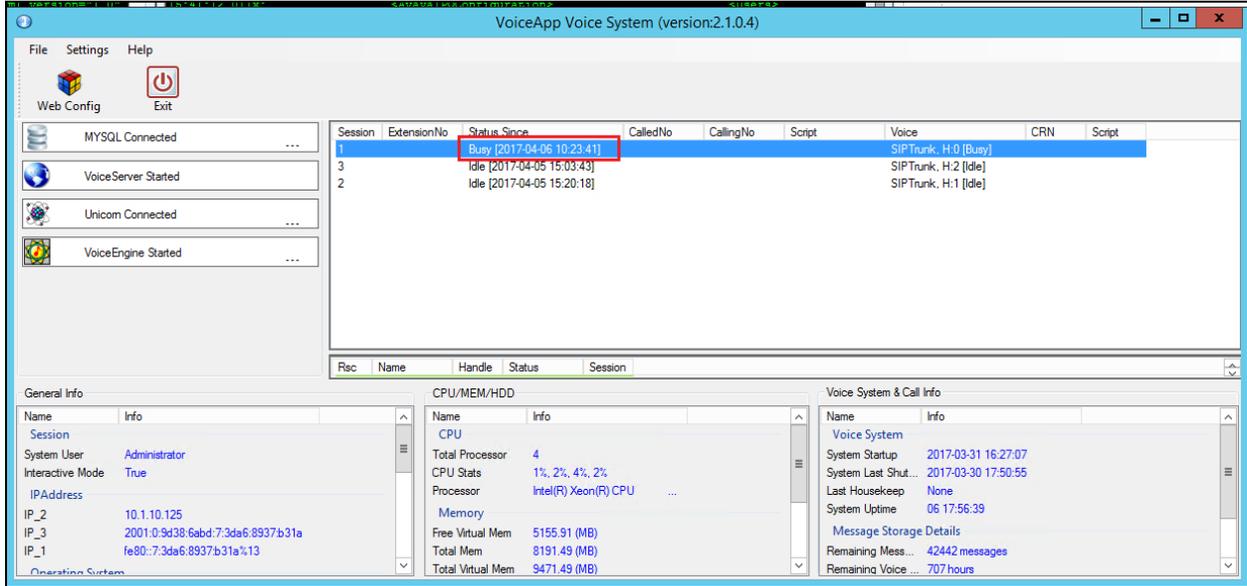
Session	ExtensionNo	Status Since	CalledNo	CallingNo	Script	Voice	CRN	Script
1		Idle [2017-04-06 10:24:02]				SIPTrunk. H.0 [Idle]		
3		Idle [2017-04-06 10:29:09]				SIPTrunk. H.2 [Idle]		
2		Idle [2017-04-06 10:30:47]				SIPTrunk. H.1 [Idle]		

Name	Info
Session	
System User	Administrator
Interactive Mode	True
IPAddress	
IP_2	10.1.10.125
IP_3	2001:0:9d38:6abd:7:3da6:8937b31a
IP_1	fe80::7:3da6:8937b31a%13
Operating System	

Name	Info
CPU	
Total Processor	4
CPU Stats	7%, 12%, 4%, 7%
Processor	Intel(R) Xeon(R) CPU ...
Memory	
Free Virtual Mem	5126.77 (MB)
Total Mem	8191.49 (MB)
Total Virtual Mem	9471.49 (MB)

Name	Info
Voice System	
System Startup	2017-03-31 16:27:07
System Last Shut...	2017-03-30 17:50:55
Last Housekeep	None
System Uptime	06 18:09:42
Message Storage Details	
Remaining Mess...	42442 messages
Remaining Voice ...	707 hours

Dial one of the guest room or front office phone and let it cover to voicemail. Observe that one channel of the SIP Channel is busy as shown below. Verify that leaving a voice mail message to either a guest or front office mailbox works. Also, to verify the Operator transfer function, call any checked-in guest room and let it go to coverage on the voicemail. Press the prompted digit to select for call to be routed to Operator. Verify call is connected to Operator.



8. Conclusion

These Application Notes describe the configuration steps required for WinExpress 3.0 to successfully interoperate with Avaya IP Office Server Edition R10. All features and serviceability test cases were completed with observation noted in **Section 2.2**.

9. Additional References

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

- [1] *IP Office KnowledgeBase 10.0 Documentation Library*, available at <http://marketingtools.avaya.com/knowledgebase/>

Product information and documents for WinExpress Phoenix and Unicorn can be obtained from FCS Computer Systems Sdn Bhd.

©2017 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.