



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring WinExpress 3.0 with Avaya IP Office R9.1 – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for WinExpress 3.0 to interoperate with Avaya IP Office 9.1. WinExpress is a universal interface 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 call accounting package and interface solution. In the compliance testing, WinExpress used SIP Users, TAPI, SMDR, and Configuration Web Service interfaces from Avaya IP Office to provide voicemail, wake-up call, room status, mini-bar posting, call billing, as well as name and user profile template change features.

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 R9.1. WinExpress is a Windows-based hospitality system that provides a seamless interface with a hotel's Front Office System and Avaya IP Office. In the compliance testing, WinExpress used SIP Users, TAPI, SMDR, and Configuration Web Service interfaces from Avaya IP Office to provide voicemail, wake-up call, room status and mini-bar posting, call billing, name and user profile template change, and do not disturb features.

The SIP User and TAPI interfaces were used by WinExpress to provide hospitality features such as voicemail, wake-up call, do not disturb, room status and mini-bar posting. In the compliance testing, Phoenix registers as SIP users on Avaya IP Office for voice mail and wakeup services and posting of mini-bar and room status through the phones. The SIP users were configured as members of a hospitality hunt group. The TAPI interface sets the divert setting for Do Not Disturb for guest room phones when requested manually by the guests.

For the voicemail coverage scenarios, voicemail messages were recorded and saved on WinExpress. The TAPI lineDevSpecific capability was 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 and Avaya IP Office. In the compliance testing, two user rights templates were set up on Avaya IP Office for use with check-in and check-out guests. Unicorn used the Configuration Web Service to send updates to Avaya IP Office on the guest name and user rights template as part of the check-in, check-out, and move process. Two other user rights templates were set up on Avaya IP Office for use with barring and unbarring of guest phones for outgoing calls.

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 wake-up call schedule. The Unicorn was used to manually initiate check-in/check-out/move requests, to activate/deactivate the MWI for Voicemail and to set Do Not Disturb. For SMDR testing, incoming and outgoing calls were made to/from the PSTN 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 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.

### 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 messages and message waiting lamps for check-in, check-out and move requests.
- Voicemail recording and retrieval, with proper message waiting lamp activation/deactivation for users with analog, digital and IP telephone types.
- Scheduling and delivering of wake-up call requests, including retried attempts and escalation to Operator.
- Setting of MWI for both voice and text messages and do not disturb divert parameters using the TAPI interface.
- Posting of room status and mini-bar usage from the room phones.
- Use of Configuration Web Services to update guest name and user rights template associated with check-in, check-out, and move requests from the 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 and rebooting of IP Office and WinExpress server.

## 2.2. Test Results

All test cases were executed and passed. A point to note is that SIP registration with TCP is not successful due to the format of the URL request in the SIP Invite.

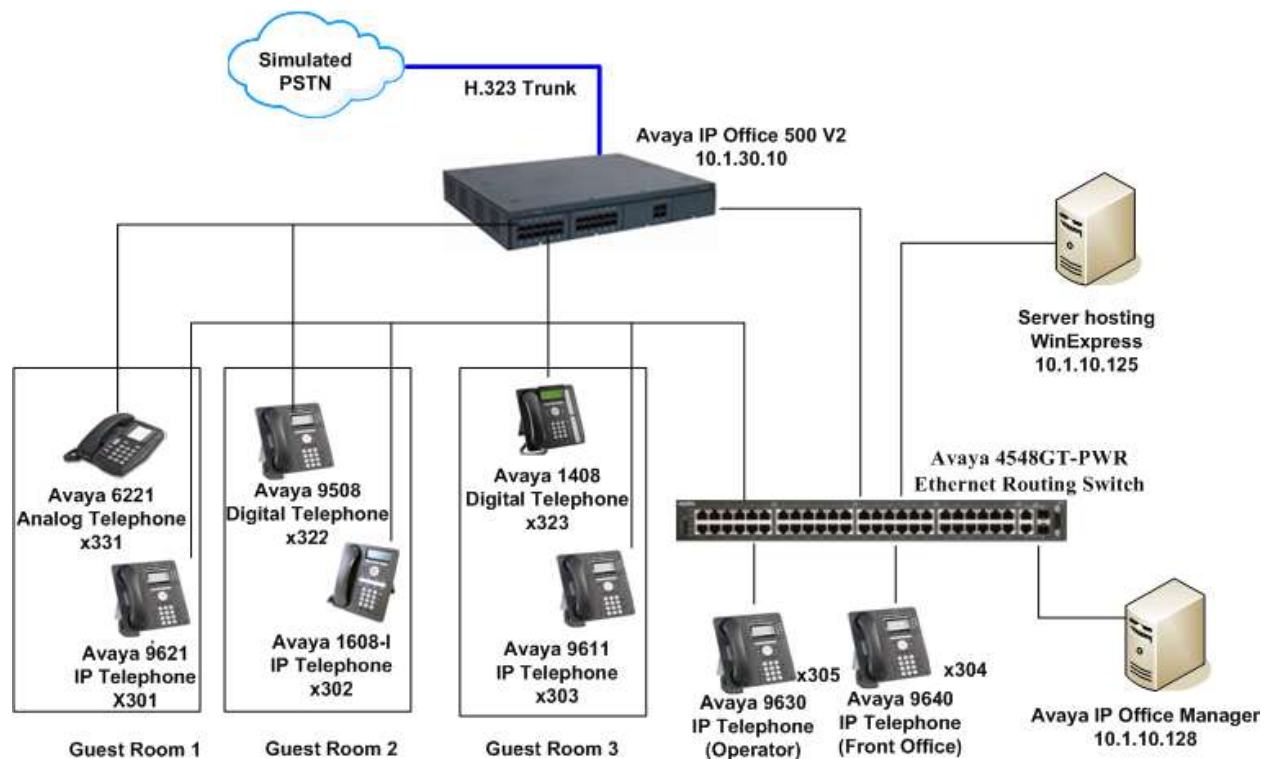
## 2.3. Support

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 server. Unicorn initiate room check-in/check-out and move via an Opera Simulator, capture SMDR, and to set Do Not Disturb. Phoenix handles the voicemail reception, recording and playback, wake-up calls as well as room and mini-bar status setting and reporting.



**Figure 1: Test Configuration of WinExpress 3.0 and Avaya IP Office R9.1**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office 500 V2	9.1.300.120
Avaya IP Office Manager	9.1.300.120
Avaya IP Office TAPI2 Service Provider	1.0.0.42
Avaya 96x1 H323 IP Telephones	6.6029
Avaya 96x0 H323 IP Telephones	3.250A
Avaya 950x H323 IP Telephones	R55
Avaya 16xx H323 IP Telephones	1.360A
Avaya 14xx Digital Telephones	R40
Avaya 6221 Analog Telephone	-
FCS Phoenix running on Microsoft Windows 2012 R2 SP1 on VMware 5.x platform	2.1
FCS Unicorn running on Microsoft Windows 2012 R2 SP1 on VMware 5.x platform	1.2

*Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 only*

## 5. Configure Avaya IP Office

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

- Verify Avaya IP Office license
- Obtain LAN IP address
- Administer SIP Registrar
- Administer SIP Extensions
- Administer SIP Users
- Administer Hospitality Hunt Group
- Administer Incoming Call Route
- Administer System Voicemail
- Administer Voicemail Users
- Administer Analog User MWI
- Administer User Rights
- Administer Security Service
- Administer System Password
- Administer SMDR

### 5.1. Verify Avaya IP Office License

From a PC running the Avaya IP Office Manager application, select **Start → All Programs → IP Office → Manager** to launch the Manager application. Select the correct IP Office system, and log in with the appropriate credentials.

From the home screen configuration tree in the left pane, select **License** and on the right pane scroll down to display the **3rd Party IP Endpoints**. Verify that the **License Status** is “Valid”. This license is required for Phoenix to register to IP Office as a SIP User. The **CTI Link Pro** screen is also shown. Verify that the **License Status** is “Valid”. This license is required for Unicorn to use third-party TAPI control mode on IP Office.

The screenshot shows the Avaya IP Office Manager application. The left pane displays a configuration tree with 'License' selected. The right pane shows the 'License' configuration screen. The 'License Mode' is set to 'License Normal'. The 'Licensed Version' is 9.1. The 'Serial Number (ADT)' is 1347985536. The 'PLDS Host ID' is 111347985536. The 'PLDS File Status' is 'Not Present / Invalid'.

Feature	License Key	Instances	Status	Expiry Date	Source
CTI Link Pro	DvHqOS5x4S20yd3HqRw_HYRVD3yGRLz	255	Valid	Never	ACT Node
Wave User	HvQ8vngpAw2kugf3mXldgS2pl3	255	Valid	Never	ACT Node
Preferred Edition (Voicemail Pro)	anv6GLd3d7H0d35EduGrv6rdsb7Bw	255	Valid	Never	ACT Node
DECT Integration (ports)	aTugd46zvvvNA0xW1DhdxJ6VegxWQHL	255	Obsolete	Never	ACT Node
Phone Manager Pro	Q4kyQWbC0LmJas1ggedugV15rLtpoC	255	Valid	Never	ACT Node
Phone Manager Pro IP Audio Enabled...	14x0eAdE5r5kwh@hag3u16d20j08Dfme	255	Valid	Never	ACT Node
Receptionist	g0uGtmqA5gd38xVqcc13d8Vx0HfJ	255	Valid	Never	ACT Node
Preferred Edition Additional Voicemail...	Hmsu1THAG03FRcV4kue2584no5OPyz	255	Valid	Never	ACT Node
3rd Party IP Endpoints	3v0tsA5p3BcAEfrRucLHGfOswO0qmwH	255	Valid	Never	ACT Node

## 5.2. Obtain LAN IP Address

From the configuration tree in the left pane, select **System** → **SGIP500V2** 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 WinExpress. Note that IP Office can support SIP on the LAN1 and/or LAN2 interfaces, in this compliance testing LAN1 interface is used.



## 5.3. Administer SIP Registrar

From the same screen in **Section 5.2**, select the **VoIP** sub-tab. Ensure that **SIP Registrar Enable** is checked. Enter a valid **Domain Name** for SIP endpoints to use for registration with IP Office. In this compliance testing, the **Domain Name** is left **blank** so that the LAN IP address is used for registration. Ensure the **UDP** and **TCP** is selected for Layer 4 Protocol with **UDP Port 5060**. In this compliance testing, the UDP port is used for SIP registration by Phoenix. TCP port was not successful in registration due to the format of the SIP Invite URL request that can be accepted in this IP Office version.

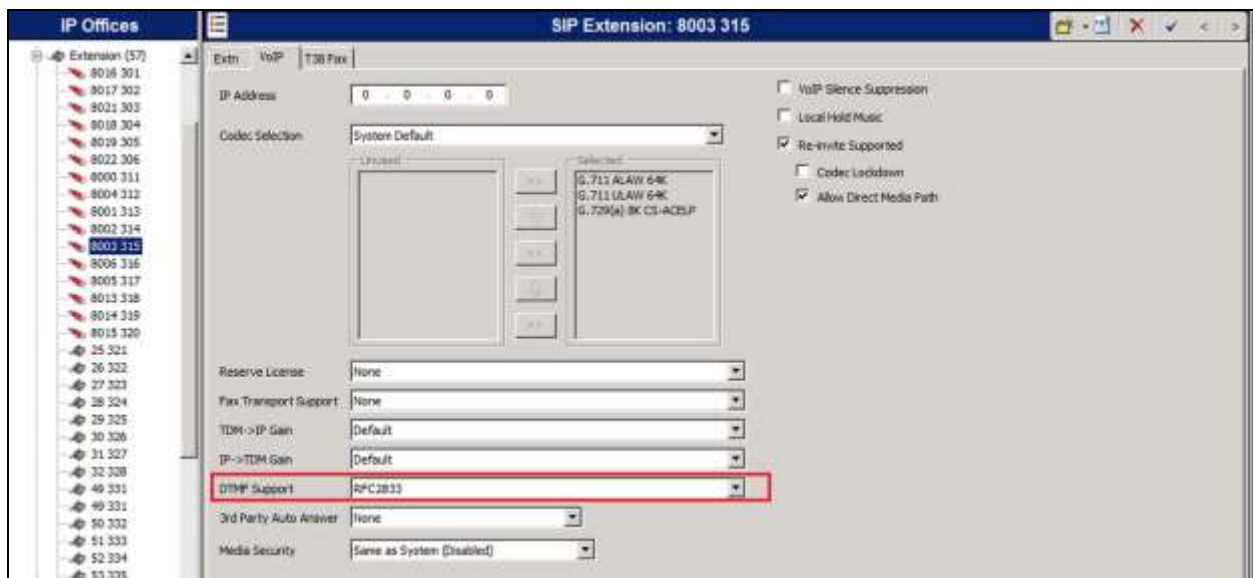


## 5.4. Administer SIP Extensions

From the configuration tree in the left pane, right-click on **Extension** and select **New → SIP Extension** (not shown) from the pop-up list to add a new SIP extension. Enter the desired digits for **Base Extension**, and check **Force Authorization**, as shown below.



Click on the **VoIP** tab and select **RFC2833** from the drop down menu for the DTMF Support.



Repeat this section to add other 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.

**Note:** The number of SIP extensions required depends on the number of Phoenix SIP ports purchased by the customer as well as the number of services they would like to configure.

Call receive by Phoenix at 315-317 will detect the type of call based on the called-party number in the SIP INVITE to determine whether the call is routed from another phone or direct incoming. If it is direct hospitality hunt group 310, 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

## 5.5. Administer SIP Users

SIP users are administered for the SIP extensions created in **Section 5.4**. 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 via a hospitality hunt group configured in **Section 5.6**.

### 5.5.1. Administer Primary SIP Users

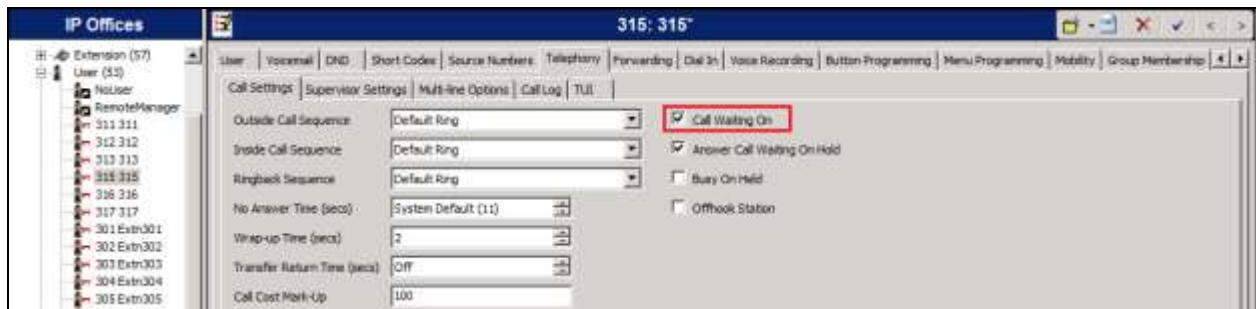
From the configuration tree in the left pane, right-click on **User** and select **New** from the pop-up list (not shown). Enter the desired values for **Name** and **Full Name**. For **Extension**, enter the first Base Extension from **Section 5.4**. Phoenix registers using this primary SIP User to receive calls.

The screenshot displays the 'New User' configuration window in the Avaya IP Office software. The left pane shows the 'IP Offices' tree with 'User (53)' selected. The main pane shows the configuration form for a new user. The 'Name' field is set to '315', 'Full Name' is 'WinExpress VM1', and 'Extension' is '315'. Other fields like 'Password', 'Confirm Password', 'Conference PIN', 'Account Status', 'Email Address', 'Locale', 'Priority', and 'System Phone Rights' are also visible.

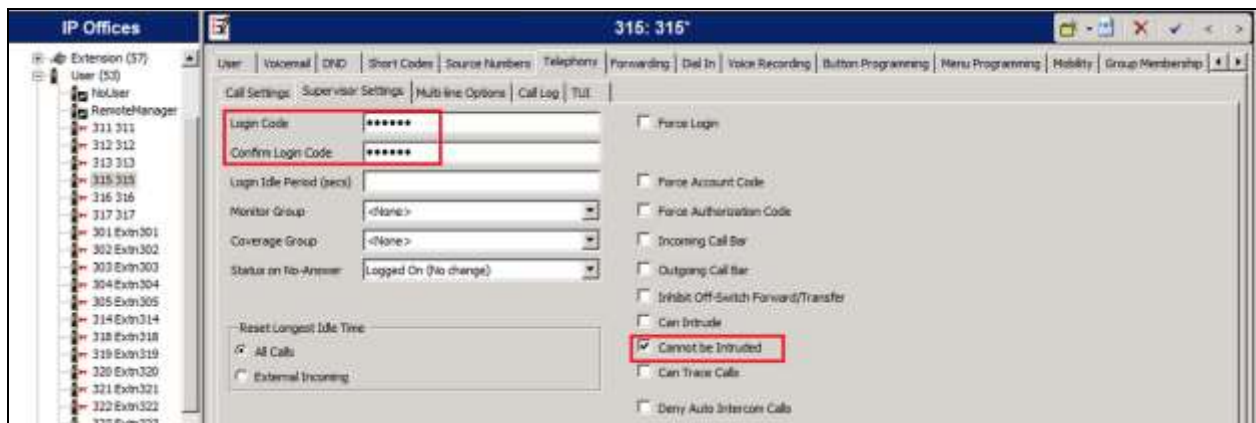
Select the **Voicemail** tab and uncheck **Voicemail On**, as shown below.



Select the **Telephony** tab, followed by the **Call Settings** sub-tab. Check **Call Waiting On**, as shown below.



Select the **Supervisor Settings** sub-tab. Check the **Cannot be Intruded** field, as shown below. Specify the **Login Code** and **Confirm Login Code** field, which will be used by Phoenix to log in as the SIP User.



Repeat this section to add another two primary SIP Users associated with the last two primary SIP Extensions from **Section 5.4**. In this compliance testing, SIP Users 315-317 were created.

## 5.5.2. Administer Secondary SIP Users

From the configuration tree in the left pane, right-click on **User** and select **New** (not shown) from the pop-up list. Enter desired values for **Name** and **Full Name**. For **Extension**, enter the secondary SIP users Base Extension from **Section 5.4**, in this case starting from “311”.

The screenshot shows the 'User' configuration window for user 311. The left pane shows the 'IP Offices' tree with 'User (53)' expanded. The main pane has tabs for 'User', 'Voicemail', 'DND', 'Short Codes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', 'Voice Recording', 'Button Programming', 'Menu Programming', 'Mobility', and 'Group Membership'. The 'User' tab is active. Fields include: Name (311), Password (\*\*\*\*\*), Confirm Password (\*\*\*\*\*), Conference PIN, Confirm Conference PIN, Account Status (Enabled), Full Name (Minibar and Room Status), Extension (311), Email Address, Locale, Priority, System Phone Rights (None), and Profile (Basic User). Red boxes highlight the Name, Full Name, and Extension fields.

Select the **Forwarding** tab. Check **Forward Unconditional** and set the **Forward Number** to the primary SIP Users hunt group, in this case “310”, as shown below. Check **Forward Internal Calls**.

The screenshot shows the 'Forwarding' tab for user 311. Fields include: Block Forwarding (unchecked), Follow Me Number, Forward Unconditional (checked), To Voicemail (unchecked), Forward Number (310), Forward Hunt Group Calls (unchecked), Forward Internal Calls (checked), Forward On Busy (unchecked), Forward On No Answer (unchecked), and Forward Number. Red boxes highlight the Forward Unconditional, Forward Number, and Forward Internal Calls fields.

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 configuration tree in the left pane, right-click on **Group** and select **New** (not shown) from the pop-up list 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, retain the default values in the remaining fields. Click on **Edit** in the **User List** section below the page to add members.

IP Offices

Sequential Group WinVoice: 310

Group | Queuing | Overflow | Fallback | Voicemail | Voice Recording | Announcements | SIP

Name: WinVoice

Extension: 310

Profile: Standard Hunt Group

Ex Directory: ☐

No Answer Time (secs): System Default (11)

Ring Mode: Sequential

Hold Music Source: No Change

Ring Tone Override: None

Agent's Status on No-Answer Applies To: None

The **Select Members** screen is displayed. Select the SIP primary users from **Section 0**, and click the **Append** button to move the selected entries to the right.

Sequential | Hunt Group | 310 WinVoice - Select Members

Filters

Extn Name:

Extn Number:

Available Users (51/51)

Name	Extn
311	311
312	312
313	313
315	315
316	316
317	317
Extn301	301
Extn302	302
Extn303	303
Extn304	304
Extn305	305
Extn314	314
Extn318	318
Extn319	319
Extn320	320
Extn321	321
Extn322	322
Extn323	323

Members (3/3)

Order	Enabled	Name	Extn
1	<input checked="" type="checkbox"/>	315	315
2	<input checked="" type="checkbox"/>	316	316
3	<input checked="" type="checkbox"/>	317	317

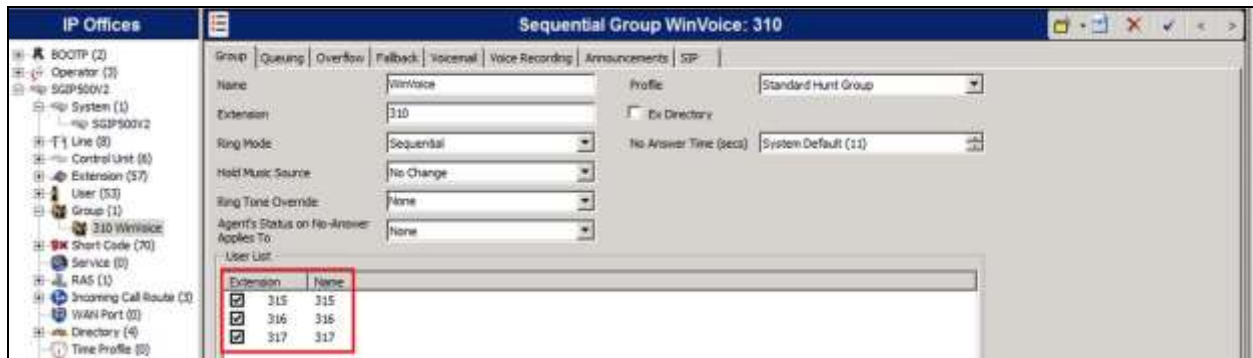
Add Before

Add After

Append

Remove

The **Sequential Group** screen is displayed again and updated with the selected member.



Select the **Voicemail** tab, and make sure **Voicemail On** is unchecked, as shown below.



Select the **Queuing** tab, and uncheck **Queuing On**, as shown below.



## 5.7. Administer Incoming Call Route

If necessary, create an incoming call route to route incoming calls to the desired phones. During compliance testing, an incoming call route was created to route incoming calls for the Trunk, to the front office phone.

As shown in the screen below, the **Incoming Number** for the ISDN PRI line “0” is “33100310”.

The screenshot shows the 'IP Offices' configuration window. On the left is a tree view with the following structure: BOCTP (2), Operator (3), SGP500V2, SGP500V2, Line (8), Control Unit (8), Extension (57), User (53), Group (1), 310 WinVoice, Short Code (70), Service (0), RAS (1), Incoming Call Route (3), 1, 0 33100310, 17 304, WAN Port (0), and Directory (4). The main panel is titled '0 33100310' and has tabs for 'Standard', 'Voice Recording', and 'Destinations'. The 'Standard' tab is active, showing fields for 'Bearer Capability' (Any Voice), 'Line Group ID' (0), 'Incoming Number' (33100310), 'Incoming Sub Address', 'Incoming CLI', 'Locale', 'Priority' (1 - Low), 'Tag', 'Hold Music Source' (System Source), and 'Ring Tone Override' (None). The 'Incoming Number' field is highlighted with a red box.

In the **Destinations** tab, select the front office phone extension from the **Destination** drop-down menu to route all incoming trunk calls to it. During the compliance testing, Extension “304” was used, as shown below.

The screenshot shows the same 'IP Offices' configuration window, but with the 'Destinations' tab selected. The 'Destination' field is a drop-down menu showing '304 Extn 304', which is highlighted with a red box. The 'Fallback Extension' field is empty. The tree view on the left is the same as in the previous screenshot.



## 5.8. Administer System Voicemail

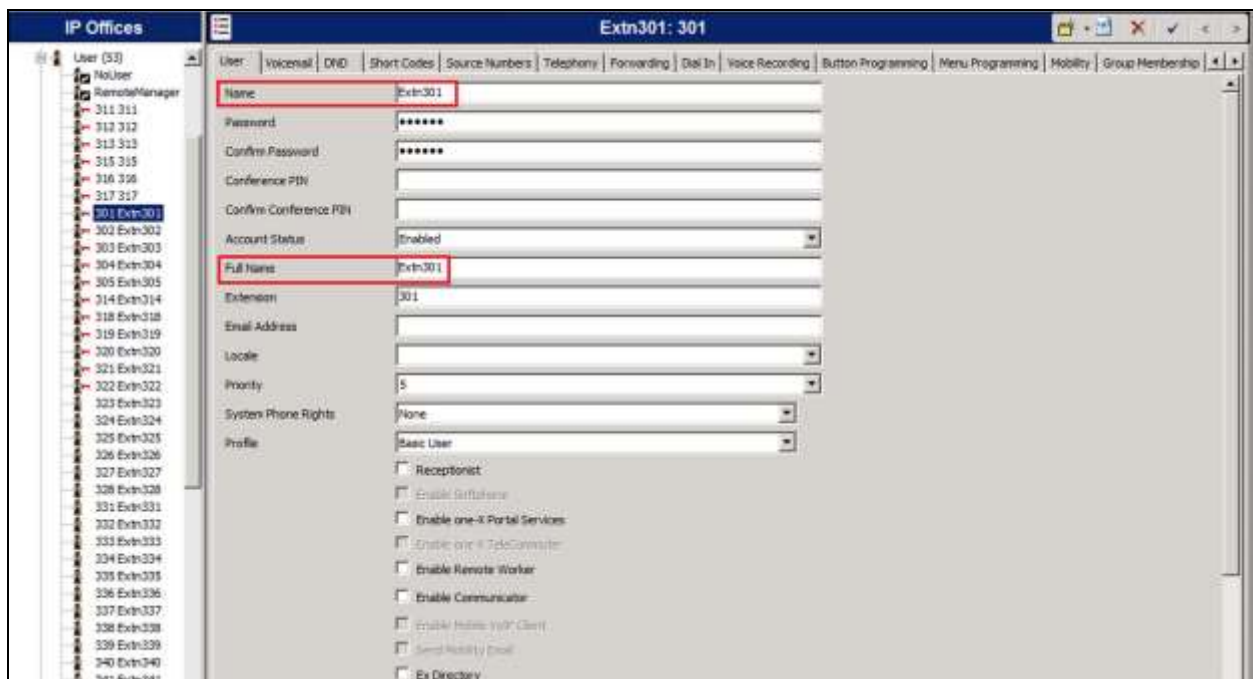
From the configuration tree in the left pane, select **System (1) → SGIP500V2** to display the **SGIP500V2** screen in the right pane. Select the **Voicemail** tab in the right pane.

For **Voicemail Type**, select “Group Voicemail” from the field drop-down list. For **Voicemail Destination**, select the name of the hospitality hunt group from **Section 5.6**.



## 5.9. Administer Voicemail Users

From the configuration tree in the left pane, select the first user that will be using WinExpress for voicemail – these can be Guests and/or Admin staff. In this case, the user is “301”. Enter a descriptive **Name**. The **Full Name** can be completed as a template for identification or blank as it will be used by Unicorn to update the guest name through Configuration Web Services of IP Office.





Select the **Voicemail** tab. Check **Voicemail On**, and uncheck **Voicemail Help**, as shown below.

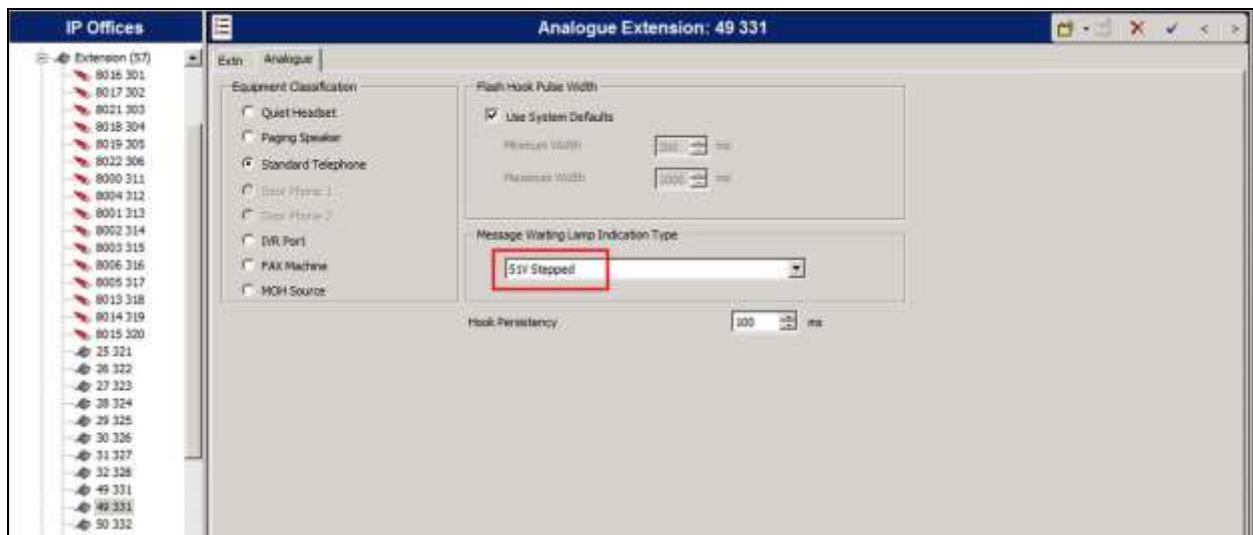
Select the **Forwarding** tab. Uncheck and unselect all fields, as shown below.

Repeat this section for all users using Phoenix for voicemail, including all guest rooms, front desk, and staff. In the compliance testing, the voicemail users consisted of one front desk with extension “304” and four guest rooms with extensions “301, 302, 303, 322, 323 and 331”, as shown in **Figure 1**.

## 5.10. Administer Analog User MWI

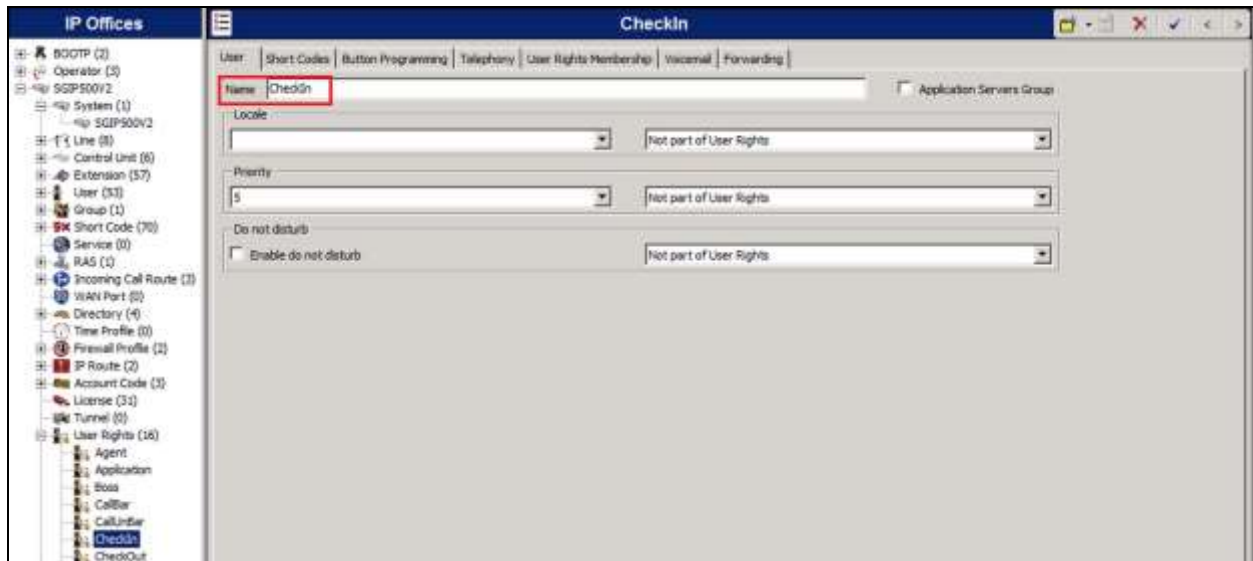
For voicemail users with analog telephones, the MWI setting on the analog extension may need modification, depending on the type of analog telephone. Please refer to **Section 9** of these Application Notes for information on the specific analog telephone types requiring the MWI setting.

From the configuration tree in the left pane, select **Extension**, followed by the extension corresponding to the analog user. In this case, the extension is “331”. In the **Message Waiting Lamp Indication Type** section, “51V Stepped” is selected from the drop-down list, as shown below.

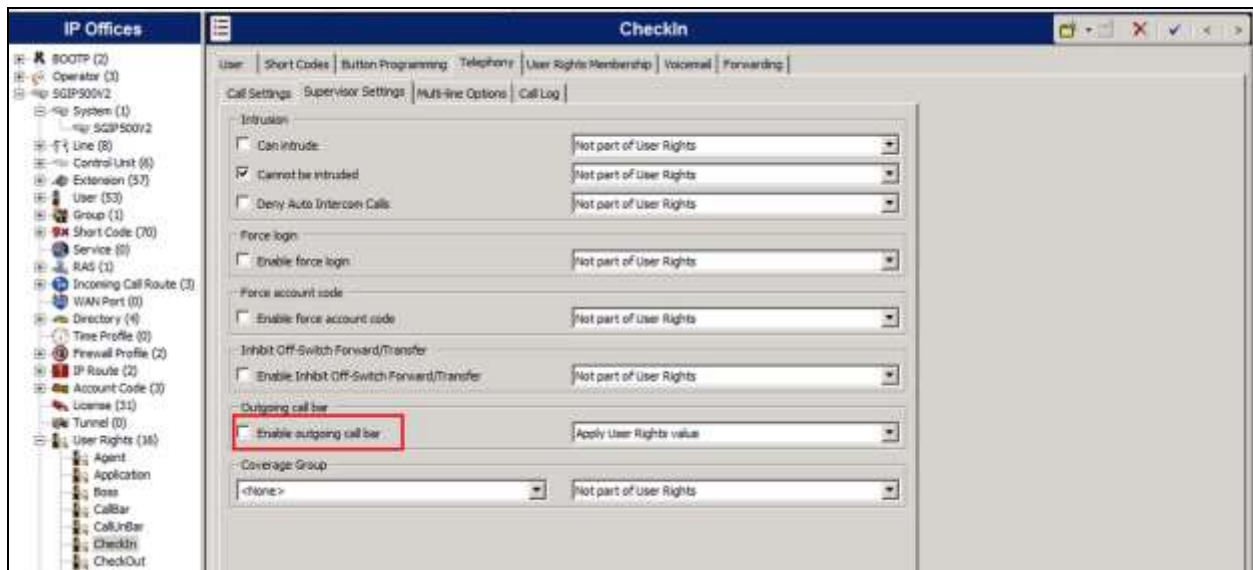


## 5.11. Administer User Rights

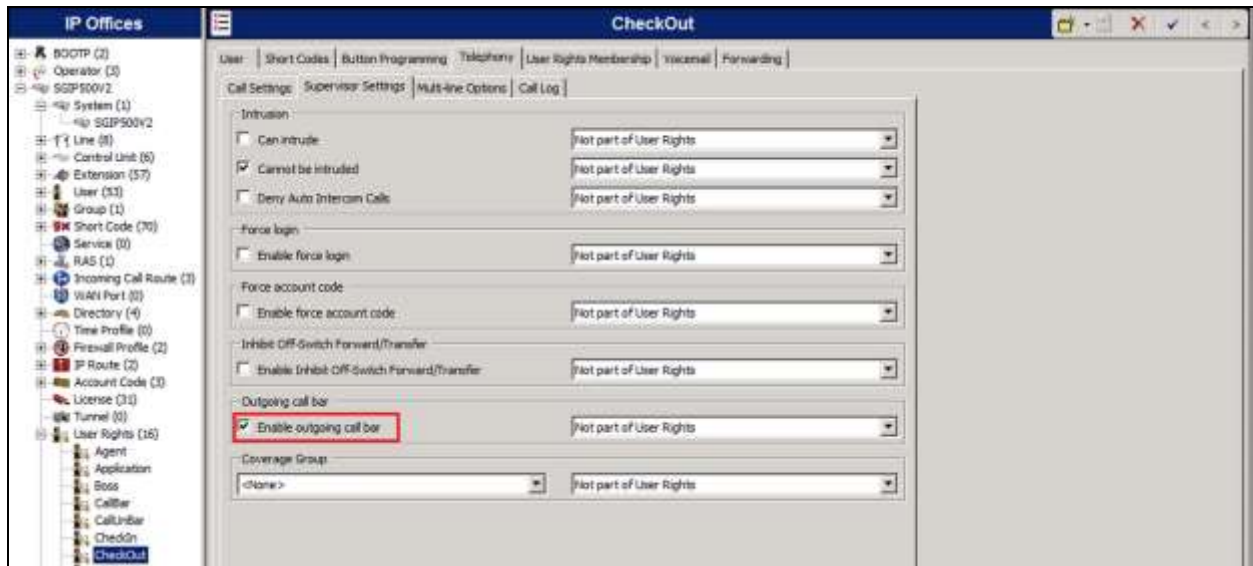
From the configuration tree in the left pane, right-click on **User Rights** and select **New** (not shown) to create a new user rights template. Enter a desired **Name** to designate user rights for guests in the check-in state. In the compliance testing, the name was set to “**CheckIn**” as shown below.



Select the **Telephony** tab and then the **Supervisor Settings** sub-tab. Uncheck **Enable outgoing call bar** field towards the bottom, and select “Apply User Rights Value” from the corresponding drop-down box, as shown below.



Repeat this section to create the desired number of user rights templates for guests in various states. In the compliance testing, four user rights templates with names of “CheckIn”, “CheckOut”, “CallBar” and “CallUnBar” were created, as shown below in the left pane. During this compliance testing, the **Enable outgoing call bar** field was checked for the user rights “CheckOut” and “CallBar” to prevent the guest room users from making calls out to the PSTN when either of these user rights is applied.



## 5.12. Administer Security Service

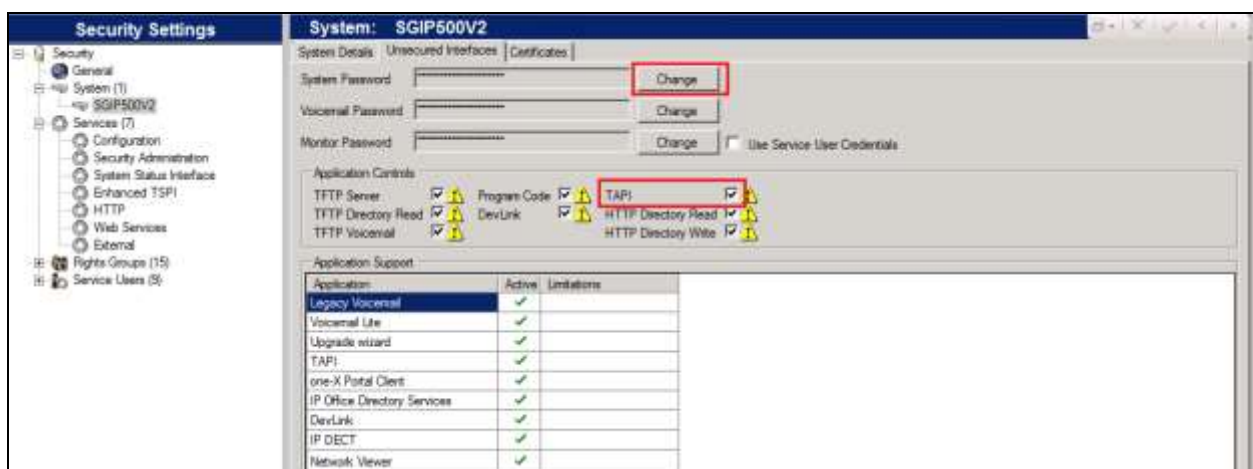
From the **Avaya IP Office Manager** screen, select **File → Advanced → Security Settings** from the top menu. Select the correct IP Office system and log in with the appropriate security user credentials.

The **Avaya IP Office Manager - Security Administration** 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 “**Unsecure + Secure**” as shown below. In this compliance testing, Unicorn used the “Unsecure” level for the Configuration Web Service interface.



## 5.13. Administer System Password

From the **Avaya IP Office Manager – Security Administration** screen, select **Security → System** from the configuration tree in the left pane to display the **System: SGIP500V2** screen in the right pane. In the **Unsecured Interfaces** tab, click the **Change** button next to the **System Password** to configure the IP Office System Password. The System Password is used in **Section 6.1** to configure the TAPI Driver. Also ensure that **TAPI** interface is enabled by checking the box.



## 5.14. Administer SMDR

From the configuration tree in the left pane, select **System** to display the **SGIP500V2** screen in the right pane, next select the **SMDR** tab. 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 to “**3000**” and check **Call Splitting for Diverts**.



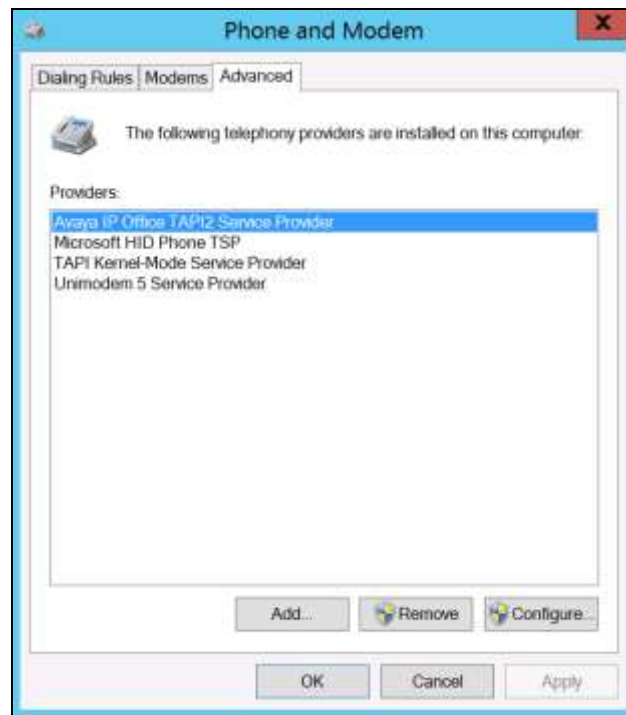
## 6. Configure WinExpress

This section provides the procedures for configuring WinExpress. WinExpress comprises of 2 main components, i.e., Phoenix guest voicemail and Unicorn call accounting package and interface solution. The procedures include the following:

- Administer TAPI driver
- Obtaining IP Office Configuration Web Service SDK
- Configuring Unicorn
- Configuring Phoenix

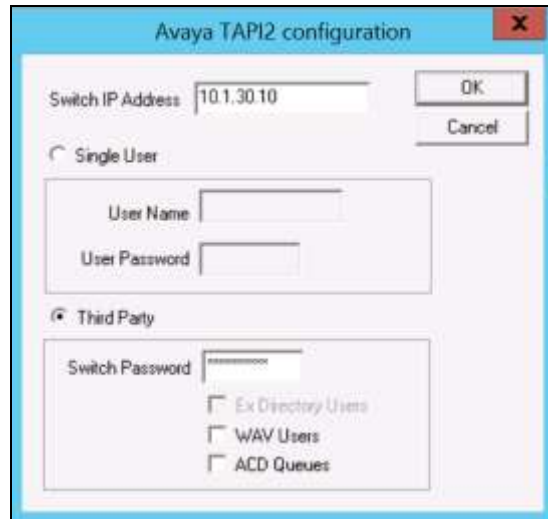
### 6.1. Administer TAPI Driver

Download and install the Avaya IPO TAPI Driver first (not shown). From the WinExpress server as shown in **Figure 1**, select **Start → Control Panel**, and click on the **Phone and Modem** icon (not shown). In the **Phone and Modem** screen, select the **Advanced** tab. Select the **Avaya IP Office TAPI2 Service Provider** entry, and click **Configure**.





The **Avaya TAPI2 configuration** screen is displayed. For **Switch IP Address**, enter the LAN1 IP address of IP Office defined in **Section 5.2**. Select the radio button for **Third Party**, and enter the IP Office **System Password** configured in **Section 5.13** into the **Switch Password** field. Reboot the WinExpress server.

The image shows a Windows-style dialog box titled "Avaya TAPI2 configuration". It has a light blue border and a red close button in the top right corner. Inside the dialog, there is a text field for "Switch IP Address" containing the value "10.1.30.10". To the right of this field are "OK" and "Cancel" buttons. Below this, there are two radio buttons: "Single User" (which is unselected) and "Third Party" (which is selected). Under the "Single User" section, there are text fields for "User Name" and "User Password". Under the "Third Party" section, there is a text field for "Switch Password" which contains a series of asterisks. Below the "Switch Password" field are three unchecked checkboxes labeled "Ex Directory Users", "WAV Users", and "ACD Queues".

## 6.2. 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 Configuration Web Service SDK must match the release of the IP Office that is deployed, in this case Release 9.1. To obtain the IP Office Configuration Web Service SDK, browse to <http://www.devconnectprogram.com/> using a web browser and login using a valid DevConnect member account. Then click **Downloads → IP Office™ → Configuration Web Services**. Locate and download the latest Configuration Web Service SDK which in this case is 9.1.1.0. An FCS implementation engineer will then deploy the files from the Configuration Web Service SDK onto the WinExpress server.

### 6.3. 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 personnel.

1. Unicorn Interface configuration to enable Phoenix, Avaya IPO PMS WS, Avaya IPO TAPI and Avaya IPO CDR in **Unicorn.xml** located is in the “C:\Program Files(x86)\FCS\Unicorn\Control\” directory.

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

```
Child Id="VMS1">
    <PropertyId>MY99</PropertyId>
    <EXENAME>Phoenix.VMS.exe</EXENAME>
    <LogFilePattern>VMS\VMS1-</LogFilePattern>
    <Description>Phoenix.VMS</Description>
    <XMLFile>Phoenix-VMS.xml</XMLFile>
    <IntfInQueueName>.\Private$\VMS1In</IntfInQueueName>
    <IntfOutQueueName>.\Private$\VMS1Out</IntfOutQueueName>

    <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
    <UnicornMotherIPPort>4017</UnicornMotherIPPort>
    <MemoryPage>7</MemoryPage>
</Child>

<Child Id="PBX1">
    <PropertyId>MY99</PropertyId>
    <EXENAME>AvayaIPOPMS.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>
    <LogFilePattern>PBX\PBX2-</LogFilePattern>
    <EXENAME>AvayaIPOTAPI.PBX.exe</EXENAME>
    <Description>AvayaIPOTAPI PBX Interface</Description>
    <XMLFile>AvayaIPOTAPI-PBX.xml</XMLFile>
    <IntfInQueueName>.\Private$\PBX2In</IntfInQueueName>
    <IntfOutQueueName>.\Private$\PBX2Out</IntfOutQueueName>
    <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
```

```

    <UnicornMotherIPPort>9302</UnicornMotherIPPort>
    <MemoryPage>11</MemoryPage>
  </Child>

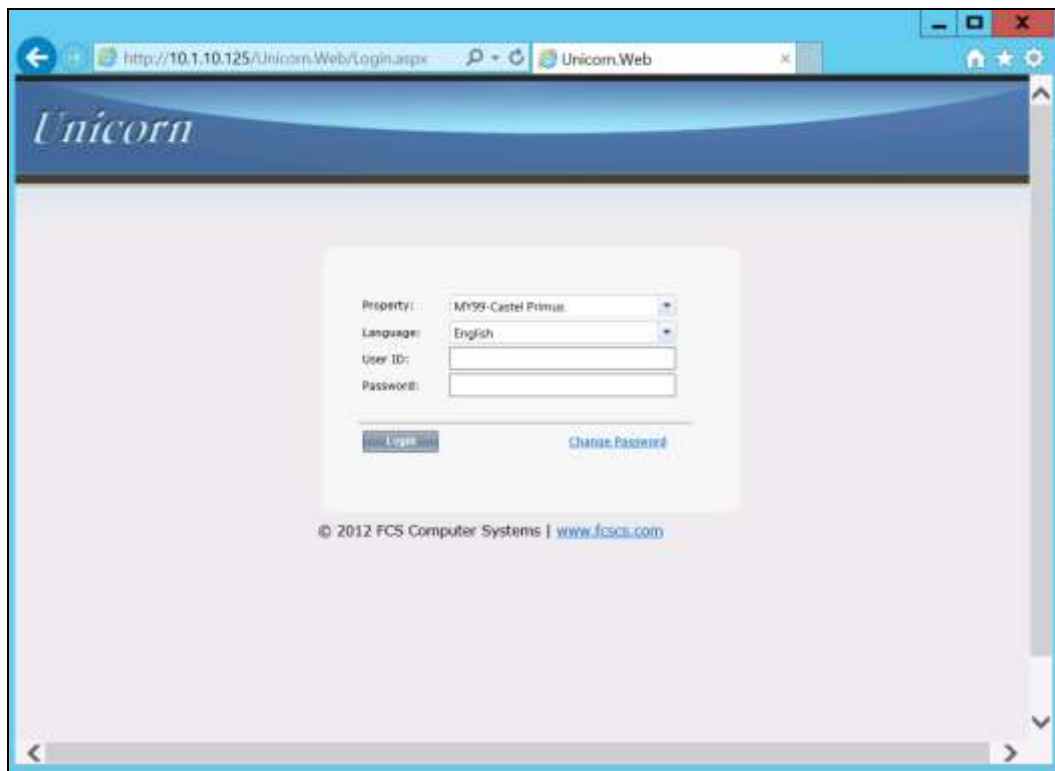
  <Child Id="CDR1">
    <PropertyId>MY99</PropertyId>
    <LogFilePattern>CDR\CDR1-</LogFilePattern>
    <EXENAME>AvayaIPO.CDR.exe</EXENAME>
    <Description>AvayaIPO CDR Interface </Description>
    <XMLFile>AvayaIPO-CDR.xml</XMLFile>
    <IntfInQueueName>.\Private$\SMDRIn</IntfInQueueName>
    <IntfOutQueueName>.\Private$\SMDROut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


    <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
    <UnicornMotherIPPort>4001</UnicornMotherIPPort>
    <MemoryPage>9</MemoryPage>

  </Child>

```

2. FCS Unicorn provides a web interface for configuration, posting and 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 login with the appropriate credentials.



3. Click **Home → System → Interface Listing** to show the interface integrated and their status which should show up . Below is the **Device ID** list and their purpose.
  - a. **FOS1** – Front Office System
  - b. **VMS1**- Phoenix Voicemail
  - c. **PBX1** – IP Office PMS
  - d. **PBX2** – IP Office TAPI
  - e. **CDR1** – IP Office SMDR




Unicorn

Hi, Administrator Language: English sign out change password

Home Posting Reporting Configuration Business Date: 11-Oct-2012 26-Aug-2015 03:00 : Manual Buffer Start(CDR1)

**Interface Listing**

Refresh Last refreshed at 2:38:01 PM

DEVICE ID	DEVICE DESC	EXE NAME	VERSION	STATUS	POSTING
FOS1	Fidelio FIAS	FIAS.FOS.exe	1.2.3.74		OFF
VMS1	Phoenix.VMS	Phoenix.VMS.exe	1.2.2.30		ON
PBX1	AvayaIPOPMS	AvayaIPOPMS.PBX.exe	1.0.0.19		ON
PBX2	AvayaIPOPAPI PBX Interface	AvayaIPOPAPI.PBX.exe	1.2.1.8		ON
CDR1	AvayaIPO CDR Interface	AvayaIPO.CDR.exe	1.2.1.7		N/A

Occupancy 66.67%

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

```
    S = 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://localhost:8085/IPOConfigurationService</InterfaceSetting>
<UDPSvrInterfaceSetting>U,127.0.0.1:4544</UDPSvrInterfaceSetting>
-->
```

In the same configuration file at the lower portion, the host is set as **tcp.ip** type listening to port **50805** which corresponds with the IP Office port at **Section 5.12** and the appropriate **AccountName** and **password** administered. The password is not revealed for security reasons.

```
-->
<InterPacketDelay>100</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>100</InterStringDelay>
<!--in second-->
<SendRetry>3</SendRetry>
<AccountName>Administrator</AccountName>
<PassWord> </PassWord>
<IPAddress>10.1.30.10</IPAddress>
<PortNumber>50805</PortNumber>
</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 5.14**.

```
<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,192.168.42.10,5050</InterfaceSetting>
    <!-- if tcp.ip, interface setting 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>
    <CheckRTSSignal>No</CheckRTSSignal>
  </CommunicationSetting>
</PBX ID="CDR1">
```

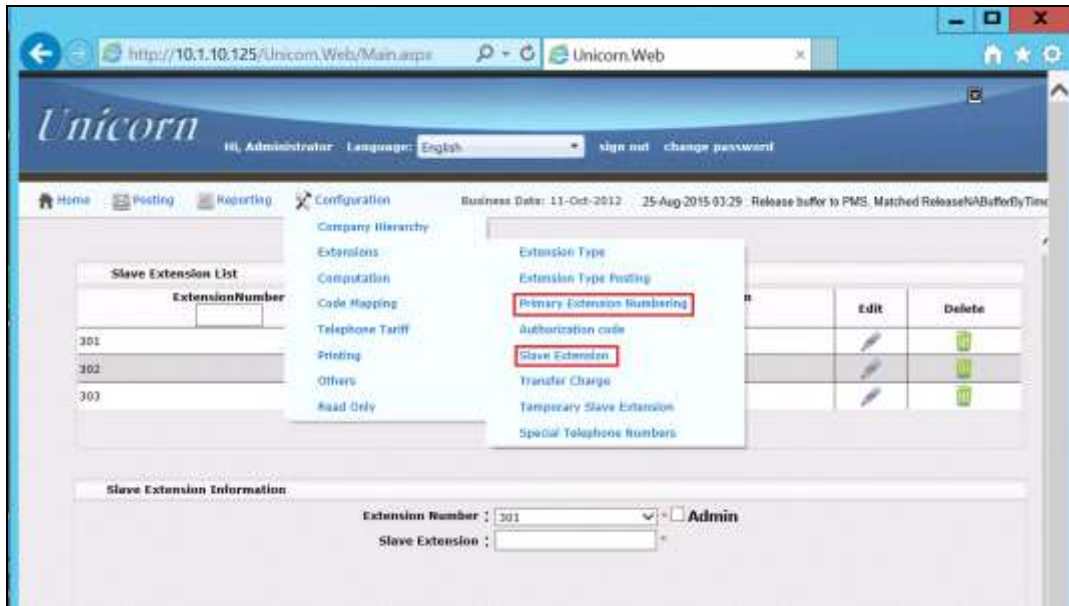
6. The **Posting** tab below shows the various PMS features such as Check In/Out, Edit Guest Profile, etc. that can be performed from the web interface. The screenshot below shows the **Check In/Out** page for checking a guest with name, date, room number and check in/out date etc.

The screenshot displays the Unicorn PMS web interface. The browser address bar shows 'http://10.1.10.125/Unicorn.Web/Main.aspx'. The page title is 'Unicorn'. The navigation menu includes 'Home', 'Posting', 'Reporting', and 'Configuration'. The 'Posting' menu is expanded, showing 'Guest', 'Room', 'Charges', 'Check In/Out', 'Edit Profile', and 'Room Change'. The 'Check In/Out' page contains the following fields:

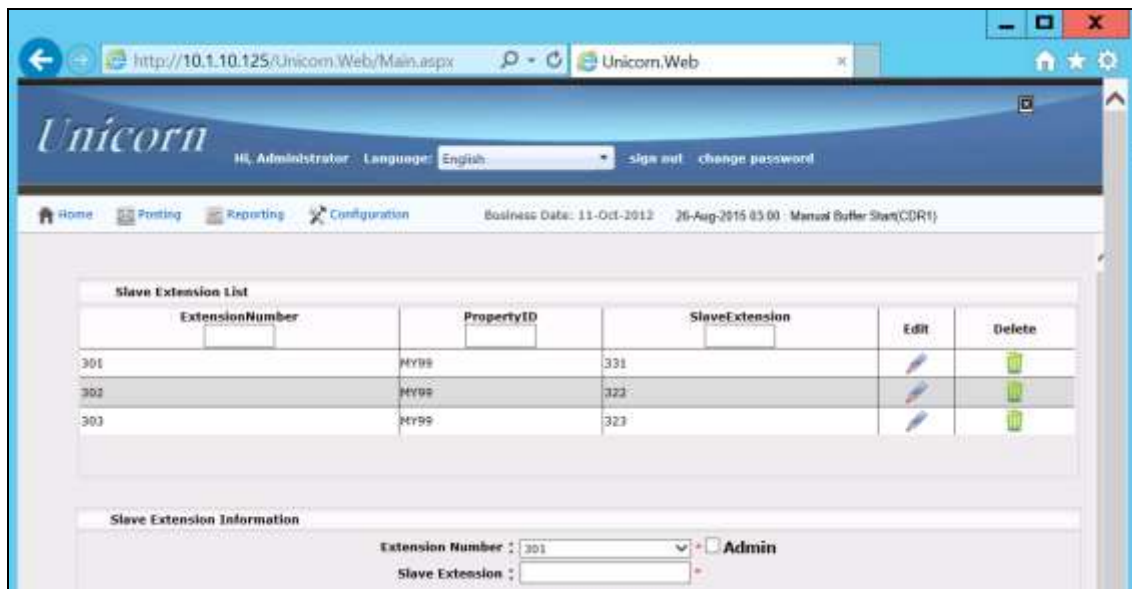
- Ext. No.: (Placeholder: (Mandatory) Ext. No. e.g. 2000 or 2000,2000,3000)
- Room No.: (Placeholder: (Mandatory) Room No.) ☐ Share Room
- Guest Name: (Placeholder: (Mandatory) Guest Name) Title
- First Name: (Placeholder: (Mandatory) First Name) Last Name: (Placeholder: (Mandatory) Last Name)
- Check In: 26 Aug 2015, Wednesday 00:00
- Check Out: 27 Aug 2015, Thursday 12:00
- Folio No.: (Placeholder: Folio No.) Group No.: (Placeholder: Group No.)
- VIP No.: (Placeholder: VIP No.) Password: (Placeholder: Password)
- Language: EN-English
- CDS: UA-Universal (DDO/Intl and STD/Domestic and local call)



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



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



## 6.4. Configure Phoenix

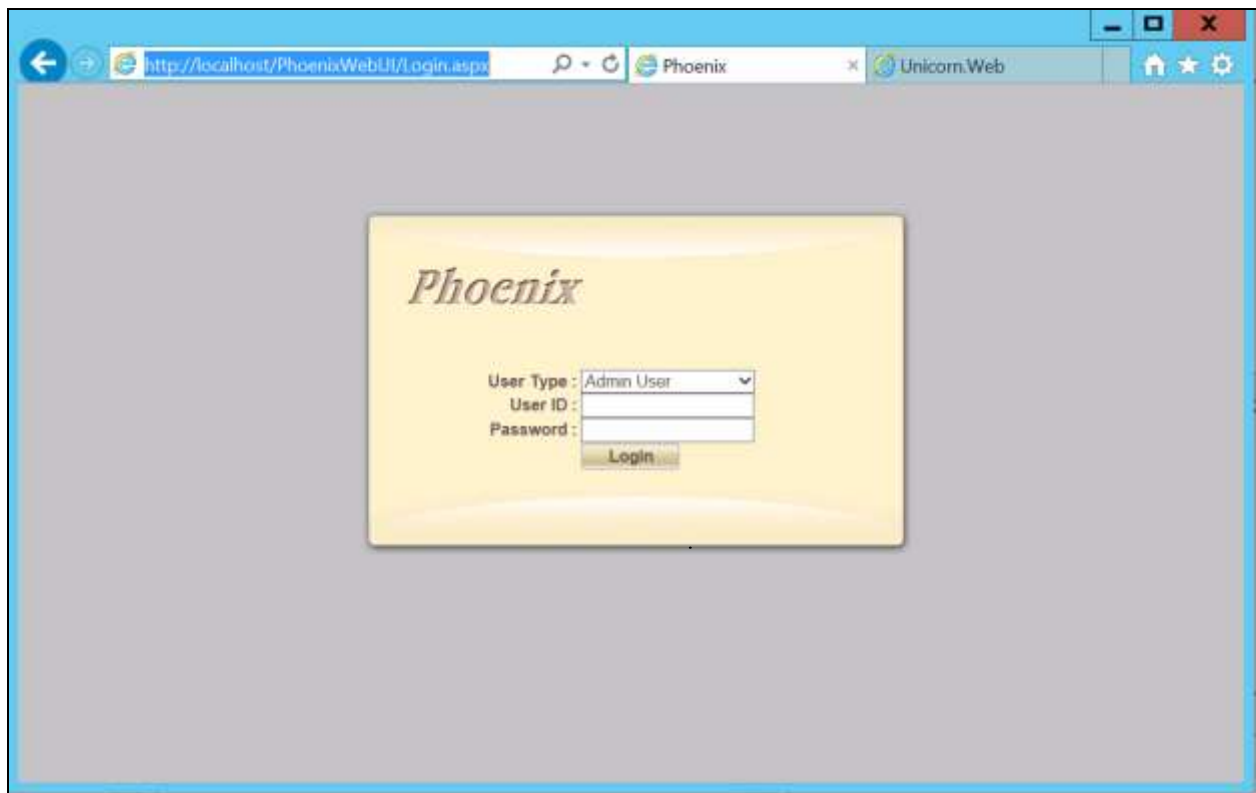
This section details the essential portion of the Phoenix configuration to interoperate with IP Office. These Application Notes assume that the Phoenix application has already been properly installed by FCS professional services personnel.

The following settings will be verified:

- License Verification
- PBX setting
- Server setting
- Service Numbers

### 6.4.1. License Verification

To log into the Phoenix System, launch Microsoft Internet Explorer and type in the Phoenix Configuration URL, in this case <http://<server name or ip address>/PhoenixWebUI/Login.aspx> as shown below by substituting the appropriate server ip address. At the login screen, log in using an account with administrative privileges.





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

The screenshot shows the Phoenix System Wide Setting interface. At the top, there's a header with the 'Phoenix' logo and navigation links for 'Property' (System Wide Setting) and 'Language' (English). Below this, a 'System Wide Setting' section contains tabs for 'License' and 'Upload License File'. The 'License' tab is active, showing a sub-tab for 'Active Licenses'. A dropdown menu for 'Please Select Organization' is set to 'CastelPrimus'. Below this is a table with columns: Organization Code, Property Name, Property Code, Expiry Date, License Type, and Action. The first row shows 'EV0001', 'CastelPrimus', '001', '2015-10-03', 'Temporary', and a pen icon in the Action column.

Organization Code	Property Name	Property Code	Expiry Date	License Type	Action
EV0001	CastelPrimus	001	2015-10-03	Temporary	

Click on the pen under **Action** 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. The left section contains a list of license parameters and their values: License Type (Temporary), Expiry Date (2015-10-03), MAC Address\* (00:0C:29:93:97:E5), Organization (Evaluation), Organization Code (EV0001), Property (CastelPrimus), External Code (1), Address (empty field), Number Of Rooms (Unlimited), Number Of Mailboxes (10000), Number Of Super Users (Unlimited), Number Of Web Users (Unlimited), Number Of SIP Ports (MAX), Number Of Analog Ports (0), Number Of E1 Ports (0), Number Of Fax Ports (MAX), and Number Of Enhanced RTP (0). The right section contains two lists: 'Modules' and 'Languages'. The 'Modules' list includes Room Status, Auto WakeUp, Auto Attendant, VPIM, ConsoleXML, MiniBar, Voicemail, Fax, IVR, Agent-Assisted VIP Wakeup Call, and Voicemail to Email. The 'Languages' list includes English, arabic, british, and CANTONESE.

Parameter	Value
License Type	Temporary
Expiry Date	2015-10-03
MAC Address*	00:0C:29:93:97:E5
Organization	Evaluation
Organization Code	EV0001
Property	CastelPrimus
External Code	1
Address	
Number Of Rooms	Unlimited
Number Of Mailboxes	10000
Number Of Super Users	Unlimited
Number Of Web Users	Unlimited
Number Of SIP Ports	MAX
Number Of Analog Ports	0
Number Of E1 Ports	0
Number Of Fax Ports	MAX
Number Of Enhanced RTP	0

**Modules:**

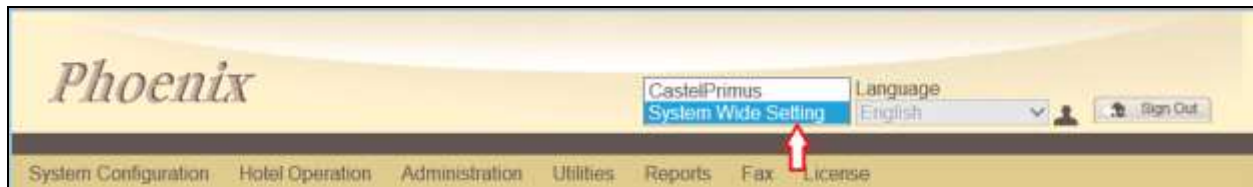
- Room Status
- Auto WakeUp
- Auto Attendant
- VPIM
- ConsoleXML
- MiniBar
- Voicemail
- Fax
- IVR
- Agent-Assisted VIP Wakeup Call
- Voicemail to Email

**Languages:**

- English
- arabic
- british
- CANTONESE

### 6.4.2. PBX Setting

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



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

- **PBX Name:** Enter the appropriate name
- **PBX Type:** Select **Avaya\_IPOffice\_v6.1** from the drop down menu
- **PBX Version:** Enter 9.1 for the version number
- **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



### 6.4.3. Server Setting

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

The screenshot shows the Phoenix web interface. The top navigation bar includes the 'Phoenix' logo, a 'Property' dropdown set to 'System Wide Setting', and a 'Language' dropdown set to 'English'. The left sidebar has a 'Server' tab selected, with a red arrow pointing to the 'Phoenix' server entry. The main content area displays the configuration for the 'Phoenix' App Server. A red arrow points to the 'Edit' (pencil) icon next to the 'Phoenix' server name. The configuration fields include:

- App Server Name:** Phoenix
- IP:** 127.0.0.1
- Port:** 18888
- Channel Monitor IP 1, 2, 3:** Checkboxes are checked.
- System Trace:** Debug, Info Log, and Warning checkboxes are checked.
- Info Log Level:** NORMAL (dropdown)
- E-connect IVR Host Port:** 11003
- SMTP:** Enable checkbox is unchecked.
- IMAP:** Enable checkbox is unchecked.
- Server, Port No., SMTP SSL Port No., Email Address, SMTP Username, SMTP Password:** Fields are present but empty.
- PBX Assigned:** Avaya IPO checkbox is checked.
- Interoperability:** Edit (pencil) icon.
- Property:** CastelfPrimus (dropdown).

At the bottom of the configuration area, there is a red arrow pointing to the 'Edit' (pencil) icon.

A pop-up form appears, below is a sample of the SIP User settings configured.

- **Connection Type:** Select **SIP Register**
- **SIP Registration Name:** Provide an appropriate name
- **PBX IP:** Enter Avaya IP Office IP address
- **Local IP:** Enter WinExpress server IP address
- **Transport protocol:** Select **UDP**
- **Client Extension:** Enter the SIP User in a URL form: “[316@10.1.30.10](#)”
- **Contact:** Enter the SIP contact as: “[316@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**

The screenshot shows a configuration window titled "PBX Interoperability - Avaya IPO". It has two radio buttons at the top: "SIP Register" (selected) and "SIP Trunk". Below are various input fields and checkboxes:

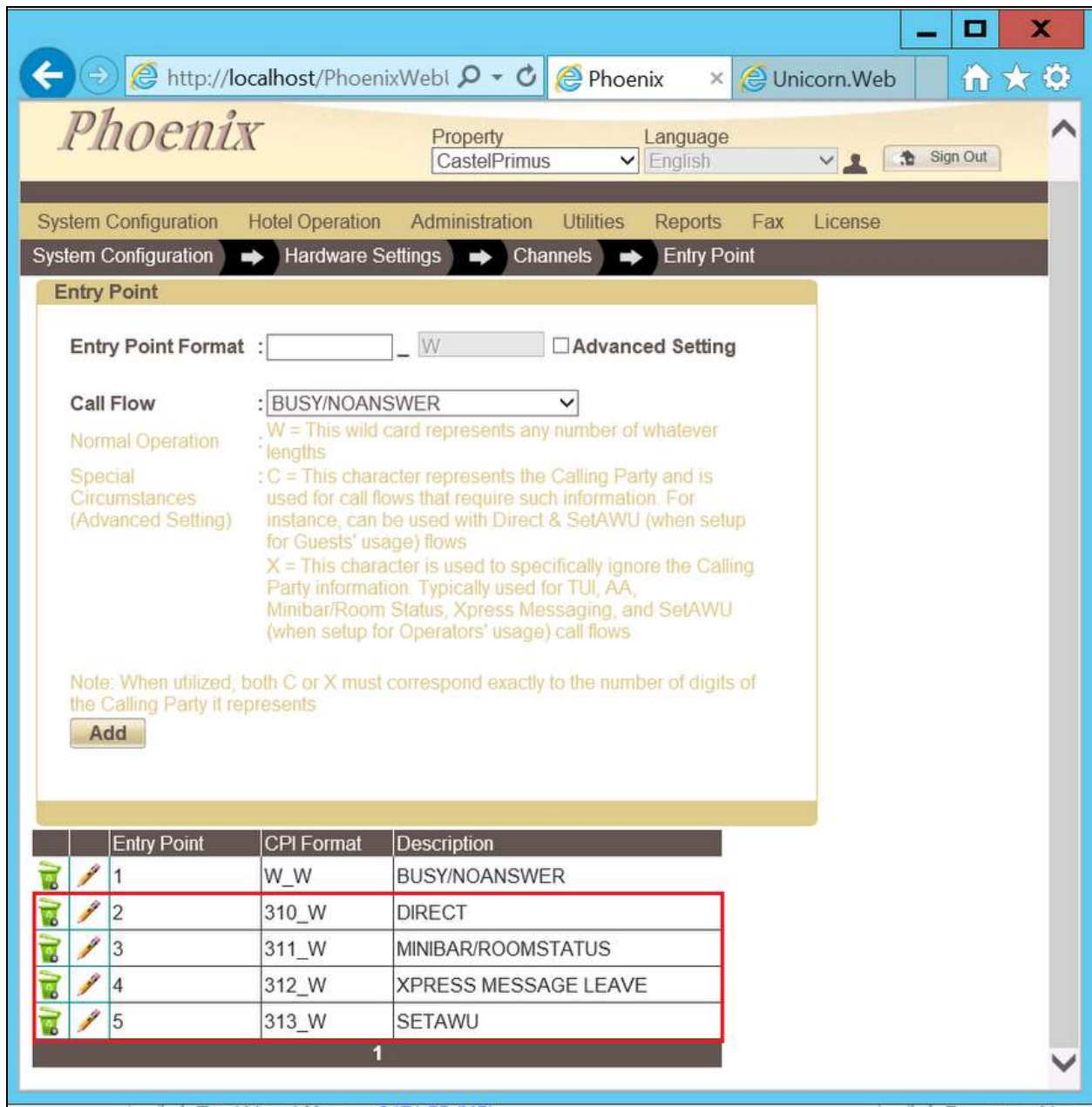
- SIP Registration Name:** Text box containing "AvayaIPO".
- PBX IP:** Text box containing "10.1.30.10".
- Local IP:** Text box containing "10.1.10.125".
- Transport protocol:** Two radio buttons: "TCP" and "UDP" (selected).
- Client Extension:** Text box containing "316@10.1.30.10".
- Contact:** Text box containing "316@10.1.10.125".
- Time Alive:** Text box containing "120".
- Authentication:** Two radio buttons: "Yes" (selected) and "No".
- Identity:** Text box containing "316@10.1.30.10".
- Realm:** Text box containing "ipoffice".
- User Name:** Text box containing "316".
- Password:** Text box containing "\*\*\*\*\*".

At the bottom right, there are two buttons: "Save" and "Reset".

**Note:** The input of the other SIP Users can only be done via the DB at this point in time

#### 6.4.4. Service Numbers

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 5.4**. Create an entry with W\_W mapped to Busy/No Answer Call Flow and one more with the Pilot Number (in this case, that's 310) to Direct. The Entry Points configured are shown at the bottom of the home screen.



**Phoenix** Property: CastelPrimus Language: English Sign Out

System Configuration Hotel Operation Administration Utilities Reports Fax License

System Configuration → Hardware Settings → Channels → Entry Point

**Entry Point**

Entry Point Format :  \_ W ☐ Advanced Setting

Call Flow : BUSY/NOANSWER











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

**Add**

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

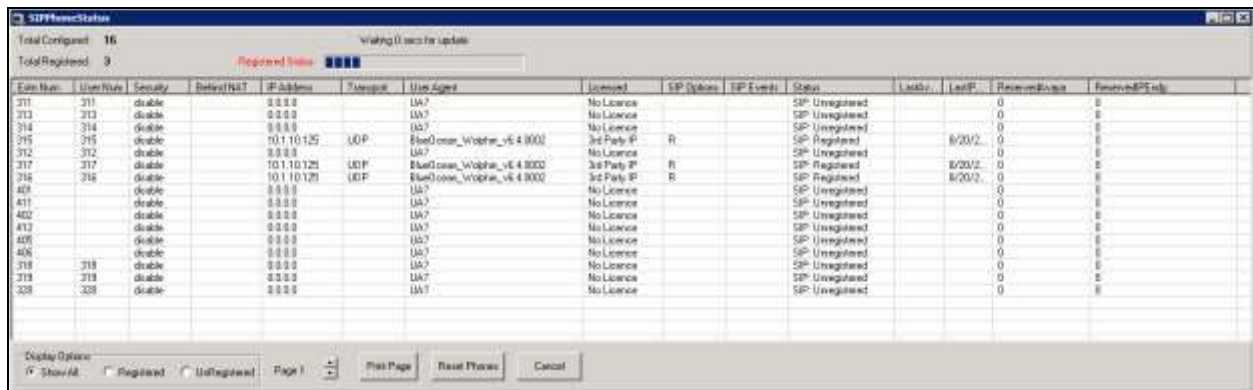
1

## 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. Select **Status → SIP Phone Status** from the top menu. The **SIPPhoneStatus** screen is displayed. Verify that there are entries for the 3 Primary SIP Extensions 315, 316 and 317 from **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: 16' and 'Total Registered: 3'. A progress bar shows 'Registered Status' with 3 bars filled. Below this is a table with columns: Date/Time, User/Name, Security, Referral/NAT, IP Address, Transport, User Agent, License, SIP Options, SIP Events, Status, Load, LastP, Reason/Busy, and Reason/DTMF. The table lists 16 entries. The first three entries (311, 313, 314) are marked as 'Unregistered'. The next three entries (315, 316, 317) are marked as 'Registered'. The remaining nine entries (318, 319, 320, 401, 402, 403, 404, 405, 406) are marked as 'Unregistered'.

Date/Time	User/Name	Security	Referral/NAT	IP Address	Transport	User Agent	License	SIP Options	SIP Events	Status	Load	LastP	Reason/Busy	Reason/DTMF
311	311	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
313	313	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
314	314	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
315	315	disable	10.1.10.125	10.1.10.125	UDP	BlueDome_Woipha_v6.4.0000	3rd Party IP	R		SIP Registered	0	0	0	0
316	316	disable	10.1.10.125	10.1.10.125	UDP	BlueDome_Woipha_v6.4.0000	3rd Party IP	R		SIP Registered	0	0	0	0
317	317	disable	10.1.10.125	10.1.10.125	UDP	BlueDome_Woipha_v6.4.0000	3rd Party IP	R		SIP Registered	0	0	0	0
318	318	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
319	319	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
320	320	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
401	401	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
402	402	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
403	403	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
404	404	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
405	405	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
406	406	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
318	318	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
319	319	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0
320	320	disable	0.0.0.0	0.0.0.0	UDP	UA?	No License			SIP Unregistered	0	0	0	0

### 7.2. Verify TAPI Integration

Place a call to a guest room and leave a voice message or call the express leave message number to leave a voice message directly. Verify that the MWI is turned on for the guest room. Place a call from the guest room to the Hospitality Hunt Group number. Verify that Phoenix recognizes the calling party as a voicemail user. Verify that the voice message can be retrieved and that MWI is turned off after message is reviewed.

### 7.3. Verify Configuration Web Service Integration

Use the Opera Simulator to perform a guest check-in request. Verify from IP Office Manager that the guest name on the phone display or User Full Name and user rights template shown on IP Office Manager User, is updated correctly on IP Office as part of the check-in process.

The screenshot shows the IP Office Manager interface. On the left, a tree view lists various system components, including 'User (53)'. The main pane displays the configuration for 'Ext302: 302'. The 'Full Name' field is highlighted with a red box and contains the text 'Dante Gomez'. Other fields include Name (Ext302), Password (\*\*\*\*\*), Confirm Password (\*\*\*\*\*), Conference PIN, Confirm Conference PIN, Account Status (Enabled), Extension (302), Email Address, Locale, Priority (5), System Phone Rights (Phone), and Profile (Basic User).

The screenshot shows the IP Office Manager interface with the 'Checkin' configuration. The left tree view shows the 'User Rights (16)' section, with 'Checkin' highlighted by a red box. The main pane displays the 'Checkin' configuration, including a table of users with checkboxes. The 'Ext302 302' entry is checked, highlighted with a red box.

Name	Extension
<input type="checkbox"/> 311	311
<input type="checkbox"/> 312	312
<input type="checkbox"/> 313	313
<input type="checkbox"/> 315	315
<input type="checkbox"/> 316	316
<input type="checkbox"/> 317	317
<input type="checkbox"/> Ext301	301
<input checked="" type="checkbox"/> Ext302	302
<input type="checkbox"/> Ext303	303
<input type="checkbox"/> Ext304	304
<input type="checkbox"/> Ext305	305
<input type="checkbox"/> Ext314	314
<input type="checkbox"/> Ext318	318
<input type="checkbox"/> Ext319	319
<input type="checkbox"/> Ext320	320
<input type="checkbox"/> Ext321	321



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:

**Unicorn**  
 Hi, Administrator Language: English sign out change password

Home Posting Reporting Configuration Business Date: 11-Oct-2012 26-Aug-2015 03:00 Auto night audit starts(UWR1)

**Billing**

Data last refreshed: 21:33:56 PM Data will be refreshed every 30 sec.


☒ Auto refresh Refresh

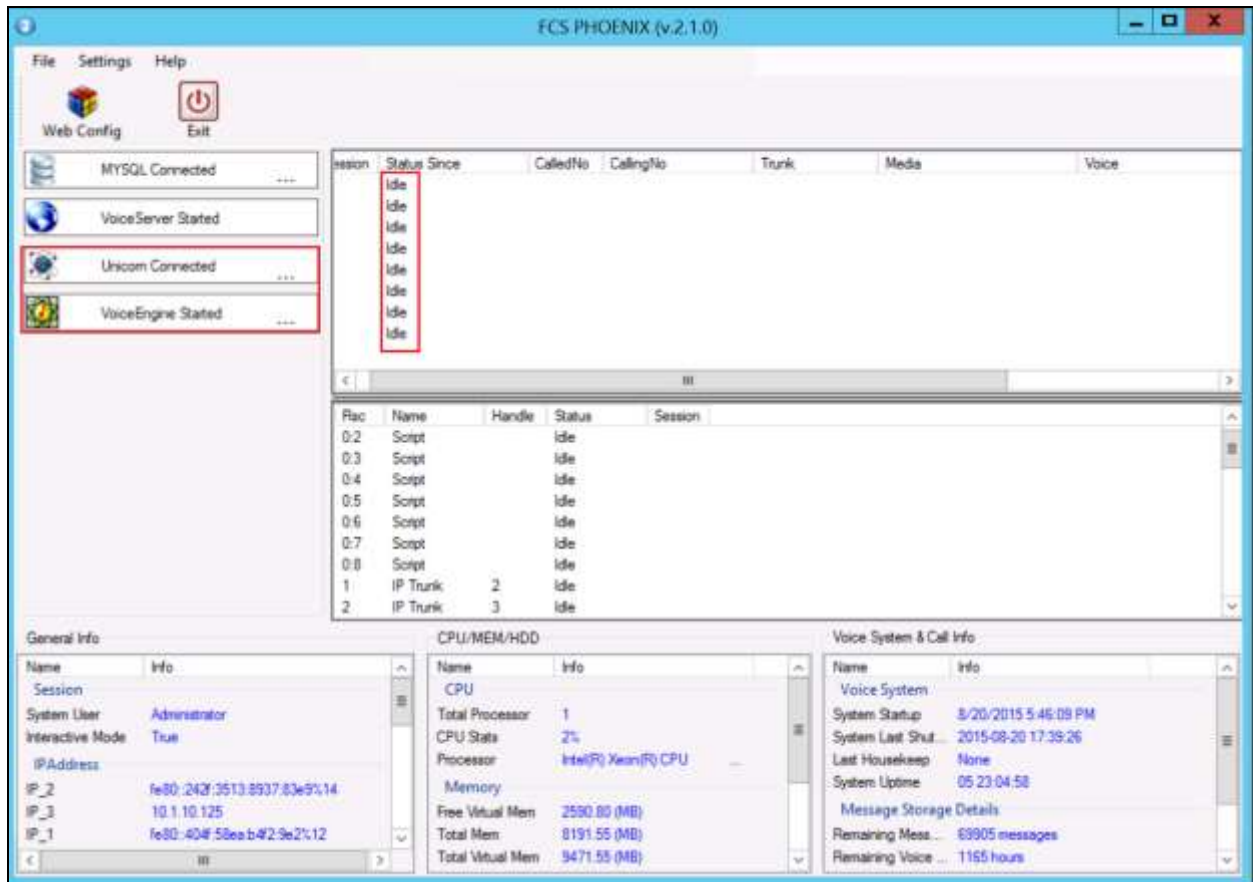
CDR	Account	Date	Time	Description	Duration	Rate 1	Rate 2	Rate 3	Rate 4	Rate 5	Rate 6	Rate 7	Rate 8
CDR1	301	2015/08/19	16:01:21	Internal Call	0s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	16:01:13	Internal Call	0s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:59:25	Internal Call	0s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:59:25	Internal Call	0s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:54:21	Singapore	1s	0.20	0.20	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:53:41	Internal Call	0s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:38:59	Internal Call	13s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:38:23	Singapore	13s	0.20	0.20	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:37:53	Toll Free	15s	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CDR1	301	2015/08/19	15:37:19	Kuala Lumpur	20s	0.20	0.20	0.00	0.00	0.00	0.00	0.00	0.00

Page size: 15 233 items in 16 pages



## 7.5. Verify Phoenix Voicemail Integration

From the FCS Phoenix 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**. Once the Unicorn communication has been successfully established, the Unicorn status will show up as 'Connected'.



The screenshot displays the FCS PHOENIX (v.2.1.0) application interface. The left sidebar contains status indicators: 'MySQL Connected', 'VoiceServer Started', 'Unicorn Connected', and 'VoiceEngine Started' (highlighted with a red box). The main window features a table with columns: 'Session', 'Status Since', 'CalledNo', 'CallingNo', 'Trunk', 'Media', and 'Voice'. The 'Status Since' column shows 'Idle' for multiple sessions. Below this, a table lists sessions with columns: 'Pac', 'Name', 'Handle', 'Status', and 'Session'. The bottom section is divided into three panels: 'General Info' (showing system user, mode, and IP addresses), 'CPU/MEM/HDD' (showing processor, memory, and total virtual memory), and 'Voice System & Call Info' (showing system startup, last shut, last housekeep, system uptime, and message storage details).

Session	Status Since	CalledNo	CallingNo	Trunk	Media	Voice
0:2	Idle					
0:3	Idle					
0:4	Idle					
0:5	Idle					
0:6	Idle					
0:7	Idle					
0:8	Idle					
1	Idle					
2	Idle					

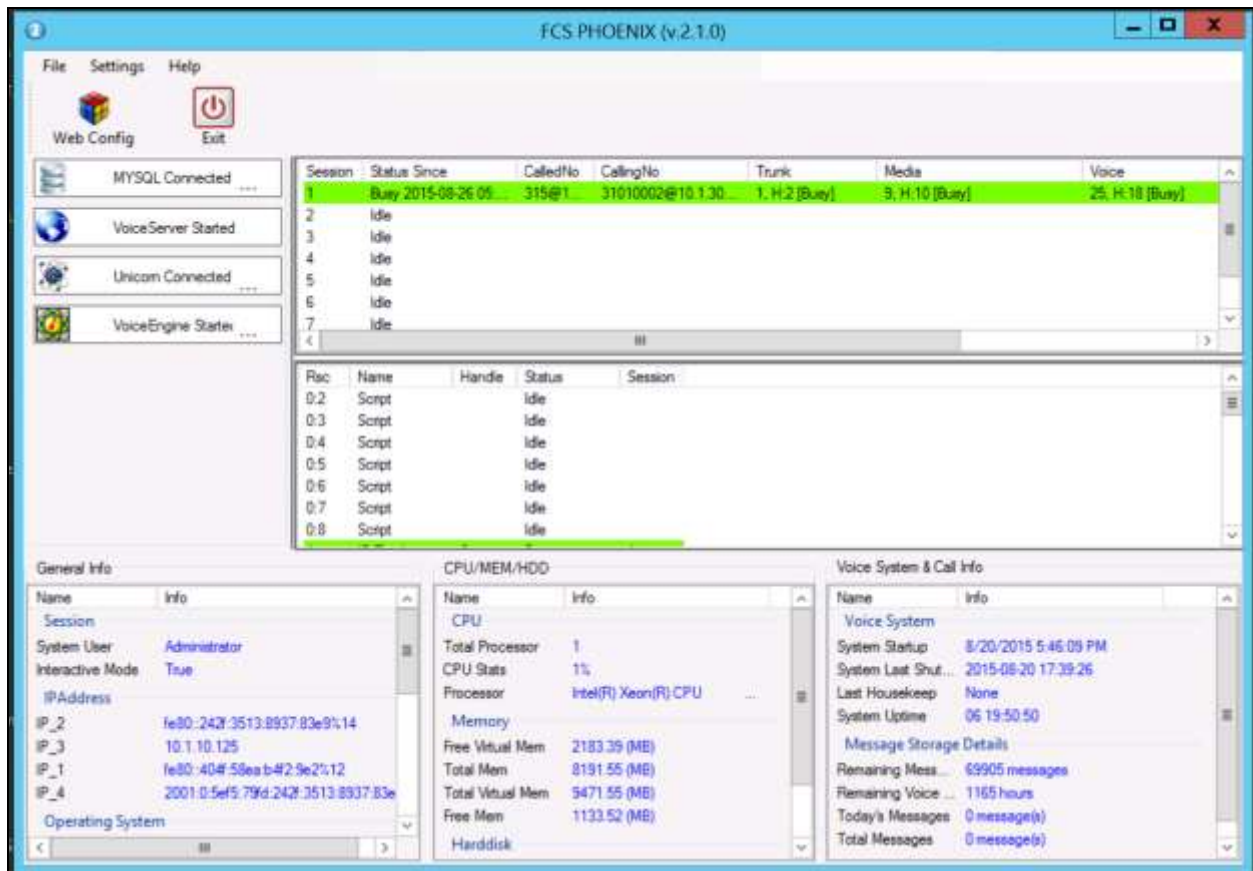
Pac	Name	Handle	Status	Session
0:2	Script		Idle	
0:3	Script		Idle	
0:4	Script		Idle	
0:5	Script		Idle	
0:6	Script		Idle	
0:7	Script		Idle	
0:8	Script		Idle	
1	IP Trunk	2	Idle	
2	IP Trunk	3	Idle	

Name	Info
Session	
System User	Administrator
Interactive Mode	True
IP Address	
IP_2	fe80::243:3513:8937:83e9%14
IP_3	10.1.10.125
IP_1	fe80::404f:58ea:b4f2:9e2%12

Name	Info
CPU	
Total Processor	1
CPU State	2%
Processor	Intel(R) Xeon(R) CPU
Memory	
Free Virtual Mem	2590.80 (MB)
Total Mem	8191.55 (MB)
Total Virtual Mem	9471.55 (MB)

Name	Info
Voice System	
System Startup	8/20/2015 5:46:08 PM
System Last Shut	2015-08-20 17:39:26
Last Housekeep	None
System Uptime	05:23:04:58
Message Storage Details	
Remaining Mess...	69905 messages
Remaining Voice ...	1165 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 DTMF digit '0' 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 R9.1. All feature 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 9.1 Documentation Library*, Apr 2015, available at <http://support.avaya.com>

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

---

**©2015 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](mailto:devconnect@avaya.com).