



Avaya Solution & Interoperability Test Lab

Application Notes for FCS WinExpress 3.1.2 with Avaya IP Office 11.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for FCS WinExpress 3.1.2 to interoperate with Avaya IP Office Release 11.1. FCS 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 two main components, FCS Voice and FCS Gateway, which includes call billing and interface solution. In the compliance testing, FCS WinExpress used SIP Users, Short Codes, SMDR, and Configuration Web Service interfaces from Avaya IP Office Server Edition 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 particular attention to the scope of testing as outlined in **Section 2.1**, as well as 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 FCS WinExpress 3.1.2 to interoperate with Avaya IP Office 11.1. FCS 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 two main components, FCS Voice (Voice) and FCS Gateway (Gateway), which includes calls billing and interface solution. In the compliance testing, FCS 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 minibar posting, call billing, name and user profile template change, and Do Not Disturb features.

In the compliance testing, voice lines register as SIP users on Avaya IP Office Server Edition for voicemail 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 no answer within the specified time. Each voicemail line will forward to another voicemail line in a round-robin fashion until one is available.

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

The FCS Gateway component was used in the compliance testing to initiate the room Check-In, Check-Out, and Move requests on FCS WinExpress. In the compliance testing, multiple rights templates were set up on Avaya IP Office Server Edition for use with Check-In and Check-Out guests. FCS Gateway uses the Configuration Web Service to send updates to Avaya IP Office Server Edition 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 FCS 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. FCS Gateway (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 FCS WinExpress call billing reports were verified. The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to FCS WinExpress, and rebooting Avaya IP Office Server Edition and the FCS 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 these Application Notes, the interface between Avaya systems and the FCS WinExpress did not include use of any specific encryption features as requested by FCS.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following on FCS 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 Gateway)

- 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 Gateway
- Capture calls made from room phones for the purpose of call billing

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

2.2. Test Results

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

- An issue was encountered during the initial testing where a checked-in extension (from FCS Gateway) will result in the deletion of all extensions' login codes in IP Office including the SIP Registrar Domain Name. FCS implemented a fix which resolved the issue.
- Check-in/Check-out for IPO Expansion Users can take up to one minute.
- Move room from IP Office Expansion User to IP Office Primary User and vice versa is not supported.

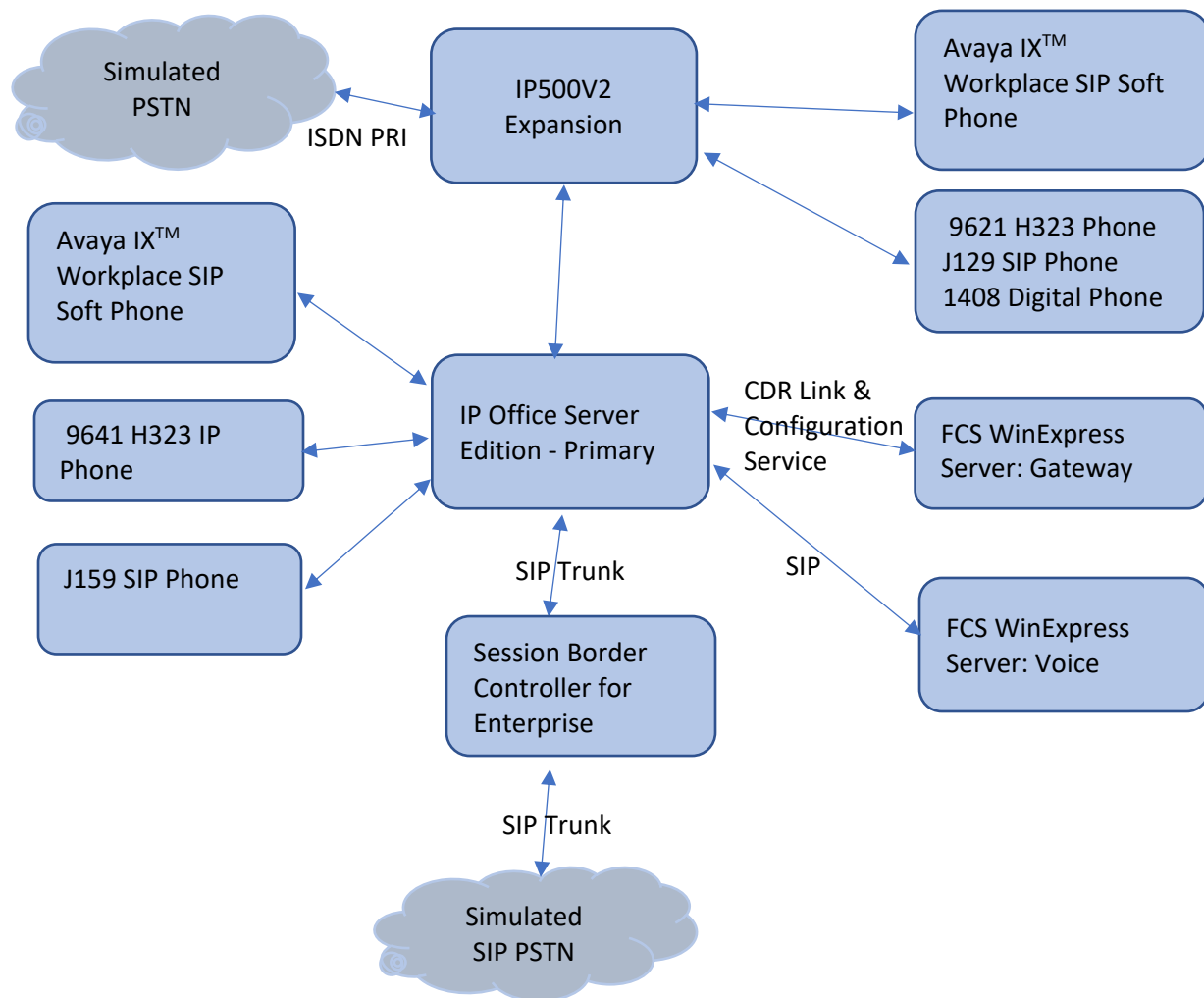
2.3. Support

Technical support on FCS WinExpress can be obtained through the following:

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

3. Reference Configuration

The configuration used for the compliance testing is shown below. In the compliance testing, FCS WinExpress was installed on a single server. FCS Gateway initiates room Check-In/Check-Out and room move via a PMS Simulator, capture SMDR, and to set Do Not Disturb. FCS Voice handles the voicemail reception, recording and playback, message waiting lamps, wake-up calls as well as room status and mini-bar posting and reporting. In this compliance testing, Avaya IP Office was comprised of a Primary Server and an Expansion Module (IP500 V2). Avaya IP Deskphones H.323 96x1, Avaya IP Deskphones SIP 96x1/J129/J159, Avaya Digital Deskphones 1408 as well as Avaya IX™ Workplace SIP Softphone are deployed as guest room, front desk, operator and admin phones.



Note: There is only 1 FCS WinExpress Server

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition (Primary)	11.1.0.0.0 build 237
Avaya IP Office 500 V2 (Expansion)	11.1.0.0.0 build 237
Avaya IP Office Manager	11.1.0.0.0 build 237
Avaya 9608G & 9641G IP Deskphone (H.323)	6.8
Avaya IX Workplace	3.8.4.10.2
Avaya 9641 & 9621 IP Deskphone (SIP)	7.1.9
Avaya J129 & J159 IP Deskphone (SIP)	4.0.5
Avaya IP Office Configuration Web Service SDK	10.1
WinExpress Server - FCS Gateway & Voice running on Microsoft Windows 2012 R2 SP1 hosted on VMware 6.7 Platform	3.1.2

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

5. Configure Avaya IP Office

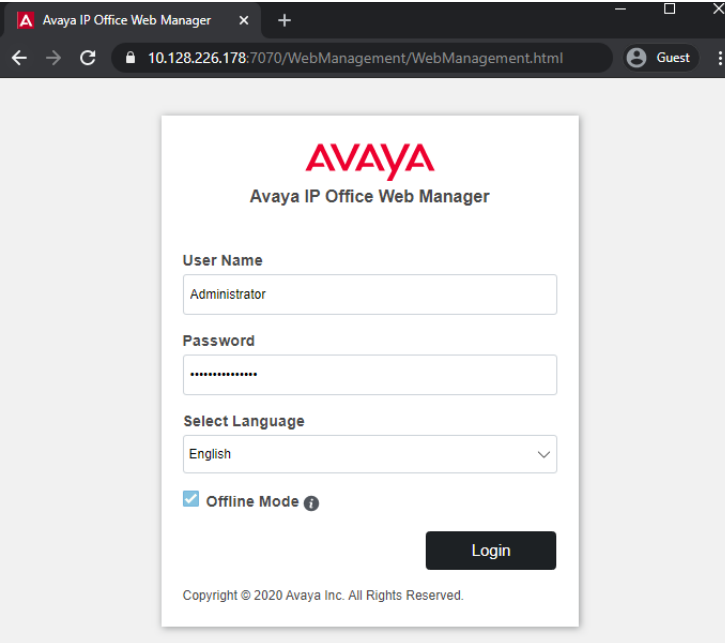
This section provides the procedures for configuring Avaya IP Office. The procedures include the following:

- 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

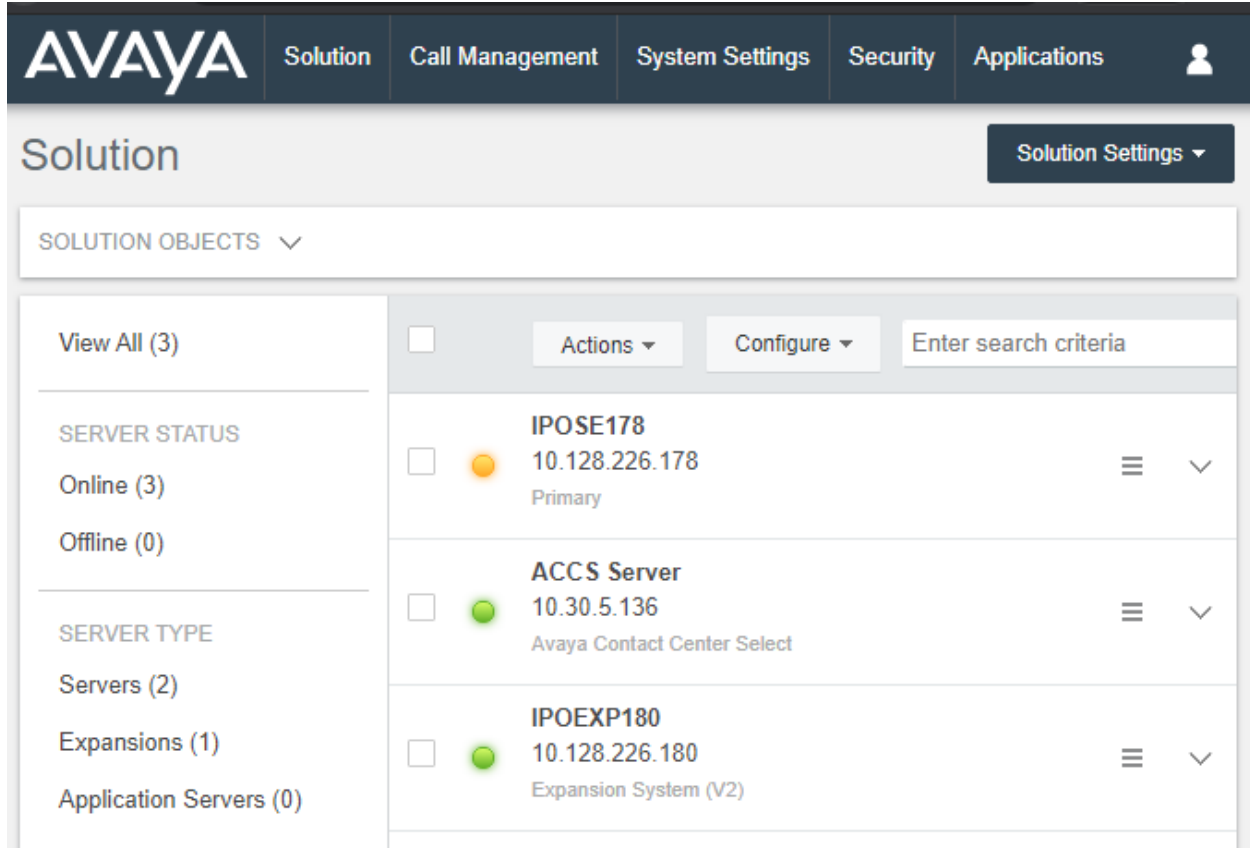
5.1. Launch Avaya IP Office Web Manager

Access 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.

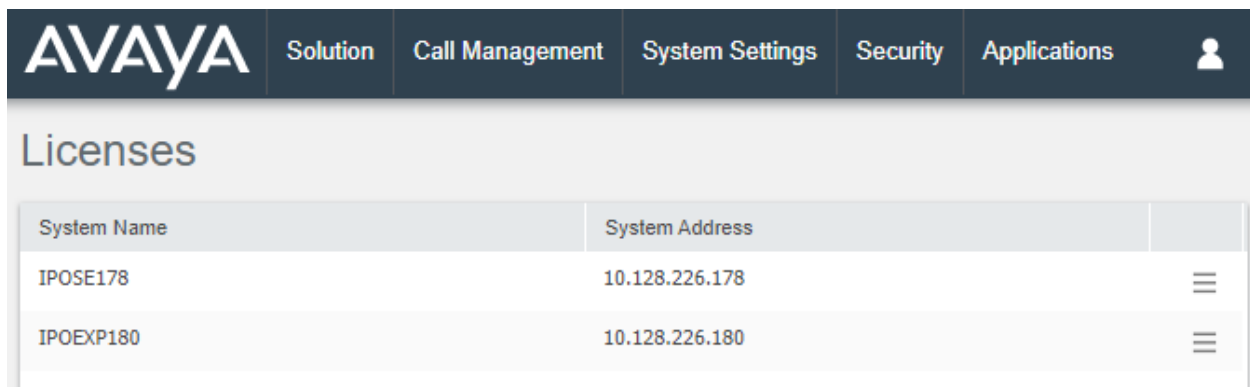


The Avaya Solution home screen features a dark blue header with the Avaya logo and navigation tabs: Solution, Call Management, System Settings, Security, and Applications. A user icon is in the top right. Below the header, the 'Solution' section includes a 'Solution Objects' dropdown and a 'Solution Settings' button. The main content area has a left sidebar with filters: 'View All (3)', 'SERVER STATUS' (Online (3), Offline (0)), and 'SERVER TYPE' (Servers (2), Expansions (1), Application Servers (0)). The main table lists three objects: IPOSE178 (Primary, 10.128.226.178, orange status), ACCS Server (Avaya Contact Center Select, 10.30.5.136, green status), and IPOEXP180 (Expansion System (V2), 10.128.226.180, green status). Each row has a checkbox, a status indicator, and menu icons.

View All (3)	<input type="checkbox"/>	Actions ▾	Configure ▾	Enter search criteria
SERVER STATUS	<input type="checkbox"/>			
Online (3)	<input type="checkbox"/>		IPOSE178 10.128.226.178 Primary	≡ ▾
Offline (0)	<input type="checkbox"/>		ACCS Server 10.30.5.136 Avaya Contact Center Select	≡ ▾
SERVER TYPE	<input type="checkbox"/>		IPOEXP180 10.128.226.180 Expansion System (V2)	≡ ▾
Servers (2)				
Expansions (1)				
Application Servers (0)				

5.2. Verify Avaya IP Office Server License

From the home screen, select **System Settings** → **Licenses**. Select the **Primary Server (IPOSE178)** where the SIP user will be administered.



The Avaya Licenses screen has a dark blue header with the Avaya logo and navigation tabs: Solution, Call Management, System Settings, Security, and Applications. A user icon is in the top right. Below the header, the 'Licenses' section contains a table with two columns: 'System Name' and 'System Address'. The table lists two systems: IPOSE178 (10.128.226.178) and IPOEXP180 (10.128.226.180). Each row has a menu icon in the third column.

System Name	System Address	
IPOSE178	10.128.226.178	≡
IPOEXP180	10.128.226.180	≡

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 FCS Voice to register to IP Office as SIP Users.

Solution
Call Management
System Settings
Security
Applications

License | IPOSE178

Manage Licenses
Manage Solution-Wide Licenses

Remote Server
Configure License Server

License Mode
License Normal

Licensed Version
11.0

PLDS Host ID
602060891596

PLDS File Status
Valid

Feature	Instances	Status	Expiry ...	Source
Avaya Mac Softphone	384	Valid	Never	PLDS No...
Office Worker	384	Valid	Never	PLDS No...
UMS Web Services	384	Valid	Never	PLDS No...
Power User	384	Valid	Never	PLDS No...
Allow Virtualization	1	Valid	Never	PLDS No...
3rd Party IP Endpoints	384	Valid	Never	PLDS No...
Essential Edition	384	Obsolete	Never	PLDS No...
VMPro TTS Professional	384	Valid	Never	PLDS No...
Voice Networking Chann...	384	Obsolete	Never	PLDS No...
Web Collaboration	384	Valid	Never	PLDS No...

Displaying 1 - 33 of 33

Cancel

5.2.1. Obtain LAN IP Address

From the home screen, select **System Settings** → **System** → **IPOSE178** → **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 displays the Avaya System Configuration web interface for the IPOSE178 system. The top navigation bar includes the Avaya logo and tabs for Solution, Call Management, System Settings, Security, and Applications. The main header shows 'System Configuration | IPOSE178'. On the left, a sidebar lists various system components, with 'LAN1' selected. The main content area is divided into three tabs: 'LAN Settings', 'VoIP', and 'Network Topology'. Under the 'LAN Settings' tab, the following configuration fields are visible: 'IP Address' set to 10.128.226.178, 'IP Subnet Mask' set to 255.255.255.192, 'Number Of DHCP IP Addresses' set to 12, 'DHCP Mode' set to Disabled, and an 'Advanced' section with a 'NO' button.

System	LAN Settings	VoIP	Network Topology
System	IP Address		
	10 . 128 . 226 . 178		
VoiceMail	IP Subnet Mask		
	255 . 255 . 255 . 192		
System Events	Number Of DHCP IP Addresses		
	12		
SMTP	DHCP Mode		
	Disabled		
DNS	Advanced		
	NO		
SMDR			
LAN1			
LAN2			
VoIP			
Directory Services			
Telephony			

Similarly, for Expansion server, select **System Settings** → **System** → **IPOEXP180** → **LAN1**.
Note the same for the Expansion Server **IPOEXP180**.

The screenshot displays the Avaya System Configuration web interface. At the top, a dark navigation bar contains the Avaya logo and tabs for Solution, Call Management, System Settings, Security, and Applications. Below this, the page title is "System Configuration | IPOEXP180". On the left, a sidebar lists various system components: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (highlighted with a blue border), LAN2, and VoIP. The main content area is titled "LAN Settings" and includes sub-tabs for LAN Settings, VoIP, and Network Topology. Under the "LAN Settings" tab, the following fields are visible: IP Address (10 . 128 . 226 . 180), IP Subnet Mask (255 . 255 . 255 . 192), Primary Transfer IP Address (0 . 0 . 0 . 0), and RIP Mode (set to None with a dropdown arrow). A partially visible "Enable NAT" checkbox is at the bottom.

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 → IPOSE178 → LAN → 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 Voice. Leave the rest as default. Click **Update** at bottom of screen (not shown) to save.

The screenshot displays the Avaya System Configuration interface for the IPOSE178 system. The top navigation bar includes the Avaya logo and tabs for Solution, Call Management, System Settings, Security, and Applications. The left sidebar lists various system components, with LAN1 selected under the System category. The main content area is titled 'System Configuration | IPOSE178' and shows the 'SIP REGISTRAR' settings. The 'SIP REGISTRAR' section includes a 'YES' toggle for 'SIP Registrar Enable', a 'YES' toggle for 'SIP Remote Extension Enable', and a dropdown menu for 'Allowed SIP User Agents' set to 'Block blacklist only'. Below these are text input fields for 'Auto-create Extension/User' (set to 'NO'), 'SIP Domain Name' (set to 'ipodevconnect.com'), and 'SIP Registrar FQDN' (set to 'ipose178.hcm.com'). A 'Challenge Expiry Time (sec)' dropdown is set to '10'. The 'LAYER 4 PROTOCOL' section includes 'UDP' and 'TCP' toggles, both set to 'YES', and 'TLS' set to 'YES'. The 'UDP Port' is set to '5060', 'Remote UDP Port' to '5060', 'TCP Port' to '5060', 'Remote TCP Port' to '5060', and 'TLS Port' to '5061'.

Section	Setting	Value
SIP REGISTRAR	SIP Registrar Enable	YES
	SIP Remote Extension Enable	YES
	Allowed SIP User Agents	Block blacklist only
	Auto-create Extension/User	NO
	Challenge Expiry Time (sec)	10
LAYER 4 PROTOCOL	UDP	YES
	TCP	YES
	TLS	YES
	UDP Port	5060
	Remote UDP Port	5060
	TCP Port	5060
	Remote TCP Port	5060

5.4. Administer SIP Extensions

In the compliance testing, the following SIP extensions with base extensions of **1004-1006** and **1001-1003** were created. FCS Voice used the called-party number **1004-1006** for various hospitality features. Voice registered as extensions **1001-1003** to function as Voicemail ports.

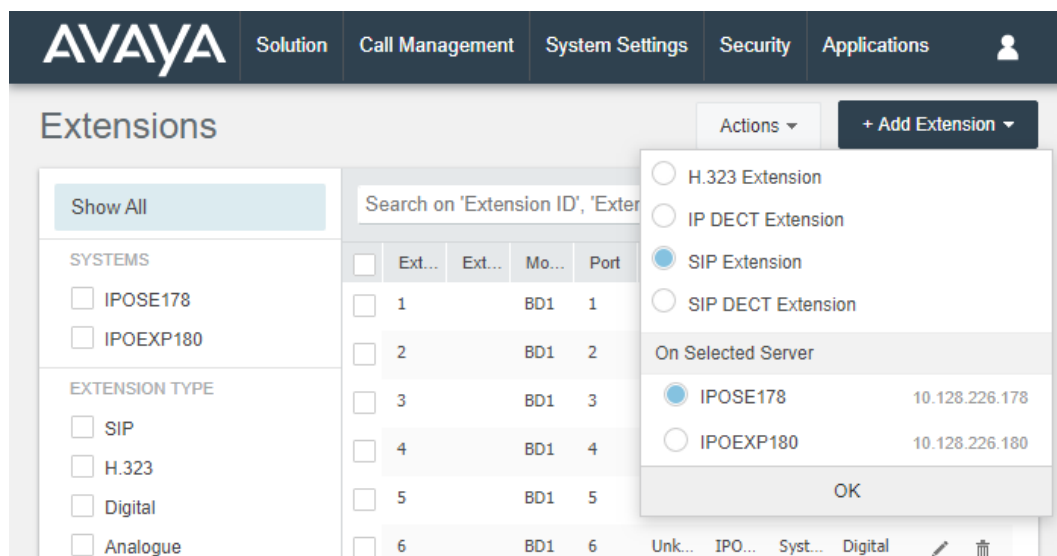
Note: Customer needs to purchase sufficient SIP ports to provide for the voicemail lines and services.

FCS Voice 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.

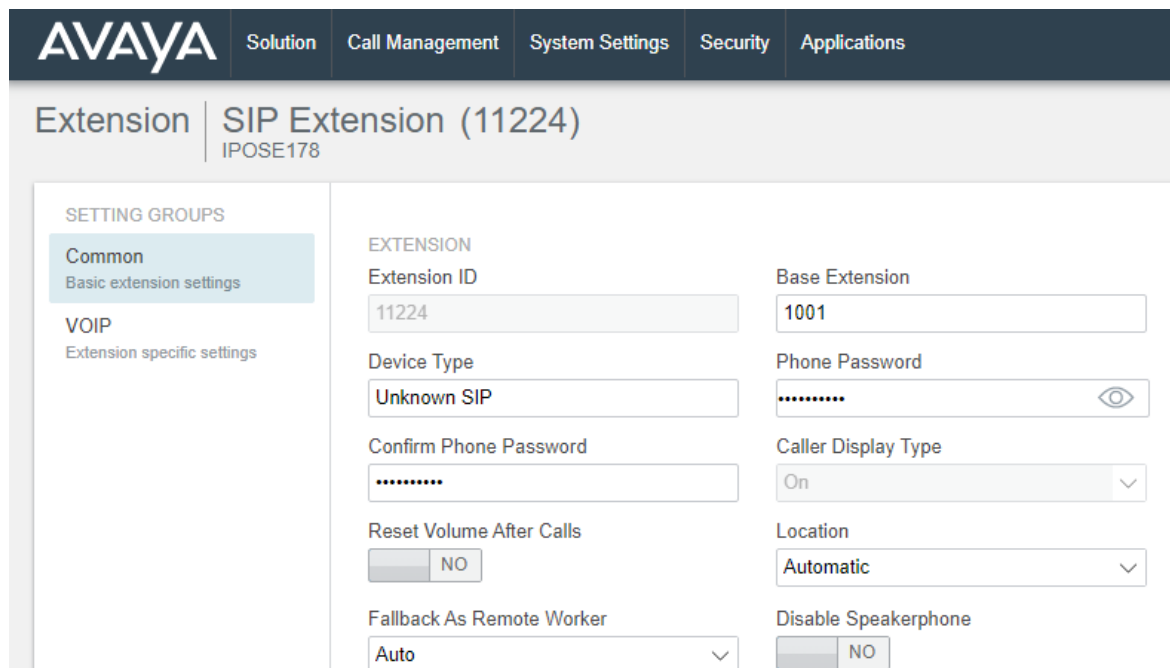
SIP Extension	Usage
1001, 1002 & 1003	FCS Voice registers to these extension for receiving voicemail calls
1004	Post mini-bar/room status
1005	Express leave voice message
1006	Set wakeup call

Note: The above services tied to the numbers (1004-1006) are merely a sample configuration

From the home screen, select **Call Management** → **Extensions**. Click on **+Add Extension** and check **SIP Extension**, **IPOSE178**, and click **OK** to add a new SIP extension.



Enter the desired digits for **Base Extension** and **Phone Password** as well as **Confirm Phone Password**, as shown below.



AVAYA | Solution | Call Management | System Settings | Security | Applications

Extension | SIP Extension (11224)
IPOSE178

SETTING GROUPS

- Common
Basic extension settings
- VOIP
Extension specific settings

EXTENSION

Extension ID: 11224


Device Type: Unknown SIP

Confirm Phone Password:

Reset Volume After Calls: ☐ NO

Fallback As Remote Worker: Auto

Base Extension: 1001

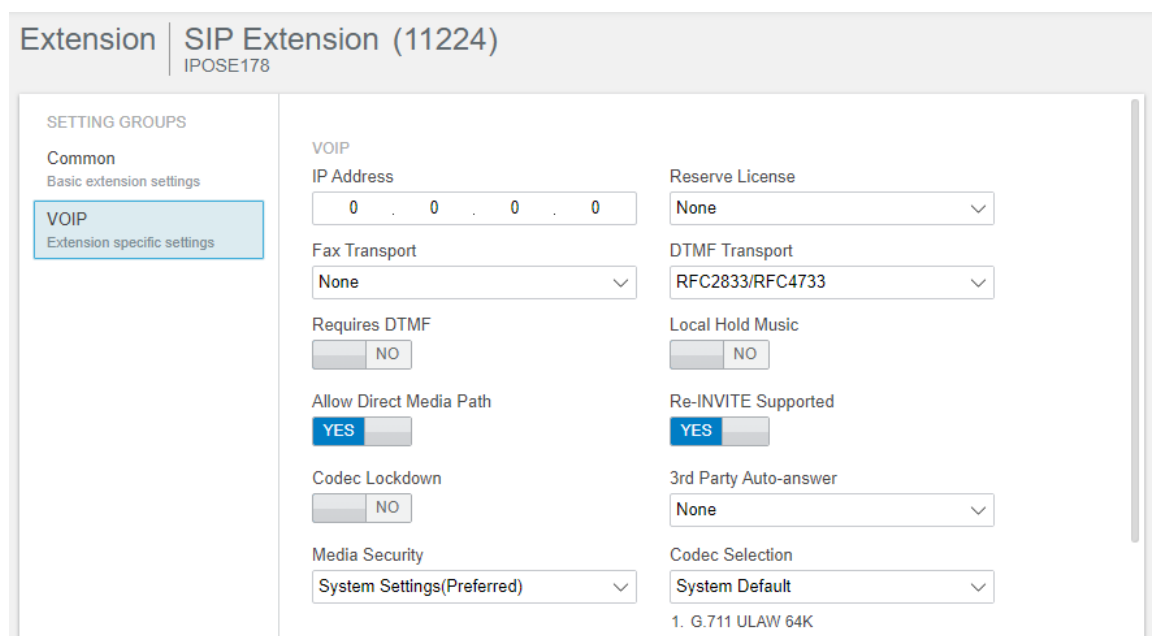
Phone Password: 

Caller Display Type: On

Location: Automatic

Disable Speakerphone: ☐ NO

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



Extension | SIP Extension (11224)
IPOSE178

SETTING GROUPS

- Common
Basic extension settings
- VOIP
Extension specific settings

VOIP

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

Codec Lockdown: ☐ NO

3rd Party Auto-answer: None

Media Security: System Settings(Preferred)

Codec Selection: System Default

1. G.711 ULAW 64K

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 **1001**, **1002** and **1003** are for receiving calls and the secondary SIP users **1004**, **1005** and **1006** are to forward calls to primary SIP users.

	Name	Full N...	Exten...	Hunt ...	Voice...	Email...	Pass...	Voice...	Login...	Syste...	
<input type="checkbox"/>	5501	Extn5...	5501	SE Gr...	On		*****	*****	IPOSE...		
<input type="checkbox"/>	ACCS...	ACCS...	5555		On		*****	*****	IPOSE...		
<input type="checkbox"/>	Agent...	sampl...	6001		On		*****		IPOSE...		
<input type="checkbox"/>	Agent...	sampl...	6002		On		*****		IPOSE...		
<input type="checkbox"/>	Agent...	sampl...	6003		On		*****		IPOSE...		
<input type="checkbox"/>	Agent...	sampl...	6004		On		*****		IPOSE...		

5.5.1. Administer Primary SIP Users

Click on **+Add User**, check **IPOEXP180**, and click **OK** to add a new User.

On Selected Server

- ☒ IPOSE178 10.128.226.178
- ☐ IPOEXP180 10.128.226.180

OK

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 Voice to log in as the SIP User. Voice registers using this primary SIP User to receive calls.

The screenshot shows the Avaya User Management console. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security', and 'Applications'. The 'User' tab is selected in the left sidebar. The main form is titled 'NewUser' and is for 'IPOSE178'. The form contains the following fields:

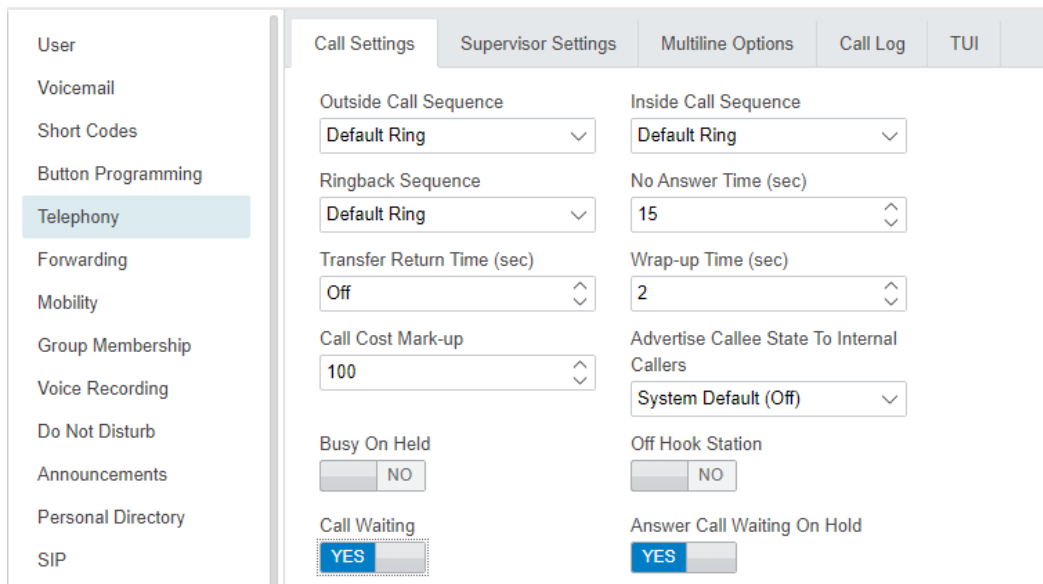
- Name: VM1
- Full Name: WinExpress VM1
- Password: [Redacted]
- Confirm Password: [Redacted]
- Unique Identity: [Redacted]
- Extension: 1001 (dropdown)
- Account Status: Enabled (dropdown)
- Profile: Essential User (dropdown)
- Locale: Select... (dropdown)
- Priority: 5 (dropdown)
- Login Code: [Redacted]
- Confirm Login Code: [Redacted]

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 Management console with the 'Voicemail' tab selected in the left sidebar. The main form is titled 'NewUser' and is for 'IPOSE178'. The form contains the following fields:

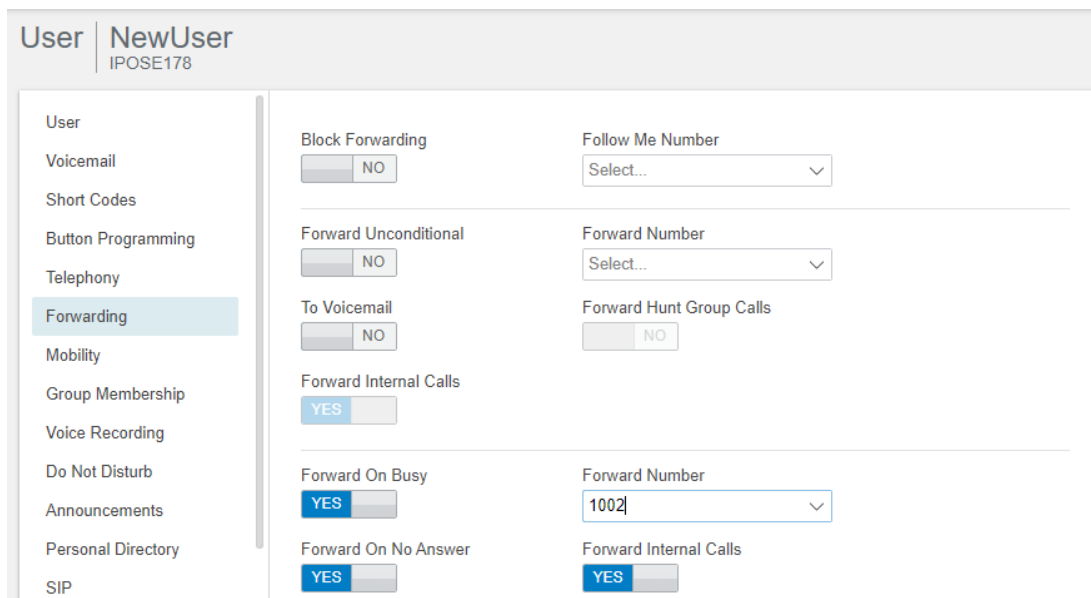
- Voicemail Code: [Redacted]
- Confirm Voicemail Code: [Redacted]
- Voicemail Email: [Redacted]
- Voicemail Email Mode: Off (dropdown)
- Voicemail On: NO (radio button)
- Voicemail Help: NO (radio button)

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



Call Settings	Supervisor Settings	Multiline Options	Call Log	TUI
Outside Call Sequence	Inside Call Sequence			
Default Ring	Default Ring			
Ringback Sequence	No Answer Time (sec)			
Default Ring	15			
Transfer Return Time (sec)	Wrap-up Time (sec)			
Off	2			
Call Cost Mark-up	Advertise Callee State To Internal Callers			
100	System Default (Off)			
Busy On Held	Off Hook Station			
NO	NO			
Call Waiting	Answer Call Waiting On Hold			
YES	YES			

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. 1002. The last primary SIP User will forward back to the first Voicemail Hunt Group member i.e. 1001. Click **Create** to save (not shown).



User	NewUser
IPOSE178	
User	Block Forwarding
Voicemail	NO
Short Codes	Follow Me Number
Button Programming	Select...
Telephony	Forward Unconditional
Forwarding	NO
Mobility	Forward Number
Group Membership	Select...
Voice Recording	To Voicemail
Do Not Disturb	NO
Announcements	Forward Hunt Group Calls
Personal Directory	NO
SIP	Forward Internal Calls
	YES
	Forward On Busy
	YES
	Forward Number
	1002
	Forward On No Answer
	YES
	Forward Internal Calls
	YES

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 “1004”.

The screenshot shows the Avaya User Management console. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security', and 'Applications'. The left sidebar lists various user settings, with 'User' selected. The main area contains the following fields:

- Name: NewUser
- Full Name: MiniBar and Room Status
- Password: *****
- Confirm Password: *****
- Unique Identity: (empty)
- Extension: 1004
- Account Status: Enabled
- Profile: Essential User
- Locale: Select...
- Priority: 5
- Login Code: *****
- Confirm Login Code: *****

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 “1000” (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 console. The left sidebar lists various user settings, with 'Forwarding' selected. The main area contains the following fields:

- Block Forwarding: NO
- Follow Me Number: Select...
- Forward Unconditional: YES
- Forward Number: Select...
- To Voicemail: NO
- Forward Hunt Group Calls: NO
- Forward Internal Calls: YES
- Forward On Busy: NO
- Forward Number: 1000
- Forward On No Answer: NO
- 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 1004-1006 were created.

5.6. Administer Hospitality Hunt Group

From the home screen, select **Call Management** → **Groups**. Click on **+Add Group** and check **IPOEXP180** and click **OK** to add a new hunt group.



This hunt group will be used to deliver calls to Voice 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 5.5.1**.

The screenshot shows the 'Group' configuration page for group 'IPOSE178'. The left sidebar lists 'Group Settings' with sub-items: Group, Queuing, Overflow, Fallback, Voicemail, Voice Recording, Announcements, and SIP. The main area contains fields for Name (WinVoice), Extension (1000), Ring Mode (Sequential), Hold Music Source (No Change), and Agent's Status on No-Answer Applies To (None). A 'Select Members' dialog is open, showing a list of users with checkboxes. VM1, VM2, and VM3 are selected. The dialog also includes 'Select All Users', 'OK', and 'Cancel' buttons. Below the dialog, there are buttons for '- Remove Users' and '+ Add Users'.

Membership	Extension	Name	System Name
<input checked="" type="checkbox"/>			

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

The screenshot shows the 'Group' configuration page after the members have been added. The 'USER LIST (3/3)' table now contains three entries: VM1 (1001), VM2 (1002), and VM3 (1003), all with 'YES' in the Membership column. The 'Group' configuration fields remain the same as in the previous screenshot.

Membership	Extension	Name	System Name
<input checked="" type="checkbox"/>	1001	VM1	IPOSE178
<input checked="" type="checkbox"/>	1002	VM2	IPOSE178
<input checked="" type="checkbox"/>	1003	VM3	IPOSE178

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

The screenshot shows the 'Group Settings' page for group 'IPOSE178'. The left sidebar lists 'Group Settings', 'Group', 'Queuing', 'Overflow', and 'Fallback'. The main content area is for 'Voicemail' configuration. It includes a 'Voicemail On' toggle set to 'NO', a 'Voicemail Answer Time (sec)' dropdown set to '45', a 'Voicemail Code' text field containing '*****', and a 'Confirm Voicemail Code' text field containing '*****'.

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 'Group Settings' page for group 'IPOSE178'. The left sidebar lists 'Group Settings', 'Group', 'Queuing' (highlighted), 'Overflow', 'Fallback', 'Voicemail', 'Voice Recording', 'Announcements', and 'SIP'. The main content area is for 'Queuing' configuration. It includes a 'Queuing On' toggle set to 'NO', a 'Queue Type' dropdown set to 'Assign Call On Agent Answer', a 'Queue Length' dropdown set to 'No Limit', a 'Normalize Queue Length' toggle set to 'YES', a 'CALLS IN QUEUE ALARM' section with a 'Calls In Queue Threshold' dropdown set to '1', and an 'Analog Extension to Notify' dropdown 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 Gateway will update the guest name through IP Office Configuration Web Services regardless.

AVAYA Solution Call Management System Settings Security Applications

User Room 1-1 (1011)
IPOSE178

User

Voicemail

Short Codes

Button Programming

Telephony

Forwarding

Mobility

Group Membership

Voice Recording

Do Not Disturb

Announcements

Personal Directory

SIP

Name: Room 1-1

Full Name: Extn1011

Password: *****

Unique Identity:

Extension: 1011

Account Status: Enabled

Profile: Essential User

Locale: Select...

Priority: 5

Login Code: *****

Confirm Login Code: *****

Audio Conference PIN:

Confirm Audio Conference PIN:

System Phone Rights: None

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.

AVAYA Solution Call Management System Settings Security Applications

User Room 1-1 (1011)
IPOSE178

User

Voicemail

Short Codes

Button Programming

Telephony

Forwarding

Mobility

Group Membership

Voice Recording

Voicemail Code: *****

Confirm Voicemail Code: *****

Voicemail Email:

Voicemail Email Mode: Off

Voicemail On: NO

Voicemail Ringback: NO

Voicemail Email Reading: NO

UMS Web Services: NO

Enable GMAIL API: NO

Exception/Breakout (DMTF):

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 Management interface for a user named 'Room 1-1 (1011)' with ID 'IPOSE178'. The left sidebar contains a list of settings: User, Voicemail, Short Codes, Button Programming, Telephony, Forwarding (highlighted), Mobility, Group Membership, Voice Recording, Do Not Disturb, Announcements, Personal Directory, and SIP. The main content area displays the 'Forwarding' settings for this user. The settings are organized into sections with toggle switches and dropdown menus. The 'Forwarding' section is active, showing options for 'Block Forwarding' (set to NO), 'Follow Me Number' (set to Select...), 'Forward Unconditional' (set to NO), 'Forward Number' (set to Select...), 'To Voicemail' (set to NO), 'Forward Hunt Group Calls' (set to NO), 'Forward Internal Calls' (set to YES), 'Forward On Busy' (set to YES), 'Forward Number' (set to 1001), 'Forward On No Answer' (set to YES), and 'Forward Internal Calls' (set to YES).

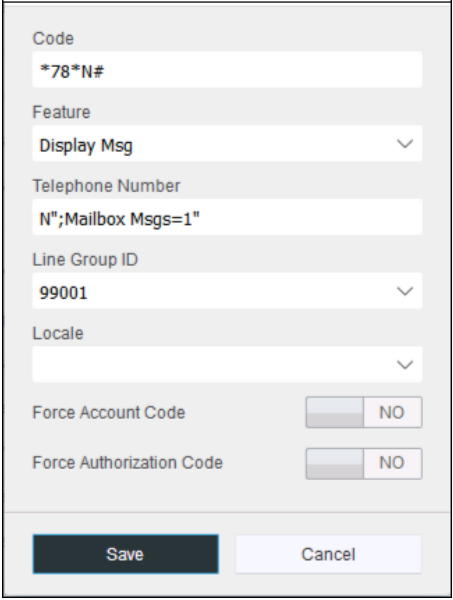
Repeat this section for all users using Voice for voicemail, including all guest rooms, front desk, and administrative staff. In the compliance testing, the voicemail users consisted of one front desk with extension “1005”, admin phone with extension “1010” and guest rooms with extensions “1011, 1012, 1031, 1032, 1061 and 1062”, 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 (selected from a dropdown menu)
- Telephone Number:** N"; Mailbox Msgs=1"
- Line Group ID:** 99001 (selected from a dropdown menu)
- Locale:** (empty dropdown menu)
- Force Account Code:** NO (toggle switch)
- Force Authorization Code:** NO (toggle switch)
- Buttons:** Save and 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"**

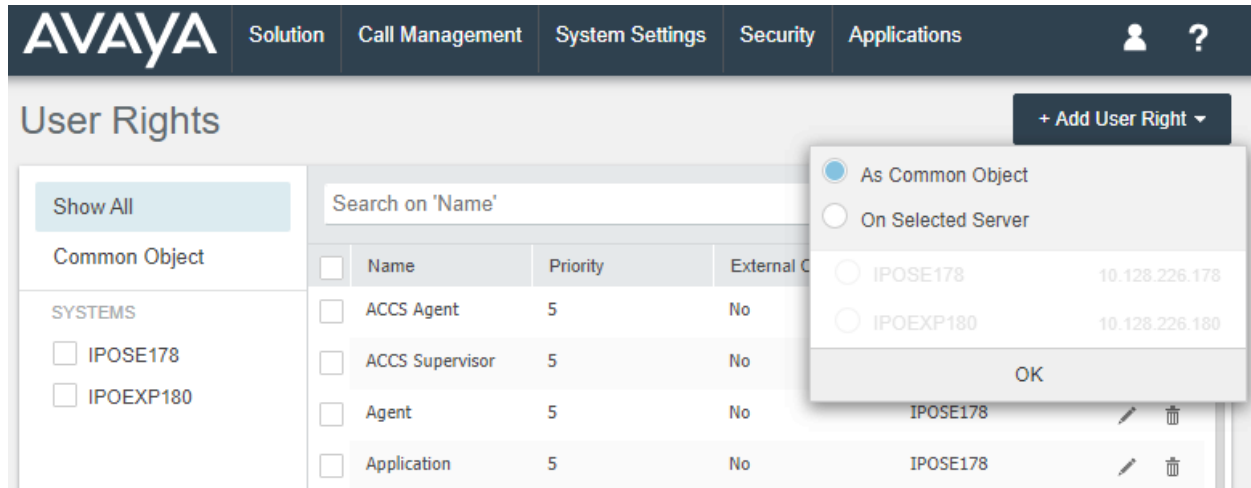
Leave the rest as default and click **Save**.

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

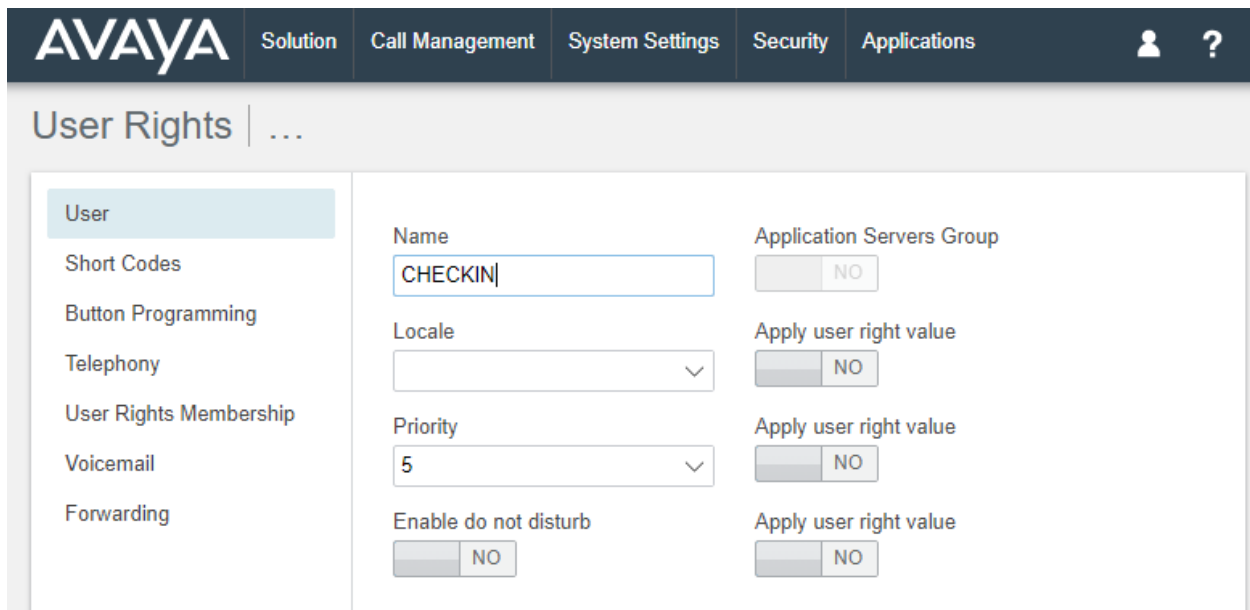
- Code:** *79*N#
- Feature:** Display Msg (selected from a dropdown menu)
- Telephone Number:** N";Mailbox Msgs=0"
- Line Group ID:** 99001 (selected from a dropdown menu)
- Locale:** (empty dropdown menu)
- Force Account Code:** NO (checkbox)
- Force Authorization Code:** NO (checkbox)
- Buttons:** Save and Cancel

5.9. 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 uppercase 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).

User Rights | ...

User

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Can intrude

NO

Apply user right value

NO

Cannot be intruded

NO

Apply user right value

NO

Deny Auto Intercom Calls

NO

Apply user right value

NO

Enable force login

NO

Apply user right value

NO

Enable force account code

NO

Apply user right value

NO

Inhibit Off-Switch Forward/Transfer

NO

Apply user right value

NO

Enable outgoing call bar

NO

Apply user right value

YES

Coverage Group

None

Apply user right value

NO

Cancel

Create

AVAYA

Solution

Call Management

System Settings

Security

Applications

User Rights

+ Add User Right

Show All

Common Object

SYSTEMS

☐ IPOSE178
 ☐ IPOEXP180

CHECK

☐

Name

Priority

External Call Barr...

System Name

☐ CHECKIN
 5
 No
 IPOSE178

☐ CHECKIN_BAR
 5
 Yes
 IPOSE178

☐ CHECKIN_BAR_DND
 5
 Yes
 IPOSE178

☐ CHECKIN_DND
 5
 No
 IPOSE178

☐ CHECKIN_DOM
 5
 No
 IPOSE178

☐ CHECKIN_DOM_DND
 5
 No
 IPOSE178

☐ CHECKIN_LOC
 5
 No
 IPOSE178

☐ CHECKIN_LOC_DND
 5
 No
 IPOSE178

☐ CHECKOUT
 5
 Yes
 IPOSE178

☐ CHECKIN
 5
 No
 IPOEXP180

☐ CHECKIN_BAR
 5
 Yes
 IPOEXP180

☐ CHECKIN_BAR_DND
 5
 Yes
 IPOEXP180

☐ CHECKIN_DND
 5
 No
 IPOEXP180

☐ CHECKIN_DOM
 5
 No
 IPOEXP180

☐ CHECKIN_DOM_DND
 5
 No
 IPOEXP180

☐ CHECKIN_LOC
 5
 No
 IPOEXP180

☐ CHECKIN_LOC_DND
 5
 No
 IPOEXP180

☐ CHECKOUT
 5
 Yes
 IPOEXP180

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.

The screenshot shows the Avaya User Rights configuration interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security', and 'Applications'. The main header displays 'User Rights' and 'CHECKOUT IPOSE178'. The left sidebar lists various user rights categories: 'User', 'Short Codes', 'Button Programming', 'Telephony' (highlighted), 'User Rights Membership', 'Voicemail', and 'Forwarding'. The main content area is divided into tabs: 'Call Settings', 'Supervisor Settings', 'Multiline Options', and 'Call Log'. Under 'Call Settings', several fields are visible, each with a 'NO' button and an 'Apply user right value' button. The 'Enable outgoing call bar' field is set to 'YES' (indicated by a blue 'YES' button). Other fields include 'Can Intrude', 'Cannot be Intruded', 'Deny Auto Intercom Calls', 'Enable force login', 'Enable force account code', 'Inhibit Off-Switch Forward/Transfer', and 'Coverage Group' (set to 'None').

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.

The screenshot shows the Avaya User Rights configuration interface for the 'CHECKIN_DND' user right. The top navigation bar is the same as the previous screenshot. The main header displays 'User Rights' and 'CHECKIN_DND IPOSE178'. The left sidebar is the same. The main content area shows fields for 'Name' (CHECKIN_DND), 'Locale' (dropdown), 'Priority' (5), and 'Enable do not disturb' (YES). Each field has an 'Apply user right value' button. The 'Application Servers Group' field is also visible with a 'NO' button.

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.

User Rights

CHECKIN_LOC

IPOSE178

User

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Apply user right value

YES

+ Add

Code	Telephone ...	Feature	Line Group ID	Force Acco...	Force Autho...	
90N	0N	Dial	0	No	No	
91N	1N	Dial	0	No	No	

AVAYA

Solution

Call Management

System Settings

Security

Applications

User Rights

CHECKIN_DOM

IPOSE178

User

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Apply user right value

NO

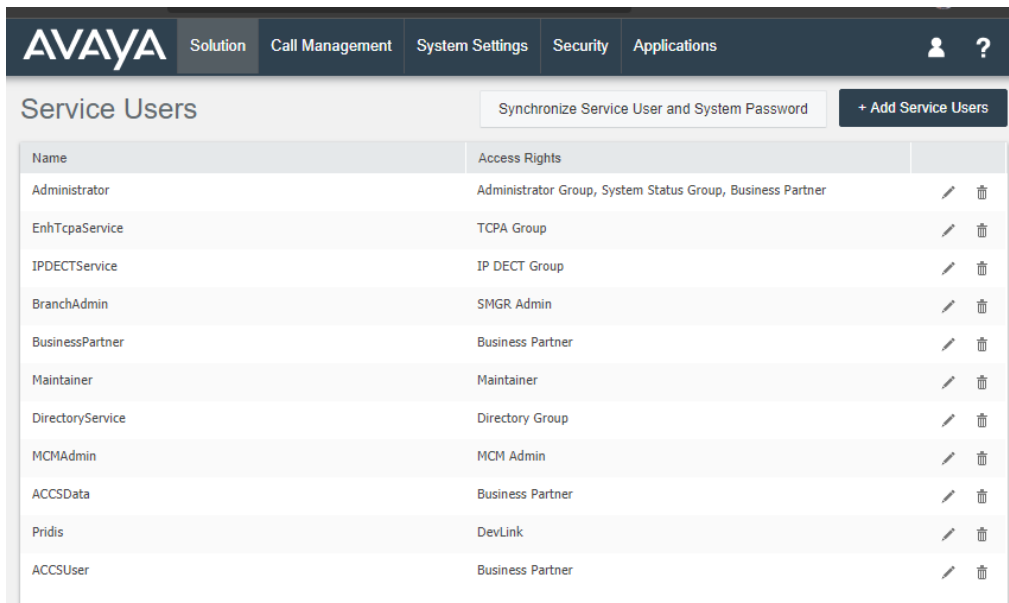
+ Add























Code	Telephone ...	Feature	Line Group ID	Force Acco...	Force Autho...	
91N	1N	Dial	0	No	No	

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

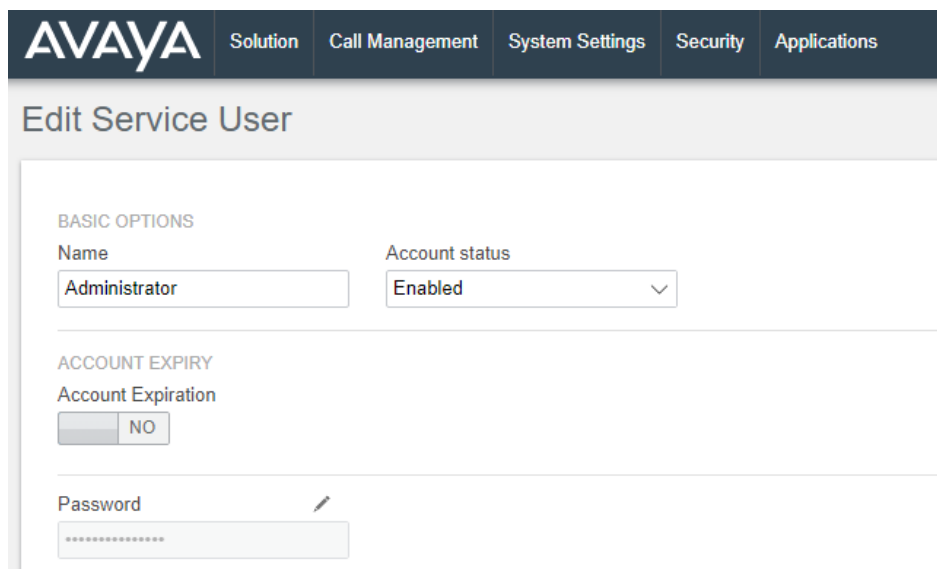
5.10. Administer System Password

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	 
EnhTcpsService	TCPA Group	 
IPDECTService	IP DECT Group	 
BranchAdmin	SMGR Admin	 
BusinessPartner	Business Partner	 
Maintainer	Maintainer	 
DirectoryService	Directory Group	 
MCMAdmin	MCM Admin	 
ACCSDData	Business Partner	 
Pridis	DevLink	 
ACCUser	Business Partner	 

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.



AVAYA Solution Call Management System Settings Security Applications


Edit Service User

BASIC OPTIONS

Name: Account status:

ACCOUNT EXPIRY

Account Expiration:

Password 

5.11. Administer SMDR

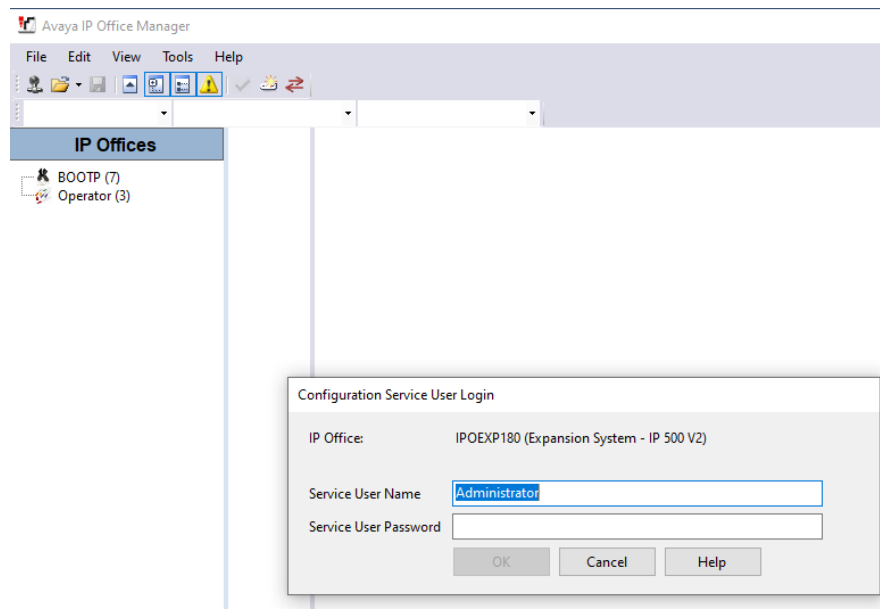
From the home menu, select **System Settings** → **System** → **IPOPRI** → **SMDR**. For the Output field, select “**SMDR Only**” from the drop-down box. Set **IP Address** to the WinExpress server IP address, and set the **TCP Port** to **5050**. Optionally, you can increase the **Records to Buffer** 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).

The screenshot shows the Avaya System Configuration interface for IPOSE178. The top navigation bar includes the Avaya logo and tabs for Solution, Call Management, System Settings, Security, and Applications. The main header reads "System Configuration | IPOSE178". On the left, a sidebar lists configuration categories: System, Voicemail, System Events, SMTP, DNS, SMDR (highlighted), LAN1, and LAN2. The main content area is titled "STATION MESSAGE DETAIL RECORDER COMMUNICATIONS" and contains the following fields:

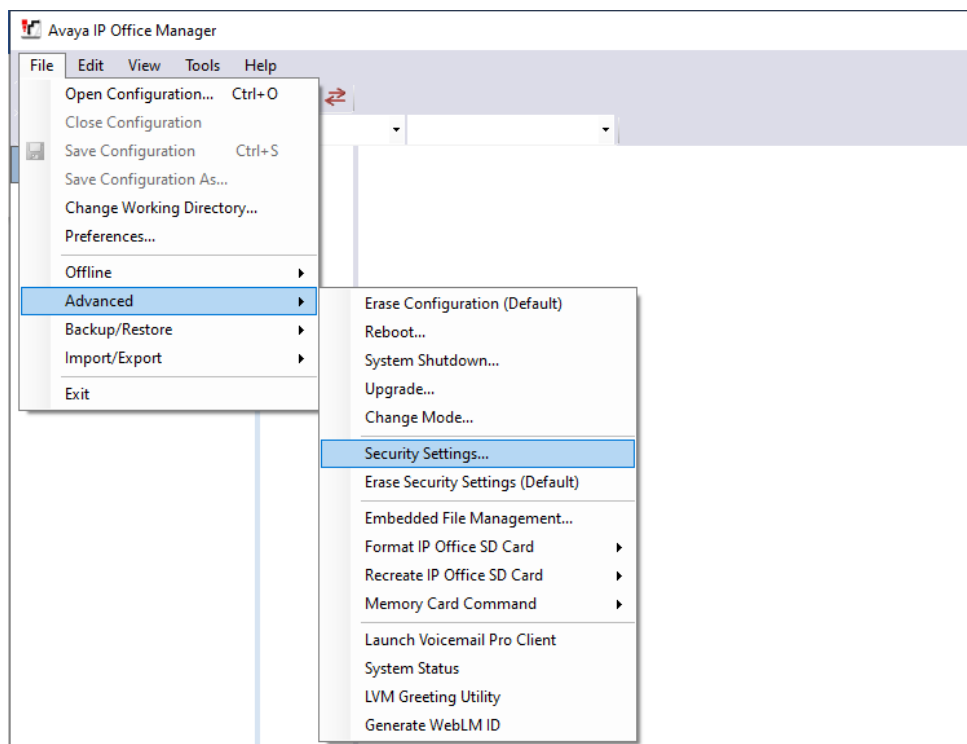
- Output:** A dropdown menu set to "SMDR Only".
- IP Address:** A field containing the IP address "10 . 30 . 5 . 90".
- TCP Port:** A field containing the port number "5050".
- Records to Buffer:** A field containing the value "3000".
- Call Splitting for Diverts:** A toggle switch set to "NO".

5.12. Administer Security Settings

From the home screen, select **Applications** → **IP Office Manager** to launch the Manager application. Press **Cancel**

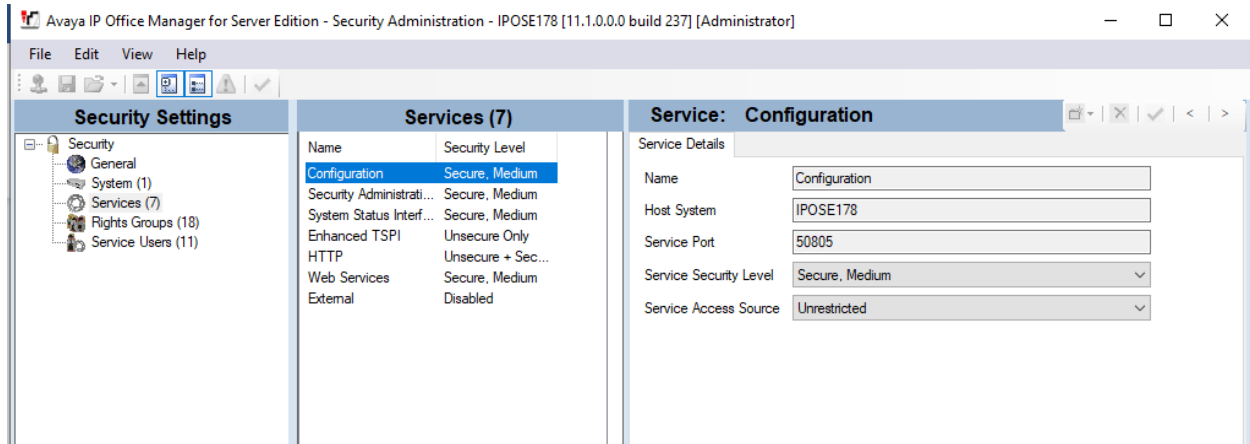


Click on **File** → **Advanced** → **Security Settings** from the top menu.

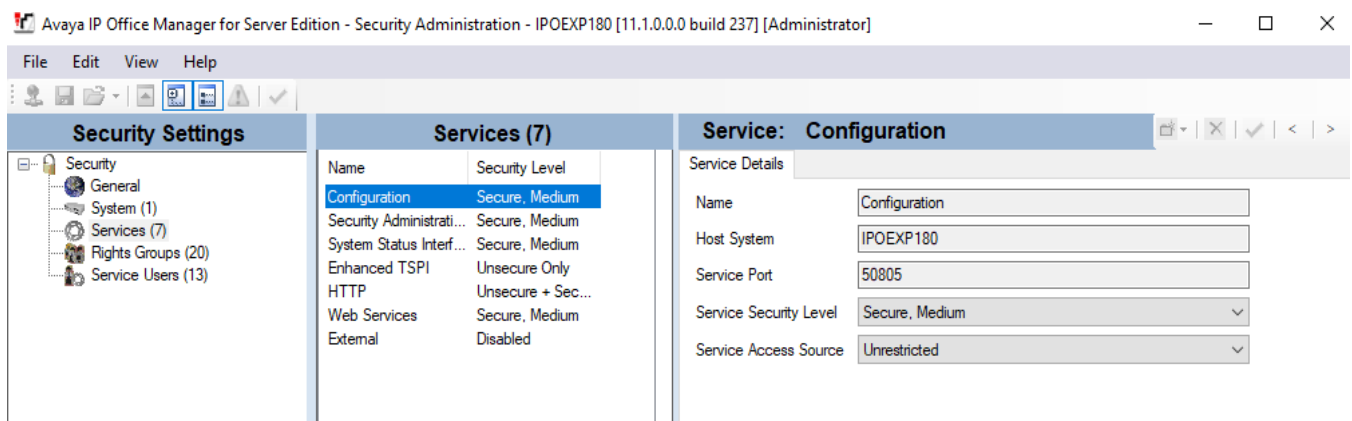


The **Avaya IP Office Manager for Server Edition - Security Administration – IPOSE178** screen is displayed. From the configuration tree in the left pane, select **Security** → **Services** → **Configuration** to display the **Service: Configuration** screen in the right pane. For **Service**

Security Level, select “**Secure, Medium**” as shown below. In this compliance testing, Gateway 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 **IPOEXP180** as shown in the screen above.



6. Configure FCS WinExpress

This section provides the procedures for configuring WinExpress. WinExpress comprises two main components, i.e., FCS Voice and FCS Gateway call billing package and interface solution.

The procedures include the following:














- Obtaining IP Office Configuration Web Service SDK
- Configuring Gateway
- Configuring Voice

6.1. Obtaining Avaya IP Office Configuration Web Service SDK

Avaya provides the IP Office Configuration Web Service SDK for 3rd party solution to incorporate IP Office configuration changes in their solutions. The latest Configuration Web Service SDK can be obtained from FCS.

Navigate to

\IPOfficeConfigurationService_Jun2017\IPO_XML_Sample.zip\IPO_XML_Sample\Sample_Host\ConfigServiceHost\bin\Release and unzip them (13 in total) into a location of your choice, preferably, as a sub-folder under the \FCS\Gateway directory.

Name	Type	Compressed size	Password p...	Size	Ratio	Date modified
 AvailabilityValidationVisibility.dll	Application extension	25 KB	No	331 KB	93%	6/23/2017 7:08 PM
 AvayaIPOConfigBaseServices.dll	Application extension	18 KB	No	43 KB	60%	6/23/2017 7:16 PM
 ConfigServiceHost.exe	Application	3 KB	No	6 KB	61%	6/23/2017 7:16 PM
 ConfigServiceHost.exe.config	CONFIG File	1 KB	No	2 KB	68%	6/7/2016 7:31 PM
 CoreServices.dll	Application extension	1,475 KB	No	5,206 KB	72%	6/23/2017 7:15 PM
 IPOConfigService.dll	Application extension	4 KB	No	10 KB	62%	6/23/2017 7:16 PM
 IPOConfigServiceInterface.dll	Application extension	3 KB	No	7 KB	62%	6/23/2017 7:16 PM
 IPOUnitDetails.dll	Application extension	4 KB	No	13 KB	69%	6/23/2017 7:16 PM
 LegacySettings.dll	Application extension	20 KB	No	83 KB	77%	6/23/2017 7:16 PM
 SecurityManager.dll	Application extension	1,269 KB	No	2,196 KB	43%	6/23/2017 7:16 PM
 UpgdWiz.dll	Application extension	137 KB	No	425 KB	68%	6/23/2017 7:16 PM
 Whols2.dll	Application extension	20 KB	No	67 KB	72%	6/23/2017 7:16 PM
 WindowsControlLibrary.dll	Application extension	25 KB	No	99 KB	76%	6/23/2017 7:16 PM

Note: The SDK version that was used is version 10.1 (June 2017)

6.2. Configure FCS Gateway

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

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

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

```
<Child Id="PBX1">
  <PropertyId>01</PropertyId>
  <EXENAME>AvayaIPOPMS.PBX.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidelio.exe-->
  <LogFilePattern>PBX\PBX1-</LogFilePattern>
  <Description>Avaya IPO PBX</Description>
  <XMLFile>AvayaIPOPMS-PBX.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX1In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX1Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>4015</UnicornMotherIPPort>
  <MemoryPage>4</MemoryPage>
</Child>

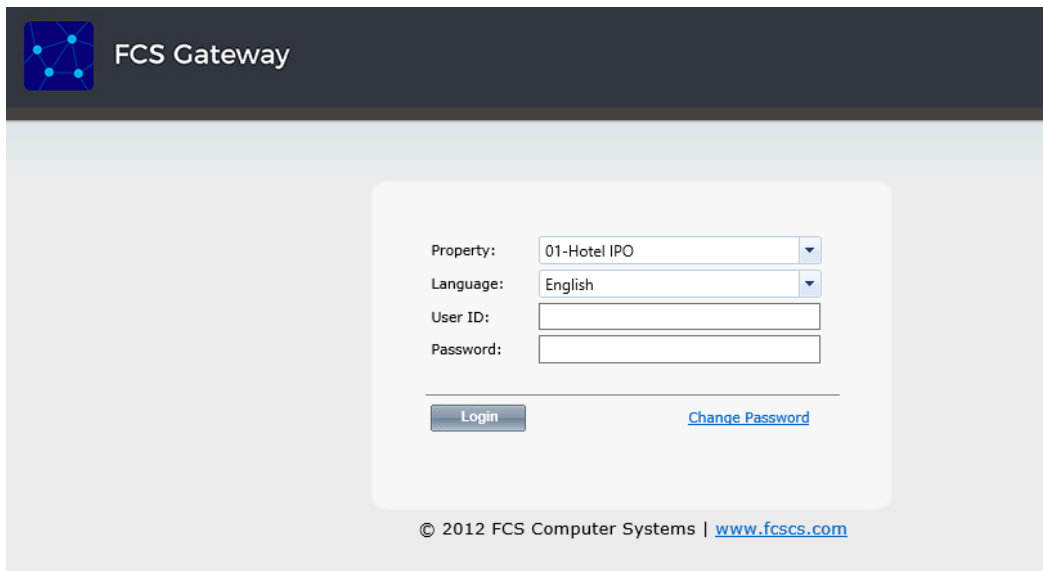
<Child Id="PBX2">
  <PropertyId>01</PropertyId>
  <EXENAME>AvayaIPOPMS2.PBX.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidelio.exe-->
  <LogFilePattern>PBX\PBX2-</LogFilePattern>
  <Description>Avaya IPO PBX 2</Description>
  <XMLFile>AvayaIPOPMS2-PBX.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX2In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX2Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>4025</UnicornMotherIPPort>
  <MemoryPage>5</MemoryPage>
</Child>
```

```

<Child Id="CDR1">
  <PropertyId>01</PropertyId>
  <LogFilePattern>CDR\CDR1-</LogFilePattern>
  <EXENAME>AvayaIPO.CDR.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidelio.exe-->
  <Description>Avaya IPO CDR Interface </Description>
  <XMLFile>AvayaIPO-CDR.xml</XMLFile>
  <IntfInQueueName>.\Private$\SMDRIn</IntfInQueueName>
  <!--can be a remote MSMQ queue-->
  <IntfOutQueueName>.\Private$\SMDROut</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <!-- interface will filter the packet if it's more than this value (in hour) as compared to system clock-->
  <!--during startup, the child has to initial a dialog with mother via tcp/ip before can send the info.
  to the message queue The message queue name to be assigned by unicorn , and be part of the XML dialog string -->
  <UnicornMotherIPPort>4001</UnicornMotherIPPort>
  <MemoryPage>6</MemoryPage>
</Child>
<Child Id="VMS1">
  <PropertyId>01</PropertyId>
  <EXENAME>Phoenix.VMS.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidelio.exe-->
  <LogFilePattern>VMS\VMS1-</LogFilePattern>
  <Description>FCSVM3.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 compared to system clock-->
  <!--during startup, the child has to initial a dialog with mother via tcp/ip before can send the info.
  to the message queue The message queue name to be assigned by unicorn , and be part of the XML dialog string -->
  <UnicornMotherIPPort>4017</UnicornMotherIPPort>
  <MemoryPage>7</MemoryPage>
</Child>

```

2. FCS Gateway 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 ip address>/FCSGateway.Web/Login.aspx> as shown below by substituting the appropriate server IP address. Select the **Property** and log in with the appropriate credentials.



The screenshot shows the FCS Gateway web interface. At the top left is the FCS Gateway logo. Below it is a login form with the following fields:

- Property: A dropdown menu with "01-Hotel IPO" selected.
- Language: A dropdown menu with "English" selected.
- User ID: A text input field.
- Password: A text input field.

Below the input fields are two buttons: "Login" and "Change Password". At the bottom of the page, there is a copyright notice: "© 2012 FCS Computer Systems | www.fcscs.com".

3. Click **Home** → **System** → **Interface Listing** to show the integrated interfaces and their status. The list below shows the **Device ID** list and the **description** of each interface:
 - a. **FOS1** – Front Office System
 - b. **VMS1** – FCS Voice
 - c. **PBX1** – IP Office Primary Server PMS
 - d. **PBX2** – IP Office Expansion Module PMS
 - e. **CDR1** – IP Office SMDR

FCS Gateway
 Hi, Administrator Language: English [sign out](#) [change password](#)

This is a temporary license. It will expire in 3 days on 15 August 2020. Your system will be inoperable from the expiry date. Please obtain a valid license.

[Home](#) [Posting](#) [Reporting](#) [Configuration](#)
Business Date: 24-Feb-2018
12-Aug-2020 03:00 : Auto night audit starts(UWR1)

Interface Listing

Refresh

	DEVICE ID	DEVICE DESC	EXE NAME	VERSION	STATUS	POSTING
	FOS1	Fidelio FIAS	FIAS.FOS.exe	1.2.5.9	↑	ON
	PBX1	Avaya IPO PBX	AvayaIPOPMS.PBX.exe	1.2.1.34	↑	OFF
	PBX2	Avaya IPO PBX 2	AvayaIPOPMS2.PBX.exe	1.2.1.34	↑	ON
	CDR1	Avaya IPO CDR Interface	AvayaIPO.CDR.exe	1.2.1.27	↑	N/A
	VMS1	FCSVM3.VMS	Phoenix.VMS.exe	1.2.2.56	↑	ON

Occupancy 40%

4. The FCS Gateway Avaya PMS interface module port and data configuration is defined in both the **AvayaIPOPMS-PBX.xml** and **AvayaIPOPMS-PBX2.xml** located in the “C:\Program Files(x86)\FCS\Gateway\Control\” directory.

```

      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://127.0.0.1:8085/IPOConfigurationService</InterfaceSetting>
  <UDPSvrInterfaceSetting>U,127.0.0.1:4544</UDPSvrInterfaceSetting>
  
```

In both configuration xml files, the **IPAddress** points to the IP Office server (and Expansion Module) listening to port **50805** which corresponds with the IP Office port at **Section 5.12** and the **AccountName** and **Password** administered in **Section 5.10**. The password is not revealed for security reasons.

```
<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>[REDACTED]</PassWord>
<IPAddress>10.128.226.178</IPAddress>
<PortNumber>50805</PortNumber>
</CommunicationSetting>
```

```
<SendRetry>3</SendRetry>
<AccountName>Administrator</AccountName>
<PassWord>[REDACTED]</PassWord>
<IPAddress>10.128.226.180</IPAddress>
<PortNumber>50805</PortNumber>
<SendDelay>2000</SendDelay>
</CommunicationSetting>
```

SDKFile is the location of IPO Configuration Web Services files.

```
<DeviceDependentSetting>
  <InterfaceType>8</InterfaceType>
  <GetSlaveExtn>Yes</GetSlaveExtn>
  <AckRequired>No</AckRequired>
  <AutoLaunchSDK>Yes</AutoLaunchSDK>
  <SDKFile>C:\Program Files (x86)\FCS\Gateway\ConfigServiceHost\ConfigServiceHost.exe</SDKFile>
  <AutoResetSDKTime>03:00</AutoResetSDKTime>
  <MaxSDKResource>100000</MaxSDKResource>

<DeviceDependentSetting>
  <InterfaceType>8</InterfaceType>
  <GetSlaveExtn>Yes</GetSlaveExtn>
  <AckRequired>No</AckRequired>
  <AutoLaunchSDK>Yes</AutoLaunchSDK>
  <SDKFile>C:\Program Files (x86)\FCS\Gateway\ConfigServiceHost2\ConfigServiceHost2.exe</SDKFile>
  <AutoResetSDKTime>03:00</AutoResetSDKTime>
  <MaxSDKResource>100000</MaxSDKResource>
```

Note: Both the above *ConfigServiceHost* folders need to be manually created – see 6.1 for more info

- Open both ConfigServiceHost.exe.config & ConfigServiceHost2.exe.config files and make the following changes:

```
<services>
  <service behaviorConfiguration="mex" name="IPOConfigService.Service.IPOfficeService">
    <endpoint address="http://10.128.226.178:8085/IPOConfigurationService"
      binding="basicHttpBinding" bindingConfiguration="NewBinding0"
      bindingNamespace="http://avaya.com/IPOffice/ConfigService/2007/01"
      contract="IPOConfigService.Service.Interface.IConfigurationService" />
    <host>
      <baseAddresses>
        <add baseAddress="http://10.128.226.178:8085/IPOConfigurationService" />
      </baseAddresses>
    </host>
  </service>
</services>

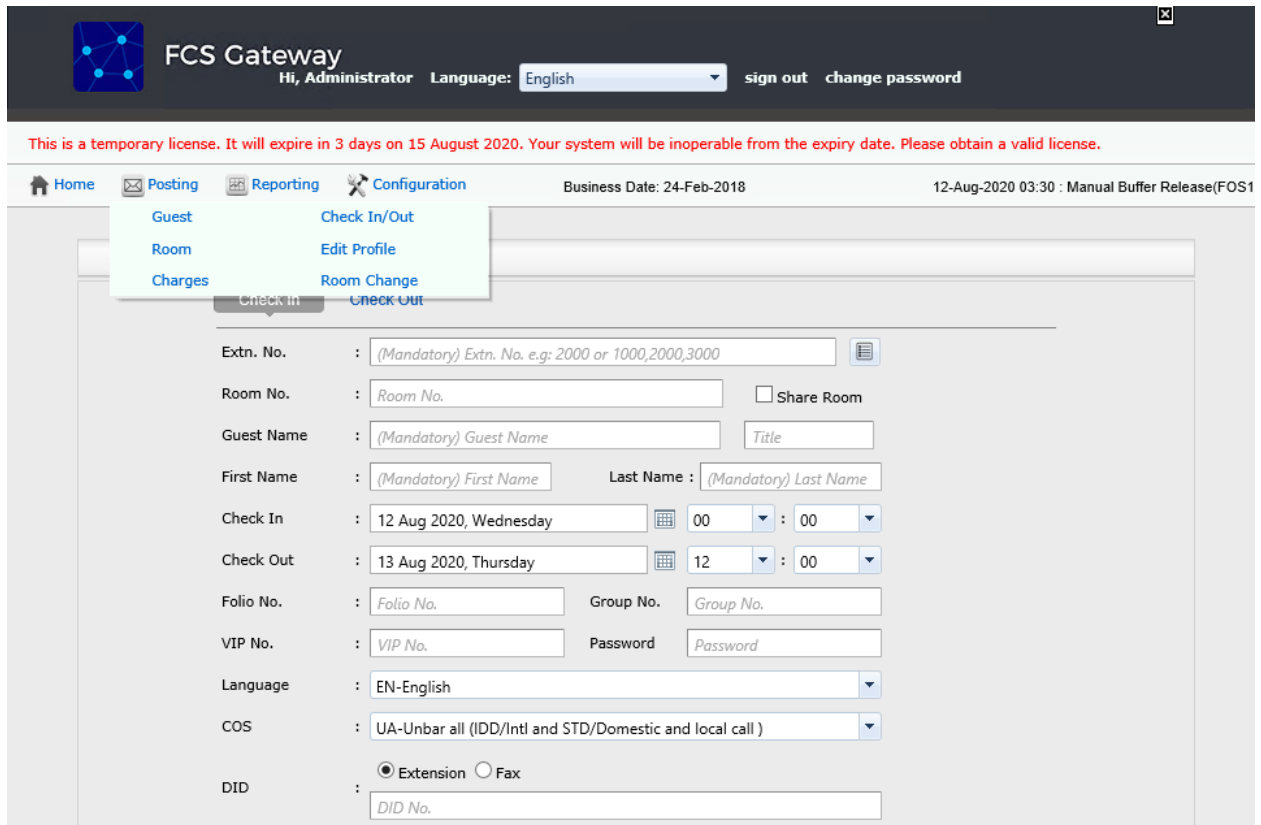
<services>
  <service behaviorConfiguration="mex" name="IPOConfigService.Service.IPOfficeService">
    <endpoint address="http://10.128.226.180:8086/IPOConfigurationService"
      binding="basicHttpBinding" bindingConfiguration="NewBinding0"
      bindingNamespace="http://avaya.com/IPOffice/ConfigService/2007/01"
      contract="IPOConfigService.Service.Interface.IConfigurationService" />
    <host>
      <baseAddresses>
        <add baseAddress="http://10.128.226.180:8086/IPOConfigurationService" />
      </baseAddresses>
    </host>
  </service>
</services>
```

- The Gateway Avaya CDR interface module port & data configuration is defined in the **AvayaIPO-CDR.xml** located in the “C:\Program Files (x86)\FCS\Gateway\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 5.11**.

```
<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 Lenght-->
    <InterfaceType>2</InterfaceType>
    <!--1 = RS232, 2=tcp.ip 3=udp, 4=telnet,5=bisync 6=file sharing-->
    <InterfaceSetting>H,10.128.226.178:5050</InterfaceSetting>
```


7. 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.



FCS Gateway
Hi, Administrator Language: English sign out change password

This is a temporary license. It will expire in 3 days on 15 August 2020. Your system will be inoperable from the expiry date. Please obtain a valid license.

Home Posting Reporting Configuration Business Date: 24-Feb-2018 12-Aug-2020 03:30 : Manual Buffer Release(FOS1)

Guest Check In/Out
Room Edit Profile
Charges Room Change
Check In Check Out

Extn. No. : (Mandatory) Extn. No. e.g: 2000 or 1000,2000,3000

Room No. : Room No. ☐ Share Room

Guest Name : (Mandatory) Guest Name Title

First Name : (Mandatory) First Name Last Name : (Mandatory) Last Name

Check In : 12 Aug 2020, Wednesday 00 : 00

Check Out : 13 Aug 2020, Thursday 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)

DID : ☒ Extension ☐ Fax
DID No.

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

The screenshot displays the FCS Gateway web application interface. At the top, the header shows the FCS Gateway logo, the user 'Hi, Administrator', the language 'English', and links for 'sign out' and 'change password'. A red banner below the header states: 'This is a temporary license. It will expire in 3 days on 15 August 2020. Your system will be inoperable from the expiry date. Please obtain a valid license.'

The main navigation bar includes links for Home, Posting, Reporting, and Configuration. The Configuration menu is expanded, showing options like Company Hierarchy, Extensions, Computation, Code Mapping, Telephone Tariff, Printing, Others, Read Only, Rights Config, Database Connection, Extension Type, Extension Type Posting, Primary Extension Numbering, Authorization code, Slave Extension, Transfer Charge, Temporary Slave Extension, and Special Telephone Numbers. The 'Primary Extension Numbering' option is selected.

Below the navigation bar, the 'Primary Extension Numbering' configuration page is visible. It features a table with columns for Extension Number, Extn, and a third column. The table contains five rows of data: 1006, 1007, 1008, 1009, and 1010, each with an 'Extn' value of 01. To the right of the table is a 'Next Last' link and buttons for 'Edit' and 'Delete'.

Below the table, the 'Primary Extension Numbering Information' section is displayed. It contains various fields for configuration, including Extension Number From, Extension Name, Section (Dept), Cost Center, Budget Charge, Budget Duration, Designation, Surcharge Code, Tax Code, Service Charge Code, Voucher Code, Log Code, Device Id, Post To FOS, Guest, Extension Type, Pager, and Email. The 'Extension Type' field is set to 'AA' and has a red asterisk next to it.

6.3. Configure FCS Voice

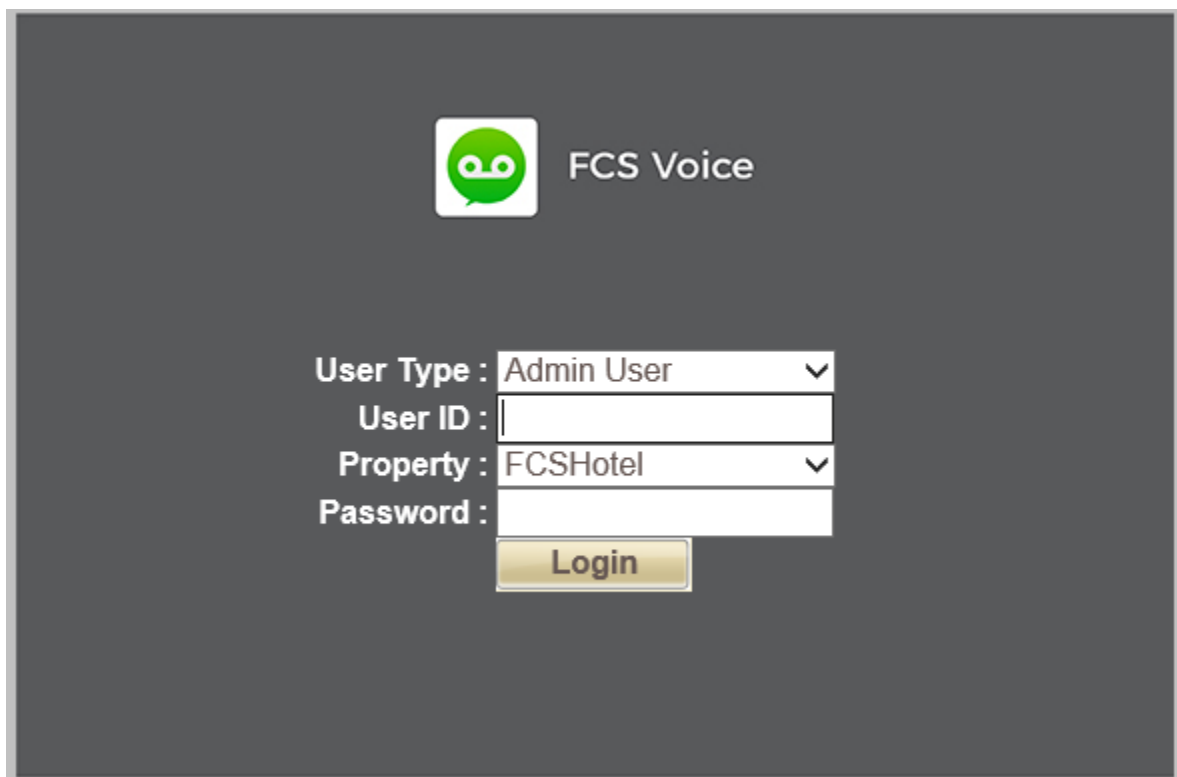
This section details the essential portion of the FCS Voice configuration to interoperate with IP Office. These Application Notes assume that the FCS Voice application has already been properly installed by FCS services engineer.


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 Voice System, launch any browser and type in the Voice Web URL; in this case <http://<server ip address>/VoicemailWebUI/Login.aspx> as shown below by substituting the appropriate server IP Address. At the login screen, enter an account with administrative privileges.

The image shows the login interface for FCS Voice. At the top center is a green circular logo with a white 'vo' inside, followed by the text 'FCS Voice'. Below this, there are four labeled input fields: 'User Type' with a dropdown menu showing 'Admin User', 'User ID' with an empty text box, 'Property' with a dropdown menu showing 'FCSHotel', and 'Password' with an empty text box. A yellow 'Login' button is positioned below the password field. The entire interface is set against a dark gray background.

 FCS Voice

User Type : Admin User ▼

User ID :

Property : FCSHotel ▼

Password :

Login

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

Organization Code	Property Name	Property Code	Expiry Date	License Type	Action
EV0001	FCSHotel	001	2020-12-01	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.

License Details	
License Type:	Temporary
Expiry Date :	2020-12-01
MAC Address* :	00:0C:29:CF:7D:E4
Organization:	Evaluation
Organization Code :	EV0001
Property :	FCSHotel
External Code :	1
Address :	<input type="text"/>
FCS Housekeeping property code :	<input type="text"/>
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
Modules:	<div>Room Status Auto WakeUp Auto Attendant VPIM ConsoleXML MiniBar Voicemail Fax Agent-Assisted VIP Wakeup Call Voicemail to Email Check Out Reminder</div>
Languages:	<div>English</div>
WebUI Languages:	<div>English</div>

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 **Avaya IP Office**
- **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**

A screenshot of the FCS Voice application showing the PBX configuration screen. The top bar includes the FCS Voice logo, a 'Property' dropdown set to 'System Wide Setting', and a 'Language' dropdown set to 'English'. Below this is a yellow bar for 'System Wide Setting'. The main area has two tabs: 'PBX' and 'Server'. The 'PBX' tab is active, showing a table with one entry: 'Avaya IP Office'. To the right of the table is a configuration form for 'Avaya IP Office' with fields for PBX Name, PBX Type, PBX Version, DTMF Type, Fax Protocol, and Trunk Type, each with a dropdown menu. At the bottom of the form are 'Save' and 'Reset' buttons.

6.3.3. Server Setting

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

FCS Voice

System Wide Setting

PBX **Server**

Server	Action
VoiceApp	

VoiceApp

Please restart application for the changes to take effect

App Server Name VoiceApp

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

SMTP **IMAP**

Enable ☐ ☐

Server

Port No.

SMTP SSL Port No. ☐ **IMAP use SSL**

Email Address

SMTP Username

SMTP Password

License Expiry Reminder

Notification Before Expiry 7 **Day(s)**

PBX Assigned	Interoperability	Property
--------------	------------------	----------

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 IP address
Local IP	Enter WinExpress Server IP address
Transport protocol	Select UDP
Client Extension	Enter the SIP User in a URL form: “ 1001@10.128.226.178 ”
Contact	Enter the SIP contact as: “ 1001@10.30.5.90 ”
Time Alive	Enter a time less than 120 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

10.128.226.178

PortNo

Local IP

10.30.5.90

PortNo

Transport protocol

☐ TCP
☒ UDP

Client Extension

1001@10.128.226.178

Contact

1001@10.30.5.90

Time Alive

120

Authentication

☒ Yes
☐ No

Identity

1001@10.128.226.178

Realm

ipoffice

User Name

1001

Password


•••••

Edit

Cancel

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, “1001_W” mapped to **DIRECT** Entry Point for Voice Mail Pilot Number **1000** and **DIRECT** Entry Point for the rest of the Voice Mail SIP lines **1001-1003**. The Entry Points configured as shown at the bottom of the home screen.

 **FCS Voice**

System Configuration Hotel Operation Administration Utilities Reports Fax License

Hardware Settings System Settings Database Setup User Setup

Hardware Settings → Channels → Entry Point

Entry Point Format

1004 _ 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

Added successfully

	Entry Point	CPI Format	Description
 	1	W_W	BUSY/NOANSWER
 	2	1001_W	DIRECT
 	3	1002_W	DIRECT
 	4	1003_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.

Select System to Monitor

Enter Control Unit FQDN / IP Address
[nnn.nnn.nnn.nnn]
or
Control Unit IP Address:Dev No.
[nnn.nnn.nnn.nnn:mm]
or
COM FQDN or IP Address / Customer ID

10.128.226.178

Protocol
UDP

Port
50794

Certificate
...

Username
...

Password
XXXXXXXXXX

Trace Log Settings Filename
C:\Users\AQ\AppData\Roaming\Avaya\IP ...

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 1001, 1002 and 1003 configured in **Section 5.4** and the Status shown is “SIP: Registered” for each (not show).

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.

The screenshot displays the Avaya IP Office System Status application. The left sidebar contains a navigation menu with the following items: System, Alarms (3), Extensions (4), Trunks (2), Active Calls, Resources, Voicemail, IP Networking, and Locations. The 'Extensions (4)' section is expanded, showing a list of extensions: 1011, 1012, 1031, and 5555. The extension 1011 is selected, and its status is displayed in the main pane. The status is 'SIP: Registered'. The main pane also shows a list of extension details, including IP address, MAC address, Standard Location, Gatekeeper, Telephone Type, Firmware Version, Media Stream, Layer 4 Protocol, Current User Extension Number, Current User Name, Forwarding, Twinning, Do Not Disturb, Message Waiting, Phone Manager Type, Licensed, License Reserved, and Last Date and Time License Allocated. The status 'SIP: Registered' is highlighted in the list. The bottom status bar shows the time as 11:01:35 AM and the status as Online.

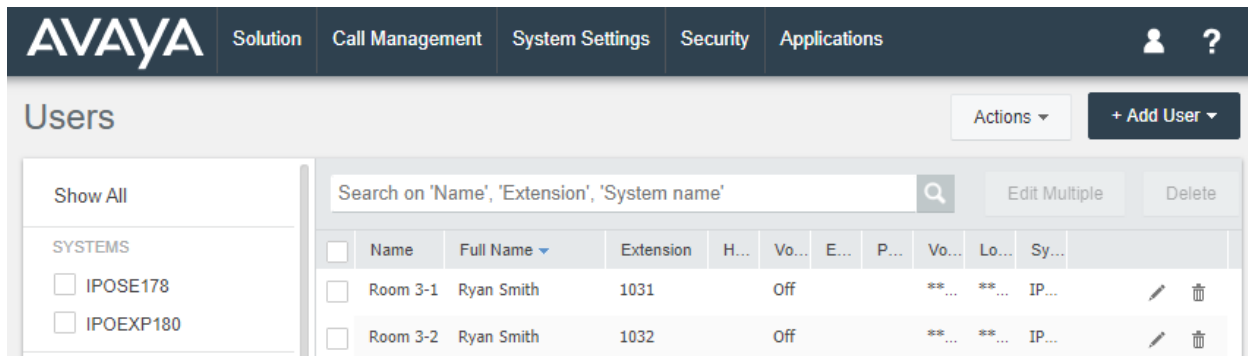
Extension Status	
Extension Number:	1011
IP address:	10.133.100.17
MAC address:	CC-F9-54-A9-6D-C8
Standard Location:	None
Gatekeeper:	Primary
Telephone Type:	9608
Firmware Version:	6.8304
Media Stream:	Best Effort
Layer 4 Protocol:	TCP
Current User Extension Number:	1011
Current User Name:	Room 1-1
Forwarding:	Off
Trinning:	Off
Do Not Disturb:	Off
Message Waiting:	On
Phone Manager Type:	None
Licensed:	Yes
License Reserved:	No
Last Date and Time License Allocated:	8/5/2020 11:11:49 PM

Buttons: Trace, Trace All, Pause, Ping, Call Details, Reregister, Restart, Print..., Save As...

Status Bar: 11:01:35 AM, Online, [Icon]

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.

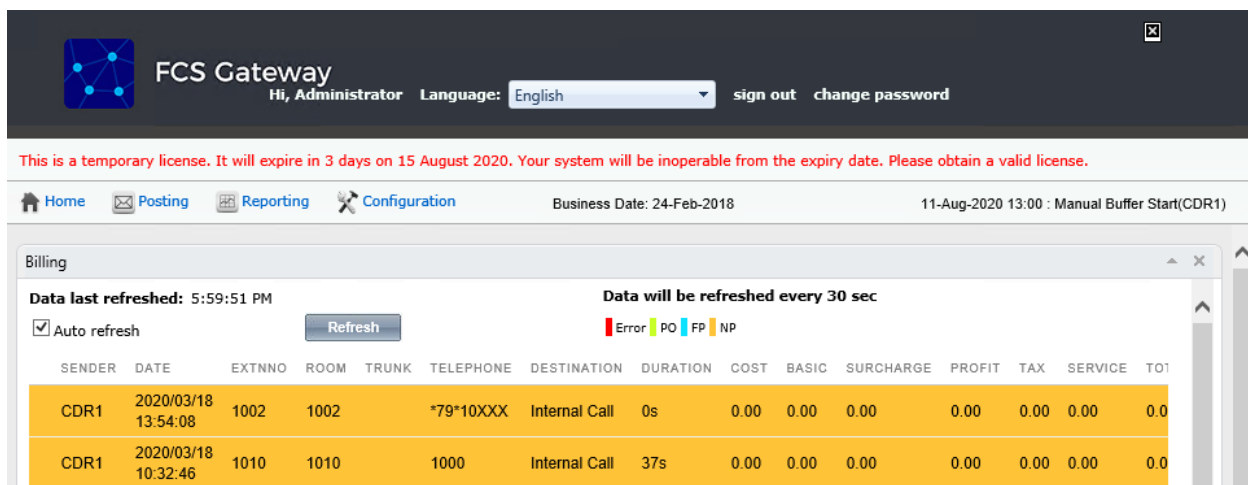


The screenshot shows the Avaya IP Office Web Manager interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security', and 'Applications'. The 'Users' page is active, showing a list of users. The left pane has a 'Show All' button and a list of systems: 'IPOSE178' and 'IPOEXP180'. The main pane has a search bar and a table of users. The table has columns: Name, Full Name, Extension, H..., Vo..., E..., P..., Vo..., Lo..., Sy..., and two action icons (pen and trash). Two users are listed: 'Room 3-1' and 'Room 3-2', both with 'Full Name' 'Ryan Smith' and 'Extension' 1031 and 1032 respectively. The 'Room 3-1' user has a pen icon next to the 'Full Name' field.

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


7.4. Verify SMDR

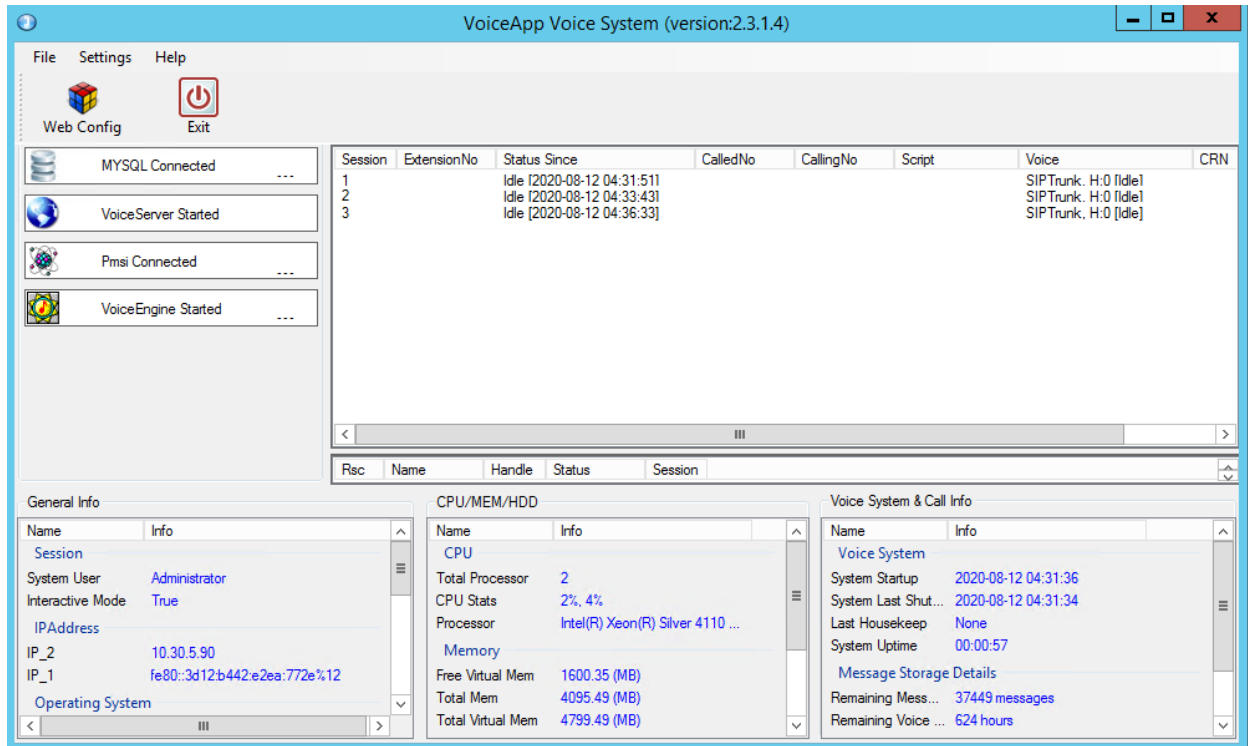
On the Gateway web interface, click **Home** → **System** → **Billing**. Place a few outbound calls to an internal, local, mobile, toll free and international location. Verify that the calls are all processed correctly as shown below:



The screenshot shows the FCS Gateway web interface. The top bar includes 'Hi, Administrator', 'Language: English', 'sign out', and 'change password'. A red banner indicates a temporary license expiration on 15 August 2020. The navigation bar includes 'Home', 'Posting', 'Reporting', and 'Configuration'. The 'Billing' page is active, showing a table of billing records. The table has columns: SENDER, DATE, EXTNN, ROOM, TRUNK, TELEPHONE, DESTINATION, DURATION, COST, BASIC, SURCHARGE, PROFIT, TAX, SERVICE, and TO1. Two records are shown: one for 'CDR1' on 2020/03/18 at 13:54:08, and another for 'CDR1' on 2020/03/18 at 10:32:46. Both records show 'Internal Call' with a duration of 0s and 37s respectively.

7.5. Verify Voice Integration

From the server, launch **FCS Voice** 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 FCS Voice communication has been successfully established, the FCS Voice status will show up as **Connected**.



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. 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 R11.1. All features and serviceability test cases were completed with observations noted in **Section 2.2**.

9. Additional References

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

- i. *Administering Avaya IP Office™ Platform with Web Manager, Release 11.1 Issue 2 May 2020*
- ii. *Administering Avaya IP Office™ Platform with Manager, Release 11.1 Issue 2 May 2020*

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

©2020 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.