



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring FCS Gateway 2.0 with Avaya IP Office 11.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for FCS Gateway 2.0 to interoperate with Avaya IP Office Release 11.1. FCS Gateway provides PMS integration, call billing, and 3rd party interfacing solution. In the compliance testing, FCS Gateway used Station Message Detail Reporting (SMDR), and Management API interfaces from Avaya IP Office Server to provide room status, call billing, as well as name and user profile template change, outgoing call barring and do not disturb features.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1**, as well as 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 Gateway 2.0 to interoperate with Avaya IP Office 11.1. FCS Gateway is a Windows-based hospitality system that provides a seamless interface with a hotel's Front Office System and Avaya IP Office Server.

Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion system. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network.

FCS Gateway was used in the compliance testing to initiate the room Check-In, Check-Out, and Move requests. During compliance testing, multiple rights templates were set up on Avaya IP Office Server for use with Check-In and Check-Out guests. FCS Gateway uses the Management API to send updates to Avaya IP Office Server on the guest's name and user rights template as part of the Check-In, Check-Out, Room Move, Guest Info update process. Check-In guest are also block from outgoing calls or turn on with Do-Not-Disturb using the appropriate user rights template. The SMDR interface was used by FCS Gateway to capture calls made from room phones for the purpose of call billing.

Previous Application Notes were used as a reference, as stated in **Section 9** reference [1]. In that document, FCS Gateway used Configuration Web Services interface which will not be supported in future. Other than SMDR interface, this Compliance Testing uses the new Management API.

2. General Test Approach and Test Results

The feature test cases were performed manually. 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 or outgoing call bar. For SMDR testing, outgoing calls were made to the PSTN (simulated) and the Gateway call billing reports were verified. All these were performed on both IP Office primary server and the expansion server. The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet cable to FCS Gateway, and rebooting the Avaya IP Office server of both primary and expansion server, and FCS Gateway 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 these DevConnect Application Notes includes 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 FCS Gateway utilized enabled capabilities of TLS, specifically for Management API.

2.1. Interoperability Compliance Testing

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

- Use of Management API to update guest name and user rights template associated with Check-In, Check-Out, Do Not Disturb, outgoing Call Bar, Guest Info update, and Move requests from Gateway
- Making calls to verify guest rooms with Call Bar and Do Not Disturb activated from appropriate user rights template
- Capture calls made from room phones for the purpose of call billing for simulated local, long distance and international calls

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

2.2. Test Results

All test cases were executed and passed.

2.3. Support

Technical support on FCS Gateway 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, FCS Gateway was installed on a single server. Gateway initiates room Check-In/Check-Out, Room Move, & Guest Info update via a PMS Simulator, capture SMDR, and to set Do Not Disturb or outgoing Call Bar. In the compliance testing, Avaya IP Office Server Edition comprises of a Primary Server and an Expansion Server (IP500 V2). Avaya IP Deskphones H.323 96x1, Avaya IP Deskphones SIP 96x1/J100 Series, Avaya Digital Deskphones 1408 and Analog Deskphone are deployed as guest rooms, front desk, operator and admin phones.

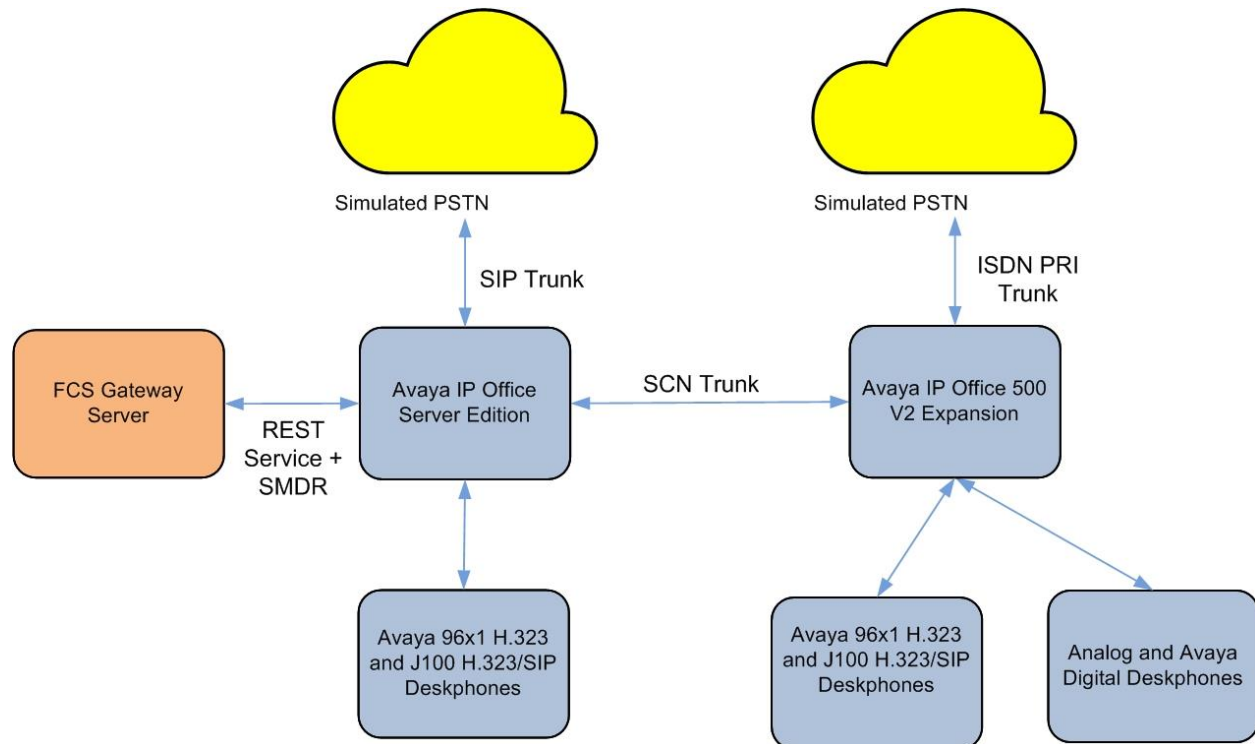


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

Below are the extensions created for the IP Office Server Edition setup.

Station Type	Extension	Server	Remarks
96x1 H.323	301	IPO Server Edition	Telephone Operator
J100 H.323	302	IPO Server Edition	Front Office (Admin)
J100 SIP	303	IPO Server Edition	Guest Room 1
96x1 H.323	333	IPO Server Edition	Guest Room 1
96x1 H.323	304	IPO Server Edition	Guest Room 2
J100 H.323	334	IPO Server Edition	Guest Room 2
96x1 H.323	601	IP500 v2 Expansion	Guest Room 3
1408 Digital	631	IP500 v2 Expansion	Guest Room 3
J100 SIP	602	IP500 v2 Expansion	Guest Room 4
Analog	632	IP500 v2 Expansion	Guest Room 4
J100 H.323	603	IP500 v2 Expansion	Admin

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition (Primary)	11.1.1.1.0 build 18 (11.1 FP1 SP1)
Avaya IP Office 500 V2 (Expansion)	11.1.1.1.0 build 18 (11.1 FP1 SP1)
Avaya IP Office Manager	11.1.1.1.0 build 18 (11.1 FP1 SP1)
Avaya 96x1 IP Deskphone (H.323)	6.8502
Avaya J100 Series IP Deskphone (SIP)	4.0.10.0.4
Avaya J100 Series IP Deskphone (H.323)	6.8502
Avaya 1408 Digital Deskphone	R4 SP10
Analog Deskphone	NA
Avaya IP Office Management API	11.0
FCS Gateway Server - FCS Gateway running on Microsoft Windows 2019 hosted on VMware 6.5 platform	2.0

** 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

It is assumed that the extensions for the admin, front office, guest rooms and telephone operator would have been setup. Note that Voice Mail was not included in the Compliance Testing and hence administration related to this will not be mentioned below. Refer to reference [1] in **Section 9** for more details.

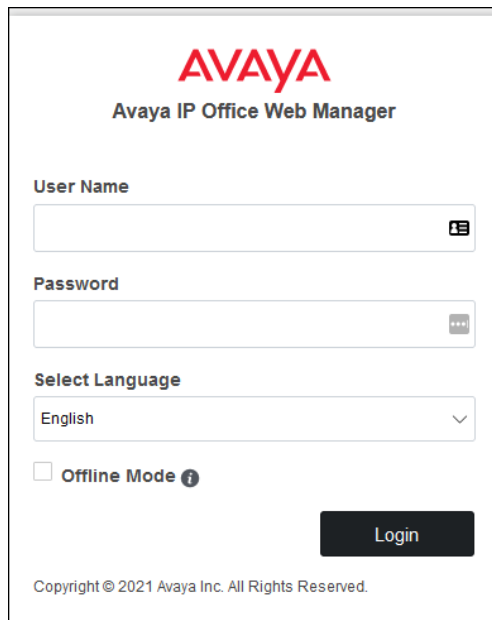
This section provides the procedures for configuring Avaya IP Office. The procedures include the following:

- Launch Avaya IP Office Web Manager
- Verify Avaya IP Office Server license
- Obtain LAN IP address
- Administer User Rights
- Create Management API service user
- Administer SMDR

5.1. Launch Avaya IP Office Web Manager

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

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



The image shows the Avaya IP Office Web Manager login interface. At the top, the Avaya logo is displayed in red, followed by the text "Avaya IP Office Web Manager". Below this, there are three input fields: "User Name" with a search icon, "Password" with a show/hide icon, and "Select Language" with a dropdown menu currently set to "English". Below the language selection is a checkbox labeled "Offline Mode" with an information icon. A dark "Login" button is positioned to the right of the "Offline Mode" checkbox. At the bottom, a copyright notice reads "Copyright © 2021 Avaya Inc. All Rights Reserved."

The home screen is shown below.

AVAYA

Solution

Call Management

System Settings

Security

Applications

Solution

SOLUTION OBJECTS ▾

View All (3)

SERVER STATUS

Online (3)

Offline (0)

SERVER TYPE

Servers (1)

Expansions (1)




Application Servers (1)

☐

Actions ▾

Configure ▾

Enter search criteria

<input type="checkbox"/>		IPOPRI	10.1.10.121	Primary: Select
<input type="checkbox"/>		005056A08841	10.1.10.108	Application Server
<input type="checkbox"/>		IPOEXP	10.1.10.110	Expansion System (V2): Select

5.2. Verify Avaya IP Office Server License

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

AVAYA		Solution	Call Management	System Settings	Security	Applications
Licenses						
System Name					System Address	
IPOPRI					10.1.10.121	
IPOEXP					10.1.10.110	

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 extensions to register to IP Office as SIP Users.

AVAYA
Solution
Call Management
System Settings
Security
Applications

License | IPOPRI

Manage Licenses
Manage Solution-Wide Licenses
Remote Server
Configure License Server

License Mode	Licensed Version	PLDS Host ID	PLDS File Status	Select Licensing
License Normal	11.0	232251352729	Valid	Valid

Enter search criteria

Feature	Instances	Status	Expiry Date	Source
Devlink3 External Recorder	1	Valid	Never	PLDS Nodal
Allow Virtualization	10	Valid	Never	PLDS Nodal
VMPro Media Manager	1	Valid	Never	PLDS Nodal
UMS Web Services	1000	Valid	Never	PLDS Nodal
Avaya Mac Softphone	1000	Valid	Never	PLDS Nodal
Server Edition	150	Valid	Never	PLDS Nodal
SM Trunk Channels	128	Valid	Never	PLDS Nodal
Receptionist	10	Valid	Never	PLDS Nodal
Additional Voicemail Pro (ports)	252	Valid	Never	PLDS Nodal
Avaya Softphone	1000	Valid	Never	PLDS Nodal
VMPro Recordings Administra...	1	Valid	Never	PLDS Nodal
CTI Link Pro	10	Valid	Never	PLDS Nodal
3rd Party IP Endpoints	1000	Valid	Never	PLDS Nodal
VMPro TTS Professional	40	Valid	Never	PLDS Nodal
Power User	2000	Valid	Never	PLDS Nodal
Office Worker	1000	Valid	Never	PLDS Nodal

5.3. Obtain LAN IP Address

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

The screenshot shows the Avaya System Configuration interface for the IPOPRI system. The left sidebar lists various system settings, with 'LAN1' selected. The main content area is titled 'System Configuration | IPOPRI' and has tabs for 'LAN Settings', 'VoIP', and 'Network Topology'. A red warning banner states: 'These settings can only be changed in Offline mode.' The 'LAN Settings' tab is active, showing the following configuration:

Field	Value
IP Address	10 . 1 . 10 . 121
IP Subnet Mask	255 . 255 . 255 . 0
Number Of DHCP IP Addresses	133
DHCP Mode	Disabled
Advanced	NO

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

The screenshot shows the Avaya System Configuration interface for the IPOEXP system. The left sidebar lists various system settings, with 'LAN1' selected. The main content area is titled 'System Configuration | IPOEXP' and has tabs for 'LAN Settings', 'VoIP', and 'Network Topology'. A red warning banner states: 'These settings can only be changed in Offline mode.' The 'LAN Settings' tab is active, showing the following configuration:

Field	Value
IP Address	10 . 1 . 10 . 110
IP Subnet Mask	255 . 255 . 255 . 0
Primary Transfer IP Address	0 . 0 . 0 . 0
RIP Mode	None
Enable NAT	NO
Number Of DHCP IP Addresses	1
DHCP Mode	Disabled
Advanced	NO

5.4. Administer SIP Registrar

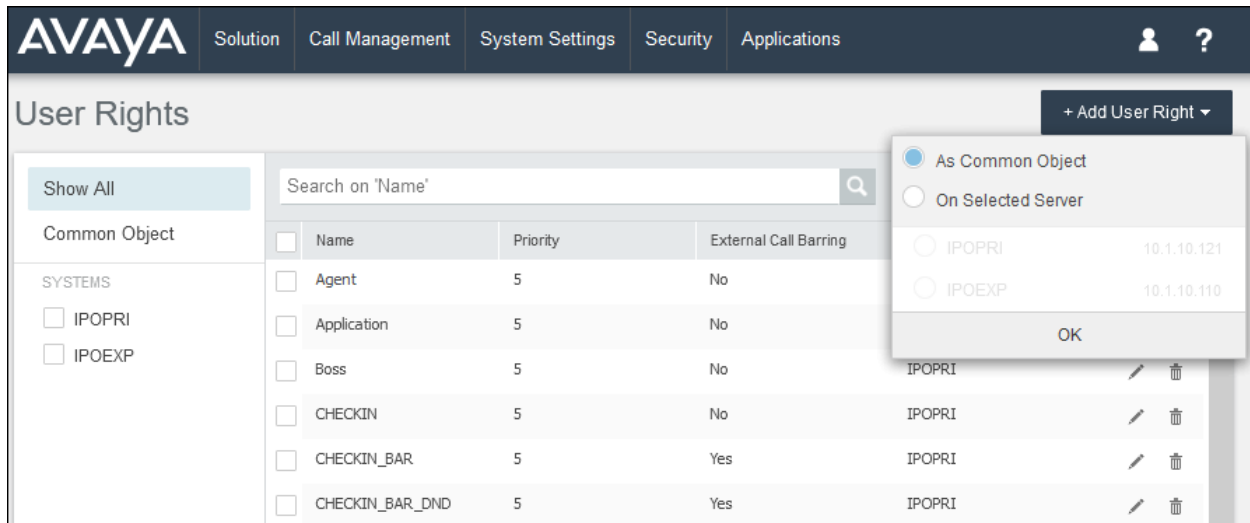
This portion of the administration required login in Offline mode as mentioned in **Section 5.1**. Select **System Settings → System → IPOPRI → LAN → VOIP**. Ensure that **SIP Registrar Enable** is set to **YES**. Enter a valid **SIP Domain Name** for SIP endpoints to use for registration with IP Office.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

The screenshot shows the Avaya System Configuration interface. The top navigation bar includes 'AVAYA', 'Solution', 'Call Management', 'System Settings', 'Security', and 'Applications'. The main header is 'System Configuration | IPOPRI'. On the left is a sidebar menu with options: System, Voicemail, System Events, SMTP, DNS, SMDR, LAN1 (selected), LAN2, VoIP, Directory Services, Telephony, Contact Center, Avaya Cloud Services, and Avaya Push Notification Services. The main content area is titled 'SIP Trunks Enable' with a 'YES' toggle. Below this is the 'SIP REGISTRAR' section, which includes 'SIP Registrar Enable' (YES), 'SIP Remote Extension Enable' (NO), 'Allowed SIP User Agents' (Block blacklist only), 'Auto-create Extension/User' (NO), 'SIP Domain Name' (sglab.com), and 'SIP Registrar FQDN' (ipopri.sglab.com). The 'Challenge Expiry Time (sec)' is set to 10. The 'LAYER 4 PROTOCOL' section includes 'UDP' (YES), 'UDP Port' (5060), 'TCP' (YES), 'TCP Port' (5060), 'TLS' (NO), and 'TLS Port' (5061).

Category	Setting	Value
SIP Trunks	SIP Trunks Enable	YES
	SIP REGISTRAR	
SIP Registrar	SIP Registrar Enable	YES
	SIP Remote Extension Enable	NO
SIP User Agents	Allowed SIP User Agents	Block blacklist only
	Auto-create Extension/User	NO
SIP Domain	SIP Domain Name	sglab.com
	SIP Registrar FQDN	ipopri.sglab.com
Challenge	Challenge Expiry Time (sec)	10
LAYER 4 PROTOCOL	UDP	YES
	UDP Port	5060
	TCP	YES
	TCP Port	5060
	TLS	NO
	TLS Port	5061

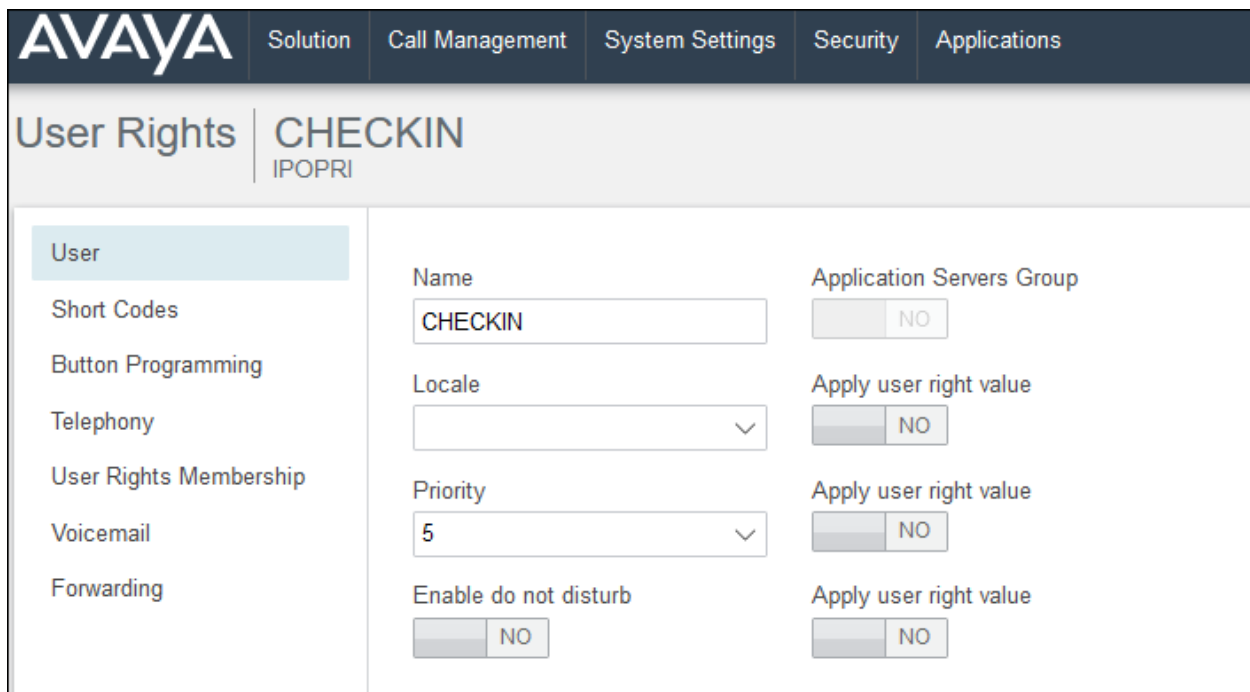
5.5. Administer User Rights

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**.



Name	Priority	External Call Barring
Agent	5	No
Application	5	No
Boss	5	No
CHECKIN	5	No
CHECKIN_BAR	5	Yes
CHECKIN_BAR_DND	5	Yes

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.



User	Name	Application Servers Group
Short Codes	CHECKIN	NO
Button Programming	Locale	Apply user right value
Telephony	Priority	Apply user right value
User Rights Membership	5	NO
Voicemail	Enable do not disturb	Apply user right value
Forwarding	NO	NO

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

CHECKIN
IPOPRI

User

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Call Settings

Supervisor Settings

Multiline Options

Call Log

Can Intrude	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Cannot be Intruded	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Deny Auto Intercom Calls	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Enable force login	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Enable force account code	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Inhibit Off-Switch Forward/Transfer	<input type="checkbox"/> NO	Apply user right value	<input type="checkbox"/> NO
Enable outgoing call bar	<input type="checkbox"/> NO	Apply user right value	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
Coverage Group	None <input type="button" value="v"/>	Apply user right value	<input type="checkbox"/> NO

During the 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 user rights is applied, i.e., when the guest Check-Out.

AVAYA		Solution	Call Management	System Settings	Security	Applications
User Rights		CHECKOUT IPOPRI				
User	Call Settings	Supervisor Settings		Multiline Options	Call Log	
Short Codes	Can Intrude	Apply user right value				
Button Programming	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
Telephony	Cannot be Intruded	Apply user right value				
User Rights Membership	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
Voicemail	Deny Auto Intercom Calls	Apply user right value				
Forwarding	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
	Enable force login	Apply user right value				
	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
	Enable force account code	Apply user right value				
	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
	Inhibit Off-Switch Forward/Transfer	Apply user right value				
	<input type="checkbox"/> NO	<input type="checkbox"/> NO				
	Enable outgoing call bar	Apply user right value				
	<input checked="" type="checkbox"/> YES <input type="checkbox"/>	<input checked="" type="checkbox"/> YES <input type="checkbox"/>				
	Coverage Group	Apply user right value				
	None <input type="button" value="v"/>	<input type="checkbox"/> NO				

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.

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

User Rights | **CHECKIN_DND**
IPOPRI

User (selected)

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Name: CHECKIN_DND

Application Servers Group: NO

Locale: [dropdown]

Apply user right value: NO

Priority: 5

Apply user right value: NO

Enable do not disturb: YES

Apply user right value: YES

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**
IPOPRI

User

Short Codes (selected)

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Apply user right value: NO

+ Add

Code	Telephone Nu...	Feature	Line Group ID	Force Accou...	Force Author...		
902N;	902N	Barred	0	No	No		
9001N;	9001N	Barred	0	No	No		

AVAYA

Solution

Call Management

System Settings

Security

Applications

?

User Rights

CHECKIN_DOM

IPOPRI

User

Short Codes

Button Programming

Telephony

User Rights Membership

Voicemail

Forwarding

Apply user right value

NO

+ Add

Code	Telephone Nu...	Feature	Line Group ID	Force Accou...	Force Author...		
9001N;	9001N	Barred	0	No	No		

The rest of the user rights will be a combination of the above. Below is the list of user rights template created for primary server. The same list will be created for expansion server.

AVAYA

Solution

Call Management

System Settings

Security

Applications

?

User Rights

+ Add User Right

Show All

Search on 'Name'

Delete

Common Object

SYSTEMS

☐ IPOPRI
 ☐ IPOEXP

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

5.6. Create Management API Service User

The IP Office Management API is a set of REST-based services which return results in XML or JSON. To consume the Management API's, a Management API service user must be created. Access to these services requires a session with the IP Office to be created by using the 'authenticate' REST service with an account and password having administrator privileges. When a session has been established, all other REST based Management APIs are available.

For the compliance testing configuration, the Primary Server provided the consolidated web services for the entire solution. There is no need to access the individual node like expansion server. Authentication for all nodes will be done against the Primary node. If the passwords are different for whatever reason, the Primary node will fail to consolidate the object data and the data from all other nodes, will not be accessible from the Primary node.

From the home menu, select **Security** → **Security Settings**. Click on the pencil icon to edit the **Primary** Server.

AVAYA


Solution


Call Management

System Settings

Security

Applications





Security Settings

Show All

System Type

☐ Primary


☐ Secondary




☐ Expansion System (L)

☐ Expansion System (V2)

☐ Application Server

Search...



System Name	System Type	System Address	
IPOPRI	Primary	10.1.10.121	
005056A08841	Application Server	10.1.10.108	
IPOEXP	Expansion System (V2)	10.1.10.110	

On the next screen, select **Service Users** (not shown) on the left pane and click **+Add Service Users**. Enter the following information. The user's name and password created here will be used for Management API access in **Section 6.2**. Click **Save** at the bottom.

- **Name** Enter username
- **Password and Confirm Password** Enter user password
- **Account status** Check that this is **Enabled**
- **Management API Group** Set to **YES**

Add Service User

BASIC OPTIONS

Name

FCSUser

Password

••••••

Confirm Password

••••••

Account status

Enabled

ACCOUNT EXPIRY

Account Expiration

NO

RIGHTS GROUPS

Administrator Group

NO

Backup Admin

NO

Business Partner

NO

Customer Admin

NO

Directory Group

NO

IPDECT Group

NO

MCM Admin

NO

Maint Admin

NO

Maintainer

NO

Management API Group

YES

Manager Group

NO

Operator Group

NO

SMCR Admin

SNMPv3 Admin

Security Admin

Cancel

Save

5.7. 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 FCS Gateway 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 the IPOPRI SMDR settings. The left sidebar contains a menu with options: System, Voicemail, System Events, SMTP, DNS, SMDR (highlighted), LAN1, and LAN2. The main content area is titled 'System Configuration | IPOPRI'. It features an 'Output' dropdown menu set to 'SMDR Only'. Below this is a section titled 'STATION MESSAGE DETAIL RECORDER COMMUNICATIONS' containing the following fields: 'IP Address' (10 . 1 . 10 . 126), 'TCP Port' (5050), 'Records to Buffer' (3000), and 'Call Splitting for Diverts' (set to NO).

Below is the configuration of SMDR for expansion server.

The screenshot shows the Avaya System Configuration interface for the IPOEXP SMDR settings. The left sidebar contains a menu with options: System, Voicemail, System Events, SMTP, DNS, SMDR (highlighted), LAN1, and LAN2. The main content area is titled 'System Configuration | IPOEXP'. It features an 'Output' dropdown menu set to 'SMDR Only'. Below this is a section titled 'STATION MESSAGE DETAIL RECORDER COMMUNICATIONS' containing the following fields: 'IP Address' (10 . 1 . 10 . 126), 'TCP Port' (5000), 'Records to Buffer' (3000), and 'Call Splitting for Diverts' (set to NO).

6. Configure FCS Gateway

This section provides the procedures for configuring FCS Gateway. The procedures include the following:

- Obtaining IP Office Management API access
- Configuring Gateway

6.1. Obtaining IP Office Management API

Avaya provides the IP Office Management API access requires a login and password created as in **Section 5.5**. Note that only the primary server login and password is required to access the whole IP Office Server Edition solution.

6.2. Configuring Gateway

This section details the essential portion of the Gateway configuration to interoperate with IP Office. These Application Notes assume that the Gateway application has already been properly installed by a qualified FCS Engineer.

1. To enable Gateway Interface configuration for **AvayaIPOWSC.PBX**, **AvayaIPOWSC.PBX_Expansion**, **AvayaIPO-CDR** and **AvayaIPO-CDR_Expansion**, use **FCSGateway.xml** located in the “C:\Program Files (x86)\FCS\Gateway\Control\” directory. Note that these interface configuration names are created for ease of identifying the object and varies according to installation.

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

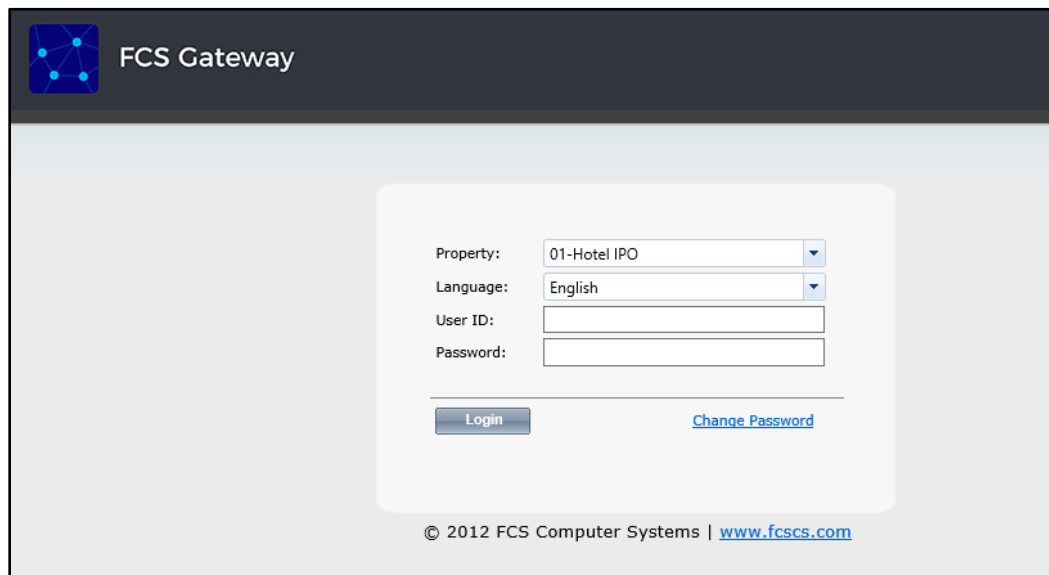
```
<Child Id="PBX1">
  <PropertyId>01</PropertyId>
  <LogFilePattern>PBX\PBX1-</LogFilePattern>
  <EXENAME>AvayaIPOWSC.PBX.exe</EXENAME>
  <Description>AvayaIPOWSC.PBX.exe</Description>
  <XMLFile>AvayaIPOWSC.PBX.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX1In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX1Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>9998</UnicornMotherIPPort>
  <MemoryPage>10</MemoryPage>
</Child>
<Child Id="PBX2">
  <PropertyId>01</PropertyId>
  <LogFilePattern>PBX\PBX2-</LogFilePattern>
  <EXENAME>AvayaIPOWSC.PBX_Expansion.exe</EXENAME>
  <Description>AvayaIPOWSC.PBX_Expansion.exe</Description>
  <XMLFile>AvayaIPOWSC.PBX_Expansion.xml</XMLFile>
  <IntfInQueueName>.\Private$\PBX2In</IntfInQueueName>
  <IntfOutQueueName>.\Private$\PBX2Out</IntfOutQueueName>
  <IntfOutQueueFilterThresholdInHour>99999</IntfOutQueueFilterThresholdInHour>
  <UnicornMotherIPPort>9990</UnicornMotherIPPort>
  <MemoryPage>11</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>AvayaIPO.CDR Interface </Description>
  <XMLFile>AvayaIPO-CDR.xml</XMLFile>
  <IntfInQueueName>.\Private$\CDR1In</IntfInQueueName>
  <!--can be a remote MSMQ queue-->
  <IntfOutQueueName>.\Private$\CDR1Out</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 me
  <UnicornMotherIPPort>4001</UnicornMotherIPPort>
  <MemoryPage>6</MemoryPage>
</Child>
<Child Id="CDR2">
  <PropertyId>01</PropertyId>
  <LogFilePattern>CDR\CDR2-</LogFilePattern>
  <EXENAME>AvayaIPO.CDR_Expansion.exe</EXENAME>
  <!--can be a remote child ; need to insert full path \\192.168.2.1\Unicorn\Fidelio.exe-->
  <Description>AvayaIPO.CDR Expansion Interface </Description>
  <XMLFile>AvayaIPO-CDR_Expansion.xml</XMLFile>
  <IntfInQueueName>.\Private$\CDR2In</IntfInQueueName>
  <!--can be a remote MSMQ queue-->
  <IntfOutQueueName>.\Private$\CDR2Out</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 me
  <UnicornMotherIPPort>4002</UnicornMotherIPPort>
  <MemoryPage>7</MemoryPage>
</Child>

```

- 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 a logo with a blue square and white dots. To its right is the text "FCS Gateway". Below this is a large white box containing a login form. The form has four fields: "Property:" with a dropdown menu showing "01-Hotel IPO", "Language:" with a dropdown menu showing "English", "User ID:" with a text input field, and "Password:" with a text input field. Below the 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".

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

```
<!--
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>8</InterfaceType>

<!--START: get credentials of IPO -->
<InterfaceSetting>https://10.1.10.121:7070/WebManagement/ws/sdk/security/authenticate</InterfaceSetting>
<!--END: get credentials of IPO -->

<!--START: perform actions -->
<InterfaceSetting2>https://10.1.10.121:7070/WebManagement/ws/sdk/admin/v1</InterfaceSetting2>
<!--END: perform actions -->
```

In order to begin using the API Administration and Configuration REST services, a session must be established with IP Office. A session is created using the following REST API. Refer to reference [2] in **Section 9** for details.

Method: GET

Description: REST service which creates a session with the IP Office.

URI: https://{host}:7070/WebManagement/ws/sdk/security/authenticate

Accept: text/xml

Headers:

X-User-Client: Avaya-WebAdmin

X-User-Agent: Avaya-SDKUser

Content-Type: application/xml OR application/json.

Authorization: The username and password are combined into a string with the format "username:password", which is then base64 encoded.

Note, the **host** mentioned above is the IP Office Primary Server IP address. Note that the **AvayaIPOWSC.PBX_Expansion.xml** has the same configuration since only the Primary Server node is needed for the Web services as explain earlier in **Section 5.5**.

The **LoginUserName** and **LoginPassword** are defined in the later part of the xml file as shown below. The password is not revealed for security reasons. The user's name and password were created earlier in **Section 5.5** in IP Office.

```
<DeviceDependentSetting>
  <!-- IPO API username -->
  <LoginUserName>FCSUser</LoginUserName>
  <!-- IPO API password -->
  <LoginPassword>FCSUser</LoginPassword>
  <ReceiveTimeout>5</ReceiveTimeout>
  <DefaultPid>01</DefaultPid>
  <GetSlaveExtn>Yes</GetSlaveExtn>
  <FixedCOSDND>Yes</FixedCOSDND>

  <URL_getusers>users</URL_getusers>

  <!-- below is used for expansion server -->
  <!--<URL_getusers>users/?ipaddress=10.1.10.110</URL_getusers>-->
</DeviceDependentSetting>
```

5. 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 for the IP Office Primary Server. The host is set as **tcp.ip** type listening to port **5050**. This corresponds with the setup of IP Office SMDR port at **Section 5.6**.

```
<PBX ID="CDR1">
  <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,10.1.10.126:5050</InterfaceSetting>
```

Similarly, the **AvayaIPO-CDR_Expansion.xml** located in the “C:\Program Files (x86)\FCS\Gateway\Control\” directory define the CDR interface module & data configuration for the expansion server.

```
<PBX ID="CDR2">
  <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,10.1.10.126:5000</InterfaceSetting>
```

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

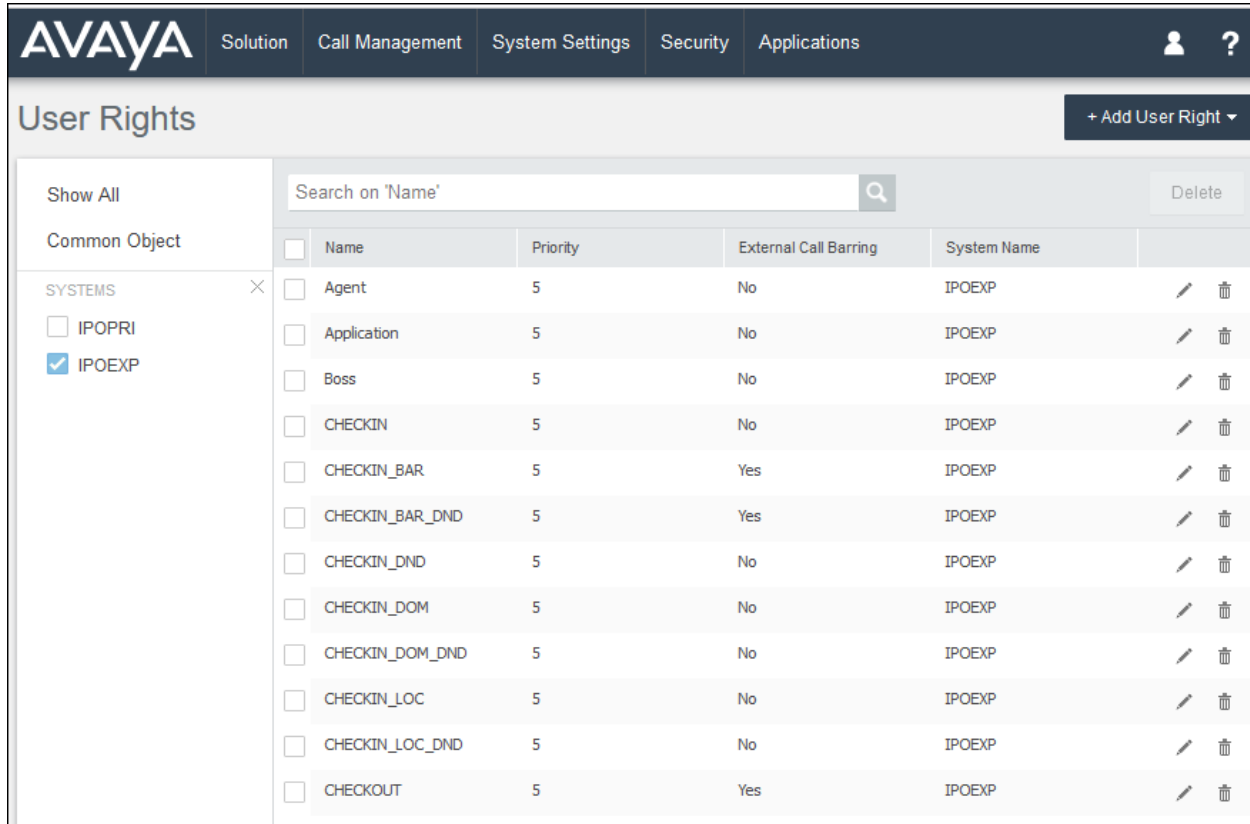
7. Click **Configuration** → **Extensions** and select **Primary Extension Numbering** or **Slave Extension** to view the extensions configured with each room.

7. Verification Steps

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

7.1. Verify Management API Integration

Use a simulator to perform a guest Check-In request. From the home menu of the IP Office Web Manager, select **System Settings** → **User Rights**. Select the appropriate node on the left pane and click on the pen icon for **CHECKIN** box on the right pane.



The screenshot displays the Avaya IP Office Web Manager interface. The top navigation bar includes the Avaya logo and tabs for Solution, Call Management, System Settings, Security, and Applications. The 'System Settings' tab is active, and the 'User Rights' page is shown. On the left, under 'Common Object', the 'IPOEXP' system is selected. The main table lists various user rights, with 'CHECKIN' highlighted. Each row includes a checkbox, a name, a priority, an external call barring status, a system name, and edit/delete icons.

Show All		Search on 'Name'				Delete	
Common Object		<input type="checkbox"/>	Name	Priority	External Call Barring	System Name	
SYSTEMS		<input type="checkbox"/>	Agent	5	No	IPOEXP	
<input type="checkbox"/> IPOPRI		<input type="checkbox"/>	Application	5	No	IPOEXP	
<input checked="" type="checkbox"/> IPOEXP		<input type="checkbox"/>	Boss	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN_BAR	5	Yes	IPOEXP	
		<input type="checkbox"/>	CHECKIN_BAR_DND	5	Yes	IPOEXP	
		<input type="checkbox"/>	CHECKIN_DND	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN_DOM	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN_DOM_DND	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN_LOC	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKIN_LOC_DND	5	No	IPOEXP	
		<input type="checkbox"/>	CHECKOUT	5	Yes	IPOEXP	

Click on the **User Rights Membership** on the left pane. Verify on the right pane that the appropriate rooms are Check-In and that physically the guest's name is updated on the phone display (depending on phone type). Guest name can also be checked by selecting **Call Management → Users** and look for the extension **Full Name**. Repeat this check for all nodes and in this compliance test, there are 2 nodes i.e., primary and expansion server.

Name	Extension
<input checked="" type="checkbox"/> Guest Room 3-1	601
<input type="checkbox"/> BTRemoteIPO	388
<input type="checkbox"/> Guest Room 4-1	602
<input type="checkbox"/> NoUser	
<input checked="" type="checkbox"/> Guest Room 3-2	631
<input type="checkbox"/> Test Room	633
<input type="checkbox"/> Admin	603
<input type="checkbox"/> Guest Room 4-2	632

Name	Extension
The list is empty.	

7.2. Verify SMDR

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. Repeat this check for the other nodes in the solution and in this compliance test, there are 2 nodes i.e., primary and expansion server.

```

10:12:38,0|IP.Any:5000|LISTENING
10:17:27,1|10.1.10.110:5000|CONNECTED(10.1.10.110:5000)
10:17:27,1|10.1.10.110:5000|>2021/12/03 10:17:10,00:00:00,12,601,0,602,602,,1,1000094,0,E601,Guest Room 3-1,E602,Gue
10:51:13,1|10.1.10.110:5000|>2021/12/03 10:50:53,00:00:14,2,601,0,603,603,,1,1000096,0,E601,Guest Room 3-1,E603,Admi
10:52:58,1|10.1.10.110:5000|>2021/12/03 10:52:42,00:00:13,3,301,I,601,601,,1,1000097,0,E301,Operator,E601,Guest Room
10:54:14,1|10.1.10.110:5000|>2021/12/03 10:53:54,00:00:14,3,601,0,301,301,,1,1000098,0,E601,Guest Room 3-1,E301,Oper
  
```

8. Conclusion

These Application Notes describe the configuration steps required for FCS Gateway to successfully interoperate with Avaya IP Office Server Edition R11.1 using the Management API and SMDR interfaces. All features and serviceability test cases were completed with observation noted in **Section 2.2**.

9. Additional References

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

- [1] *Application Notes for Configuring FCS WinExpress 3.1.2 with Avaya IP Office 11.1*, dated Jul 2020
- [2] *IP Office 11.0 Management API Developer Reference Guide*, Issue 2.0, dated May 2018
- [3] *FCS Gateway v2 – User Manual*, dated Dec 2018
- [4] *FCS Gateway Installation Manual (Windows Server 2016/2019)*, dated Aug 2020.

©2021 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.