



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

---

### **Application Notes for Configuring Avaya IP Office Server Edition Release 10 with Connected Guests iCharge Version 50.2 - Issue 1.0**

#### **Abstract**

These Application Notes describe the configuration steps required for Avaya IP Office Server Edition with Connected Guests iCharge.

Readers should pay attention to section 2, in particular the scope of testing as outlined in Section 2.1 as well as the 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

Connected Guests iCharge (iCharge) is a graphical hospitality and call logging user interface. It is commonly used in hotels to provide a means of controlling usage of room facilities. The iCharge utilizes XML based communication for hospitality control of the IP Office. Hospitality features are translated into a set of XML commands which are passed via a secure IP port to the IP Office while call logging feature uses the Station Message Detail Recording (SMDR) records from Avaya IP Office to track phone calls and produce detailed reports.

Avaya IP Office Server Edition solution consists of a primary Linux Server Edition and a 500V2 expansion. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and user names. This allows calls between systems and support for a range of internal call features.

## 2. General Test Approach and Test Results

The general test approach was to configure the iCharge to communicate with the Avaya IP Office Server Edition (IPO SE) as implemented on a customer's premises. Feature functionality testing was performed manually.

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

### 2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of iCharge to carry out hospitality functions through XML based communication with IPO SE.

The hospitality feature testing included: Check-In, DDI, Do Not Disturb (DND), Update Name, Room Transfer, Telephone Service Class, Check-out, and Room/Maid Status.

The call logging feature testing focused on verifying the proper parsing and displaying of SMDR data call scenarios including internal, voicemail, inbound PSTN, outbound PSTN, hold, reconnect, transfer, forward and conference.

The serviceability testing introduced failure scenarios to see if Connected Guests iCharge could resume after a link failure with IPO SE.

## 2.2. Test Results

Tests were performed to ensure full interoperability between Connect Guests iCharge and IP Office Server Edition. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with following observations:

- Avaya IP Office release 9.1 introduced changes in the SMDR logger related to IP Office Server Edition. Four fields 31, 32, 33, and 34 in the SMDR log identify calls made through the IP Office Line IP trunks in Small Community Network (SCN) solution, but the current version of iCharge does not use these 4 fields to associate calls made through the IP Office Line IP trunk. Therefore, the iCharge generates report on calls across a SCN solution by duplicating call record. For example, consider the case of an outgoing PSTN call initiated from a user in the IPO Server Edition Linux server going through the IP Office Line and exiting through the PRI trunk in the IPO 500V2 expansion to PSTN. This is one outgoing external call but the iCharge reports this call as two outgoing external calls: one call record in the IPO primary and another call record in the 500V2 expansion.
- The DDI feature which allocates a hunt group number to a room extension as checked-in was not working during the testing. This feature is being developed and will be added in a future release of iCharge.

## 2.3. Support

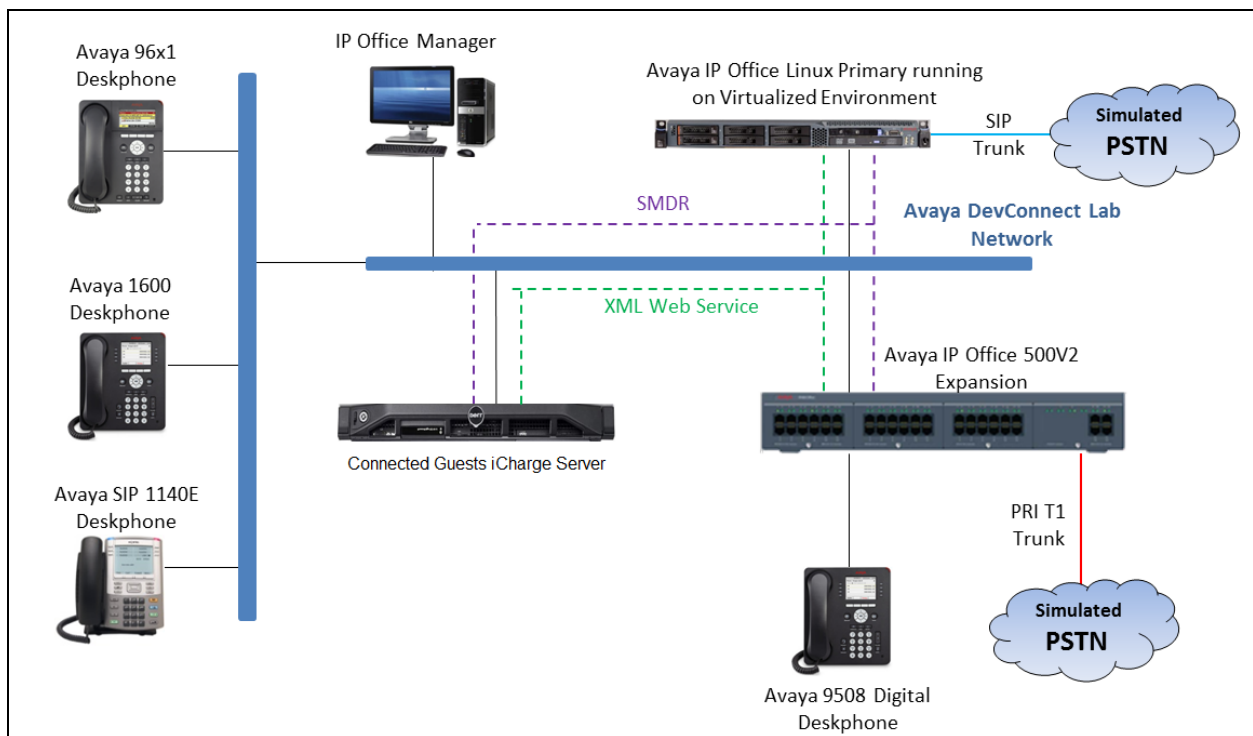
Technical support from Connected Guests iCharge can be obtained through the following:

Phone:            Technical Support Department  
                     +44 1425 891 090

Website: <http://www.innovationtw.com/support.php>

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya IP Office solution consists of an IP Office Linux primary and a 500V2 expansion which has a TCP/IP link established to the Connected Guests iCharge server. From the iCharge server, XML commands were passed via secure IP port on the IP Office Server Edition solution for replication of the hospitality features. Digital, H323 and Softphones were configured on the IP Office to generate outbound/inbound calls to/from the PSTN and also simulate Hotel room phones. PRI T1 trunk from the 500V2 expansion and SIP trunk in the primary were configured to connect to the simulated PSTN.



**Figure 1: Avaya IP Office Server Edition Solution and Connected Guests iCharge Reference 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 Running on Virtualized Environment	10 SP3 (10.0.0.3 build 53)
Avaya IP Office 500 V2 Expansion	10 SP3 (10.0.0.3 build 53)
Avaya IP Office Manager	10 SP3 (10.0.0.3 build 53)
Avaya 96x1 H323 Telephone	6.641
Avaya 1140E SIP Telephone	04.04.23.00
Avaya 1160 H323 Telephone	1.380B
Avaya 9508 Digital Telephone	R15
Avaya IP Office Web Service SDK	10.0.0.3
<b>TigerTMS Equipment</b>	<b>Software / Firmware Version</b>
Generic Server running Windows 7 SP1	Connected Guests iCharge 50.3

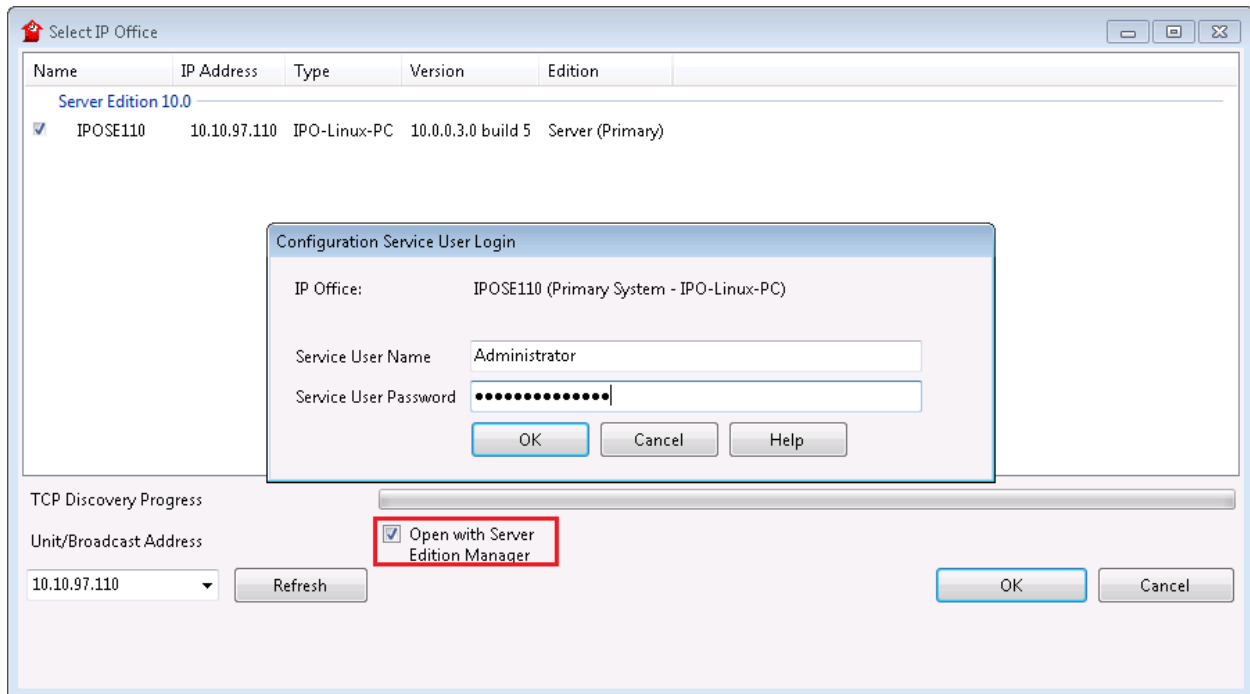
## 5. Avaya IP Office Configuration

Configuration and verification operations on the Avaya IP Office Server Edition solution illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of the Avaya IP Office for this solution. It is implied a working system is already in place and all Users/Extensions are configured including DDI, and Room Status. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

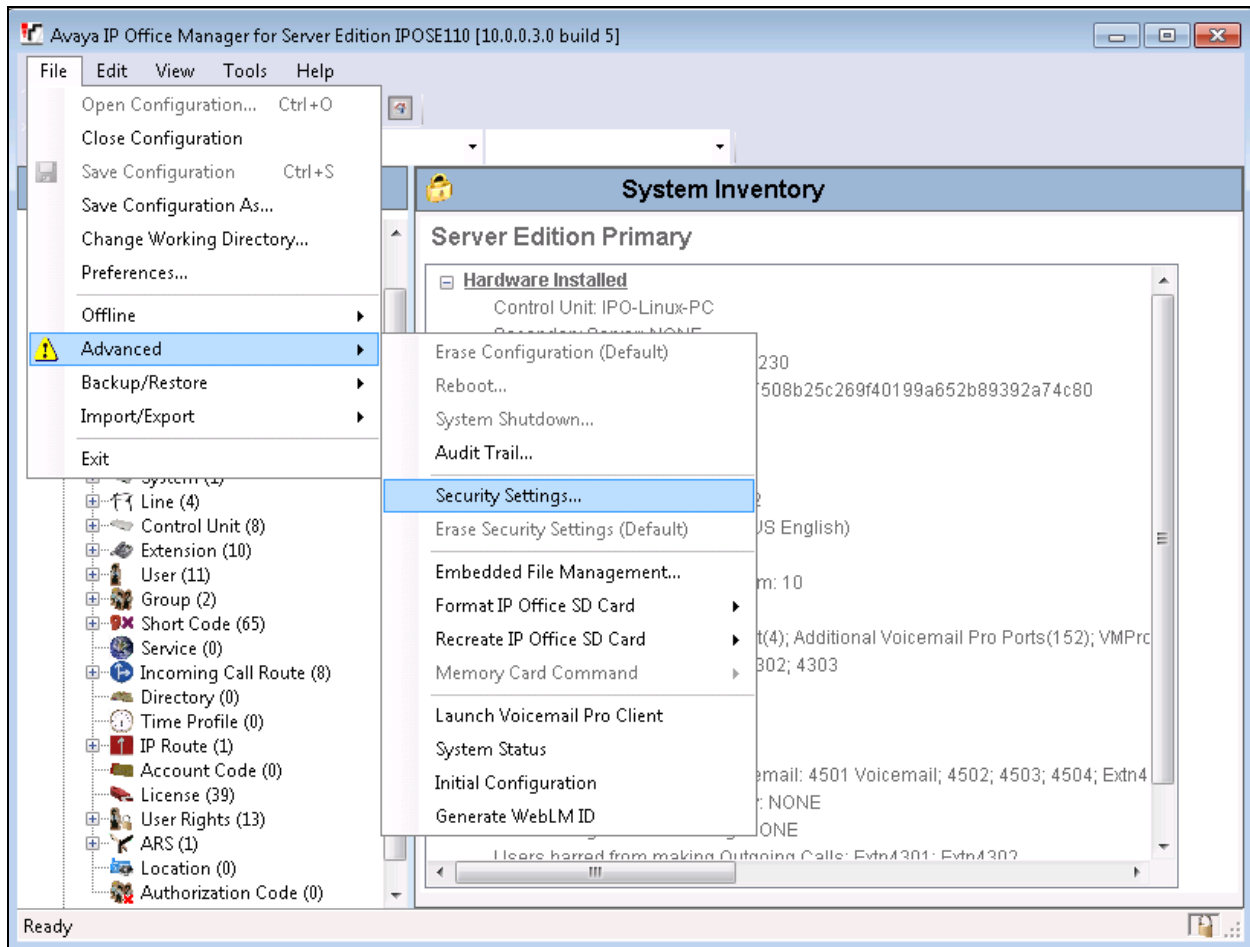
- Launch Avaya IP Office Manager (Security)
- Security Level
- Launch Avaya IP Office Manager (Administration)
- Modify User Rights Barred and BarredDND
- Modify User Rights Unbarred and UnbarredDND
- Create DDI Hunt Groups
- Configure SMDR
- Save Configuration

## 5.1. Launch Avaya IP Office Manager (Security)

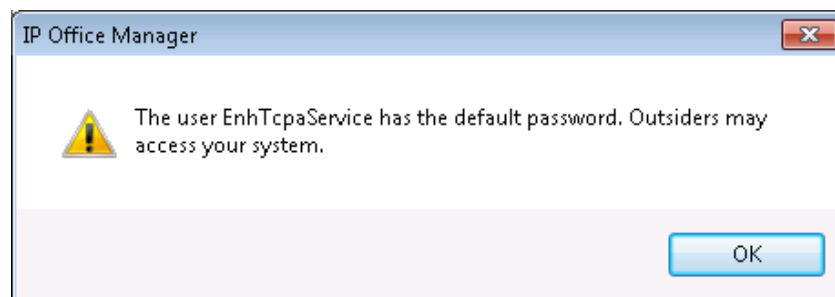
To Log in as a Security administrator, first Log in as Administrator. From the IP Office Manager PC, go to **Start→Programs→IP Office→Manager** to launch the Manager application. Select **File →Open Configuration** then select the appropriate IP Office. Log in to IP Office using the **Service User Name** of **Administrator** and the appropriate **Service User Password** and click on the **OK** button. During compliance testing the System was called **IPOSE110**. Note that the check box **Open with Server Edition Manager** should be checked if logging on the Server Edition primary.




Once the Configuration is opened select **File → Advanced → Security Settings**.

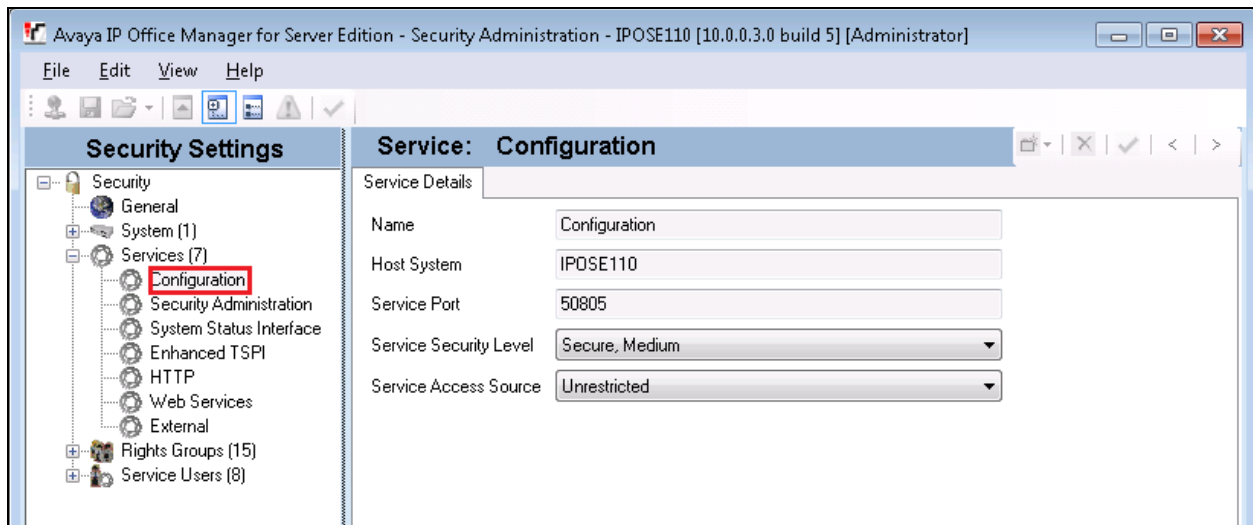


The IP Office Manager popup window displays a warning message regarding the default password of the user EnhTcpaService, click **OK** button to continue.

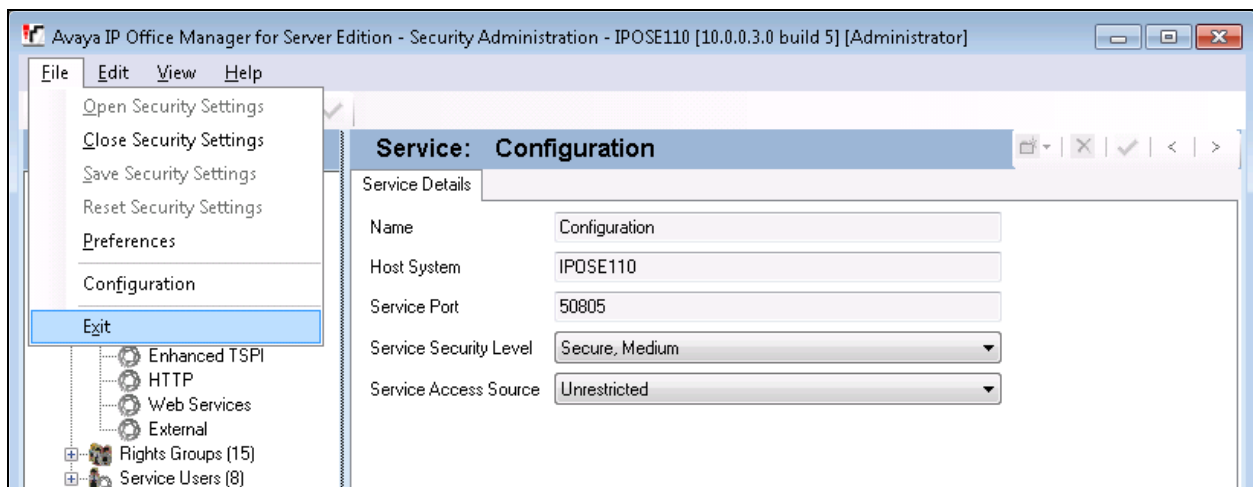


## 5.2. Security Level

Once the **Security Administration** page opens, select **Services** → **Configuration** and select **Secure, Medium** from the **Service Security Level** drop-down box and click on the **OK** button (not shown). Click on the **Save** icon  on the top of the window to save the new setting and enter the appropriate **Service User Name** and **Service User Password** and click on **OK** button to complete (not shown).

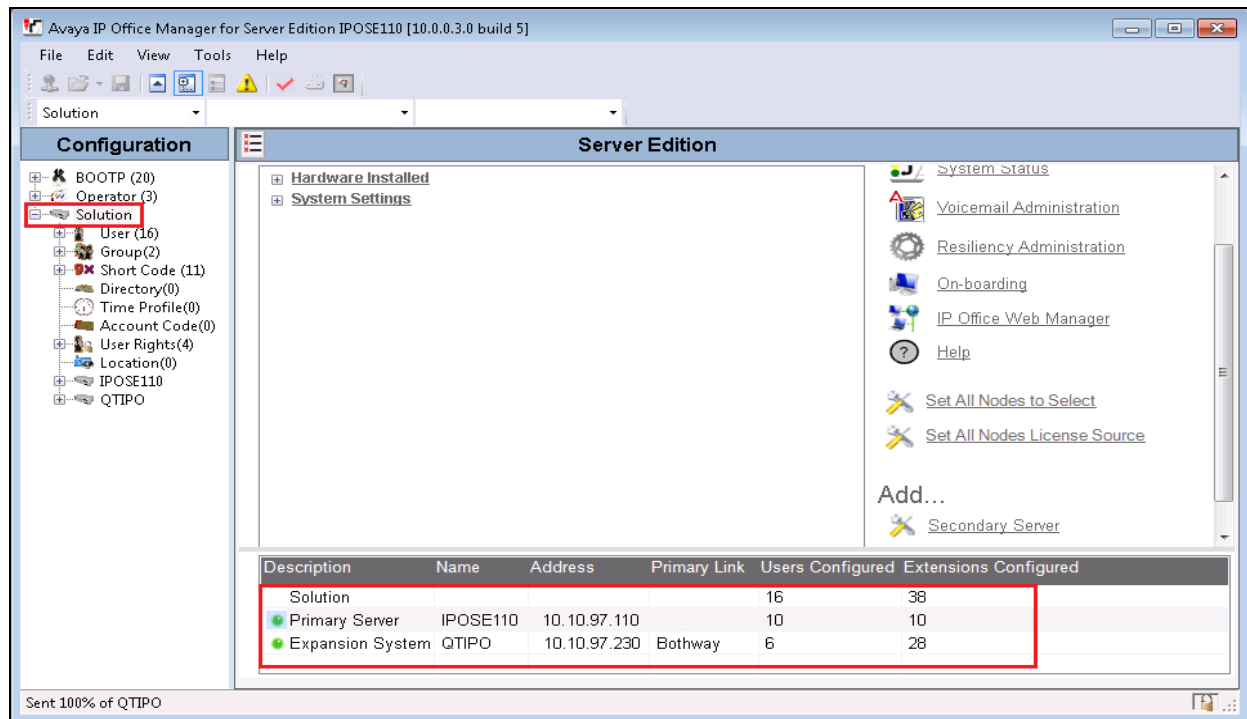


To log out of the **Security Administration** click **File** → **Exit**.



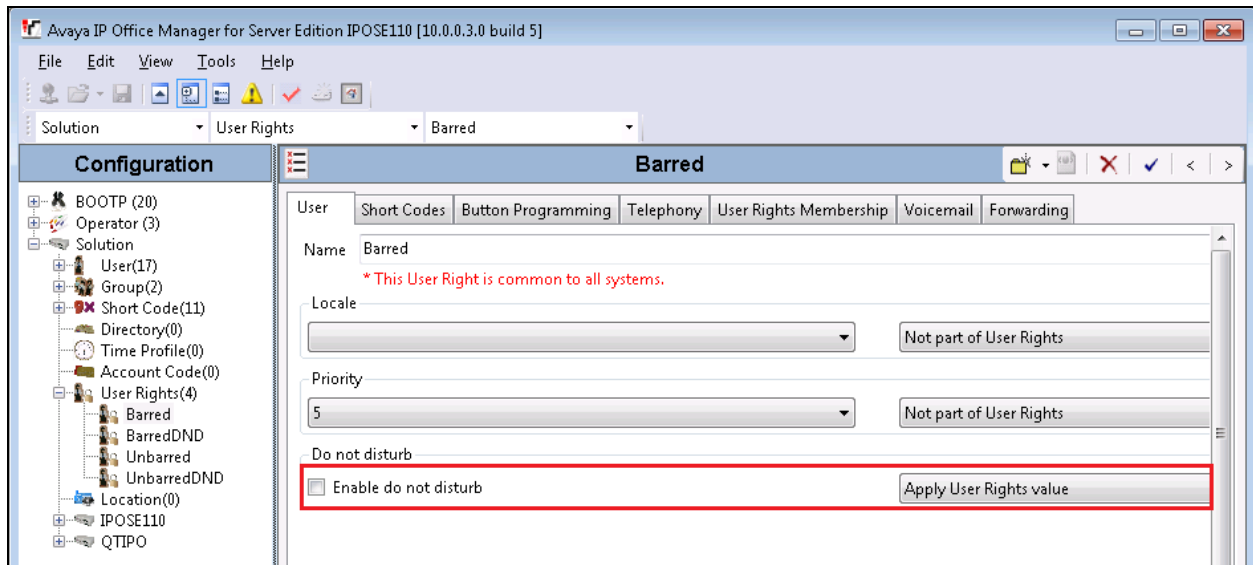
### 5.3. Launch Avaya IP Office Manager (Administration)

From the IP Office Manager PC, click **Start→Programs→IP Office→Manager** to launch the Manager application. Log in to IP Office using the appropriate credentials (not shown) to receive the IP Office configuration.

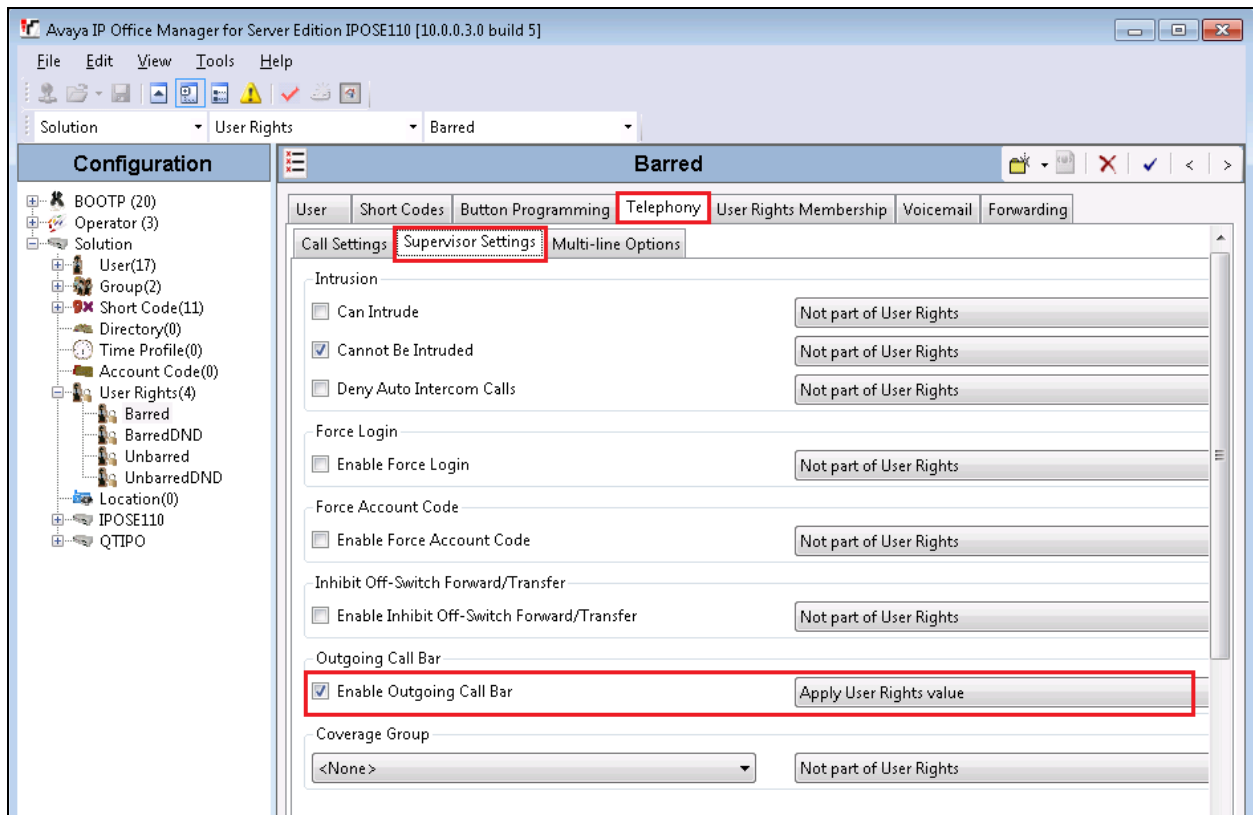


## 5.4. Create User Rights – Barred and BarredDND

In the Manager window, navigate to **Solution** → **User Rights**. Right click on **User Rights**, and select the **New** option (not shown). When the New User Rights window appears click on the **User** tab. In the **Name** field set value **Barred**. Select **Apply User Rights value** from the drop-down menu in the **Enable do not disturb** field.



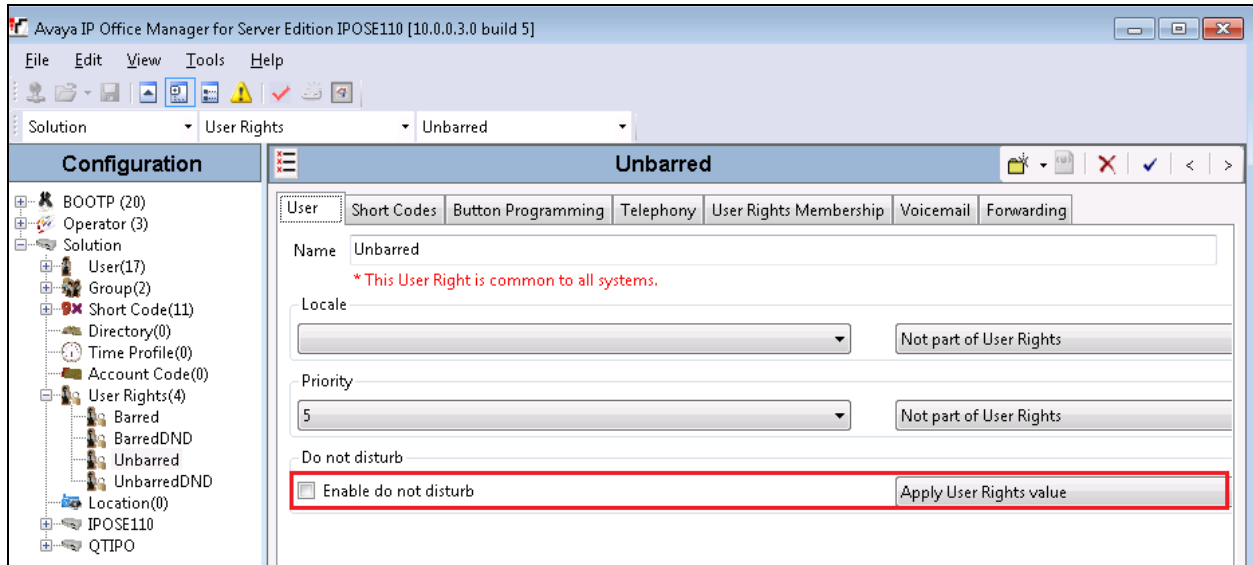
Click on the **Telephony** tab followed by the **Supervisor Settings** tab. In the **Outgoing call bar** section check the **Enable outgoing call bar** check box and select **Apply User Rights** value from the drop-down box. Click the **OK** button.



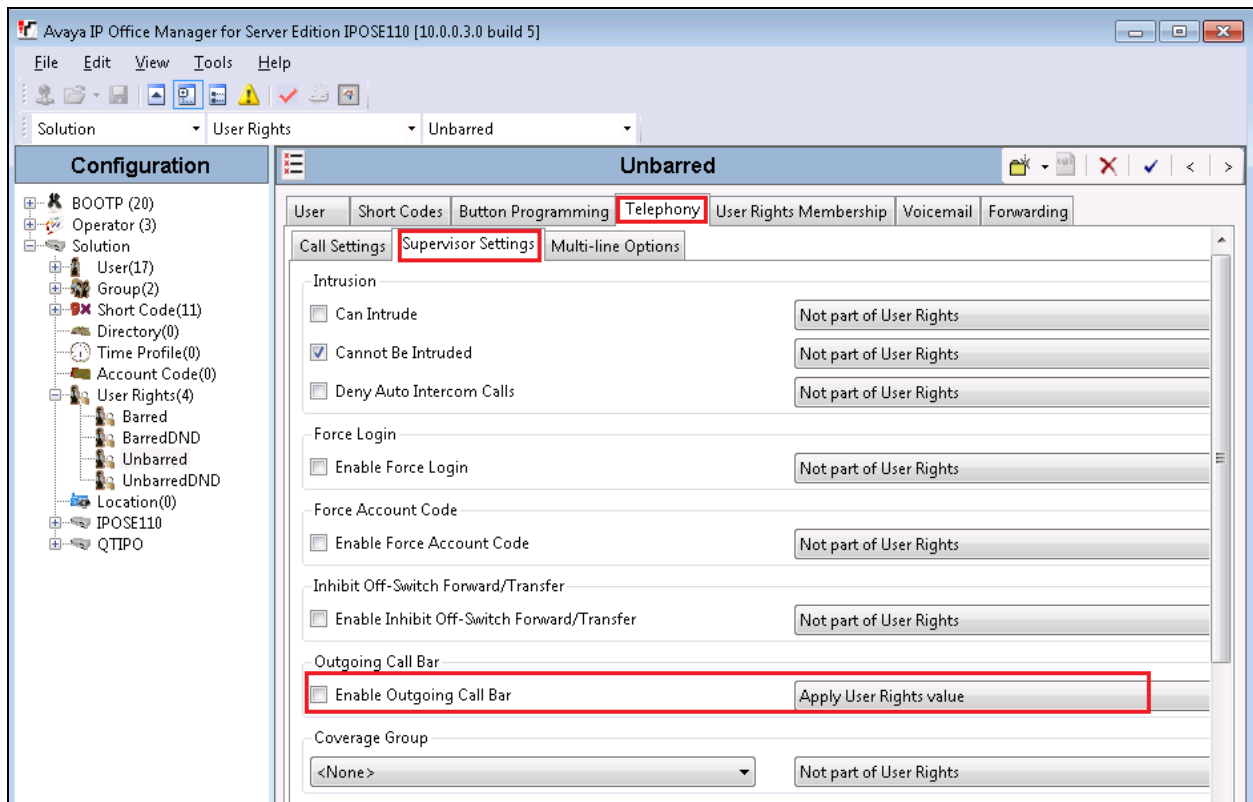
Repeat this procedure to create the **BarredDND** user right, in this user right the **Enable do not disturb** field must be checked in the **Apply User Rights** value field in the **User** tab

## 5.5. Create User Right – Unbarred and UnbarredDND

In the Manager window, navigate to **Solution → User Rights**. Right click on **User Rights**, and select the **New** option (not shown). When the New User Rights window appears click on the **User** tab. In the **Name** field, set value **Unbarred**. Select **Apply User Rights value** from the appropriate drop-down boxes.



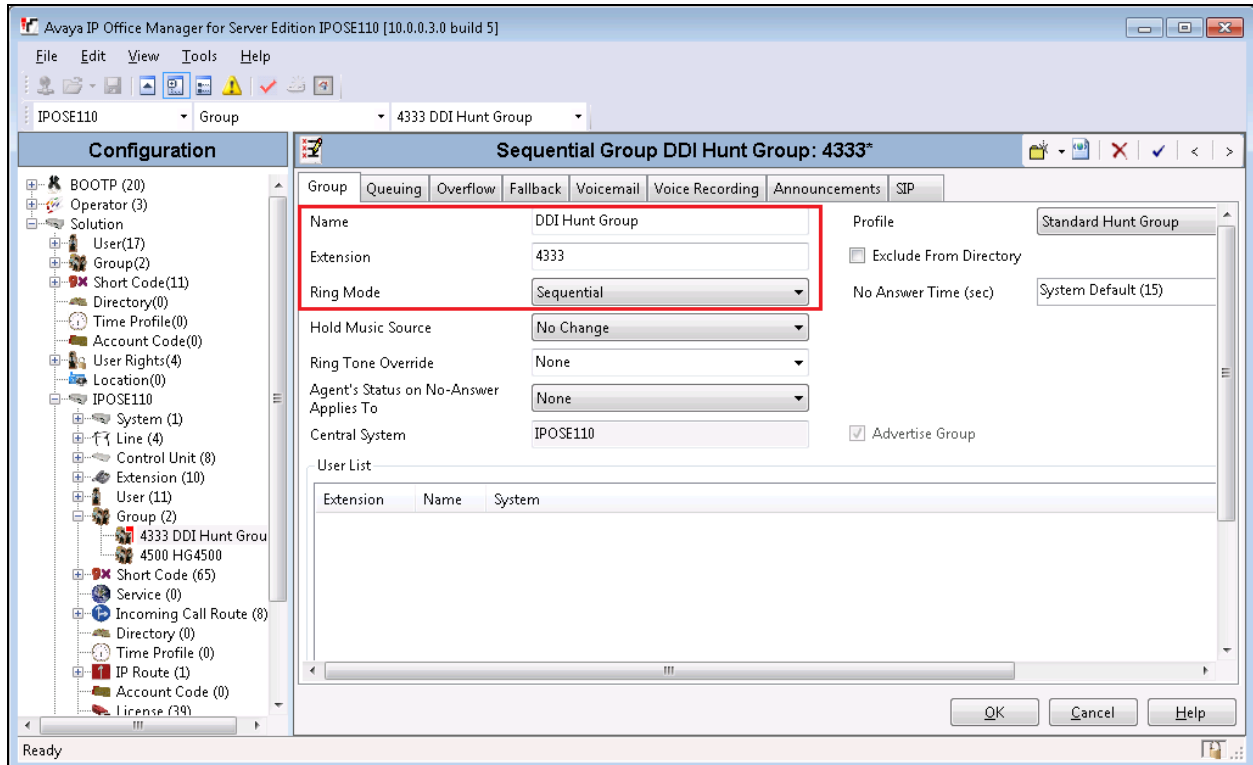
Click on the **Telephony** tab followed by the **Supervisor Settings** tab. In the **Outgoing call bar** section uncheck the **Enable outgoing call bar** check box and Select **Apply User Rights** value from the drop-down box. Click the **OK** button.



Repeat this procedure to create the **UnbarredDND** user right, in this user right the **Enable do not disturb** field must be checked in the **Apply User Rights** value field in the **User** tab.

## 5.6. Create DDI Hunt Groups

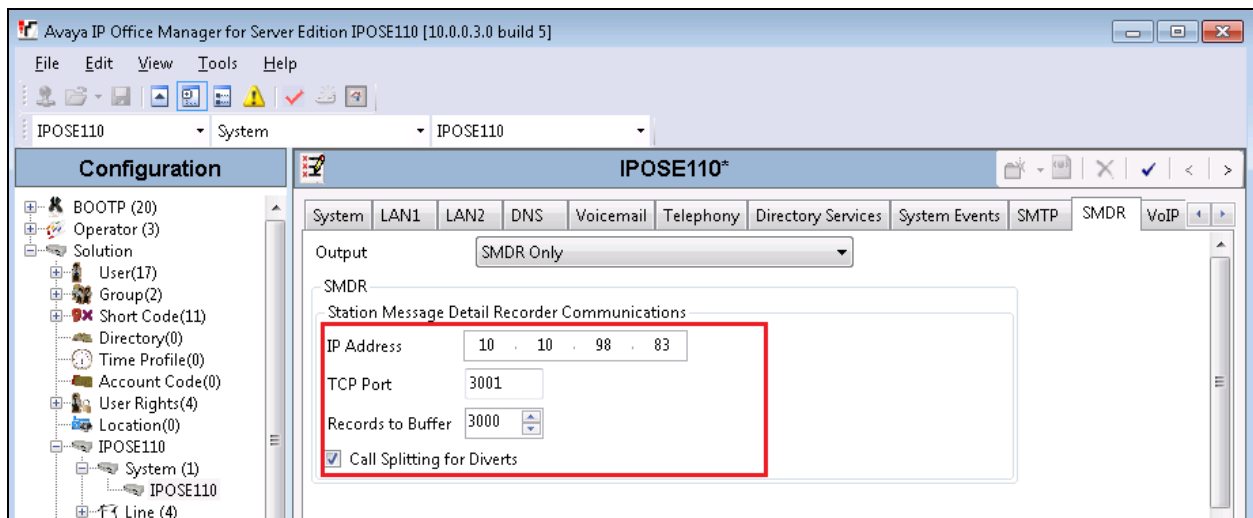
In the Manager window, navigate to **IPOSE110 → Group**, right-click **Group** and select **New** in the popup that appears (not shown). In the subsequent Hunt Group window, set **Name** to something appropriate (e.g. **DDI Hunt Group**). Enter an **Extension** (e.g. **4333**) and for **Ring Mode** select **Sequential** from drop-down box. Ensure that no extensions are added to the **User List** as they will be automatically added by the iCharge once a DDI is allocated to an extension. Click the **OK** button. Note: repeat this for each DDI required.



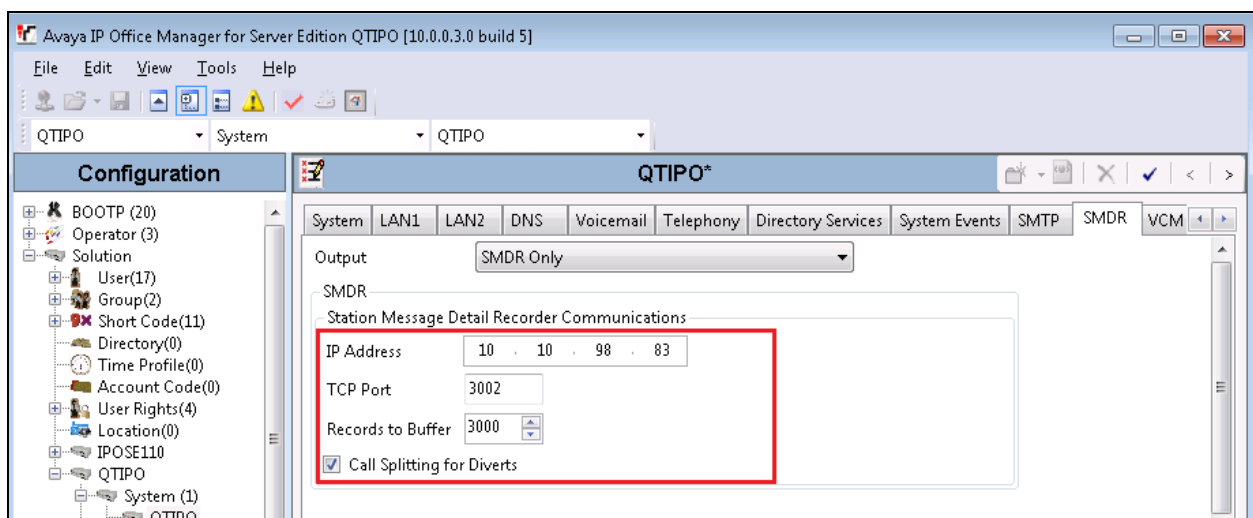
## 5.7. Configure Station Message Detail Recording (SMDR)

In the Manager window, navigate to **IPOSE VM1 → System → IPOSE110** to display the Server Edition screen in the right pane. Select the **SMDR** tab. Select “SMDR Only” from the **Output** drop-down list, to display the SMDR sub-section.


For IP Address, enter the IP address 10.10.98.83 which is the IP address of iCharge. For TCP Port, enter a desired port supported by the iCharge, in this case the port **3001** inputted. Modify Records to Buffer to the desired value, and check **Call Splitting for Diverts**. The record buffer is used by IP Office to cache SMDR records in case of communication failure with the iCharge. Click OK button to save the configuration.

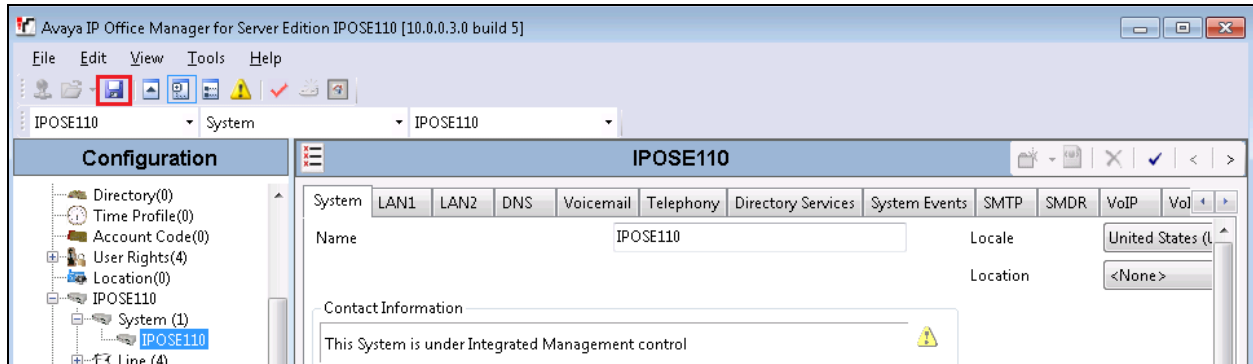


Repeat the steps above to configure SMDR in the QTIPO expansion, the TCP Port **3002** was used in the SMDR of the IPO expansion.

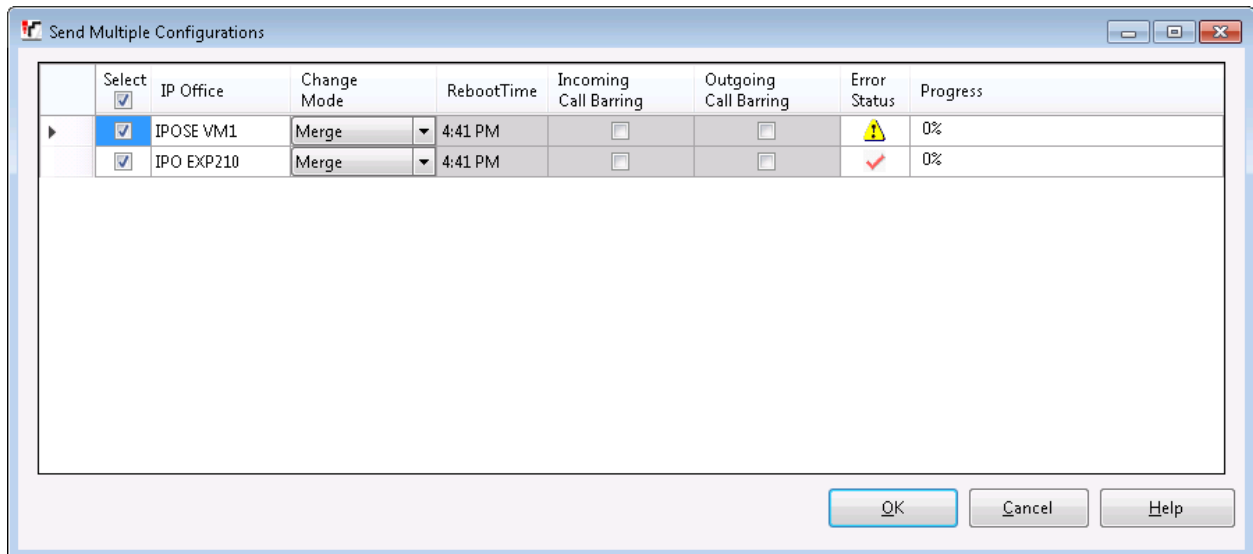


## 5.8. Save Configuration

Once all the configurations have been made it must be sent to the IP Office. Click on the **Save** icon  as shown in the picture below.



Once the **Save Configuration** window opens, click on the **OK** button.



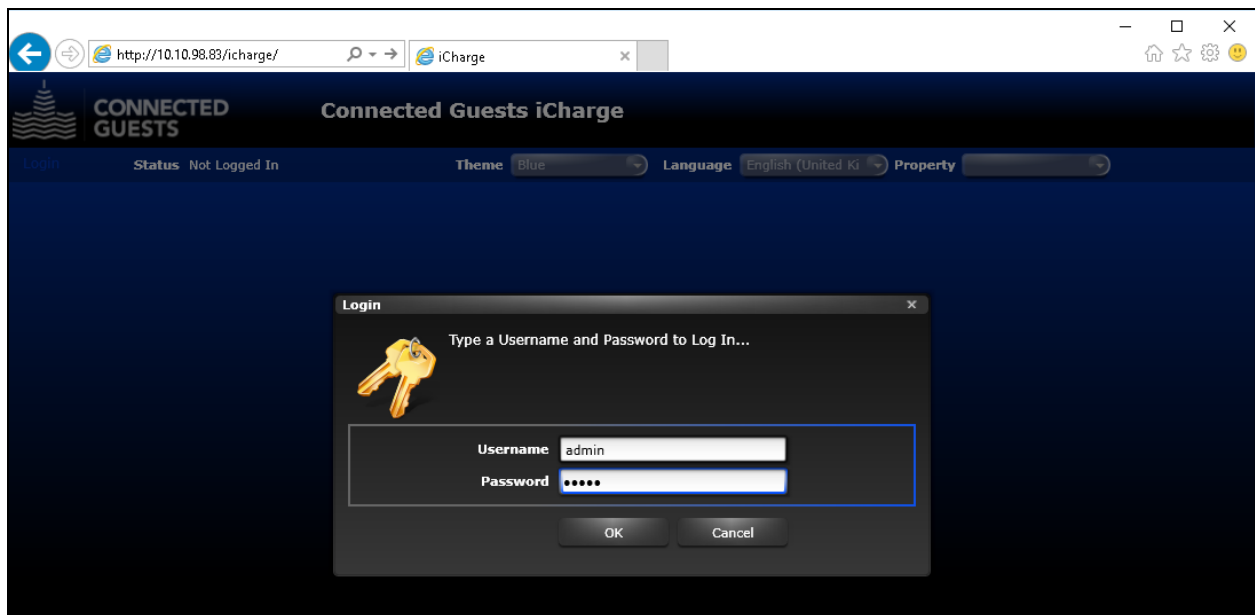
## 6. Configure Connected Guests iCharge

The configuration of Connected Guests iCharge system is done by Connected Guests engineer and is outside of the scope of these Application Notes. To obtain further information on Connected Guests iCharge system configuration please contacts an authorized Connected Guests representative.

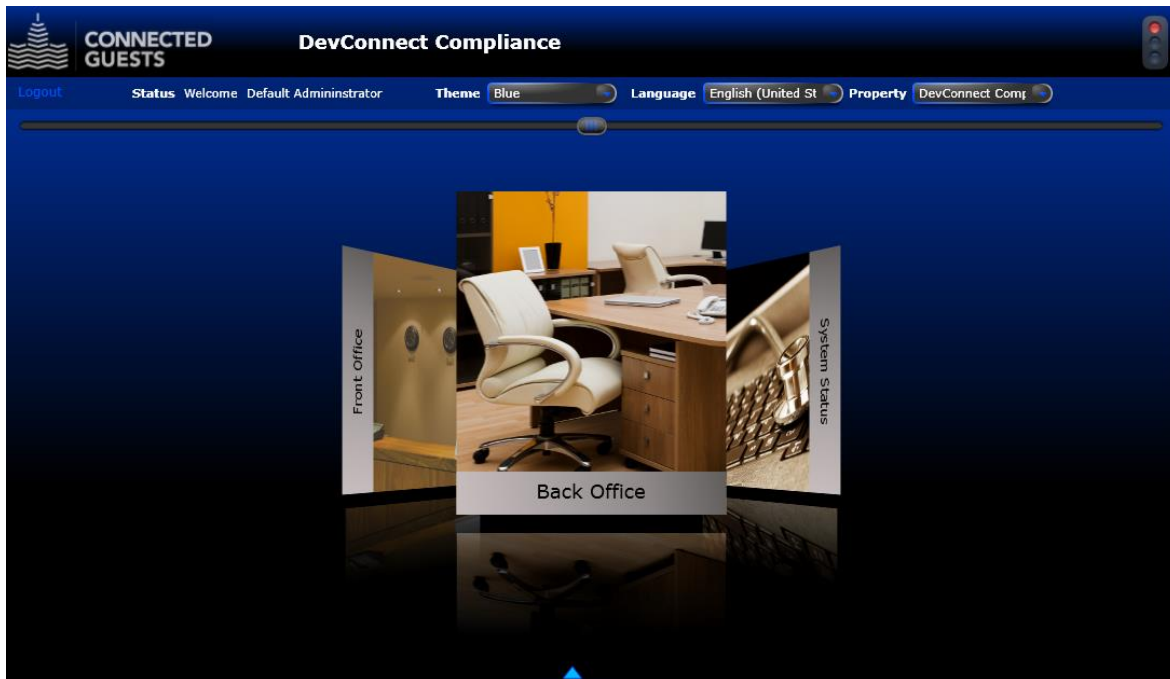
## 7. Verification Steps

This section provides the basic tests that can be performed to verify correct configuration of the IP Office and Connected Guests iCharge solution.

1. Open a browser and enter the ip address of the iCharge system as following format <http://<ipaddress of iCharge>/icharge> to launch the iCharge hospitality management page. Enter the proper user name and password to access to the system.



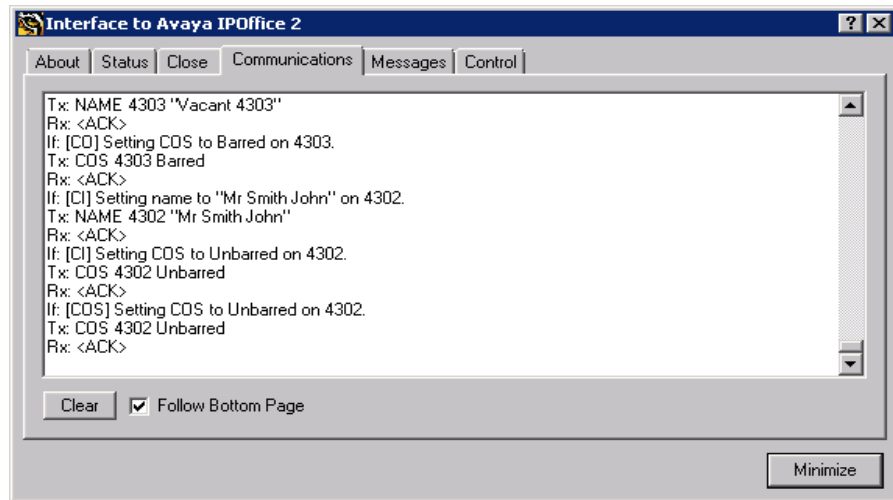
The homepage of Connected Guests iCharge is displayed as shown in the screenshot below.



2. To do a check-in a Guests room, from the home page navigates to **Front Office** → **Check-In**. Select **Walk-in**, **Reservation Code** and a room extension in the dropdown menu, enter Surname and First name in the Guests Details tab and click on **Check-In** button.

The screenshot shows the 'Check-In' form within the Connected Guests iCharge system. The header and navigation bar are identical to the previous screenshot. The main content area is titled 'Check-In a guest or guests for a reservation or walk-in...'. It features a 'Walk-In' dropdown menu, a 'Reservation Code' field with the value '650-000072', a 'Room Type' dropdown menu with the value '<Unknown>', a 'Room' dropdown menu with the value '4302', and a 'Do Not Disturb' toggle switch set to 'Off'. Below these fields are three tabs: 'Guest Details', 'Contact Details', and 'Reservation Details'. The 'Guest Details' tab is active, showing fields for 'Surname' (John), 'First Name' (Smith), 'Title' (Mr), 'VIP Status' (dropdown), 'Language Code' (dropdown), 'Extension Name Display' (Mr Smith John), and 'Guest Group'. To the right of the form is a grid of buttons: 'Extension Attributes', 'Additional Guests', 'Message Waiting', 'Budget Limit', 'Wake-up Calls', 'PIN Attributes', 'DDI Attributes', 'Account Details', 'Room Status', 'Check-In', and 'Back'.


1. From the iCharge server, launch the **Interface to Avaya IPOffice** click on the **Communications** tab and verify that the iCharge has passed the correct details onto the IP office.



3. The IPO user 4302 should now reflect the name entered in the **Full Name** field and the **Working hour User Rights** is set to Unbarred that allows making outgoing call.

Extn4302: 4302

User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming	Menu Progra
Name	Extn4302									
Password	••••••••									
Confirm Password	••••••••									
Unique Identity										
Conference PIN										
Confirm Audio Conference PIN										
Account Status	Enabled									
Full Name	Mr Smith John 4302									
Extension	4302									
Email Address										
Locale										
Priority	5									
System Phone Rights	None									
Profile	Basic User									
	<input type="checkbox"/> Receptionist									
	<input type="checkbox"/> Enable Softphone									
	<input type="checkbox"/> Enable one-X Portal Services									

Device Type  Avaya 9641

User Rights

User Rights view Working hours User Rights

Working hours time profile <None>

Working hours User Rights **Unbarred**

Out of hours User Rights

- To quickly show the call record, navigate to the bottom of the page and select Ez Report, the Report Parameter popup window is displayed (not shown). Select a desired extension and click OK button, the Report Viewer popup window shows all call records for the extension. Note that in order to run a full report for call record, navigate to **Back Office** → **Advanced Reports**.

**Report Viewer**

**Ez Report**

**Report For Period** 3/16/2017 - 3/16/2017

**Report Run On** 3/16/2017 1:51:19 PM

**Reported By** ADMIN

**Report Type** Department - 4302

**Filter** Outgoing,Incoming,Internal,Tandem,Cost,Bill

Date and Time	Call direction	Source	Destination	Dialled Digits	Duration	Cost
3/16/2017 12:33:33 PM	Internal	E 4302	E 4303		00:00:01	\$0,00
3/16/2017 1:40:22 PM	Internal	E 4302	E 4303		00:00:02	\$0,00
3/16/2017 1:40:27 PM	Outgoing	E 4302	T 2001	3300	00:00:00	\$0,00
3/16/2017 1:49:22 PM	Outgoing	E 4302	T 2001	4169663406	00:00:12	\$2,01
<b>Total</b>					<b>Calls</b> 4	<b>Cost</b> \$2,01

Page 1 / 1

Zoom 100%

## 8. Conclusion

These Application Notes describe the configuration steps required for Connected Guests iCharge to successfully interoperate with Avaya IP Office Server Edition Release 10. All feature and serviceability test cases were completed with an observation noted in **Section 2.2**.

## 9. Additional References

This section references product documentation relevant to these Application Notes.

Documentation for Avaya products can be found at <http://support.avaya.com>.

- [1] Administering Avaya IP Office™ Platform with Manager, Release 10, Issue 10.33, October 2016.
- [2] Deploying Avaya IP Office™ Platform Servers as Virtual Machines, Release 10, November 20156.
- [3] IP Office™ Platform 9.1 Using IP Office System Monitor, Release 10, September 2016.
- [4] Administering Avaya IP Office with Manager, Release 10, September 2016.

---

**©2017 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).