



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

---

# **Application Notes for aurenz GmbH AlwinPro Hotel / AlwinPro Care with Avaya IP Office Server Edition – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps necessary for provisioning aurenz GmbH's product AlwinPro Hotel/Care v13.2 to successfully interoperate with Avaya IP Office Server Edition R11.1.

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

These Application Notes describe the configuration steps necessary for provisioning aurenz GmbH's product AlwinPro Hotel/Care v13.2 to successfully interoperate with Avaya IP Office Server Edition R11.1. AlwinPro Hotel/Care from aurenz GmbH is a Windows-based system that provides a seamless interface to the Avaya IP Office Server Edition.

AlwinPro Care is used by hospitals for checking in/out hospital patients and associating telephones as well as other devices. It is an option for today's requirements when it comes to billing of entertainment services for hospital patients. AlwinPro Hotel is used by hotels and guesthouses for checking in/out and associating telephones as well as call billing. AlwinPro Hotel can also act as middleware between the PBX and the hotel management system. Services, such as telephone connection, Internet and TV, are easy and comfortable to calculate and bill. In addition, AlwinPro Hotel offers the full scope of a modern call accounting solution.

Both AlwinPro Hotel and AlwinPro Care have a built-in interface for managing guests/patients (checking in/out, ...). Also, it is possible to use a front office system/property management system (PMS) to provide data, such as a username and receive data, and call costs. More often, AlwinPro Hotel/Care is used as middleware to the Avaya IP Office. A property management system (PMS) is a management software suite that property owners and front desk workers use to manage their business by coordinating reservations, online booking availability, payments, and reporting in one central place. The hotel PMS streamlines operations for front office staff and guest services in a hotel or care business to check-in and check-out guests/patients, see room availability, make adjustments to existing reservations, and even can have back-office functionality (schedule housekeeping or maintenance).

Both AlwinPro Hotel/Care use the same interface for CDR processing as AlwinPro UC-Edition (or UC-Analytics). Please see *Application Notes for aurenz GmbH AlwinPro UC-Edition with Avaya IP Office to collect Call Detail Records (CDR)* for further information on the setup of the call billing module.

**Note:** AlwinPro Hotel/Care use a module called "Data Collector" to connect to IP Office to provide PMS integration. This module and its interaction with IP Office is the primary focus of these Application Notes.

**Note:** To provide additional services such as Wakeup Call and Cost Announcements, AlwinPro Hotel/Care use TE-SYSTEM XCAP Voice over IP to connect to IP Office using a SIP or H.323 trunk. This allows users on IP Office to dial into services on AlwinPro Hotel/Care. This is deemed to be part of the aurenz setup.

**Note:** The 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 an expansion cabinet. 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. A connection to IP Office 500 V2 as a standalone is possible with the use of an IP Office Application Server but this was not the focus of these Application Notes.

## 2. General Test Approach and Test Results

The test approach was to connect AlwinPro Hotel/Care to IP Office and to manually check in, check out guests and associate them with Avaya SIP and H.323 phones on IP Office. Commands were also issued to change the Class of Service or User Rights on these phones and call billing reports were also observed although were not the main focus of the compliance testing.

The main difference between AlwinPro Hotel and AlwinPro Care is, that normally with “Care” virtual numbers are used, so every patient gets a “virtual number”. This number can be called externally and is routed to the physical phone the patient is currently at. This is achieved via hunt groups, so every hunt group is a virtual number. When a patient then moves to a room the physical phone is added to the hunt group.

In contrast, “Hotel” is normally where a guest is assigned to a room and never moves, so the guest is reached via the physical number.

AlwinPro Hotel/Care makes use of two connections to IP Office, using the Management API to make changes to the User Rights and User’s Names, as well as a H.323 trunk connection to allow the XCAP connection to give IP Office users the ability to make changes on AlwinPro PMS to buy various dialling numbers associated with different services. AlwinPro Hotel/Care use the same interface for CDR processing as AlwinPro UC-Edition (or UC-Analytics).

Introduced in IP Office Release 10.1, the IP Office Management API consists of a set of REST-based services, which enables developers to consume IP Office configuration objects and incorporate configuration changes to an expanded set of IP Office entities into applications. Requests and responses utilize XML and JSON formats. Read/write access is provided to privileged service users only. The Management API is used to change/set the following values on IP Office Server Edition.

- Set username
- Change User Rights (allow external calls)
- Use hunt groups for virtual numbers (so that patients can be reached on the same number regardless of the physical number)

XCAP is a windows-based product from TE-SYSTEMS that allows the use of an existing CAPI 2.0-compatible application for Unified Messaging (UMS), Automatic Call Distribution (ACD) or Interactive Voice Response (IVR) via Voice over IP. It enables the use of telephone and fax functions without conventional hardware, such as modems or ISDN cards.

Compliance testing focused on verifying that external calls could be made when a user was “checked in” and were barred once a user was checked out. Also, verifying that the name was changed appropriately as well as checking that other User Rights were changed accordingly. Inbound calls were also made to the extension directly (for Hotel) and to the hunt group (for

Care). Also, the verification that IP Office users could dial into various AlwinPro services via H.323 trunk.

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 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 the Avaya IP Office and AlwinPro Hotel/Care did use a secure SSL link.

## **2.1. Interoperability Compliance Testing**

The objective of Interoperability Compliance Testing is to provide assurance to the potential customers that the tested products operate as specified and can interoperate in an environment similar to the one that will be encountered at a customer's premises. The interoperability compliance testing focused ensuring that the connection between AlwinPro Hotel/Care PMS and IP Office was successful and to do that the following tests were carried out.

- Use of Management API to update guest name and user rights template associated with Check-In, Check-Out, outgoing Call Bar, Guest Info update, and Move requests from AlwinPro Hotel/Care.
- Making calls to verify guest rooms with Call Bar 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.
- Allowing users make changes on the AlwinPro system such as initiating a wakeup call or changing the room status.
- The serviceability testing focused on verifying the behaviour of AlwinPro Hotel/Care under different simulated LAN failures.

## **2.2. Test Results**

Tests were performed to ensure full interoperability of Communication Manager with aurenz GmbH AlwinPro Hotel/Care. Performance and load testing is outside the scope of the compliance testing. All the test cases passed successfully.

## 2.3. Support

Information on AlwinPro Hotel/Care and product support can be obtained through the following:

Phone: [+49 \(0\) 7021 73888-0](tel:+49(0)7021738880)

Fax: [+49 \(0\) 7021 73888-30](tel:+49(0)70217388830)

E-Mail: [info@aurenz.de](mailto:info@aurenz.de)

### **Support-Hotline**

Mon-Fri 08:00-17:00

Phone: [+49 \(0\) 7021 73888-33](tel:+49(0)70217388833)

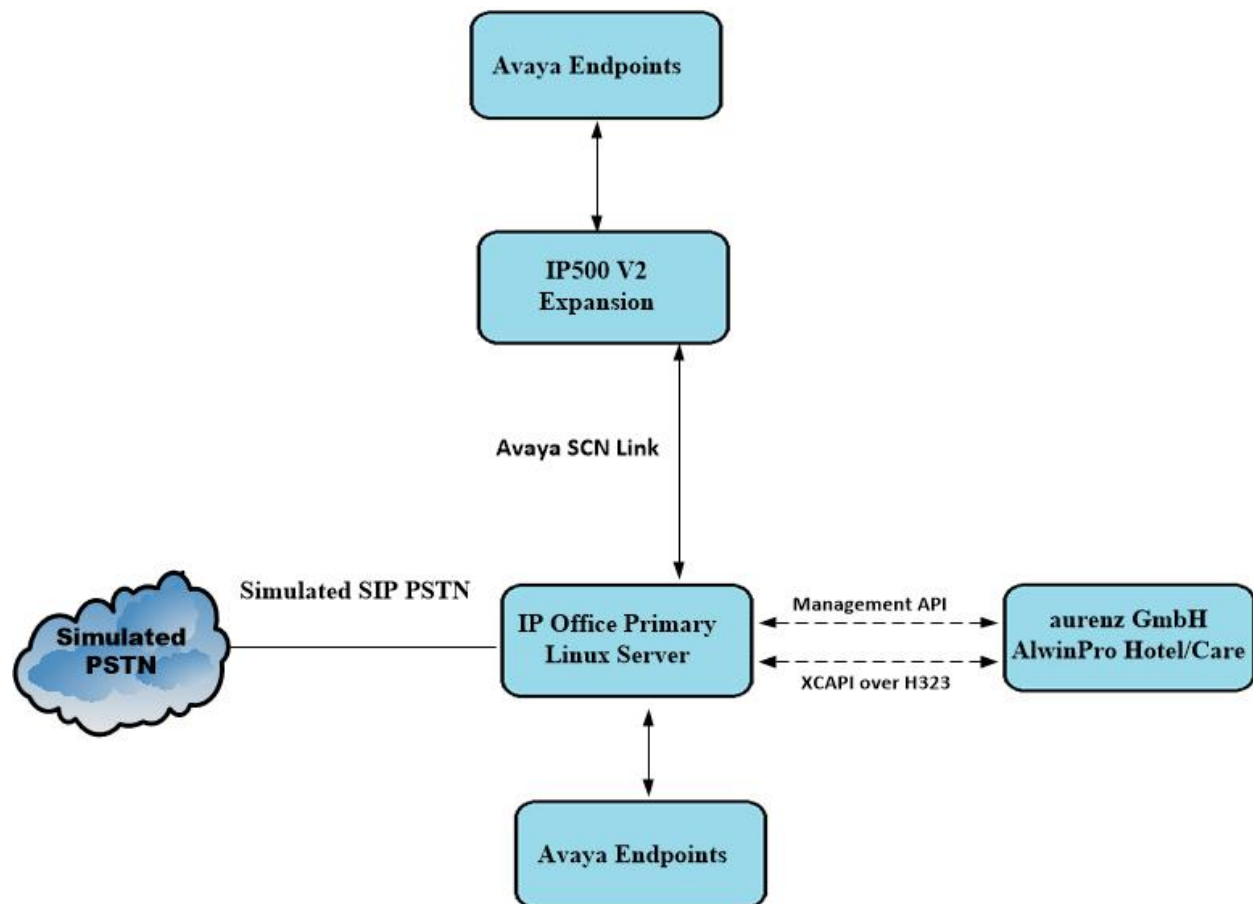
Fax: [+49 \(0\) 7021 73888-30](tel:+49(0)70217388830)

E-Mail: [support@aurenz.de](mailto:support@aurenz.de)

### 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office Primary Linux Server and IP500 V2 Expansion. The AlwinPro Hotel/Care makes use of two connections to IP Office, the Management API to make changes to the User Rights and User Names, as well as a H.323 trunk connection to allow the XCAP connection to give IP Office users the ability to make changes on the AlwinPro PMS and to buy various dialling numbers associated with different services. A variety of Avaya deskphones were used to generate intra-switch calls, and outbound/inbound calls to/from the PSTN. Session Manager shown in the diagram is used for SIP telephones and SIP trunks.

**Note:** One simulated PSTN line was used, consisting of a SIP trunk connection to Session Manager.



**Figure 1:** Avaya IP Office Server Edition and aurenz GmbH AlwinPro Hotel/Care 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 running on a Virtual Platform	11.1.2.0.0 Build 239
Avaya IP Office 500 V2 Expansion	11.1.2.0.0 Build 239
Avaya J179 IP Phone (H.323)	6.8304
Avaya J159 IP Phone (SIP)	4.0.7.0.7
aurenz GmbH AlwinPro Hotel/Care	13.2.1.07

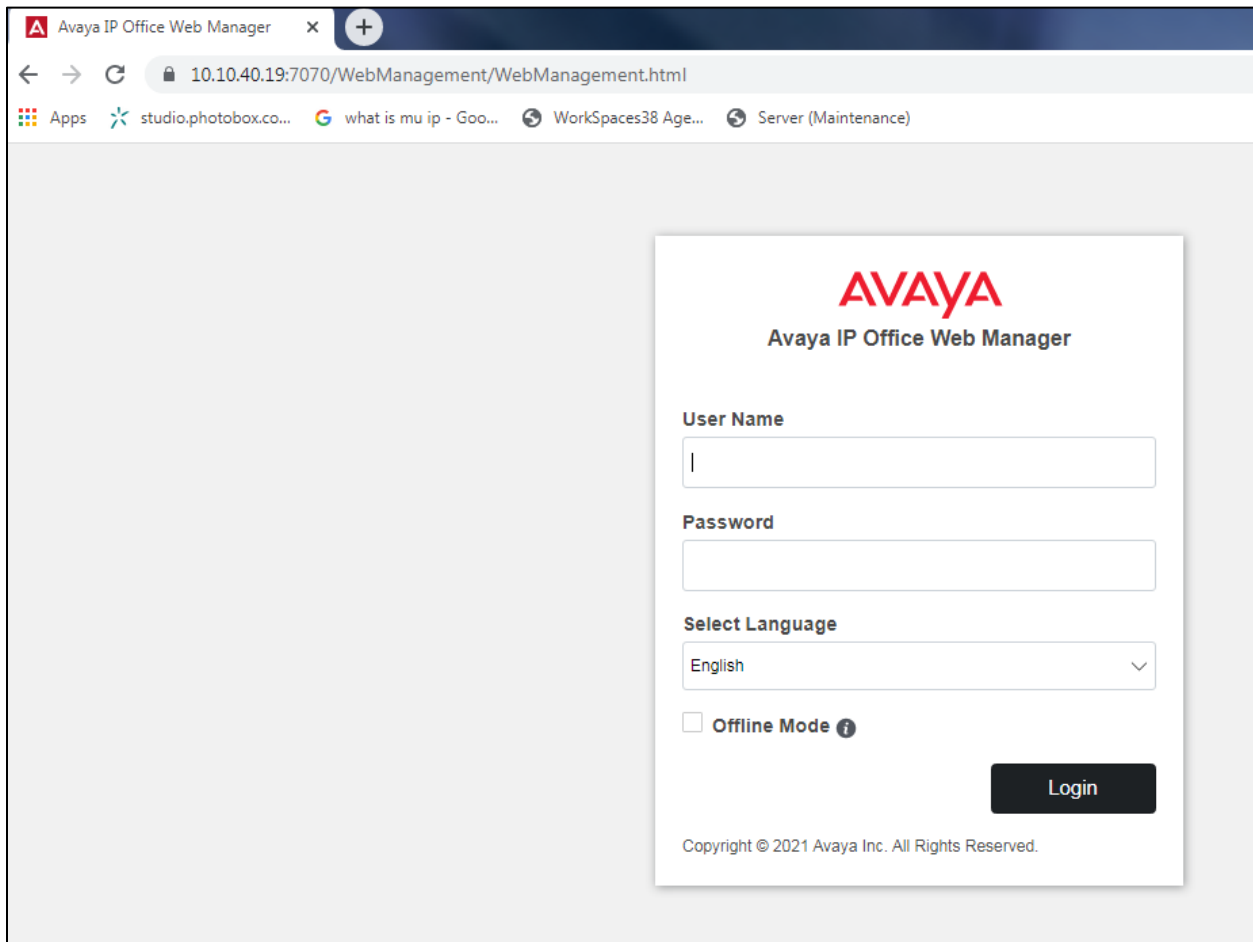
**Note:** Compliance Testing is applicable when the tested solution is deployed with IP Office Server Edition in any configuration. For a standalone IP500V2 configuration an additional Avaya IP Office Application Server is required and was not tested as part of this compliance testing.

## 5. Configure Avaya IP Office

The configuration of IP Office can be carried out using the traditional IP Office Manager or the newer IP Office Web Manager. For compliance testing, both were used to set up the connection to AlwinPro Car/Hotel. An IP Office Service User must be added on both the Server Edition and the IP500V2 expansion, to allow the connection to IP Office via the Management API. Also, a set of User Rights were added on both servers, to allow AlwinPro switch between allowing outbound calls and barring them. Hunt Groups were added specifically for AlwinPro Care, to allow the allocation of a virtual number. Some setups may want to bar incoming direct dial-in (DDI) calls to phones and only allow incoming calls to the virtual number, i.e., the hunt group number, and this is shown in the **Appendix**. A H.323 trunk was added to allow users on IP Office dial into AlwinPro Car/Hotel and make changes to the Room Status and to setup a 'wakeup call'.

### 5.1. Configure Service User on the Primary Server

The addition of the Service User and User Rights for the Server Edition were carried out using Web Manager. Open a URL to the IP Address of the IP Office Server Edition and enter the appropriate credentials, as shown below.

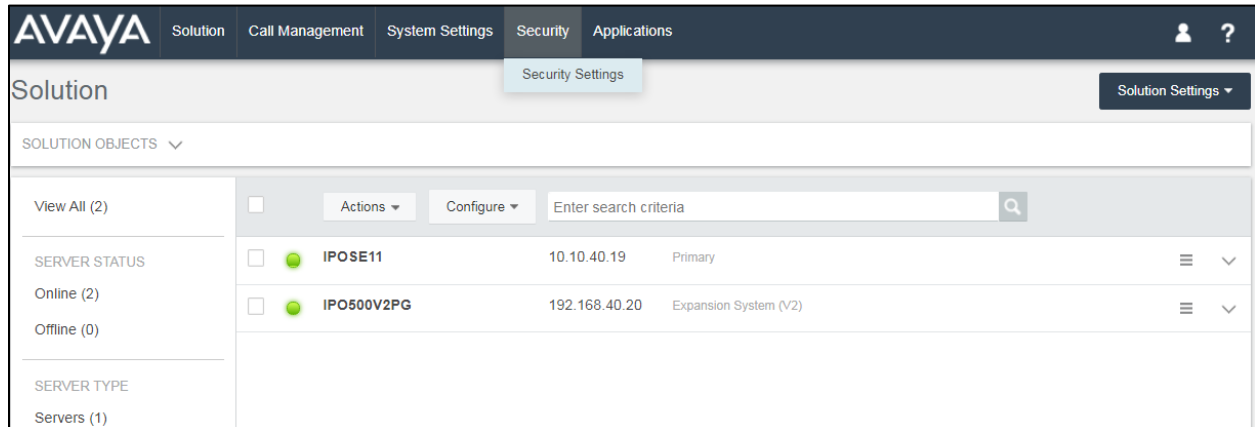


The screenshot displays the Avaya IP Office Web Manager login interface within a web browser. The browser's address bar indicates the URL is `10.10.40.19:7070/WebManagement/WebManagement.html`. The login form is centered and contains the following elements:

- AVAYA** logo and **Avaya IP Office Web Manager** title.
- User Name** input field.
- Password** input field.
- Select Language** dropdown menu, currently set to **English**.
- ☐ **Offline Mode** checkbox with an information icon.
- Login** button.
- Footer text: **Copyright © 2021 Avaya Inc. All Rights Reserved.**



From the top menu, navigate to **Security** → **Security Settings**.



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

Solution Security Settings Solution Settings

SOLUTION OBJECTS

View All (2)

SERVER STATUS

Online (2)

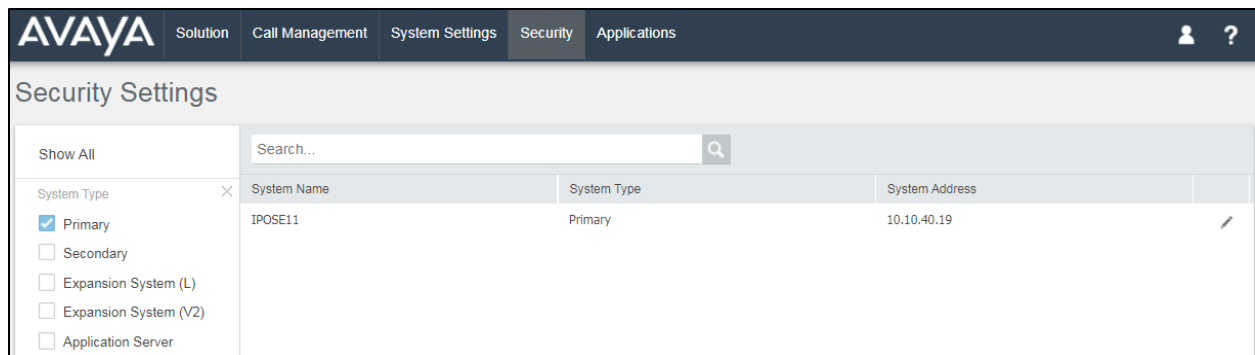
Offline (0)

SERVER TYPE

Servers (1)

	Actions	Configure	Enter search criteria	
<input type="checkbox"/>		<b>IPOSE11</b>	10.10.40.19	Primary
<input type="checkbox"/>		<b>IPO500V2PG</b>	192.168.40.20	Expansion System (V2)

The **Primary** Server Edition is chosen.



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

Security Settings

Show All Search...

System Type

☒ Primary

☐ Secondary

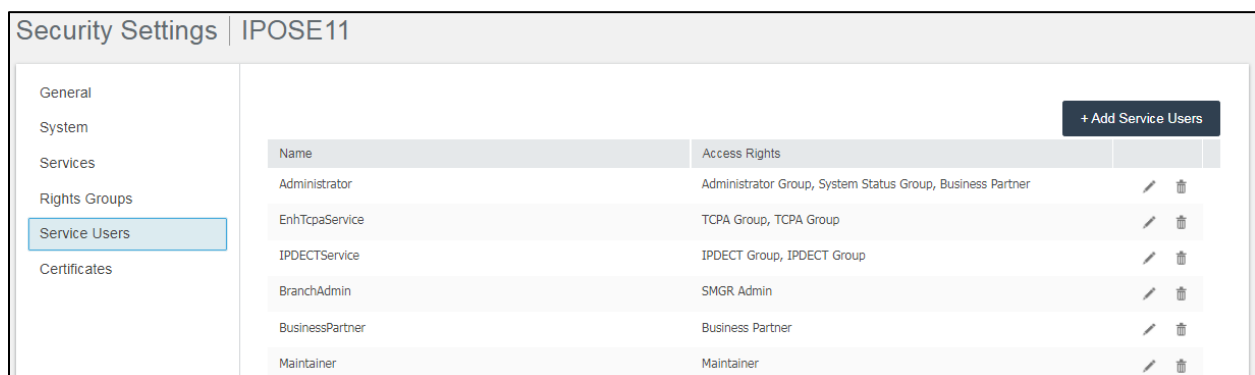
☐ Expansion System (L)

☐ Expansion System (V2)

☐ Application Server

System Name	System Type	System Address
IPOSE11	Primary	10.10.40.19

**Service Users** in the left window is highlighted and **Add Service Users** in the main window is clicked.



Security Settings IPOSE11

General

System

Services

Rights Groups

**Service Users**

Certificates

+ Add Service Users

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

The new user **aurenzSDKuser** is added with an appropriate **Password**. **Management API Group** is ticked and **Save** is clicked.

### Add Service User

**BASIC OPTIONS**

Name: aurenzSDKuser Password: Password Confirm Password: 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 Operator Group: NO SMGR Admin: NO

SNMPv2 Admin: NO Security Admin: NO System Admin: NO

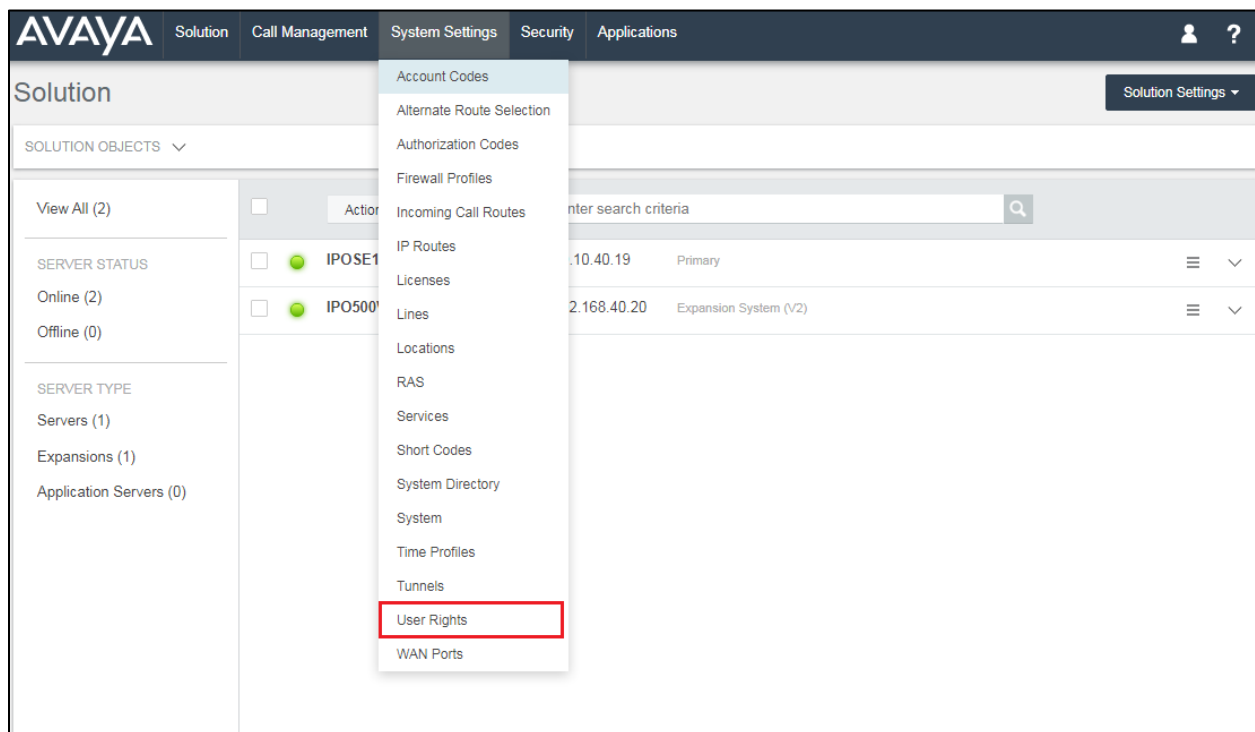
Cancel Save

The new user can be seen at the bottom of the screen below.

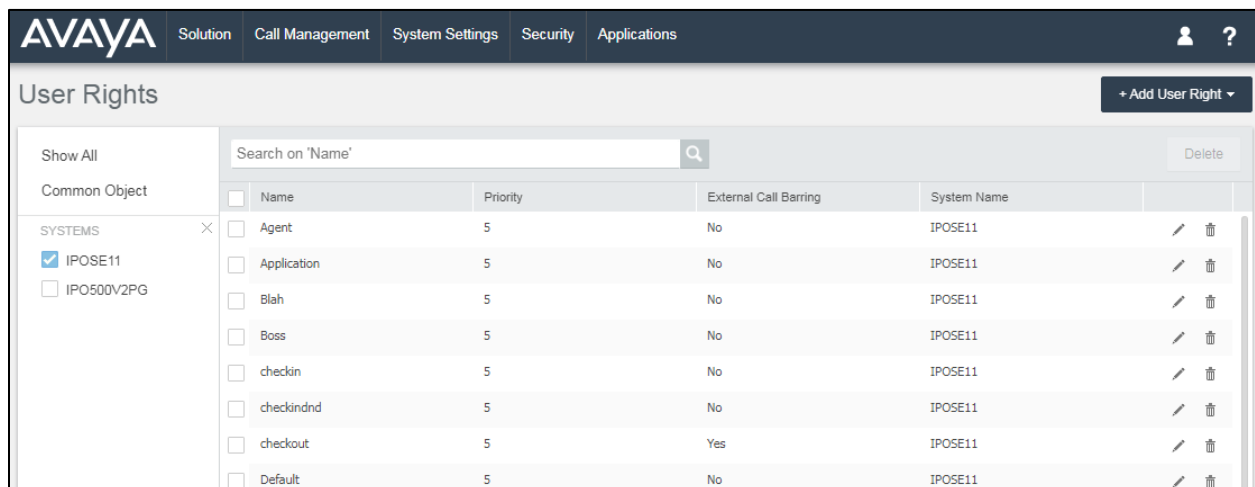
Security Settings IPOSE11	
General	
System	
Services	
Rights Groups	
Service Users	
Certificates	
+ Add Service Users	
Name	Access Rights
Administrator	Administrator Group, System Status Group, Business Partner
EnhTcpservice	TCPA Group, TCPA Group
IPDECTService	IPDECT Group, IPDECT Group
BranchAdmin	SMGR Admin
BusinessPartner	Business Partner
Maintainer	Maintainer
DirectoryService	Directory Group
MCMAdmin	MCM Admin
aurenzSDKuser	Management API Group

## 5.2. Configure User Rights

From the top menu, navigate to **Account Codes** → **User Rights**.



In the main window, click on **Add User Right**.



The following window will appear, where the User Right can be selected as a Common Object, meaning it can be used by the Primary server and all expansions, or if a particular server was ticked on the screen on the previous page, then **On Selected Server** could be chosen also. For compliance testing, **As Common Object** was chosen.

+ Add User Right	
<input checked="" type="radio"/>	As Common Object
<input type="radio"/>	On Selected Server
<input type="radio"/>	IPOSE11 10.10.40.19
<input type="radio"/>	IPO500V2PG 192.168.40.20
OK	

A suitable **Name** is given to the User Rights, this name will need to be noted and added in **Section 6.3**.

User Rights   ...		
User	Name: Blocked	Application Servers Group: NO
Short Codes	Locale: Ireland (UK English)	Apply user right value: NO
Button Programming	Priority: 5	Apply user right value: NO
Telephony	Enable do not disturb: NO	Apply user right value: NO
User Rights Membership		
Voicemail		
Forwarding		

Under the **Telephony** tab in the left window and **Supervisor Settings** in the main window, **Enable outgoing call bar** is ticked as well as **Apply user right** value next to it. Click on **Create** once these are chosen.

The screenshot shows the 'User Rights' configuration window with the 'Supervisor Settings' tab selected. The left sidebar lists various settings, with 'Telephony' highlighted. The main area displays a list of settings with checkboxes and 'Apply user right value' options.

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

At the bottom, there are 'Cancel' and 'Create' buttons.

A second User Rights is added, again this name is specific to that configured in **Section 6.3**, so the **Name** here must be noted and must match.

The screenshot shows the 'User Rights' configuration window with the 'User' tab selected. The left sidebar lists various settings, with 'User' highlighted. The main area displays a list of settings with text boxes, dropdowns, and checkboxes.

Setting	Value	Apply user right value
Name	Unblocked	<input type="checkbox"/> NO
Locale	Ireland (UK English)	<input type="checkbox"/> NO
Priority	5	<input type="checkbox"/> NO
Enable do not disturb	<input type="checkbox"/> NO	<input type="checkbox"/> NO

Here the same **Enable outgoing call bar** is now unticked but **Apply user right value** beside it remains ticked. Again, **Create** is clicked to add this new User Right to the system.

**User Rights | ...**

Call Settings Supervisor Settings Multiline Options Call Log

Can Intrude ☐ NO Apply user right value ☐ NO

Cannot be Intruded ☒ YES 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 ☒ YES Apply user right value ☐ NO

Coverage Group  Apply user right value ☐ NO

These User Rights can then be seen added with **Blocked** showing on the first page.

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

**User Rights**

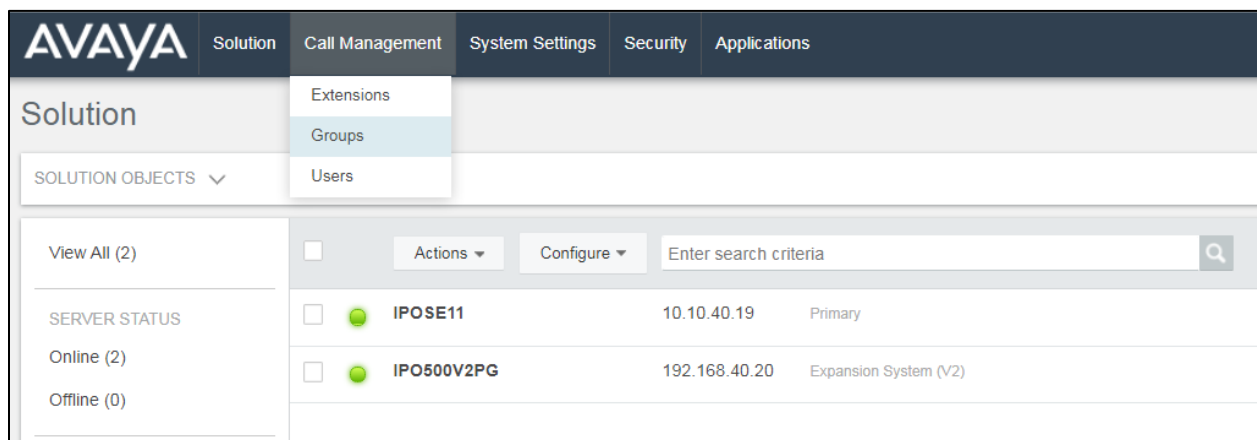
Show All Search on 'Name'

	Name	Priority	External Call Barring	System Name	
<input type="checkbox"/>	Agent	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	Application	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	Blah	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input checked="" type="checkbox"/>	Blocked	5	Yes	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	Boss	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	checkin	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	checkindnd	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	checkout	5	Yes	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/>	Default	5	No	All Systems	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

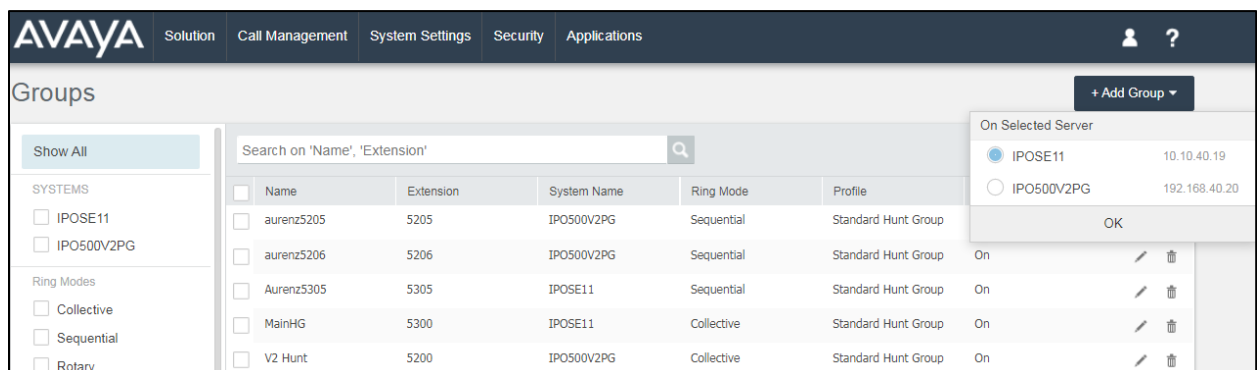
### 5.3. Configure Hunt Groups for AlwinPro Care

Hunt groups are added specifically for AlwinPro Care, as this setup requires the use of virtual numbers to allow patients move rooms and keep the same number. It is the hunt group number that is associated with the patient and that is the number that is contactable from either inside or outside the care facility. An IP Office phone is then associated with this hunt group and AlwinPro makes use of the Management API to added or remove phones from these hunt groups. Typically, there are enough hunt groups created to suit the maximum patient capacity of the facility in question.

To add a new hunt group, navigate to **Call Management** → **Groups** on the top menu.



Click on **Add Group** at the top right of the screen and selected the appropriate IP Office system to add it to.



Enter an appropriate **Name** and **Extension** and the rest of the fields can be left as default, noting that **Ring Mode** is set to **Sequential** by default. Click on **Create**.

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

Group ... IPOSE11

Group Settings

Group

Queuing

Overflow

Fallback

Voicemail

Voice Recording

Announcements

SIP

Name: aurenz5306

Profile: Standard Hunt Group

Extension: 5306

Exclude From Directory: NO

Ring Mode: Sequential

No Answer Time (sec): System Default (15)

Hold Music Source: No Change

Ring Tone Override: None

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

Advertise Group: YES

USER LIST ( 0/0 )

- Remove Users + Add Users

Membership Extension Name System Name

Cancel Create

The example below shows the two hunt groups that were used for compliance testing.

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

Groups + Add Group

Show All

Search on 'Name', 'Extension'

Edit Delete

Name	Extension	System Name	Ring Mode	Profile	Queuing
aurenz5205	5205	IPO500V2PG	Sequential	Standard Hunt Group	On
aurenz5206	5206	IPO500V2PG	Sequential	Standard Hunt Group	On
Aurenz5305	5305	IPOSE11	Sequential	Standard Hunt Group	On
Aurenz5306	5306	IPOSE11	Sequential	Standard Hunt Group	Off
MainHG	5300	IPOSE11	Collective	Standard Hunt Group	On
V2 Hunt	5200	IPO500V2PG	Collective	Standard Hunt Group	On

SYSTEMS

☐ IPOSE11

☐ IPO500V2PG

Ring Modes

☐ Collective

☐ Sequential

☐ Rotary

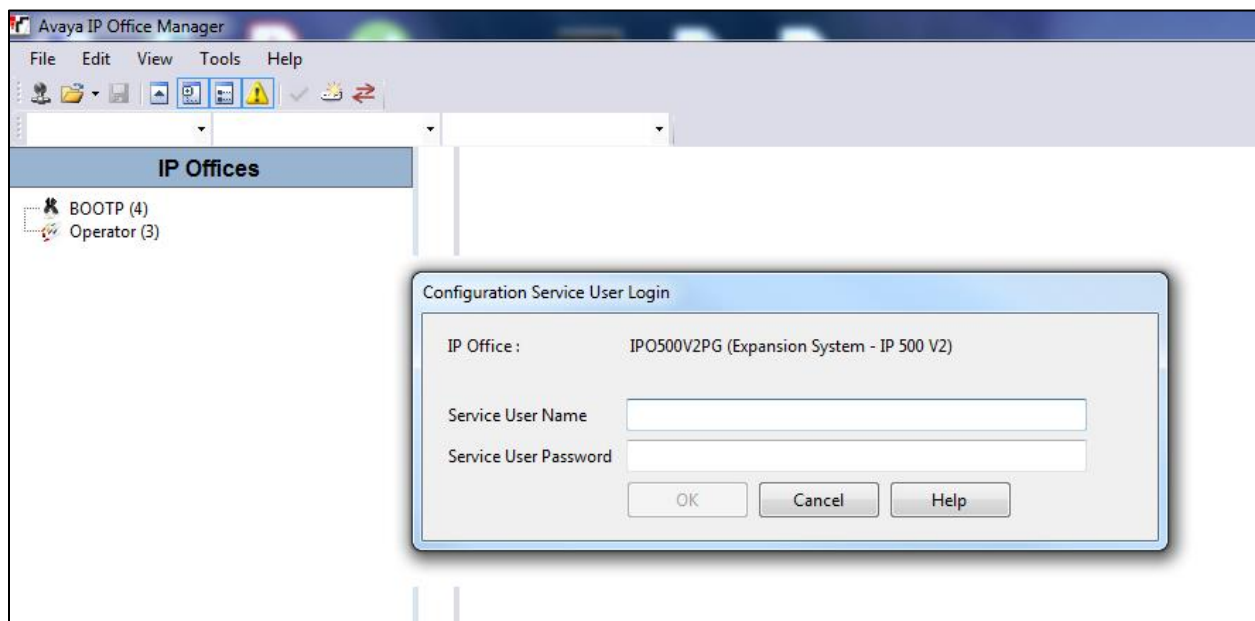
☐ Longest Waiting

☐ Collective Call Waiting

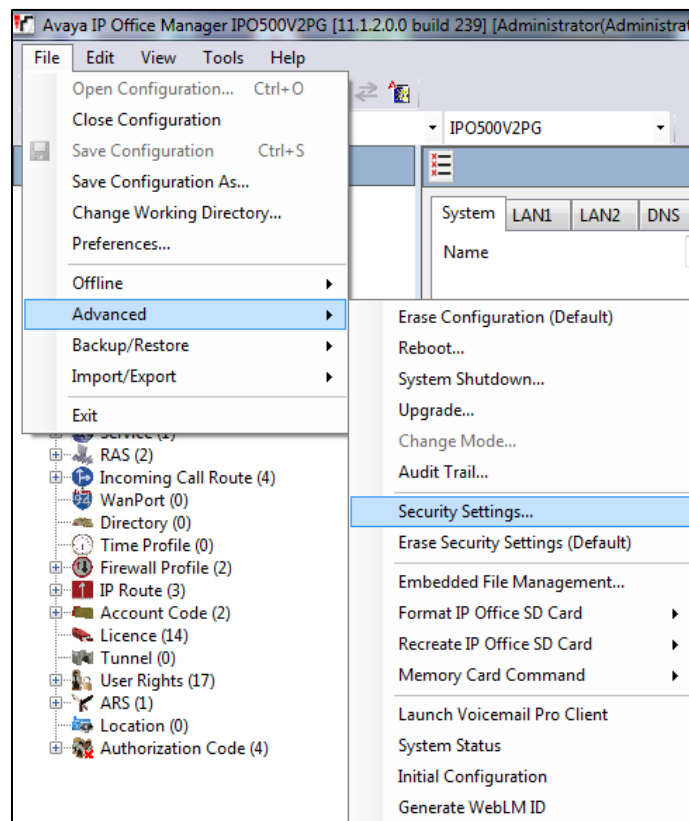


## 5.4. Configure Service User on the IP Office 500V2 Expansion

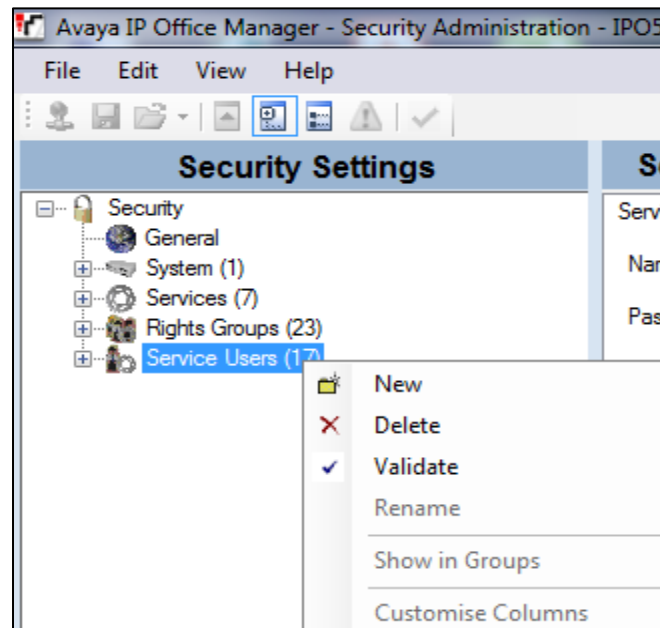
Log into the IP500V2 Expansion using IP Office Manager, as shown below.



Once logged in, navigate to **File → Advanced → Security Settings**, as shown below.



A new Service User is added as shown, by right-clicking on the **Service Users** and selecting **New**.



There is a **Rights Group Membership** called **Management API Group**, ensure that is ticked as shown below. The **Name** and **Password** must match that exactly as the user setup in **Section 5.1**.

**Service User: aurenzSDKuser**

Service User Details

Name: aurenzSDKuser

Password: [masked] Change Clear Cache

Account Status: Enabled

<None>

No Account Expiry ☒

Account Expiry

February 2022						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

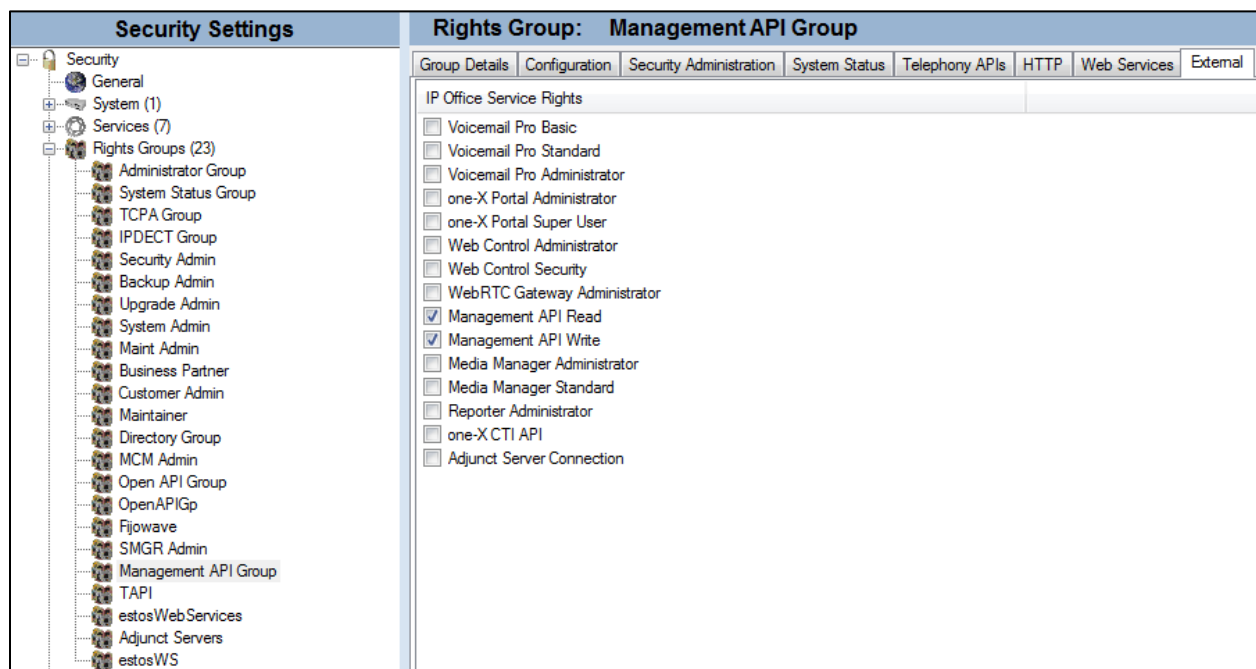
Today: 11/02/2022

Rights Group Membership

- ☐ Open API Group
- ☐ OpenAPIGp
- ☐ Fijowave
- ☐ SMGR Admin
- ☒ Management API Group
- ☐ TAPI
- ☐ estosWebServices
- ☐ Adjunct Servers
- ☐ estosWS

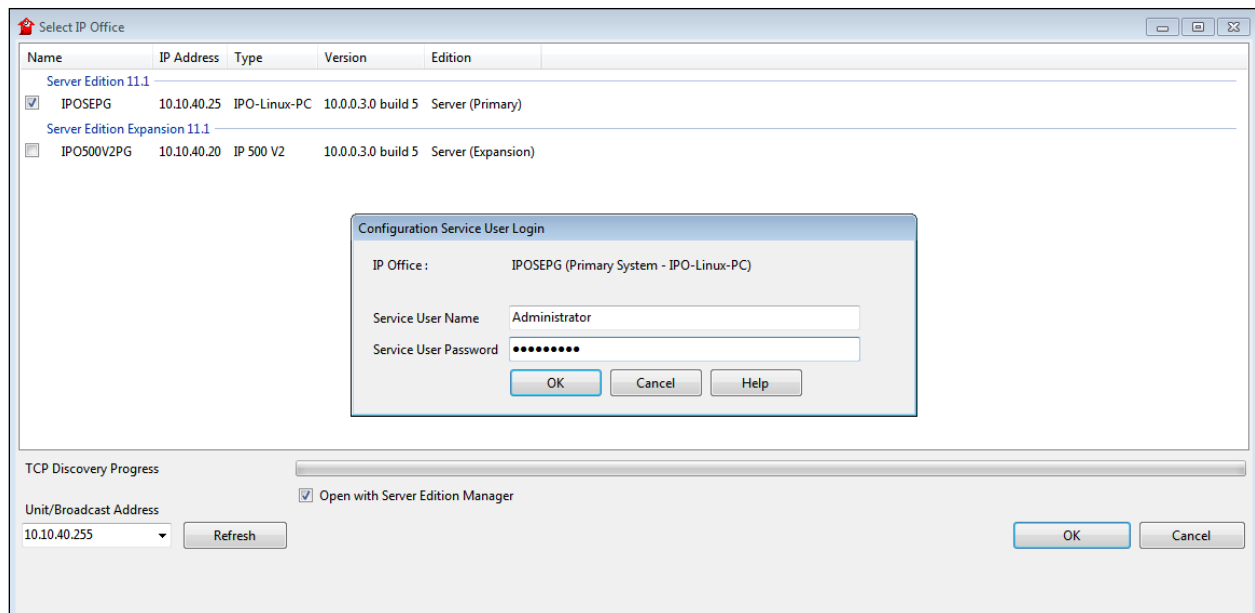
The Rights Groups are shown in the left window... clicking on the Management API Group shows the details for that group that the user above is a part of. Navigating through the tabs should show nothing ticked apart from that shown below in the **External** tab. The **Management API Read** and **Management API Write** should be the only **Service Rights** ticked.

Once the User is added and the setup is complete, click in the **Save** icon at the top left of the screen (not shown).

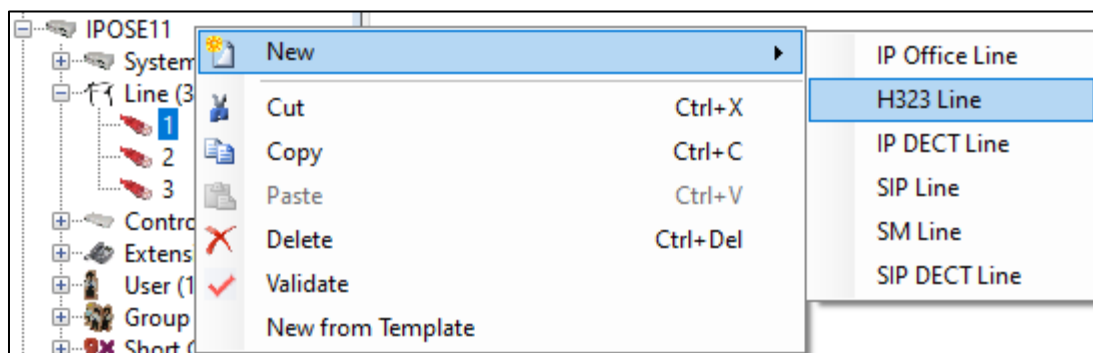


## 5.5. Configure H.323 Trunk for XCAPI

XCAPI can use setup to use either a SIP trunk or a H.323 trunk to connect to IP Office, for compliance testing a H.323 trunk was setup on both sides for this connection. Users on IP Office will use the H.323 trunk to dial across to certain services on AlwinPro Hotel/Care. The configuration of the H.323 trunk for XCAPI was added using the traditional IP Office Manager. From the IP Office Manager PC, click **Start → Programs → IP Office → Manager** to launch the Manager application (not shown). Select the required Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button.



From the left window, select the system and right-click on **Line** and select **New**. From the choices in the drop-down menu, select **H323 Line**.



Looking at the **VoIP Line** tab, the next available **Line Number** is given along with the **Outgoing Group ID**, any of these fields can be changed if required but for compliance testing everything was left as default, or as it was given when the line was selected.

The screenshot shows the 'H323 Line - Line 3' configuration window with the 'VoIP Line' tab selected. The fields are as follows:

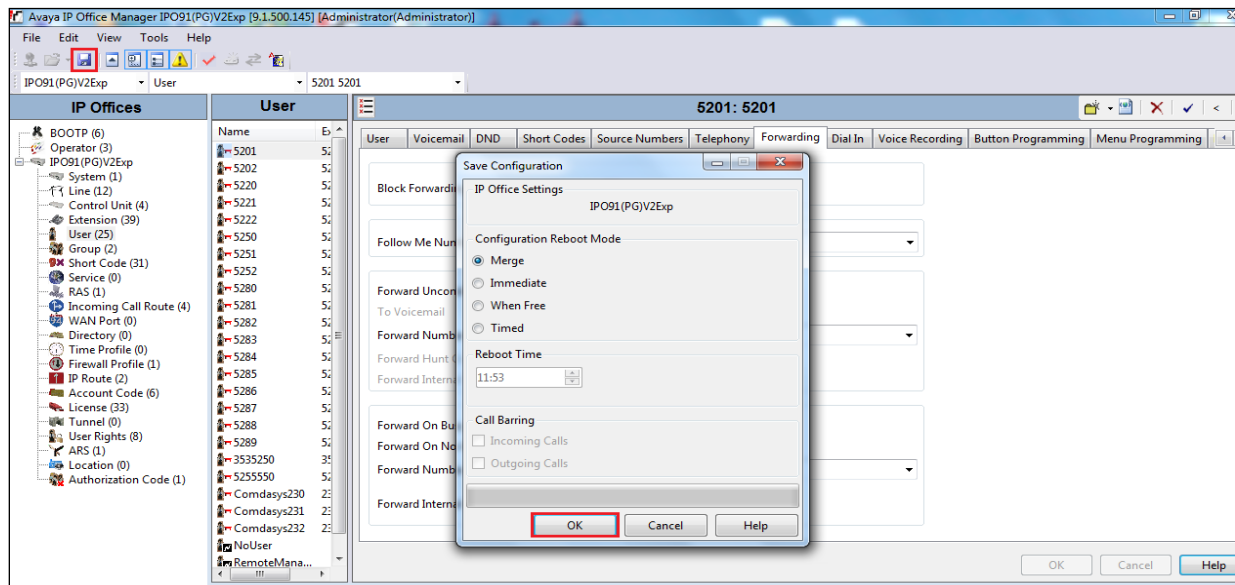
Line Number	3	TEI	0
Telephone Number			
Prefix		Outgoing Group ID	99002
National Prefix	0	Number of Channels	20
International Prefix	00	Outgoing Channels	20
Location	Cloud		
Description			
<input type="checkbox"/> Send original calling party for forwarded and twinning calls			

Under the **VoIP Settings** tab, the IP address of the server hosting the AlwinPro Hotel/Care is added as the **Gateway IP Address**. The default **Port 1720** was used. All other fields were left as default.

The screenshot shows the 'H323 Line - Line 3' configuration window with the 'VoIP Settings' tab selected. The fields are as follows:

Gateway IP Address	10 . 10 . 40 . 182	Port	1720	<input type="checkbox"/> Enable Fast Start
Codec Selection	System Default		<input checked="" type="checkbox"/> Out Of Band DTMF	<input type="checkbox"/> Local Tones
<div>Unused</div> <div>G.711 ULAW 64K G.722 64K G.729(a) 8K CS-ACELP</div> <div>Selected</div> <div>G.711 ALAW 64K</div>		<input type="checkbox"/> Default Name From Display	<input checked="" type="checkbox"/> Allow Direct Media Path	
Supplementary Services	H450			
Call Initiation Timeout (s)	4			

Once all the configurations have been made, it must be saved to IP Office. Click on the **Save** icon at the top of the screen and the following window appears. Click on **OK** to commit the changes.

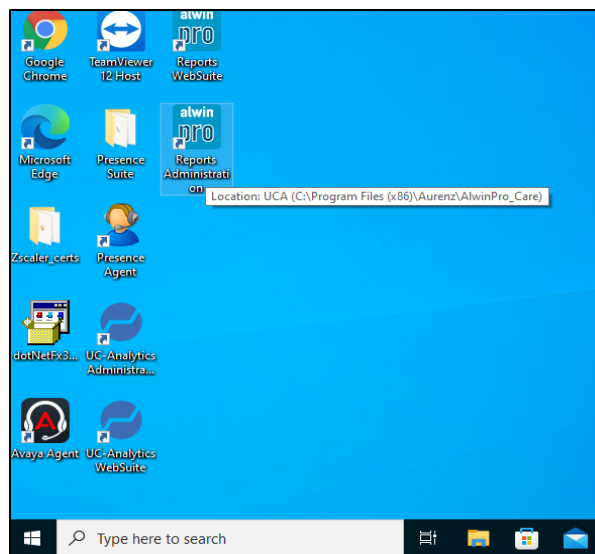


## 6. Configuration of aurenz GmbH AlwinPro Hotel/Care

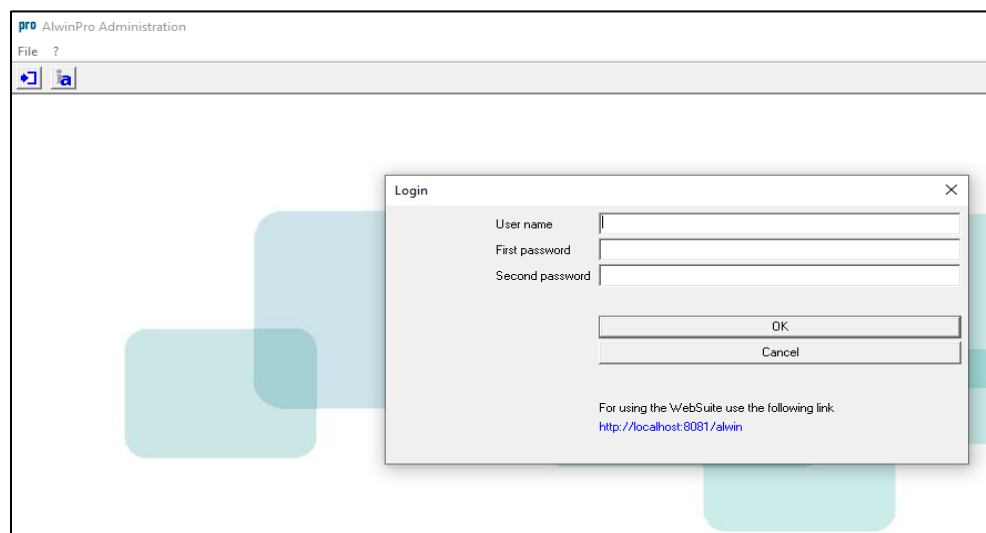
This section outlines the steps to configure the AlwinPro Hotel/Care to connect to IP Office. AlwinPro Hotel/Care can be installed on a server or desktop PC. Installation is carried out using software provide by aurenz GmbH. Installation instructions are outside the scope of this document but information on installation of AlwinPro Hotel/Care can be found in **Section 9** of this document.

### 6.1. Alwin Pro Care Hospital Module Setup

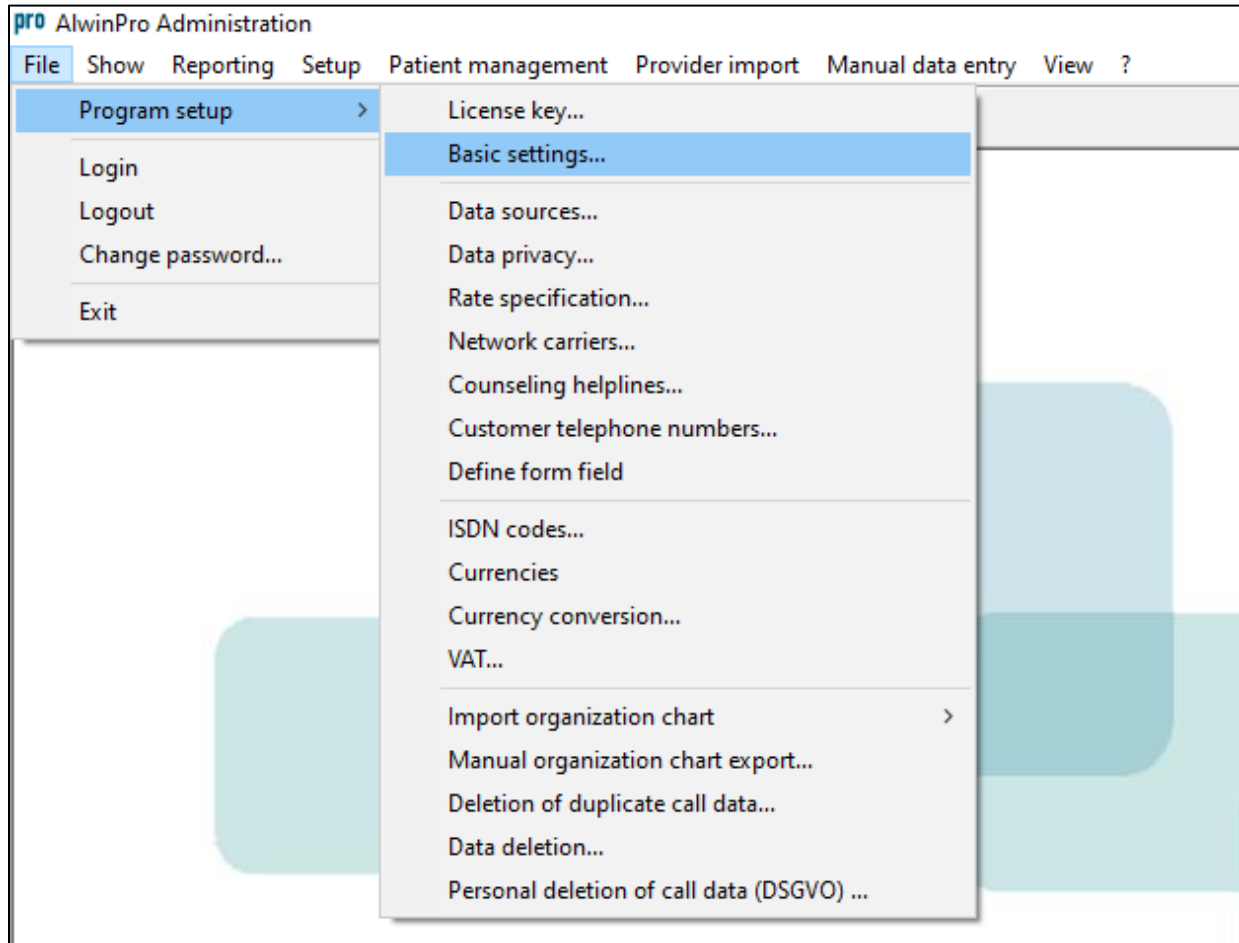
Before the connection to IP Office Management API can be configured, the Hospital Module on AlwinPro Hotel/Care must be set up. Open **Administration** from a shortcut on the desktop.



Enter the appropriate **User name** and **password**.

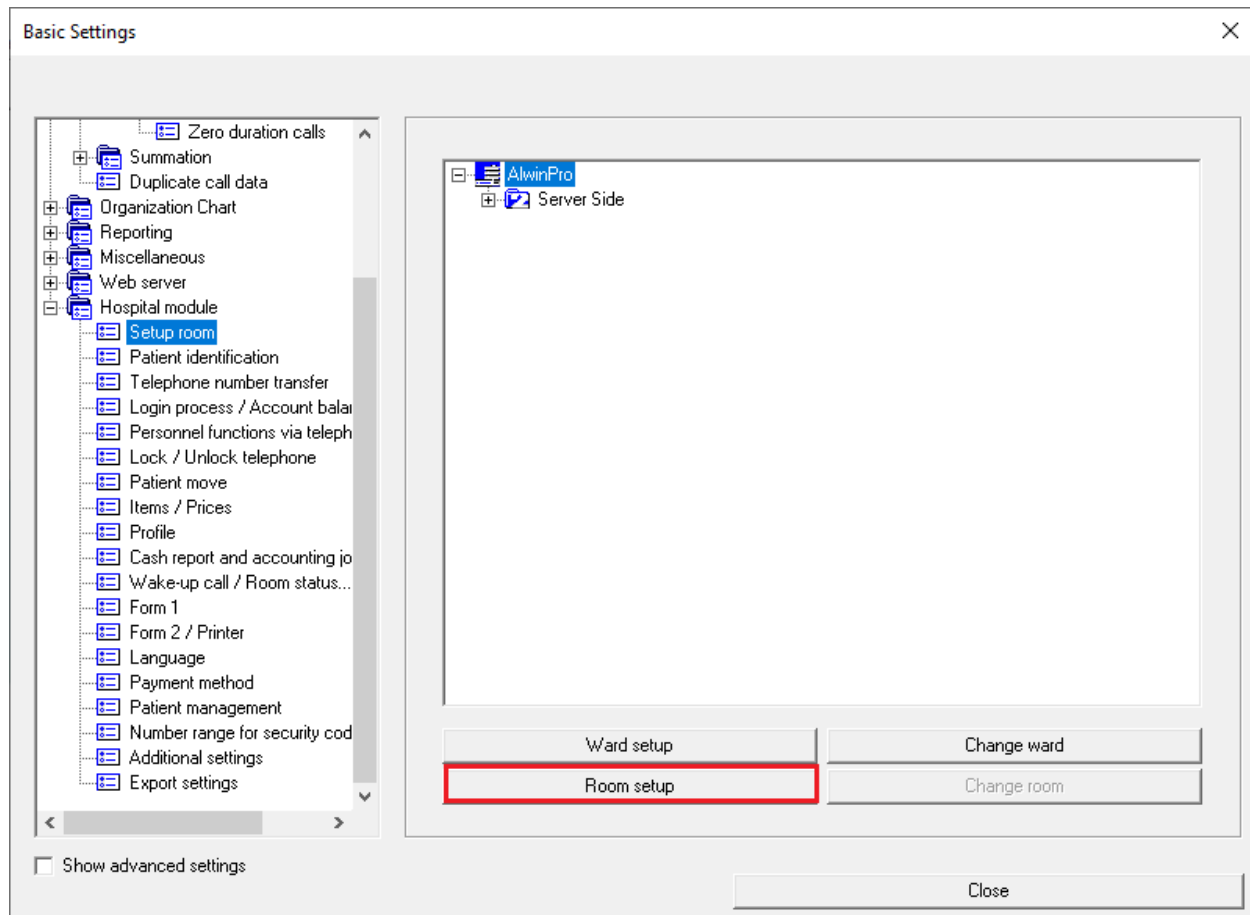


Navigate to **File → Program setup → Basic settings...**, as shown below.

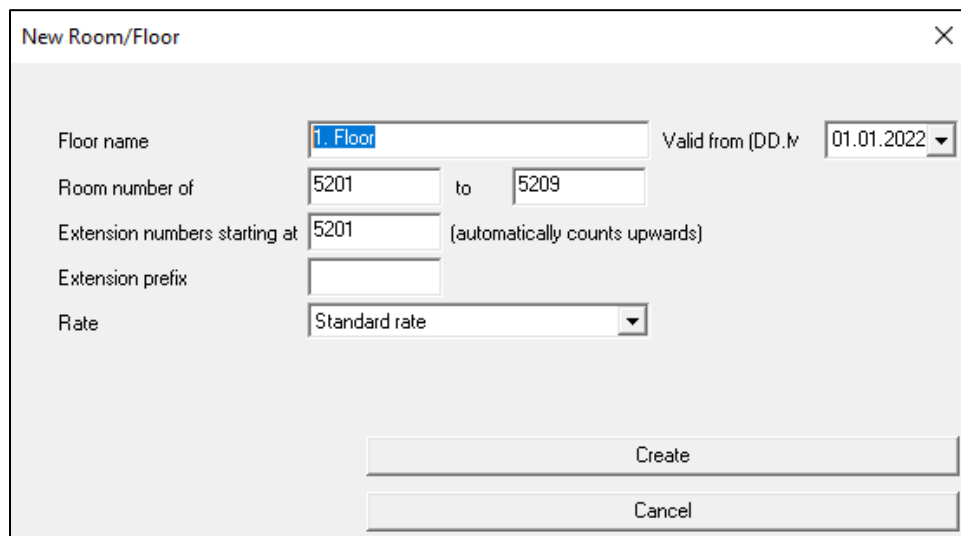




Open the **Hospital module** in the left window and click on **Setup room**. In the main window, click on **Room setup**.



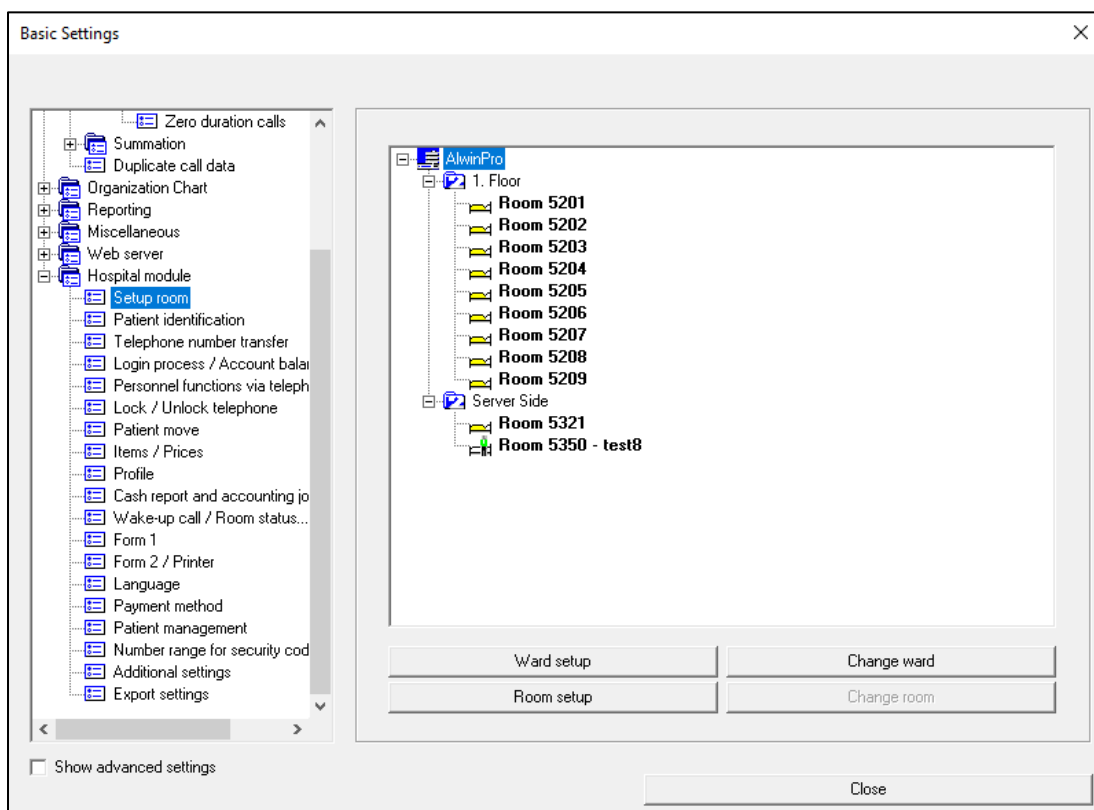
A number of telephones can be added or a single telephone. Screen below shows a range of telephones added, **5201** to **5209**. These were associated with a whole floor, where perhaps rooms 201 to 209 are located.



The 'New Room/Floor' dialog box contains the following fields and controls:

- Floor name:** A text field containing '1. Floor'.
- Valid from (DD.MM):** A date field containing '01.01.2022' with a dropdown arrow.
- Room number of:** A text field containing '5201'.
- to:** A text field containing '5209'.
- Extension numbers starting at:** A text field containing '5201'.
- (automatically counts upwards):** A label text.
- Extension prefix:** An empty text field.
- Rate:** A dropdown menu showing 'Standard rate'.
- Create:** A button at the bottom right.
- Cancel:** A button at the bottom right.

The screen below shows the newly added phones as well as the two phones **5321** and **5350** that were already added for compliance testing.



The 'Basic Settings' dialog box features a tree view on the left and a main display area on the right.

**Left Tree View:**

- Zero duration calls
  - Summation
  - Duplicate call data
- Organization Chart
- Reporting
- Miscellaneous
- Web server
- Hospital module
  - Setup room** (highlighted)
  - Patient identification
  - Telephone number transfer
  - Login process / Account balance
  - Personnel functions via telephone
  - Lock / Unlock telephone
  - Patient move
  - Items / Prices
  - Profile
  - Cash report and accounting job
  - Wake-up call / Room status...
  - Form 1
  - Form 2 / Printer
  - Language
  - Payment method
  - Patient management
  - Number range for security code
  - Additional settings
  - Export settings

**Main Display Area:**

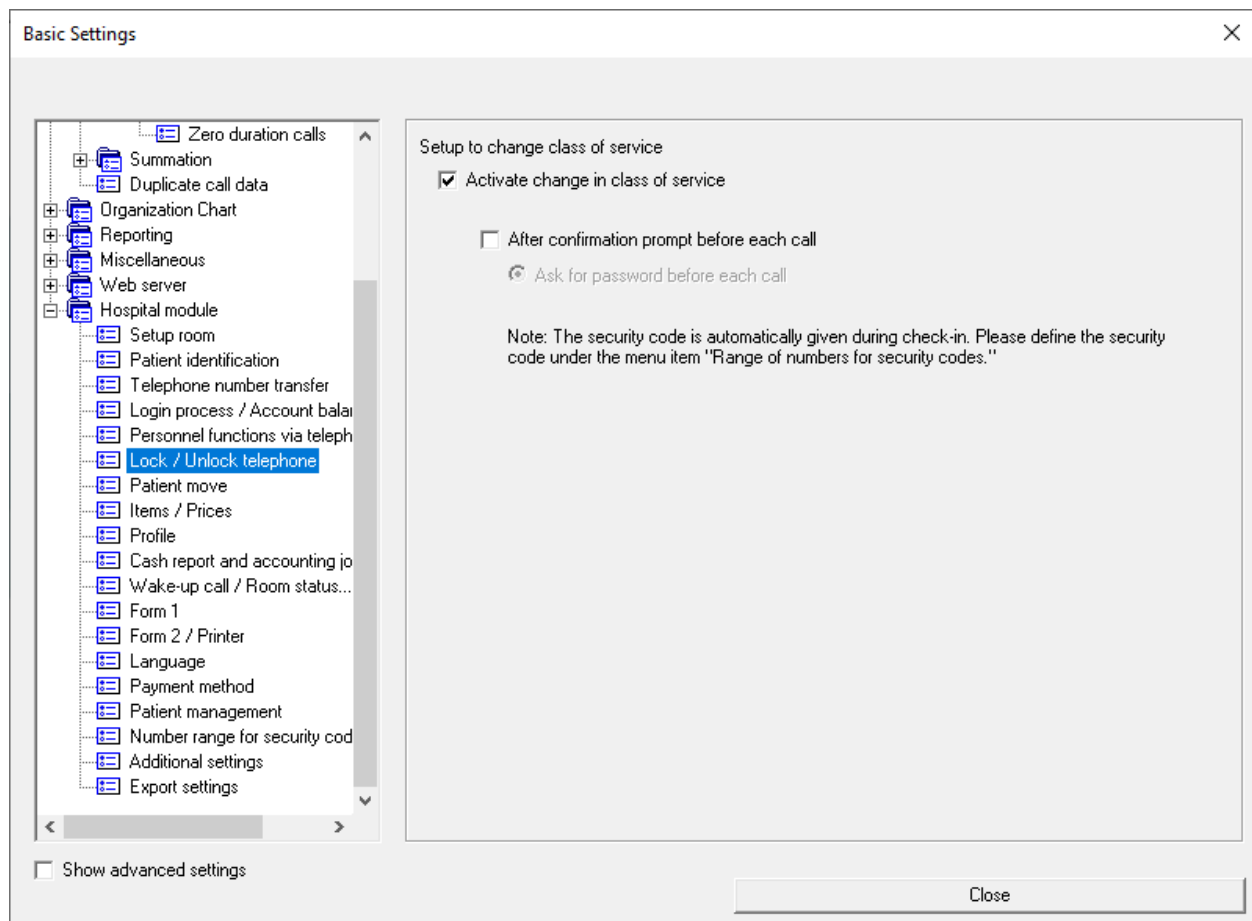
- AlwinPro** (selected)
  - 1. Floor**
    - Room 5201
    - Room 5202
    - Room 5203
    - Room 5204
    - Room 5205
    - Room 5206
    - Room 5207
    - Room 5208
    - Room 5209
  - Server Side**
    - Room 5321
    - Room 5350 - test8

**Buttons:**

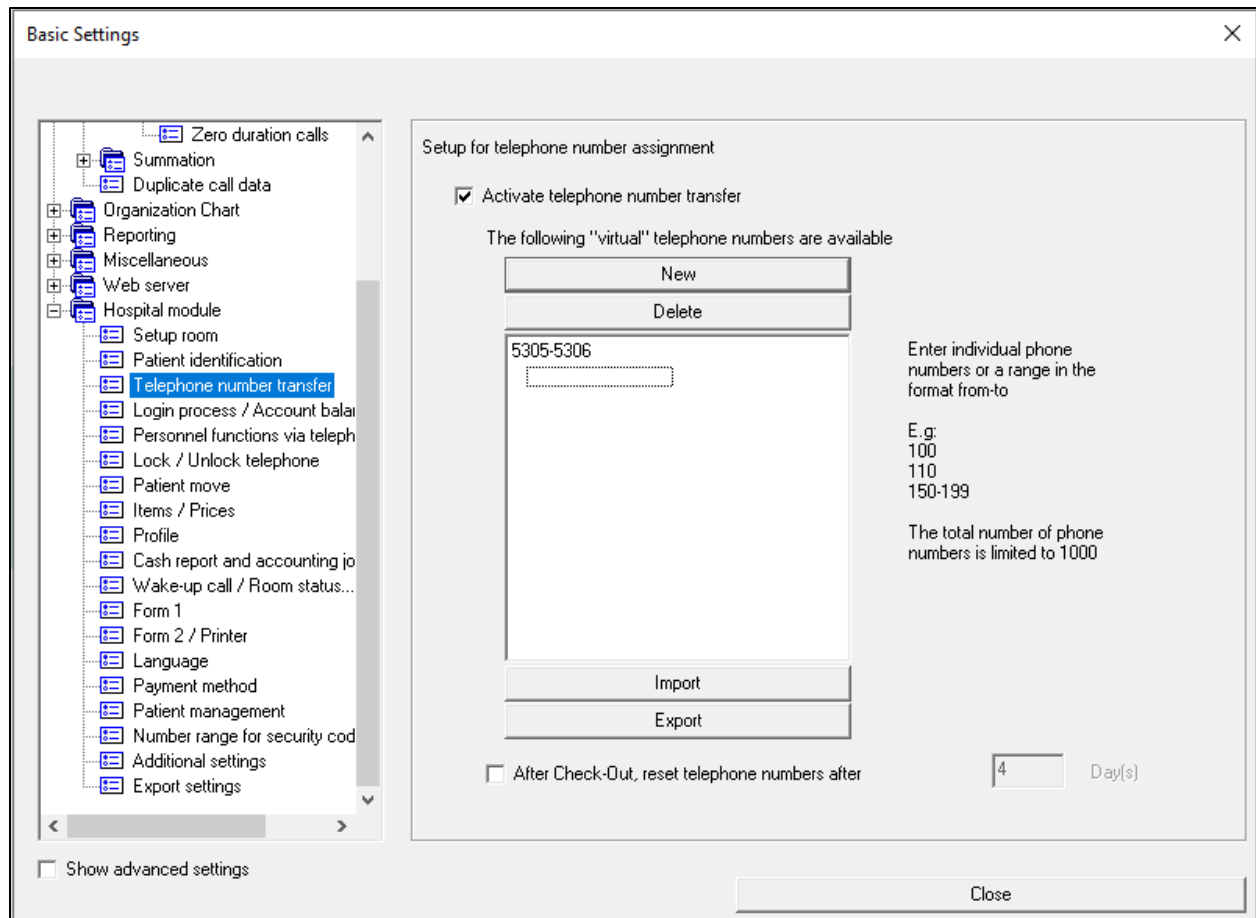
- Ward setup
- Change ward
- Room setup
- Change room
- Close

☐ Show advanced settings

Click on **Lock / Unlock telephone** in the left window and ensure that **Activate change in class of service** is ticked in the main window. This must be ticked to allow the configuration of the Management API in **Section 6.3**.



The following is set up for AlwinPro Care only, as that makes use of Hunt Groups on IP Office to use as “virtual” numbers. Two Hunt Groups (**5305** and **5306**) were setup for testing to allow two phones get assigned simultaneously. Click on **Activate telephone number transfer** and click on **New** to add a range of numbers to be used as virtual numbers in AlwinPro Care.



## 6.2. XCAPI Setup

To allow users make use of the services on AlwinPro Hotel/Care using the XCAPI connection, the following must be configured on the Hospital Module. Following from **Section 6.1**, click on **Login process / Account balance** in the left window and ensure that all the tick boxes are ticked. A number associated with each service is added, this will allow guests/patients dial certain number for example a “wake-up” service can be accessed by dialling **1114**. These numbers are dialled from IP Office over a H.323 trunk as configured in **Section 5.5**.

The screenshot shows the 'Basic Settings' window for the 'Hospital module'. The left sidebar lists various settings, with 'Login process / Account balance' selected. The main area is titled 'Setup for the login process / Account balance message' and contains the following text and configuration options:

With the login process the patients can register on the phone by themselves. Only after successful login is the telephone activated for them. There is also the possibility to request the account balance over the phone. An ISDN card is absolutely necessary for both services (optional accessories).

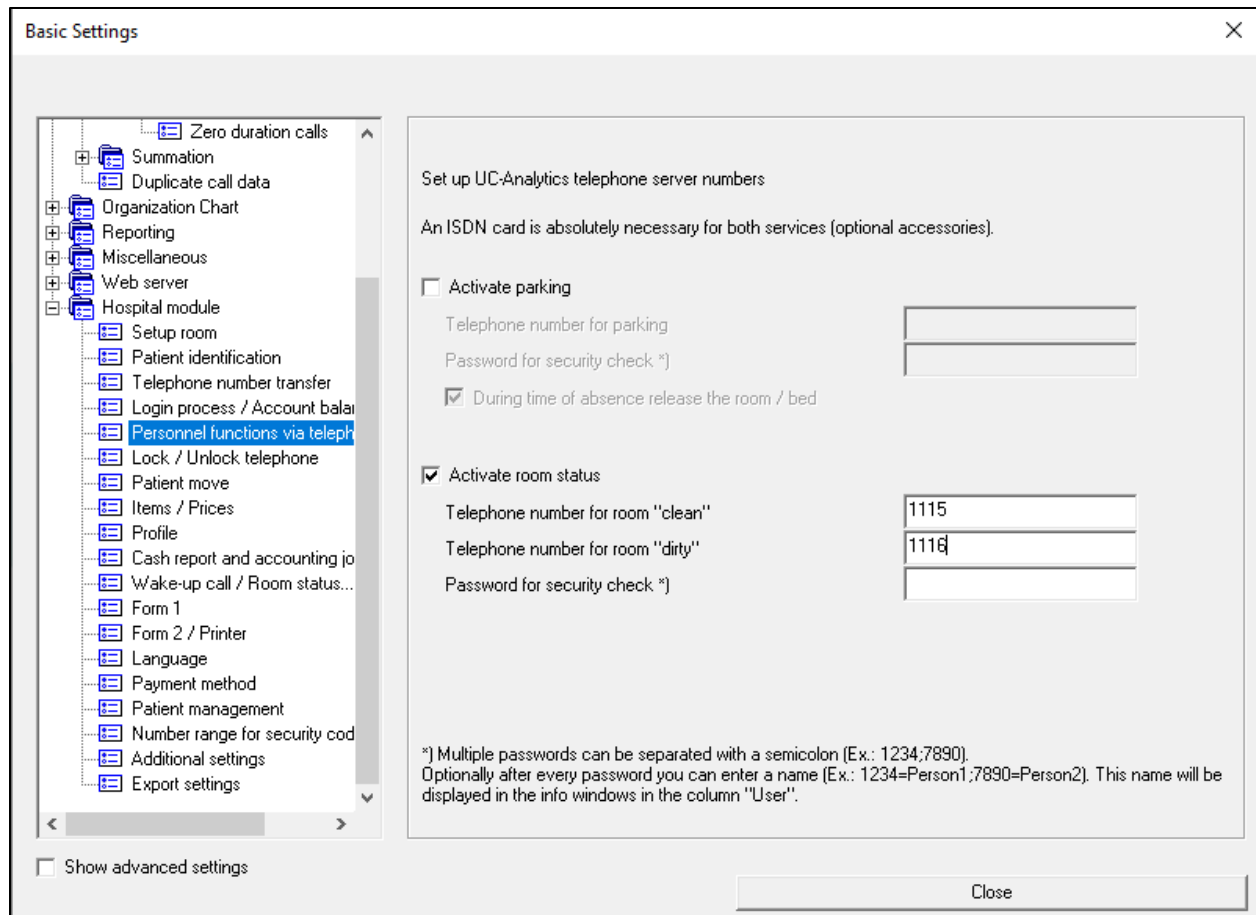
The login process is absolutely necessary for chip card telephones!

- ☒ Activate login process
  - Telephone number for unlocking: 1112
  - Telephone number for locking: 1113
  - Telephone number to unlock using the chip card telephone: (empty)
- ☒ Activate account balance announcement
  - Announcement via the following telephone number: 1111
- ☒ Activate wake-up calls via telephone server
  - Unanswered wake-up calls retry count: 3
  - Calling party number: (empty)
- ☒ Phone number for wake-up call programming by the patient: 1114

Note: The personal login number is automatically given out at check-in. The security codes are used for the login numbers.

At the bottom left, there is a checkbox for 'Show advanced settings' which is currently unchecked. At the bottom right is a 'Close' button.

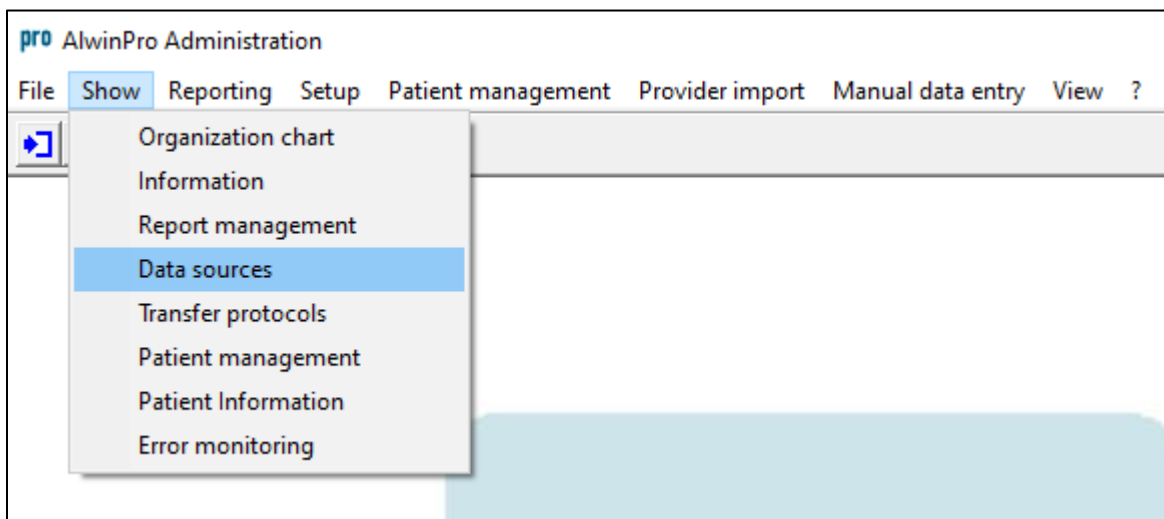
Click on **Personnel functions via telephone** in the left window and ensure that **Active room status** is ticked in the main window. This will allow the cleaners change the status of the room using the telephone. Dialling **1115** will change the status from dirty to **clean** and dialling **1116** will change the status back to **dirty**.



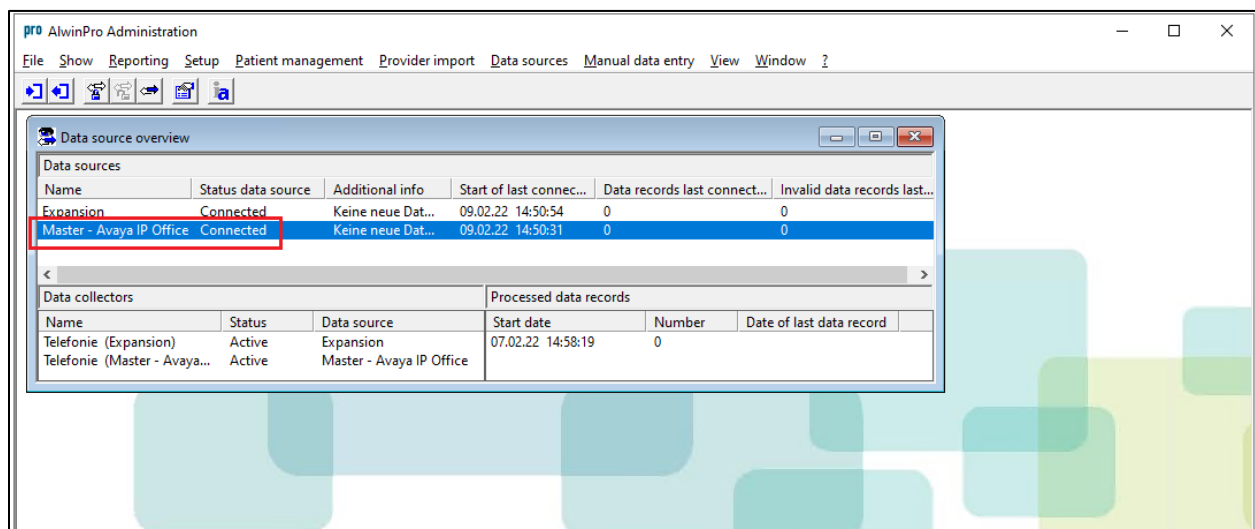
There are a number of other changes that can be made depending on the setup required, but the changes above were carried out for compliance testing. Once the Hospital module changes are complete, the Data Collector can be configured to connect to the IP Office Management API.

### 6.3. Configure AlwinPro Hotel/Care Data Collector

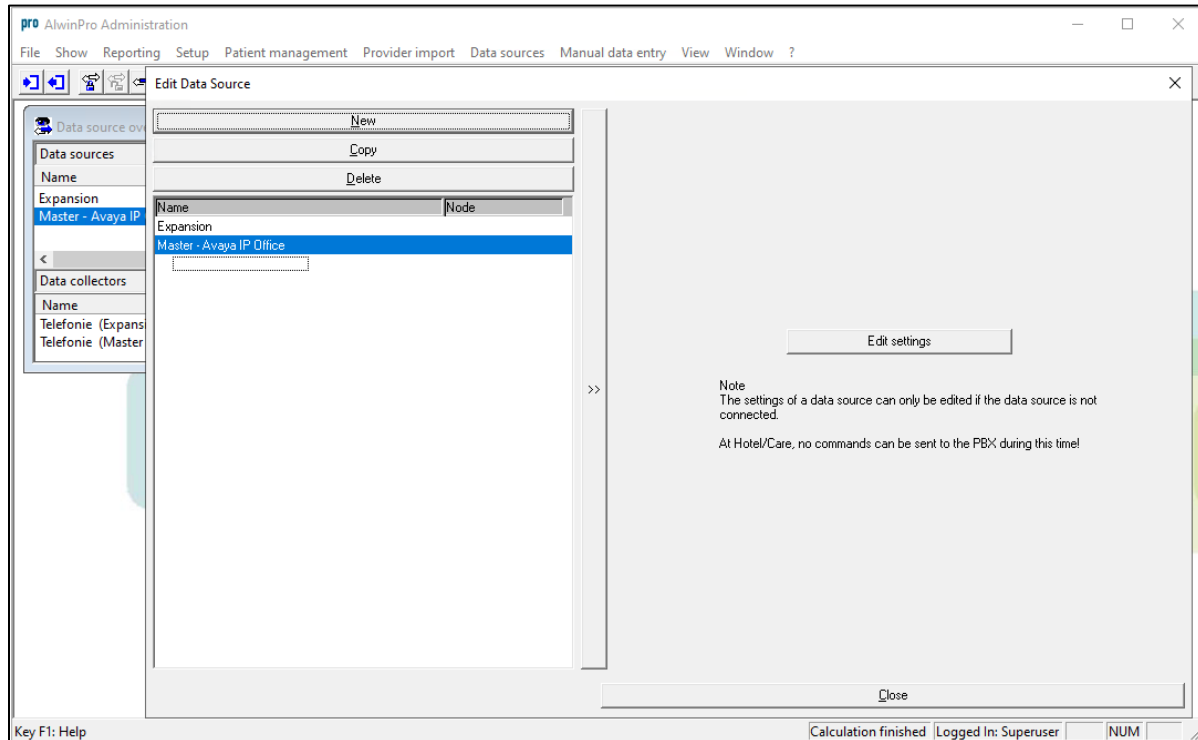
From the application menu, navigate to **Show → Data Sources**, as shown below.



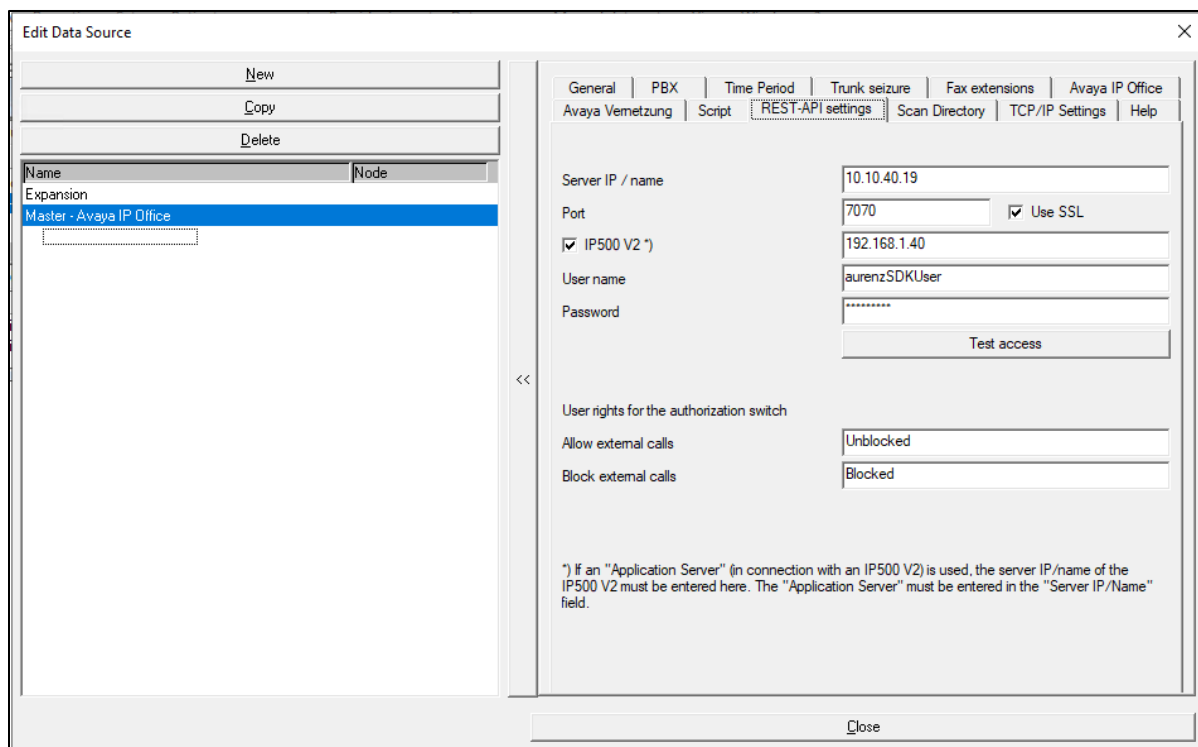
Double-click on the **Data source**, as highlighted below.



Click on **Edit settings** in the main window.



The following group of tabs are available for configuration.





Under the **REST-API settings** tab. The following fields are configured.

- **Server IP / name** This is the IP address of IP Office Server Edition.
- **Port** Port **7070** is used as the default port.  
**Use SSL** is ticked to ensure that a secure connection is used.
- **IP500 V2 \*)** This is the IP address of the Expansion.
- **User name** This is set to the same user configured in **Section 5.1**.
- **Password** This is the corresponding password for the user.
- **Allow external calls** This is set to the User Rights setup in **Section 5.2**.
- **Block external calls** This is set to the corresponding User Rights setup in **Section 5.2**. These names must match exactly.

The screenshot shows the 'REST-API settings' tab in a configuration window. The tabs at the top are: General, PBX, Time Period, Trunk seizure, Fax extensions, Avaya IP Office, Avaya Vernetzung, Script, REST-API settings (selected), Scan Directory, TCP/IP Settings, and Help. The configuration fields are as follows:

Server IP / name	10.10.40.19
Port	7070
<input checked="" type="checkbox"/> IP500 V2 *)	192.168.1.40
User name	aurenzSDKUser
Password	*****
<input type="button" value="Test access"/>	
User rights for the authorization switch	
Allow external calls	Unblocked
Block external calls	Blocked

\*) If an "Application Server" (in connection with an IP500 V2) is used, the server IP/name of the IP500 V2 must be entered here. The "Application Server" must be entered in the "Server IP/Name" field.

**Note:** The other tabs are also configured as part of the AlwinPro setup but are not the focus of these Application Notes.

The Expansion is configured as a separate data source to collect the CDR. The only difference to Server Edition is that the no REST API is used. There is only a connection from AlwinPro to the Server Edition. To configure this, leave the **Server IP / name** empty (so all the other parameters are unimportant for the Expansion).

General	PBX	Time Period	Trunk seizure	Fax extensions	Avaya IP Office
Avaya Vernetzung	Script	REST-API settings	Scan Directory	TCP/IP Settings	Help

Server IP / name		
Port	7070	<input checked="" type="checkbox"/> Use SSL
<input type="checkbox"/> IP500 V2 *)		
User name	aurenz	
Password	*****	
<button>Test access</button>		
User rights for the authorization switch		
Allow external calls	Unblocked	
Block external calls	Blocked	

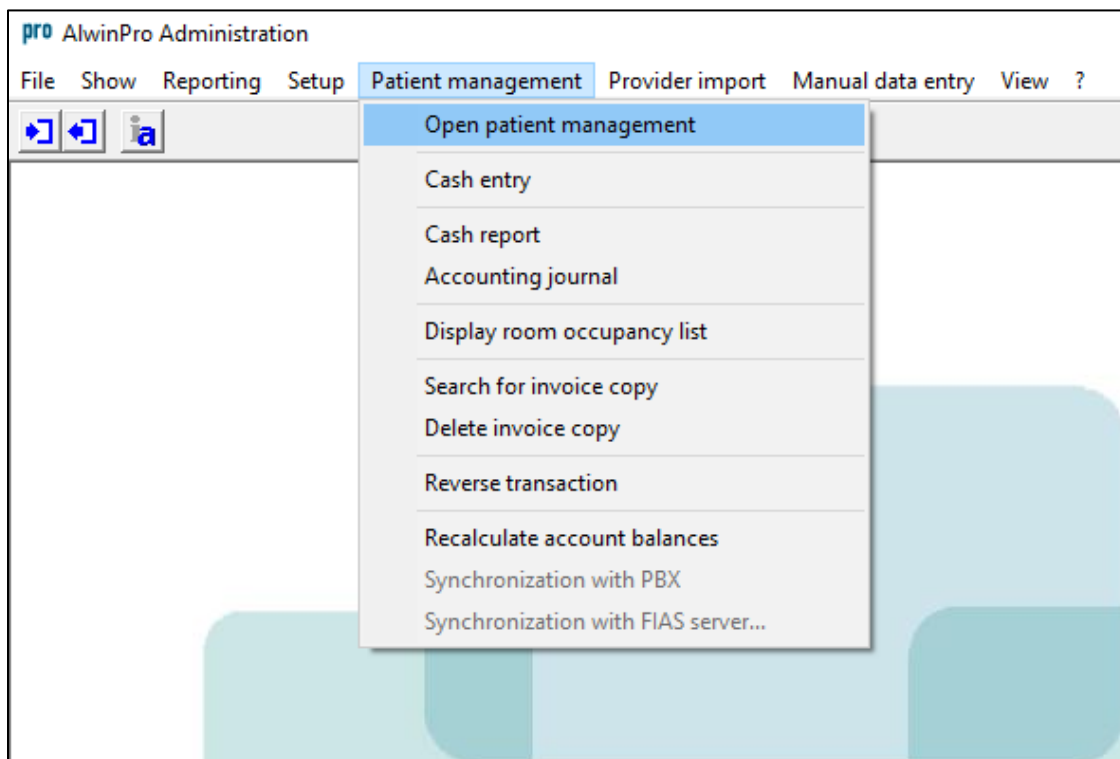
\*) If an "Application Server" (in connection with an IP500 V2) is used, the server IP/name of the IP500 V2 must be entered here. The "Application Server" must be entered in the "Server IP/Name" field.

## 7. Verification Steps

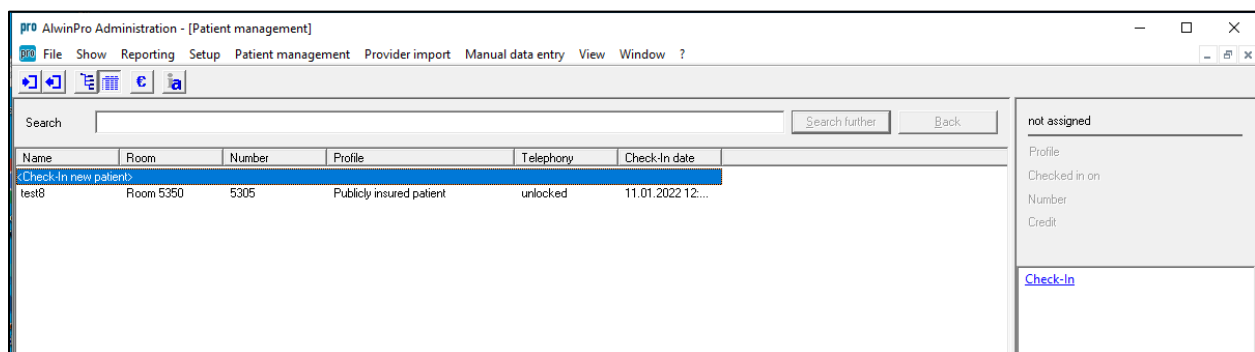
This section provides tests that can be performed to verify correct configuration of the Avaya and aurenz GmbH solution. To verify the solution, a client is “checked in” on the AlwinPro Hotel/Care and the User Rights and Name are then verified on IP Office.

### 7.1. Verify AlwinPro Hotel/Care Management

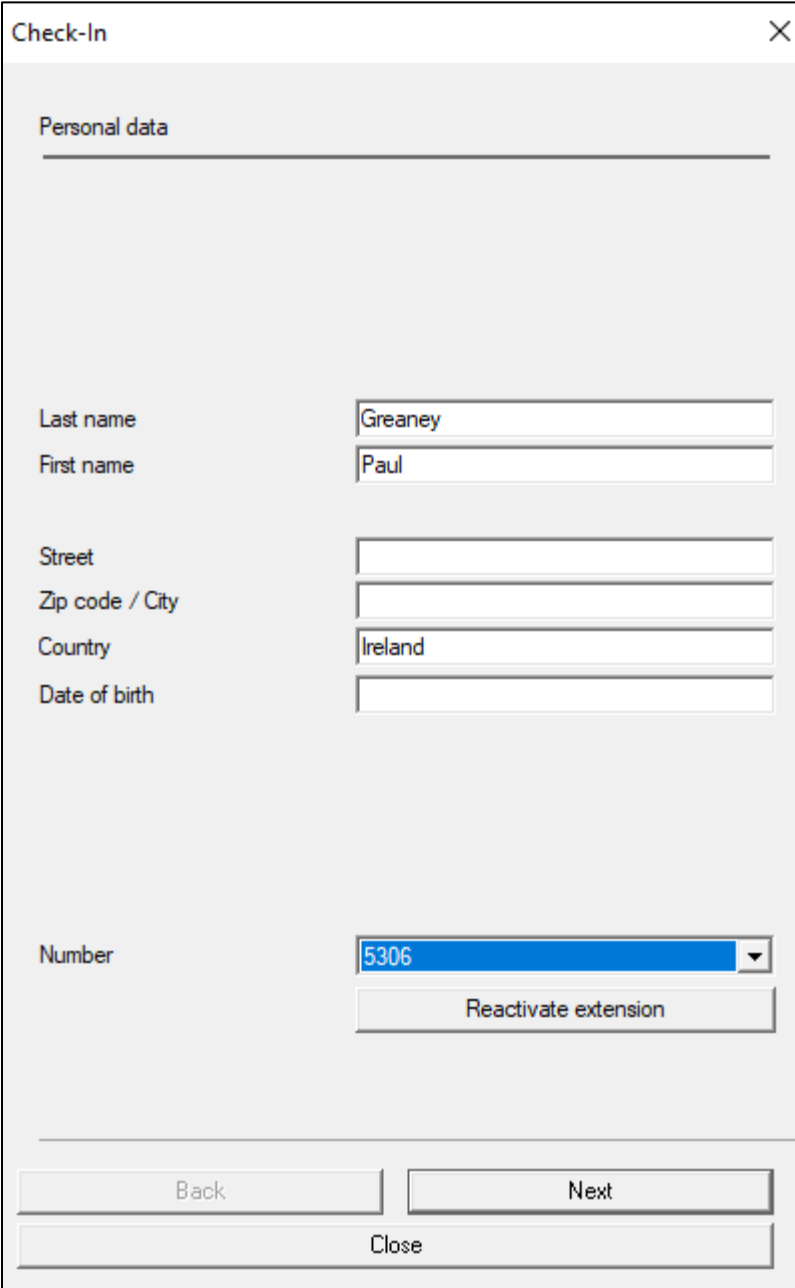
A user/client is ‘checked in’ on **AlwinPro Administration**. Open the AlwinPro Administration as per **Section 6.1**. Navigate to **Patient management** → **Open patient management**.



<Check-In new patient> is highlighted in the main window and **Check-In** is clicked in the right window.



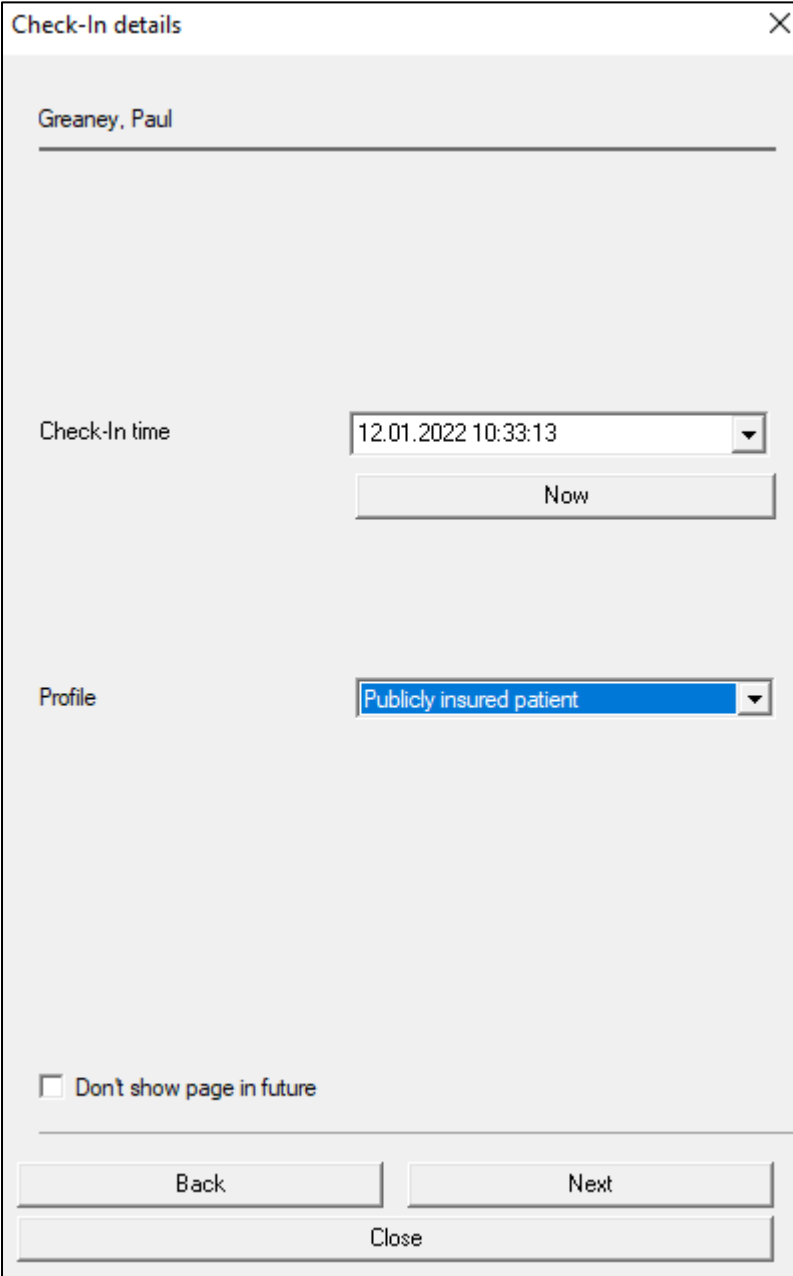
A distinct name is given and noted. The **Number** added here is a hunt group number that was configured earlier in **Section 5.3** on the IP Office setup. Click on **Next** to continue.



The image shows a 'Check-In' dialog box with a close button (X) in the top right corner. The dialog is titled 'Check-In' and contains a section labeled 'Personal data' with a horizontal line underneath. Below this line are several input fields: 'Last name' with the value 'Greaney', 'First name' with the value 'Paul', 'Street' (empty), 'Zip code / City' (empty), 'Country' with the value 'Ireland', and 'Date of birth' (empty). Below these fields is a 'Number' dropdown menu showing '5306' and a 'Reactivate extension' button. At the bottom of the dialog are three buttons: 'Back', 'Next', and 'Close'.

Personal data	
Last name	Greaney
First name	Paul
Street	
Zip code / City	
Country	Ireland
Date of birth	
Number	5306
<button>Reactivate extension</button>	
<hr/>	
<button>Back</button>	<button>Next</button>
<button>Close</button>	

The **Check-In time** is automatically filled in and the **Profile** can be selected depending on whether the patient is insured or not. Click on **Next** to continue.



A screenshot of a 'Check-In details' dialog box. The dialog has a title bar with a close button (X). Inside, the patient's name 'Greaney, Paul' is displayed at the top. Below this, there are two main sections. The first section is for 'Check-In time', showing a dropdown menu with the value '12.01.2022 10:33:13' and a 'Now' button below it. The second section is for 'Profile', showing a dropdown menu with the value 'Publicly insured patient'. At the bottom left, there is a checkbox labeled 'Don't show page in future'. At the bottom, there are three buttons: 'Back', 'Next', and 'Close'.

Check-In details

Greaney, Paul

Check-In time 12.01.2022 10:33:13

Now

Profile Publicly insured patient

☐ Don't show page in future

Back Next

Close

These details were left as default but could be changed to suit the client's needs. Click on **Next** to continue.

The screenshot shows a software window titled "Enable check-in services" with a close button (X) in the top right corner. The window contains the following elements:

- Patient Information:** The name "Greaney, Paul" is displayed at the top.
- Profile:** A label "Profile" is followed by the text "Publicly insured patient".
- Enable telephone use:** A checked checkbox is followed by the text "Enable telephone use".
- Daily usage charge:** A label "Daily usage charge" is followed by a dropdown menu showing "Daily charge for telephone usage".
- Enable use till (included):** An unchecked checkbox is followed by the text "Enable use till (included)".
- Other daily charge:** A label "Other daily charge" is followed by a checkbox labeled "Daily newspaper".
- One-time charge at check-in:** A label "One-time charge at check-in" is followed by an empty text input field.
- Don't show page in future:** An unchecked checkbox is followed by the text "Don't show page in future".
- Navigation Buttons:** At the bottom, there are three buttons: "Back", "Next", and "Close".

When assigning a room, a telephone is also assigned. Because this client is a patient, a virtual number was already assigned as their DDI, this being the hunt group number. The number below is the actual IP Office extension number that will then be associated with the hunt group. Click on **Next** to continue.

Check-In assign bed

Greaney, Paul

☒ Assign patient a bed/room

Search

AlwinPro

- 1. Floor
  - Server Side
    - Room 5321

Back Next Close

Here, credit can be added to is user, where €10 is added below. This will allow them to make outgoing calls or access other services on the system. Click on **Execute** to complete the check-in.

Check in

Greaney, Paul

Cash register Cash register

Advance payment

Amount that was paid in advance by the patient 10.00

Total amount to be paid 10.00

☐ Print receipt Number 1

Back Execute

Close



Once checked in, other changes can be then made to this user by selecting any of the menu options in the right window.

The screenshot shows the 'AlwinPro Administration - [Patient management]' window. It features a menu bar with options: File, Show, Reporting, Setup, Patient management, Provider import, Manual data entry, View, Window, and ?. Below the menu is a toolbar with icons for search, list, and other functions. A search bar is present with a 'Search further' button and a 'Back' button. The main area displays a table of patients with columns: Name, Room, Number, Profile, Telephony, and Check-in date. The table has two rows: 'Greaney, Paul' (Room 5321, Number 5306, Profile: Publicly insured patient, Telephony: unlocked, Check-in date: 12.01.2022 10:...) and 'test8' (Room 5350, Number 5305, Profile: Publicly insured patient, Telephony: unlocked, Check-in date: 11.01.2022 12:...). The 'Greaney, Paul' row is selected. To the right of the table is a panel for the selected patient, 'Greaney, Paul'. It shows details: Profile (Publicly insured patient), Checked in on (12.01.2022 10:33:13), Number (5306), and Credit (9.00). Below this are several action links: 'Additional information', 'Change personal data', 'Change check-in data', 'Move to new room', 'Enter time of absence', 'Check out', 'Make advance payment', and 'Create interim bill'.

Name	Room	Number	Profile	Telephony	Check-in date
Greaney, Paul	Room 5321	5306	Publicly insured patient	unlocked	12.01.2022 10:...
test8	Room 5350	5305	Publicly insured patient	unlocked	11.01.2022 12:...

Greaney, Paul

Profile Publicly insured patient

Checked in on 12.01.2022 10:33:13

Number 5306

Credit 9.00

[Additional information](#)

[Change personal data](#)

[Change check-in data](#)

[Move to new room](#)

[Enter time of absence](#)

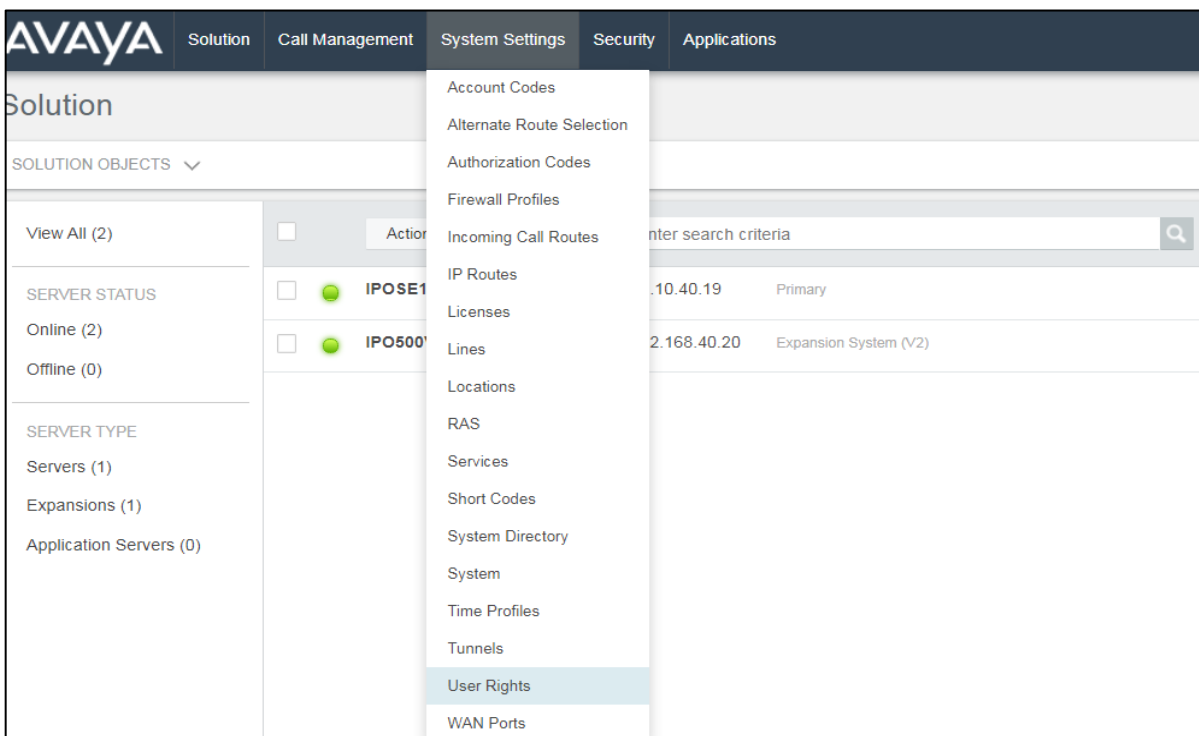
[Check out](#)

[Make advance payment](#)

[Create interim bill](#)

## 7.2. Verify IP Office

From the home menu of the IP Office Web Manager, select **System Settings** → **User Rights**.



To see what users are checked in, the **Unblocked** User Rights is selected, as that will show what users can call outbound, this should be the case for any user that is checked in, with all other users not checked on in having the Blocked User Rights.

The screenshot shows the 'User Rights' page in the Avaya IP Office Web Manager. The page has a search bar and a 'Delete' button. A table lists various user rights, with 'Unblocked' selected. The table columns are Name, Priority, External Call Barring, and System Name. The 'Unblocked' row is highlighted.

Name	Priority	External Call Barring	System Name
Paging	5	No	IPOSE11
T3 default	5	No	IPOSE11
<b>Unblocked</b>	5	No	IPOSE11
Agent	5	No	IPOS00V2PG
Application	5	No	IPOS00V2PG
Blah	5	No	IPOS00V2PG
Blocked	5	Yes	IPOS00V2PG
Boss	5	No	IPOS00V2PG
checkin	5	No	IPOS00V2PG
checkindnd	5	No	IPOS00V2PG
checkout	5	Yes	IPOS00V2PG
Default	5	No	IPOS00V2PG

Displaying 1 - 34 of 34

Click on the **User Rights Membership** on the left pane. Verify on the right pane that the appropriate rooms are Checked-In. The screen shot below shows that both IP Office phones **5321** and **5350** are Unblocked, so that means that two guests assayed with these phones are checked in. Further investigations (shown below) can be made to ensure the name on the phones are correct.

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

**User Rights** | **Unblocked**  
IPOSE11

User  
Short Codes  
Button Programming  
Telephony  
**User Rights Membership**  
Voicemail  
Forwarding

Members of this User Right

<input type="checkbox"/>	Name	Extension
<input type="checkbox"/>	5322	5322
<input type="checkbox"/>	5352	5352
<input type="checkbox"/>	5330	5330
<input checked="" type="checkbox"/>	5321	5321
<input type="checkbox"/>	5381	5381
<input type="checkbox"/>	5351	5351
<input type="checkbox"/>	5331	5331
<input type="checkbox"/>	NoUser	
<input checked="" type="checkbox"/>	5350	5350
<input type="checkbox"/>	5332	5332
<input type="checkbox"/>	5382	5382
<input type="checkbox"/>	5380	5380

Navigate to **Call Management → Users** in the top menu and selected one of the phones above, the example below shows that **Paul Greaney** is logged into extension **5321** as per **Section 7.1**.

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

**Users**

Extensions  
Groups  
Users

Show All

SYSTEMS  
☒ IPOSE11  
☐ IPO500V2PG

PROFILE  
☐ Basic User  
☐ Power User  
☐ Office Worker User  
☐ Non-licensed User

Actions + Add User

Search: "Extension", "System name"

Edit Multiple Delete

<input type="checkbox"/>	Name	Full Name	Extension	Hunt Groups	Voicemail	Email A...	Password	Voicem...	Login C...	System ...	
<input checked="" type="checkbox"/>	5321	Greaney Paul	5321	Aurenz5306	On			****	****	IPOSE11	
<input type="checkbox"/>	5322	SIP SE 5322	5322		On			****	****	IPOSE11	
<input type="checkbox"/>	5330	Equinox5330	5330		Off			****	****	IPOSE11	
<input type="checkbox"/>	5331	Equinox5331	5331		Off			****	****	IPOSE11	
<input type="checkbox"/>	5332	Equinox5332	5332		Off			****	****	IPOSE11	
<input type="checkbox"/>	5350	test8	5350	MainHG	Off			****	****	IPOSE11	

## 8. Conclusion

A full and comprehensive set of feature functional test cases were performed during compliance testing. aurenz GmbH AlwinPro Hotel/Care v13.2 is considered compliant with Avaya IP Office R11.1.

## 9. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

- [1] *Administering Avaya IP Office™ Platform with Manager*. Release 11.0, February 2019
- [2] *Application Notes for aurenz GmbH AlwinPro UC-Edition with Avaya IP Office to collect Call Detail Records (CDR)*

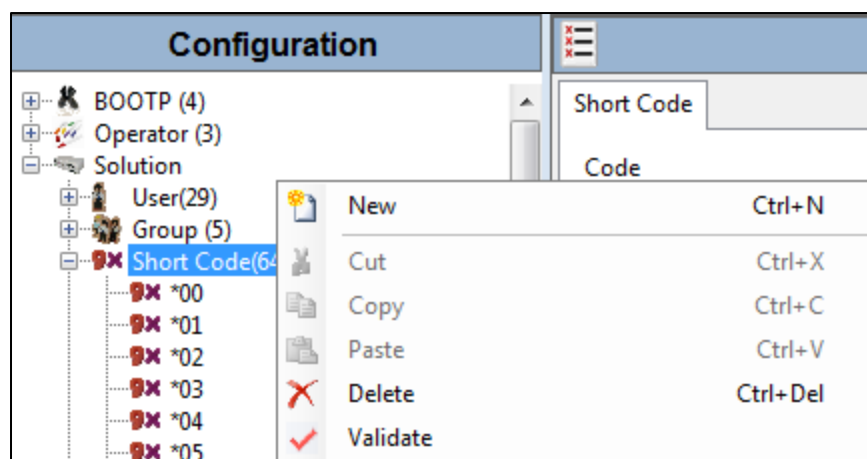
Information on the installation and configuration of AlwinPro Hotel/Care can be found at <https://www.aurenz.de>.

# Appendix

## 10. Barring of Direct Incoming Calls to an Extension

The following shows one way of insuring that a certain direct dial-in (DDI) numbers can be barred so as only the hunt group number can be used to contact the user externally.

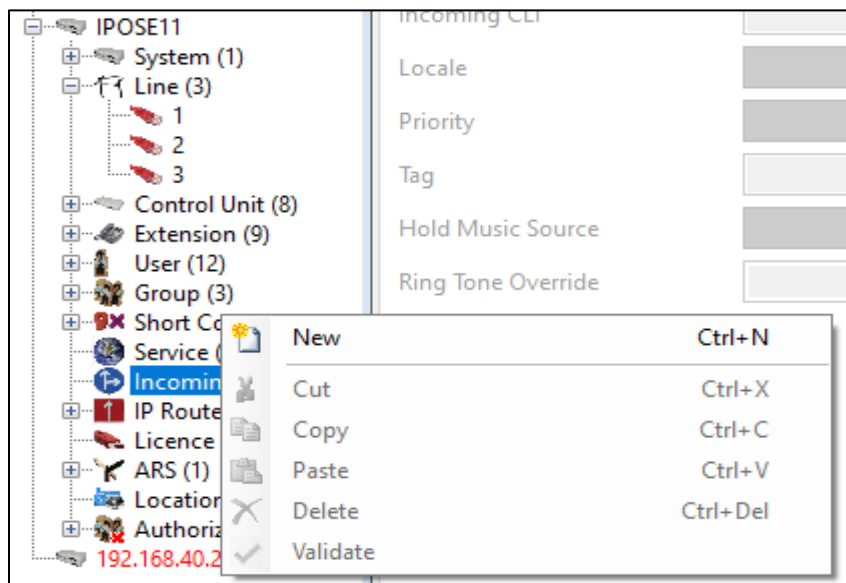
Log into IP Office Manager as shown in **Section 5.4**. To add a new Short Code, right-click on **Short Code** in the left window and select **New**.



Enter a suitable **Code** for the **Barred Feature**.

A screenshot of the '90: Barred' configuration form. The form has a title bar '\*90: Barred'. Below it, there are several fields: 'Short Code' (a tab), 'Code' (text box with '\*90'), 'Feature' (dropdown menu with 'Barred'), 'Telephone Number' (text box), 'Line Group ID' (text box with '9'), 'Locale' (dropdown menu), 'Force Account Code' (checkbox), and 'Force Authorization Code' (checkbox). A red message says '\* This Short Code is common to all systems.'

A new Incoming Call Route must be added to divert the DDI call to the new Barred Short Code. From the left window, right-click on **Incoming Call Route** and select **New**.

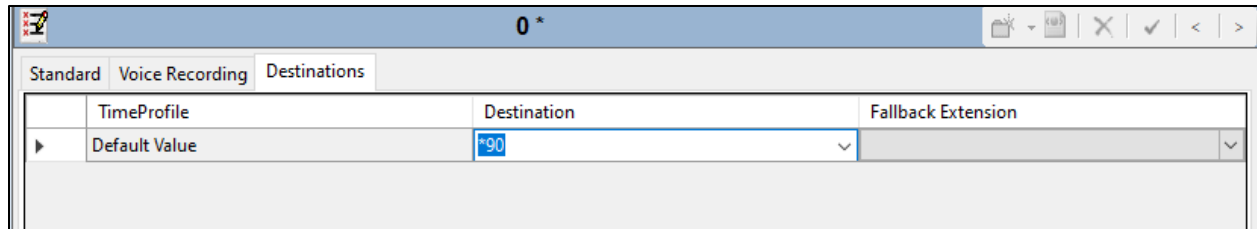


Here, the incoming calls are received on Line 9, so **9** is entered as the **Line Group ID**. Also, the example below shows a DDI of **091735350** as the **Incoming Number**, this call was headed for extension 5350 but will now be diverted to Short Code \*90, which is the barred feature.

A screenshot of the 'Incoming Call Route' configuration form. The form has tabs for 'Standard', 'Voice Recording', and 'Destinations'. The 'Standard' tab is active. The form contains the following fields:

- Bearer Capability: Any Voice (dropdown)
- Line Group ID: 9 (dropdown)
- Incoming Number: 091735350 (text input)
- Incoming Sub Address: (empty text input)
- Incoming CLI: (empty text input)
- Locale: (empty dropdown)
- Priority: 1 - Low (dropdown)
- Tag: (empty text input)
- Hold Music Source: System Source (dropdown)
- Ring Tone Override: None (dropdown)

Under the **Destinations** tab, the **Destination** is changed from 5350 to **\*90**. That means that when 091735350 is dialled, it will come into the Incoming Call Route and the DDI is matched with that from the previous page and the new Destination is the Barred feature, meaning the call will not be completed as dialled.



The screenshot shows a software interface with a top bar containing a logo, the text "0\*", and several icons. Below the bar are three tabs: "Standard", "Voice Recording", and "Destinations". The "Destinations" tab is active. It contains a table with three columns: "TimeProfile", "Destination", and "Fallback Extension".

TimeProfile	Destination	Fallback Extension
Default Value	*90	

---

**©2022 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).