



Avaya Solution & Interoperability Test Lab

Application Notes for configuring GT-HOSP / HOTELIUM 1.0.1.5 from GT2F with Avaya IP Office IP500 V2 Standalone R10.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for call accounting and billing functionality of the GT-HOSP / HOTELIUM from GT2F to successfully interoperate with Avaya IP Office IP500 V2 R10.0.

Readers should pay particular 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 compliance tested configuration of GT-HOSP / HOTELIUM from GT2F to interoperate with Avaya IP Office IP500 V2 Standalone R10.0.

GT-HOSP is a graphical hospitality user interface. It is commonly used in hotels to provide a way to control usage of room facilities and bill the calls. GT-HOSP uses XML based communication for hospitality control of the IP Office. Hospitality features are translated into a set of XML commands which are passed by a secure IP port to the IP Office.

GT-HOSP provides the following features with the IP Office:

- Check-In (Used to make changes to the user rights on IP Office)
- DDI Allocation (Allocate an IP Office hunt group to the user)
- Update Name (A facility that updates the display name of the user on IP Office)
- Room Transfer (Moves the rights and name display from one IP Office user to another)
- DND (Do not Disturb)
- Telephone Service Class (User rights to allow the blocking of outgoing calls)
- Check-out (Similar to check-in)
- Room Status (Allows the cleaners apply short codes to update the room status)
- Prepayment (Allows the addition of Credit to a client's bill)
- SMDR - Call billing (Call Detail Records from IP Office)

Note: GT-HOSP / HOTELIUM will be referred to as GT-HOSP throughout the remainder of these Application Notes.

Note: These Application Notes focus on two modules/connections to IP Office. The SMDR connection for call billing and the XML connection to show the ability of GT-HOSP to change User Rights on IP Office extensions.

Note: IP Office CDR is called Station Message Detail Reporting (SMDR), so CDR may be referred to as CDR or SMDR throughout the remainder of this document as they both refer to call detail records.

2. General Test Approach and Test Results

The general test approach was to configure the GT-HOSP to communicate with the IP Office as implemented on a customer's premises. Testing focused on two complementing modules of GT-HOSP verifying that Station Message Detail Reports (SMDR) are collected by the GT-HOSP and received in the format as generated by the IP Office, in addition customers were checked in/out to verify that GT-HOSP was able to make the necessary changes to user rights on the phone sets in question. Various call scenarios were preformed to simulate real call types as would be observed on a customer's premises. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of GT-HOSP to carry out hospitality functions through XML based communication with IP Office. The serviceability testing introduced failure scenarios to see if GT-HOSP could resume after a link failure with IP Office. The Hospitality testing included:

- Check-in/Check-out
- DDI update/Name update
- Telephone Service Class
- Room Status
- Room Transfer
- DND
- Prepayment
- Link Failure/Recovery

The SMDR test cases included:

- Local internal call handling
- Handling of Incoming calls
- Handling of Outgoing Calls
- Call Forwarding on Busy/No Answer/Unconditional
- Transfers – Blind and Supervised
- Conference Calls
- Account Codes/Authorization Codes
- Call Park

2.2. Test Results

Tests were performed to insure full interoperability between GT2F GT-HOSP / HOTELIUM and IP Office. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully except for the following issues which were noted.

Observations for SMDR:

1. Sending Short Code for SMDR - This is an issue with the SMDR data not displaying the short code when inputted from H323 phones. This is displayed when inputted from a SIP phone.
2. Call Park – When a SIP phone parks the call, there is an ‘extra’ record produced. This record resembles that like a call to a number with DND.
3. Conference Call - On IP Office R9, the field party 2 was filled with V<1>conf#channel# On IP Office R10 the same kind of call shows V83896083. According to the last SMDR documentation, the format is still described with V<1>conf#channel#. Either there is a bug or the documentation needs to be updated. This was reported to the IP Office R&D team.
4. AUTH Code & Account Code –The fields seem to be swapped in the Rel 10.0 docs. This was reported to the IP Office R&D team.

Observations for Hospitality:

1. Short Code for Room Status – When the short code plus the digits are dialled the phone returns a “number busy” which would lead to the person dialling thinking that it was not accepted. GT2F is looking at implementing a more user friendly design in a future release.
2. LAN Disconnect – When the LAN is disconnected the user can still check in/check out people but the phones are not actually being checked in/out.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 9** of these Application Notes. Technical support for the GT2F GT-HOSP / HOTELIUM product can be obtained as follows.

- Phone: +33 8 92 140 150 (French Customers)
+33 4 66 62 94 65 – Choice number 2 (International Customers)
- E-mail: hotline@gt2f.com

3. Reference Configuration

Figure 1 shows an Avaya IP Office IP500 V2 R10.0 serving H323, SIP and Digital endpoints. GT-HOSP / HOTELIUM was configured on the same IP network for the transfer of CDR data from Avaya IP Office IP500 V2 to the GT-HOSP server using the SMDR output on the IP Office. The Web Service host was used for room management through XML.

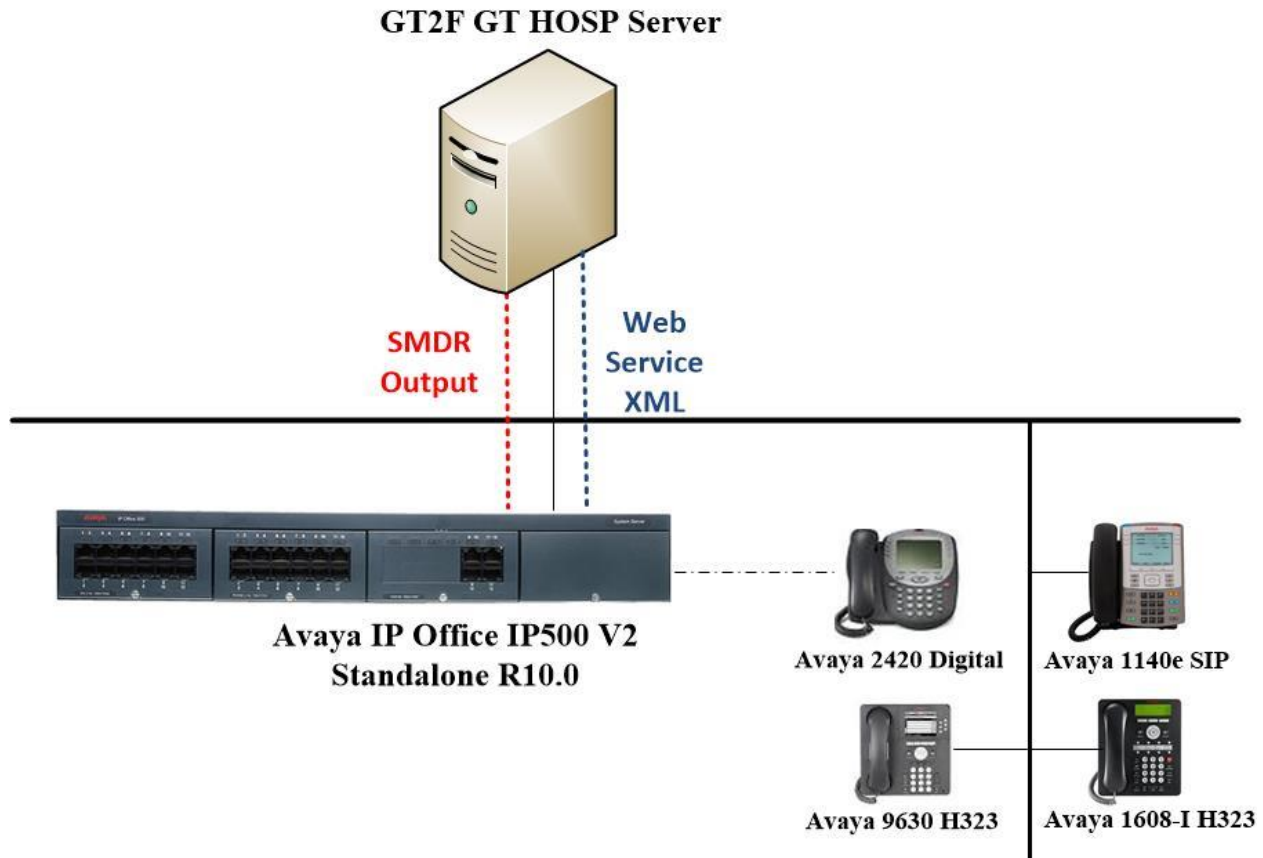


Figure 1: Network solution of GT2F GT-HOSP / HOTELIUM and Avaya IP Office IP500 V2 R10.0

4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|--|--------------------------------|
| Avaya IP Office IP500 V2 Standalone | R10.0.0.3.0 Build 5 |
| Avaya IP Office Manager running on a Windows 7 PC | R10.0.0.3.0 Build 5 |
| Avaya 9630 H323 Deskphone | R6.4014U |
| Avaya 1140e SIP Deskphone | R04.04.28.00 |
| Avaya 1608 I Deskphone | H323 1608UA1_350B.bin |
| Avaya 2420 Digital Deskphone | V5.0 |
| GT-HOSP / HOTELIUM CONNECTOR MODULE (SMDR and hospitality command) | 1.0.1.5 Build 2 |
| GT-HOSP / HOTELIUM CENTRAL MODULE (DB and software management) | 1.0.1.5 Build 2 |
| GT-HOSP / HOTELIUM REPORT MODULE (HOSPITALITY – end user interface) | 1.0.1.5 Build 2 |
| Client PC running Windows 7 FireFox Firebird MS C++ Runtime 2012 MS .Net | 53.0.0 2.5.2 11.0 4.0 |

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office IP500 V2 only.

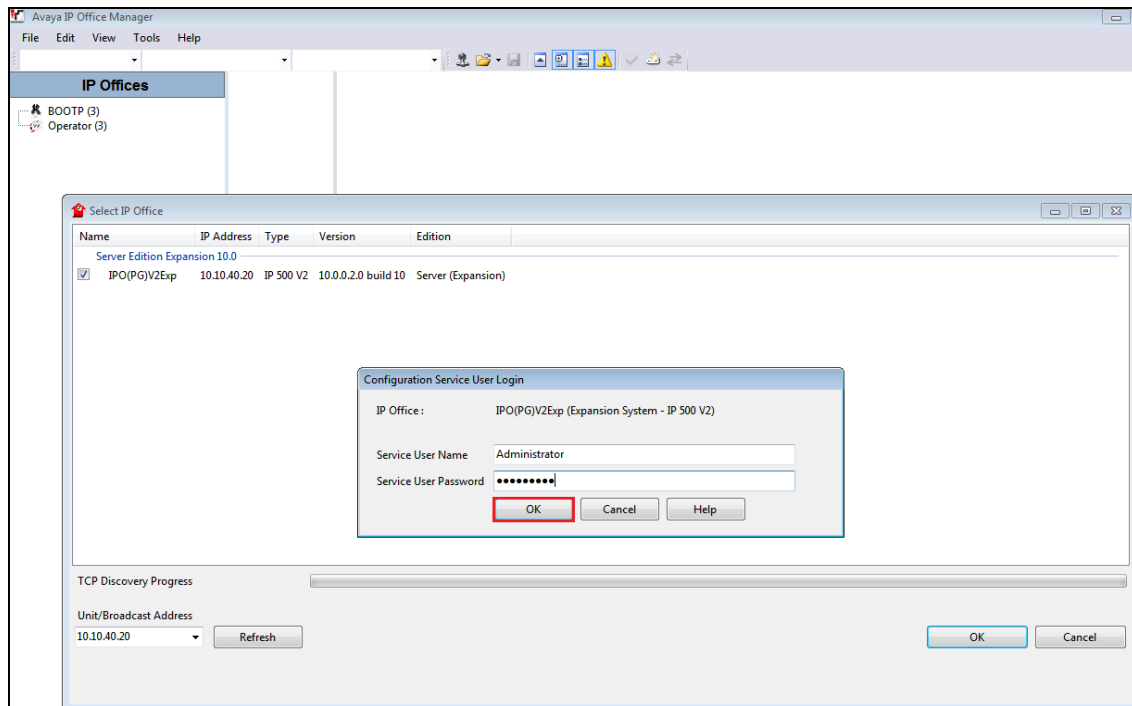
5. Avaya IP Office Configuration

Configuration and verification operations on the Avaya IP Office 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. 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.
- Display LAN Configuration.
- SMDR Configuration.
- Check IP Office Security.
- Create Virtual User.
- Modify User Rights.
- Create DDI Hunt Group.
- Add Incoming Call Route.
- Create Short Codes.
- Update Existing Users.
- Save Configuration.

5.1. Launch Avaya IP Office Manager (Administration)

From the IP Office Manager PC, click **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application (not shown). Enter the appropriate credentials and click on the **OK** button to receive the IP Office configuration.



5.2. Display LAN Configuration

From the left window navigate to **System** as shown and in the main window click on the **LAN1** tab and within that tab select the **LAN Settings** tab. The **IP Address** of the IP Office along with the information below in **Section 5.3** will be required in the GT-HOSP setup in **Section 6.1**.

The screenshot shows the IP Office configuration interface. On the left, the 'System' tree is expanded, showing 'IPO91(PG)V2Exp' and 'System (1)'. The main window has tabs for 'System', 'LAN1', 'LAN2', 'DNS', 'Voicemail', 'Telephony', 'Directory Services', and 'System Events'. The 'LAN1' tab is selected, and within it, the 'LAN Settings' sub-tab is active. The 'IP Address' field is highlighted with a red box and contains the value '10 . 10 . 40 . 20'. Other fields include 'IP Mask' (255 . 255 . 255 . 0), 'Primary Trans. IP Address' (10 . 10 . 40 . 1), 'RIP Mode' (None), 'Enable NAT' (unchecked), 'Number Of DHCP IP Addresses' (10), and 'DHCP Mode' (Disabled). An 'Advanced' button is visible at the bottom right.

5.3. SMDR configuration

Select the **SMDR** tab and enter the following information:

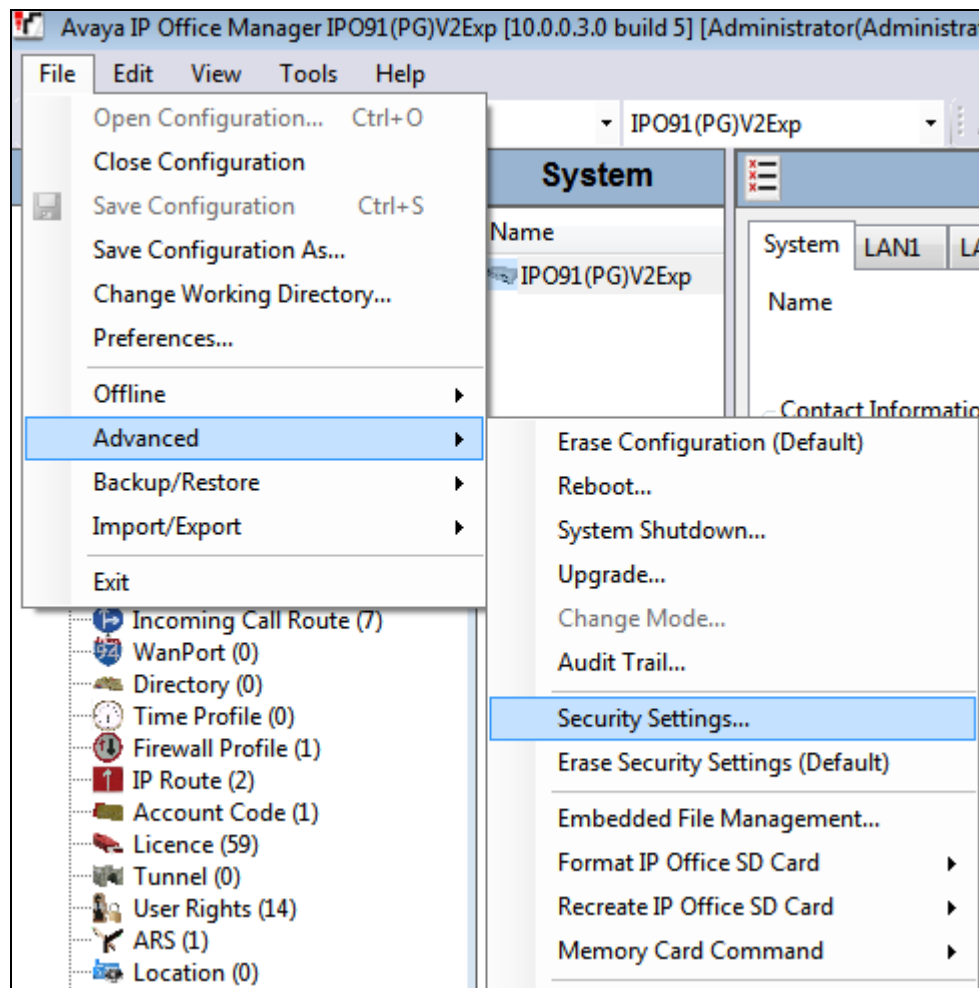
- **Output** Select **SMDR Only** from the drop box.
- **IP Address** Enter **0.0.0.0** for the IP Address.
- **TCP Port** Enter **8000**
- **Records to buffer** Enter **500**, this was left as default. (**Note:** 3000 is the maximum and was recommended).
- Click the **Call Splitting for Diverts**, check the box.

Click the **OK** button to save (not shown).

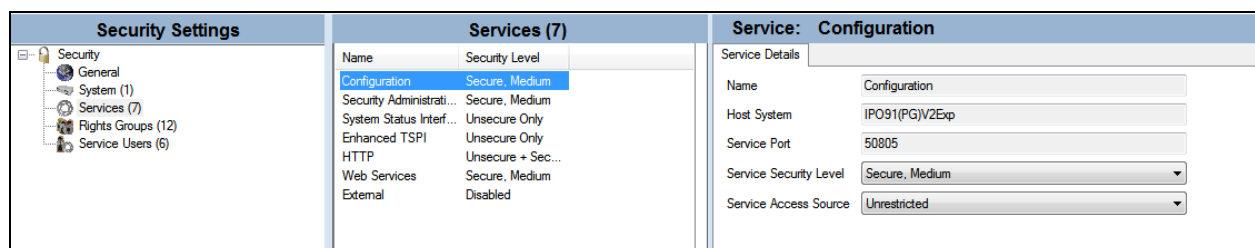
The screenshot shows the 'SMDR' configuration window in the IP Office interface. The 'Output' dropdown is set to 'SMDR Only'. The 'SMDR' section contains the following fields: 'Station Message Detail Recorder Communications' (a sub-section header), 'IP Address' (0 . 0 . 0 . 0), 'TCP Port' (8000), 'Records to Buffer' (500), and a checked checkbox for 'Call Splitting for Diverts'. The window title is 'IPO91(PG)V2Exp'.

5.4. Check Avaya IP Office Security

Open IP Office Security navigating to **File → Advanced → Security Settings**.

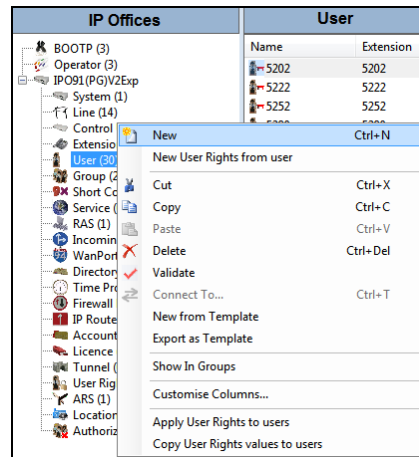


Navigate to **Services** in the left window and **Configuration** in the middle window and make the necessary changes to the **Service Port** or **Service Security Level** as shown below.



5.5. Create Virtual User

A user must be created for changing the room state. This is done by dialing a Short Code that in turn dials this virtual user. In the left window right-click on **User** and click on **New** as shown below.



Enter a suitable **Name** and **Password**. Enter the **Extension** for this new user, even if this extension does not exist yet.

RoomStatus: 5270

User | Voicemail | DND | ShortCodes | Source Numbers | Telephony | Forwarding | Dial In | Voice Recording | Button Programming | Menu Pro

Name: RoomStatus

Password: ****

Confirm Password: ****

Unique Identity:

Audio Conference PIN:

Confirm Audio Conference PIN:

Account Status: Enabled

Full Name:

Extension: 5270

Email Address:

Locale:

Priority: 5

System Phone Rights: None

Profile: Basic User

☒ Receptionist

☐ Enable Softphone

☐ Enable one-X Portal Services

☐ Enable one-X TeleCommuter

☒ Enable Remote Worker

☒ Enable Communicator

☐ Enable Mobile VoIP Client

☐ Send Mobility Email

☐ Web Collaboration

☒ Exclude From Directory

Device Type: Unknown IP handset

Under the **Telephony** → **Supervisor Settings** tab enter the **Login Code**.

RoomStatus: 5270

User Voicemail DND ShortCodes Source Numbers **Telephony** Forwarding Dial In Voice Recording Button Programming Menu Pro

Call Settings **Supervisor Settings** Multi-line Options Call Log TUI

Login Code: ••••

Confirm Login Code: ••••

Login Idle Period (secs):

Monitor Group: <None>

Coverage Group: <None>

Status on No-Answer: Logged On (No change)

Reset Longest Idle Time:

☒ All Calls

☐ External Incoming

☐ Force Login

☐ Force Account Code

☐ Force Authorization Code

☐ Incoming Call Bar

☐ Outgoing Call Bar

☐ Inhibit Off-Switch Forward/Transfer

☐ Can Intrude

☒ Cannot be Intruded

☐ Can Trace Calls

☐ Deny Auto Intercom Calls

Once the user is saved the system will automatically ask to create the extension that was entered, add a **H323 Extension** as shown below.

Avaya IP Office Manager

Would you like a new VoIP extension created with this number?

☐ None

☒ H323 Extension

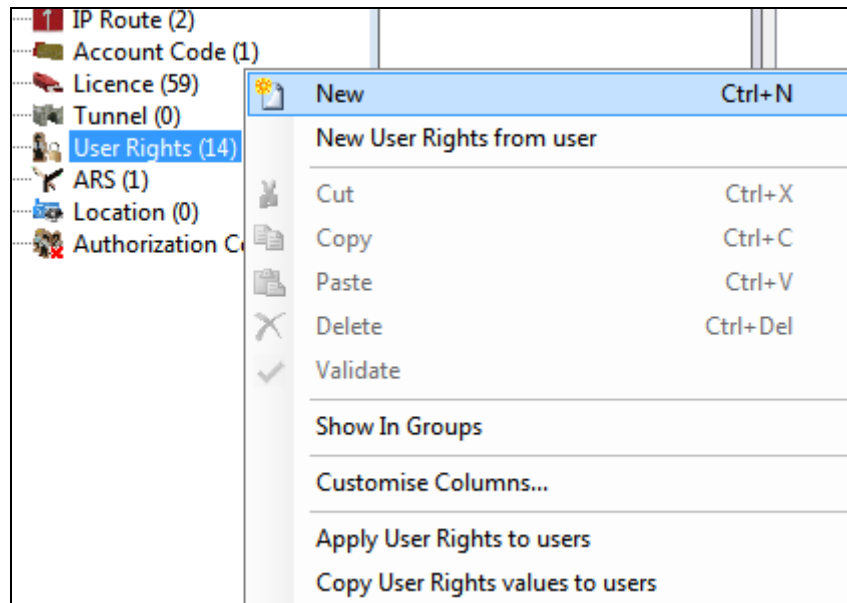
☐ SIP Extension

☐ IP DECT Extension

OK

5.6. Modify User Rights

Some user rights need to be added now also, this will determine if each user will be allowed call out from the hotel room or not. In the left window right-click on **User Rights** and click on **New** as shown below.



5.6.1. Modify User Rights (checkin)

Under the **User** tab, enter the **Name**, **checkin**. (Note: This must be entered exactly as shown below as it is case sensitive).

| checkin | |
|--|---|
| User | ShortCodes Button Programming Telephony User Rights Membership Voicemail Forwarding |
| Name | <input type="text" value="checkin"/> <input type="checkbox"/> Application Servers Group |
| Locale | |
| <input type="text"/> | <input type="text" value="Not part of User Rights"/> |
| Priority | |
| <input type="text" value="5"/> | <input type="text" value="Not part of User Rights"/> |
| Do not disturb | |
| <input type="checkbox"/> Enable do not disturb | <input type="text" value="Not part of User Rights"/> |

Click on the **Telephony** → **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 dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot shows the 'checkin' configuration window with the 'Supervisor Settings' tab selected. The 'Outgoing call bar' section is highlighted, showing the 'Enable outgoing call bar' checkbox unchecked and the dropdown menu set to 'Apply User Rights value'. Other sections like 'Intrusion', 'Force login', 'Force account code', and 'Inhibit Off-Switch Forward/Transfer' are also visible with their respective settings.

5.6.2. Modify User Rights (checkout / locked)

Under the **User** tab, enter the **Name**, **checkout**. (Note: This must be entered exactly as shown below as it is case sensitive).

The screenshot shows the 'checkout' configuration window with the 'User' tab selected. The 'Name' field is set to 'checkout'. The 'Locale', 'Priority', and 'Do not disturb' sections are visible, each with a dropdown menu set to 'Not part of User Rights'.

Click on the **Telephony → 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 dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot shows the 'checkout' configuration window with the 'Supervisor Settings' tab selected. The 'Outgoing call bar' section is expanded, showing the 'Enable outgoing call bar' checkbox checked and the dropdown menu set to 'Apply User Rights value'. Other sections like 'Intrusion', 'Force login', 'Force account code', and 'Inhibit Off-Switch Forward/Transfer' are also visible with their respective settings.

Repeat the process to create an identical user rights with the name “locked” that will be used to block the outgoing calls for prepayment management.

5.6.3. Modify User Rights (checkindnd)

Under the **User** tab, enter the **Name**, **checkindnd**. (Note: This must be entered exactly as shown below as it is case sensitive). Under the section **Do not disturb** at the bottom of the screen, check the box called **Enable do not disturb**, as shown below and ensure that **Apply User Rights Value** is selected opposite Do not disturb from the drop-down box.

The screenshot shows the 'checkindnd' configuration window with the 'User' tab selected. The 'Name' field is set to 'checkindnd'. The 'Do not disturb' section is expanded, showing the 'Enable do not disturb' checkbox checked and the dropdown menu set to 'Apply User Rights value'. Other fields like 'Locale' and 'Priority' are also visible.

Click on the **Telephony → 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 dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot shows the 'checkindnd' configuration window with the 'Supervisor Settings' tab selected. The 'Outgoing call bar' section is expanded, showing the 'Enable outgoing call bar' checkbox unchecked and the dropdown menu set to 'Apply User Rights value'. Other sections like 'Intrusion', 'Force login', 'Force account code', and 'Inhibit Off-Switch Forward/Transfer' are also visible with their respective settings.

5.6.4. Modify User Rights (lockednd)

Under the **User** tab, enter the **Name**, **lockednd**. (Note: This must be entered exactly as shown below as it is case sensitive). Under the section **Do not disturb** at the bottom of the screen, check the box called **Enable do not disturb**, as shown below and ensure that **Apply User Rights Value** is selected opposite Do not disturb from the drop-down box.

The screenshot shows the 'lockednd' configuration window with the 'User' tab selected. The 'Do not disturb' section is expanded, showing the 'Enable do not disturb' checkbox checked and the dropdown menu set to 'Apply User Rights value'. Other fields like 'Name' (lockednd), 'Locale', and 'Priority' are also visible.

Click on the **Telephony → 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 dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot shows a web application window titled "lockedndnd". It has a top navigation bar with tabs: "User", "ShortCodes", "Button Programming", "Telephony", "User Rights Membership", "Voicemail", and "Forwarding". Below this is a sub-navigation bar with "Call Settings", "Supervisor Settings", "Multi-line Options", and "Call Log". The "Supervisor Settings" tab is active. It contains several sections with checkboxes and dropdown menus:

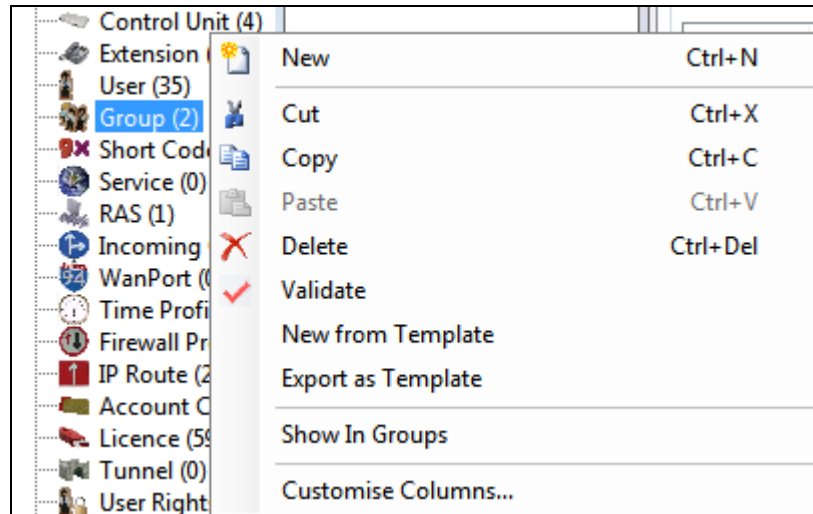
- Intrusion**
 - ☐ Can intrude (dropdown: Not part of User Rights)
 - ☒ Cannot be intruded (dropdown: Not part of User Rights)
 - ☐ Deny Auto Intercom Calls (dropdown: Not part of User Rights)
- Force login**
 - ☐ Enable force login (dropdown: Not part of User Rights)
- Force account code**
 - ☐ Enable force account code (dropdown: Not part of User Rights)
- Inhibit Off-Switch Forward/Transfer**
 - ☐ Enable Inhibit Off-Switch Forward/Transfer (dropdown: Not part of User Rights)
- Outgoing call bar**
 - ☒ Enable outgoing call bar (dropdown: Apply User Rights value)
- Coverage Group**
 - Dropdown: <None> (dropdown: Not part of User Rights)

Any other User Right groups can be added in the same fashion as the ones above. For example, User Rights that restrict specific type of calls (no international).

Note: The value for code must be strictly identical to the name on the manager (case sensitive).

5.7. Create DDI Hunt Group

From the left window, right-click on **Group** and click on **New**.

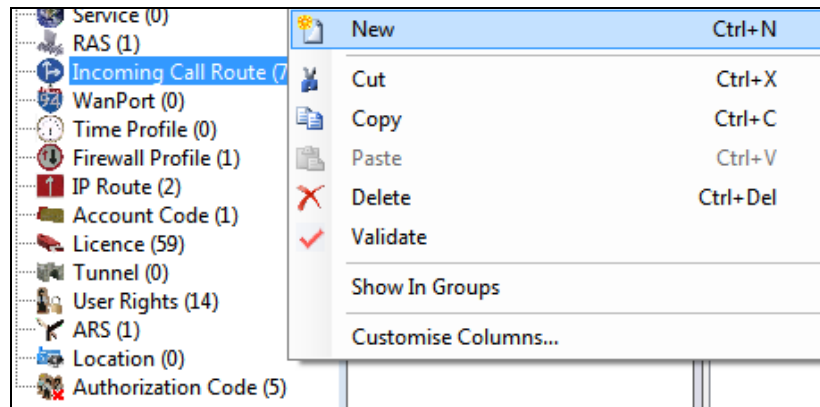


Enter a suitable **Name** and **Extension**. A Hunt Group will need to be added for every “room” in the hotel so as a DDI number can be assigned.

| Extension | Name |
|-----------|------|
|-----------|------|

5.8. Add Incoming Call Route

From the left window, right-click on **Incoming Call Route** and click on **New**.



Enter the **Line Group ID**, this will be the incoming line used for incoming calls to the IP Office, in the example below this was line **17**. The incoming number should be set to that configured for the Hunt Group created in **Section 5.7**.

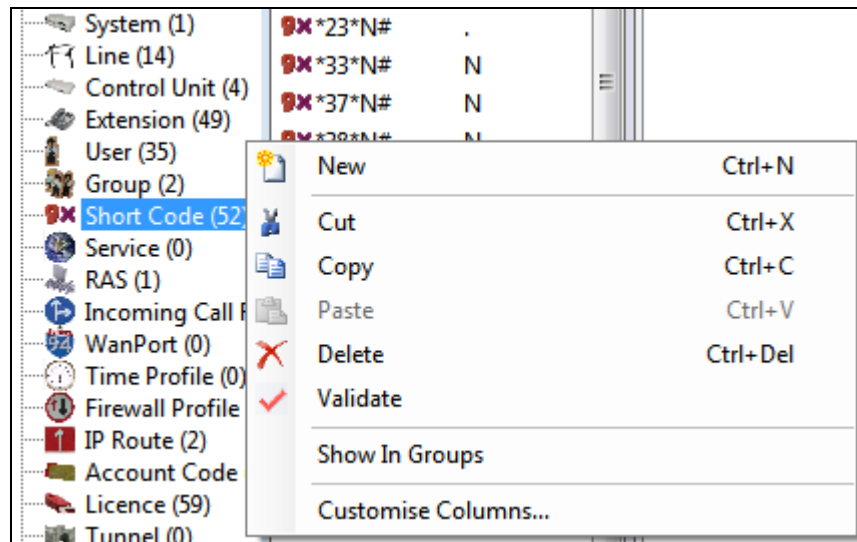
A screenshot of a configuration window titled '17 5295'. It has three tabs: 'Standard', 'Voice Recording', and 'Destinations'. The 'Standard' tab is active. It contains several fields and dropdown menus: 'Bearer Capability' (Any Voice), 'Line Group ID' (17), 'Incoming Number' (5295), 'Incoming Sub Address' (empty), 'Incoming CLI' (empty), 'Locale' (empty), 'Priority' (1 - Low), 'Tag' (empty), 'Hold Music Source' (System Source), and 'Ring Tone Override' (None).

The **Destination** will be set to the same Hunt Group. Click on **OK** once this is completed (not shown).

A screenshot of the same configuration window, but with the 'Destinations' tab active. It shows a table with three columns: 'TimeProfile', 'Destination', and 'Fallback Extension'. The first row has 'Default Value' in the 'TimeProfile' column, '5295 DDI5295' in the 'Destination' column, and an empty dropdown in the 'Fallback Extension' column.

5.9. Create Short Codes

From the left window, right-click on **Short Code** and click on **New**.



*77 was used to initiate this Short Code, *77XXX was entered as the three digits following *77 will determine the room status. The **Feature** is set to **Dial Direct** and the number dialed will be that of the virtual extension that was added in **Section 5.5**.

A screenshot of a configuration window titled '*77XXX: Dial Direct*'. It has a 'Short Code' tab. The fields are: Code (*77XXX), Feature (Dial Direct), Telephone Number (5270), Line Group ID (0), and Locale (empty). There are checkboxes for 'Force Account Code' and 'Force Authorization Code', both of which are unchecked.

For user 5270 (used for room status short code) **Voicemail** must be disabled by unchecking the box **Voicemail On**.

A screenshot of a configuration window with tabs: User, Voicemail, DND, ShortCodes, Source Numbers, Telephony, Forwarding, Dial In, and Voice Recording. The 'Voicemail' tab is selected. It shows a 'Voicemail Code' field and a 'Voicemail On' checkbox, which is unchecked.

5.10. Update Existing Users

Users on IP Office are setup as room numbers, these users will all be set with **Working hours** **User Rights** set to **checkout**. Click on **OK** at the bottom to save these changes (not shown).

The screenshot shows the 'Room5250: 5250*' configuration window. The 'User' tab is selected. The form contains the following fields and options:

- Name:** Room5250
- Password:** [Masked with dots]
- Confirm Password:** [Masked with dots]
- Unique Identity:** [Empty field]
- Audio Conference PIN:** [Empty field]
- Confirm Audio Conference PIN:** [Empty field]
- Account Status:** Enabled (dropdown)
- Full Name:** [Empty field]
- Extension:** 5250
- Email Address:** [Empty field]
- Locale:** [Empty dropdown]
- Priority:** 5 (dropdown)
- System Phone Rights:** None (dropdown)
- ACCS Agent Type:** None

Profile: Basic User (dropdown)

- ☐ Receptionist
- ☐ Enable Softphone
- ☐ Enable one-X Portal Services
- ☐ Enable one-X TeleCommuter
- ☒ Enable Remote Worker
- ☒ Enable Communicator
- ☐ Enable Mobile VoIP Client
- ☐ Send Mobility Email
- ☐ Web Collaboration

☒ Exclude From Directory

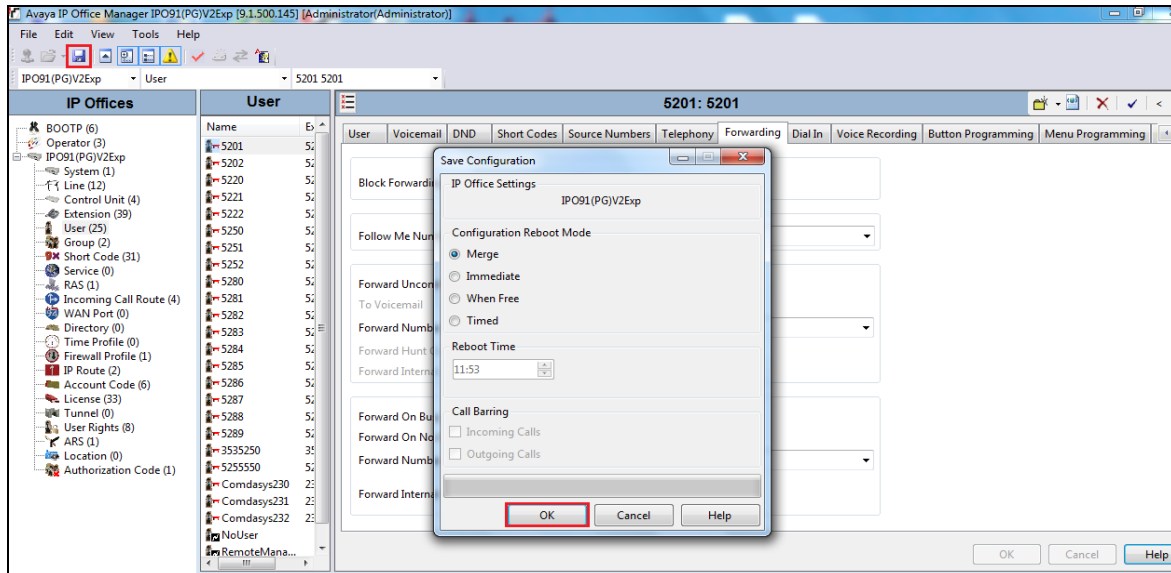
Device Type: Avaya 9630 (with phone icon)

User Rights:

- User Rights view:** Working hours User Rights (dropdown)
- Working hours time profile:** <None> (dropdown)
- Working hours User Rights:** checkout (dropdown)
- Out of hours User Rights:** [Empty dropdown]

5.11. Save Configuration

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 to memory.



6. Configure GT-HOSP

This section describes the steps performed to configure GT-HOSP to connect to IP Office. It is implied that the GT-HOSP server software is already installed and has the appropriate licences. It is also implied that a 'Site' is configured, an 'Operator' is imported, and 'Tariffs' are set.

Also the service for XML commands connection must have been already installed. Refer to the product help guide provided with the software to install it.

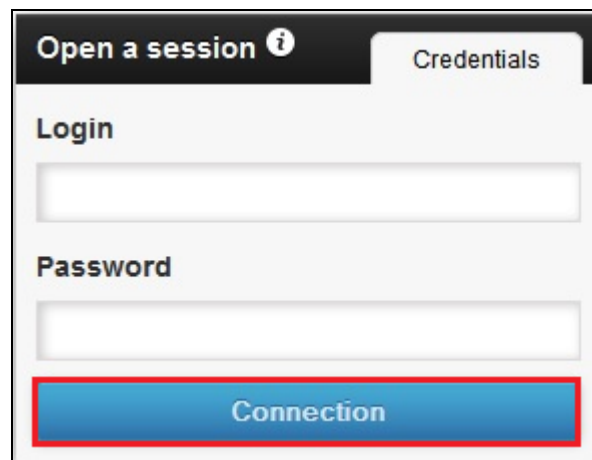
For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. The configuration operations described in this section can be summarized as follows:

- Logging in to GT-HOSP Server.
- GT Connector Configuration.
- Advanced Settings.
- Links Setup.
- Register the GT Connector.

6.1. Logging in to GT-HOSP Server

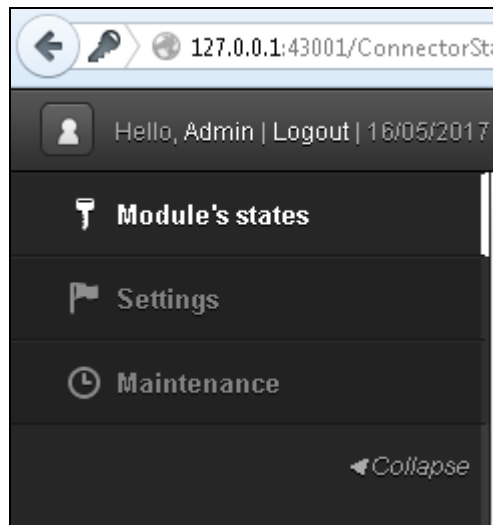
To access the OAM web-based interface of the GT-HOSP server use the URL **http://x.x.x.x:43001**, where **x. x. x. x** is the selected IP address of the GT-HOSP server. When the **Open a session** window opens, log in using the appropriate credentials and click on the **Connection** button.

Note: If logging in on the same server that GT-HOSP is installed on use the URL 172.0.0.1:43001.

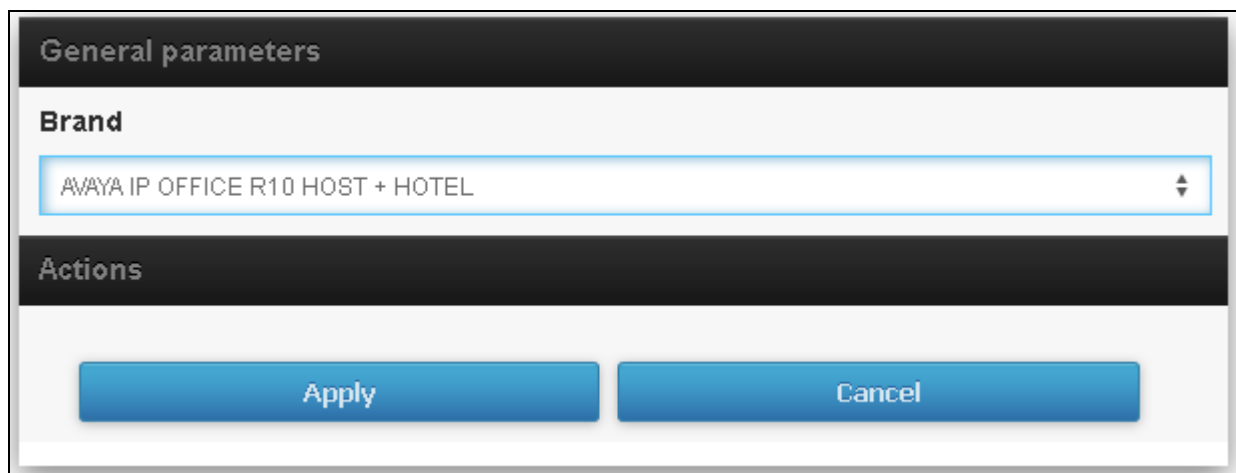


6.2. GT Connector Configuration

Once logged in, click on **Settings** in the left window.



In the **General parameters** window select **AVAYA IP OFFICE R10 HOST + HOTEL** from the **Brand** drop down box.



6.3. Advanced Settings

In the **Advanced parms** window on the right enter the following:

- **CHECKIN** Enter **checkin**
- **CHECKOUT** Enter **checkout**
- **LOCKED** Enter **locked**
- **MANAGEDND** Enter **checkindnd;lockednd**
- **TEMPODHM** Enter **60**
- **USRLOGIN** Enter **Administrator** [Another user can be used with special privileges defined in Security Settings (TAB configuration / Web Services: read/write/merge)]
- **USRPASSWORD** Enter the password set as per **Section 5.1**
- **WEBSERVICE_URL** Enter
http://###WEBSERVICE_IP###:###WEBSERVICE_PORT###/IPOConfigurationService?wsdl
- **WEBSERVICE_PORT** Enter **8085**
- **WEBSERVICE_IP** Enter **127.0.0.1**
- **IPOTYPE** Enter **IPOfficeMMManager**
- **ROOMSTATUS_CODE** Enter ***77**, this is as per **Section 5.9**

| GT-HOSP GT27 | | |
|---------------------|---|--|
| CHECKIN | checkin | CheckIn Group Name |
| CHECKOUT | checkout | CheckOut Group Name |
| LOCKED | locked | Group Name "LOCK" |
| MANAGEDND | checkindnd;lockednd | Manage list of Avaya User's rights in DND without call permissions |
| CHECKOUT_TEXT | Free | |
| TEMPODHM | 60 | Tempo DHM (seconds) |
| CRYPTPWD | 0 | Crypte password (0 = No, 1 = Yes) |
| USRLOGIN | Administrator | User (Avaya) |
| USRPASSWORD | •••••••• | Password (Avaya) |
| WEBSERVICE_URL | http://###WEBSERVICE_IP###:###WEBSERVICE_PORT###/IPOConfigurationService?wsdl | WebService : URL |
| WEBSERVICE_PORT | 8085 | WebService : Port |
| WEBSERVICE_IP | 127.0.0.1 | WebService : IP |
| IPOTYPE | IPOfficeMMManager | IPO Type |
| FORCEREFRESH | 0 | Force reload information, after command sending (0 = No, 1 = Yes) |
| MANAGEHOST | 1 | Manage Avaya Host (Reboots the Avaya HOST Service) (0 = No, 1 = Yes) |
| SERVICE_HOST_NAME | GTConfigServiceHost_Ser | Name of AVAYA host service (present in Windows services) |
| CHECKCONFIGEACH | 60 | Check configuration (Ext. State) each XX mn |
| TRACETYPE | 3 | 0: tstNone 1: tstBefore 2: tstAfter 3: tstBoth |
| DISPLAYTRACE | 1 | Display Trace |
| SAVECMD | 1 | Save commands (0 = No, 1 = Yes) |
| ROOMSTATUS_CODE | *77 | Room status. |

Scroll to the down along the page and enter the remaining information:

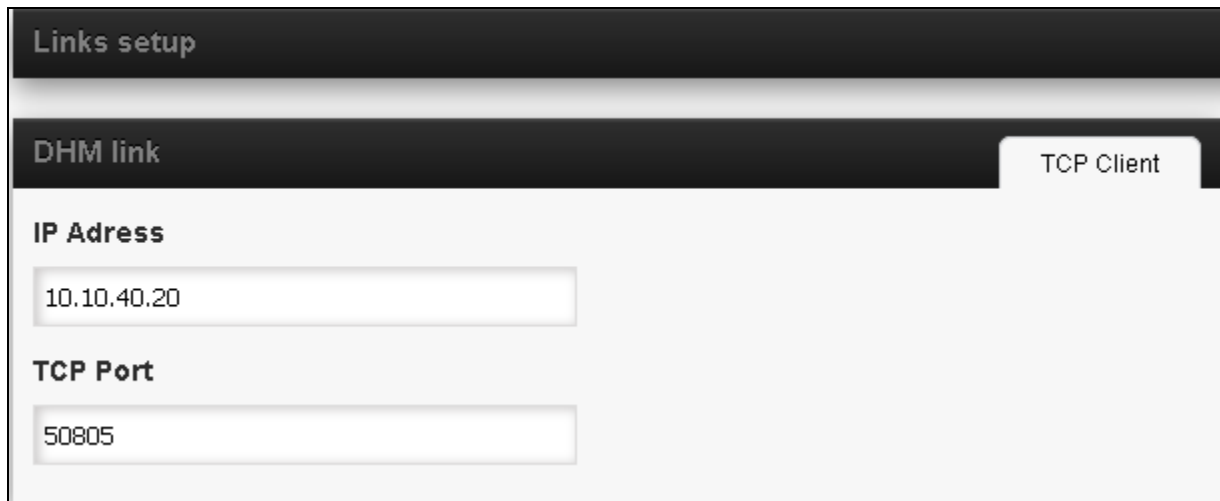
- **CONFERENCEID** Enter **8389**
- **SEPAREVM** Enter **1**
- **FORCEVMNA** Enter **1**
- **ESURGRP** Enter **1**
- **INVERTAUTCOD** Enter **1**
- **FORCECHARGETARGETER** Enter **1**

| GT-HOSP GT27 | | |
|----------------------|-----------------------------------|--|
| GESTION_CONTINUATION | <input type="text" value="0"/> | Group calls with continuation = 1 in one call (0 = No, 1 = Yes) |
| TEMPS_ATTENTE | <input type="text" value="0"/> | Waiting time before rebuilding tickets |
| DROP_INTERNE_ENTRANT | <input type="text" value="0"/> | Drop incoming internal calls |
| ACTIVER_TRANSFERT | <input type="text" value="0"/> | Enable management of information retrieval TR_A and TR_PAR (0 = No, 1 = Yes) |
| GERER_FAISCEAU | <input type="text" value="0"/> | Enable trunc management (0 = No, 1 = Yes) |
| CONFERENCEID | <input type="text" value="8389"/> | CONFERENCEID |
| CONFNBLENGHT | <input type="text" value="3"/> | CONFNBLENGHT |
| CONFCHLENGHT | <input type="text" value="4"/> | CONFCHLENGHT |
| SEPAREVM | <input type="text" value="1"/> | SEPAREVM (0 = No, 1 = Yes) |
| FORCEVMNA | <input type="text" value="1"/> | FORCEVMNA (0 = No, 1 = Yes) |
| ESURGRP | <input type="text" value="1"/> | ESURGRP (0 = No, 1 = Yes) |
| INVERTAUTCOD | <input type="text" value="1"/> | Invert AuthCode and AuthValid |
| FORCECHARGETARGETER | <input type="text" value="1"/> | Force Charge Targeter |
| TICKETIPO | <input type="text" value="0"/> | 0: tIpODefault 1: tIpOR4 2: tIpOR9x 3: tIpOR91x 4: tIpOR10 5: tIpOR9xCsv 6: tIpOR10Ccsv 7: tIpOR9xSpe |

6.4. Links Setup

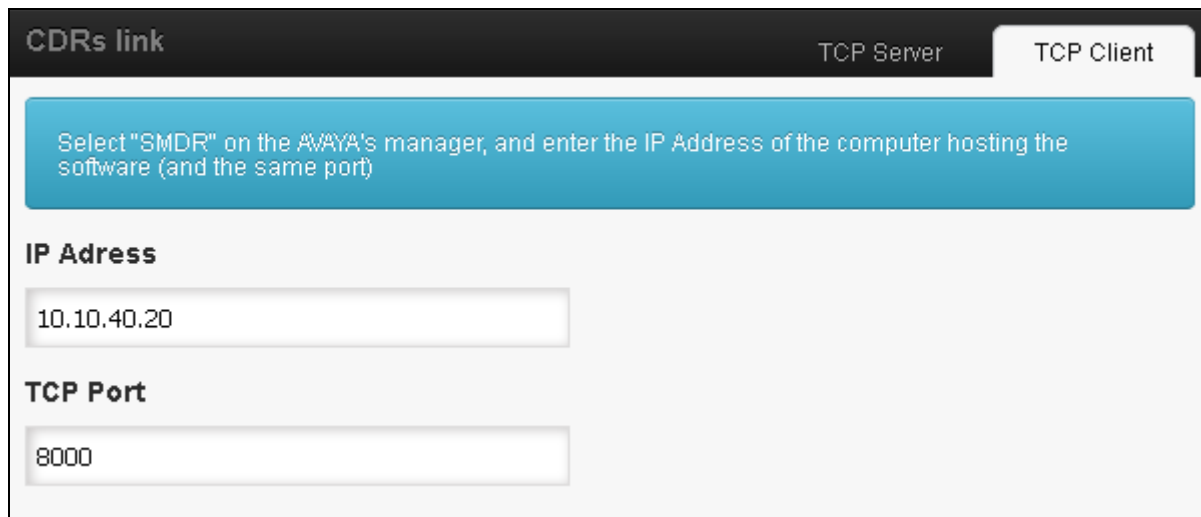
In the DHM Link window enter the following:

- **IP Address** Enter the IP address of the IP Office
- **TCP Port** Enter **50805**



The screenshot shows a web interface titled "Links setup". Below the title bar, there is a tabbed interface with two tabs: "DHM link" (selected) and "TCP Client". In the "DHM link" tab, there are two input fields. The first is labeled "IP Address" and contains the text "10.10.40.20". The second is labeled "TCP Port" and contains the text "50805".

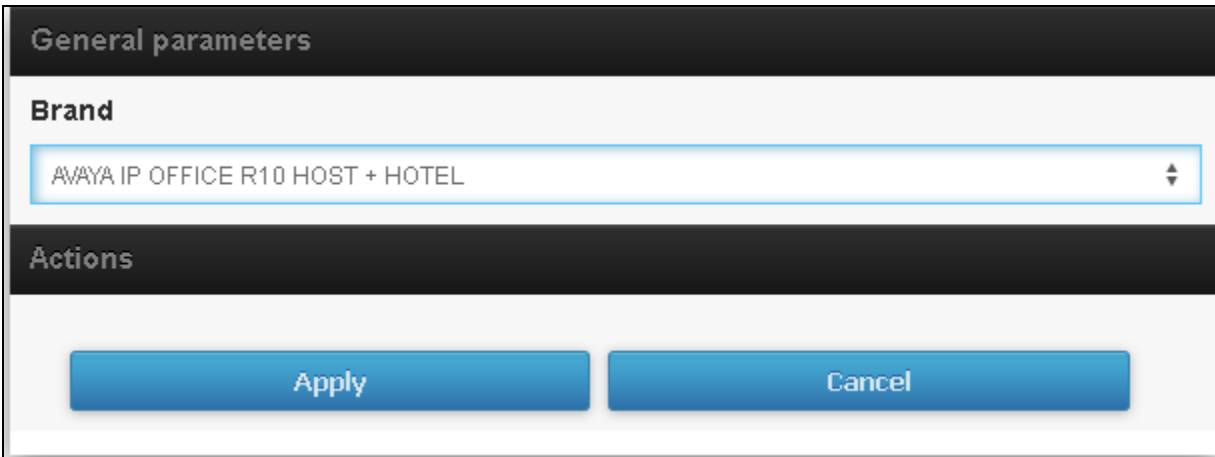
In the **CDRs link** window enter the IP Address of the IP Office and the **TCP Port** as configured in **Section 5.3** which is **8000**.



The screenshot shows a web interface titled "CDRs link". Below the title bar, there are two tabs: "TCP Server" and "TCP Client" (selected). In the "TCP Client" tab, there is a blue instruction box that reads: "Select 'SMDR' on the AVAYA's manager, and enter the IP Address of the computer hosting the software (and the same port)". Below this box, there are two input fields. The first is labeled "IP Address" and contains the text "10.10.40.20". The second is labeled "TCP Port" and contains the text "8000".

6.5. Apply GT Connector Configuration

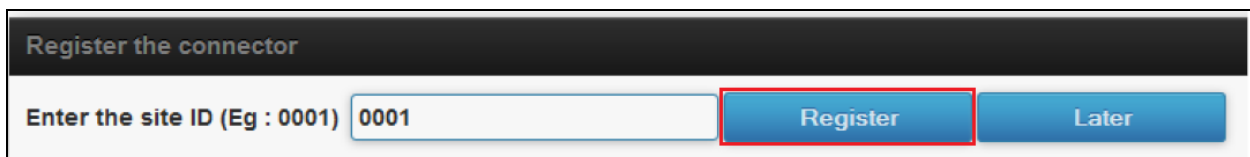
Return to the **General Parameters** window and click on the **Apply** button.



The screenshot shows a window titled "General parameters". Under the "Brand" label, a dropdown menu is open, displaying the text "AVAYA IP OFFICE R10 HOST + HOTEL". Below the dropdown, there is a section labeled "Actions" which contains two buttons: "Apply" and "Cancel".

6.6. Register the GT Connector

After applying the GT Connector configuration, the connection must be registered. When the **Register the connector** window opens, enter the ID of the site that will be linked to the connector (i.e. **0001** was used during compliance testing). Click on the **Register** button to launch the process. Wait for the process to end to be redirected to the main page of the GT-CONNECTOR module.



The screenshot shows a window titled "Register the connector". It contains a text input field with the placeholder text "Enter the site ID (Eg : 0001)" and the value "0001". To the right of the input field are two buttons: "Register" and "Later". The "Register" button is highlighted with a red rectangular border.

7. Verification

The following steps may be used to verify the configuration.

- Verify the connection status of GT-HOSP.
- Verify data collection.
- Verify that a room can be checked in.

7.1. Verify the connection status of GT-HOSP

Log on with the appropriate credentials to the GT-HOSP server, using the URL **http://x.x.x.x:43001**, where **x. x. x. x** is the IP address of the GT2F Server. Select **Modules status** and verify that the **CDRs** and **DHM** links are **Enabled** and **Connected**.

The screenshot shows the 'Module's states' page in the GT-HOSP interface. It displays two panels: 'CDRs link TCP/IP Client - 10.10.40.20:8000' and 'DHM link TCP/IP Client - 10.10.40.20:50805'. Both panels show a table with columns for 'Link', 'Connection', and 'Last error'. The 'Link' is 'Enabled' and the 'Connection' is 'Connected' for both.

| CDRs link TCP/IP Client - 10.10.40.20:8000 | |
|--|-----------|
| Link | Enabled |
| Connection | Connected |
| Last error | |
| | |

| DHM link TCP/IP Client - 10.10.40.20:50805 | |
|--|-----------|
| Link | Enabled |
| Connection | Connected |
| Last error | |
| | |

7.2. Verify data collection

Select **Maintenance** and verify that data is collected in the **CDR live capture** window.

The screenshot shows the 'Maintenance' page in the GT-HOSP interface. It displays two panels: 'CDR live capture' and 'DHM'. The 'CDR live capture' panel shows a log of data collection, including 'SEND - NO DATA', 'TAX_RCV' messages, and 'DEVLOG' messages. The 'DHM' panel shows a table of data collection, including '1. [object Object]', '2. 2017/05/16 09:09:16,00:00:24,2,5251,0,091737000,091737000,,0,1000235,0,E5251,MOM5251,T9017,Line', and '3. 2017/05/16 09:09:34,00:00:10,2,5250,0,5221,5221,,1,1000236,0,E5250,Room5250,E5221,Extn'.

CDR live capture

Logs

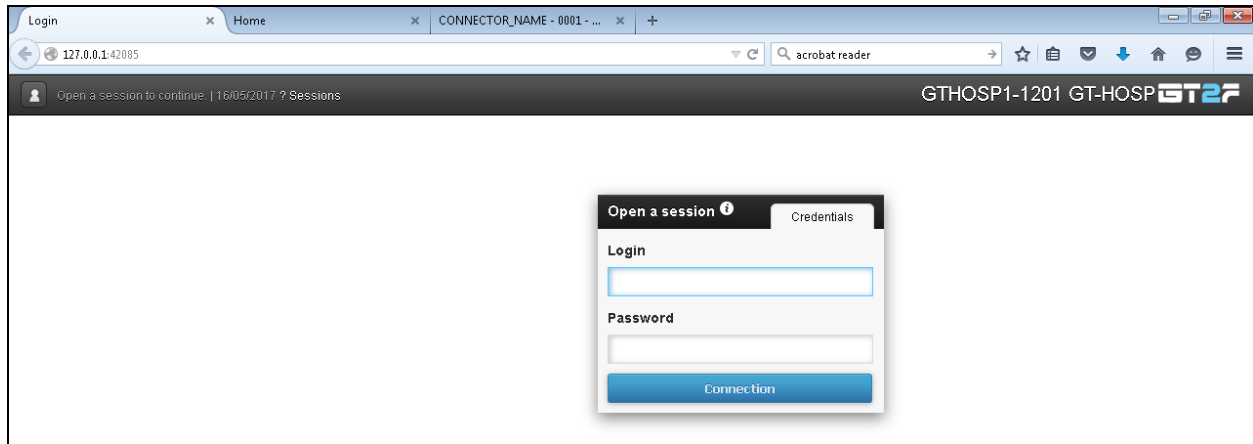
```
SEND - NO DATA
[TAX_RCV] 2017/05/16 09:09:16,00:00:24,2,5251,0,091737000,091737000,,0,1000235,0,E5251,MOM5251,T9017,Line
17.1,0,0,0,n/a,,,,,,,,,U,MOM5251,,10.10.40.20,1690,10.10.40.20,1692,2017/05/16 09:09:44[$OD] [$OA]
[TAX_RCV] 2017/05/16 09:09:34,00:00:10,2,5250,0,5221,5221,,1,1000236,0,E5250,Room5250,E5221,Extn
5221,0,0,0,n/a,,,,,,,,,10.10.40.20,1693,10.10.40.20,1695,2017/05/16 09:09:47[$OD] [$OA]
DEVLOG : IdentifierTicket format IPODefault
DEVLOG : IdentifierTicket format IPODefault
DS CENTRAL_CLIENT_CALCUL_FILE_OK 0001_20170516104956.0001.tmp
0001_20170516104956.0001.tmp
SEND - NO DATA
SEND - NO DATA
```

DHM

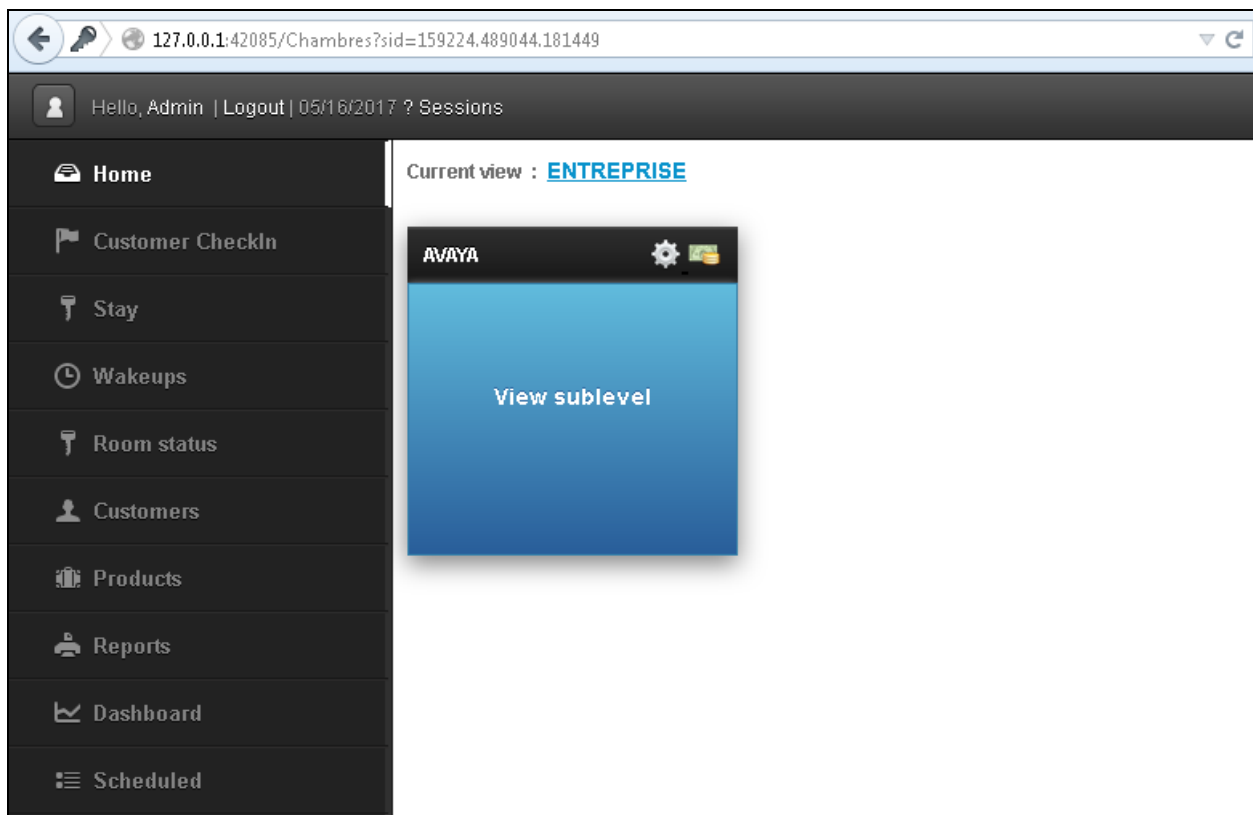
| Dialog | Raw CDR | Processed CDR | CDRs |
|--|---------|---------------|---|
| 1. [object Object] | | | 1. [object Object] |
| 2. 2017/05/16 09:09:16,00:00:24,2,5251,0,091737000,091737000,,0,1000235,0,E5251,MOM5251,T9017,Line | | | 2. "0";"1";"0";"0";"0";"0";"1";"0";"0";"5251 ";"-1 ";"091737000 " |
| 3. 2017/05/16 09:09:34,00:00:10,2,5250,0,5221,5221,,1,1000236,0,E5250,Room5250,E5221,Extn | | | 3. "0";"1";"0";"0";"0";"0";"1";"0";"0";"5250 ";"-1 ";"5221 ";" |

7.3. Verify Hospitality feature

Log on with the appropriate credentials to the GT-HOSP server, using the URL **http://x.x.x.x:42085**, where **x. x. x. x** is the IP address of the GT-HOSP server.



From the menu on the left, select **Home** as shown below. Click on **View sublevel** in the main window.



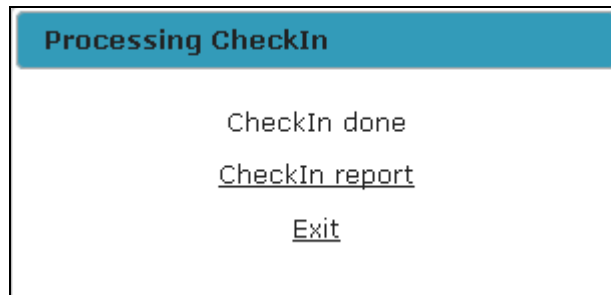
Each room that is ready to be checked in appears as **FREE** with a green base as shown below. Click on **Set Busy** to initiate the check in process.

The screenshot shows the GTHOSP1-1201 GT-HOSP interface. The top bar includes a user greeting 'Hello, Admin', a 'Logout' link, the date '05/16/2017', and session information. The main content area displays a grid of room status cards. The first card for 'Room 5201' shows a 'FREE' status with a green base and a 'Set Busy' button highlighted with a red box. Other cards show similar status for rooms 5221, 5250, and various Admin/Fax extensions. A sidebar on the left contains navigation links like 'Home', 'Customer Checkin', 'Stay', 'Wakeups', 'Room status', 'Customers', 'Products', 'Reports', 'Dashboard', and 'Scheduled'.

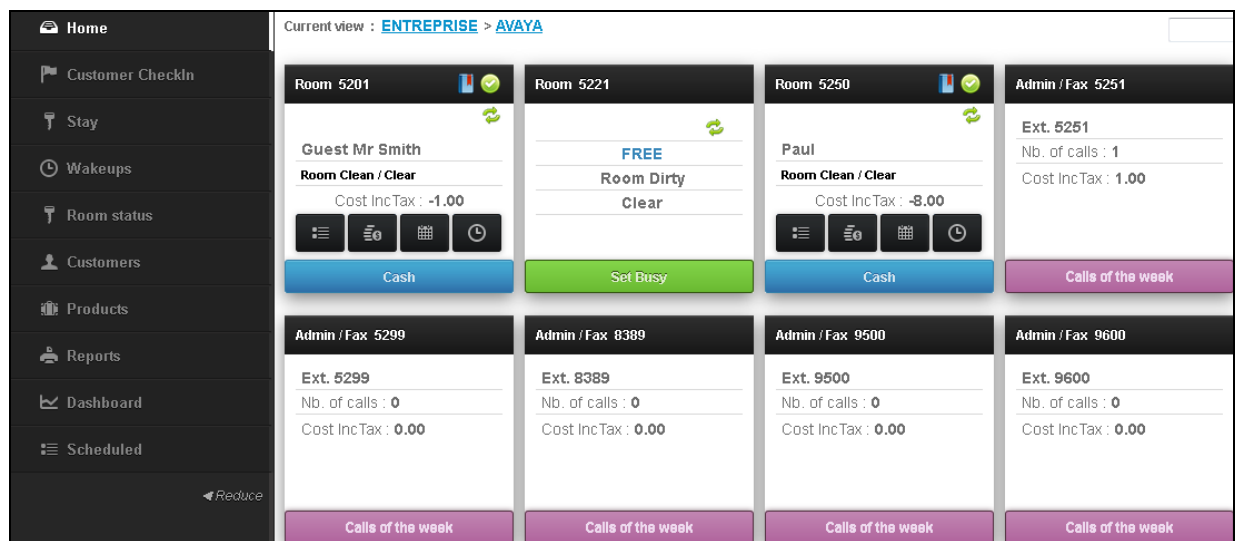
Enter a suitable **Name** and a **Prepayment** if required along with a DDI allocation, this will be a Hunt Group number on IP Office and click on **Set Busy** at the bottom of the screen to check the person into this room.

The screenshot shows the 'Room 5201' check-in form. The form has a dark header with the room number. Below it, the 'Arrival date: 16/05/2017' is displayed. There are two buttons: 'New customer' and 'Customers list'. The 'Name' field contains 'Guest Mr Smith'. The 'Firstname' field contains 'John'. The 'Email' field is empty. Below these is a 'Notes stay.' section with a text area. The 'Phone system' section includes a 'Prepayment' field with a value of '1.00' and a 'Phone number (DDI)' field with a value of '5296 (xxxx 5296) [5296]'. At the bottom, there is a checkbox for 'Send the welcome mail to the customer' and two buttons: 'Set Busy' and 'Cancel'.

Once checked in the following screen appears.



Clicking on **Exit** above will bring the user back to **Home** page where room **5201** is now checked in showing **Guest Mr Smith**.



Note: For further information on using the Checkin Assistant refer to the product documentation in **Section 9**.

8. Conclusion

A full and comprehensive set of feature and functional test cases were performed during compliance testing. GT-HOSP/HOTELIUM from GT2F is considered compliant with Avaya IP Office IP500 V2 R10.0. All test cases have passed with any issues and observations outlined in **Section 2.2**.

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] *Deploying Avaya IP Office™ Platform IP500 V2.*
- [2] *Administering Avaya IP Office™ Platform with Web Manager.*
- [3] *Administering Avaya IP Office™ Platform with Manager.*
- [4] *IP Office System Monitor*, Document Number 15-601019, Issue 03c, March 1, 2013.

Product documentation for GT2F can be obtained in the installed software or at: www.gt2f.com

©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.