



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

---

### **Application Notes for GT2F GT-HOSP with Avaya IP Office 500 v2 R9.0 - Issue 1.0**

#### **Abstract**

These Application Notes describe the configuration steps required for GT-HOSP to interoperate with Avaya IP Office 500 v2 R9.0.

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 outline the steps necessary to configure GT-HOSP from GT2F to interoperate with Avaya IP Office. GT-HOSP is a graphical hospitality user interface. It is commonly used in hotels to provide a way to control usage of room facilities. 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. The GT-HOSP software can also be supplied in a Business version.

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

- **Check-In**
- **DDI Allocation**
- **Update Name** - A facility that updates the display name of the station in Avaya IP Office.
- **Room Transfer**
- **Telephone Service Class**
- **Check-out**
- **Room Status** –
- **SMDR**: call billing (hospitality and business mode) and analysis (in business mode)

Not supported: Voicemail / Message waiting / Wakeup

## 2. General Test Approach and Test Results

The general test approach was to configure GT-HOSP to communicate with IP Office as implemented on a customer's premises. Feature functionality testing was performed manually. During compliance testing the GT- HOSP was installed on a Windows 2008 server operating system; it may also be installed on Windows XP, Windows Vista, Windows 7, Windows 2003 Server or Windows 8 operating systems.

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

## 2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of 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 testing included:

- Check-In
- DDI
- Update Name
- Room Transfer
- Telephone Service Class
- Check-out
- Room Status
- Link Failure/Recovery
- Prepay

The SMDR test cases included:

- Local internal call handling
- Handling of Incoming Network calls
- Handling of External Calls
- Call Forwarding on busy/No Answer/Unconditional
- Transfers – Blind and Supervised
- Conference Calls
- Account Codes
- Call Park
- Call Pickup
- Auto Call back

## 2.2. Test Results

Tests were performed to ensure full interoperability between GT-HOSP and IP Office. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully with the following observation:

It is possible to exceed the Prepay limit.

**Example:** Where Hotel guests are using the Prepay facility they may exceed the Prepay limit, if the limit was not reached on the previous call. GT-HOSP only calculates the cost of each call after it is completed, therefore, if the current call incurs a charge greater than the value remaining, the call will be allowed to continue. Future calls are barred.

## 2.3. Support

Technical support from GT2F can be obtained through the following:

Phone: +33 8 92 140 150 (French Customers)  
+33 4 66 62 94 65 (International Customers)

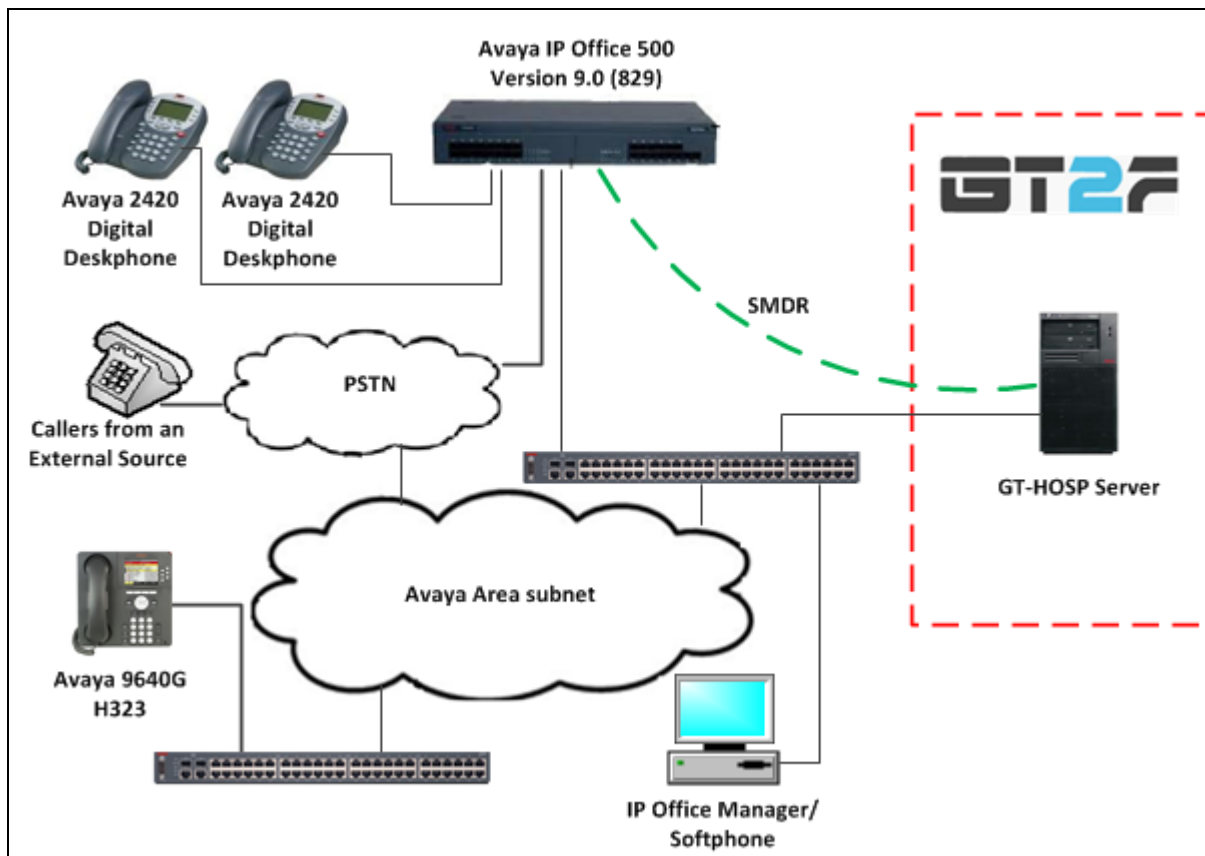
E-mail: [hotline@gt2f.com](mailto:hotline@gt2f.com)

## 3. Reference Configuration

**Figure 1** illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office 500v2 which has a TCP/IP link established to the GT-HOSP server.

- For the SMDR feature call records were sent to an agreed port number on GT-HOSP server from the IP Office.
- For the Hospitality, XML commands were passed via secure IP port on the IP Office for replication of the hospitality features.

Digital, H323 and Soft phones were configured on the IP Office to generate outbound/inbound calls to/from the PSTN. A QSIG trunk was configured to connect to the PSTN. Some telephones configured on the IP Office also acted as Hotel Room extensions when testing the GT-HOSP hospitality feature.



**Figure 1: Avaya and GT2F Reference Configuration**

## 4. Equipment and Software Validated

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

| Avaya Equipment  | Software / Firmware Version |
|--|-----------------------------|
| Avaya IP Office 500v2  | 9.0 Build 829               |
| Phone8 Analog Module   | 9.0.0.829                   |
| DIGSTA8 Digital Module                                       | 9.0.0.829                   |
| Avaya IP Office Manager                                      | 9.0 Build 829               |
| Avaya 9630 IP Telephone                                      | Release 3.2                 |
| Avaya 2420 Digital Telephones                                | --                          |
| Avaya IP Office softphone                                    | 3.2.3.49 68975              |
| Avaya Analogue Telephone                                     | --                          |
| GT2F Equipment   | Software / Firmware Version |
| GT-HOSP- CONNECTOR MODULE<br>(SMDR and hospitality command)  | 1.0.0.3                     |
| GT-HOSP- CENTRAL MODULE<br>(DB and software management)      | 1.0.0.3                     |
| GT-HOSP- REPORT MODULE<br>(HOSPITALITY – end user interface) | 1.0.0.3                     |
| FireFox  | 32.0.2                      |
| Firebird   | 2.5.2                       |
| MS C++ Runtime 2005  | 8.0                         |
| MS .Net  | 4.0                         |

**Note:** During compliance testing all GT2F Equipment was installed on a Dell PowerEdge R610 running a Windows Server 2008 R2 Enterprise SP1 operating system.

**Note:** Testing was performed with IP Office 500v2 R9.0, but it also applies to IP Office Server Edition R9.0. Note that IP Office Server Edition requires an Expansion IP Office 500 v2 R9.0 to support analog or digital endpoints or trunks. IP Office Server Edition does not support TAPI Wave or Group Voicemail.

## 5. Avaya IP Office Configuration

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

- Launch Avaya IP Office Manager (Security)
- Security Level
- Launch Avaya IP Office Manager (Administration)
- Configure System Locale
- Create Extensions
- Create Users
- Modify User Rights
- Create DDI Hunt Groups
- Create Short Codes
- SMDR Configuration
- Save Configuration

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

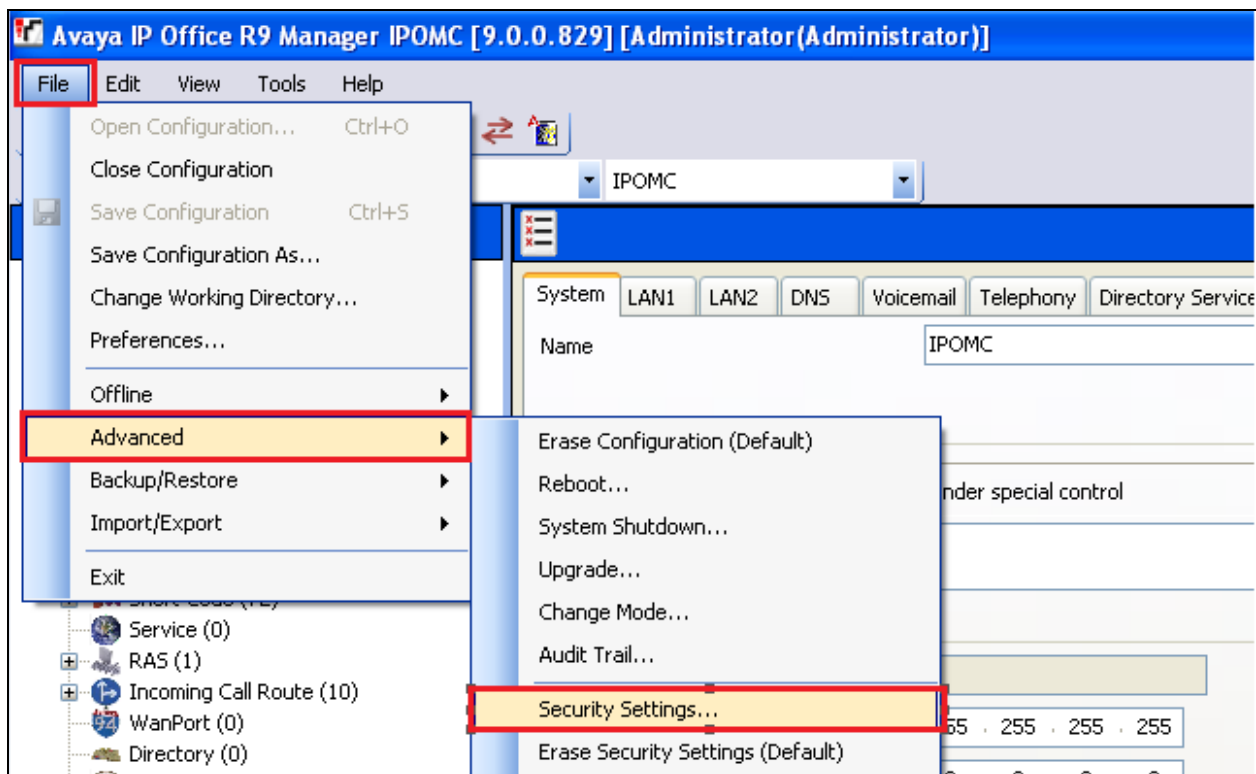
To Log in as a Security administrator first Log in as Administrator. From the IP Office Manager PC, go to **Start→Programs→IP Office→Manager** (not shown) to launch the Manager application. Select **File →Open Configuration**.



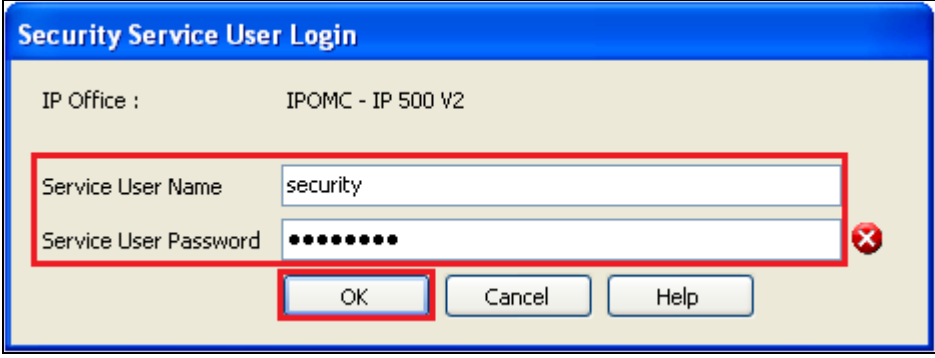
Select the appropriate IP Office and Log in using the **Service User Name** of **Administrator** and the appropriate **Service User Password** and click on the **OK** button. During compliance testing the System was called **IPOMC**.



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



In the **Security Service User Login** window Log in using the **Service User Name** of security and the appropriate **Service User Password** and click **OK**.




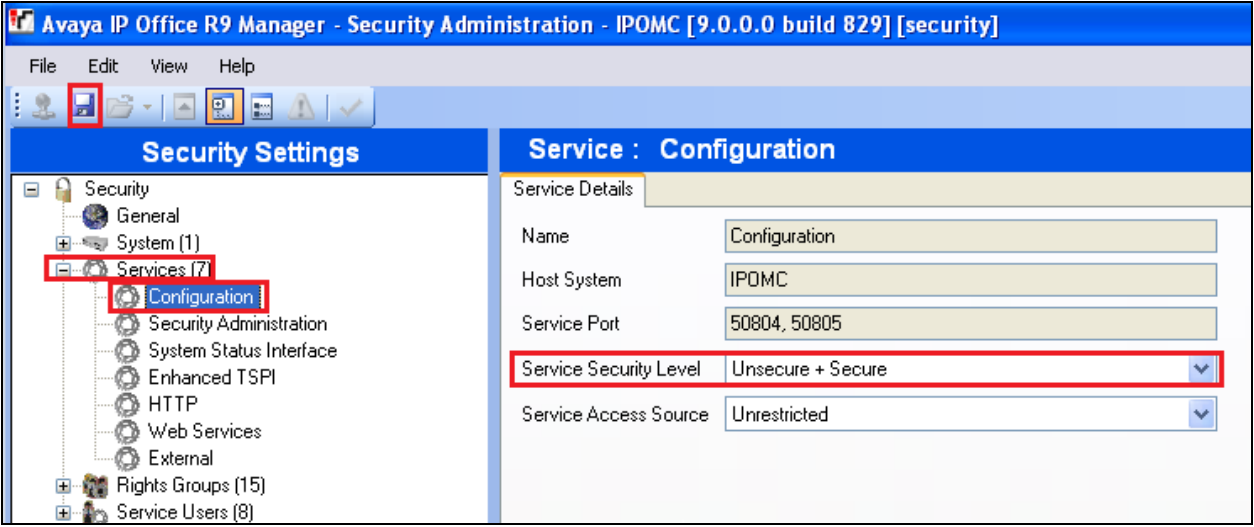
The dialog box is titled "Security Service User Login". It contains the following fields and buttons:

- IP Office :** IPOMC - IP 500 V2
- Service User Name:** security
- Service User Password:** (masked with dots)
- Buttons:** OK, Cancel, Help

A red rectangle highlights the Service User Name and Service User Password fields. A red 'X' icon is located to the right of the password field.

## 5.2. Security Level

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



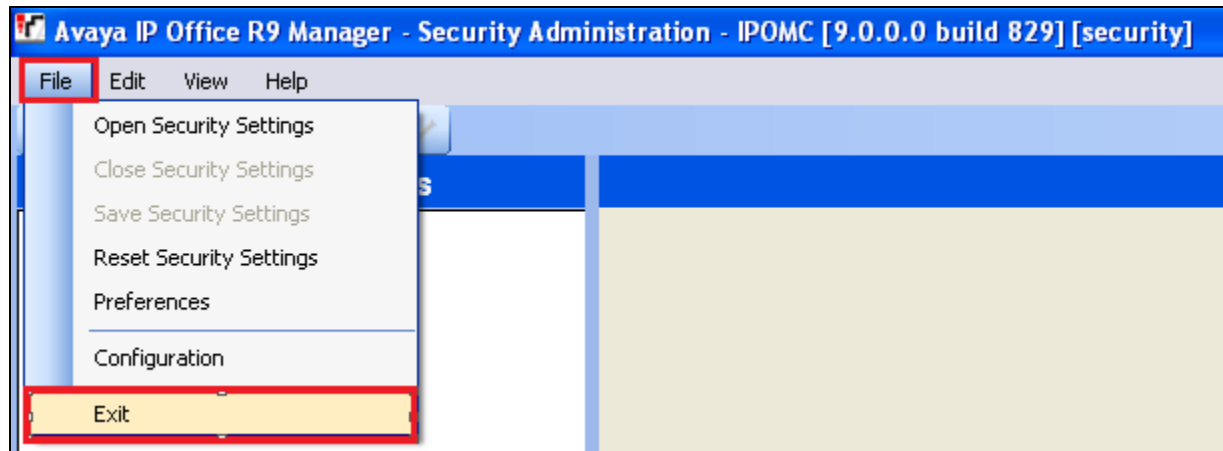
The screenshot shows the Avaya IP Office R9 Manager - Security Administration - IPOMC [9.0.0.0 build 829] [security] window. The window is divided into two main sections:

- Security Settings:** A tree view on the left showing the hierarchy: Security > General > System (1) > Services (7) > Configuration. The "Configuration" item is highlighted with a red box.
- Service : Configuration:** A form on the right with the following fields:
  - Name:** Configuration
  - Host System:** IPOMC
  - Service Port:** 50804, 50805
  - Service Security Level:** Unsecure + Secure (highlighted with a red box)
  - Service Access Source:** Unrestricted

A red box also highlights the "Save" icon in the top toolbar.



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



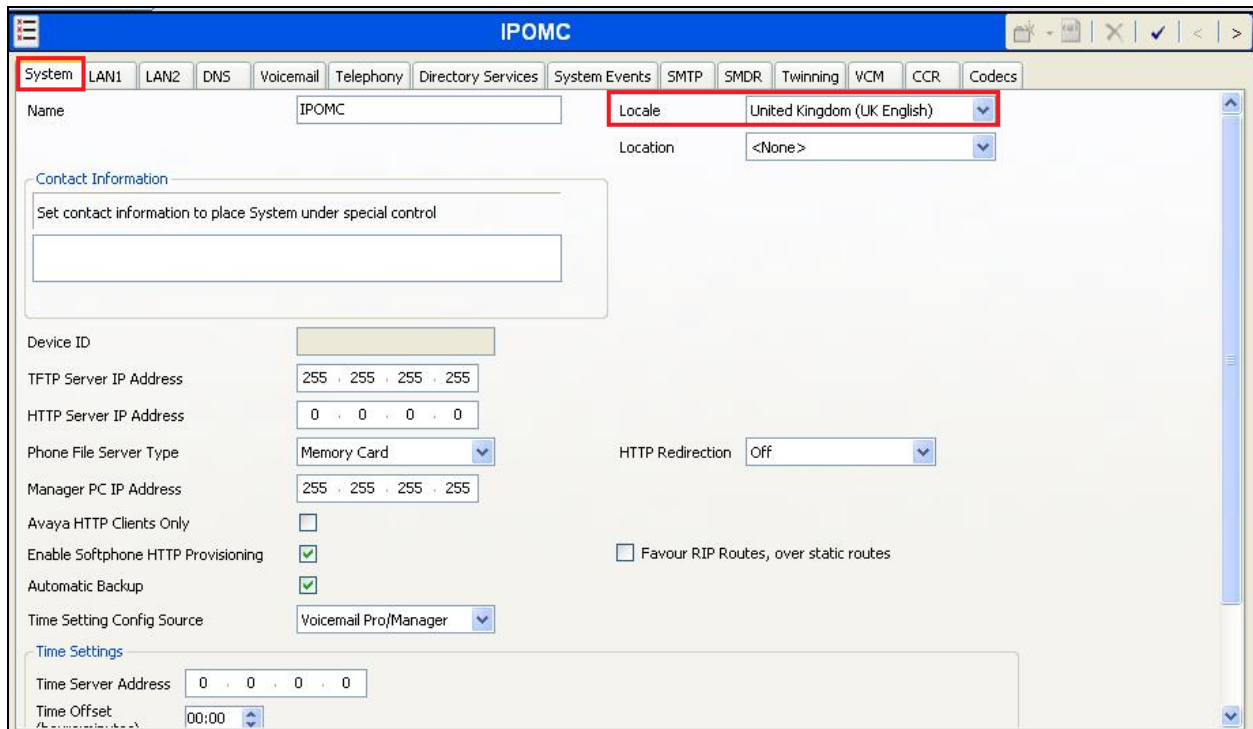
### 5.3. Launch Avaya IP Office Manager (Administration)

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



## 5.4. Configure System Locale

The Locale is usually the country where the IP Office is installed. By selecting the correct country, a number of system defaults for that country will be used by the IP Office. To configure the Locale, select **System** from the IP Office Configuration Tree (not shown). In the right hand pane select the **System** tab, and from the **Locale** dropdown box select the appropriate country (i.e. **United Kingdom (UK English)**). Click the **OK** button to save (not shown).

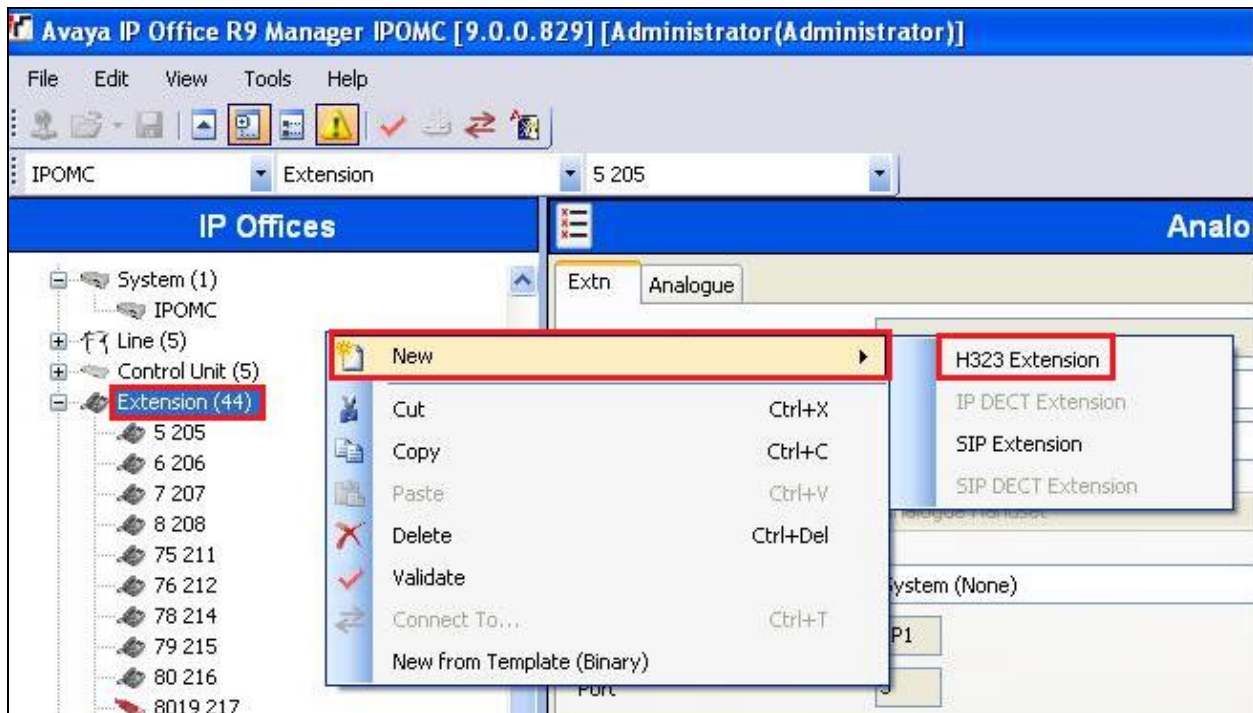


The screenshot displays the IPOMC configuration window. The 'System' tab is selected in the top navigation bar. The 'Name' field is set to 'IPOMC'. The 'Locale' dropdown menu is open, showing 'United Kingdom (UK English)' as the selected option. The 'Location' dropdown is set to '<None>'. Below these fields, there is a 'Contact Information' section with a text box for 'Set contact information to place System under special control'. The 'Device ID' field is empty. The 'TFTP Server IP Address' is '255 . 255 . 255 . 255'. The 'HTTP Server IP Address' is '0 . 0 . 0 . 0'. The 'Phone File Server Type' is 'Memory Card'. The 'Manager PC IP Address' is '255 . 255 . 255 . 255'. The 'Avaya HTTP Clients Only' checkbox is unchecked. The 'Enable Softphone HTTP Provisioning' checkbox is checked. The 'Automatic Backup' checkbox is checked. The 'Time Setting Config Source' is 'Voicemail Pro/Manager'. The 'HTTP Redirection' dropdown is set to 'Off'. The 'Favour RIP Routes, over static routes' checkbox is unchecked. The 'Time Settings' section shows the 'Time Server Address' as '0 . 0 . 0 . 0' and the 'Time Offset' as '00:00'.

## 5.5. Create Extensions

Extensions are required for each guest room and administrators. This section shows the procedure for creating H323 Extensions, for creating Analogue, Digital, etc. extensions refer to the product documentation in **Section 9**. From the configuration tree in the **IP Offices** pane, click on **Extension → New → H323 Extension**.

**Note:** Six virtual extensions are also required to create Users for configuring room status Short Codes in **Section 5.9.3**. See **Appendix A** for a list of Short codes and virtual extensions used during compliance testing. These virtual extensions were configured as H323.



In the extension pane, for **Base Extension** enter the number used for this extension (i.e. 3002). The **Extension Id** field is filled in automatically. Defaults were used for the remaining fields and tabs. Click on the **OK** button to save.

The screenshot shows a configuration window titled "H323 Extension: 8020 3002". It has two tabs: "Exttn" (selected) and "VoIP". The "Exttn" tab contains the following fields:

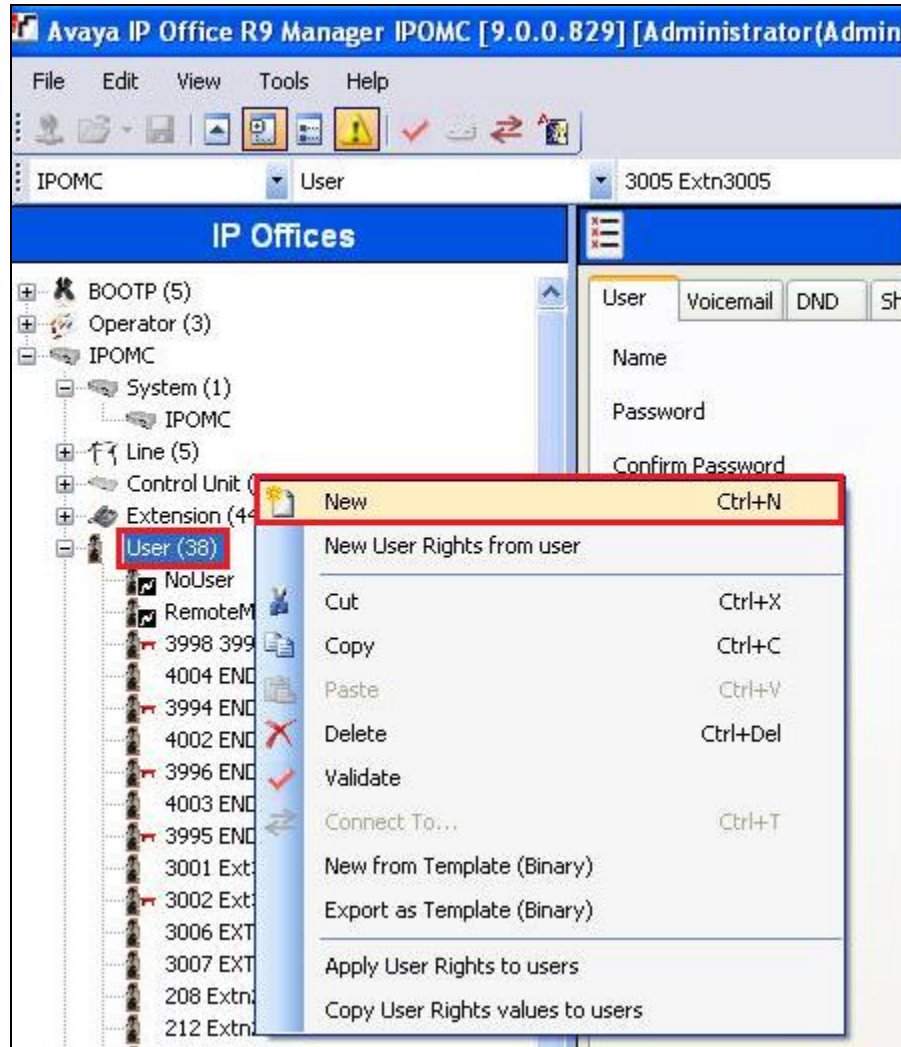
| Field                    | Value                    |
|--------------------------|--------------------------|
| Extension Id             | 8020                     |
| Base Extension           | 3002                     |
| Phone Password           |                          |
| Caller Display Type      | On                       |
| Reset Volume After Calls | <input type="checkbox"/> |
| Device Type              | Unknown IP handset       |
| Location                 | Automatic                |
| Module                   | 0                        |
| Port                     | 0                        |
| Disable Speakerphone     | <input type="checkbox"/> |

Repeat this section for each extension required.

## 5.6. Create Users

Each extension created in **Section 5.5** requires a user. From the configuration tree in the IP Offices pane, right click on **User**, and select **New**.

**Note:** Six users were created using the virtual extensions created in **Section 5.5** that will be used when creating Room Status Short Codes in **Section 5.9.3**. See **Appendix A** for a list of Short codes and Virtual Extensions used during compliance testing.



In the User pane, click on the **User** tab and enter the following:

- **Name** Enter a name for the user (i.e. Ext3002 H323)
- **Password** Enter an appropriate password (Only applicable if user applications and/or Dial In access is required)
- **Confirm** Confirm the password
- **Extension** Enter the **Extension** number as configured in **Section 5.5**

Defaults were used for the remaining fields. Click on the **OK** button (not shown) to save.

The screenshot shows a web-based configuration interface for a user named 'Ext3002 H323: 3002'. The interface includes a top navigation bar with a hamburger menu icon and a title bar. Below the title bar is a tabbed interface with tabs for 'User', 'Voicemail', 'DND', 'ShortCodes', 'Source Numbers', 'Telephony', 'Forwarding', 'Dial In', and 'Voice Recording'. The 'User' tab is selected. The form contains several fields: 'Name' (text input with 'Ext3002 H323'), 'Password' (password input with '\*\*\*\*'), 'Confirm Password' (password input with '\*\*\*\*'), 'Account Status' (dropdown menu with 'Enabled'), 'Full Name' (text input), 'Extension' (text input with '3002'), 'Email Address' (text input), 'Locale' (dropdown menu), 'Priority' (dropdown menu with '5'), 'System Phone Rights' (dropdown menu with 'None'), and 'Profile' (dropdown menu with 'Basic User'). Red rectangular boxes highlight the 'Name', 'Password', 'Confirm Password', and 'Extension' fields. The 'Locale' and 'Priority' dropdowns have a lock icon next to them.

For configuration information for the remaining fields and tabs refer to the product documentation in **Section 9**. Repeat this section for each user required.

## 5.7. Modify User Rights

A number of user rights need to be configured on the IP Office. In the Manager window expand the Configuration Tree. Right click on **User Rights**, and select **New**.



### 5.7.1. Modify User Rights (Check in)

When the New User Rights window appears click on the **User** tab. In the **Name** field enter **Checkin**.

A screenshot of the 'checkin' New User Rights window. The window has a blue header bar with the title 'checkin'. Below the header is a tabbed interface with tabs for 'User', 'ShortCodes', 'Button Programming', 'Telephony', 'User Rights Membership', and 'Voicemail'. The 'User' tab is selected and highlighted with a red box. The 'Name' field is populated with 'checkin' and is also highlighted with a red box. Below the name field are sections for 'Locale', 'Priority', and 'Do not disturb', each with a dropdown menu and a 'Not part of User Rights' option.



Click on the **Telephony** tab followed by the **Supervisor Settings** tab. In the **Outgoing call bar** section uncheck the **Enable outgoing call bar** check box and select **Apply User rights value** from the dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot displays the 'checkin\*' web application interface. At the top, there is a blue header bar with the 'checkin\*' logo. Below the header, a series of tabs are visible: 'User', 'ShortCodes', 'Button Programming', 'Telephony' (highlighted with a red box), 'User Rights Membership', and 'Voicemail'. Under the 'Telephony' tab, there are sub-tabs: 'Call Settings', 'Supervisor Settings' (highlighted with a red box), 'Multi-line Options', and 'Call Log'. The 'Supervisor Settings' sub-tab is active, showing various configuration options. These options are grouped into sections: 'Intrusion', 'Force login', 'Force account code', 'Inhibit Off-Switch Forward/Transfer', 'CCR Agent', 'After Call Work Time (seconds)', 'Outgoing call bar' (highlighted with a red box), and 'Coverage Group'. In the 'Outgoing call bar' section, the 'Enable outgoing call bar' checkbox is unchecked, and the dropdown menu next to it is set to 'Apply User Rights value'. Other sections like 'Intrusion' and 'Force login' have checkboxes for 'Can intrude', 'Cannot be intruded', 'Deny Auto Intercom Calls', 'Enable force login', and 'Enable force account code'. The 'After Call Work Time (seconds)' section has a dropdown for 'System Default (10)' and a checkbox for 'Enable Automatic After Call Work'. The 'Coverage Group' section has a dropdown for '<None>'. All dropdown menus show 'Not part of User Rights' as an option.



### 5.7.2. Modify User Rights (Check out)

When the New User Rights window appears click on the **User** tab. In the **Name** field enter **Checkout**.

The screenshot shows a web interface for configuring user rights. The title bar is blue and says "checkout". Below it is a tabbed interface with tabs: "User", "ShortCodes", "Button Programming", "Telephony", "User Rights Membership", and "Voicemail". The "User" tab is selected and highlighted with a red box. Below the tabs is a form with several fields. The "Name" field is highlighted with a red box and contains the text "checkout". Below "Name" are three sections: "Locale", "Priority", and "Do not disturb". Each section has a dropdown menu and a checkbox labeled "Not part of User Rights". The "Locale" dropdown is empty. The "Priority" dropdown is set to "5". The "Do not disturb" checkbox is unchecked.

| Field          | Value  | Not part of User Rights  |
|----------------|--|--------------------------|
| Name           | checkout                                       | <input type="checkbox"/> |
| Locale         |  | <input type="checkbox"/> |
| Priority       | 5  | <input type="checkbox"/> |
| Do not disturb | <input type="checkbox"/> Enable do not disturb | <input type="checkbox"/> |

Click on the **Telephony** tab followed by the **Supervisor Settings** tab. In the **Outgoing call bar** section check the **Enable outgoing call bar** check box and select **Apply User rights value** from the dropdown box. Defaults were used for the remaining fields and tabs. Click on the **OK** button (not shown) to save.

The screenshot displays the 'checkout' application window. The top navigation bar includes tabs for 'User', 'ShortCodes', 'Button Programming', 'Telephony' (selected), 'User Rights Membership', and 'Voicemail'. Below this, the 'Supervisor Settings' sub-tab is active. The interface is organized into several sections: 'Intrusion', 'Force login', 'Force account code', 'Inhibit Off-Switch Forward/Transfer', 'CCR Agent', 'After Call Work Time (seconds)', 'Outgoing call bar', and 'Coverage Group'. The 'Outgoing call bar' section is highlighted with a red border and contains a checked checkbox for 'Enable outgoing call bar' and a dropdown menu set to 'Apply User Rights value'. Other sections contain various checkboxes and dropdown menus, many of which are set to 'Not part of User Rights'.

| Section                             | Field                                      | Value                               |
|-------------------------------------|--|-------------------------------------|
| Intrusion                           | Can intrude                                | <input type="checkbox"/>            |
|                                     | Cannot be intruded                         | <input checked="" type="checkbox"/> |
|                                     | Deny Auto Intercom Calls                   | <input type="checkbox"/>            |
| Force login                         | Enable force login                         | <input type="checkbox"/>            |
|                                     | Enable force account code                  | <input type="checkbox"/>            |
| Inhibit Off-Switch Forward/Transfer | Enable Inhibit Off-Switch Forward/Transfer | <input type="checkbox"/>            |
|                                     | Enable CCR Agent                           | <input type="checkbox"/>            |
| After Call Work Time (seconds)      | System Default (10)                        | System Default (10)                 |
|                                     | Enable Automatic After Call Work           | <input type="checkbox"/>            |
| Outgoing call bar                   | Enable outgoing call bar                   | <input checked="" type="checkbox"/> |
|                                     | Coverage Group                             | <None>                              |

### 5.7.3. Modify User Rights (Do not Disturb)

When the New User Rights window appears click on the **User** tab. In the **Name** field enter **dnd** and check on the **Enable do not disturb** check box.

The screenshot shows a web application window titled "dnd\*". It has a tabbed interface with the following tabs: "User", "ShortCodes", "Button Programming", "Telephony", "User Rights Membership", and "Voicemail". The "User" tab is selected and highlighted with a red box. Below the tabs, there is a "Name" field containing the text "dnd", which is also highlighted with a red box. Below the "Name" field, there are three sections, each with a dropdown menu:

- Locale**: The dropdown menu is set to "Not part of User Rights".
- Priority**: The dropdown menu is set to "Not part of User Rights".
- Do not disturb**: The dropdown menu is set to "Not part of User Rights". Below this dropdown, there is a checkbox labeled "Enable do not disturb" which is checked.

Click on the **Telephony** tab followed by the **Supervisor Settings** tab. In the **Outgoing call bar** section uncheck the **Enable outgoing call bar** check box and select **Apply User rights value** from the 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 interface for configuring a system. At the top, there's a blue header with the text "dnd". Below it, a series of tabs are visible: "User", "ShortCodes", "Button Programming", "Telephony" (highlighted with a red box), "User Rights Membership", and "Voicemail". Under the "Telephony" tab, there are sub-tabs: "Call Settings", "Supervisor Settings" (highlighted with a red box), "Multi-line Options", and "Call Log". The "Supervisor Settings" sub-tab contains several sections with checkboxes and dropdown menus. The "Outgoing call bar" section is highlighted with a red box and contains the following items:

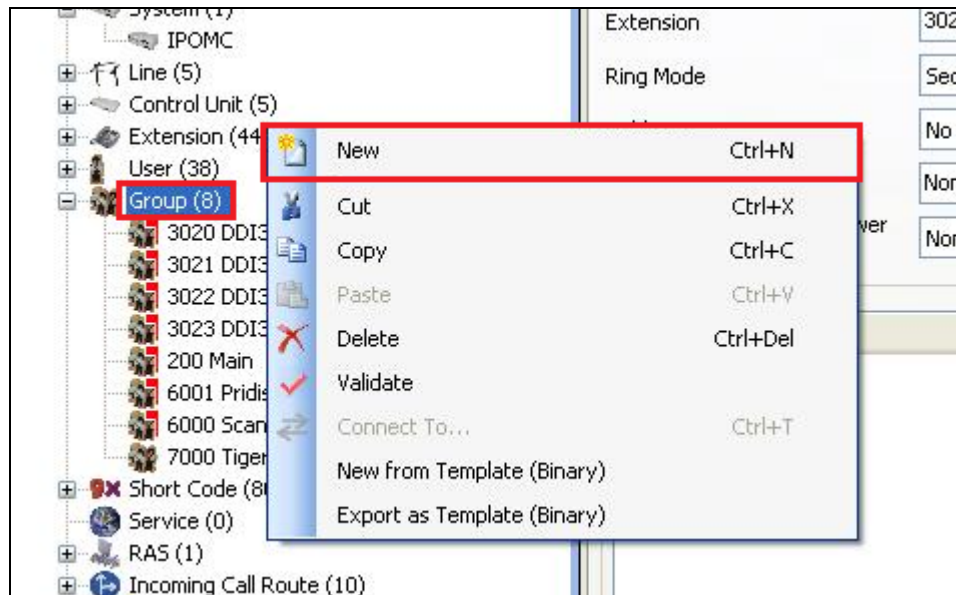
- ☐ Enable outgoing call bar
- Not part of User Rights (dropdown menu)

Other sections visible include:

- Intrusion**
  - ☐ Can intrude
  - ☒ Cannot be intruded
  - ☐ Deny Auto Intercom Calls
- Force login**
  - ☐ Enable force login
- Force account code**
  - ☐ Enable force account code
- Inhibit Off-Switch Forward/Transfer**
  - ☐ Enable Inhibit Off-Switch Forward/Transfer
- CCR Agent**
  - ☐ Enable CCR Agent
- After Call Work Time (seconds)**
  - System Default: (10)
  - ☐ Enable Automatic After Call Work
- Coverage Group**
  - <None>

## 5.8. Create DDI Hunt Groups

In the Manager window, go to the Configuration Tree, right-click **Group** and select **New** in the popup that appears.



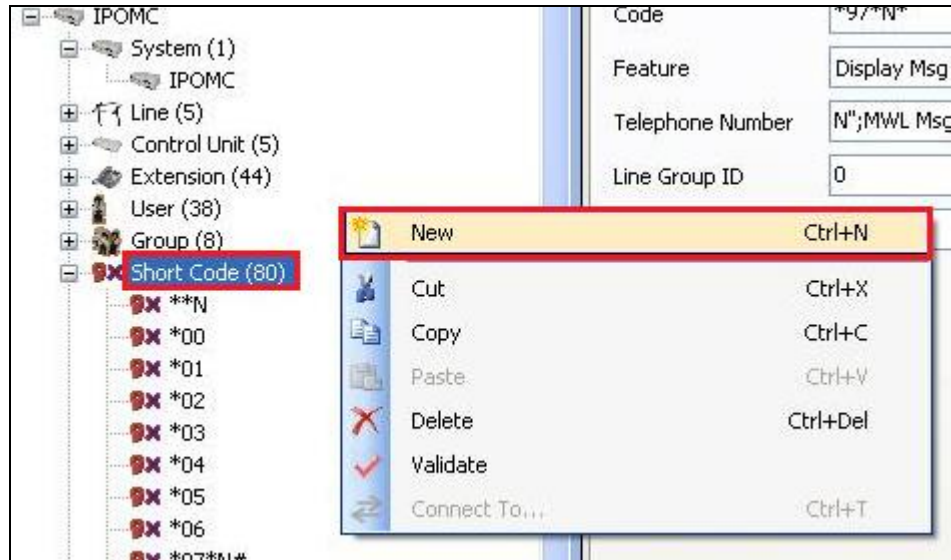
In the subsequent Hunt Group window, set **Name** to something appropriate (e.g. **DDI3020**). Enter an **Extension** (e.g. **3020**) and set the **Ring Mode** to **Sequential**. Ensure that no extensions are added to the **User List** as they will be automatically added by GT-HOSP once a DDI is allocated to an extension. Click the **OK** button (not shown) to save.

**Note:** Repeat this for each DDI required.

| Sequential Group DDI3020: 3020         |                     |
|--|---------------------|
| Name                                   | DDI3020             |
| Extension                              | 3020                |
| Ring Mode                              | Sequential          |
| Hold Music Source                      | No Change           |
| Ring Tone Override                     | None                |
| Agent's Status on No-Answer Applies To | None                |
| Profile                                | Standard Hunt Group |
| <input type="checkbox"/> Ex Directory  |                     |
| No Answer Time (secs)                  | System Default (15) |
| <b>User List</b>                       |                     |
| Extension                              | Name                |

## 5.9. Create Short Codes

A number of Short Codes needs to be configured on the IP Office. In the Manager window expand the Configuration Tree. Right click on **Short Codes**, and select **New**.



### 5.9.1. Create Short Code (Turn on Message Waiting Indication)

In the subsequent Short Code window, enter the following:

- **Code** Enter **\*97\*N\***
- **Feature** Select **Display Msg** from the drop-down menu
- **Telephone number** Enter **N";MWL Msgs=1 Old=0 Sav=0"**

Defaults were used for the remaining fields. Click the **OK** button.

A screenshot of the 'Short Code' configuration window in IP Office Manager. The window title is '\*97\*N\*: Display Msg\*'. The 'Short Code' tab is selected. The following fields are visible: 'Code' with value '\*97\*N\*', 'Feature' with a dropdown menu showing 'Display Msg', 'Telephone Number' with value 'N";MWL Msgs=1 OLD=0 Sav=0"', 'Line Group ID' with value '0', 'Locale' with a dropdown menu, and 'Force Account Code' with an unchecked checkbox. A red rectangle highlights the 'Code', 'Feature', and 'Telephone Number' fields.

### 5.9.2. Create Short Code (Turn off Message Waiting Indication)

In the subsequent Short Code window, enter the following:

- **Code** Enter **\*98\*N\***
- **Feature** Select **Display Msg** from the drop-down menu
- **Telephone number** Enter **N";MWL Msgs=0 Old=0 Sav=0"**

Defaults were used for the remaining fields. Click the **OK** button (not shown) to save.

| *98*N*: Display Msg |                            |
|---------------------|----------------------------|
| Short Code          |                            |
| Code                | *98*N*                     |
| Feature             | Display Msg                |
| Telephone Number    | N";MWL Msgs=0 OLD=0 Sav=0" |
| Line Group ID       | 0                          |
| Locale              |                            |
| Force Account Code  | <input type="checkbox"/>   |

### 5.9.3. Create Short code (Room Status)

A short code is required for the following Room Status:

- Vacant Dirty
- Vacant Clean
- Vacant Inspected
- Occupied Dirty
- Occupied Clean
- Occupied Inspected

The screen shot below shows the procedure to create the short code for **Vacant Dirty**.

In the subsequent Short Code window, enter the following:

- **Code** Enter **\*71**
- **Feature** Select **Dial Direct** from the drop-down menu
- **Telephone number** Enter **3040,,5\*E\***. 3040 is a Virtual Extension configured in **Section 5.5**.

Repeat these step for the remaining Room status, see **Appendix A** for a list of Short codes and Virtual Extensions used during compliance testing. Defaults were used for the remaining fields. Click the **OK** button (not shown) to save.

| *71: Dial Direct   |                          |
|--------------------|--------------------------|
| Short Code         |                          |
| Code               | *71                      |
| Feature            | Dial Direct              |
| Telephone Number   | 3040,,5*E*               |
| Line Group ID      | 0                        |
| Locale             |                          |
| Force Account Code | <input type="checkbox"/> |

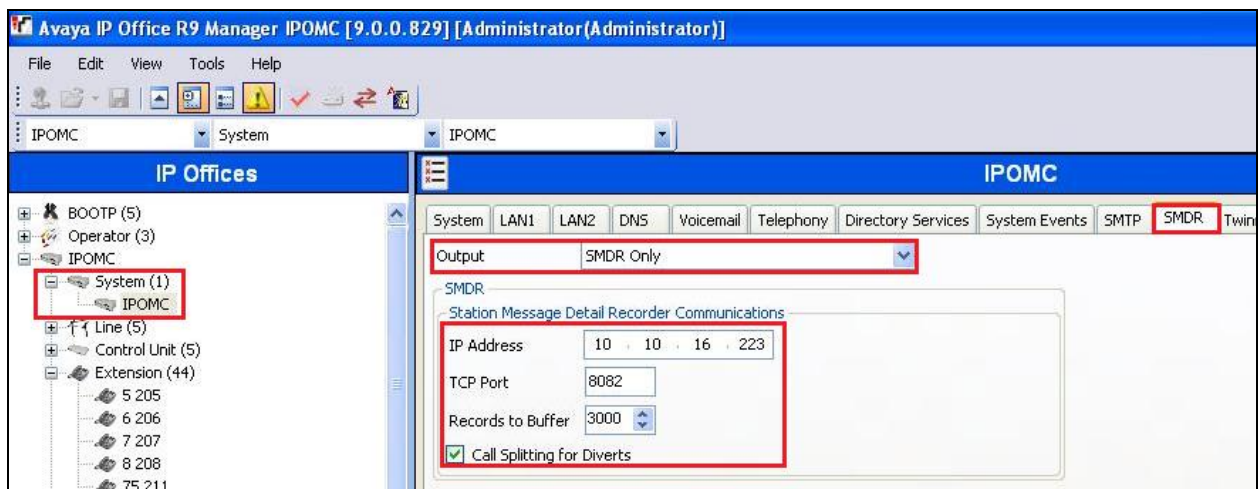


## 5.10. SMDR configuration

Select **System** from the IP Office Configuration Tree followed by the **SMDR** tab and enter the following information:

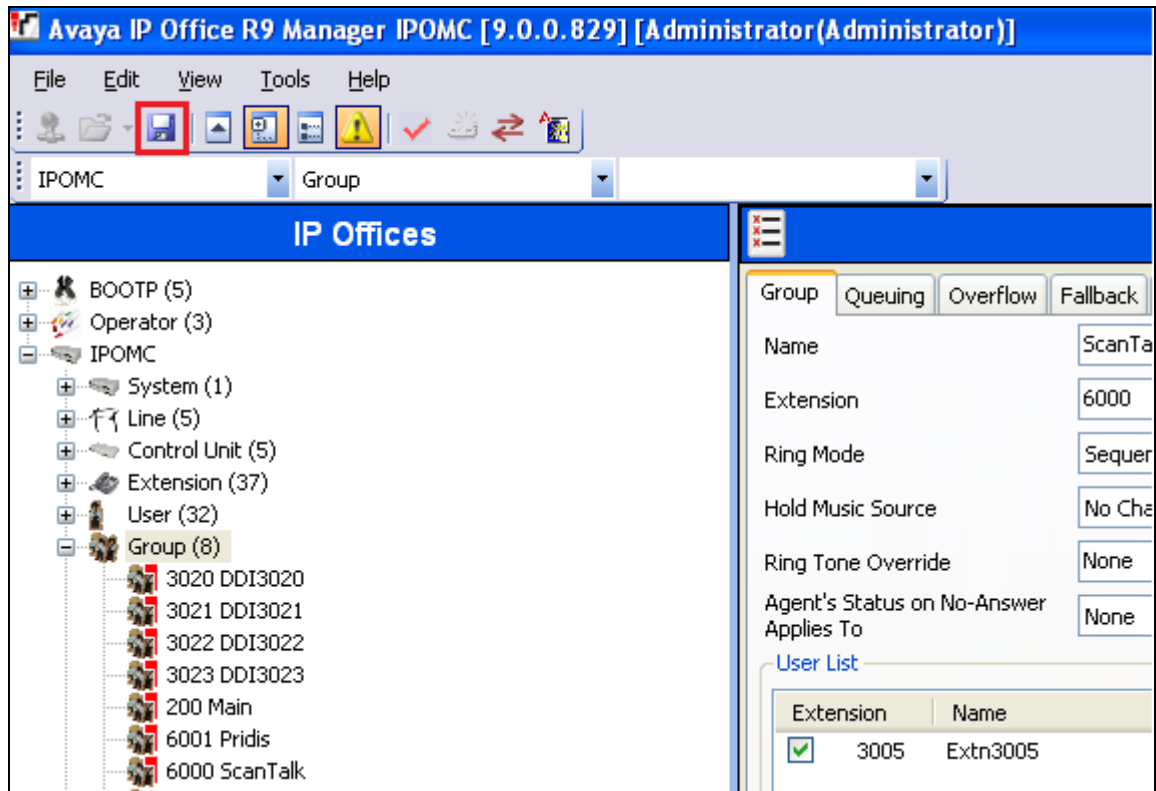
- **Output** Select **SMDR Only** from the drop box
- **IP Address** Enter the IP Address of the GT-HOSP Server
- **TCP Port** Enter **8082**
- **Records to buffer** Enter **3000**. This is maximum available
- **Call Splitting for Diverts** Click the check box.

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

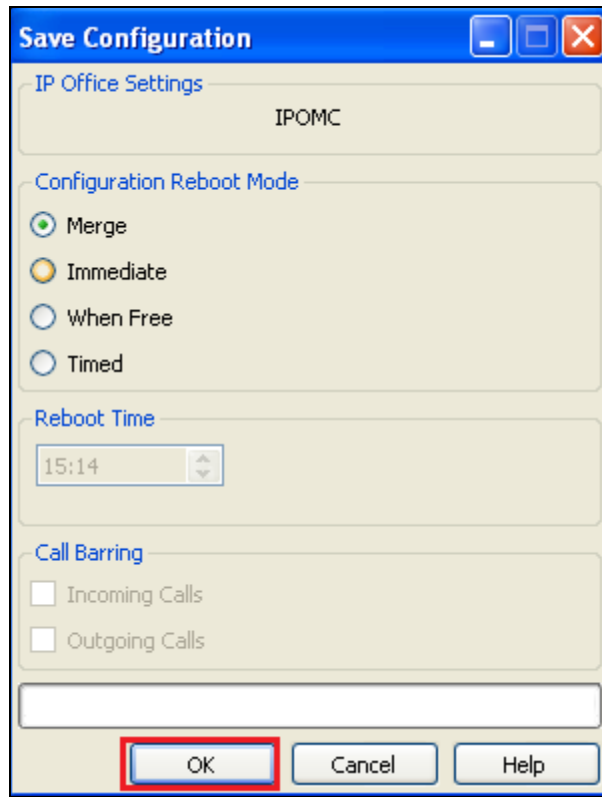


## 5.11. Save Configuration

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

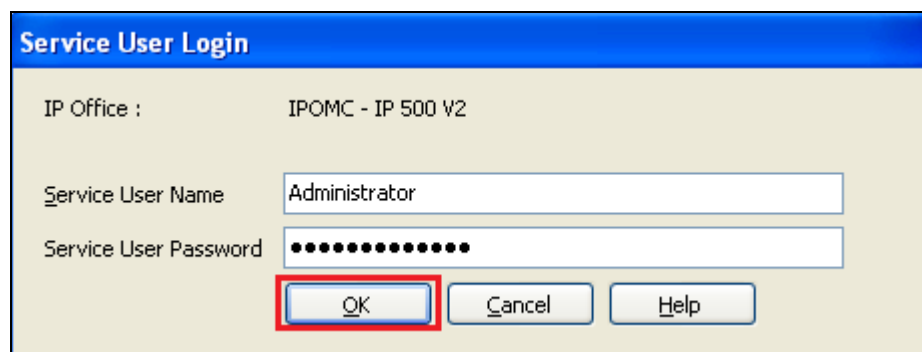


Once the **Save Configuration** Window opens, click the **OK** button.



The **Save Configuration** dialog box has a blue title bar with standard window controls. It contains several sections: **IP Office Settings** with a label 'IPOMC'; **Configuration Reboot Mode** with four radio buttons: 'Merge' (selected), 'Immediate', 'When Free', and 'Timed'; **Reboot Time** with a time selection box showing '15:14'; and **Call Barring** with two unchecked checkboxes: 'Incoming Calls' and 'Outgoing Calls'. At the bottom is an empty text field and three buttons: 'OK' (highlighted with a red rectangle), 'Cancel', and 'Help'.

When the **Service User Login** Window opens enter the appropriate credentials and click the **OK** button.



The **Service User Login** dialog box has a blue title bar. It displays 'IP Office : IPOMC - IP 500 V2'. Below this are two input fields: 'Service User Name' containing 'Administrator' and 'Service User Password' containing masked characters (dots). At the bottom are three buttons: 'OK' (highlighted with a red rectangle), 'Cancel', and 'Help'.

## 6. Configure GT2F GT-HOSP

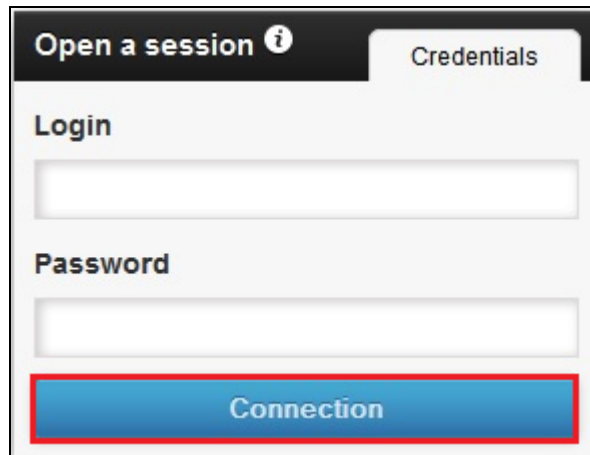
This section describes the steps preformed to configure GT-HOSP to connect to the IP Office. It is implied that the GT-HOSP Server software is already installed and has the appropriate licences. It is also implied that a Site is configured, an Operator is imported, and Tariffs are set. For all other 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 GT2F Server
- GT Connector Configuration
- Advanced Settings
- Links Setup
- Register the GT Connector

### 6.1. Logging in to GT2F Server

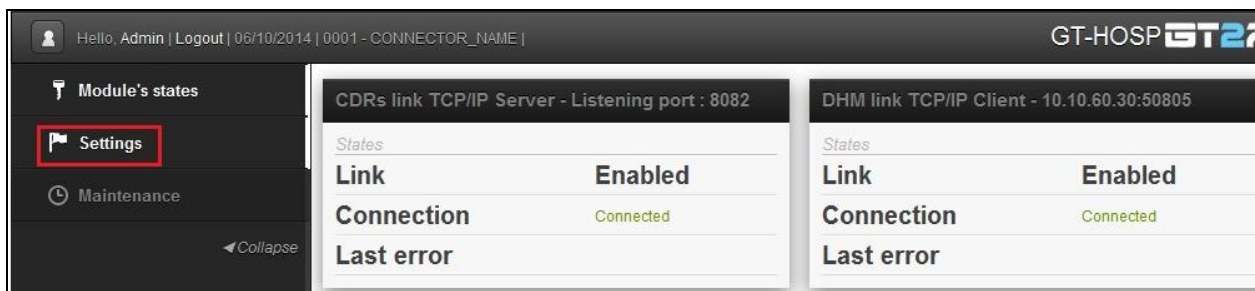
To access the OAM web-based interface of the GT2F Server use the URL **<http://x.x.x.x:43001>**, where **x. x. x. x** is the selected IP address of the GT2F Server. When the **Open a session** window opens is log in using the appropriate credentials and click on the **Connection** button.

**Note:** If logging for the same server that GT2F is installed use the URL 172.0.0.1:43001.



### 6.2. GT Connector Configuration

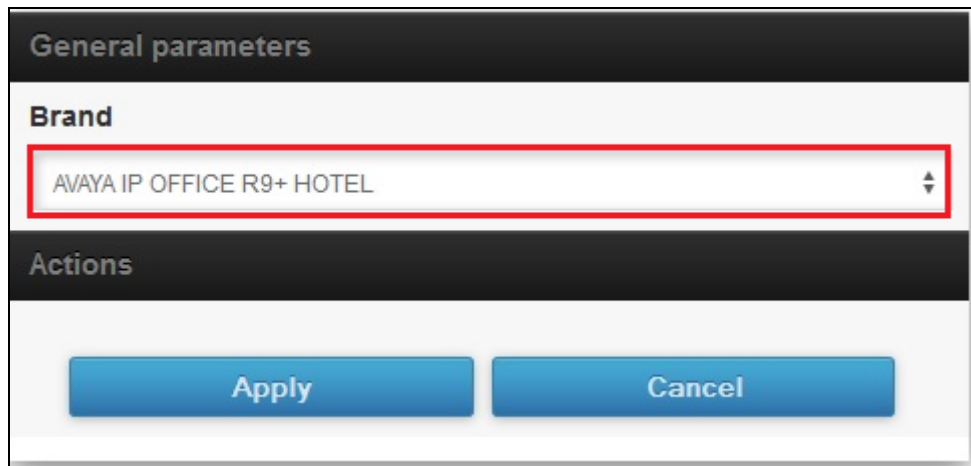
Once logged in, click on **Settings**.



| Link       | Enabled   |
|------------|-----------|
| Connection | Connected |
| Last error |           |

| Link       | Enabled   |
|------------|-----------|
| Connection | Connected |
| Last error |           |

In the **General parameters** window select **AVAYA IP OFFICE R9 + HOTEL** from the **Brand** drop down box.



The screenshot shows a window titled "General parameters". Inside, there is a section labeled "Brand" with a dropdown menu. The dropdown menu is open, showing the selected option "AVAYA IP OFFICE R9+ HOTEL". Below the "Brand" section is a section labeled "Actions" containing two buttons: "Apply" and "Cancel".

### 6.3. Advanced Settings.

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

- **CHECKIN** Enter **checkin**
- **CHECKOUT** Enter **checkout**
- **DND** Enter **dnd**
- **TEMPODHM** Enter **60**
- **USRLOGIN** Enter **Administrator**
- **USRPASSWORD** Enter **Administrator**
- **WEBSERVICE\_URL** Enter  
**http://###WEBSERVICE\_IP###:###WEBSERVICE\_P  
ORT###/IPOConfigurationService?wsdl**
- **WEBSERVICE\_PORT** Enter **8085**
- **WEBSERVICE\_IP** Enter **127.0.0.1**
- **IPOTYPE** Enter **IPOfficeMMManager**
- **BATCHTRANSACTION** Enter **0**
- **ADVLOGS** Enter **1**

| Advanced params  |  |                                       |
|------------------|--|---------------------------------------|
| ID               | Value  | Infos                                 |
| CHECKIN          | <input type="text" value="checkin"/>   | CheckIn Group Name                    |
| CHECKOUT         | <input type="text" value="checkout"/>  | CheckOut Group Name                   |
| DND              | <input type="text" value="dnd"/>   | DND Group Name (do not disturb)       |
| TEMPODHM         | <input type="text" value="60"/>  | Tempo DHM (seconds)                   |
| USRLOGIN         | <input type="text" value="Administrator"/>   | User (Avaya)                          |
| USRPASSWORD      | <input type="text" value="Administrator"/>   | Password (Avaya)                      |
| WEBSERVICE_URL   | <input type="text" value="http://###WEBSERVICE_IP###:###WEBSERVICE_PORT###/IPOConfigurationService?wsdl"/> | WebService : URL                      |
| WEBSERVICE_PORT  | <input type="text" value="8085"/>  | WebService : Port                     |
| WEBSERVICE_IP    | <input type="text" value="127.0.0.1"/>   | WebService : IP                       |
| IPOTYPE          | <input type="text" value="IPOfficeMMManager"/>   | IPO Type                              |
| BATCHTRANSACTION | <input type="text" value="0"/>   | Force save on IPO ( 0 = No, 1 = Yes ) |
| ADVLOGS          | <input type="text" value="1"/>   | Advanced logs ( 0 = No, 1 = Yes )     |

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

- **CHECK\_CMD\_DHM\_ISVALID** Enter **0**
- **ROOMSTATUS\_VACANT\_DIRTY** Enter **\*71** (See Appendix A)
- **ROOMSTATUS\_VACANT\_CLEAN** Enter **\*72** (See Appendix A)
- **ROOMSTATUS\_VACANT\_INSPECTED** Enter **\*73** (See Appendix A)
- **ROOMSTATUS\_OCCUPIED\_DIRTY** Enter **\*74** (See Appendix A)
- **ROOMSTATUS\_OCCUPIED\_CLEAN** Enter **\*75** (See Appendix A)
- **ROOMSTATUS\_OCCUPIED\_INSPECTED** Enter **\*76** (See Appendix A)
- **FORCER\_CHECKOUT\_SDA** Enter **1**

|                               |                                  |   |
|-------------------------------|----------------------------------|---|
| CHECK_CMD_DHM_ISVALID         | <input type="text" value="0"/>   | Recheck DHM Changes ( 0 = No, 1 = Yes )           |
| ROOMSTATUS_VACANT_DIRTY       | <input type="text" value="*71"/> | Free Dirty.                                       |
| ROOMSTATUS_VACANT_CLEAN       | <input type="text" value="*72"/> | Free Clean.                                       |
| ROOMSTATUS_VACANT_INSPECTED   | <input type="text" value="*73"/> | Free Inspected.                                   |
| ROOMSTATUS_OCCUPIED_DIRTY     | <input type="text" value="*74"/> | Busy Dirty.                                       |
| ROOMSTATUS_OCCUPIED_CLEAN     | <input type="text" value="*75"/> | Busy Clean.                                       |
| ROOMSTATUS_OCCUPIED_INSPECTED | <input type="text" value="*76"/> | Busy Inspected.                                   |
| FORCER_CHECKOUT_SDA           | <input type="text" value="1"/>   | Force checkout and remove DDI ( 0 = No, 1 = Yes ) |

## 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**

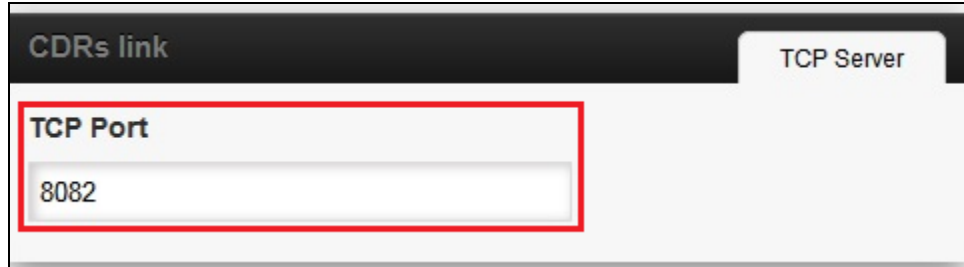
**DHM link**
TCP Client

Select "SMDR" on the AVAYA's manager, and enter the IP Address of the computer hosting the software (and the same port)

**IP Address**

**TCP Port**

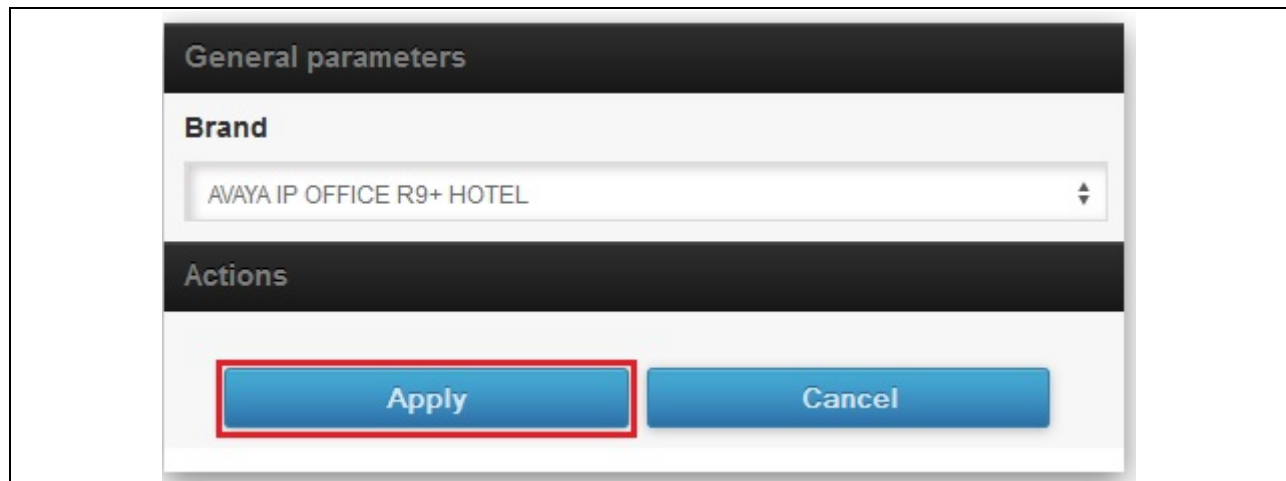
In the **CDRs link** window enter the **TCP Port** as configured in **Section 5.1.0 (8082)**.



The screenshot shows a window titled "CDRs link" with a tab labeled "TCP Server". Below the tab, there is a label "TCP Port" and a text input field containing the value "8082". The input field is highlighted with a red rectangular border.

## 6.5. Apply GT Connector Configuration

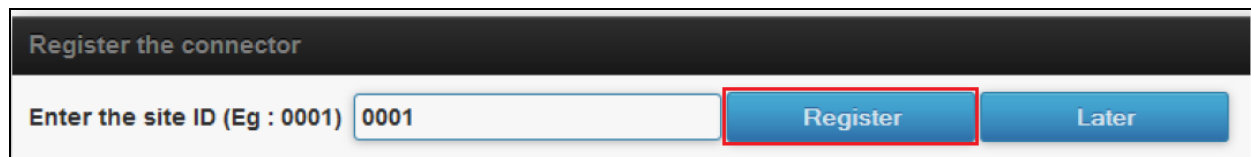
Return to the **General Parameters** window and click on the **Apply** button.



The screenshot shows a window titled "General parameters". It has a "Brand" section with a dropdown menu showing "AVAYA IP OFFICE R9+ HOTEL". Below this is an "Actions" section containing two buttons: "Apply" and "Cancel". The "Apply" button is highlighted with a red rectangular border.

## 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 has a label "Enter the site ID (Eg : 0001)" followed by a text input field containing 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 Steps

The following steps may be used to verify the configuration:

- Verify the connection status of GT-HOSP
- Verify data collection

### 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**.

| Link       | Enabled   |
|------------|-----------|
| Connection | Connected |
| Last error |           |

### 7.2. Verify data collection

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

```
<Type>IP 500 V2</Type><Version>9.0.0.0 build 829</Version>
<MacAddress>00e007051545</MacAddress><Mode>IP OFFICE</Mode></IPOfficeUnitDetails>
AvayaConnected APRES ConnectAndGetUnitDetails(10.10.60.30)
AvayaConnected AVANT GetIPOfficeUnitDetailsXML
AvayaConnected APRES GetIPOfficeUnitDetailsXML
AvayaConnected AVANT FUnitConfiguration.AvayaInfos.LoadAvayaInfos
AvayaConnected APRES FUnitConfiguration.AvayaInfos.LoadAvayaInfos
WebService connection success.
DHM : Connected.
SEND - NO DATA
SEND - NO DATA
```

### 7.3. Verify Hospitality feature

Using the **Checkin Assistant** of GT-HOSP check in a new customer and ensure that the name of the customer is updated on the telephone display and external calls are allowed.

**Note:** For information on using the **Checkin Assistant** refer to the product documentation in **Section 9**. The **Checkin Assistant** can be found by selecting **Customer Checkin** after logging on to the GT-HOSP Server.

## 8. Conclusion

A full and comprehensive set of feature and functional test cases were performed during Compliance testing. GT2F GT-HOSP is considered compliant with Avaya IP Office 500v2 9.0. All test cases have passed and met the objectives with one observation stated 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 the local Avaya representative.

*[1] Avaya IP Office Manager 9.0, Document 15-601011, Issue 9.01, September 2013*

Product Documentation for GT2F can be obtained in the installed software or at: [www.gt2f.com](http://www.gt2f.com)

## Appendix A

| <b>Room Status</b> | <b>Virtual Extension/Users</b> | <b>Short code</b> |
|--------------------|--------------------------------|-------------------|
| Vacant Dirty       | 3040                           | *71               |
| Vacant Clean       | 3041                           | *72               |
| Vacant Inspected   | 3042                           | *73               |
| Occupied Dirty     | 3043                           | *74               |
| Occupied Clean     | 3044                           | *75               |
| Occupied Inspected | 3045                           | *76               |

---

**©2014 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).