Avaya Solution & Interoperability Test Lab

Application Notes for configuring Ascom IP-DECT with Avaya IP Office - Issue 1.0

Abstract

These Application Notes describe a solution for supporting interoperability between Ascom IP-DECT R11 (V11.3.4) with Avaya IP Office R11.1.1. Ascom DECT handsets register with IP Office as SIP endpoints via the Ascom IP-DECT base station.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Ascom IP-DECT R11 solution to interoperate with Avaya IP Office. Ascom DECT handsets are configured on the IP Avaya Office as SIP users, therefore enabling them to make/receive internal and PSTN/external calls and have full voicemail and other telephony facilities available on Avaya IP Office. The wireless communication is made using Ascom IP-DECT access points connected to the same LAN as the Avaya IP Office.

Note: Ascom IP-DECT 'access points' may also be referred to as 'base stations' throughout this document.

The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion cabinet. Both systems are linked by IP Office Line IP trunks that can enable voice networking across these trunks to form a multi-site network. Each system in the solution automatically learns each other's extension numbers and usernames. This allows calls between systems and support for a range of internal call features.

The Ascom IP-DECT system is a modular solution for large and small deployments with full handover capabilities within one PBX. The Ascom IP-DECT access point works as a conduit between the Avaya IP Office and the Ascom DECT wireless handsets. After the Ascom DECT wireless handsets register with the Ascom IP-DECT access point, the access point registers the handsets to Avaya IP Office.

- IP (Internet Protocol) – Universal standard for inter-networking that maximizes scalability and interoperability.
- DECT (Digital Enhanced Cordless Telecommunications) - Secure radio communication standard that delivers superior voice quality over reserved radio frequency bands.

2. General Test Approach and Test Results

The general test approach was to configure the Ascom DECT handsets to communicate with IP Office as implemented on a customer's premises. The interoperability compliance testing evaluates the ability of the Ascom DECT handsets (DECT handsets) to make and receive calls to and from Avaya H.323, SIP, Digital desk phones and PSTN endpoints. The integrated IP Office voicemail was used to allow users leave voicemail messages and to demonstrate Message Waiting Indication and DTMF on the DECT handsets. See **Figure 1** for the network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

Note: For compliance testing the Ascom DECT handsets were registered to the primary server.

Note: Compliance testing was carried out using TCP as the transport for signalling, a selection of basic calls and transfer calls were carried out using UDP.

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's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements.

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and DECT handsets did not include use of any specific encryption features as requested by Ascom.

2.1. Interoperability Compliance Testing

Tests were performed to ensure full interoperability between the DECT handsets and IP Office. The tests were all functional in nature and performance testing was not included. The testing included:

- Registration/Invalid Registration
- Basic Calls, local and PSTN
- Hold and Retrieve
- Attended and Unattended Transfer
- Call Forwarding Unconditional, No Reply and Busy (Local and PBX)
- Call Waiting
- Call Park/Pickup
- Do Not Disturb
- Calling Line Name/Identification
- Codec Support (G.711A, G.729, G.711U tested)
- DTMF Support
- Message Waiting Indication

- Mobile Twinning
- Hunt Groups
- Serviceability Testing

Note: Compliance testing does not include redundancy testing as standard. Where some LAN failures were simulated, and the results observed, there were no redundancy or failover tests performed.

2.2. Test Results

All test cases were carried out with positive results. There were some observations and some issues noted as follows.

1. When the Ascom DECT handset has an incorrect username or password the IP Office will blacklist that IP address after 10 attempts, which means that all the DECT handsets are blacklisted until this is removed manually using IP Office System Monitor, see **Section 7.3**. This is as per IP Office design.
2. All of the transferred calls both blind and supervised complete successfully but the A-party is not updated for some of these calls, where the A-party is the Ascom DECT phone.
3. Call on Hold Reminder does not work for the Ascom DECT sets. This is not a supported feature for 3rd party SIP phones.
4. G.722.2 (AMR-WB) or G.723 is not available on IP Office. Only G.722 – 64K and this is <u>not</u> supported on the DECT handsets.
5. SIP Expires timer on Ascom DECT recommended setting at 180 seconds. This is hard coded in IP Office and cannot be changed. When the amount of IP Office Users configured exceeds 180 this timer will also increase with the number of users. For example, if there are 290 users configured the SIP Expiry Timer will be hardcoded at 290 seconds.
6. It is recommended that "Call Waiting" on IP Office and IP-DECT is turned off for the Ascom DECT users. This is to facilitate the use of DECT and semi-attended transfers, see **Sections 5.3** and **6.1.5** for details on turning this feature off/on.

2.3. Support

Technical support from Ascom can be obtained through the following:

Phone : +46 31 559450
E-mail : support@ascom.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an IP Office which the Ascom DECT handsets were configured as SIP users. The Avaya IP Office consists of an IP Office Server Edition running on a virtual platform as the primary server with an IP Office IP500 V2 running as the secondary expansion server. Digital, H.323 and SIP phones were configured on the IP Office. ISDN and SIP trunks were configured to simulate connections to the PSTN. The Ascom base station was connected to the IP Network which the DECT handsets register to. The access point or base station allows radio communication between the DECT handsets which in turn communicates with IP Office.

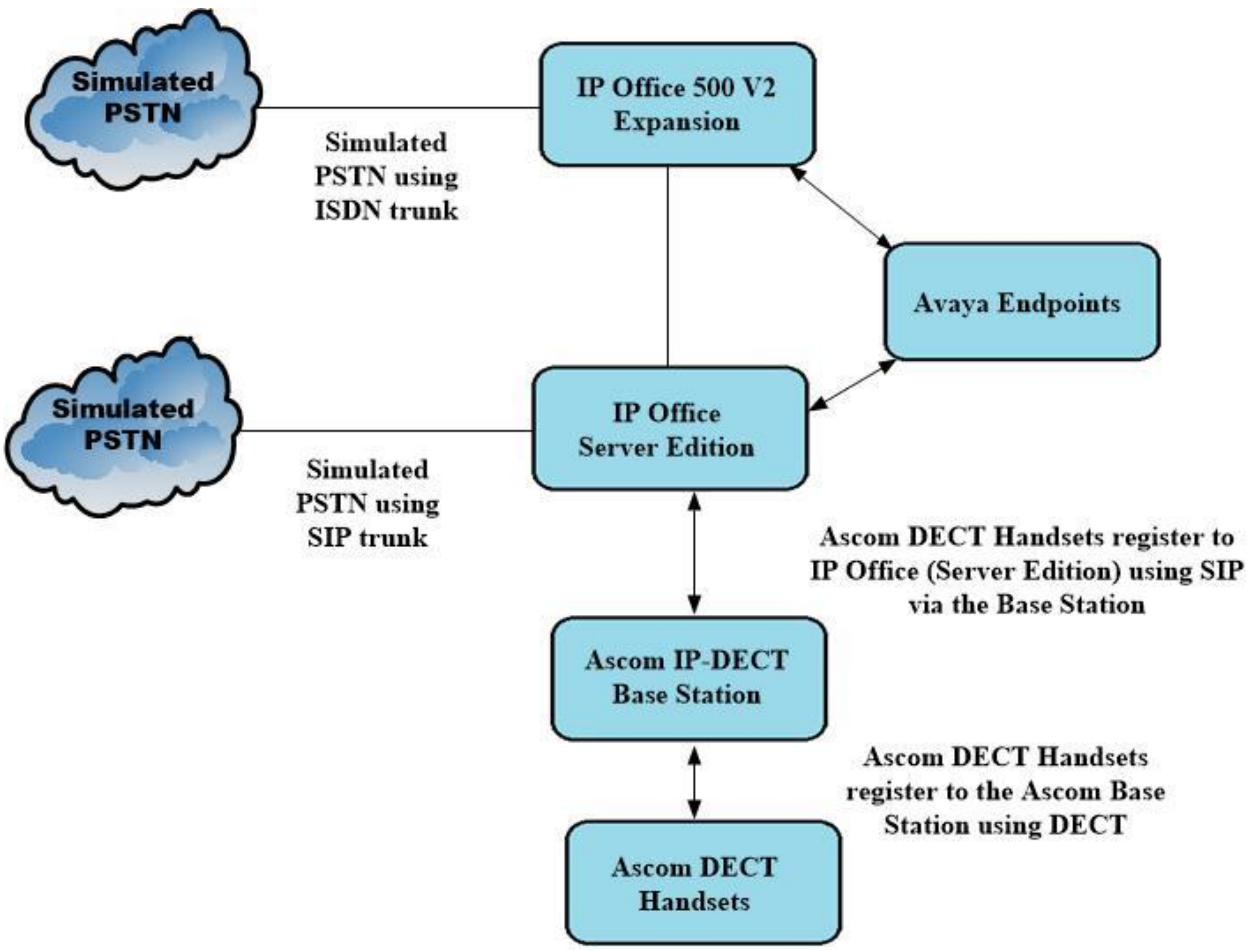


Figure 1: Avaya IP Office and Ascom Reference Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya IP Office Server Edition running on a Virtual Platform	11.1.1.0.0 Build 209
Avaya IP Office 500 V2	11.1.1.0.0 Build 209
Avaya IP Office Manager running on a Windows 7 PC	11.1.1.0.0 Build 209
Avaya J179 H323 Deskphone	6.8304
Avaya 96x1 H323 Deskphone	6.8304
Avaya J189 SIP Deskphone	4.0.6.1.1b4
Avaya 9508 Digital Deskphone	V0.6
Ascom IP-DECT Base Station (IPBS3)	V11.3.4 (R11)
Ascom DECT Handset D63 Talker	2.11.4

Note: Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.

5. Avaya IP Office Configuration

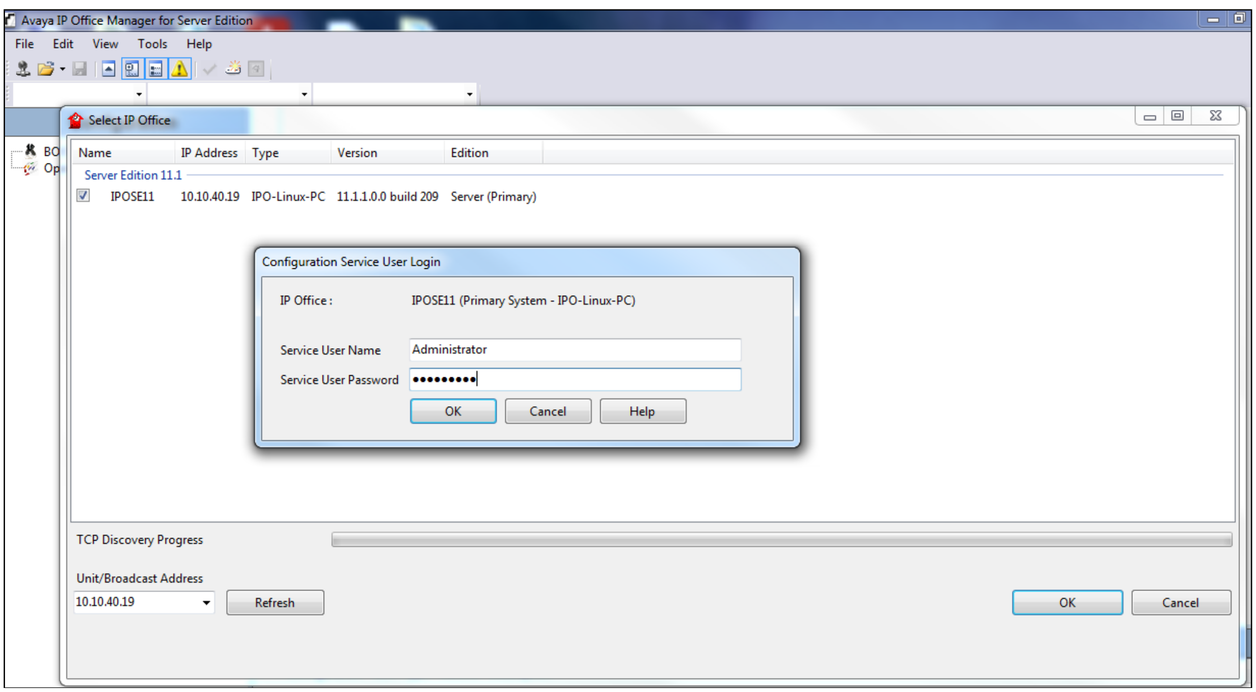
Configuration and verification operations on Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of Avaya IP Office for this solution. It is implied a working system is already in place. For 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 (Administration)
- Display LAN Properties
- Create a new User
- Check Extension Properties
- Verify the Voicemail Collect Short Code
- Save Configuration

Note: Only the unique prompts are shown in the screen captures below, all other inputs can be left at default.

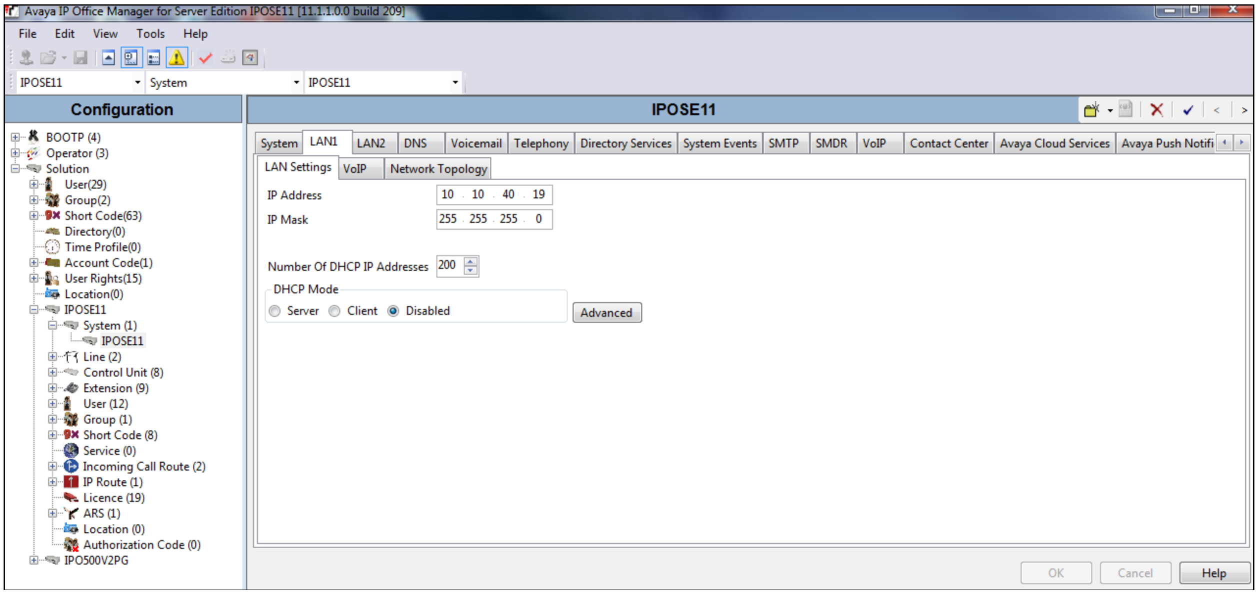
5.1. Launch Avaya IP Office Manager (Administration)

From the IP Office Manager PC, click **Start → Programs → IP Office → Manager** to launch the Manager application (not shown). Select the required Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button.

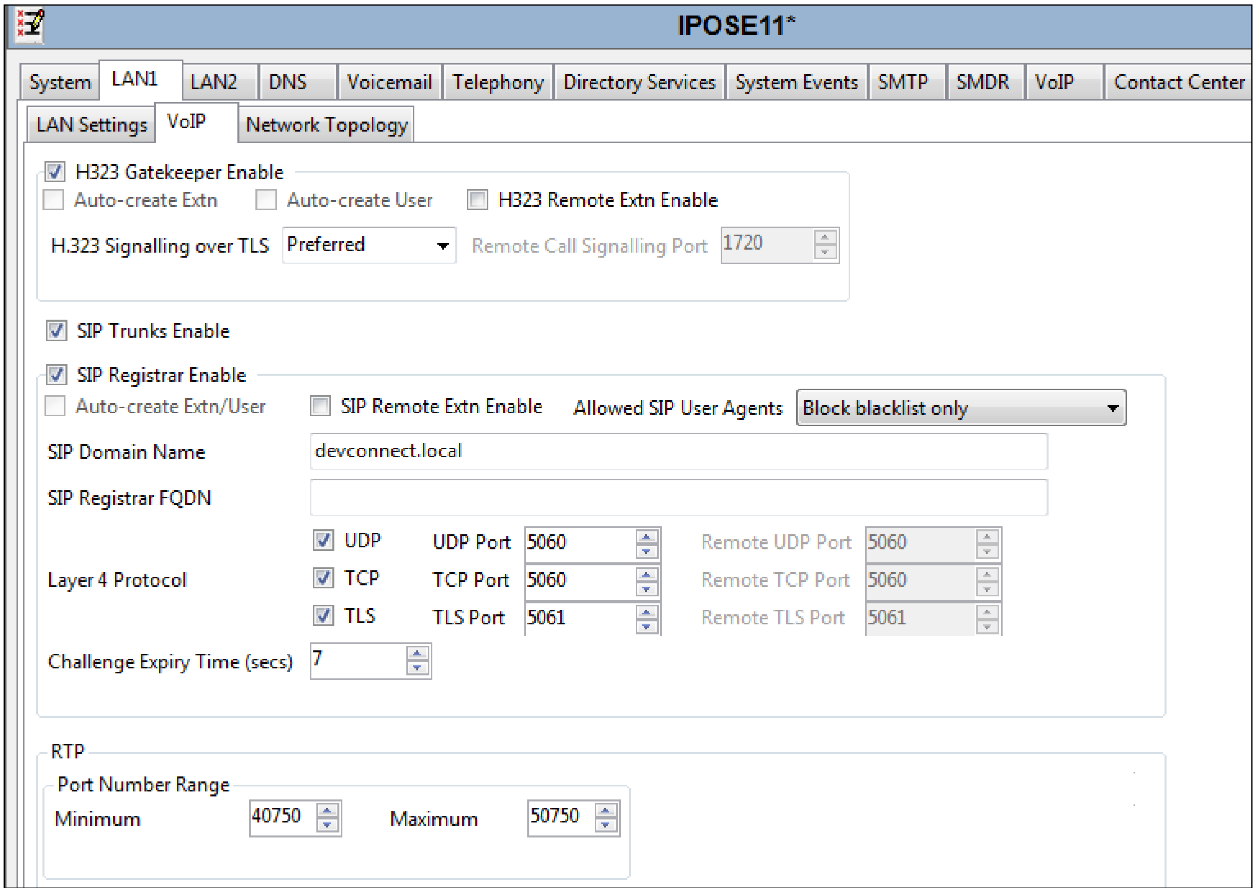


5.2. Display LAN Properties

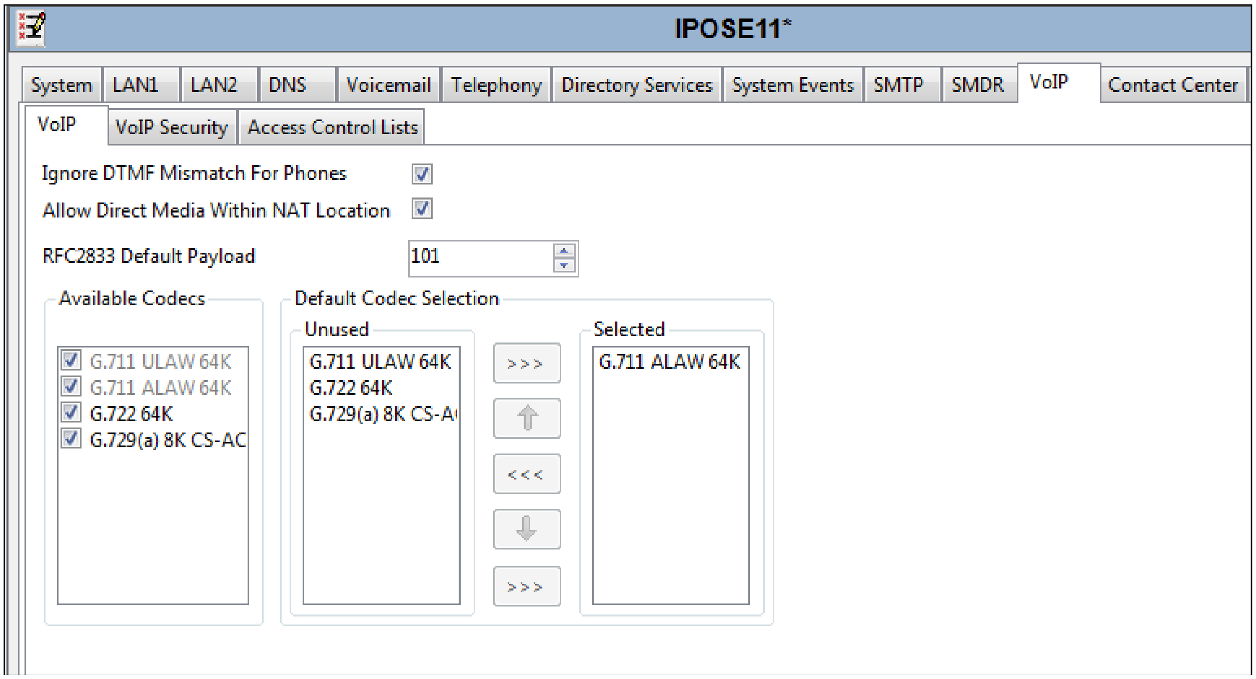
From the left window navigate to **System (1)** as shown and in the main window click on the **LAN1** tab and within that tab select the **LAN Settings** tab. The **IP Address** of the IP Office is shown, and this will be required for setup in **Section 6.1.4**.



Within the **LAN1** tab, click on the **VoIP** tab. Ensure that **TCP** and **UDP** boxes are checked and that port **5060** is being used. During compliance testing **RTP-RTCP Keepalives** were set to **30** secs (not shown).

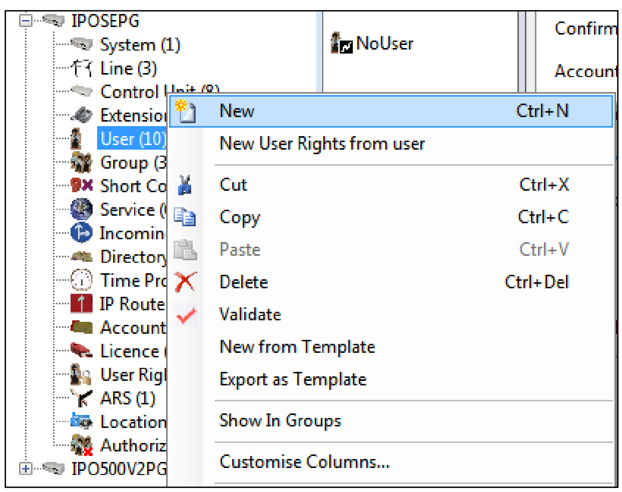


The Codec and DTMF settings can be changed under the **VoIP** tab as shown below.

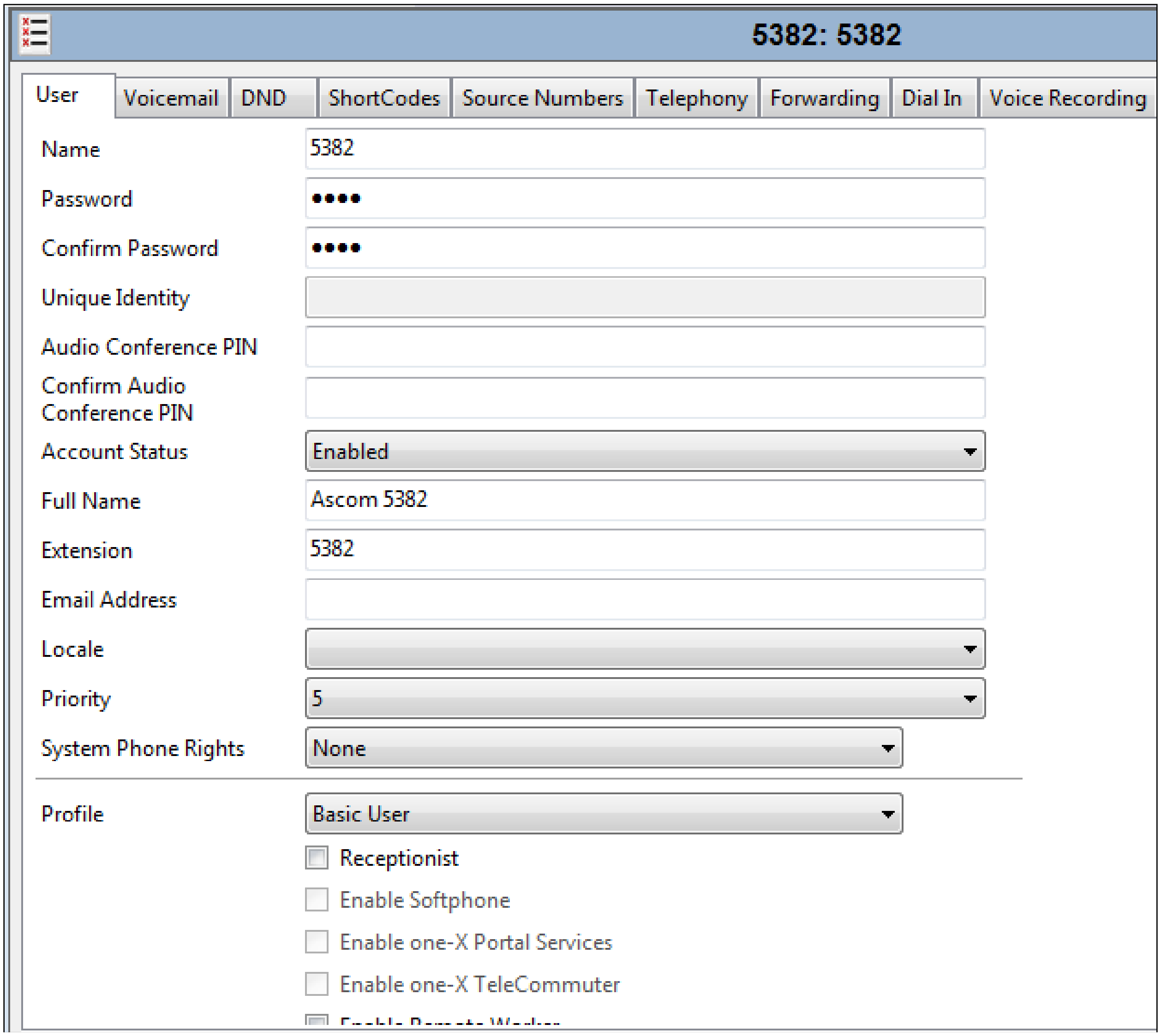


5.3. Create a new User

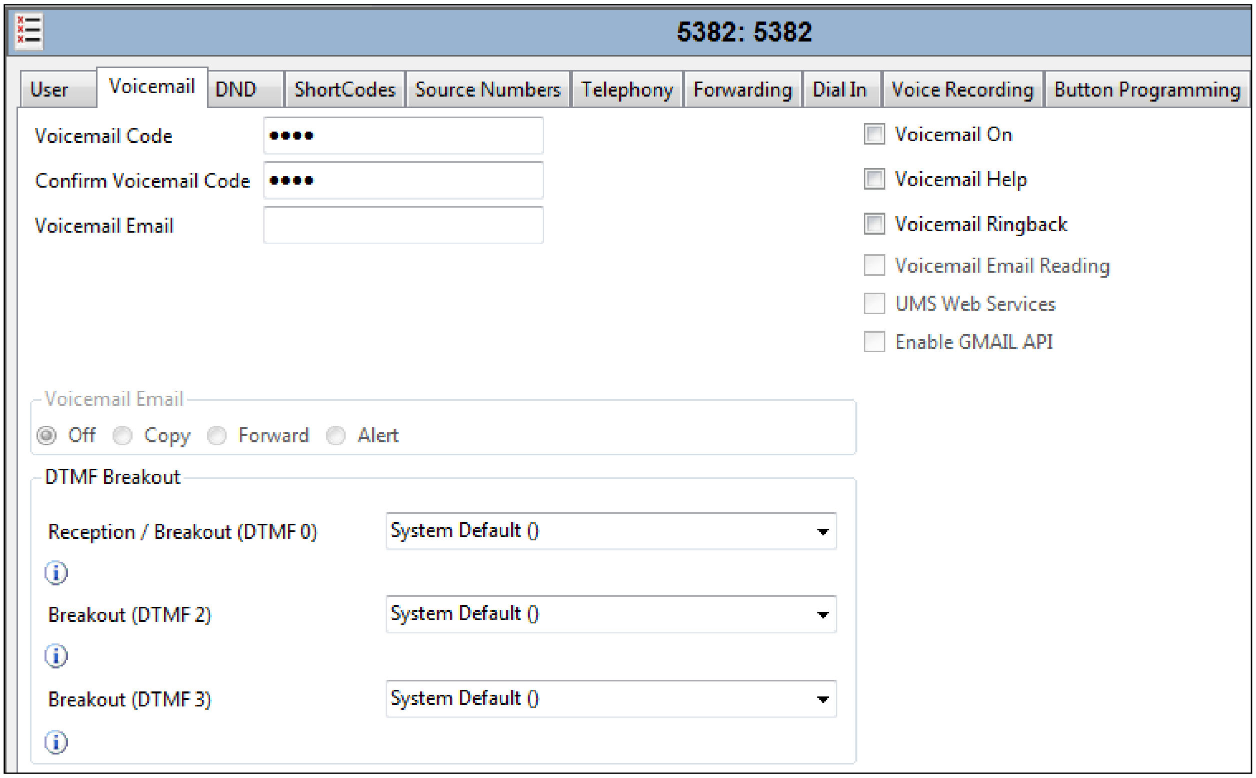
From the left window, right click on **User** and select **New**.



In the **User** tab add a **Name** and **Password** along with the **Extension**.

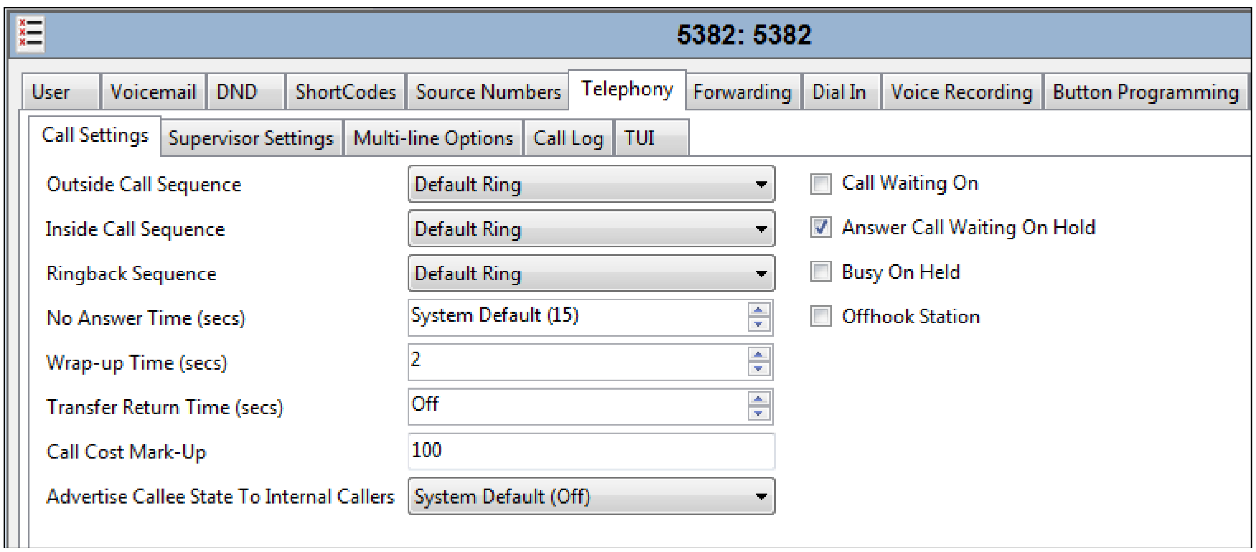


Under the **Voicemail** tab, **Voicemail On** can be selected to provide voicemail to this user/extension.

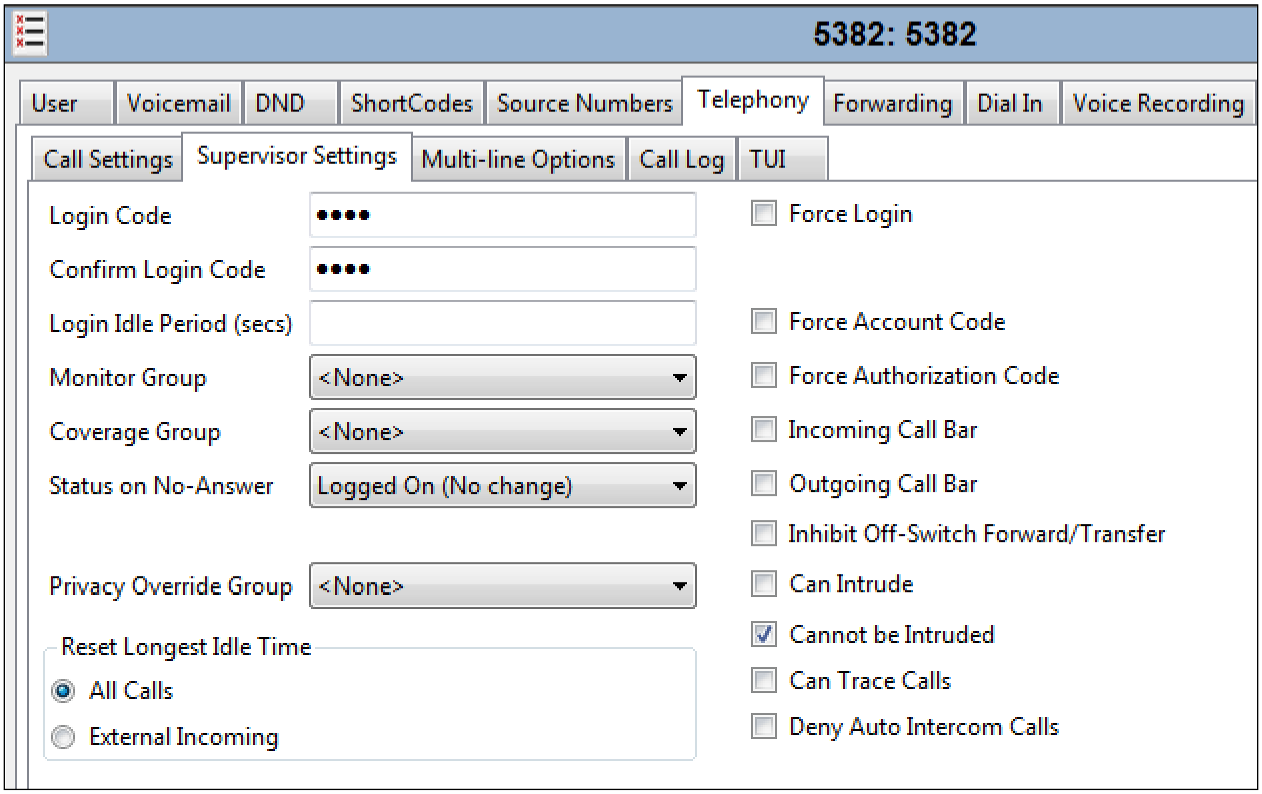


Under the **Telephony** tab and **Call Settings** tab, **Call Waiting On** can be turned on/off depending on what is required by the user.

It is recommended that "Call Waiting" on IP Office and IP-DECT is turned off. There is a scenario with DECT and semi-attended transfers where the "transfer target" and "initial caller" DECT handsets hang up whilst a second party is ringing to the "transferor" during transfer. If a call is made to the "transferor" DECT handset with Call Waiting enabled the handset accepts the call but the ringing call is cancelled. This behaviour is seen using a single R<extn> method to transfer calls. When Call waiting is off, on the IP Office (and IP-DECT base station), the call to the transferring handset shows busy until the transferred call is answered. When the RR<extn> method is used for transferring, a call can be placed to the transferring handset as this method completes the transfer on hang up. This is as per design.

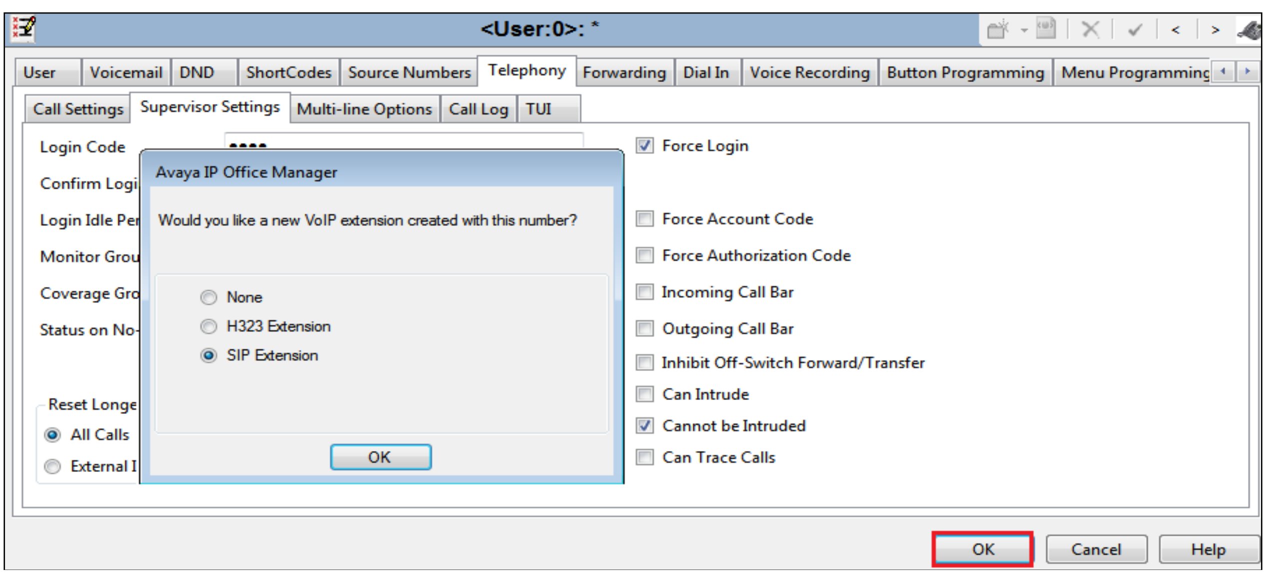


Under **Supervisor Settings** tab enter the password again for the **Login Code**.



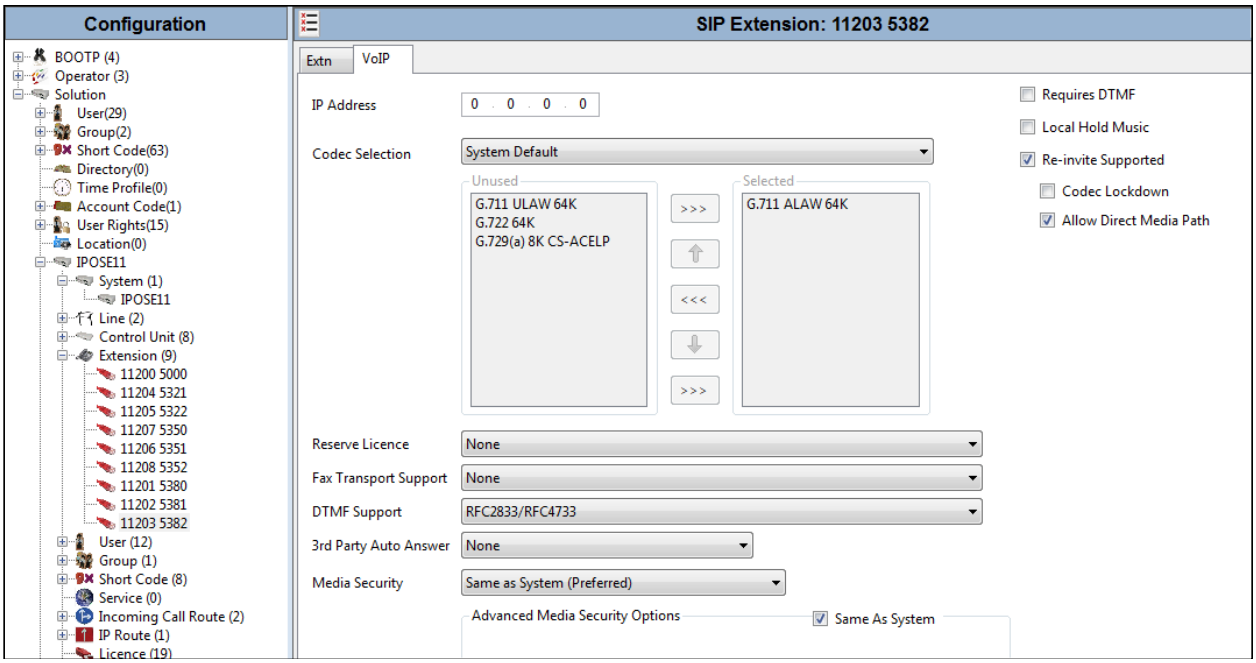
Once **OK** is clicked at the bottom of the screen a new window should appear asking to create a new extension. Select **SIP Extension** as is shown below.

Note: If the system is not setup to auto-create extensions, then a new extension can be added by right-clicking on Extension on the left window and selecting **New**, (not shown).



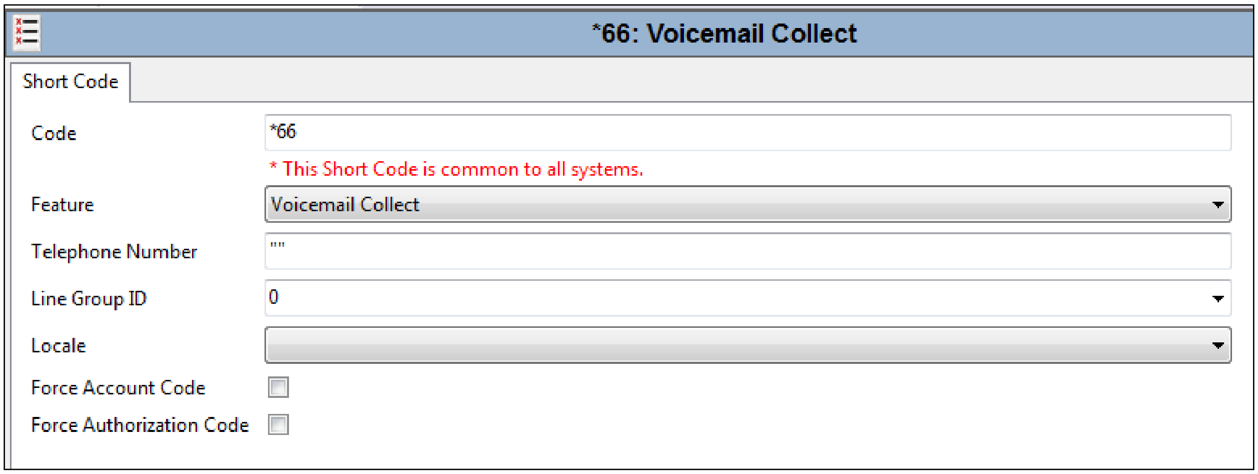
5.4. Check Extension Properties

Direct Media Path can be set on/off in the extension properties. This will allow RTP to be sent directly between devices. Once the SIP extension has been successfully created in **Section 5.3**, open the extension configuration to check to see if Allow Direct Media Path is selected. Select **Extension** in the left window and select the required extension number. In the main window under **VoIP** tab, **Allow Direct Media Path** can be checked or unchecked as shown below. Other settings such as **DTMF Support** and **Codec Selection** are possible to change here as well again if required by Ascom.



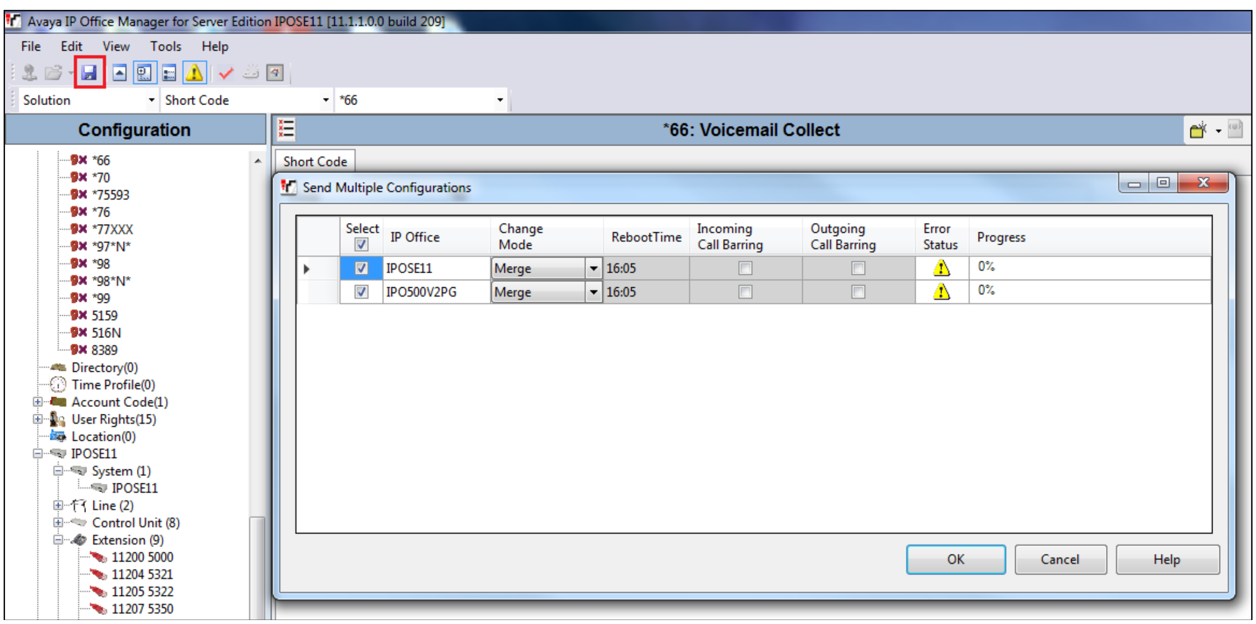
5.5. Verify the Voicemail Collect Short Code

As part of the Ascom IP-DECT base station configuration the voicemail access number is required. During compliance testing this **Feature** was set to **Voicemail Collect**, and the **Code** was ***66** also the **Telephone Number** was **“”**.



5.6. 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 Ascom IP-DECT

This section describes how to access and configure the Ascom DECT solution. The Ascom IP-DECT base stations can be configured in an Active Master/Standby Master or Mirror scenario to provide redundancy. The following configuration steps detail the configuration process used to configure an Ascom wireless IP-DECT base station in Active mode only.

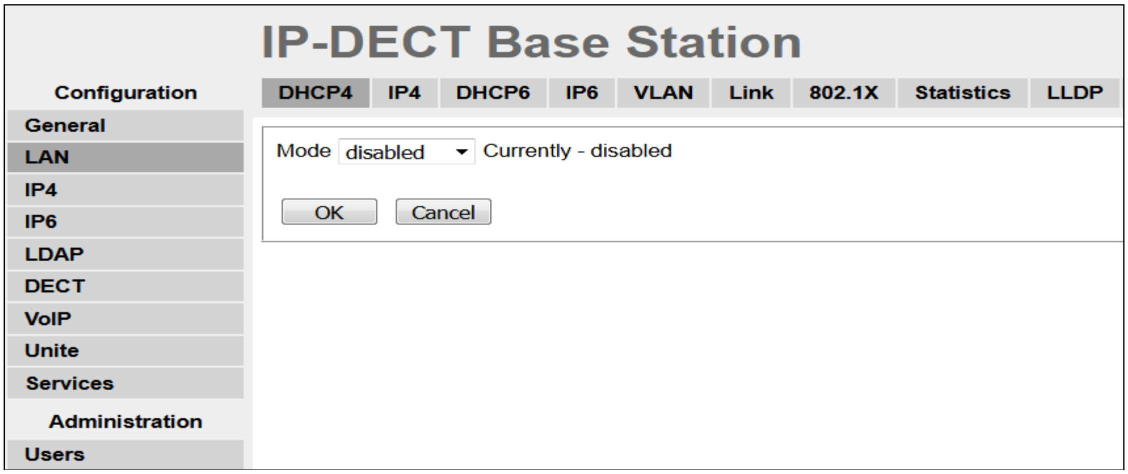
Note: Handover between multiple Ascom IP-DECT base stations was not tested. Refer to the Ascom document in **Section 9** for information on how to configure roaming/handover.

6.1. Configure the IP-DECT Base Station

To configure the IP-DECT base station, access a web browser and enter the IP address of the base station as the URL. The user will be presented with the screen shown below. Select the **System administration** for login and enter the appropriate credentials to access the Ascom IP-DECT base station and then click **OK** (not shown).

6.1.1. Configure LAN DHCP

Navigate to **LAN** and select the **DHCP4** tab. Select **Disabled** from the **Mode** dropdown box. A reset of the base station is required to activate this setting. After the reset is completed log back on to the IP-DECT base station to complete the configuration.

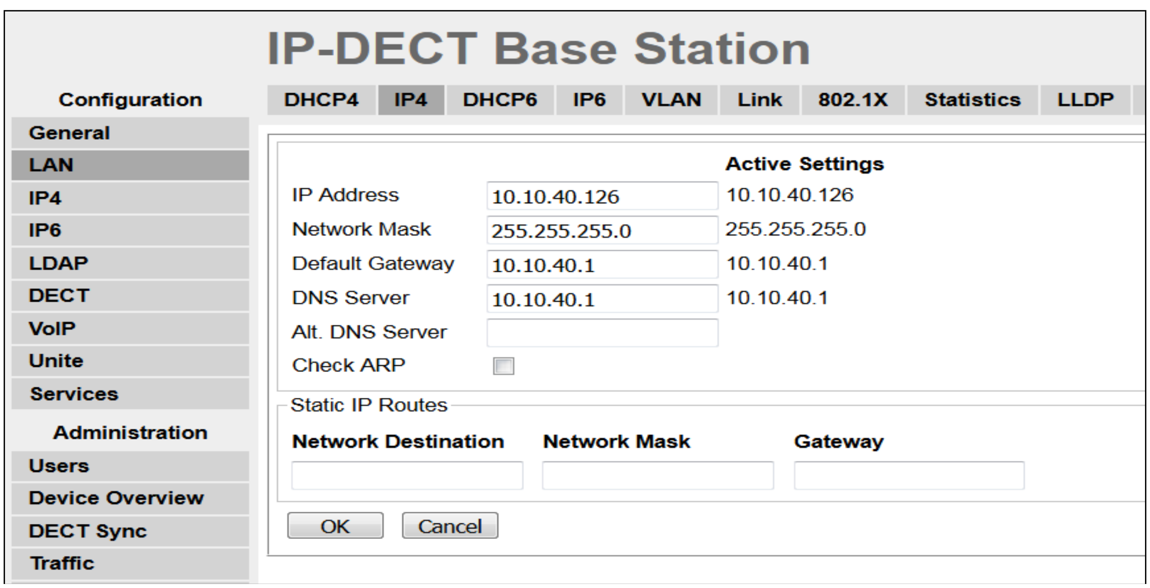


6.1.2. Configure LAN IP

Navigate **to LAN** and select the **IP** tab and enter the following:

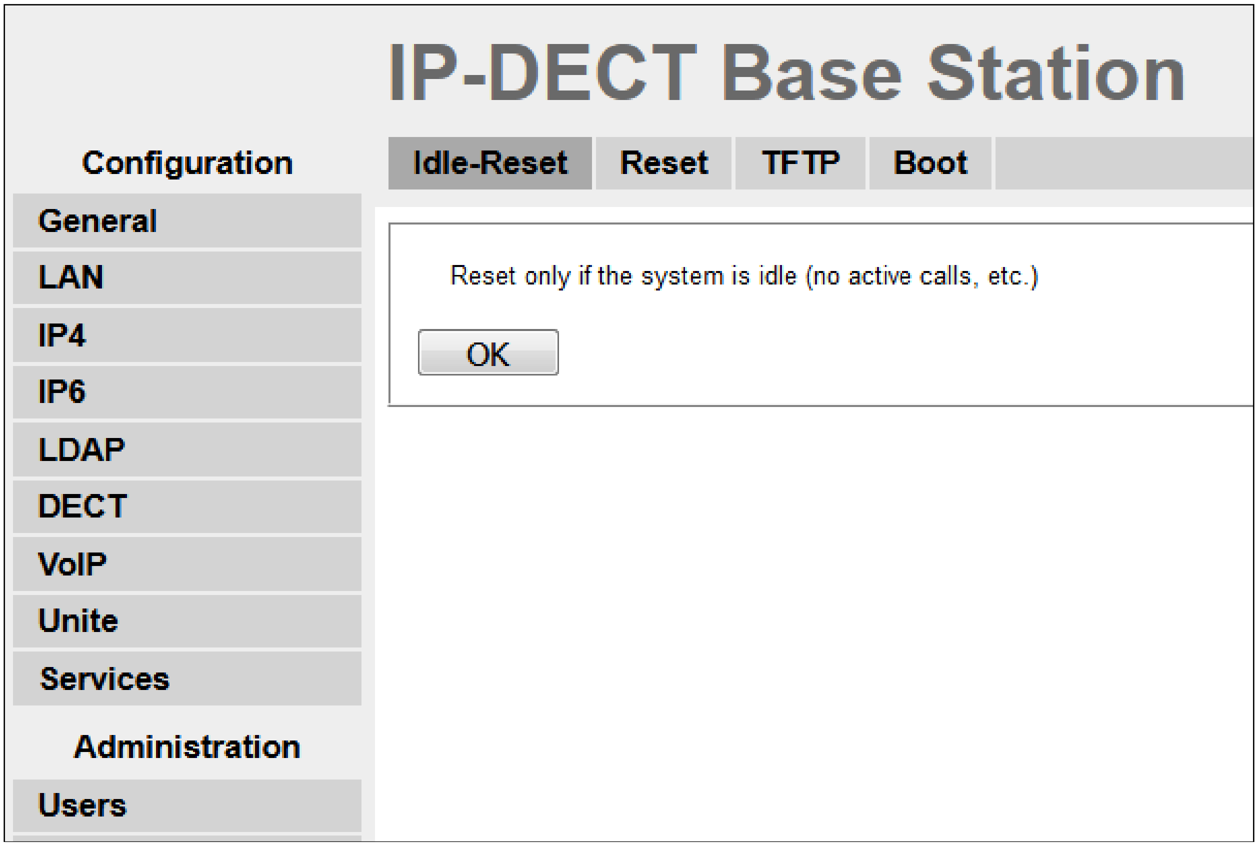
- **IP Address** Enter the IP address to be assigned to the IP-DECT Station.
- **Network Mask** Enter the Network Mask to be assigned to the IP-DECT Station.
- **Default Gateway** Enter the Default Gateway IP Address.
- **DNS Server** Enter the appropriate IP address for the DNS server.

Click on the **OK** Button to save.



6.1.3. Reset IP-DECT Base Station

Click **Reset** followed by the **OK** button to initiate the system reset. Many of the other changes made to the system during the configuration process require a reset. Repeat this process whenever a reset is required.



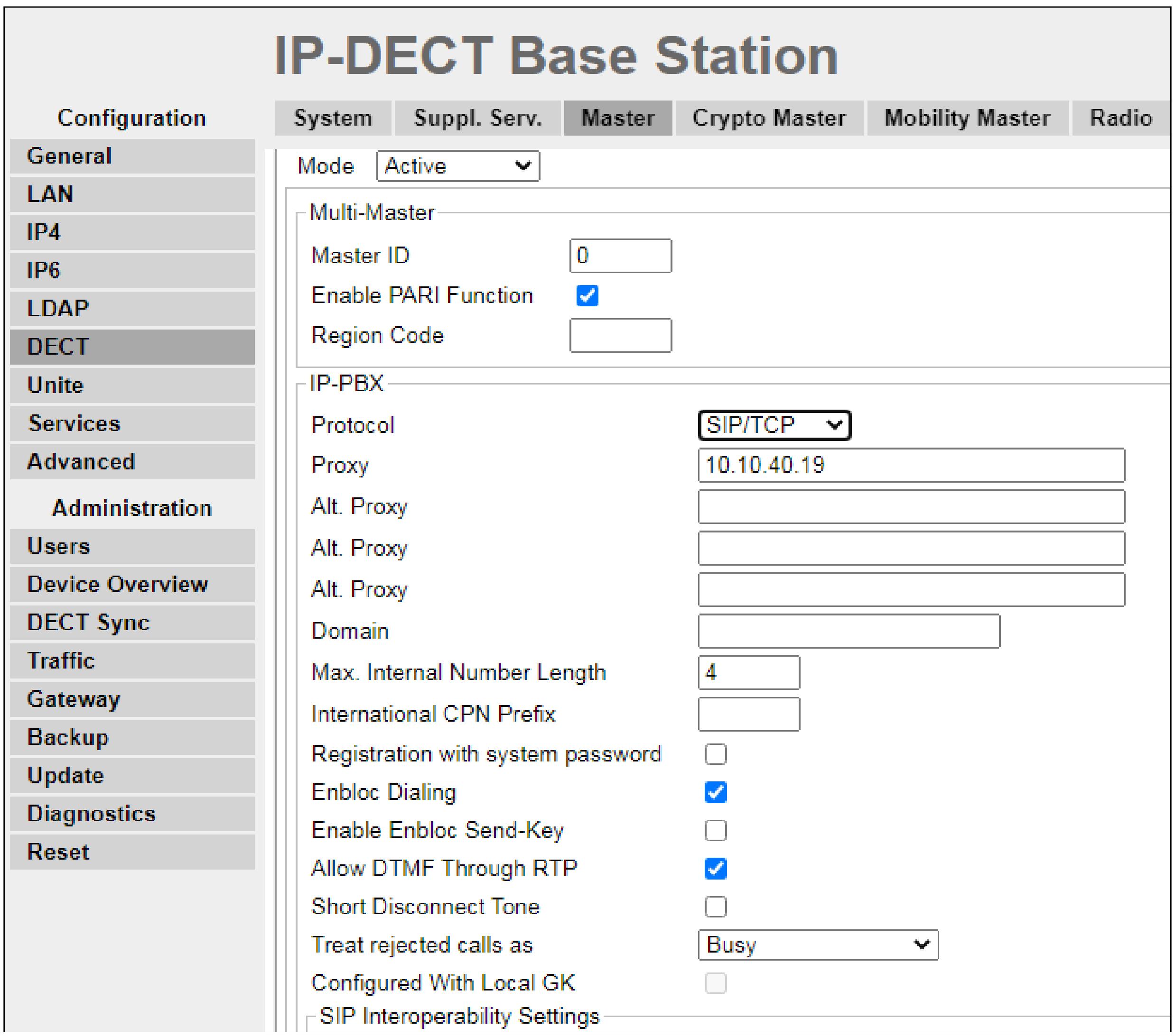
6.1.4. Configure DECT

The following were configured under the **DECT** section (from the left window).

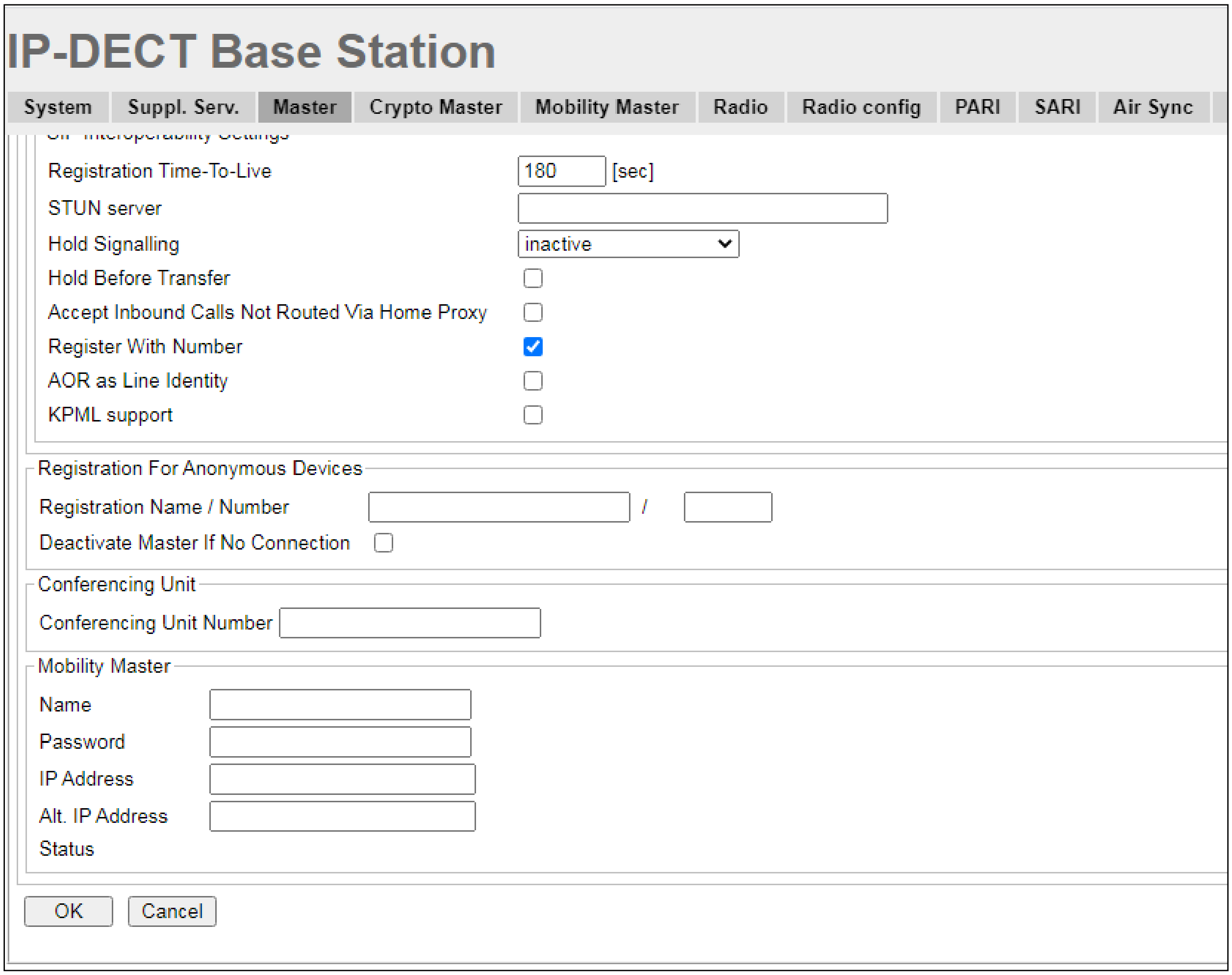
6.1.4.1 Configure Master

Navigate to the **DECT** in the left window and click on the **Master** tab in the main window and enter the following:

- **Mode** → Seen as there was only one base station present for this testing, **Active** was chosen, when there is more than one base station then mirror can be chosen.
- Check the **Enable PARI Function** check box.
- **Protocol** → Select **SIP/TCP** from the dropdown box, again this can be set to TLS or UDP depending on the requirements.
- **Proxy** → Enter the IP address of the IP Office, this was set to the IP Office Server Edition IP.
- Check the **Enbloc Dialing** check box.
- Check the **Allow DTMF through RTP** check box.



Scroll down and set **Registration Time-To-Live** to **180 (sec)**. Click the **OK** button to continue.

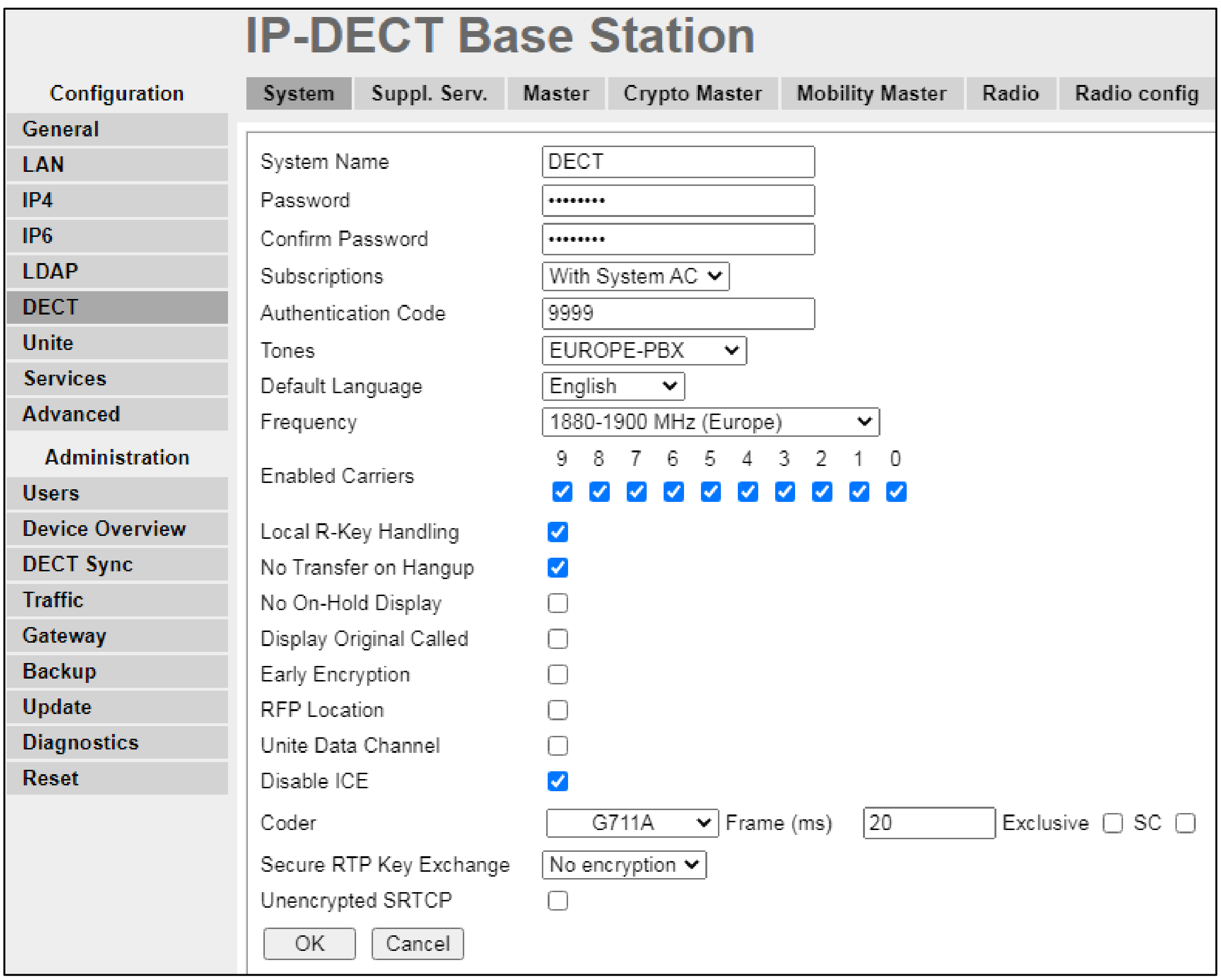


6.1.4.2 Configure System

Click on the **System** tab and enter the following:

- **System Name** → Enter the System Name as previously configured.
- **Password** → Enter the Password as previously configured.
- **Confirm Password** → Confirm the password.
- **Subscriptions** → Select **With System AC** from the dropdown box.
- **Authentication Code** → Enter the DECT handset Login code as configured in **Section 5.3**.
- **Tones** → Select the location where the IP-DECT system is located.
- **Default Language** → Select the required Language from the dropdown box.
- **Frequency** → Select the required Frequency from the dropdown box.
- **Enabled** → Select the number of Carriers required.
- Check **Local R-Key Handling** box.
- Check **Disable ICE** box.
- **Coder** → Select the required codec from the **Coder** dropdown box.

Click the **OK** button to continue.



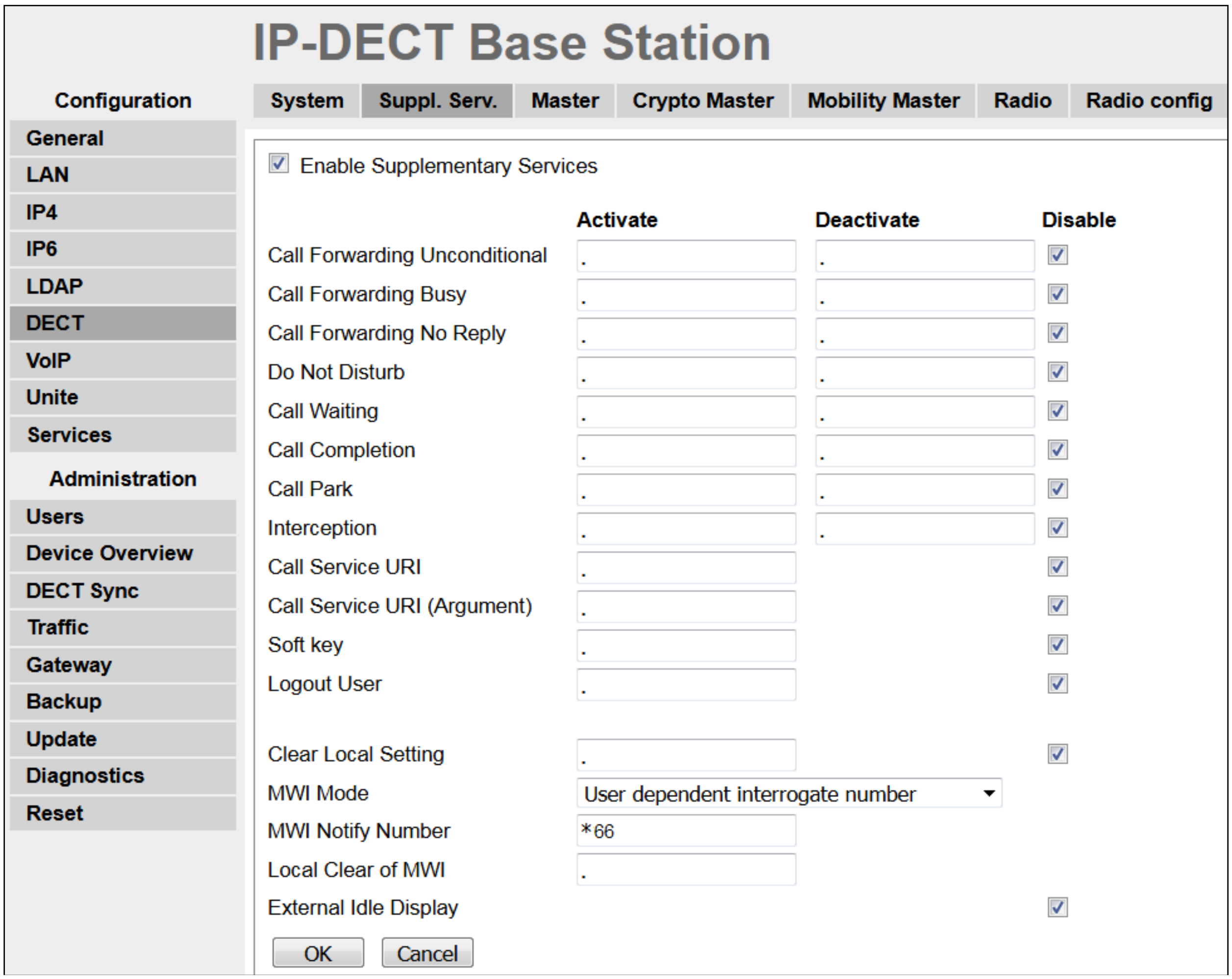
6.1.4.3 Configure Supplementary Services

Click on the **Suppl.Serv.** tab and check the **Enable Supplementary Services** check box. During compliance testing, the IP Office handled most of the features listed, so most of the functions were disabled.

The following were set.

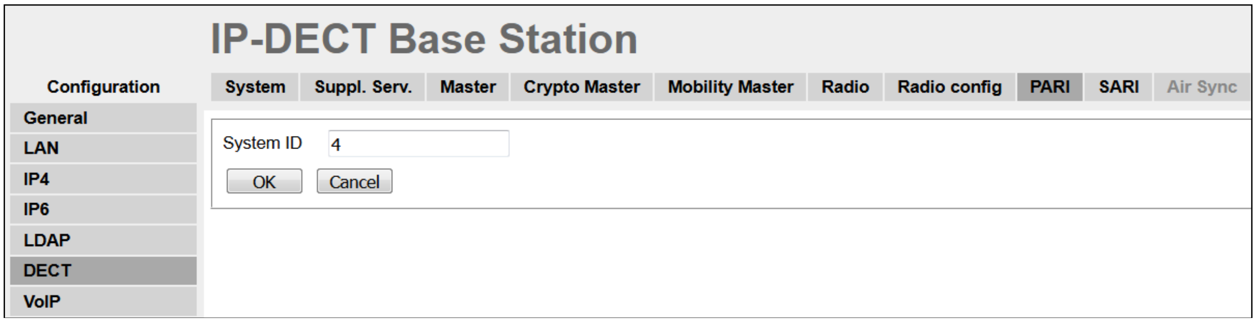
- **MWI Mode** → Select **User dependent interrogate number** from the dropdown box.
- **MWI Notify Number** → Enter ***66** as configured **in Section 5.5**.

Click the **OK** button to continue.



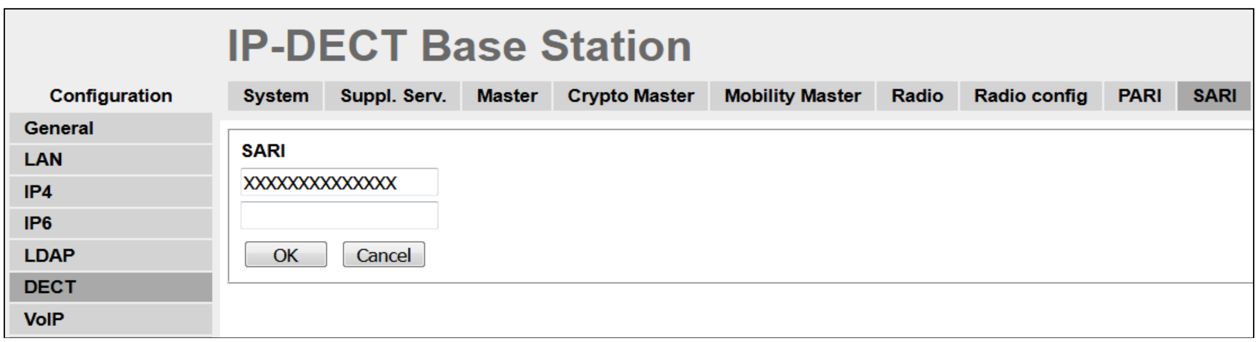
6.1.4.4 Configure PARI

Click on the **PARI** tab and enter the PARI in the System ID Field. The PARI is a user-defined system value. Enter any number from 1-292 (e.g., **4**). Click the **OK** button to continue.



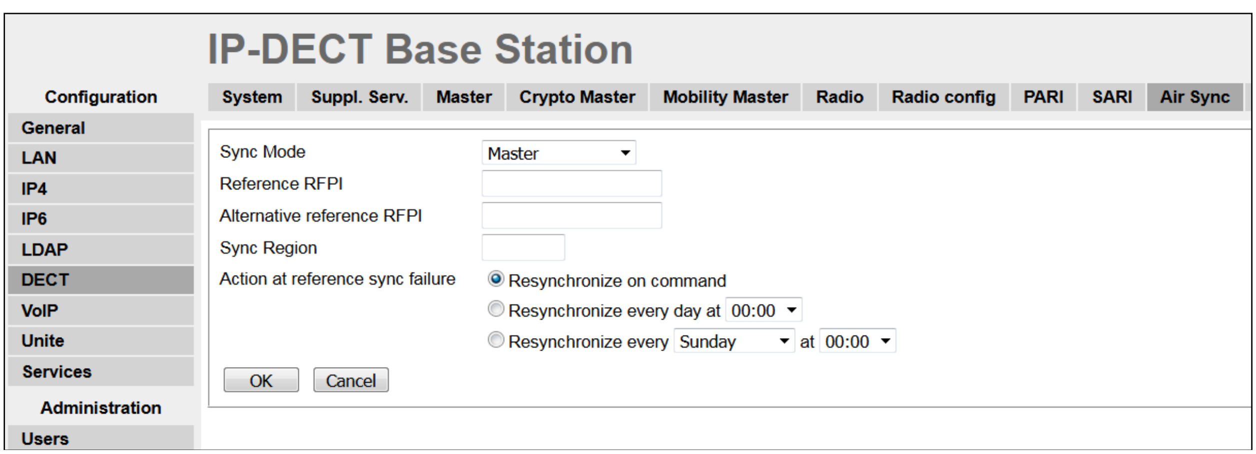
6.1.4.5 Configure SARI

Click on the **SARI** tab. The **SARI** is an Ascom provided activation code which is needed for the system to function. Contact Ascom to obtain a **SARI**. Enter the **SARI** value (note the actual value has been hidden on the screen shown below for security reasons). Click the **OK** button to continue.



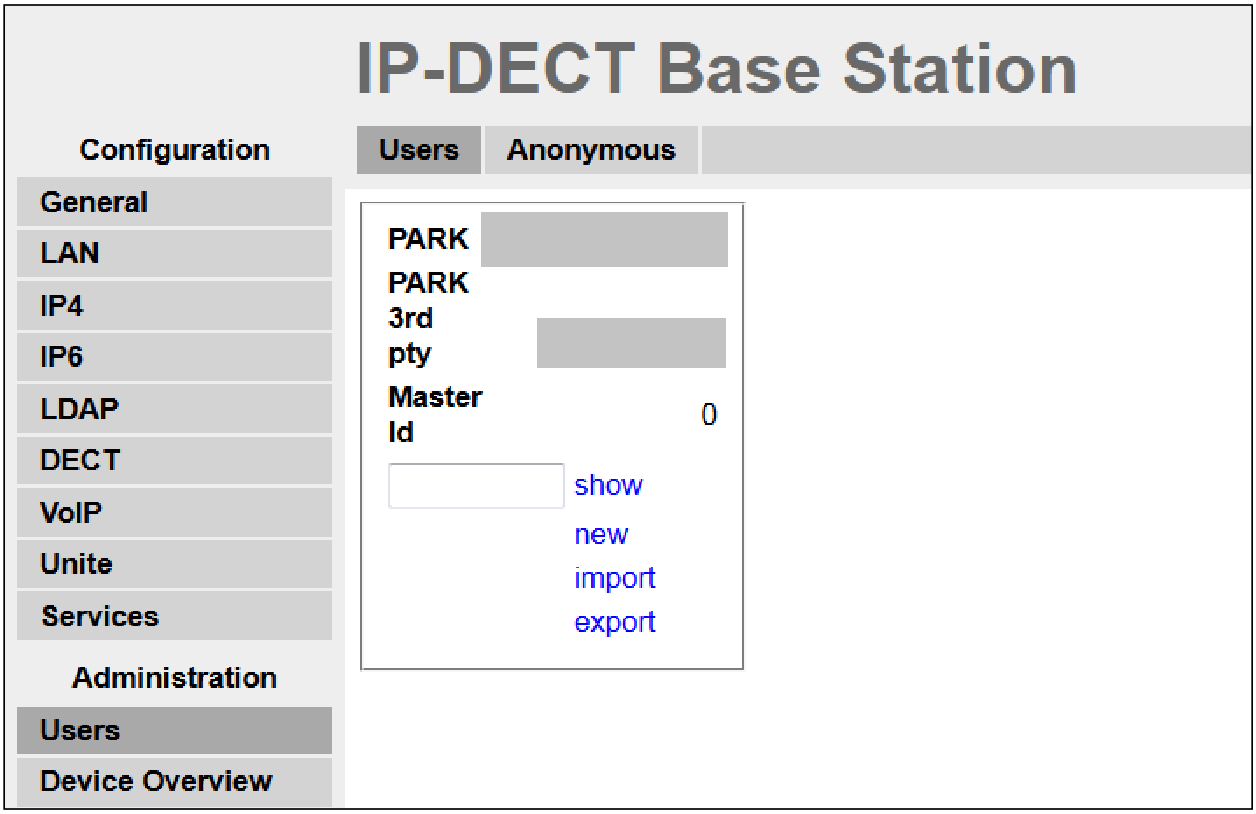
6.1.4.6 Configure Air Sync

Click on the **Air Sync** tab and select **Master** from the **Sync Mode** dropdown box. Click the **Resynchronize on command** radio button. Click the **OK** button to continue.



6.1.5. Create Users

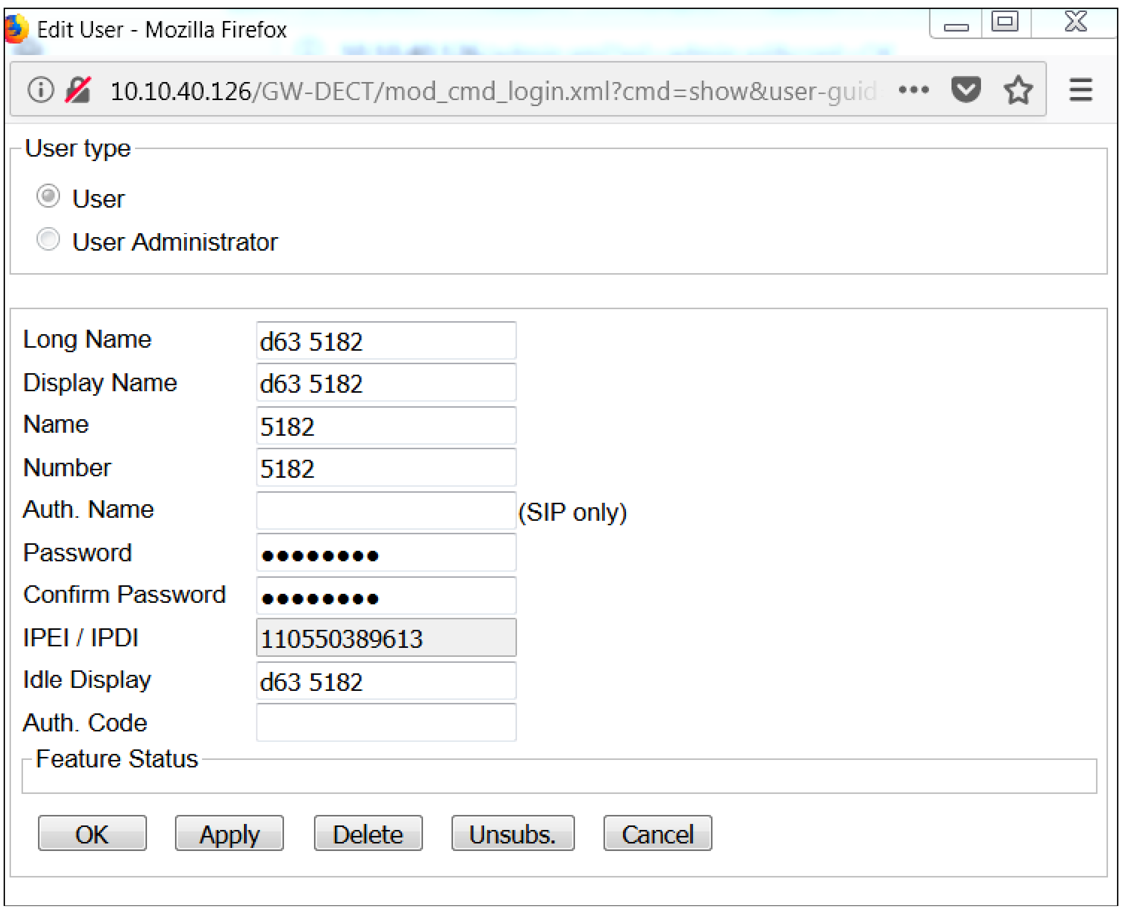
Navigate to the **Users** and click on the **Users** tab. The **Park** value is displayed. This value can be used when programming Ascom DECT handsets (optional, required only when in range of other DECT systems). Note, the **PARK** information is derived from the SARI and should be obtained from an Ascom associate (Note the actual **PARK** and **PARK 3rd pty** values have been hidden on the screen shown below for security reasons). Click the **new** link to provision a new user account.



When the **User type** page is presented click on the **User** radio button and enter the following:

- **Long Name** → Enter any descriptive name that identifies this user (i.e., **d63 5182**).
- **Display Name** → Enter a display name which will be displayed on the DECT Handset screen (i.e., **d63 5182**).
- **Name** → Enter the extension assigned to this user.
- **Number** → Enter the extension assigned to this user.
- **Password** → Enter the Password (Note, the password is the **Login Code** configured in **Section 5.3**).
- **Confirm Password** → Confirm Password.
- **Auth. Code** → Enter the **Auth. Code (**Note the Auth. Code is used only if **Subscriptions** in **Section 6.1.4.2** is set to **With System AC**.

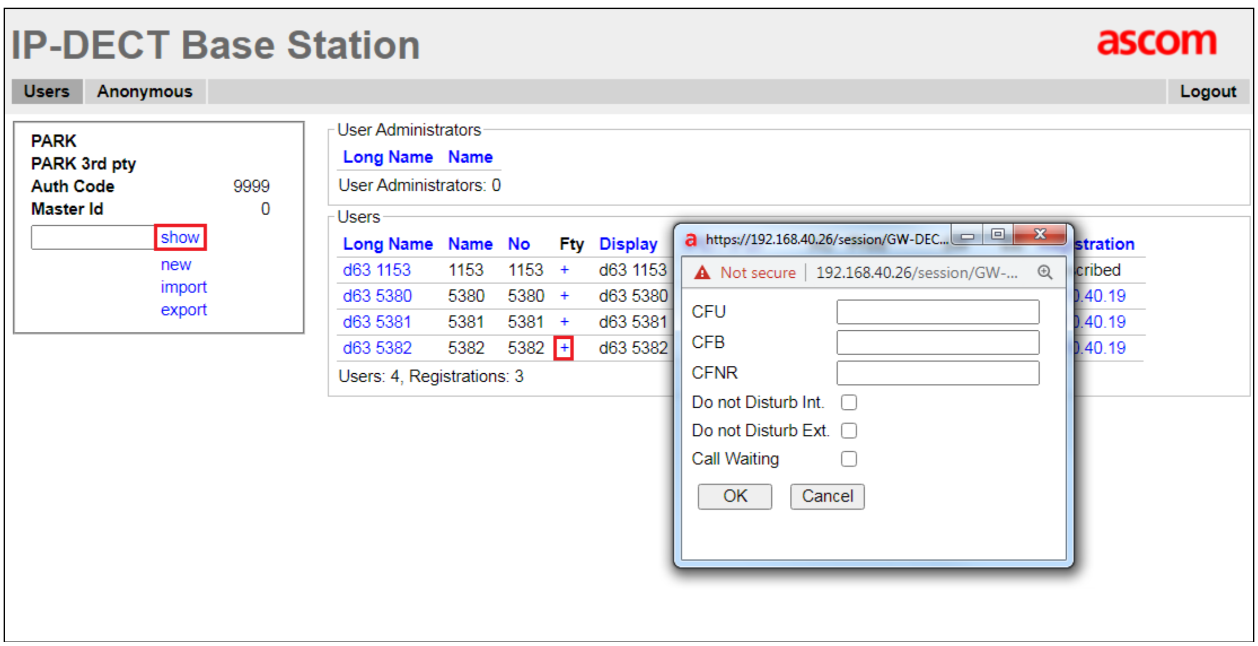
Once all the user information has been configured, click the **OK** button. Repeat this process for each user being added to the system.



The following shows what can be configured on each user, that being Call Forward Unconditional (CFU), Call Forward Busy (CFB) and Call Forward No Reply (**CFNR**). As well as **Do Not Disturb** and **Call Waiting**.

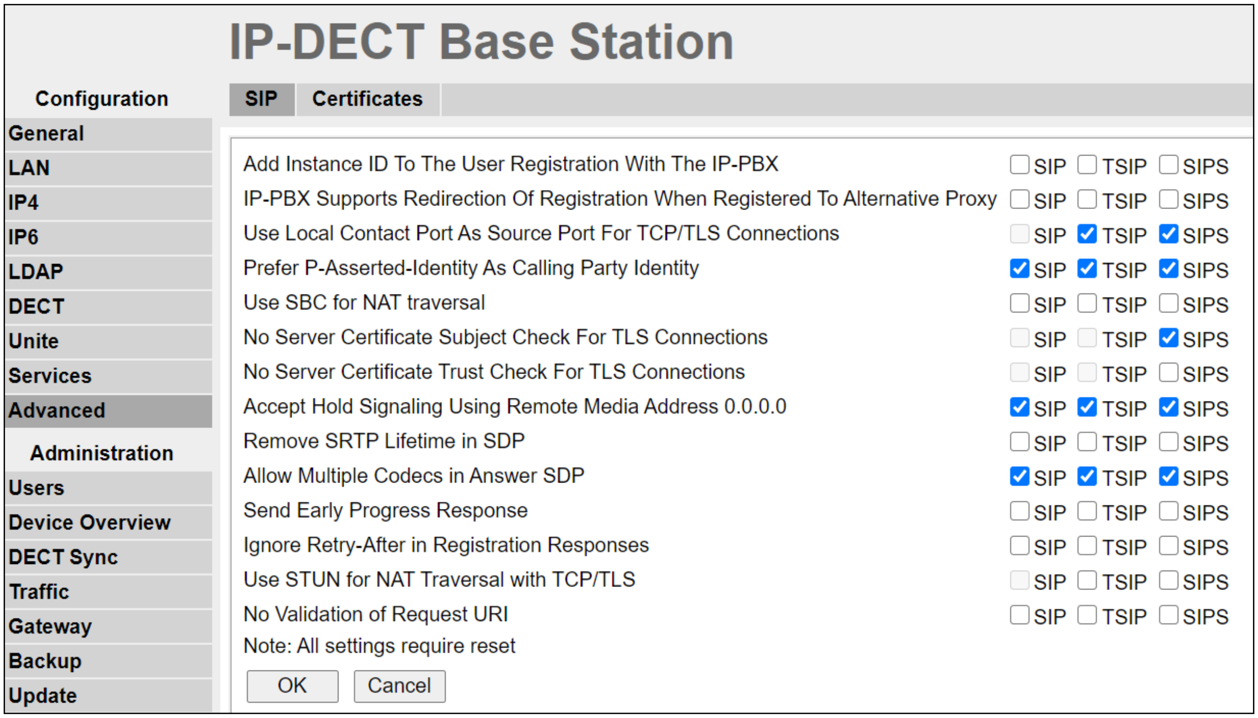
Note: These settings correspond to local features on the IPBS3. It is still recommended that IP Office should be responsible for the diversion.

Similar to **Section 5.3**, it is recommended that "Call Waiting" on IP Office and IP-DECT is turned off. There is a scenario with DECT and semi-attended transfers where the "transfer target" and "initial caller" DECT handsets hang up whilst a second party is ringing to the "transferor" during transfer. If a call is made to the "transferor" DECT handset with Call Waiting enabled the handset accepts the call but the ringing call is cancelled. This behaviour is seen using a single R<extn> method to transfer calls. When Call waiting is off, on the IP Office (and IP-DECT base station), the call to the transferring handset shows busy until the transferred call is answered. When the RR<extn> method is used for transferring, a call can be placed to the transferring handset as this method completes the transfer on hang up. This is as per design.



6.1.6. Advanced settings

These settings were used for compliance testing but can be adjusted to suit each site as required. Please refer to Ascom documentation in **Section 9** for further information.



6.2. Configure Ascom IP DECT handsets

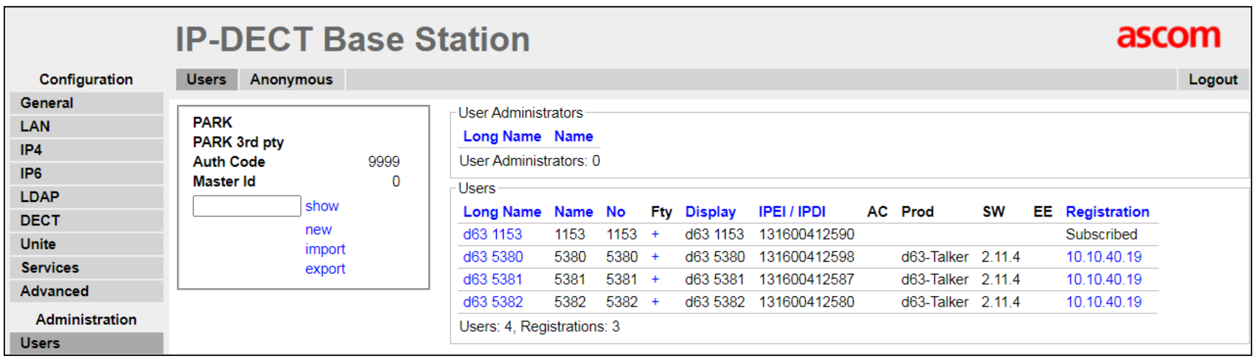
Refer to the Ascom documentation in **Section 9** to obtain information on the procedures for subscribing and registering the Ascom wireless DECT handsets to the Ascom IP-DECT base station.

7. Verification Steps

This section provides the tests that can be performed to verify correct configuration of the IP Office and Ascom solution.

7.1. Ascom DECT Handset Registration Verification

From a web browser, open a connection to the Ascom IP-DECT Master base station (see **Section 6.1**). Navigate to the **Users** and click on the **Users** tab followed by the **show** link. A **Registration** state of “Unsubscribed” (not shown) indicates an Ascom DECT handset has not registered to the Ascom IP-DECT base station. A **Registration** state of “Subscribed” indicates that an Ascom DECT handset has connected to the Ascom IP-DECT base station and requested the use of that particular extension. A **Registration** state that displays the IP Address of the IP Office indicates the extension has successfully registered to both the Ascom IP-DECT base station and IP Office. The screen shot shows three DECT handsets registered to the IP Office.

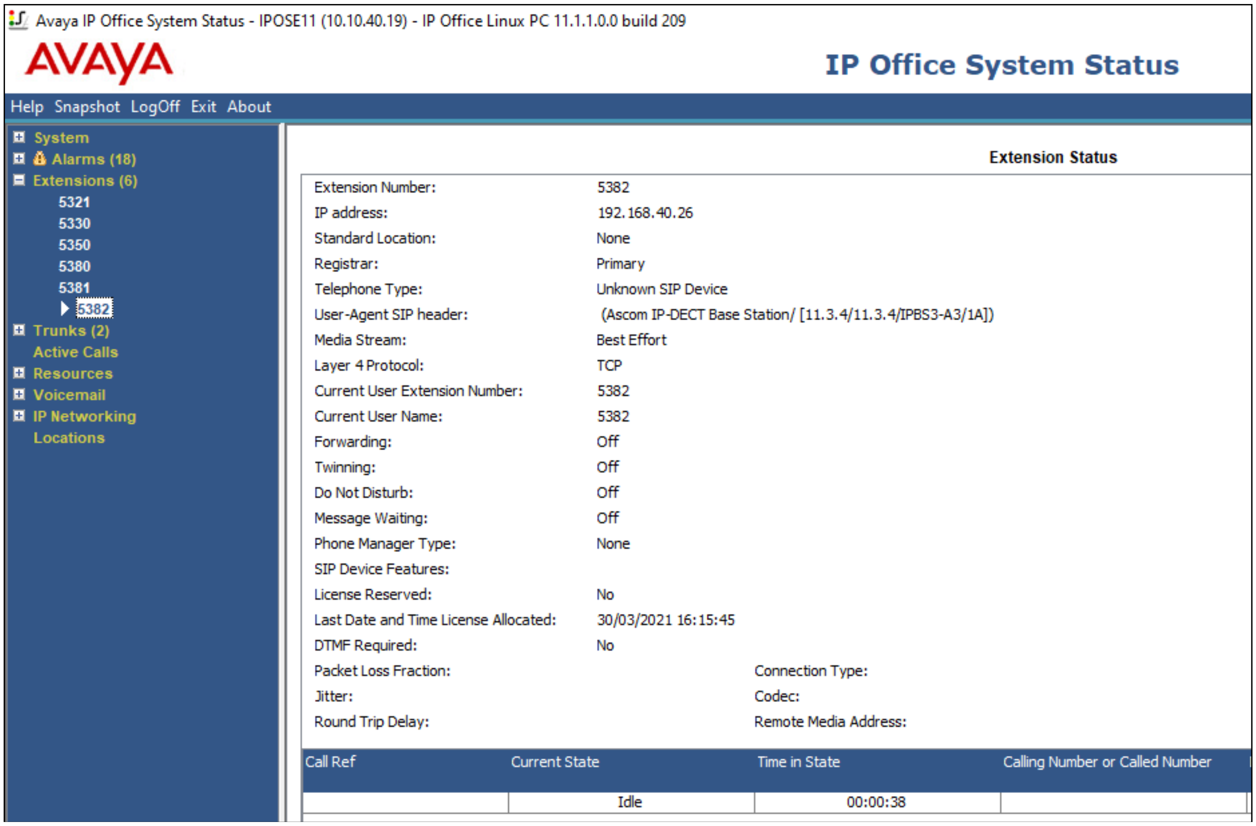


7.2. IP Office Verification

The following can be checked on IP Office System Status. Log into System Status from IP Office → System Status (not shown). This will bring up a monitoring application where various conditions of the IP Office can be examined, such as user registrations and VoIP Security, including if there are any devices that are blacklisted due to a number of incorrect login attempts.

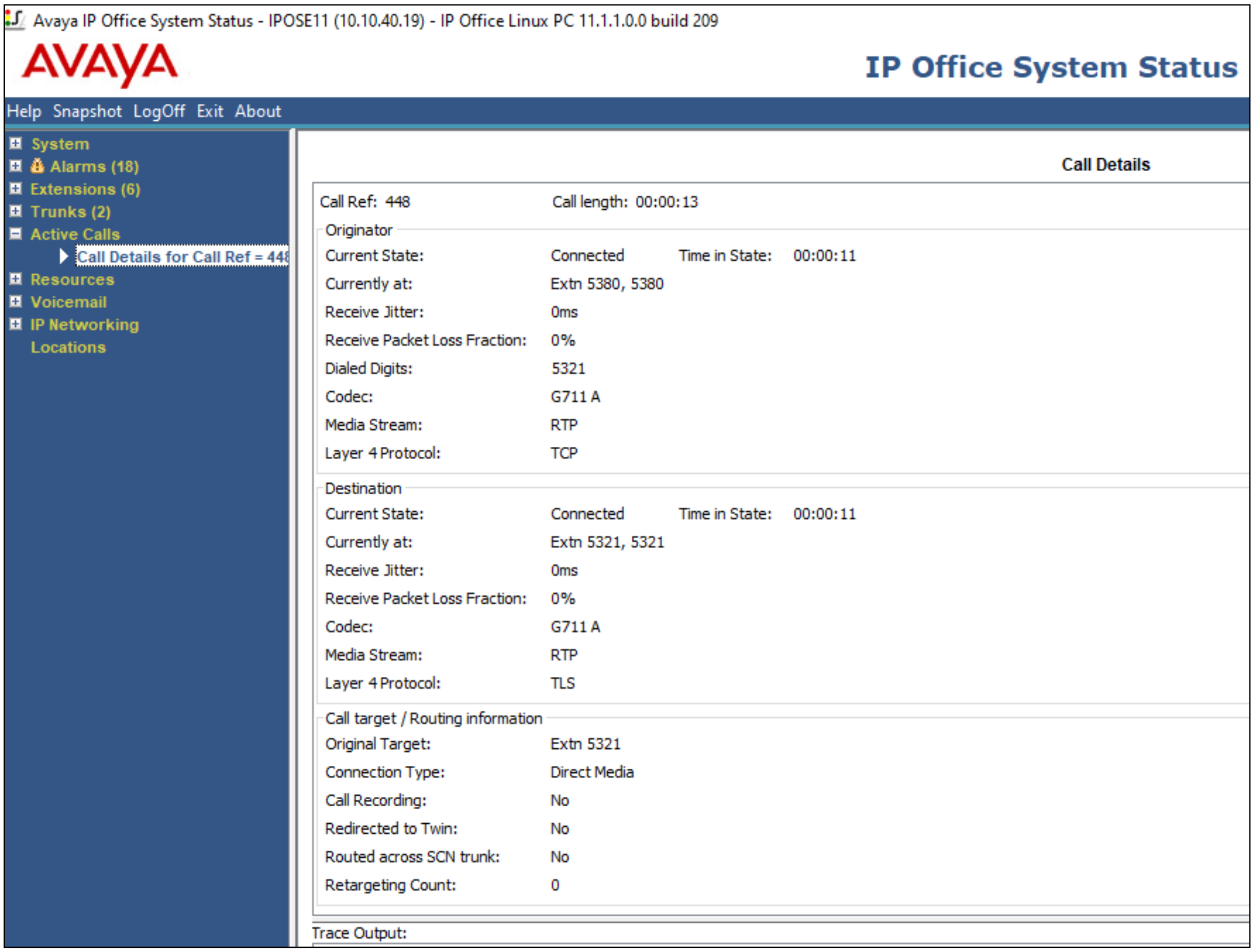
7.2.1. IP Office User Registration Verification

Each IP office extension that is registered will be displayed under **Extensions** in the left window. Clicking on the Ascom extension **5382** shows that it is connected over **TCP** and the **Media Stream** will use **Best Effort** but knowing that Ascom have their extensions set to use RTP that is what will be used for making and receiving calls.



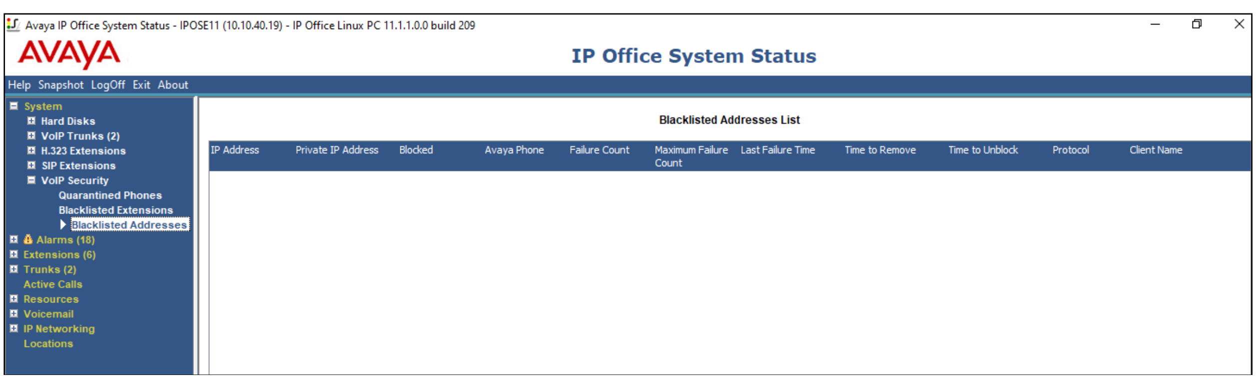
7.2.2. IP Office Call Verification

If a call is made it will show up under Active Calls as shown. The call can then be selected and the details for this call are displayed. This particular call is from the Ascom DECT **5380** to the Avaya SIP extension **5321**. A **Direct Media** connection using **RTP** is established.



7.3. IP Office VoIP Security

This is where any devices that are blacklisted are displayed and they can be manually removed.



8. Conclusion

A full and comprehensive set of feature and functional test cases were performed during compliance testing. The Ascom IP-DECT R11 solution is considered compliant with Avaya IP Office 11.1.1. All observations and issues are 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] *Administering Avaya IP Office™ Platform with Manager*, Release 11.1.1, Issue 29 Feb 2021.

Product documentation for Ascom products can be obtained from Ascom or may be requested at https://www.ascom-ws.com/AscomPartnerWeb/Templates/WebLogin.aspx (login required).

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.