



## **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 not 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

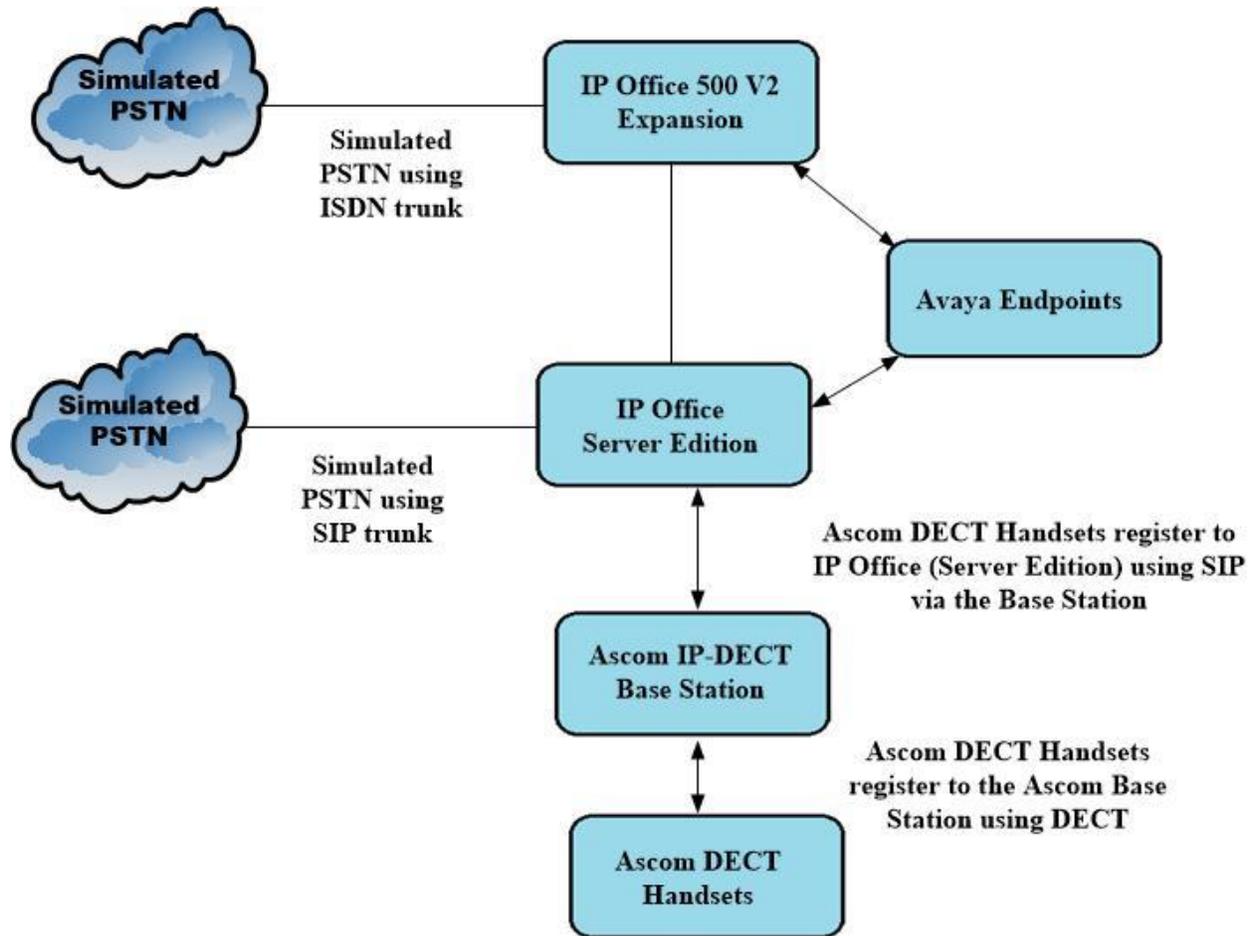
Technical support from Ascom can be obtained through the following:

Phone : +46 31 559450

E-mail : [support@ascom.com](mailto: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:

<b>Equipment/Software</b>	<b>Release/Version</b>
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

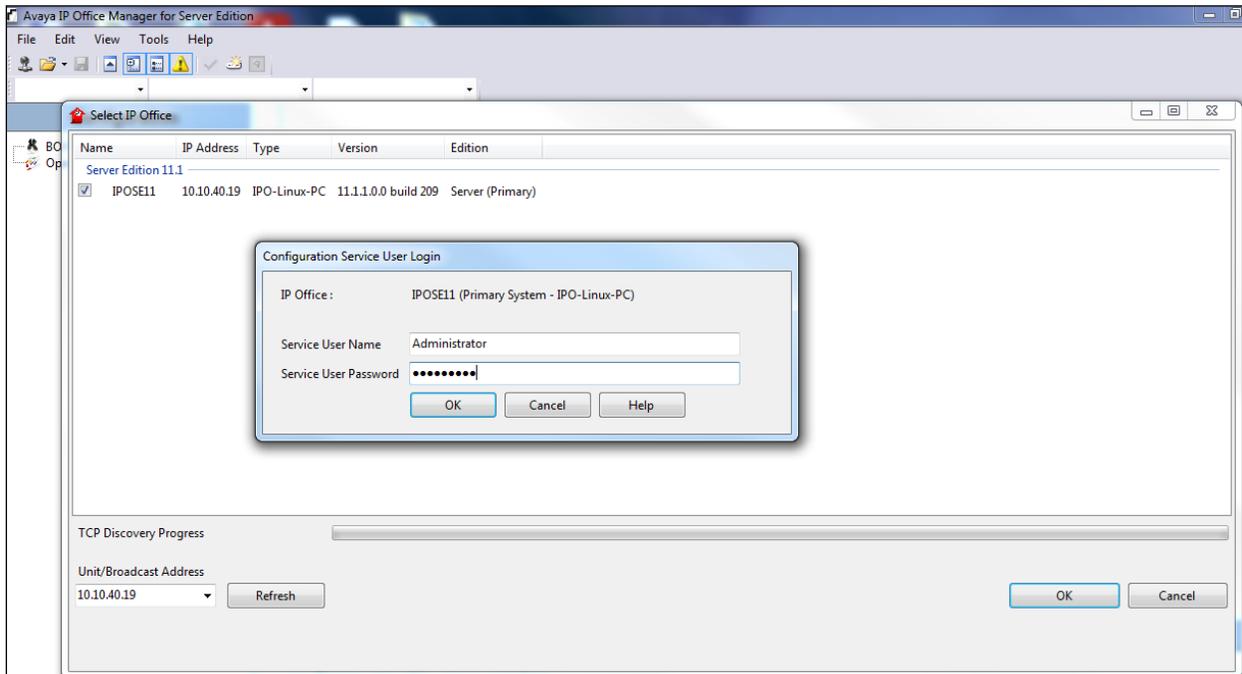
Configuration and verification operations on Avaya IP Office illustrated in this section were all performed using Avaya IP Office Manager. The information provided in this section describes the configuration of Avaya IP Office for this solution. It is implied a working system is already in place. For 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.

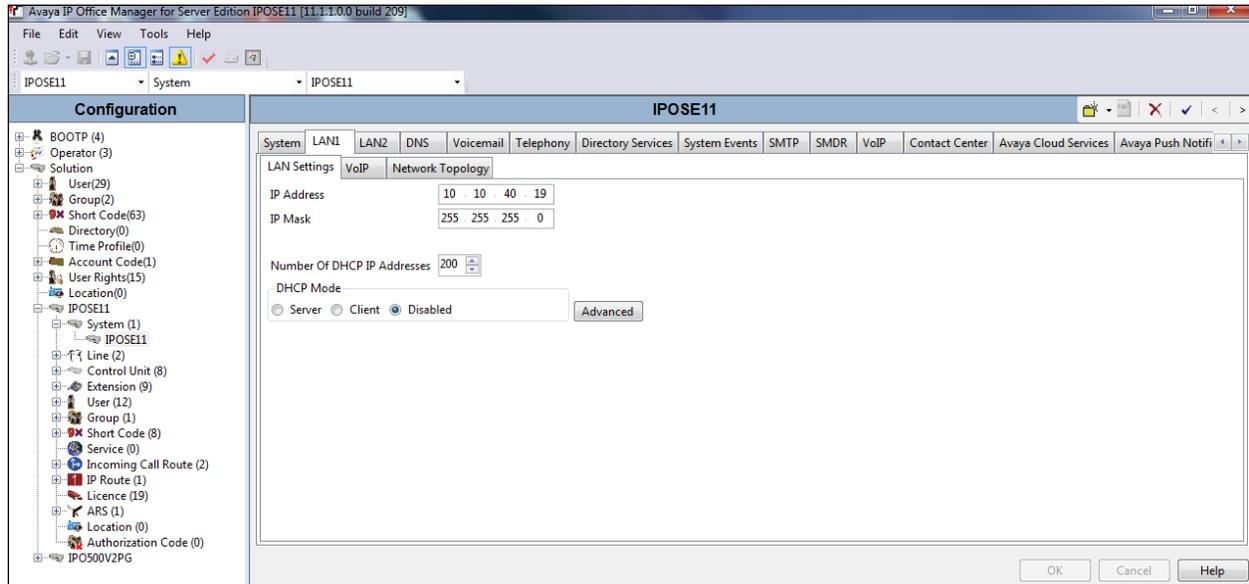
### 5.1. Launch Avaya IP Office Manager (Administration)

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**.



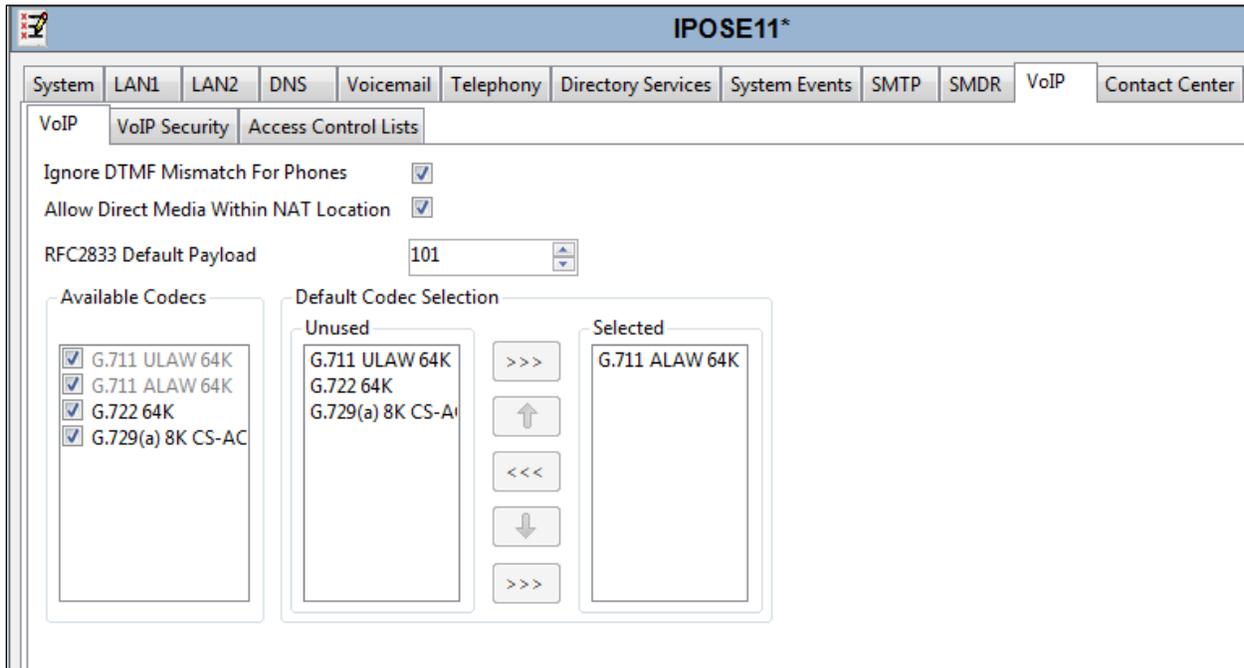
Within the **LAN1** tab, click on the **VoIP** tab. Ensure that **TCP** and **UDP** boxes are checked and that port **5060** is being used. During compliance testing **RTP-RTCP Keepalives** were set to **30** secs (not shown).

The screenshot displays the configuration interface for IPOSE11\*. The top navigation bar includes tabs for System, LAN1, LAN2, DNS, Voicemail, Telephony, Directory Services, System Events, SMTP, SMDR, VoIP, and Contact Center. The 'VoIP' tab is selected, and the 'LAN Settings' sub-tab is active. The configuration is organized into several sections:

- H323 Gatekeeper Enable:** This section is checked. It includes options for 'Auto-create Extn', 'Auto-create User', and 'H323 Remote Extn Enable'. The 'H323 Signalling over TLS' is set to 'Preferred', and the 'Remote Call Signalling Port' is set to 1720.
- SIP Trunks Enable:** This section is checked.
- SIP Registrar Enable:** This section is checked. It includes options for 'Auto-create Extn/User', 'SIP Remote Extn Enable', and 'Allowed SIP User Agents' (set to 'Block blacklist only').
- SIP Domain Name:** Set to 'devconnect.local'.
- SIP Registrar FQDN:** This field is currently empty.
- Layer 4 Protocol:** This section contains three rows of protocol settings:
  - UDP:** Checked. UDP Port is 5060, Remote UDP Port is 5060.
  - TCP:** Checked. TCP Port is 5060, Remote TCP Port is 5060.
  - TLS:** Checked. TLS Port is 5061, Remote TLS Port is 5061.
- Challenge Expiry Time (secs):** Set to 7.

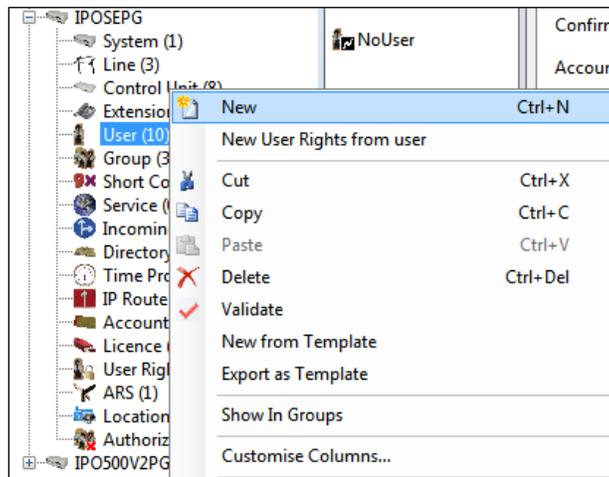
The **RTP** section is also visible, showing a 'Port Number Range' with a 'Minimum' of 40750 and a 'Maximum' of 50750.

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**.

5382: 5382								
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording
Name	<input type="text" value="5382"/>							
Password	<input type="password" value="••••"/>							
Confirm Password	<input type="password" value="••••"/>							
Unique Identity	<input type="text"/>							
Audio Conference PIN	<input type="text"/>							
Confirm Audio Conference PIN	<input type="text"/>							
Account Status	Enabled ▼							
Full Name	Ascom 5382							
Extension	<input type="text" value="5382"/>							
Email Address	<input type="text"/>							
Locale	▼							
Priority	5 ▼							
System Phone Rights	None ▼							
Profile	Basic User ▼							
	<input type="checkbox"/> Receptionist							
	<input type="checkbox"/> Enable Softphone							
	<input type="checkbox"/> Enable one-X Portal Services							
	<input type="checkbox"/> Enable one-X TeleCommuter							
	<input type="checkbox"/> Enable Remote Worker							

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

The screenshot displays the configuration interface for extension 5382: 5382. The 'Voicemail' tab is selected, showing the following settings:

- Voicemail Code:** Four dots (••••)
- Confirm Voicemail Code:** Four dots (••••)
- Voicemail Email:** Empty text field
- Voicemail On:**
- Voicemail Help:**
- Voicemail Ringback:**
- Voicemail Email Reading:**
- UMS Web Services:**
- Enable GMAIL API:**

Below these settings, there are two expandable sections:

- Voicemail Email:** Radio buttons for Off (selected), Copy, Forward, and Alert.
- DTMF Breakout:** Three dropdown menus, all set to 'System Default ()':
  - Reception / Breakout (DTMF 0)
  - Breakout (DTMF 2)
  - Breakout (DTMF 3)

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.

5382: 5382									
User	Voicemail	DND	ShortCodes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Call Settings		Supervisor Settings	Multi-line Options	Call Log	TUI				
Outside Call Sequence	Default Ring	<input type="checkbox"/>	Call Waiting On						
Inside Call Sequence	Default Ring	<input checked="" type="checkbox"/>	Answer Call Waiting On Hold						
Ringback Sequence	Default Ring	<input type="checkbox"/>	Busy On Held						
No Answer Time (secs)	System Default (15)	<input type="checkbox"/>	Offhook Station						
Wrap-up Time (secs)	2								
Transfer Return Time (secs)	Off								
Call Cost Mark-Up	100								
Advertise Callee State To Internal Callers	System Default (Off)								

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.

The screenshot displays the configuration interface for a SIP extension. The left sidebar shows a hierarchical tree of system components, with the 'Extension (9)' category expanded to show a list of extensions, including 11203 5382. The main configuration area is titled 'SIP Extension: 11203 5382' and has two tabs: 'Extn' and 'VoIP'. The 'VoIP' tab is active, showing the following settings:

- IP Address: 0 . 0 . 0 . 0
- Codec Selection: System Default
- Codec Selection List:
  - Unused: G.711 ULAW 64K, G.722 64K, G.729(a) 8K CS-ACELP
  - Selected: G.711 ALAW 64K
- Reserve Licence: None
- Fax Transport Support: None
- DTMF Support: RFC2833/RFC4733
- 3rd Party Auto Answer: None
- Media Security: Same as System (Preferred)
- Advanced Media Security Options:  Same As System

On the right side of the configuration area, there are several checkboxes:

- Requires DTMF
- Local Hold Music
- Re-invite Supported
- Codec Lockdown
- Allow Direct Media Path

## 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 **""**.

**\*66: Voicemail Collect**

Short Code

Code: \*66  
*\* This Short Code is common to all systems.*

Feature: Voicemail Collect

Telephone Number: ""

Line Group ID: 0

Locale: [Empty]

Force Account Code:

Force Authorization Code:

## 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.

Avaya IP Office Manager for Server Edition IPOSE11 [11.1.1.0.0 build 209]

File Edit View Tools Help

Solution: \*66

**\*66: Voicemail Collect**

Send Multiple Configurations

Select	IP Office	Change Mode	RebootTime	Incoming Call Barring	Outgoing Call Barring	Error Status	Progress
<input checked="" type="checkbox"/>	IPOSE11	Merge	16:05	<input type="checkbox"/>	<input type="checkbox"/>		0%
<input checked="" type="checkbox"/>	IPOS00V2PG	Merge	16:05	<input type="checkbox"/>	<input type="checkbox"/>		0%

OK Cancel Help

## 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.

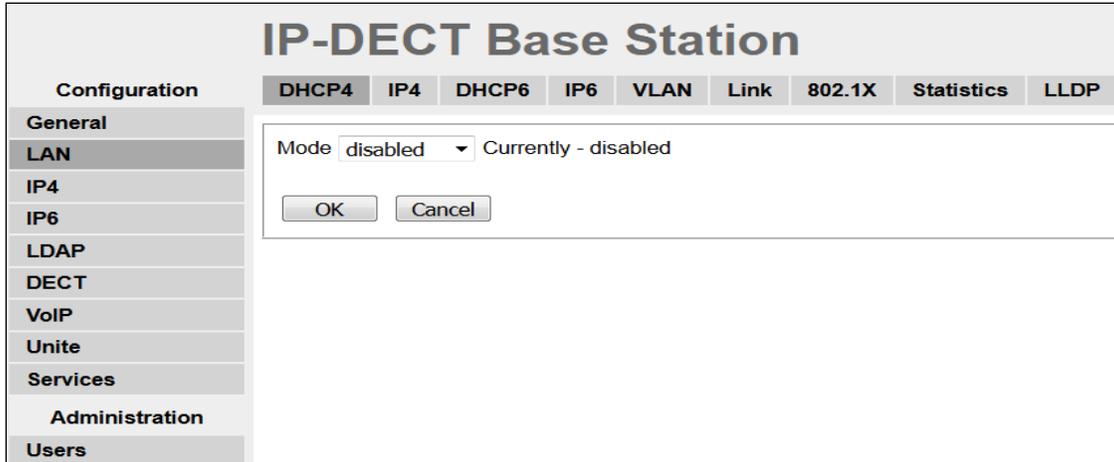
### 6.1. Configure the IP-DECT Base Station

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.



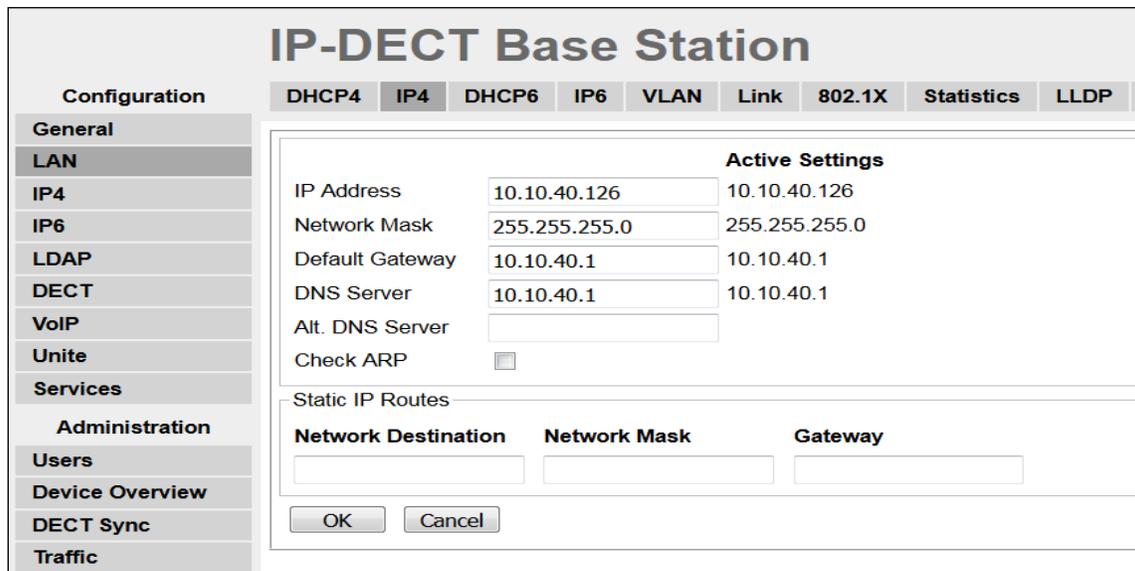
The screenshot shows the 'IP-DECT Base Station' configuration interface. The 'DHCP4' tab is selected. The 'Mode' dropdown is set to 'disabled', and the status is 'Currently - disabled'. There are 'OK' and 'Cancel' buttons at the bottom of the configuration area.

### 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.



The screenshot shows the 'IP-DECT Base Station' configuration interface with the 'IP4' tab selected. The 'Active Settings' section includes:

Field	Value	Active Settings
IP Address	10.10.40.126	10.10.40.126
Network Mask	255.255.255.0	255.255.255.0
Default Gateway	10.10.40.1	10.10.40.1
DNS Server	10.10.40.1	10.10.40.1
Alt. DNS Server		
Check ARP	<input type="checkbox"/>	

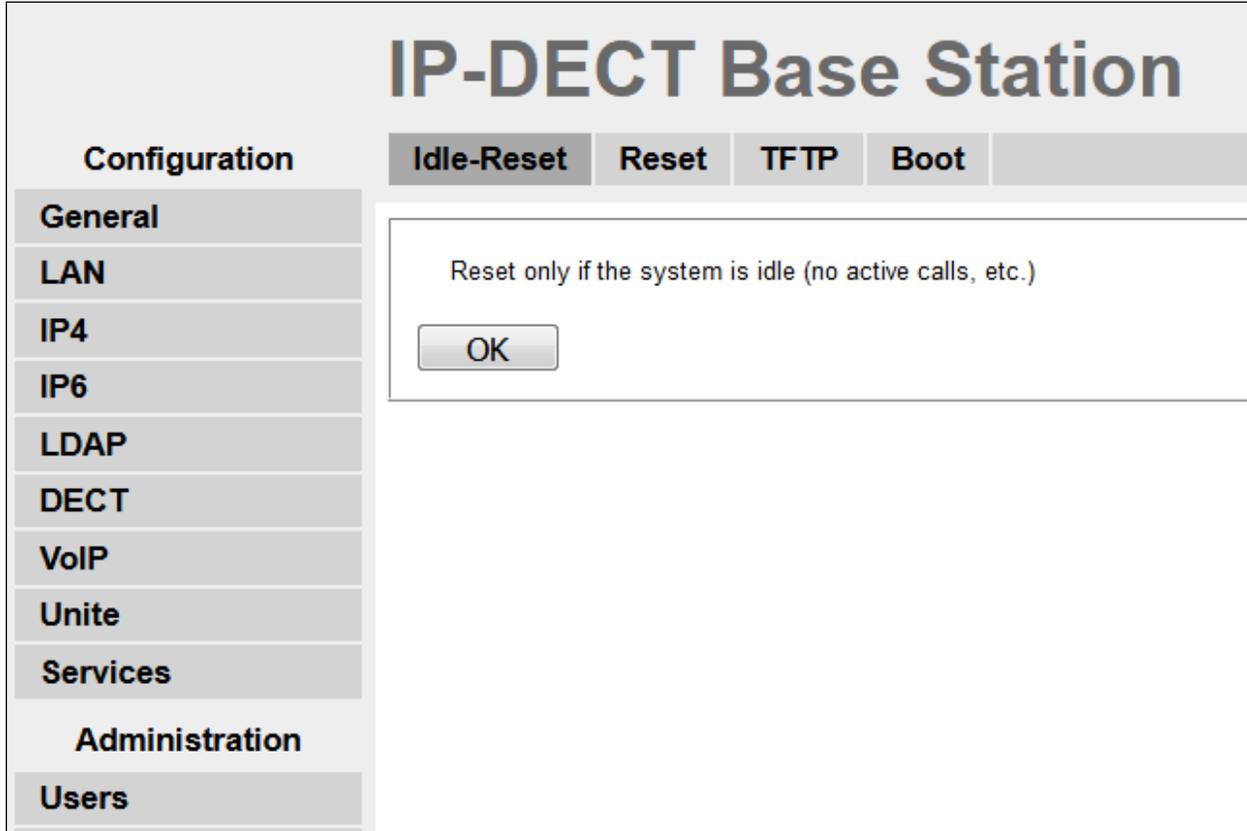
Below the active settings is a 'Static IP Routes' section with a table:

Network Destination	Network Mask	Gateway
<input type="text"/>	<input type="text"/>	<input type="text"/>

'OK' and 'Cancel' buttons are at the bottom.

### 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.



The screenshot displays the configuration interface for an IP-DECT Base Station. The main title is "IP-DECT Base Station". On the left, there is a "Configuration" menu with the following items: General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, and Users. The "Idle-Reset" tab is selected in the top navigation bar, along with "Reset", "TFTP", and "Boot". The main content area shows a dialog box with the text "Reset only if the system is idle (no active calls, etc.)" and an "OK" button.

## 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.

The screenshot displays the 'IP-DECT Base Station' configuration window. The 'Master' tab is selected, showing the following settings:

- Mode:** Active (dropdown)
- Multi-Master:**
  - Master ID: 0
  - Enable PARI Function:
  - Region Code: (empty)
- IP-PBX:**
  - Protocol: SIP/TCP (dropdown)
  - Proxy: 10.10.40.19
  - Alt. Proxy: (empty)
  - Alt. Proxy: (empty)
  - Alt. Proxy: (empty)
  - Domain: (empty)
  - Max. Internal Number Length: 4
  - International CPN Prefix: (empty)
  - Registration with system password:
  - Enbloc Dialing:
  - Enable Enbloc Send-Key:
  - Allow DTMF Through RTP:
  - Short Disconnect Tone:
  - Treat rejected calls as: Busy (dropdown)
  - Configured With Local GK:
- SIP Interoperability Settings:** (collapsed)

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

### IP-DECT Base Station

System   Suppl. Serv.   **Master**   Crypto Master   Mobility Master   Radio   Radio config   PARI   SARI   Air Sync

Interoperability Settings

Registration Time-To-Live	<input type="text" value="180"/> [sec]
STUN server	<input type="text"/>
Hold Signalling	<input type="text" value="inactive"/>
Hold Before Transfer	<input type="checkbox"/>
Accept Inbound Calls Not Routed Via Home Proxy	<input type="checkbox"/>
Register With Number	<input checked="" type="checkbox"/>
AOR as Line Identity	<input type="checkbox"/>
KPML support	<input type="checkbox"/>

Registration For Anonymous Devices

Registration Name / Number	<input type="text"/>	/	<input type="text"/>
Deactivate Master If No Connection	<input type="checkbox"/>		

Conferencing Unit

Conferencing Unit Number	<input type="text"/>
--------------------------	----------------------

Mobility Master

Name	<input type="text"/>
Password	<input type="text"/>
IP Address	<input type="text"/>
Alt. IP Address	<input type="text"/>
Status	

### 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.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'System' tab is selected. The left sidebar contains a navigation menu with categories like 'General', 'Administration', 'Users', and 'Diagnostics'. The main area displays the following configuration fields:

Configuration	System	Suppl. Serv.	Master	Crypto Master	Mobility Master	Radio	Radio config
General	System Name						
LAN	Password						
IP4	Confirm Password						
IP6	Subscriptions						
LDAP	Authentication Code						
DECT	Tones						
Unite	Default Language						
Services	Frequency						
Advanced	Enabled Carriers						
Administration	Local R-Key Handling						
Users	No Transfer on Hangup						
Device Overview	No On-Hold Display						
DECT Sync	Display Original Called						
Traffic	Early Encryption						
Gateway	RFP Location						
Backup	Unite Data Channel						
Update	Disable ICE						
Diagnostics	Coder						
Reset	Secure RTP Key Exchange						
	Unencrypted SRTCP						

At the bottom of the configuration area, there are 'OK' and 'Cancel' buttons.

### 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.

The screenshot shows the 'IP-DECT Base Station' configuration window. The 'Suppl. Serv.' tab is selected. The 'Enable Supplementary Services' checkbox is checked. Below this, a table lists various services with 'Activate', 'Deactivate', and 'Disable' columns. The 'MWI Mode' is set to 'User dependent interrogate number' and 'MWI Notify Number' is set to '\*66'. 'OK' and 'Cancel' buttons are at the bottom.

	Activate	Deactivate	Disable
Call Forwarding Unconditional	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Forwarding Busy	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Forwarding No Reply	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Do Not Disturb	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Waiting	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Completion	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Park	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Interception	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
Call Service URI	<input type="text"/>		<input checked="" type="checkbox"/>
Call Service URI (Argument)	<input type="text"/>		<input checked="" type="checkbox"/>
Soft key	<input type="text"/>		<input checked="" type="checkbox"/>
Logout User	<input type="text"/>		<input checked="" type="checkbox"/>
Clear Local Setting	<input type="text"/>		<input checked="" type="checkbox"/>
MWI Mode	User dependent interrogate number		
MWI Notify Number	*66		
Local Clear of MWI	<input type="text"/>		
External Idle Display			<input checked="" type="checkbox"/>

#### 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.

The screenshot shows the 'IP-DECT Base Station' configuration interface. The 'PARI' tab is selected. In the 'System ID' field, the number '4' is entered. Below the field are 'OK' and 'Cancel' buttons. The left sidebar shows a 'Configuration' menu with options: General, LAN, IP4, IP6, LDAP, DECT, and VoIP.

#### 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.

The screenshot shows the 'IP-DECT Base Station' configuration interface with the 'SARI' tab selected. The 'SARI' field contains the masked text 'XXXXXXXXXXXXXXXX'. Below the field are 'OK' and 'Cancel' buttons. The left sidebar shows a 'Configuration' menu with options: General, LAN, IP4, IP6, LDAP, DECT, and VoIP.

#### 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.

The screenshot shows the 'IP-DECT Base Station' configuration interface with the 'Air Sync' tab selected. The 'Sync Mode' dropdown is set to 'Master'. The 'Action at reference sync failure' section has three radio button options: 'Resynchronize on command' (which is selected), 'Resynchronize every day at 00:00', and 'Resynchronize every Sunday at 00:00'. Below the options are 'OK' and 'Cancel' buttons. The left sidebar shows a 'Configuration' menu with options: General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services, Administration, and Users.

### 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.

The screenshot displays the 'IP-DECT Base Station' configuration interface. On the left is a navigation menu with categories: Configuration (General, LAN, IP4, IP6, LDAP, DECT, VoIP, Unite, Services) and Administration (Users, Device Overview). The 'Users' tab is selected. The main content area shows 'PARK' and 'PARK 3rd pty' fields with greyed-out values, and a 'Master Id' field with the value '0'. Below these fields are links for 'show', 'new', 'import', and 'export'.

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 screenshot shows a web browser window titled "Edit User - Mozilla Firefox". The address bar shows the URL "10.10.40.126/GW-DECT/mod\_cmd\_login.xml?cmd=show&user-guid". The form contains the following fields and controls:

- User type**: Radio buttons for "User" (selected) and "User Administrator".
- Long Name**: Text input field containing "d63 5182".
- Display Name**: Text input field containing "d63 5182".
- Name**: Text input field containing "5182".
- Number**: Text input field containing "5182".
- Auth. Name**: Text input field (SIP only).
- Password**: Password input field (masked with dots).
- Confirm Password**: Password input field (masked with dots).
- IPEI / IPDI**: Text input field containing "110550389613".
- Idle Display**: Text input field containing "d63 5182".
- Auth. Code**: Text input field.
- Feature Status**: Text input field.

At the bottom of the form are five buttons: "OK", "Apply", "Delete", "Unsubs.", and "Cancel".

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.

The screenshot shows the IP-DECT Base Station web interface. The main header is "IP-DECT Base Station" with the "ascom" logo on the right. Below the header are tabs for "Users" and "Anonymous", and a "Logout" link. The "Users" tab is active, showing a list of users. On the left, there is a sidebar for the selected user "PARK" with fields for "PARK 3rd party", "Auth Code" (9999), and "Master Id" (0). A "show" button is highlighted in red. The main content area shows a table of users with columns "Long Name", "Name", "No", "Fty", and "Display". The user "d63 5382" is highlighted in red. A dialog box is open over the table, titled "https://192.168.40.26/session/GW-DEC...", with a "Not secure" warning. The dialog box contains fields for "CFU", "CFB", and "CFNR", and checkboxes for "Do not Disturb Int.", "Do not Disturb Ext.", and "Call Waiting". "OK" and "Cancel" buttons are at the bottom.

Long Name	Name	No	Fty	Display
d63 1153	1153	1153	+	d63 1153
d63 5380	5380	5380	+	d63 5380
d63 5381	5381	5381	+	d63 5381
d63 5382	5382	5382	+	d63 5382

### 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.

IP-DECT Base Station	
Configuration	SIP Certificates
<b>General</b>	
<b>LAN</b>	Add Instance ID To The User Registration With The IP-PBX <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>IP4</b>	IP-PBX Supports Redirection Of Registration When Registered To Alternative Proxy <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>IP6</b>	Use Local Contact Port As Source Port For TCP/TLS Connections <input type="checkbox"/> SIP <input checked="" type="checkbox"/> TSIP <input checked="" type="checkbox"/> SIPS
<b>LDAP</b>	Prefer P-Asserted-Identity As Calling Party Identity <input checked="" type="checkbox"/> SIP <input checked="" type="checkbox"/> TSIP <input checked="" type="checkbox"/> SIPS
<b>DECT</b>	Use SBC for NAT traversal <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Unite</b>	No Server Certificate Subject Check For TLS Connections <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input checked="" type="checkbox"/> SIPS
<b>Services</b>	No Server Certificate Trust Check For TLS Connections <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Advanced</b>	Accept Hold Signaling Using Remote Media Address 0.0.0.0 <input checked="" type="checkbox"/> SIP <input checked="" type="checkbox"/> TSIP <input checked="" type="checkbox"/> SIPS
<b>Administration</b>	Remove SRTP Lifetime in SDP <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Users</b>	Allow Multiple Codecs in Answer SDP <input checked="" type="checkbox"/> SIP <input checked="" type="checkbox"/> TSIP <input checked="" type="checkbox"/> SIPS
<b>Device Overview</b>	Send Early Progress Response <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>DECT Sync</b>	Ignore Retry-After in Registration Responses <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Traffic</b>	Use STUN for NAT Traversal with TCP/TLS <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Gateway</b>	No Validation of Request URI <input type="checkbox"/> SIP <input type="checkbox"/> TSIP <input type="checkbox"/> SIPS
<b>Backup</b>	Note: All settings require reset
<b>Update</b>	<input type="button" value="OK"/> <input type="button" value="Cancel"/>

### 6.2. Configure Ascom IP DECT handsets

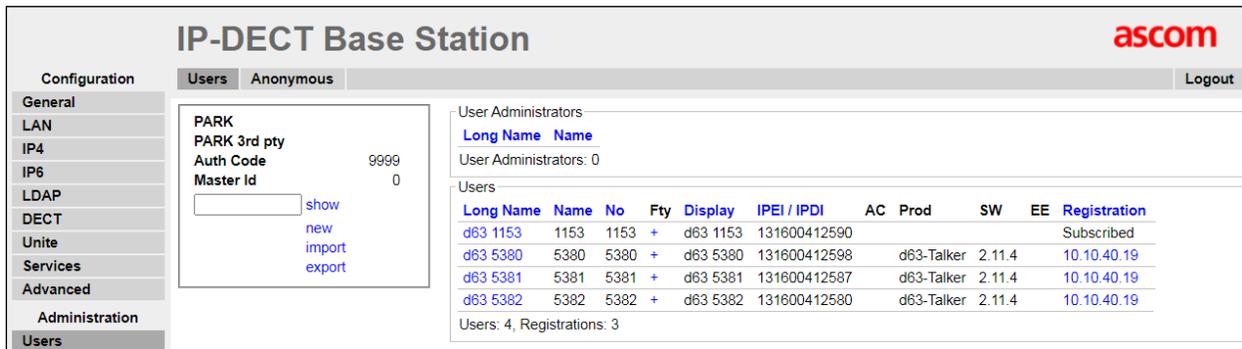
Refer to the Ascom documentation in **Section 9** to obtain information on the procedures for subscribing and registering the Ascom wireless DECT handsets to the Ascom IP-DECT base station.

## 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.



The screenshot displays the 'IP-DECT Base Station' configuration interface. The 'Users' tab is selected, showing configuration details for a user named 'PARK'. The 'Auth Code' is 9999 and the 'Master Id' is 0. Below these fields are links for 'show', 'new', 'import', and 'export'. To the right, there is a section for 'User Administrators' showing 0 administrators. Below that is a table of registered users.

Long Name	Name	No	Fty	Display	IPEI / IPDI	AC	Prod	SW	EE	Registration
d63 1153	1153	1153	+	d63 1153	131600412590					Subscribed
d63 5380	5380	5380	+	d63 5380	131600412598	d63-Talker	2.11.4			10.10.40.19
d63 5381	5381	5381	+	d63 5381	131600412587	d63-Talker	2.11.4			10.10.40.19
d63 5382	5382	5382	+	d63 5382	131600412580	d63-Talker	2.11.4			10.10.40.19

Users: 4, Registrations: 3

### 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.

Avaya IP Office System Status - IPOSE11 (10.10.40.19) - IP Office Linux PC 11.1.1.0.0 build 209

**AVAYA** **IP Office System Status**

Help Snapshot LogOff Exit About

- System
- Alarms (18)
- Extensions (6)
  - 5321
  - 5330
  - 5350
  - 5380
  - 5381
  - 5382
- Trunks (2)
- Active Calls
- Resources
- Voicemail
- IP Networking
  - Locations

### Extension Status

Extension Number:	5382		
IP address:	192.168.40.26		
Standard Location:	None		
Registrar:	Primary		
Telephone Type:	Unknown SIP Device		
User-Agent SIP header:	(Ascom IP-DECT Base Station/ [11.3.4/11.3.4/IPBS3-A3/1A])		
Media Stream:	Best Effort		
Layer 4 Protocol:	TCP		
Current User Extension Number:	5382		
Current User Name:	5382		
Forwarding:	Off		
Twinning:	Off		
Do Not Disturb:	Off		
Message Waiting:	Off		
Phone Manager Type:	None		
SIP Device Features:			
License Reserved:	No		
Last Date and Time License Allocated:	30/03/2021 16:15:45		
DTMF Required:	No		
Packet Loss Fraction:		Connection Type:	
Jitter:		Codec:	
Round Trip Delay:		Remote Media Address:	

Call Ref	Current State	Time in State	Calling Number or Called Number
	Idle	00:00:38	

## 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.

Avaya IP Office System Status - IPOSE11 (10.10.40.19) - IP Office Linux PC 11.1.1.0.0 build 209

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

- System
- Alarms (18)
- Extensions (6)
- Trunks (2)
- Active Calls
  - Call Details for Call Ref = 448
- Resources
- Voicemail
- IP Networking
  - Locations

### Call Details

Call Ref: 448      Call length: 00:00:13

Originator

Current State: Connected      Time in State: 00:00:11

Currently at: Extn 5380, 5380

Receive Jitter: 0ms

Receive Packet Loss Fraction: 0%

Dialed Digits: 5321

Codec: G711 A

Media Stream: RTP

Layer 4 Protocol: TCP

Destination

Current State: Connected      Time in State: 00:00:11

Currently at: Extn 5321, 5321

Receive Jitter: 0ms

Receive Packet Loss Fraction: 0%

Codec: G711 A

Media Stream: RTP

Layer 4 Protocol: TLS

Call target / Routing information

Original Target: Extn 5321

Connection Type: Direct Media

Call Recording: No

Redirected to Twin: No

Routed across SCN trunk: No

Retargeting Count: 0

Trace Output:

## 7.3. IP Office VoIP Security

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

Avaya IP Office System Status - IPOSE11 (10.10.40.19) - IP Office Linux PC 11.1.1.0.0 build 209

**AVAYA** IP Office System Status

Help Snapshot LogOff Exit About

- System
  - Hard Disks
  - VoIP Trunks (2)
  - H.323 Extensions
  - SIP Extensions
  - VoIP Security
    - Quarantined Phones
    - Blacklisted Extensions
    - Blacklisted Addresses
- Alarms (18)
- Extensions (6)
- Trunks (2)
- Active Calls
- Resources
- Voicemail
- IP Networking
  - Locations

### Blacklisted Addresses List

IP Address	Private IP Address	Blocked	Avaya Phone	Failure Count	Maximum Failure Count	Last Failure Time	Time to Remove	Time to Unblock	Protocol	Client Name

## 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).

---

**©2021 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).