



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

---

# **Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya IP Office Server Edition and IP Office 500 V2 Expansion R10.0 using UDP&TCP/RTP – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for provisioning NEC's IP DECT Access Points and Handsets to interoperate with Avaya IP Office using UDP&TCP/RTP.

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

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

# 1. Introduction

These Application Notes describe the configuration steps for provisioning NEC's IP DECT Access Point (AP400) and NEC's DECT handsets to interoperate with Avaya IP Office Server Edition and IP Office 500 V2 Expansion R10.0 using UDP&TCP/RTP.

An NEC IP DECT solution typically consists of a windows based instance called DAP Controller that runs the IP DECT system software (DAP Configurator and DAP Manager), one or more DECT access points (DAP) AP400, DECT handsets (e.g. G566, I766, G966) and if needed a software based DMLS open interface for messaging and alarming. The DAP's are connected to the IP network and get the needed power by using POE following 802.3af standard. Multiple NEC DECT access points (DAP) are tied together to build a single DECT system. The handsets are enrolled into that System using Digital Enhanced Cordless Technology (DECT). Each DAP is hosting (responsible for) a particular number of handsets although roaming/handover is possible across all DAPs. The DAPs are configured to register with Avaya IP Office using Session Initiation Protocol (SIP). A single DAP will register multiple times against IP Office on behalf of the handsets it is responsible for.

Each handset is configured as a SIP user on IP Office. The NEC DECT handsets behave as SIP integrated into the IP Office. They are able to make/receive internal calls, trunk calls, access the voicemail system and can take advantage of the telephony features provided by IP Office.

## 2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of NEC DECT handsets to make and receive calls to and from Avaya H.323, and SIP deskphones as well as calls via connected trunks. Avaya IP Office Voicemail Pro was used to allow users to leave voicemail messages and to demonstrate Message Waiting Indication (MWI) was working on the NEC handsets.

NEC supports UDP/RTP and TCP/RTP but also TLS/SRTP. For more information on NEC using TLS and SRTP please refer to the Application Notes titled *Application Notes for configuring NEC IP DECT Access Points AP400 and NEC DECT Handsets with Avaya IP Office Server Edition and IP Office 500 V2 Expansion R10.0 using TLS/SRTP*.

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

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya

products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

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

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

## **2.1. Interoperability Compliance Testing**

The following features have been tested. Note that when applicable, all tests were performed between NEC DECT handsets and Avaya SIP deskphones, Avaya H.323 deskphones as well as PSTN endpoints.

- Basic Calls
- Calling Line Number / Name Identification
- Hold and Retrieve
- Attended and Blind Transfer
- Call Forwarding Unconditional, No Reply and Busy
- Feature Code for Call Forward
- Call Waiting
- Call Park/Call Pickup
- Hunt-Group
- Internal Twinning
- Multi Party Conference
- Codec Support (G.711A, G.711U and G.729)
- Trunk-Calls (Simulated PSTN)
- DTMF Support (SIP Info and RFC2833)
- Message Waiting Indication

## **2.2. Test Results**

All test cases passed successfully with the following observations noted during testing.

1. NEC1 → NEC2 → TRN BLIND to AVAYA SE SIP. On some occasions the transfer fails with the call being dropped completely upon completion of the Blind Transfer. Patch 4920b655.dwl applied by NEC fixed this issue.
2. NEC3 → NEC4 → TRN BLIND to AVAYA 500V2 SIP. On some occasions the transfer fails with the call being dropped completely upon completion of the Blind Transfer. Patch 4920b655.dwl applied by NEC fixed this issue.
3. NEC1 → NEC2 → TRN BLIND to PSTN (SIP or QSIG). CLID is not updated on the NEC phone 1 after a blind transfer is complete. This is the initial NEC caller's display.

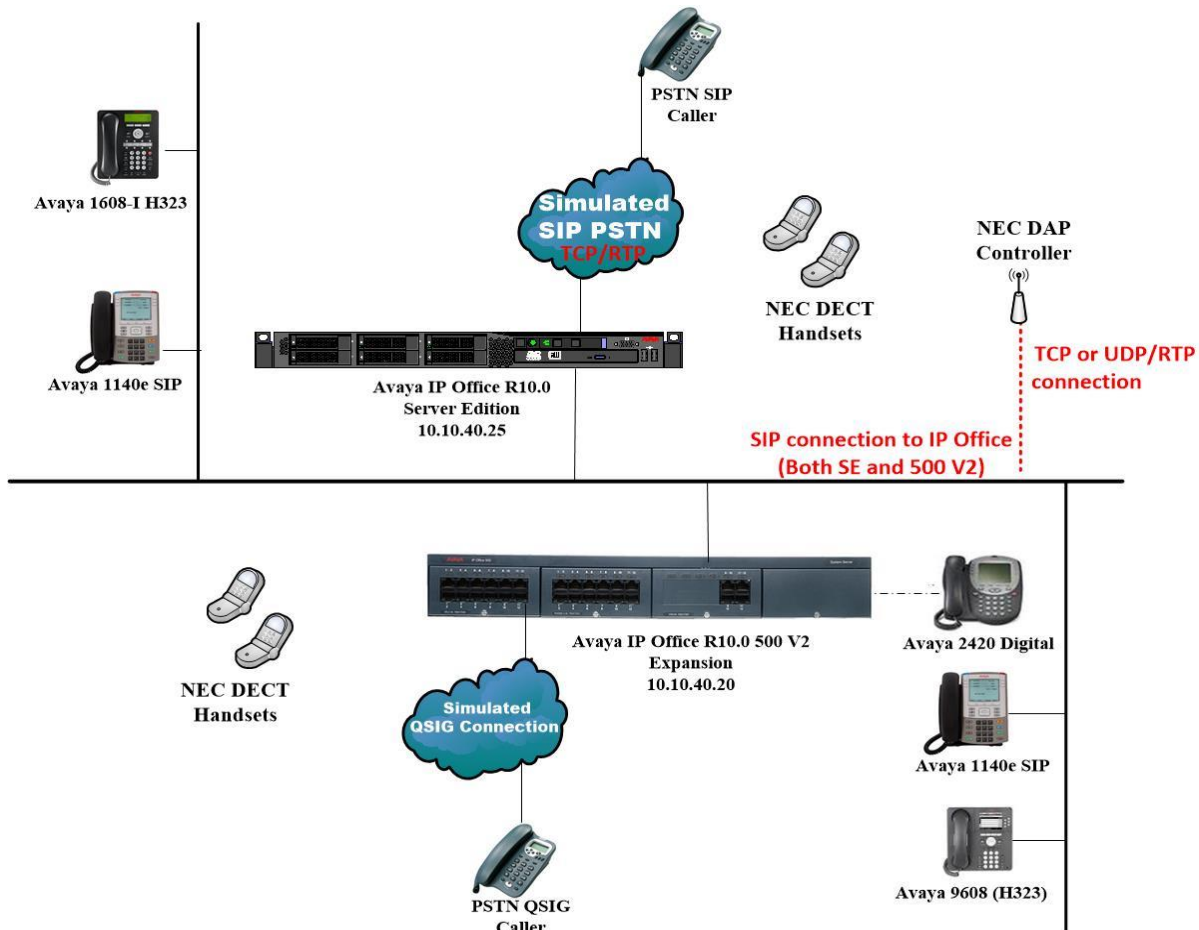
## 2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 9** of these Application Notes. Technical support for the NEC IP DECT product can be obtained through NEC global technical support by accessing the website <http://www.nec-ipdect.com/Contact-7> or <http://businessnet.nec-enterprise.com> (which is available only for partners with authorized access).

## 3. Reference Configuration

**Figure 1** shows the network topology during compliance testing. The NEC DECT handsets subscribe to the NEC DECT Access Points (DAP) which is placed on the LAN. The DECT handsets register with IP Office in order to be able to make/receive calls to and from the Avaya H.323 and SIP deskphones as well as from the trunks (PSTN).

**Note:** Two handsets were registered to the IP Office Server Edition and two with the IP Office 500V2.



**Figure 1: Network Solution of NEC DECT Handsets with Avaya IP Office Server Edition and 500 V2 R10.0**

## 4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Release/Version
Avaya IP Office Server Edition running on a Virtual Platform	R10.0.2.0 Build 10
Avaya IP Office 500 V2	R10.0.2.0 Build 10
Avaya IP Office Manager running on a Windows 7 PC	R10.0.2.0 Build 10
Avaya 1608-I H323 Deskphone	1608UA1_350B.bin
Avaya 9630 H323 Deskphone	R6.4014U
Avaya 1140e SIP Deskphone	R04.04.28.00
Avaya 2420 Digital Deskphone	V5.0
Avaya Communicator for Windows	2.1.3.80
DAP Controller software running on Windows 2012 virtual server	Release of R6.41 6.41.0624
NEC DECT Access Point	Release of R6.41 6.41.0624 Patch is Release 6.41 : 4920b655.dwl
NEC DECT Handset NEC G566 NEC DECT Handset NEC I766	1.14.00.01 1.14.00.01

## 5. Configure Avaya IP Office

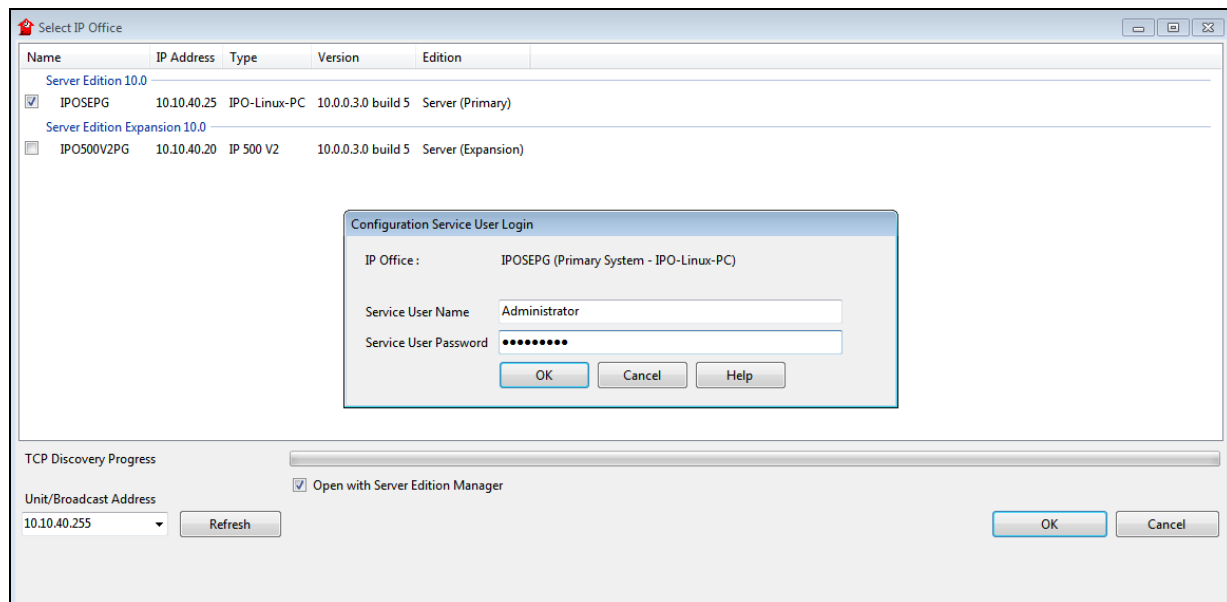
The information provided in this section describes the configuration of Avaya IP Office for this solution. Configuration and verification operations on the Avaya IP Office were all performed using Avaya IP Office Manager. It is implied a working system is already in place with the necessary licensing. 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 (Administration).
- Display LAN Properties.
- Create User.
- Save Configuration.

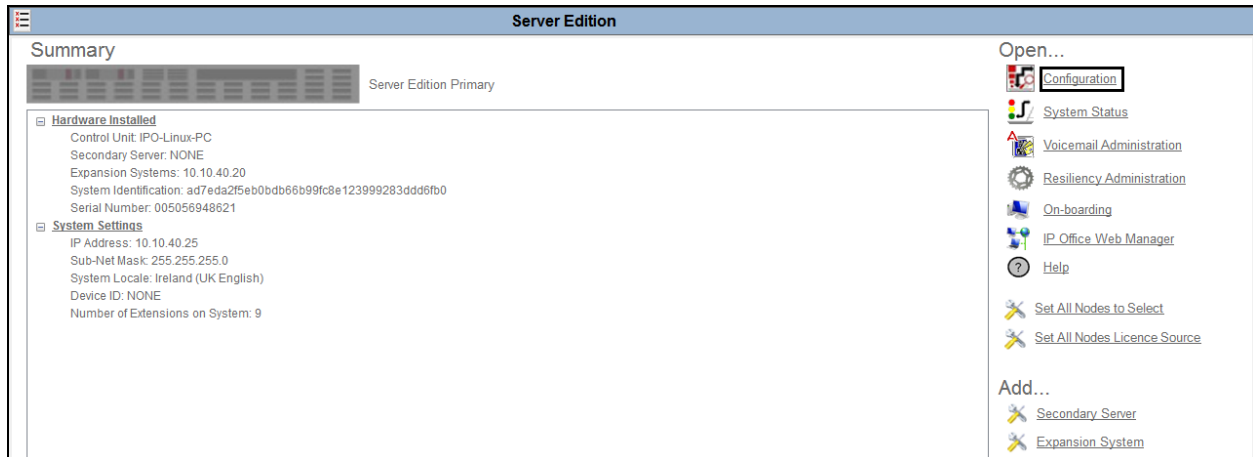
**Note:** Only the unique prompts are shown in the screen captures below, all other inputs can be left at default.

### 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). Tick on the Server Edition as shown below and enter the appropriate credentials. Click on the **OK** button..

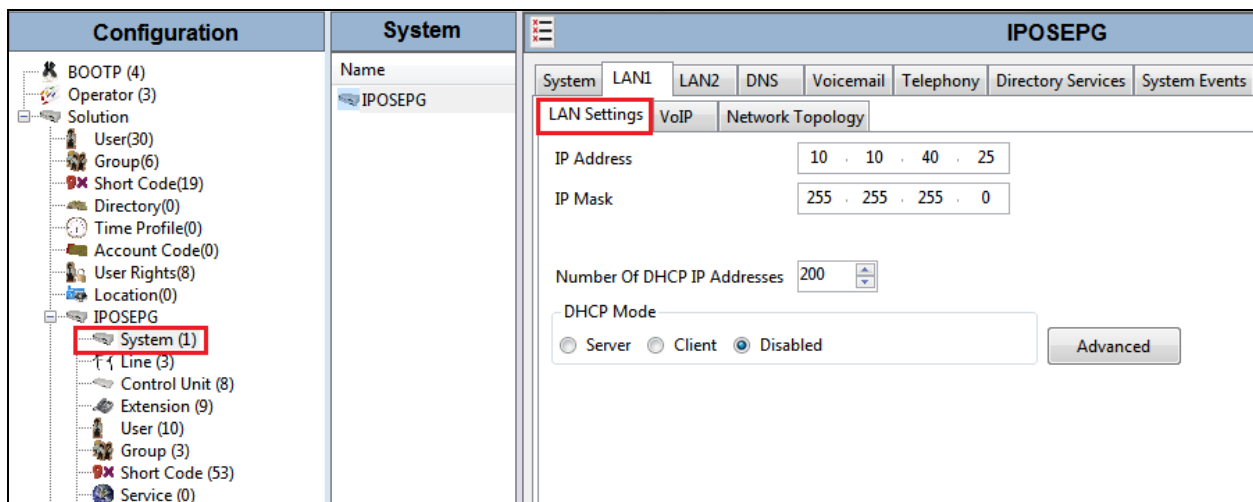


Click on **Configuration** at the top right of the page, as shown, to receive the IP Office configuration.



## 5.2. Display LAN Properties

From the left window navigate to **System** as shown and in the main window click on the **LAN1** tab and within that tab select the **LAN Settings** tab. The **IP Address** of the IP Office is shown and this will be required setup in **Section 6.1**.



Click on the **VoIP** tab. Ensure that **TCP** and **UDP** are ticked and that port **5060** is being used. During compliance testing **RTP-RTCP Keepalives** were set to **30secs**.

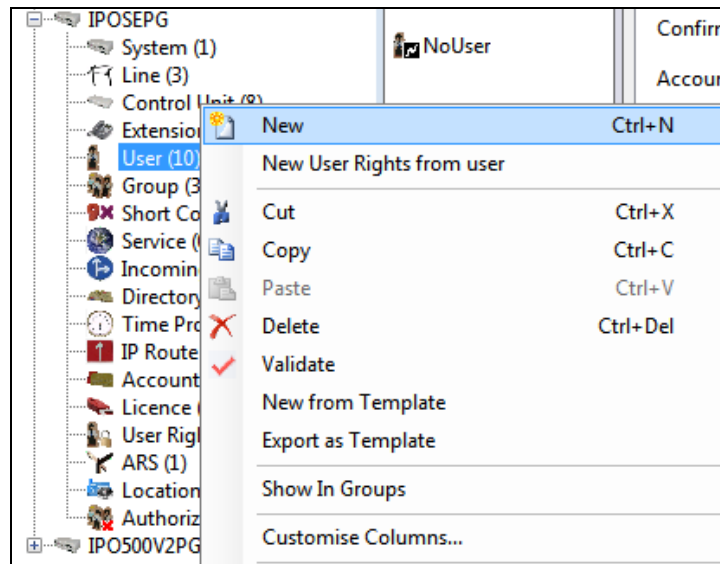
The screenshot shows the IPOSEPG configuration interface with the VoIP tab selected. The configuration is as follows:

- System** | **LAN1** | **LAN2** | **DNS** | **Voicemail** | **Telephony** | **Directory Services** | **System Events** | **SMTP** | **SMDR** | **VoIP** | **VoIP Security** | **Contact Center**
- LAN Settings** | **VoIP** | **Network Topology**
- ☒ H323 Gatekeeper Enable
  - ☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable
  - H.323 Signalling over TLS: Preferred Remote Call Signalling Port: 1720
- ☒ SIP Trunks Enable
- ☒ SIP Registrar Enable
  - ☐ Auto-create Extn/User ☐ SIP Remote Extn Enable
  - SIP Domain Name: devconnect.local
  - SIP Registrar FQDN:
- Layer 4 Protocol
  - ☒ UDP UDP Port: 5060 Remote UDP Port: 5060
  - ☒ TCP TCP Port: 5060 Remote TCP Port: 5060
  - ☒ TLS TLS Port: 5061 Remote TLS Port: 5061
- Challenge Expiry Time (secs): 10
- RTP**
  - Port Number Range: Minimum: 40750 Maximum: 50750
  - Port Number Range (NAT): Minimum: 40750 Maximum: 50750
  - ☒ Enable RTCP Monitoring on Port 5005
  - RTCP collector IP address for phones: 0 . 0 . 0 . 0
- Keepalives**
  - Scope: RTP-RTCP Periodic timeout: 30
  - Initial keepalives: Enabled

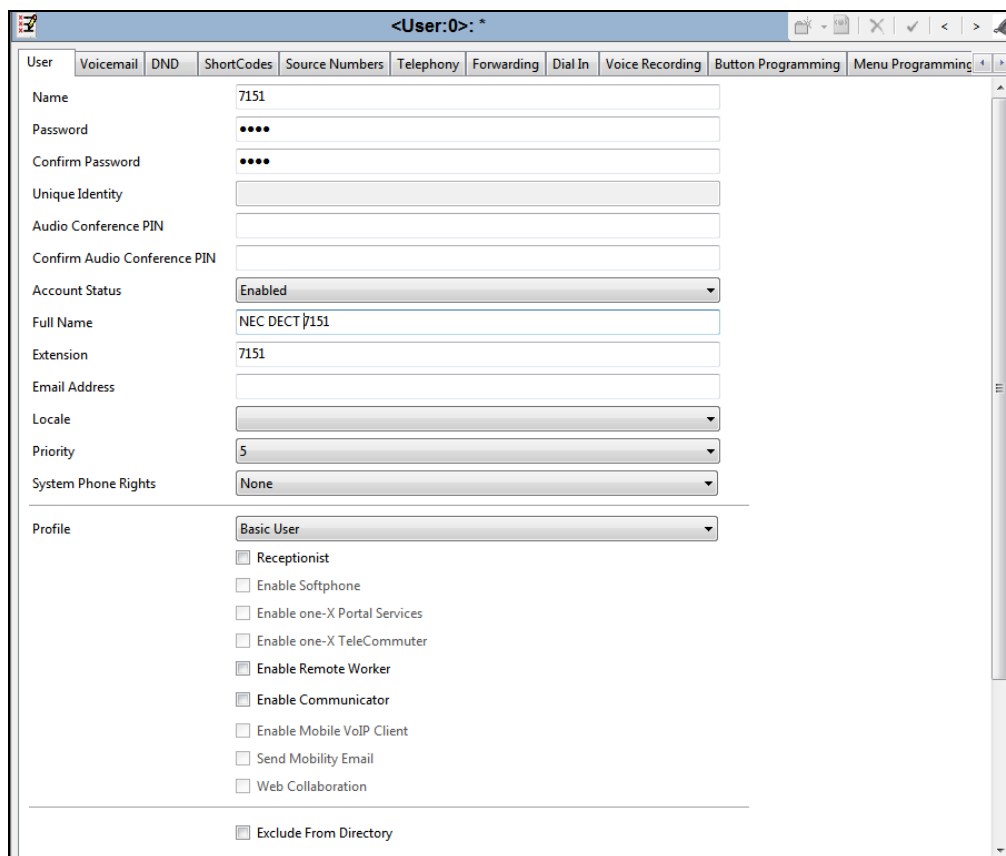


### 5.3. Create a new User

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 **Telephony** Tab select the **Supervisor Settings** tab and enter the password again for the **Login Code**. Ensure that **Force Login** is ticked.

The screenshot shows the 'Supervisor Settings' window in the Avaya IP Office Manager. The 'Telephony' tab is selected in the top navigation bar. Within the 'Supervisor Settings' sub-tab, the 'Login Code' field is highlighted with a red box. The 'Force Login' checkbox is checked. Other visible fields include 'Confirm Login Code', 'Login Idle Period (secs)', 'Monitor Group', 'Coverage Group', and 'Status on No-Answer'. A 'Reset Longest Idle Time' section at the bottom left has 'All Calls' selected.

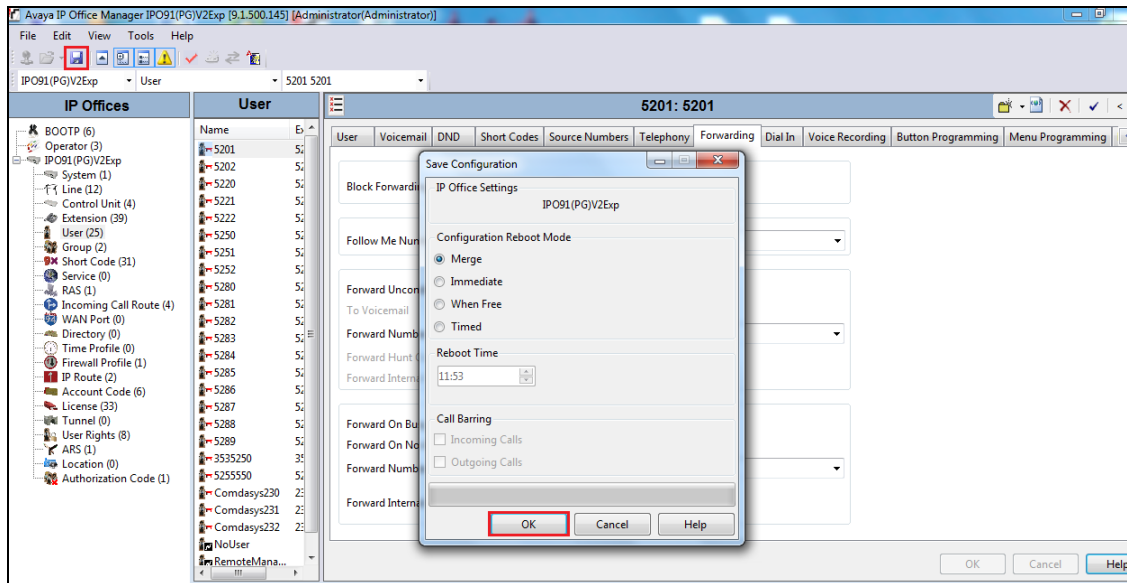
Once **OK** is ticked at the bottom of the screen a new window should appear asking to create a new extension. Select **SIP Extension** as is shown below.

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).

This screenshot shows the same 'Supervisor Settings' window as before, but with a modal dialog box titled 'Avaya IP Office Manager' open in the foreground. The dialog asks, 'Would you like a new VoIP extension created with this number?'. It has three radio button options: 'None', 'H323 Extension', and 'SIP Extension', with 'SIP Extension' being the selected option. An 'OK' button is at the bottom of the dialog. In the background window, the 'OK' button at the bottom right is also highlighted with a red box.

## 5.4. 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 NEC DECT Access Points and Handsets

The following section shows the setup used during compliance testing for the NEC DECT solution, both the configuration of the DECT Access Points and the addition and subscription of the NEC DECT handsets are clearly outlined. The installation of the NEC DECT solution is outside the scope of these Application Notes for more information on this please refer to **Section 9**.

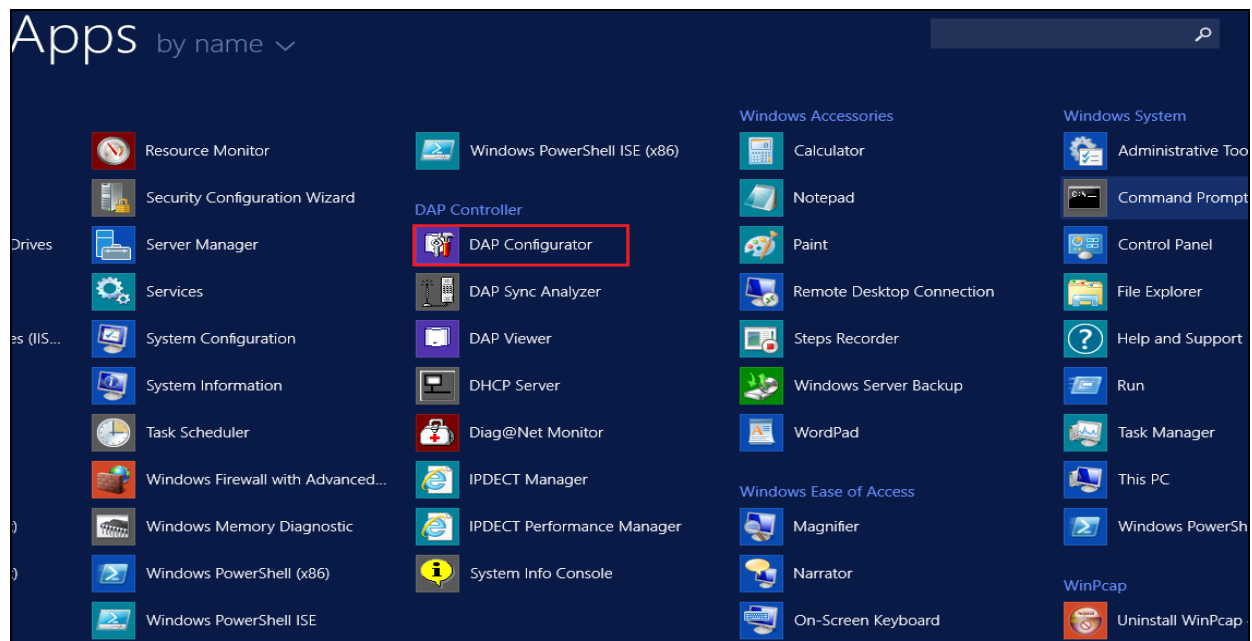
**Note:** The NEC IP DECT solution relies on DHCP (Option 66, 67), NTP and TFTP as network-services. DHCP and TFTP services can be provided from the DAP controller instance. In addition a Multi-Cast IP address is also required for the DAP's to synch.

### 6.1. DAP Configurator - Configure DECT Access Point (DAP)

The configuration of the DECT Access Point uses the DAP Configurator which creates a configuration file that is pushed to each DAP on the network. Click on DAP Configurator as shown below.

**Note:** An NEC IP DECT solution typically consists of a windows based instance called DAP Controller which includes “DAP Configurator” and “DAP Manager”.

**Note:** The DAP Controller Package must be installed in the DAP Controller server. This package is only available from NEC.



Click on the **General Settings** tab and enter the information on the main window. Enter a suitable **System Name** and ensure the **PBX type** is set to **SIP on Avaya-IPO**.

**Note:** Typically a license file is ordered and contains the licenses (number of access points (DAP's) and other features) for the new IP DECT Release 6.41 system. This license file also contains the PARI, which must be unique for each DECT System. When the license file is loaded here the PARI will be filled in automatically.

IP-DECT Configurator R6

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System

General Settings

System name : DevConnect IPO test License SW updates only allowed with SW that has a SWU date from before 2016-12-31

PBX type : SIP on Avaya-IPO

AP200/300 package : Browse...

AP400 package : 4920b655.dwl Browse... DAP build date: 2016-02

AP400 loader : Browse...

Ensure the correct AP400 package file from NEC is available on the machine with the DAP configurator. Click on **Browse** for the **AP400 package** and select the proper file (<filename>.dwl). Click on **Apply** at the bottom of the screen (not shown).

IP-DECT Configurator R6

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System

General Settings

System name : DevConnect IPO test License SW updates only allowed with SW that has a SWU date from before 2016-12-31

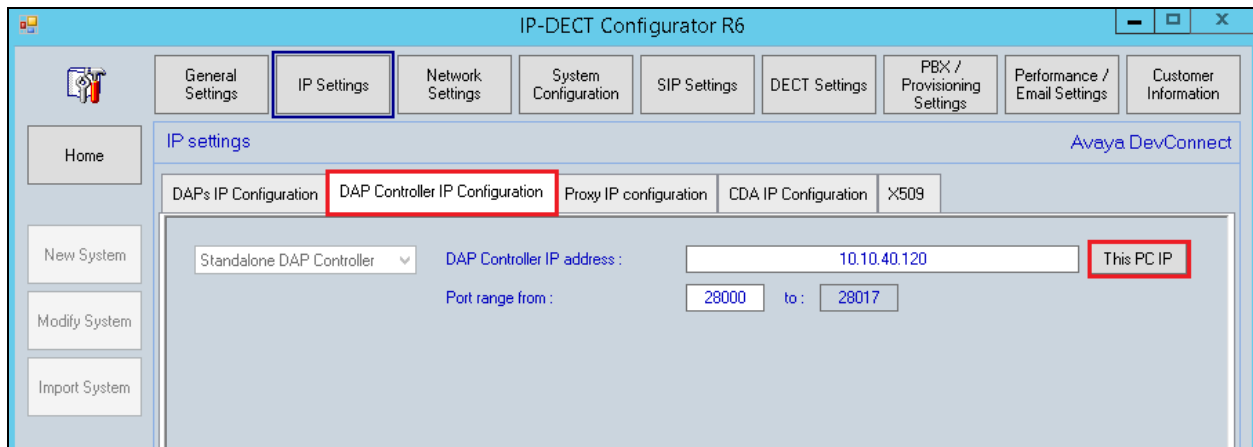
PBX type : SIP on Avaya-IPO

AP200/300 package : Browse...

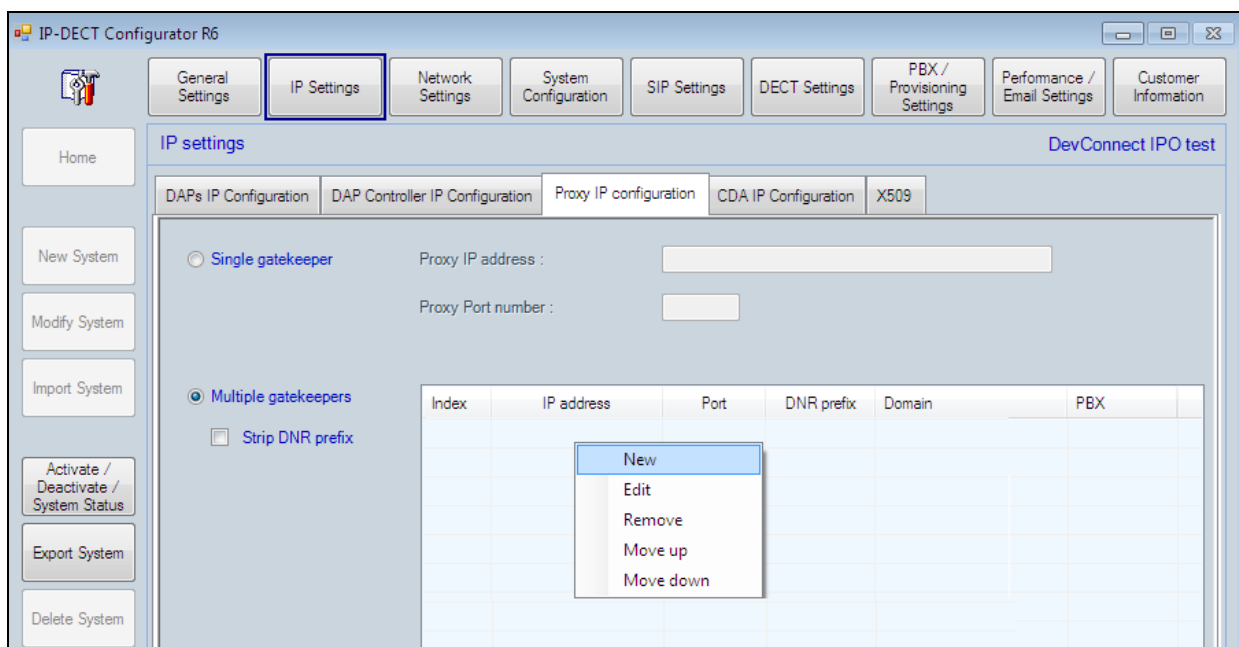
AP400 package : 4920b655.dwl Browse... DAP build date: 2016-02

AP400 loader : Browse...

Click on the **IP Settings** tab at the top of the screen and on the **DAP Controller IP Configuration** tab in the main window. Enter the IP address of the DAP Controller server. In this case just pressing **This PC IP** will fill in the required information.



Click on the **Proxy IP configuration** tab and click on **Multiple gatekeepers** in the main window. Right click in the main window and select **New** as shown.



A new window is opened where the IP Address of the IP Office is entered for the **Proxy IP address** and **5060** as the **Proxy Port number** as this is the port number used for TCP and UDP. This port will be the same as configured in IP Office. Repeat the same process for the IP Office 500 V2.

The screenshot shows the 'Edit Gatekeeper entry' dialog box. It has a title bar with standard window controls. Inside, there are four input fields: 'Proxy IP address' with the value '10.10.40.25', 'Proxy Port number' with the value '5060', 'DNR prefix' (empty), and 'Domain' (empty). To the right of the 'Proxy IP address' field is a button labeled 'This PC IP'. At the bottom right are 'OK' and 'Cancel' buttons. The dialog is overlaid on a larger window showing 'Proxy IP configuration' tabs.

Repeat the same process for the IP Office 500 V2. Note: The DNR prefix (here 52) is used to force the DNR's (numbers) starting with 52 to register upon that Gatekeeper.

The screenshot shows the main window of the IP-DECT Configurator R6. The 'IP Settings' tab is selected in the top navigation bar. Below it, the 'Proxy IP configuration' sub-tab is active. The 'Multiple gatekeepers' radio button is selected. A table displays the configured gatekeepers:

Index	IP address	Port	DNR prefix	Domain	PBX
1	10.10.40.20	5060	52		
2	10.10.40.25	5060			

On the left side of the window, there is a sidebar with buttons for 'Home', 'New System', 'Modify System', 'Import System', 'Activate / Deactivate / System Status', 'Export System', 'Delete System', 'Upgrade Installation', and 'Save System'. The 'Strip DNR prefix' checkbox is unchecked.

Click on **Network Settings** at the top of the page and within this tab select the **IP Provisioning Settings** tab to check the **TFTP** details. The NEC DAP Controller sever can be setup as a TFTP server which will send any and all details to each DAP using TFTP. This information should be filled in automatically but the screen shot below shows the setup implemented for compliance testing. Once the information here is correctly filled in, click on **Apply** at the bottom of the page to continue.

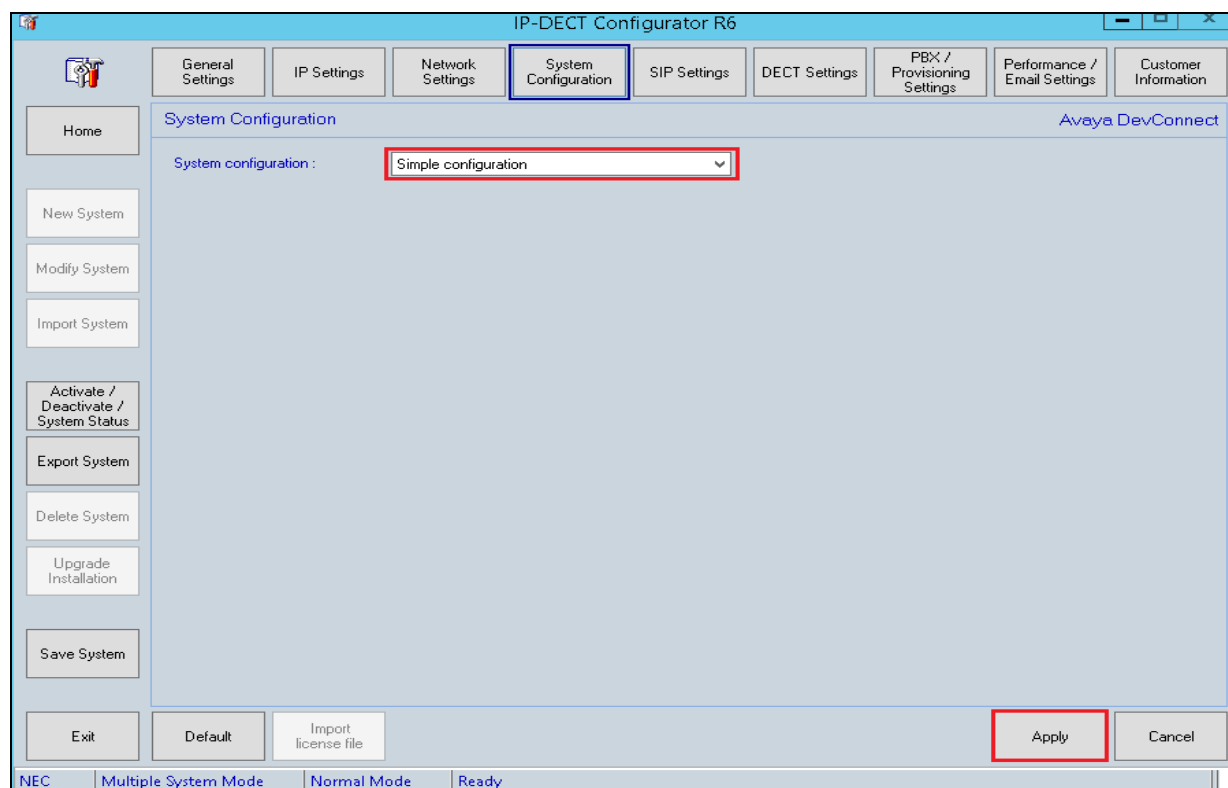
The screenshot displays the IP-DECT Configurator R6 application window. The 'Network Settings' tab is selected at the top, and within it, the 'IP Provisioning Settings' sub-tab is active. The interface includes a left-hand menu with options like 'Home', 'New System', 'Modify System', 'Import System', 'Activate / Deactivate / System Status', 'Export System', 'Delete System', 'Upgrade Installation', and 'Save System'. The main configuration area shows the following settings:

- Provisioning protocol :** TFTP (selected from a dropdown)
- Provisioning folder :** C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\ (with a 'Browse...' button)
- TFTP Server :** 3Com TFTP Server on this PC (selected from a dropdown)
- TFTP Server IP address :** (empty text field)
- ☒ **Monitor TFTP Server**

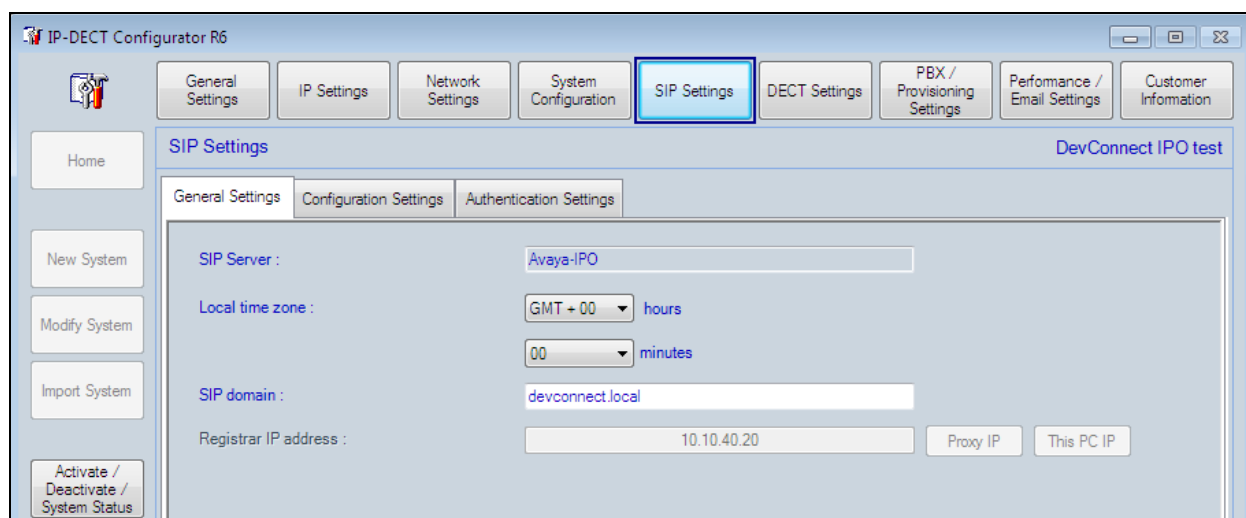
At the bottom of the window, there are buttons for 'Exit', 'Default', 'Import license file', 'Apply' (highlighted with a red box), and 'Cancel'. The status bar at the very bottom indicates 'NEC | Multiple System Mode | Normal Mode | Ready'.



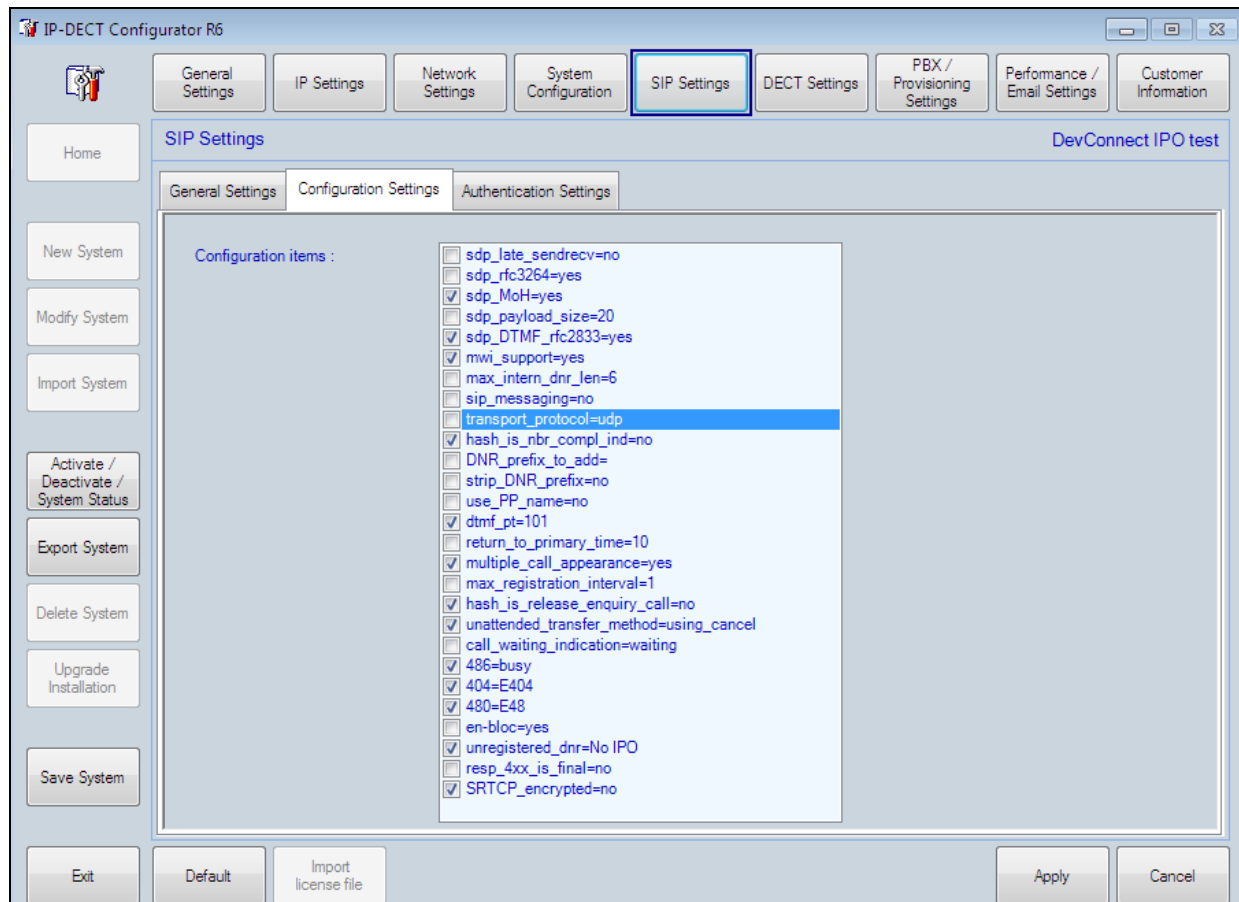
Click on **System Configuration** at the top of the page, the **System configuration** in the main window should display **Simple configuration** as shown below, click on **Apply** to continue.



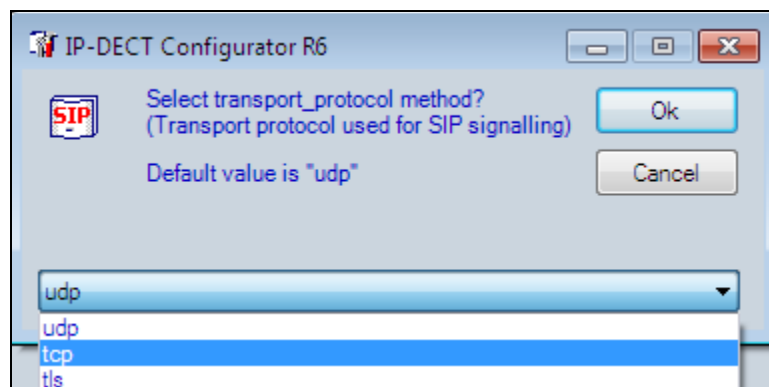
Click on **SIP Settings** at the top of the page and the **General Settings** tab in the main window. The SIP Server details will be automatically filled in. Set the time zone and the **SIP domain**, note this is the same SIP domain featured in **Section 5.2**. The **Registrar IP address** will be automatically filled in from the Proxy information (see Proxy IP Configuration setting previously).



Click on **Configuration Settings** tab, the information will be automatically filled in but the screen shot below shows the settings used during compliance testing. The **transport\_protocol** shows that **UDP** is being used and the **mw\_i\_support=yes**. These settings can be changed here.



To change the protocol simply click on **transport\_protocol** and select the correct protocol.



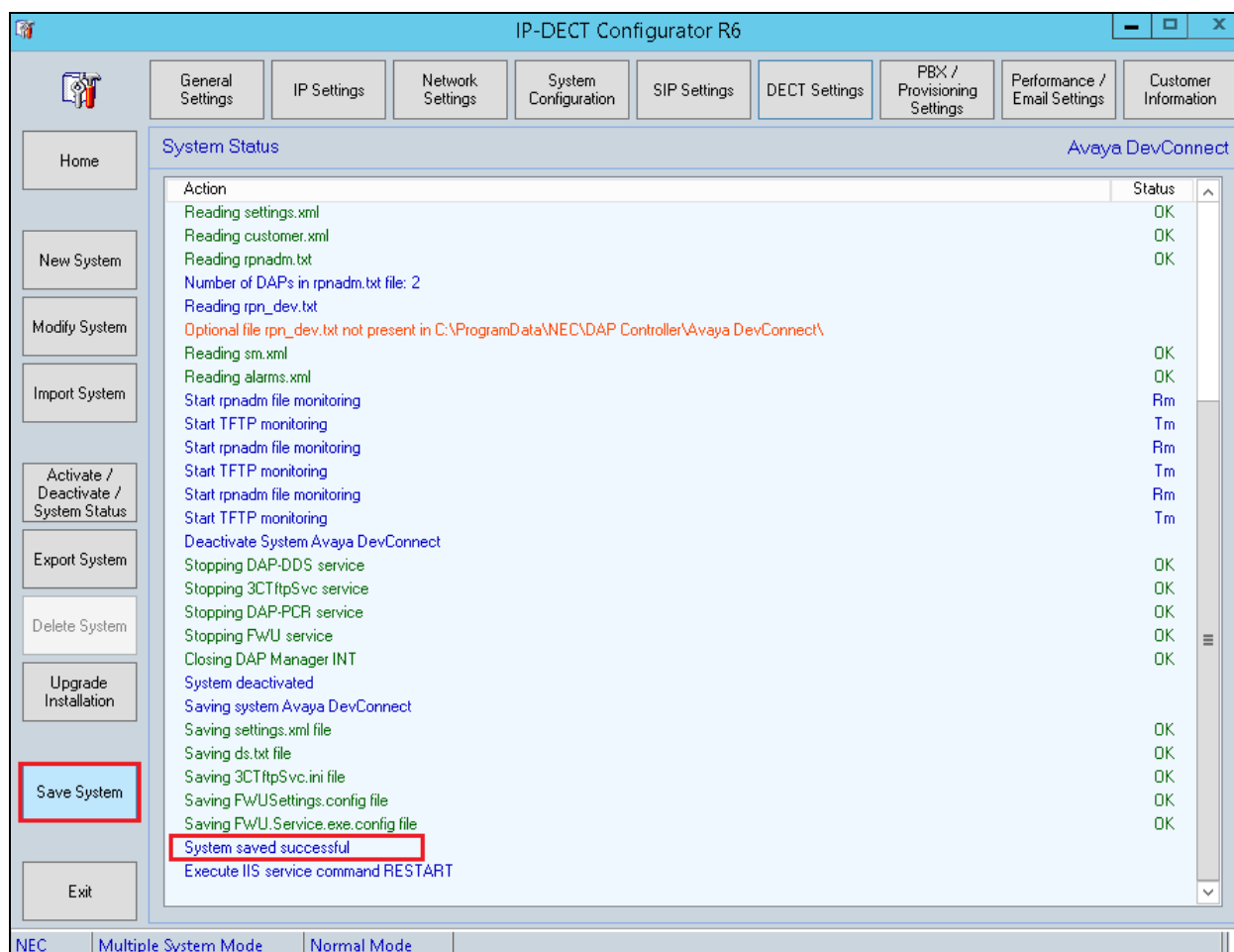
Click on **Authentication Settings** tab and enter **%s** as the user (means the DNR will be used as the SIP extension) and **1234** as the password, note that this is the same password set in **Section 5.3**.

The screenshot displays the 'IP-DECT Configurator R6' application window. The top menu bar includes 'General Settings', 'IP Settings', 'Network Settings', 'System Configuration', 'SIP Settings' (highlighted with a blue border), 'DECT Settings', 'PBX / Provisioning Settings', 'Performance / Email Settings', and 'Customer Information'. On the left, a sidebar contains buttons for 'Home', 'New System', 'Modify System', 'Import System', 'Activate / Deactivate / System Status', 'Export System', 'Delete System', 'Upgrade Installation', and 'Save System'. The main area is titled 'SIP Settings' and contains three sub-tabs: 'General Settings', 'Configuration Settings', and 'Authentication Settings' (highlighted with a red border). The 'Authentication Settings' tab shows five rows for 'Authentication Realm 1' through 'Authentication Realm 5'. Each row has a 'User' field and a 'Pswd' field. In the first row, the 'User' field contains '%s' and the 'Pswd' field contains '1234', both highlighted with red borders. To the right of each row is a 'Remove' button. At the bottom of the window, there is a status bar with 'License valid' and an 'Apply' button (highlighted with a red border) next to a 'Cancel' button. The bottom-most status bar shows 'NEC', 'Multiple System Mode', 'Normal Mode', and 'Ready'.

Click on **DECT Settings** at the top of the page and the **DECT Settings** tab in the main window. The **PARI** should be already filled in from the information provided by the license file. The **Country code** can be changed to suite and click on **Apply** once this information has been entered as the other tabs do not need to be changed.

The screenshot displays the IP-DECT Configurator R6 application window. The title bar reads "IP-DECT Configurator R6". The top menu bar includes tabs for General Settings, IP Settings, Network Settings, System Configuration, SIP Settings, DECT Settings (highlighted with a blue border), PBX / Provisioning Settings, Performance / Email Settings, and Customer Information. On the left, a vertical sidebar contains buttons for Home, New System, Modify System, Import System, Activate / Deactivate / System Status, Export System, Delete System, Upgrade Installation, and Save System. The main content area is titled "DECT Settings" and contains sub-tabs for DECT Settings (highlighted with a red border), Handset Settings, and DAP Settings. The DECT Settings sub-tab is active, showing the following fields: "Country code:" with a dropdown menu set to "Ireland"; "PARI:" with a text box containing "100F073C" (highlighted with a red border); "SARI:" with a text box containing "FFFFFFF"; "Frequency table:" with a text box containing "0"; and "Used carriers:" with a list of checkboxes for Carrier 0 through Carrier 9, all of which are checked. At the bottom right, there are "Apply" and "Cancel" buttons, with the "Apply" button highlighted by a red border. The bottom status bar shows "NEC", "Multiple System Mode", "Normal Mode", and "Ready".

Once **Save System** has been pressed at the bottom right of the screen the following will be displayed showing that the system has **saved successfully**.



Clicking on **Activate/Deactivate System Status** on the left side of the screen will bring a page on which a restart can be done by clicking the start icon (> button). The DAPs remain fully operational and making and receiving calls is still possible. The DAP controller is only necessary for Management actions regarding the handsets. Clicking on the start icon highlighted in the main screen will restart the system again after Activate/Deactivate System Status has been pressed.

**IP-DECT Configurator R6**

General Settings | IP Settings | Network Settings | System Configuration | SIP Settings | DECT Settings | PBX / Provisioning Settings | Performance / Email Settings | Customer Information

Home | New System | Modify System | Import System | **Activate / Deactivate / System Status** | Export System | Delete System | Upgrade Installation | Save System | Exit

**System Status** Avaya DevConnect

Activate	Name	Status	Action
<input checked="" type="checkbox"/>	DDS	Service stopped	<a href="#">Start</a>
<input checked="" type="checkbox"/>	PCR	Service stopped	<a href="#">Start</a>
<input checked="" type="checkbox"/>	FWU	Service stopped	<a href="#">Start</a>
<input checked="" type="checkbox"/>	TFTP Server	Service stopped	<a href="#">Start</a>
<input checked="" type="checkbox"/>	DAP Manager INT	Program not running	<a href="#">Start</a>
<input type="checkbox"/>	DHCP Server	Provided by network	<a href="#">Start</a>
<input type="checkbox"/>	DiagMonitor	Program running (5.0.2.168)	<a href="#">Stop</a>

**Required network card settings :**

IP : 10.10.40.120  
 DG : 10.10.40.1  
 SN : 255.255.255.0

[Change network](#) [Network Connections](#)

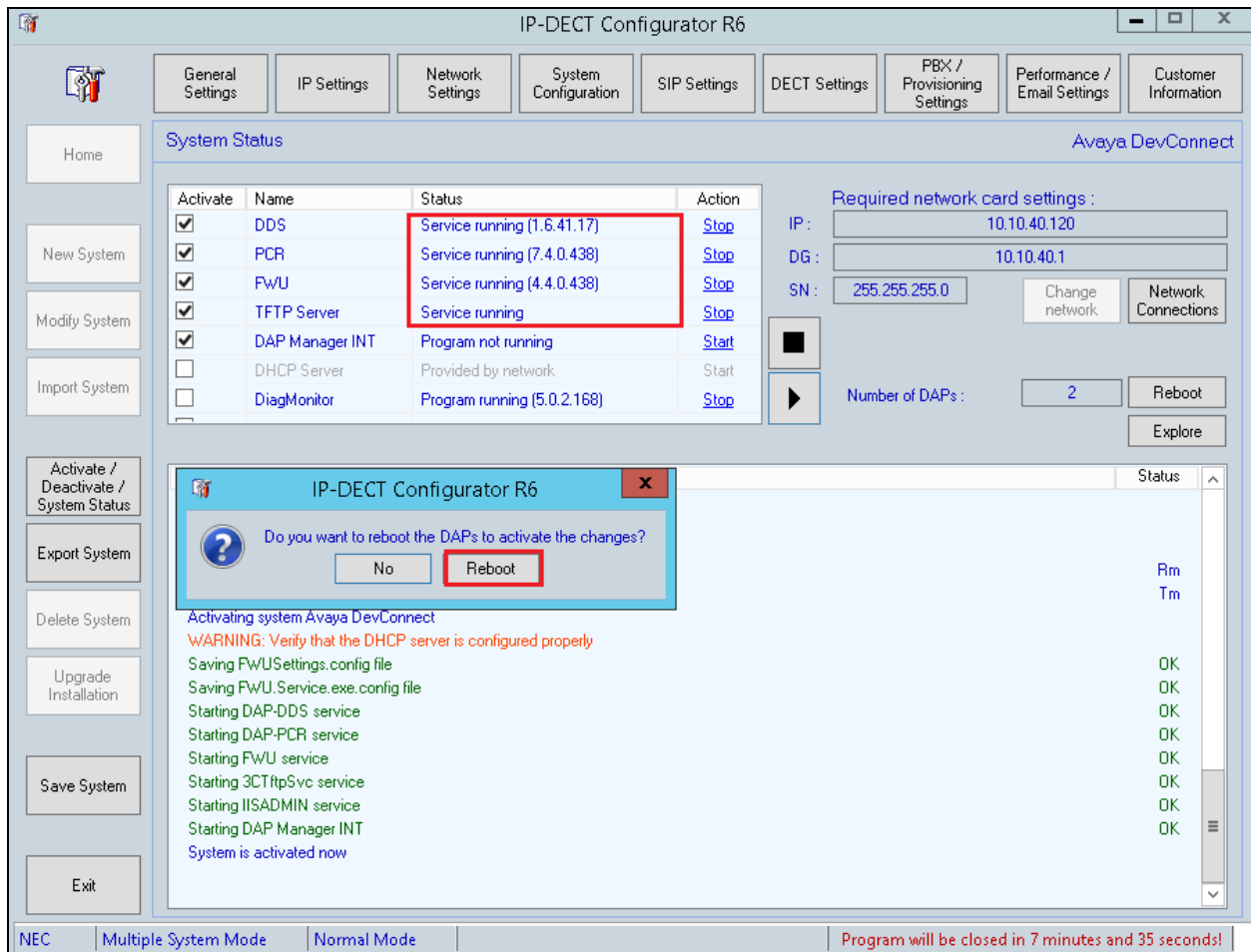
Number of DAPs : 2 [Reboot](#) [Explore](#)

**Action** **Status**

Stopping FWU service	OK
Closing DAP Manager INT	OK
System deactivated	
Saving system Avaya DevConnect	
Saving settings.xml file	OK
Saving ds.txt file	OK
Saving 3CTftpSvc.ini file	OK
Saving FWUSettings.config file	OK
Saving FWU.Service.exe.config file	OK
System saved successful	
Execute IIS service command RESTART	OK
Attempting stop...	
Internet services successfully stopped	
Attempting start...	
Internet services successfully restarted	
Start rpnadm file monitoring	Rm
Start TFTP monitoring	Tm

NEC | Multiple System Mode | Normal Mode | Program will be closed in 8 minutes and 40 seconds!

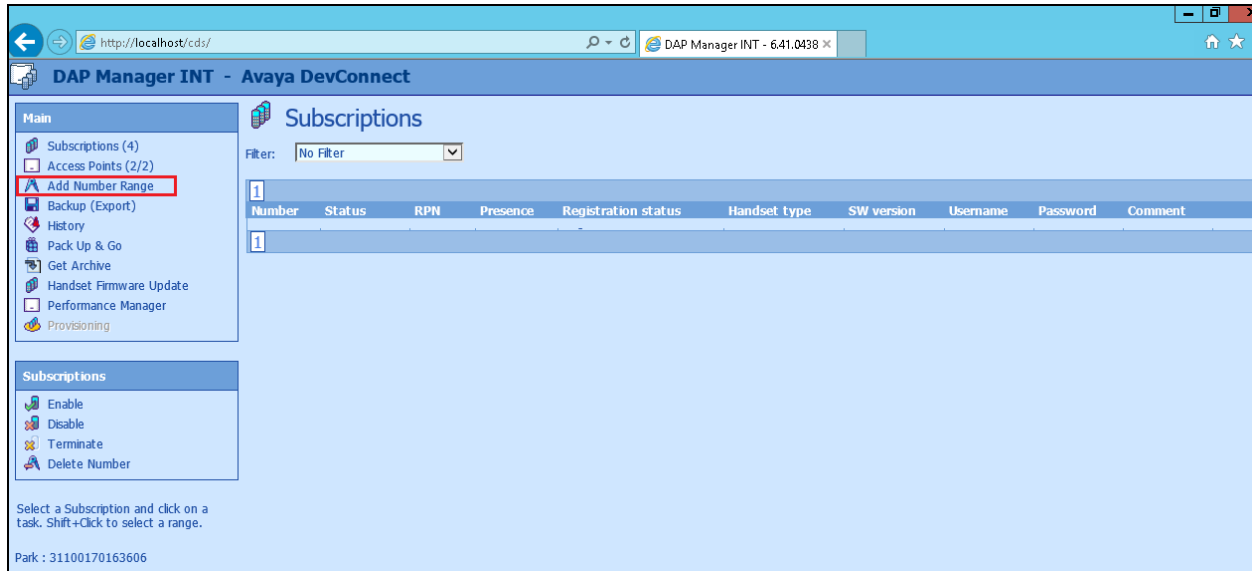
With the system up and running again a window should automatically appear asking to reboot the DAP's. Click on **Reboot** to complete the setup.



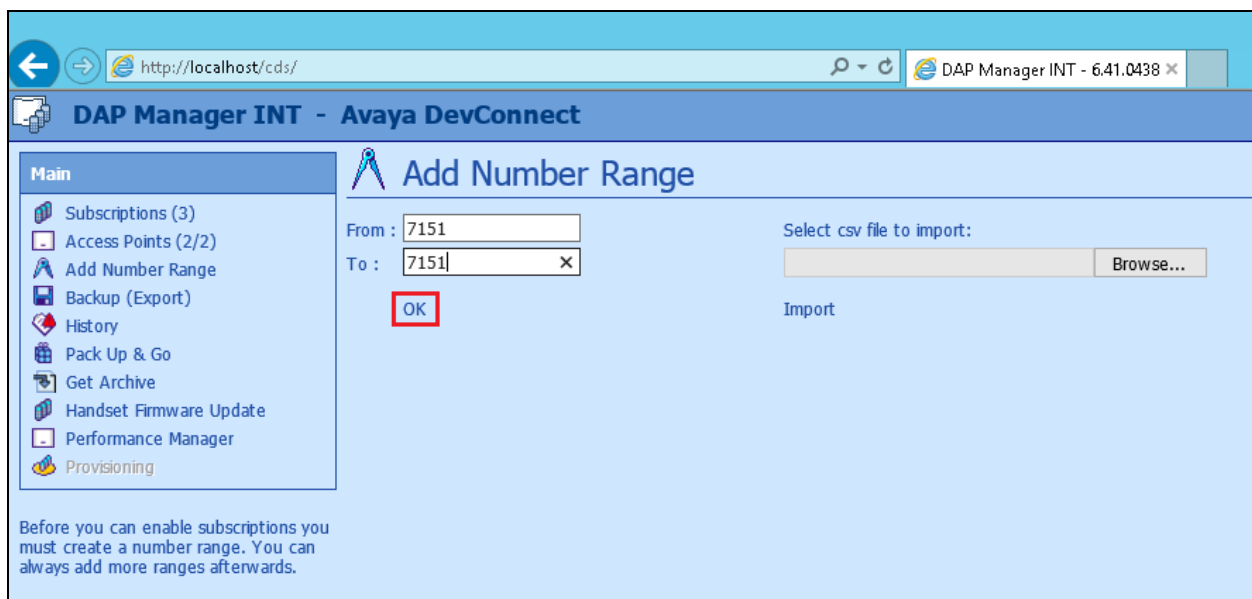
## 6.2. DAP Manager – Managing DECT users and handsets

Once the DAP configurator has been fully configured, the following window of the DAP manager is automatically popped. The DAP manager can also be reached by typing the following URL <http://<IP-of-DAP-manager>/cds/>. The DAP manager is used to manage the extensions (DNR) on the DECT system and also to subscribe the DECT handsets.

Click on **Add Number Range** in the left window.



Enter the number range or the number of the extension(s) to be added and click on **OK**.





Highlight the new extension added in the main window and click on **Enable** in the left window.

**DAP Manager INT - Avaya DevConnect**

**Main**

- Subscriptions (3)
- Access Points (2/2)
- Add Number Range
- Backup (Export)
- History
- Pack Up & Go
- Get Archive
- Handset Firmware Update
- Performance Manager
- Provisioning

**Subscriptions**

- Enable**
- Disable
- Terminate
- Delete Number

1 Subscription Selected

Park : 31100170163606

**Subscriptions**

Filter: No Filter

Number	Status	RPN	Presence	Registration status	Handset type	SW version
7150	Subscribed	010	Present	Registered	G566	1.10.00.01
7151	Free					
7152	Subscribed	011	Present	Registered	G566	1.10.00.01
7153	Subscribed	011	Present	Registered	I766	1.10.00.02

Note the **PIN** number which will be used to subscribe the handset in the next section.

**DAP Manager INT - Avaya DevConnect**

**Main**

- Subscriptions (4)
- Access Points (2/2)
- Add Number Range
- Backup (Export)
- History
- Pack Up & Go
- Get Archive
- Handset Firmware Update
- Performance Manager
- Provisioning

**Subscriptions**

Filter: No Filter

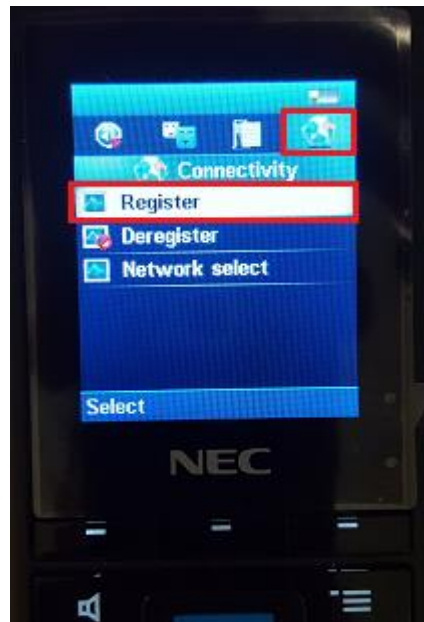
Number	Status	PIN	RPN	Presence
7150	Subscribed		010	Present
7152	Subscribed		011	Absent
7153	Subscribed		011	Absent
7151	Enabled	2475		

### 6.3. How to Subscribe the DECT Handset

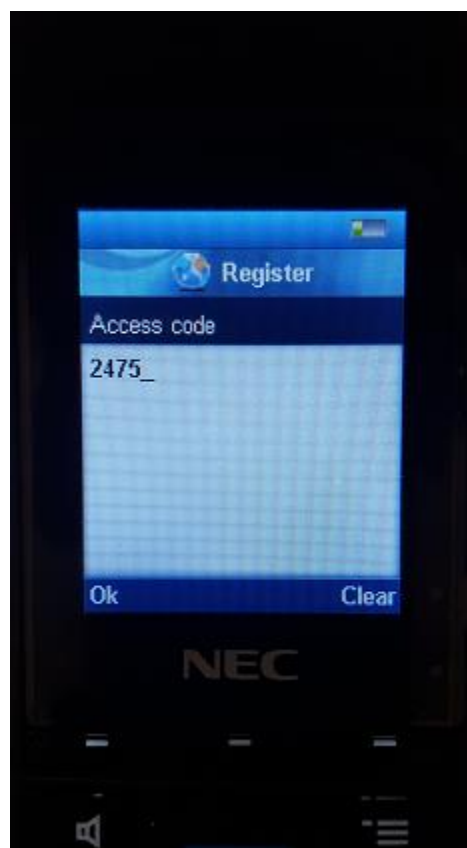
From the DECT handset click on the menu button (on top of the power button) and select **Settings** as highlighted below.



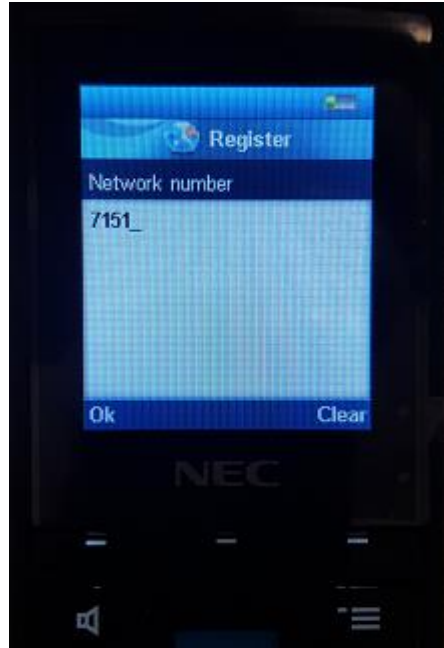
Scroll right to **Connectivity** and select **Register** as shown below.



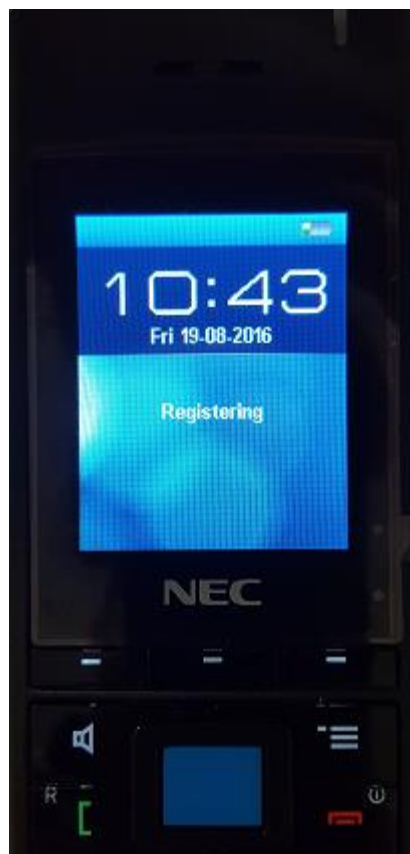
There will be a number of slots labelled **Empty** (not shown) choose one and continue pressing Ok until the Access Code is asked for. Enter the **Access code** as per **Section 6.2**.



Enter the extension number for the **Network number** as shown below for extension **7151**.



Once this are all entered the phoneset display should show **Registering**, as shown below.

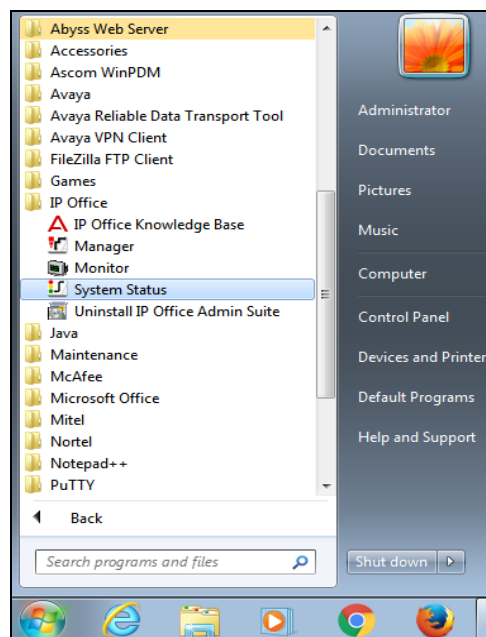


## 7. Verification Steps

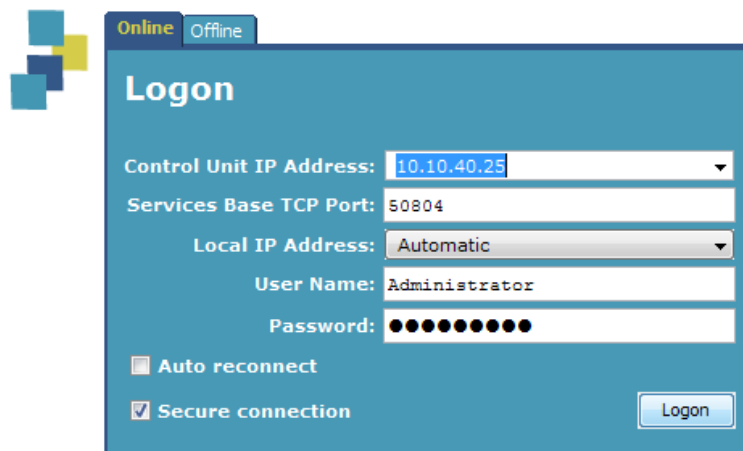
The ultimate test is to make and receive calls between the NEC DECT handsets and to and from the Avaya phones. This will verify that the NEC DECT handsets are connected correctly with the Avaya solution. The following steps can be taken to ensure that connections between NEC DECT handsets and IP Office are up.

### 7.1. Avaya IP Office Registration

To verify the 'connection type' and the 'media security' IP Office System Status can be used to monitor each handset including the NEC DECT handsets. Open IP Office System Status as shown below.



Connect to the required IP Office and enter the appropriate credentials then click on **Logon**.



Place a call to one of the NEC handsets and select the handset as shown below. Information on the call and the connection is displayed in the main window.

The screenshot shows the 'IP Office System Status' window. On the left is a navigation tree with 'System', 'Alarms (10)', 'Extensions (7)', 'Trunks (3)', 'Active Calls', 'Resources', 'Voicemail', and 'IP Networking Locations'. The 'Extensions (7)' section is expanded, and extension 5180 is selected. The main pane displays the 'Extension Status' for 5180. Below this, a table shows a single call record.

Extension Number:	5180
IP address:	10.10.40.206
Standard Location:	None
Registrar:	Primary
Telephone Type:	Unknown SIP Device
User Agent:	NEC_IP_DECT_GW_G566/4920b655_01.14.00.01
Media Stream:	RTP
Layer 4 Protocol:	TCP
Current User Extension Number:	5180
Current User Name:	5180
Forwarding:	Off
Twinning:	Off
Do Not Disturb:	Off
Message Waiting:	Off
Number of New Messages:	0
Phone Manager Type:	None
SIP Device Features:	REFER,UPDATE
License Reserved:	No
Last Date and Time License Allocated:	02/06/2017 11:01:55
DTMF Required:	No
Packet Loss Fraction:	
Jitter:	
Round Trip Delay:	
Connection Type:	Direct Media
Codec:	G711 A
Remote Media Address:	10.10.40.206

Call Ref	Current State	Time in State	Calling Number or Called Number	Direction	Other Party on Call
128	Connected	00:05:30	5181	Incoming	Extn 5181, 5181

Information on the **Media Stream** and the **Layer 4 Protocol** are shown as well as the **Connection Type**. The display below shows a **Direct Media** call using **RTP** and **TCP**.

Extension Status	
Extension Number:	5180
IP address:	10.10.40.206
Standard Location:	None
Registrar:	Primary
Telephone Type:	Unknown SIP Device
User Agent:	NEC_IP_DECT_GW_G566/4920b655_01.14.00.01
Media Stream:	RTP
Layer 4 Protocol:	TCP
Current User Extension Number:	5180
Current User Name:	5180
Forwarding:	Off
Twinning:	Off
Do Not Disturb:	Off
Message Waiting:	Off
Number of New Messages:	0
Phone Manager Type:	None
SIP Device Features:	REFER,UPDATE
License Reserved:	No
Last Date and Time License Allocated:	02/06/2017 11:01:55
DTMF Required:	No
Packet Loss Fraction:	
Jitter:	
Round Trip Delay:	
Connection Type:	Direct Media
Codec:	G711 A
Remote Media Address:	10.10.40.206

## 8. Conclusion

These Application Notes describe the configuration steps required for NEC's IP DECT Access Point (DAP) and DECT handsets to successfully interoperate with Avaya IP Office Server Edition and IP Office 500 V2 Expansion R10.0 by registering the NEC Handsets with IP Office as SIP phones. Please refer to **Section 2.2** for test results and observations.

## 9. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

- [1] *Administering Avaya IP Office™ Platform with Manager*, Release 10.0
- [2] *Deploying Avaya IP Office™ Platform Servers as Virtual Machines* Document ID 15-601011 Issue 04g - (31 January 2017)
- [3] *Deploying Avaya IP Office™ Platform IP500*, 15-601042 Issue 31m - (01 December 2016)

NEC's technical documentation is available from NEC or from <http://businessnet.nec-enterprise.com>.

- [4] *NEC, 2016, Business Mobility IP DECT CE Manual for SIP Connectivity, R6.41*, available at <http://businessnet.nec-enterprise.com>
- [5] *NEC, 2016, IP DECT Administrator Guide, R6.41*, available at <http://businessnet.nec-enterprise.com>

---

**©2017 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).