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 TLS/SRTP – 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 TLS/SRTP.

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 TLS/SRTP.

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 Avaya IP Office. The NEC DECT handsets behave as SIP integrated into the Avaya 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 Avaya 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 UDP/RTP and TCP/RTP 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 UDP&TCP/RTP*.

The primary goal of the Transport Layer Security (TLS) protocol is to provide privacy and data integrity between two communicating computer applications. When secured by TLS, connections between a client (e.g., NEC DAP) and a server (e.g., IP Office) have one or more of the following properties:

- The connection is private because symmetric cryptography is used to encrypt the data transmitted. The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret negotiated at the start of the session. The server and client negotiate the details of which encryption algorithm and cryptographic keys to use before the first byte of data is transmitted. The negotiation of a shared secret is both secure and reliable.

- The identity of the communicating parties can be authenticated using public-key cryptography. This authentication can be made optional, but is generally required for at least one of the parties (typically the server).
- The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. Since RTP is closely related to RTCP (Real Time Control Protocol) which can be used to control the RTP session, SRTP also has a sister protocol, called Secure RTCP (or SRTCP); SRTCP provides the same security-related features to SRTP, as the ones provided by RTCP to RTP. Utilization of SRTP or SRTCP is optional to the utilization of RTP or RTCP; but even if SRTP/SRTCP is used, all provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. The only exception is the message authentication feature which is indispensably required when using SRTCP.

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 utilized enabled capabilities of TLS/SRTP.

## 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.

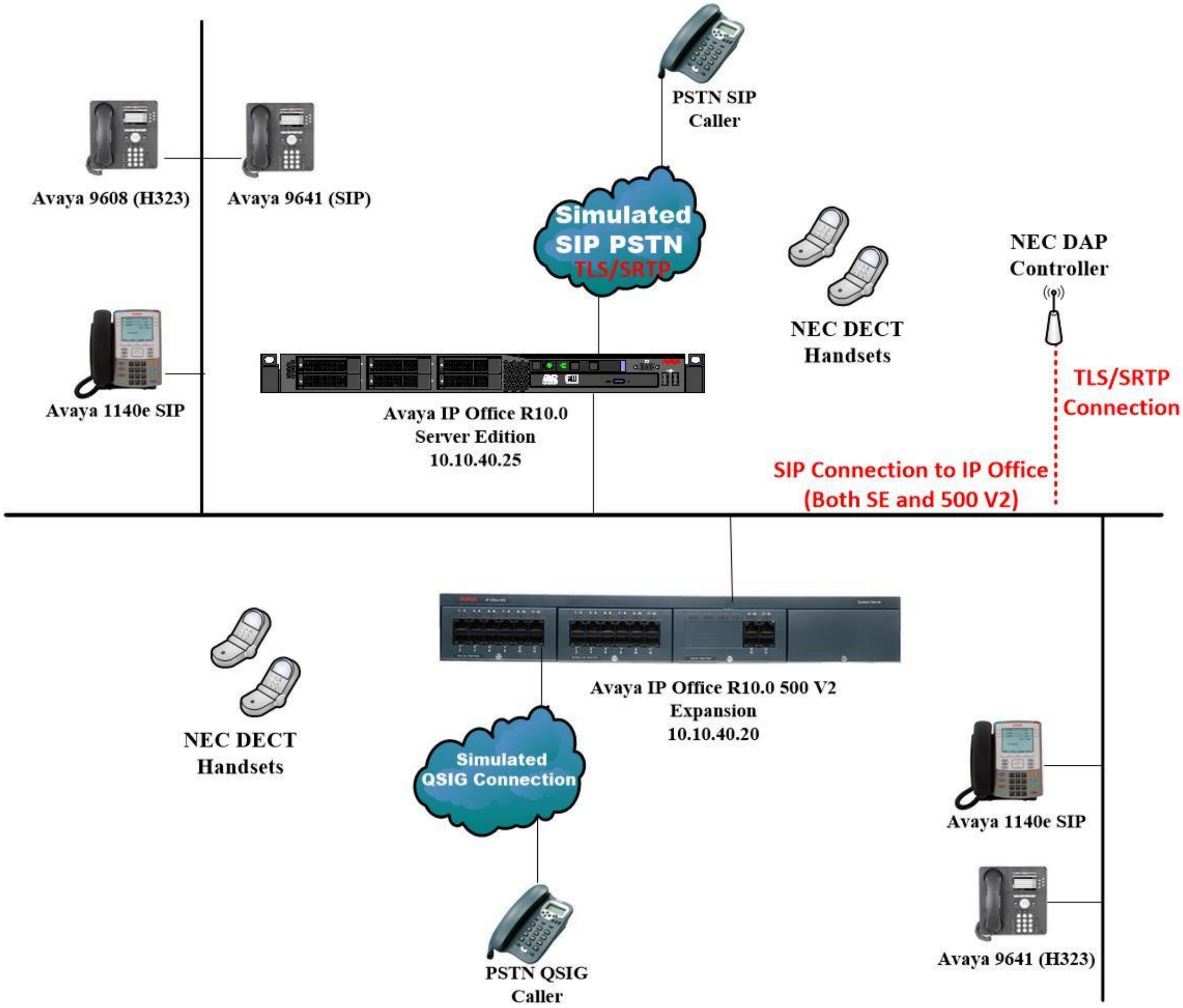


**Figure 1: Network Solution of NEC DECT Handsets with Avaya IP Office Server Edition and 500 V2 R10.0**

# 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 Primary running on a Virtual Platform | R10.0.2.0 Build 10 |
| Avaya IP Office 500 V2 Expansion | 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<br>running on Windows 2012 virtual server | Release of R6.41<br>6.41.0624 |
| NEC DECT Access Point | Release of R6.41<br>6.41.0624<br>Patch is Release 6.41 : 4920b655.dwl |
| NEC DECT Handset NEC G566<br>NEC DECT Handset NEC I766 | 1.14.00.01<br>1.14.00.01 |

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. Configure Avaya IP Office

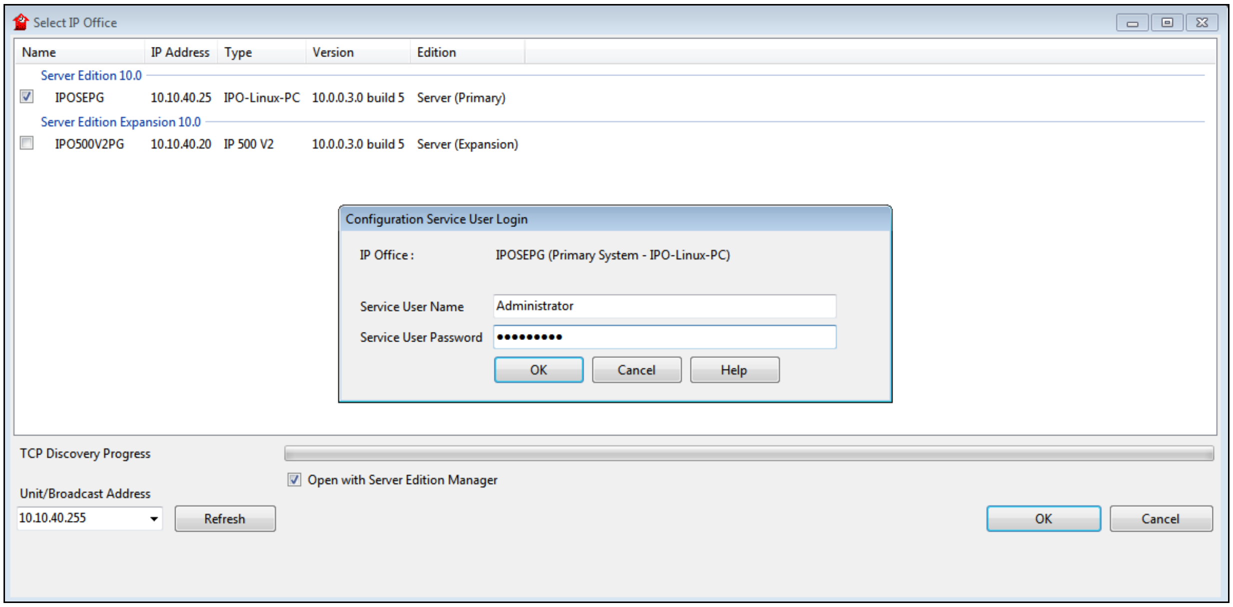
The information provided in this section describes the configuration of Avaya IP Office for this solution. Configuration and verification operations on the Avaya IP Office were all performed using Avaya IP Office Manager. It is implied a working system is already in place with the necessary licensing. 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.
- Configure Media Security Settings.
- 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..



Select IP Office

| | Name | IP Address | Type | Version | Edition |
|---|---|---|---|---|---|
| | Server Edition 10.0 | | | | |
| ☑ | IPOSEPG | 10.10.40.25 | IPO-Linux-PC | 10.0.0.3.0 build 5 | Server (Primary) |
| | Server Edition Expansion 10.0 | | | | |
| □ | IPO500V2PG | 10.10.40.20 | IP 500 V2 | 10.0.0.3.0 build 5 | Server (Expansion) |

Configuration Service User Login

IP Office : IPOSEPG (Primary System - IPO-Linux-PC)

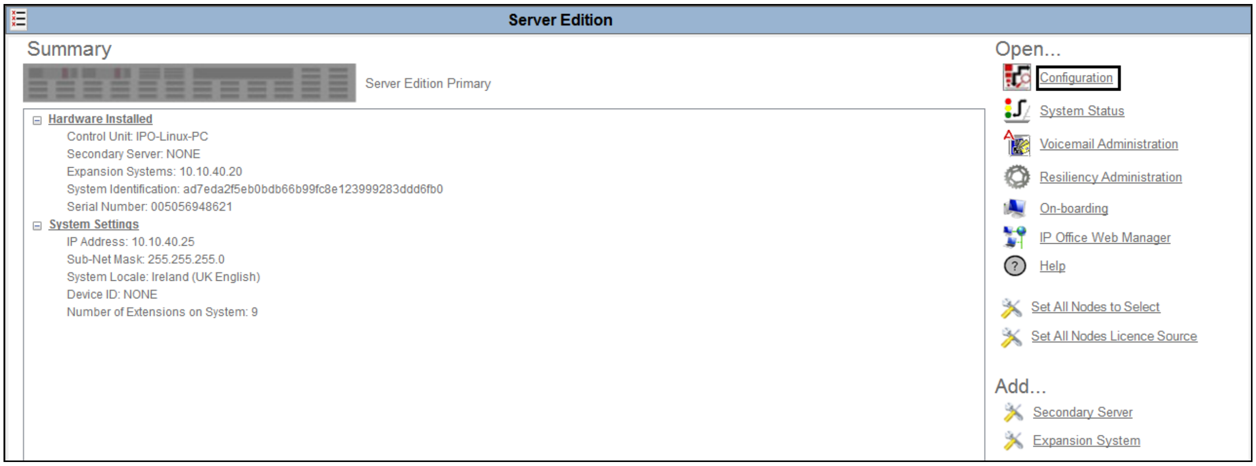
Service User Name: Administrator

Service User Password: •••••••••

☑ Open with Server Edition Manager

Unit/Broadcast Address: 10.10.40.255

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



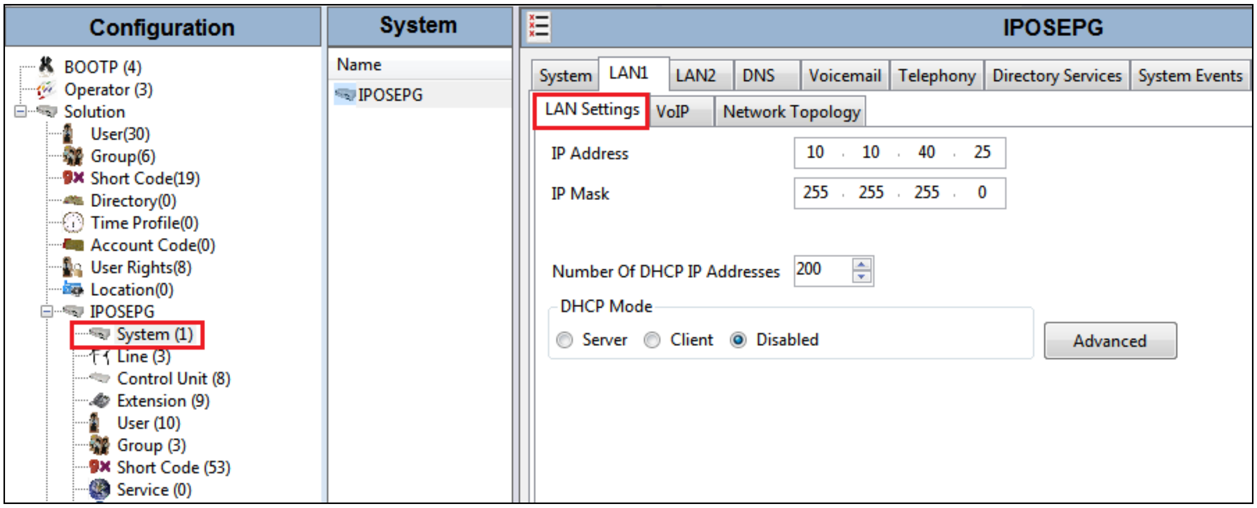
Server Edition Primary

Hardware Installed
Control Unit: IPO-Linux-PC
Secondary Server: NONE
Expansion Systems: 10.10.40.20
System Identification: ad7eda2f5eb0bdb66b99fc8e123999283ddd6fb0
Serial Number: 005056948621

System Settings
IP Address: 10.10.40.25
Sub-Net Mask: 255.255.255.0
System Locale: Ireland (UK English)
Device ID: NONE
Number of Extensions on System: 9

## 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**.



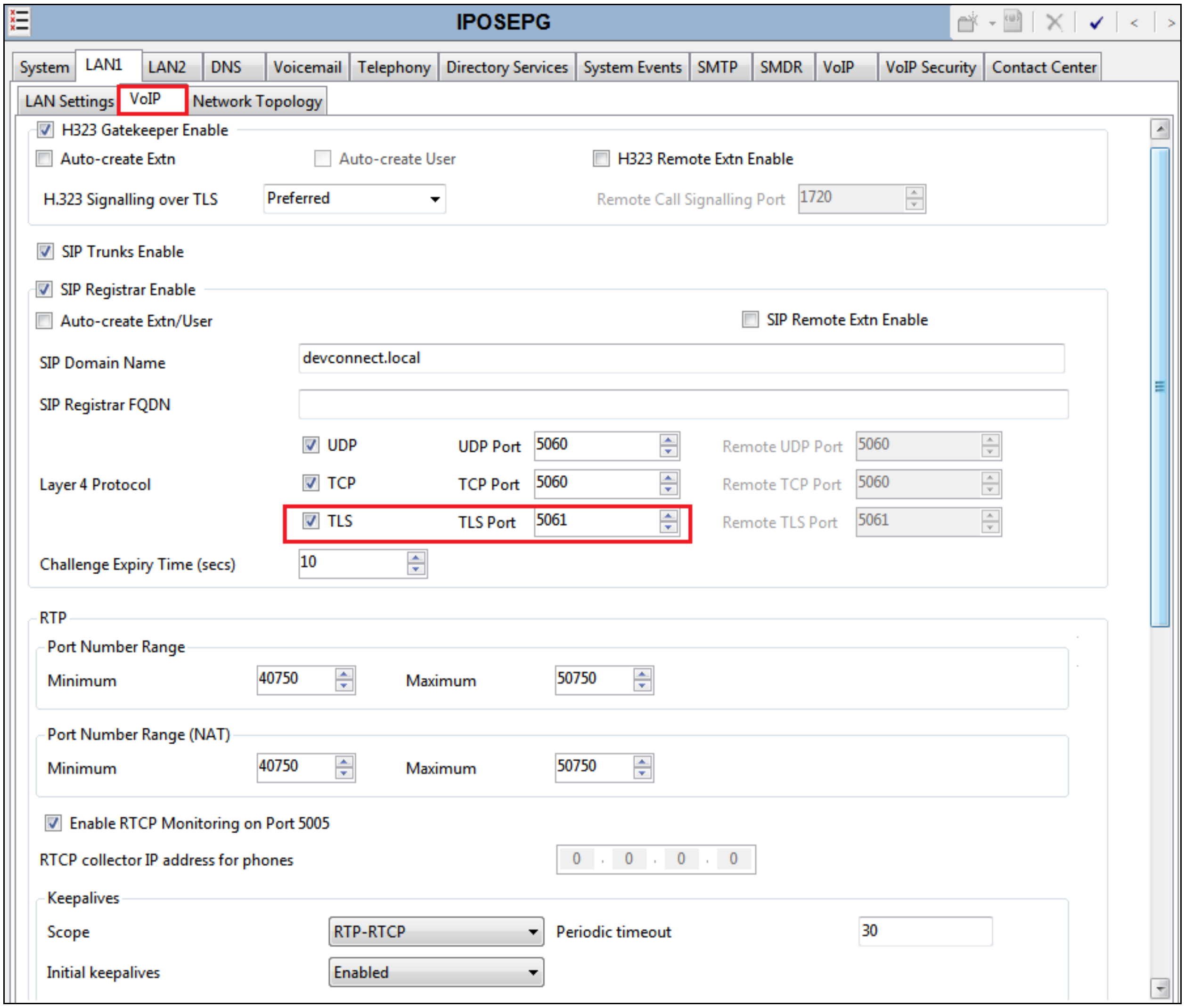
IP Address 10 . 10 . 40 . 25

IP Mask 255 . 255 . 255 . 0

Number Of DHCP IP Addresses 200

DHCP Mode ○ Server ○ Client ● Disabled

Click on the **VoIP** tab. Ensure that **TLS** is ticked and that port **5061** is being used. During compliance testing **RTP-RTCP Keepalives** were set to **30**secs.


IPOSEPG
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

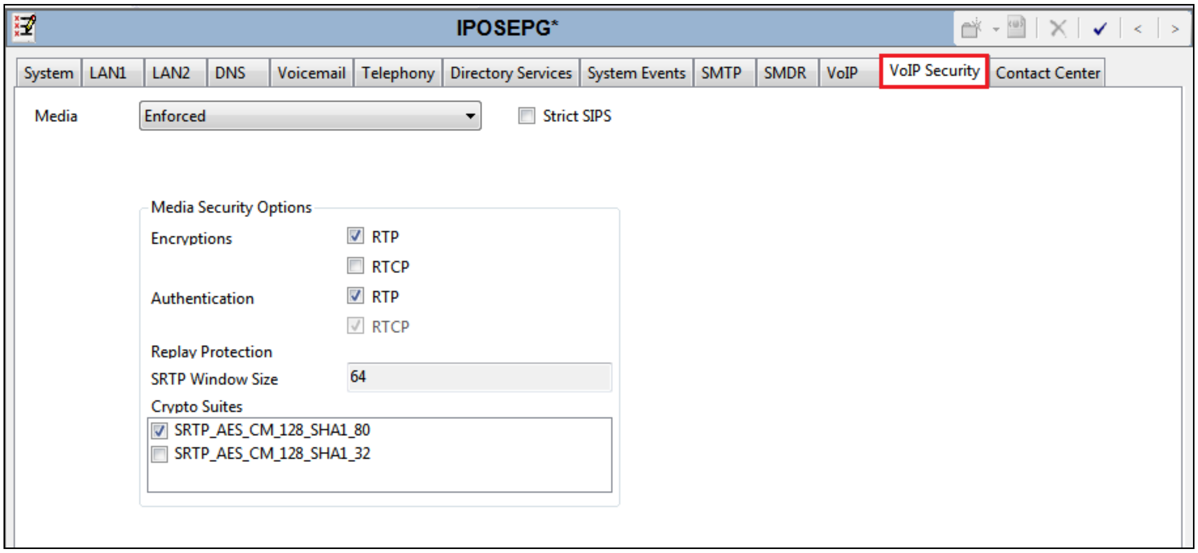
Scope: RTP-RTCP Periodic timeout: 30

Initial keepalives: Enabled

## 5.3. Configure the Media Security Settings

Click on **VoIP Security**, the **Media** can be set to Enforced or Best Effort. For compliance testing **Enforced** was set simply to ensure 100% that SRTP was used. **Encryptions** and **Authentication** were set for **RTP** and **SRTP_AES_CM_128_SHA1_80** was used as the Crypto Suite.

**Note**: **RTCP** was left unencrypted as IP Office supports unencrypted RTCP by default. This default is compatible with most Avaya endpoints which do not currently support encrypted RTCP.



Media: Enforced

□ Strict SIPS

Media Security Options

Encryptions: ☑ RTP □ RTCP

Authentication: ☑ RTP ☑ RTCP

Replay Protection

SRTP Window Size: 64

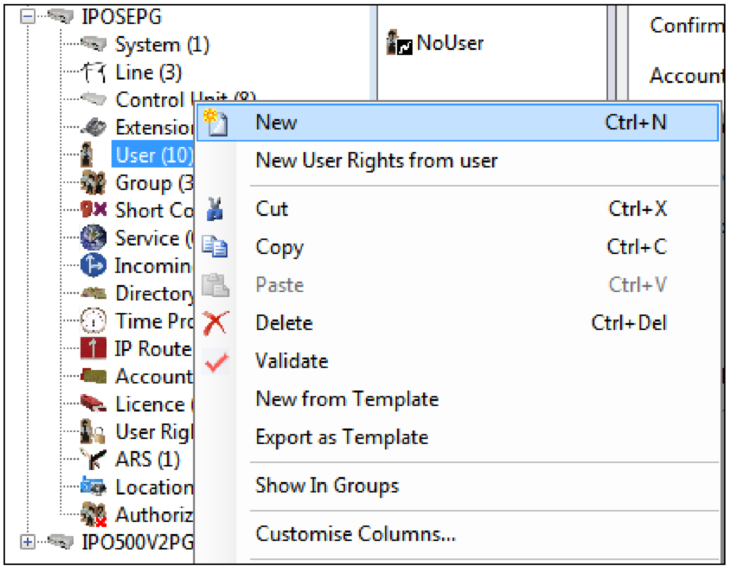
Crypto Suites

☑ SRTP_AES_CM_128_SHA1_80

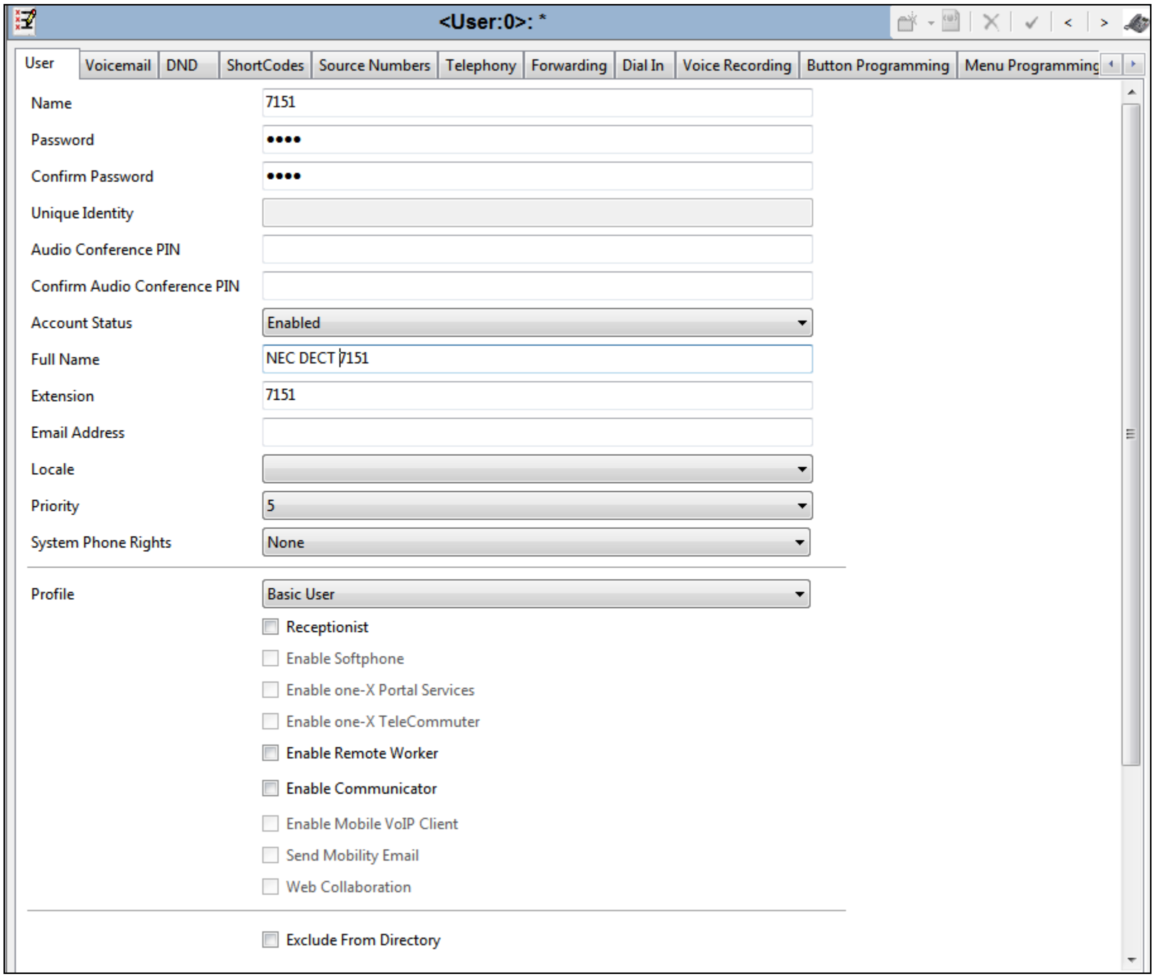
□ SRTP_AES_CM_128_SHA1_32

## 5.4. Create a new User

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



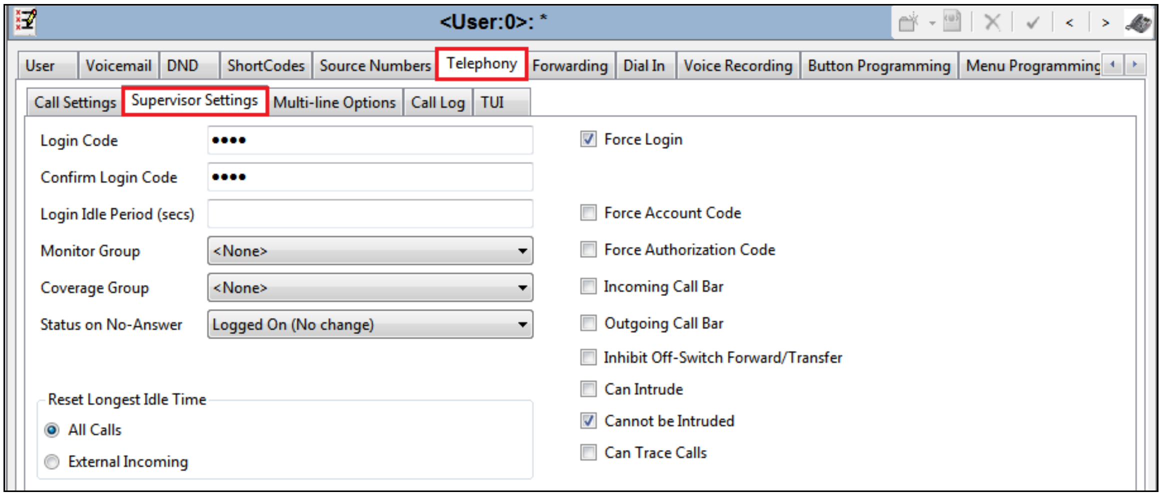
In the **User** tab add a **Name** and **Password** along with the **Extension**.



| | |
|---|---|
| Name | 7151 |
| Password | •••• |
| Confirm Password | •••• |
| Unique Identity | |
| Audio Conference PIN | |
| Confirm Audio Conference PIN | |
| Account Status | Enabled |
| Full Name | NEC DECT 7151 |
| Extension | 7151 |
| Email Address | |
| Locale | |
| Priority | 5 |
| System Phone Rights | None |
| Profile | Basic User |

□ Receptionist
□ Enable Softphone
□ Enable one-X Portal Services
□ Enable one-X TeleCommuter
□ Enable Remote Worker
□ Enable Communicator
□ Enable Mobile VoIP Client
□ Send Mobility Email
□ Web Collaboration
□ Exclude From Directory

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



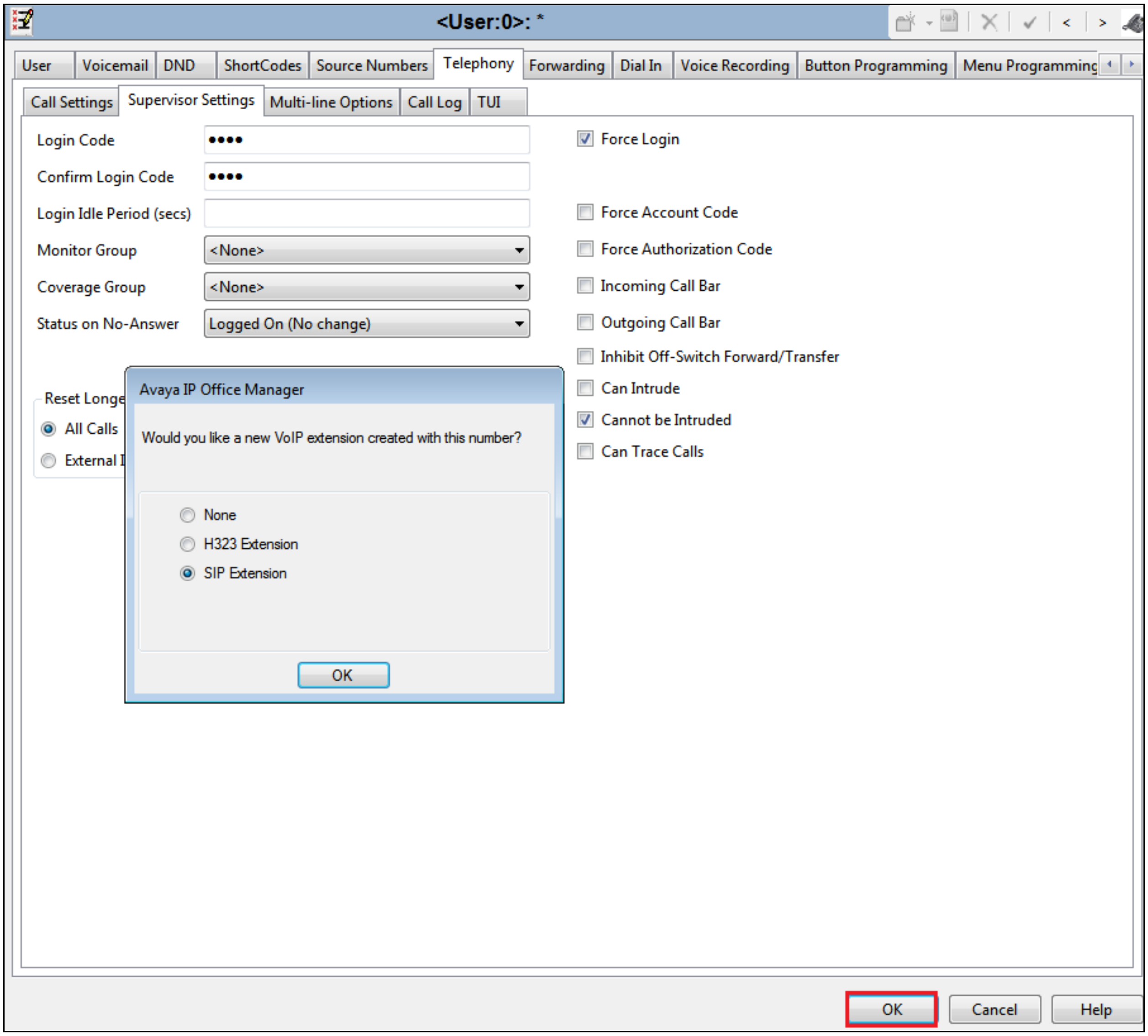
| | |
|---|---|
| Login Code | •••• |
| Confirm Login Code | •••• |
| Login Idle Period (secs) | |
| Monitor Group | <None> |
| Coverage Group | <None> |
| Status on No-Answer | Logged On (No change) |

Reset Longest Idle Time
● All Calls
○ External Incoming

☑ Force Login
□ Force Account Code
□ Force Authorization Code
□ Incoming Call Bar
□ Outgoing Call Bar
□ Inhibit Off-Switch Forward/Transfer
□ Can Intrude
☑ Cannot be Intruded
□ Can Trace Calls

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).



| | |
|---|---|
| Login Code | •••• |
| Confirm Login Code | •••• |
| Login Idle Period (secs) | |
| Monitor Group | <None> |
| Coverage Group | <None> |
| Status on No-Answer | Logged On (No change) |

- ☑ Force Login
- □ Force Account Code
- □ Force Authorization Code
- □ Incoming Call Bar
- □ Outgoing Call Bar
- □ Inhibit Off-Switch Forward/Transfer
- □ Can Intrude
- ☑ Cannot be Intruded
- □ Can Trace Calls

Reset Longe

- ● All Calls
- ○ External I

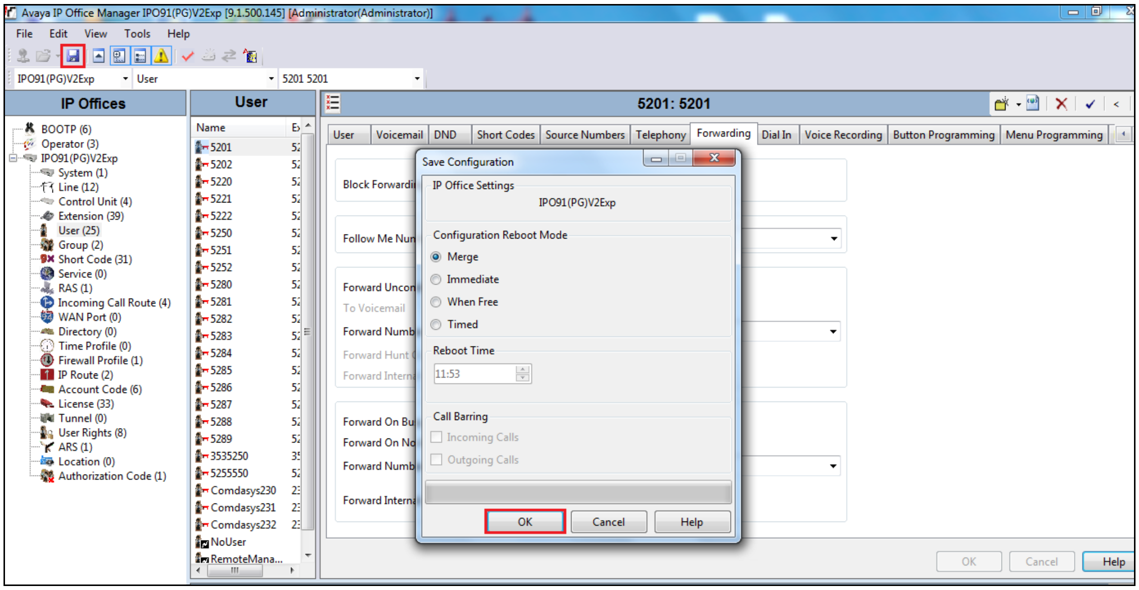
Avaya IP Office Manager

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

- ○ None
- ○ H323 Extension
- ● SIP Extension

## 5.5. 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.



Save Configuration

IP Office Settings

IPO91(PG)V2Exp

Configuration Reboot Mode

● Merge

○ Immediate

○ When Free

○ Timed

Reboot Time

11:53

Call Barring

□ Incoming Calls

□ Outgoing Calls

# 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**.

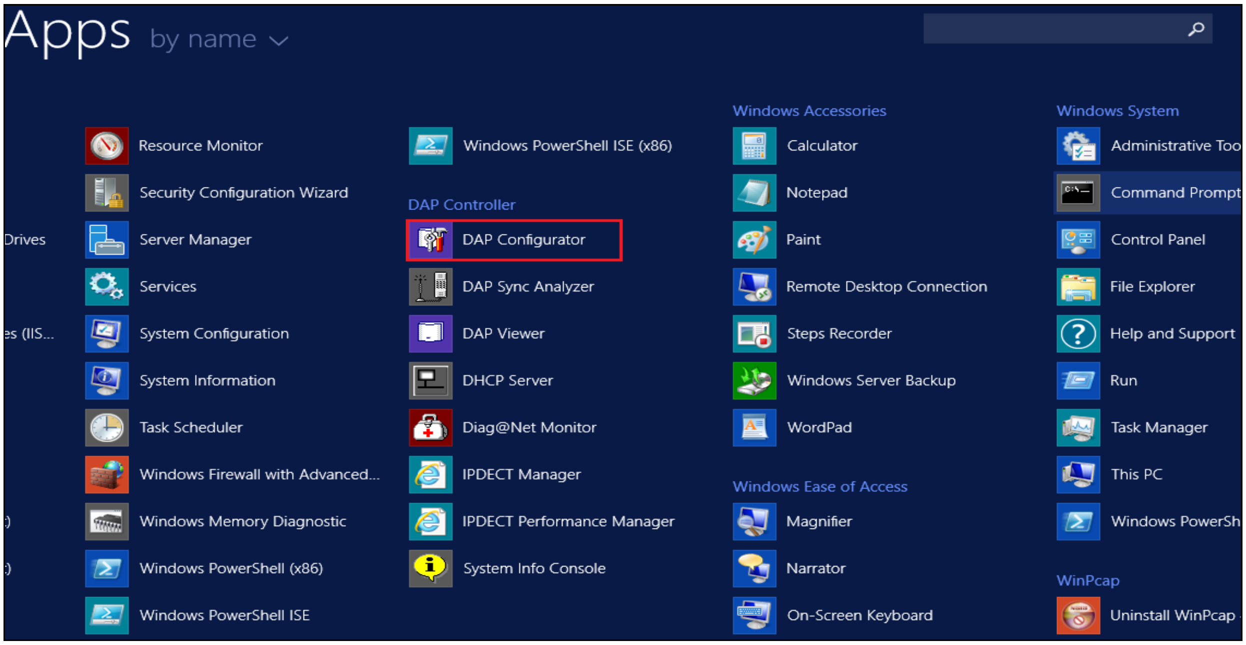
**Note:** The NEC IP DECT solution relies on DHCP (Option 66, 67), NTP and TFTP as network-services. DHCP and TFTP services can be provided from the DAP controller instance. In addition a Multi-Cast IP address is also required for the DAP´s to synch.

## 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 this pushed to each DAP on the network. Click on DAP Configurator as shown below.

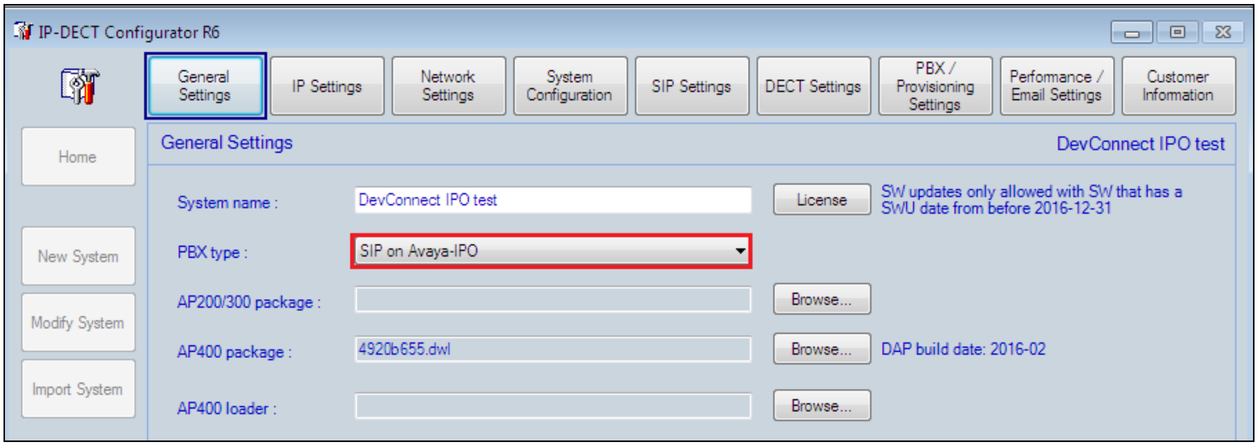
**Note**: An NEC IP DECT solution typically consists of a windows based instance called DAP Controller which includes “DAP Configurator” and “DAP Manager”.

**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.



System name : DevConnect IPO test

SW updates only allowed with SW that has a SWU date from before 2016-12-31

PBX type : SIP on Avaya-IPO

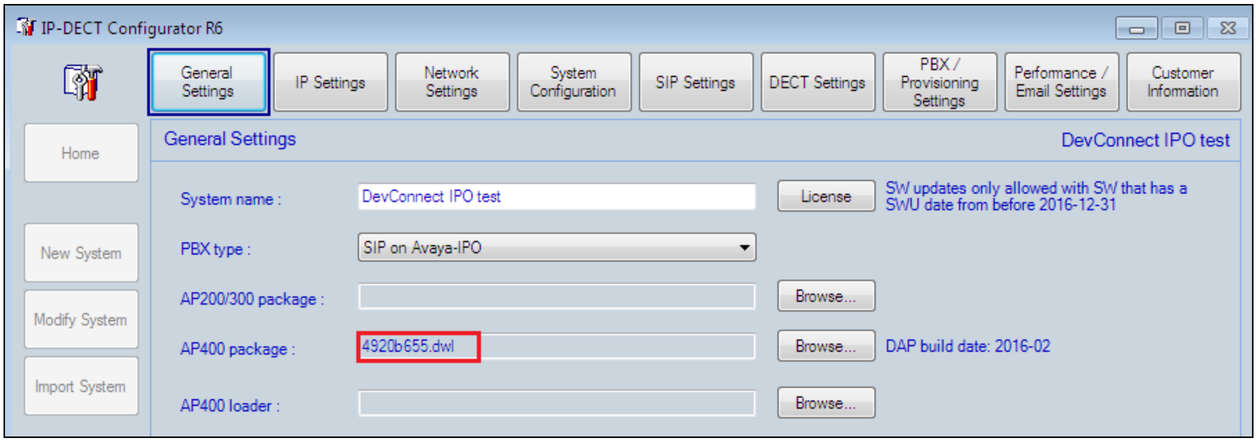
AP200/300 package :

AP400 package : 4920b655.dwl

DAP build date: 2016-02

AP400 loader :

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).



System name : DevConnect IPO test

SW updates only allowed with SW that has a SWU date from before 2016-12-31

PBX type : SIP on Avaya-IPO

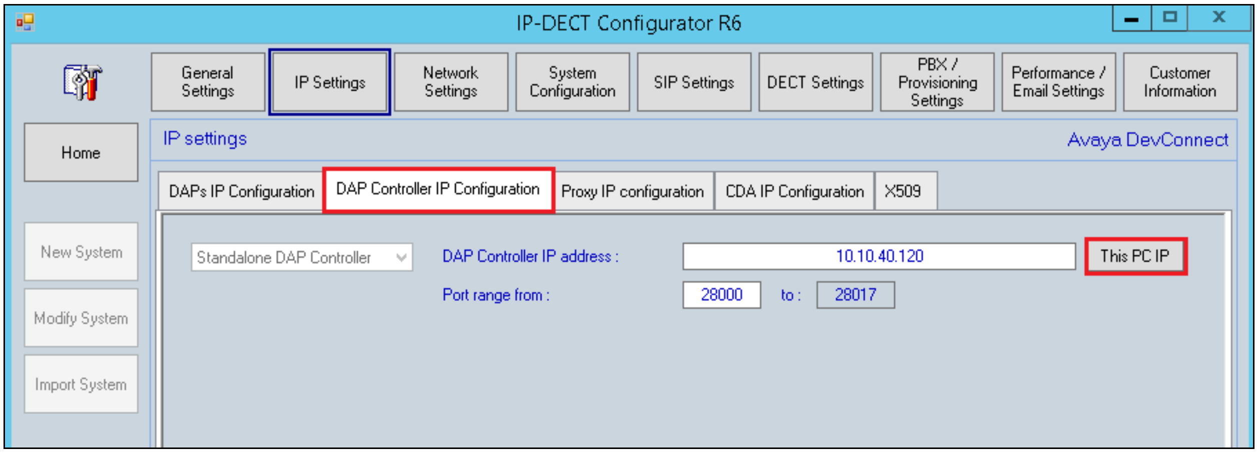
AP200/300 package :

AP400 package : 4920b655.dwl

DAP build date: 2016-02

AP400 loader :

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.

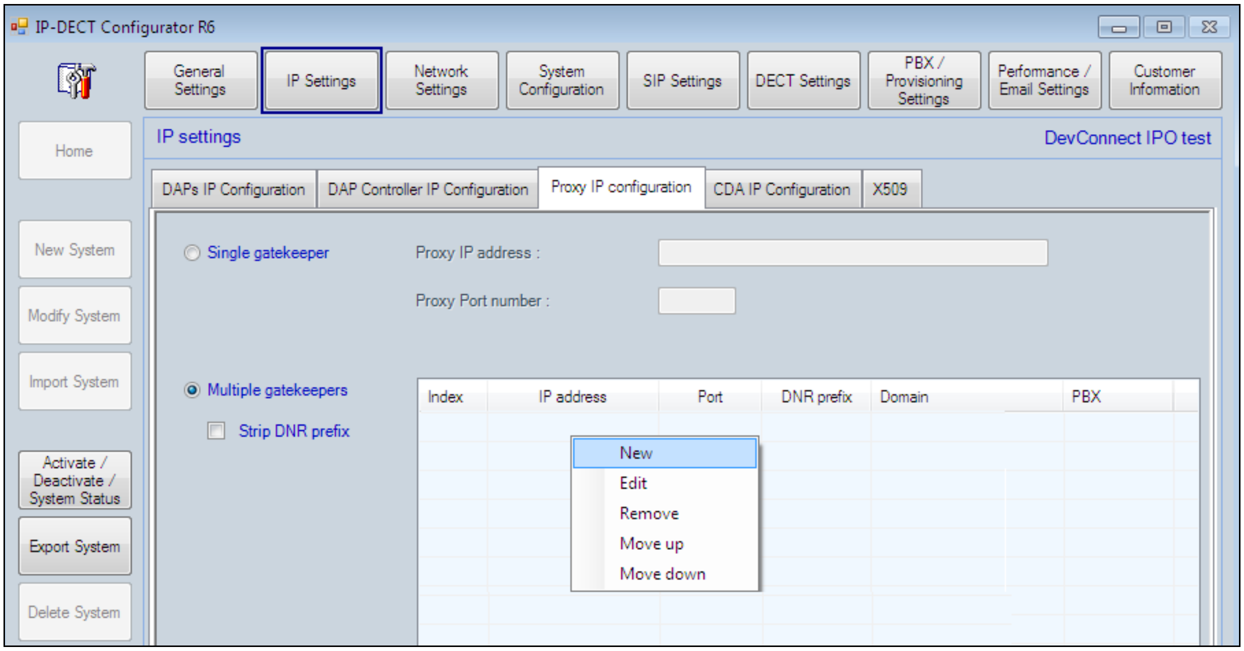


Standalone DAP Controller

DAP Controller IP address : 10.10.40.120

Port range from : 28000 to : 28017

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.



○ Single gatekeeper

Proxy IP address :

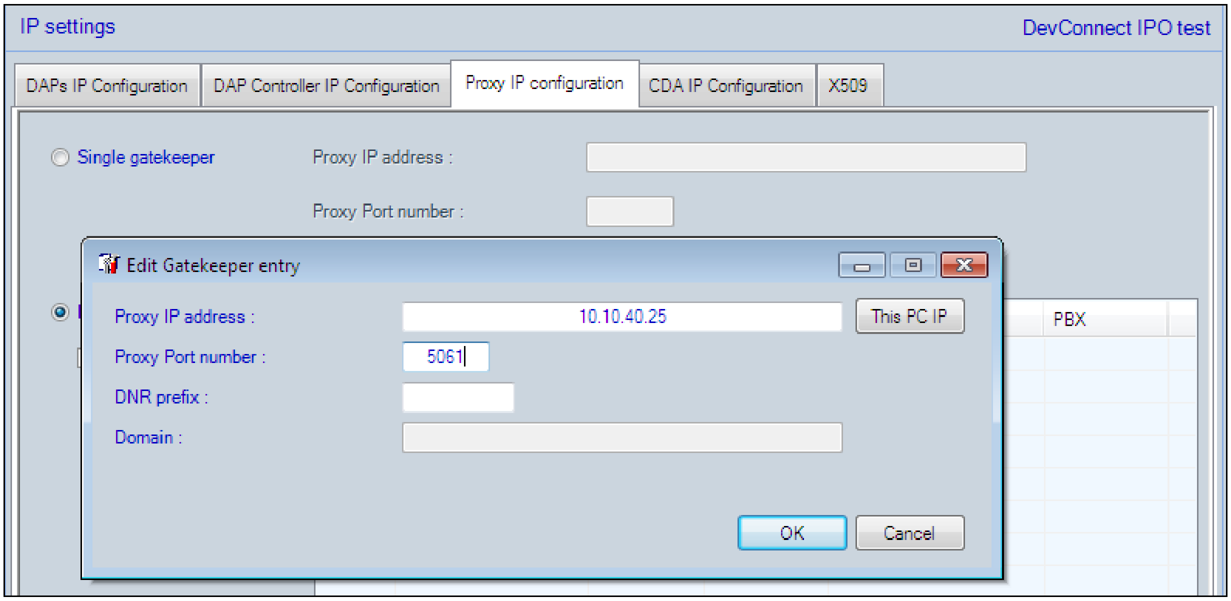
Proxy Port number :

● Multiple gatekeepers

□ Strip DNR prefix

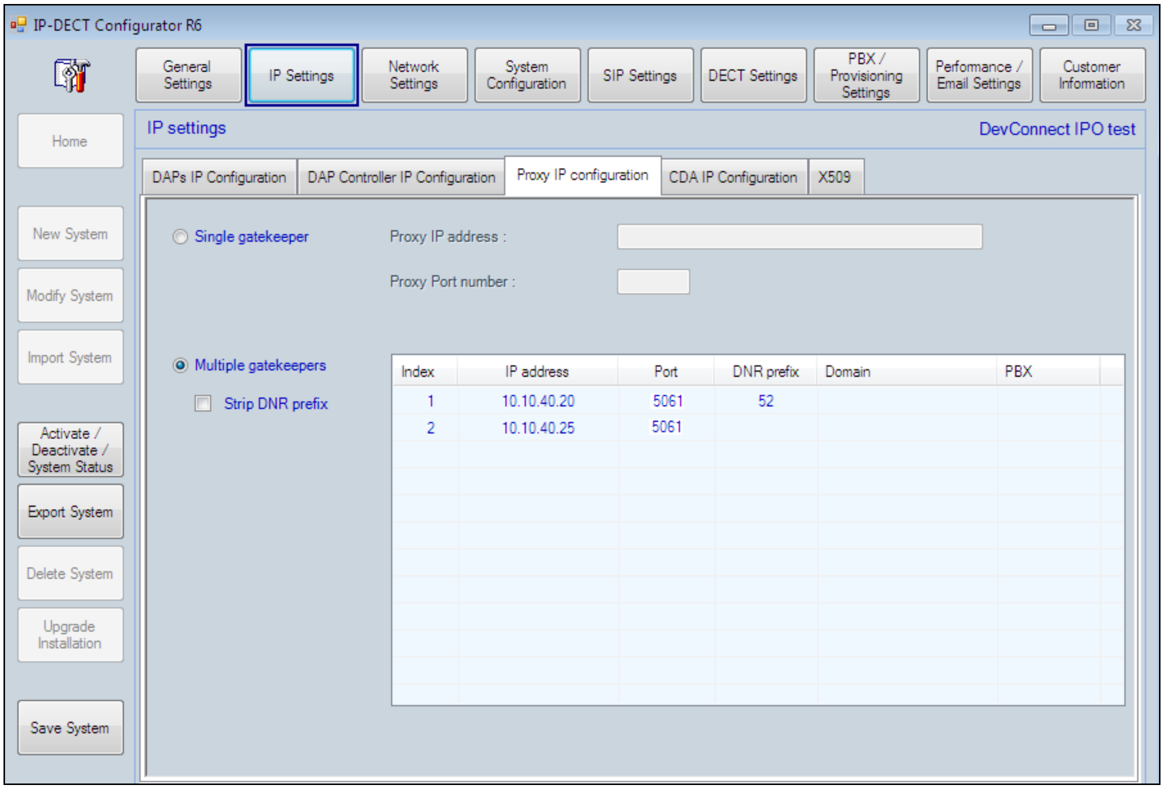
| Index | IP address | Port | DNR prefix | Domain | PBX |
|---|---|---|---|---|---|

A new window is opened where the IP Address of the IP Office is entered for the **Proxy IP address** and **5061** as the **Proxy Port number** as this is the port number used for TLS. This port will be the same as configured in IP Office. Repeat the same process for the IP Office 500 V2.



Proxy IP address : 10.10.40.25
Proxy Port number : 5061
DNR prefix :
Domain :

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.

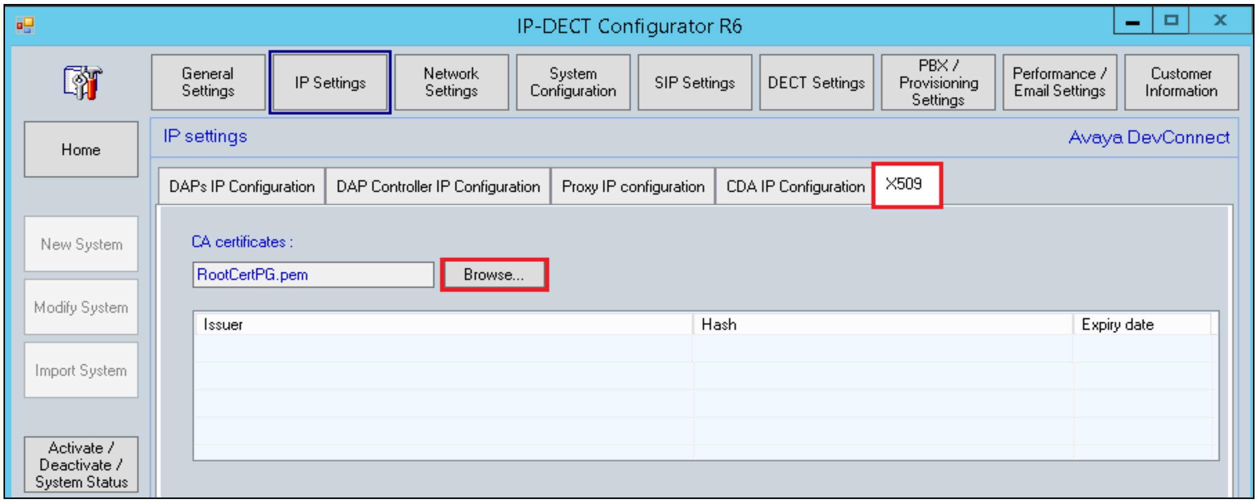


○ Single gatekeeper
Proxy IP address :
Proxy Port number :

● Multiple gatekeepers
□ Strip DNR prefix

| Index | IP address | Port | DNR prefix | Domain | PBX |
|---|---|---|---|---|---|
| 1 | 10.10.40.20 | 5061 | 52 | | |
| 2 | 10.10.40.25 | 5061 | | | |

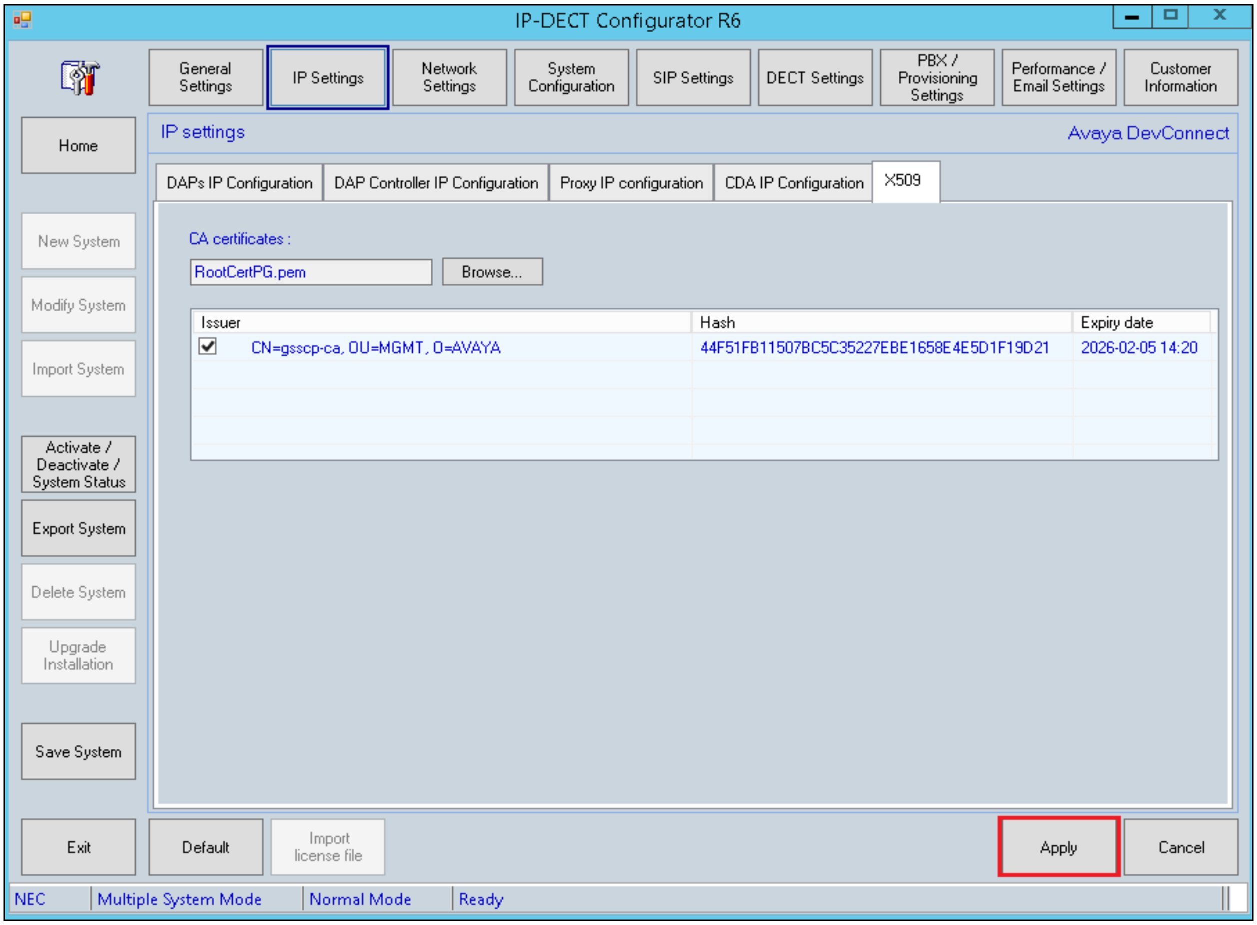
Click on the **X509** tab and import the Root Cert into the DAP Controller. This will be the same root cert that is being used on IP Office so as when the DAP sends the cert to IP Office it is the correct cert that is being sent.



CA certificates : RootCertPG.pem

| Issuer | Hash | Expiry date |
|---|---|---|

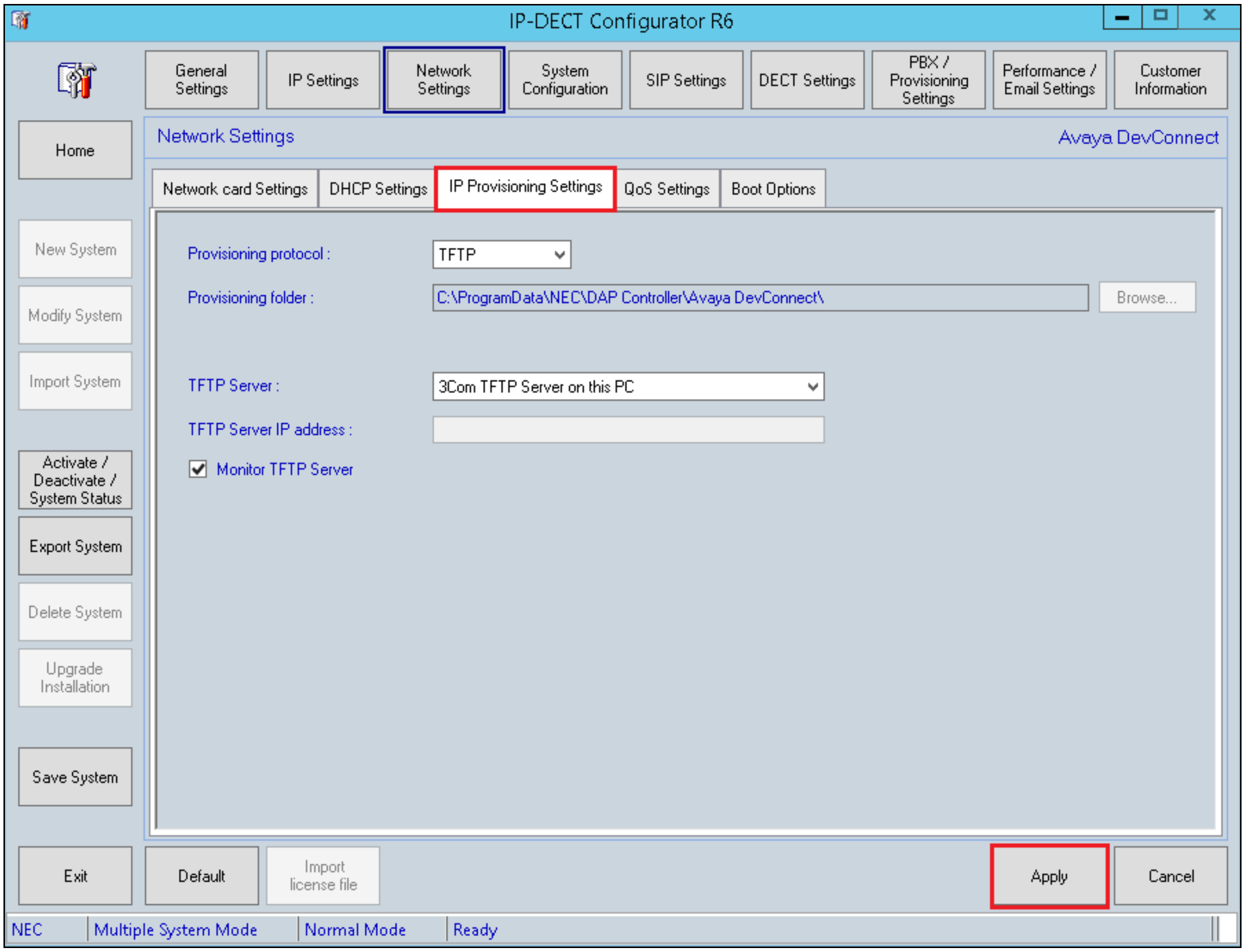
The following shows the imported cert information, click on **Apply** once done.



CA certificates : RootCertPG.pem

| Issuer | Hash | Expiry date |
|---|---|---|
| ☑ CN=gsscp-ca, OU=MGMT, O=AVAYA | 44F51FB11507BC5C35227EBE1658E4E5D1F19D21 | 2026-02-05 14:20 |

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.



Provisioning protocol : TFTP

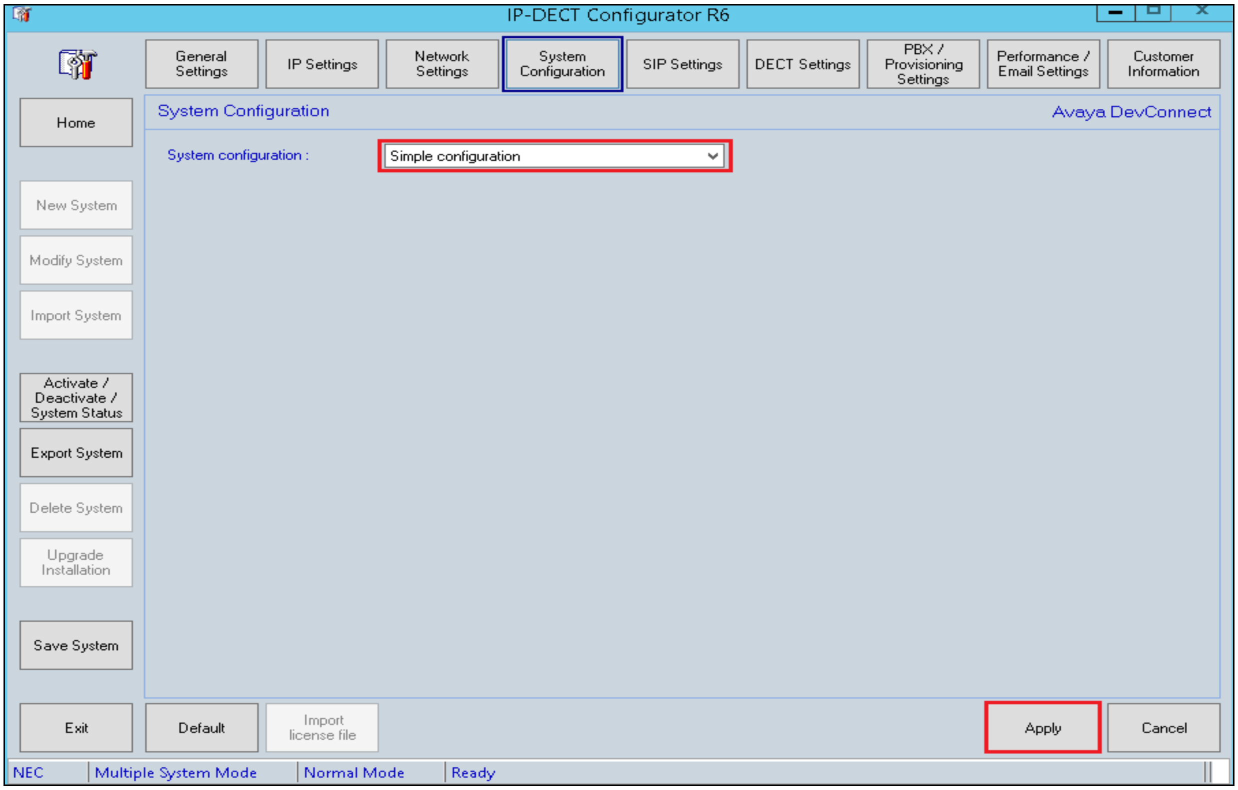
Provisioning folder : C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\

TFTP Server : 3Com TFTP Server on this PC

TFTP Server IP address :

☑ Monitor TFTP Server

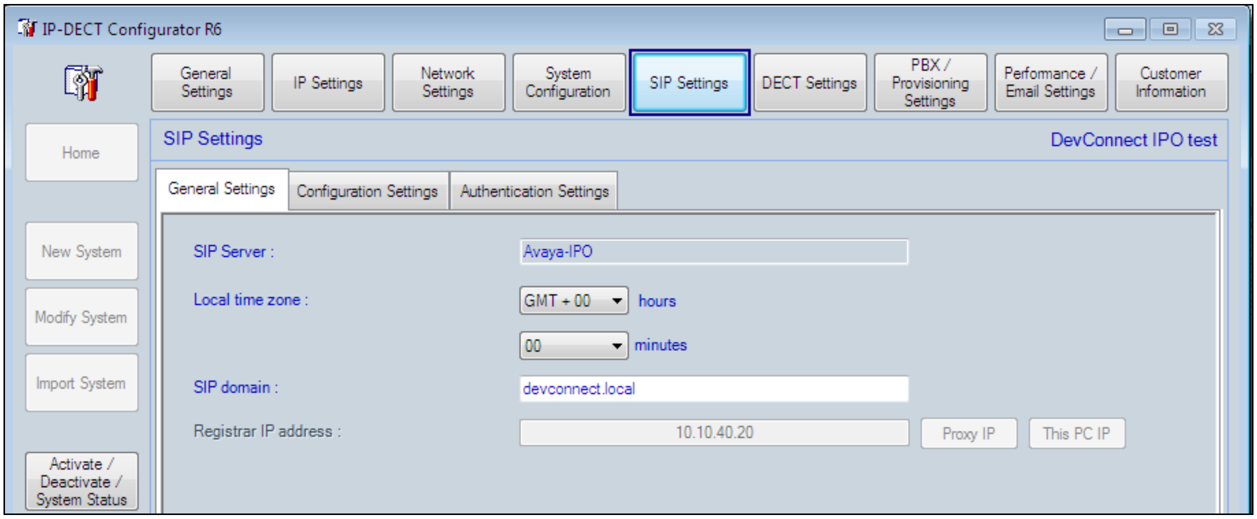
Click on **System Configuration** at the top of the page, the **System configuration** in the main window should display **Simple configuration** as shown below, click on **Apply** to continue.



System Configuration — Avaya DevConnect

System configuration : Simple configuration

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 **Local 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).



SIP Settings — DevConnect IPO test

SIP Server : Avaya-IPO

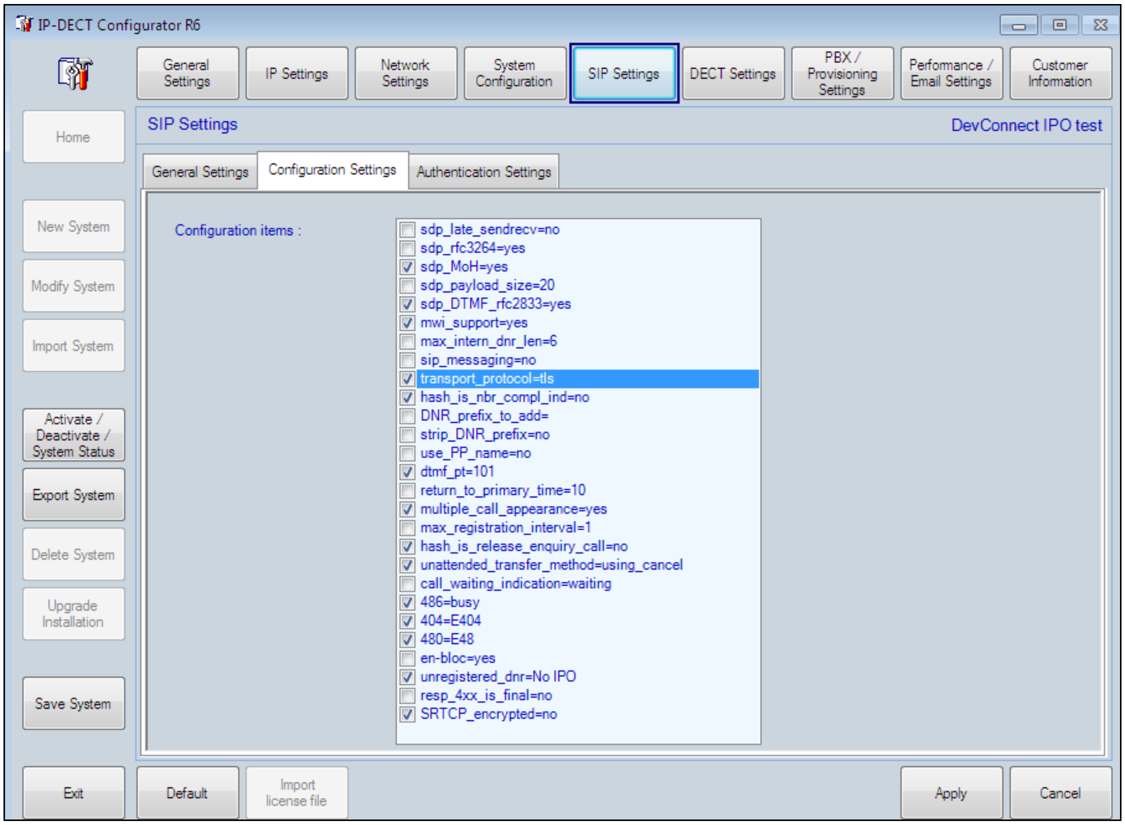
Local time zone : GMT + 00 hours

00 minutes

SIP domain : devconnect.local

Registrar IP address : 10.10.40.20

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 **TLS** is being used and the **mwi_support=yes**. These settings can be changed here.

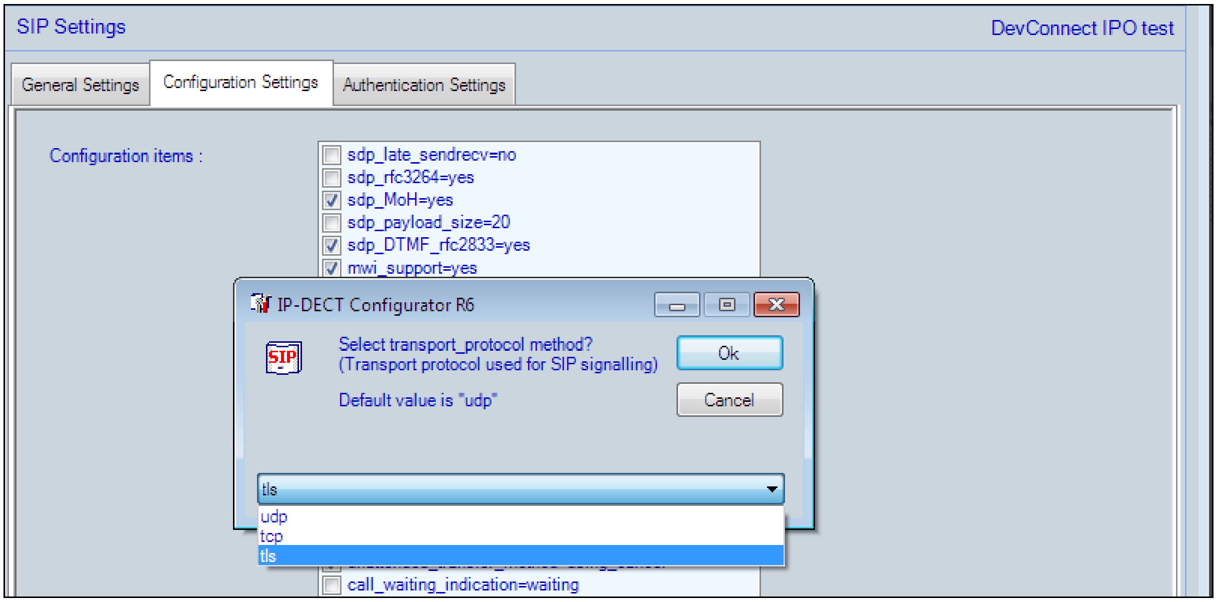


SIP Settings    DevConnect IPO test

Configuration items :

- ☐ sdp_late_sendrecv=no
- ☐ sdp_rfc3264=yes
- ☑ sdp_MoH=yes
- ☐ sdp_payload_size=20
- ☑ sdp_DTMF_rfc2833=yes
- ☑ mwi_support=yes
- ☐ max_intern_dnr_len=6
- ☐ sip_messaging=no
- ☑ transport_protocol=tls
- ☑ hash_is_nbr_compl_ind=no
- ☐ DNR_prefix_to_add=
- ☐ strip_DNR_prefix=no
- ☐ use_PP_name=no
- ☑ dtmf_pt=101
- ☐ return_to_primary_time=10
- ☑ multiple_call_appearance=yes
- ☐ max_registration_interval=1
- ☑ hash_is_release_enquiry_call=no
- ☑ unattended_transfer_method=using_cancel
- ☐ call_waiting_indication=waiting
- ☑ 486=busy
- ☑ 404=E404
- ☑ 480=E48
- ☐ en-bloc=yes
- ☑ unregistered_dnr=No IPO
- ☐ resp_4xx_is_final=no
- ☑ SRTCP_encrypted=no

To change the protocol, simply click on **transport_protocol** and select the correct protocol.



SIP Settings    DevConnect IPO test

Configuration items :

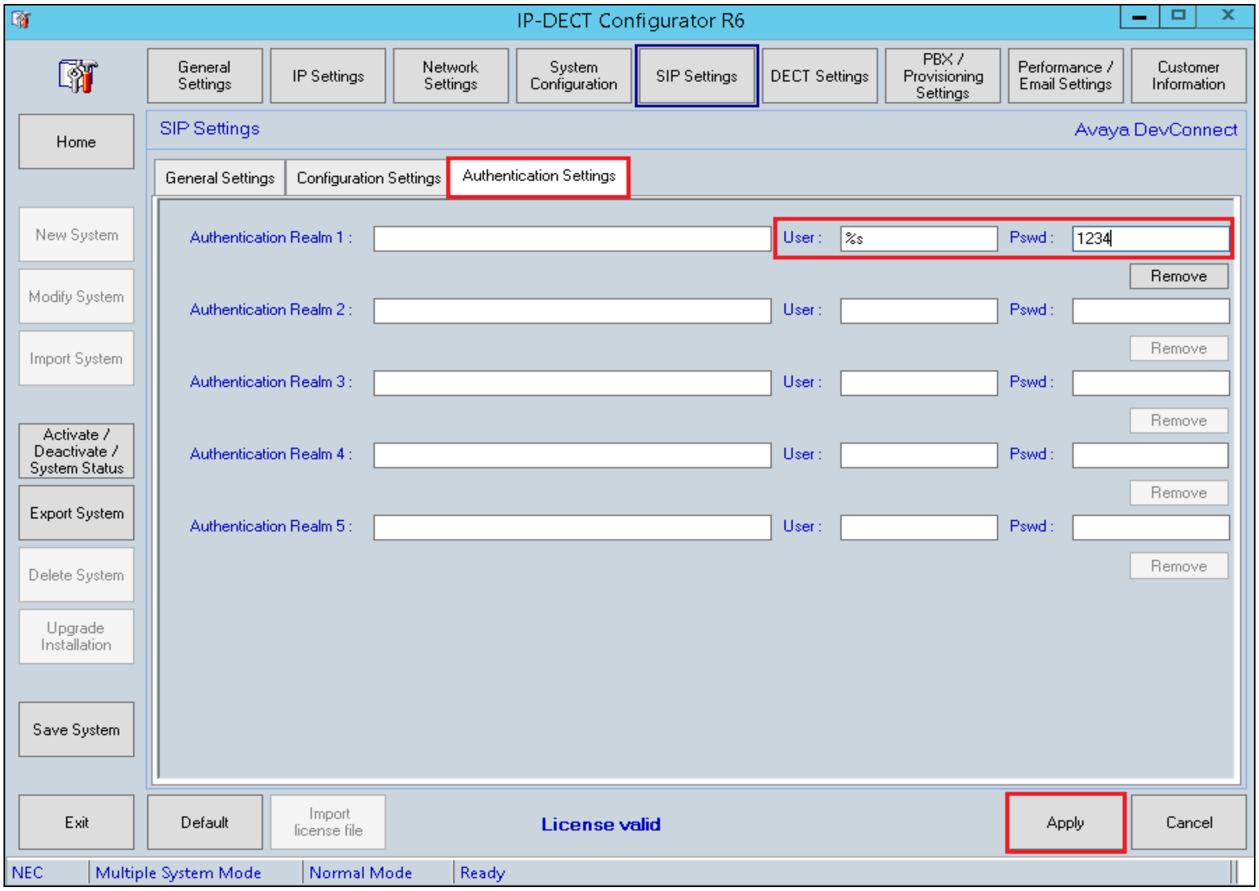
- ☐ sdp_late_sendrecv=no
- ☐ sdp_rfc3264=yes
- ☑ sdp_MoH=yes
- ☐ sdp_payload_size=20
- ☑ sdp_DTMF_rfc2833=yes
- ☑ mwi_support=yes
- ☐ call_waiting_indication=waiting

Select transport_protocol method?
(Transport protocol used for SIP signalling)

Default value is "udp"

tls

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 5.4**.



IP-DECT Configurator R6

SIP Settings — Authentication Settings

Authentication Realm 1 : User : %s Pswd : 1234

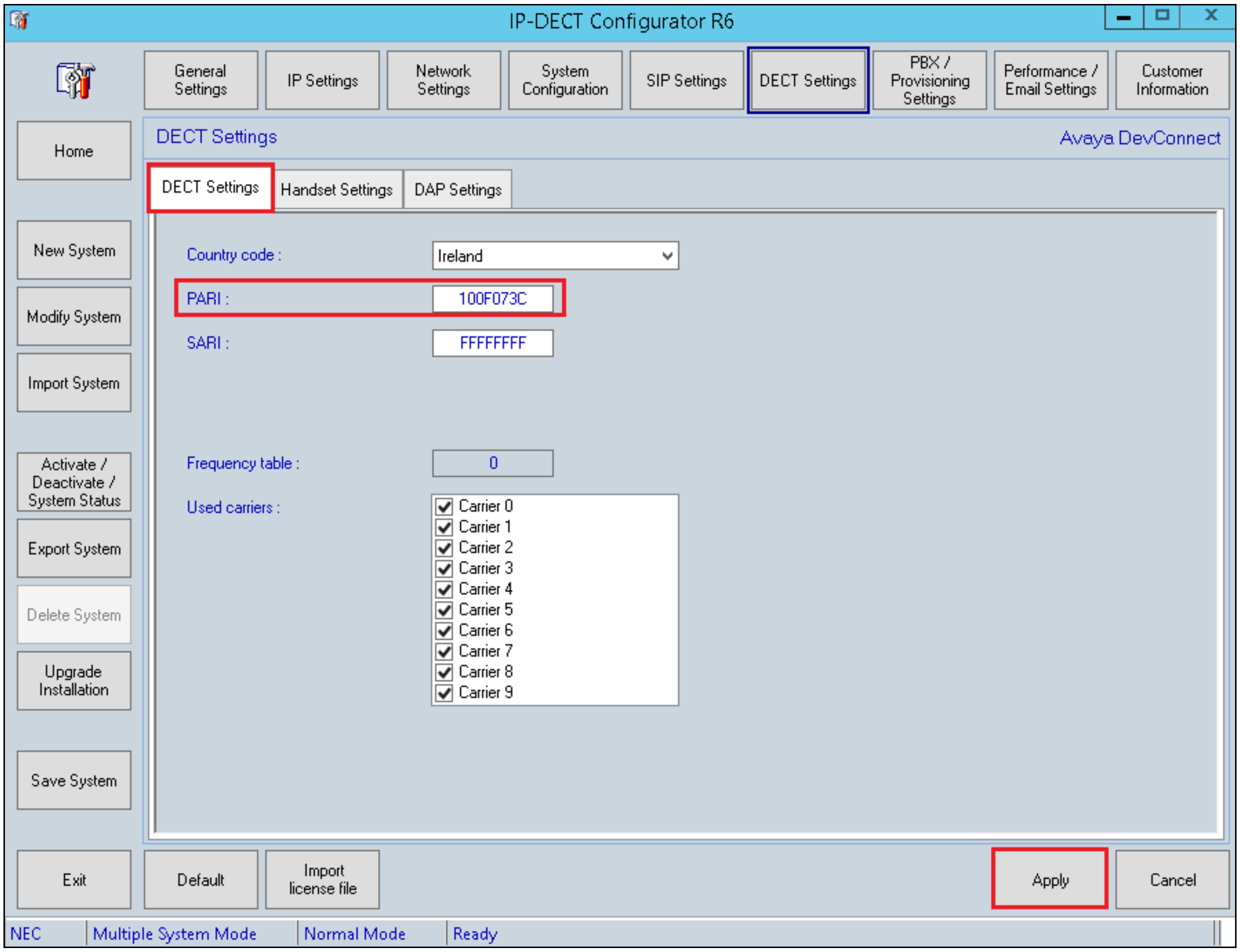
Authentication Realm 2 : User : Pswd :

Authentication Realm 3 : User : Pswd :

Authentication Realm 4 : User : Pswd :

Authentication Realm 5 : User : Pswd :

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.



Country code : Ireland

PARI : 100F073C

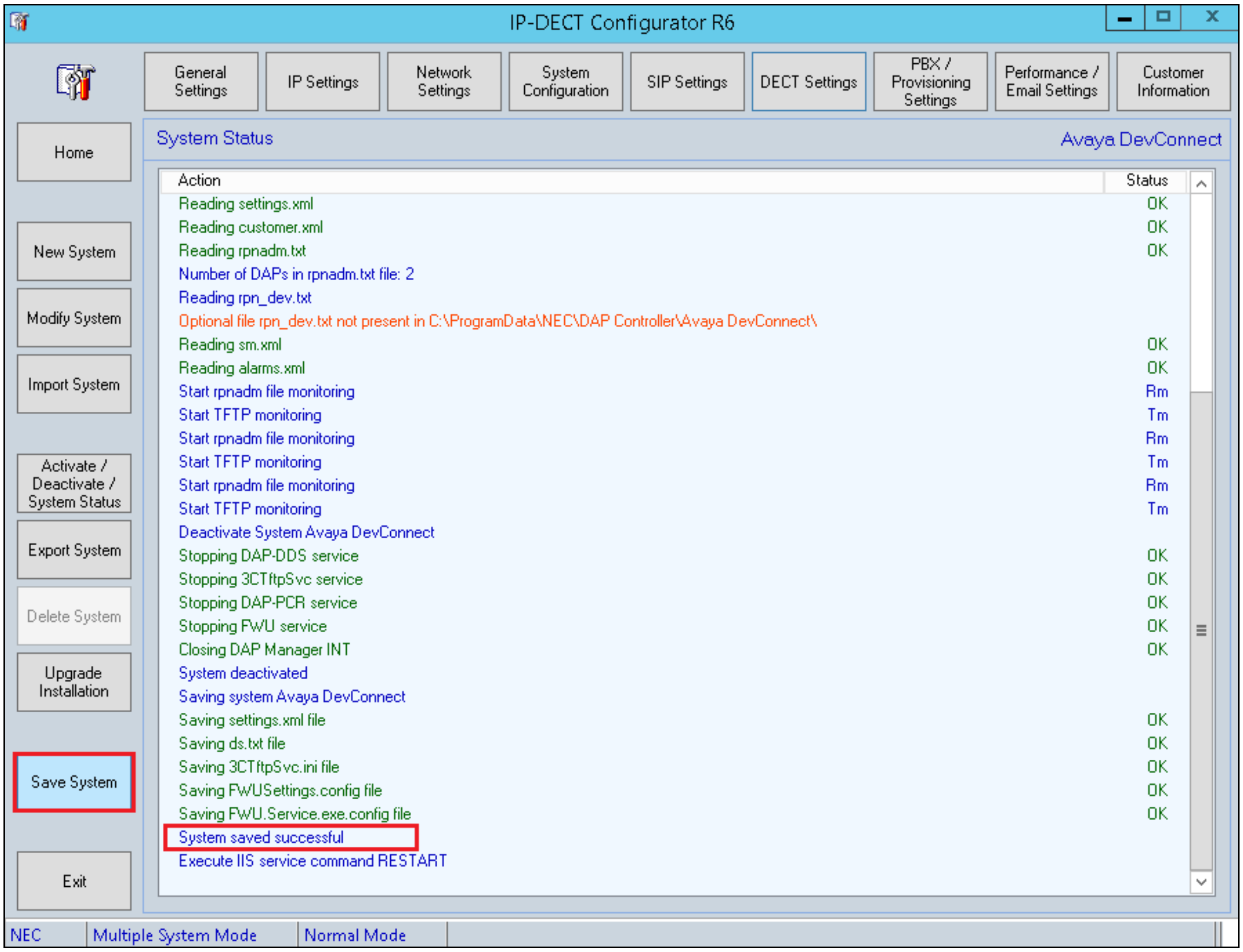
SARI : FFFFFFFF

Frequency table : 0

Used carriers :
☑ Carrier 0
☑ Carrier 1
☑ Carrier 2
☑ Carrier 3
☑ Carrier 4
☑ Carrier 5
☑ Carrier 6
☑ Carrier 7
☑ Carrier 8
☑ Carrier 9

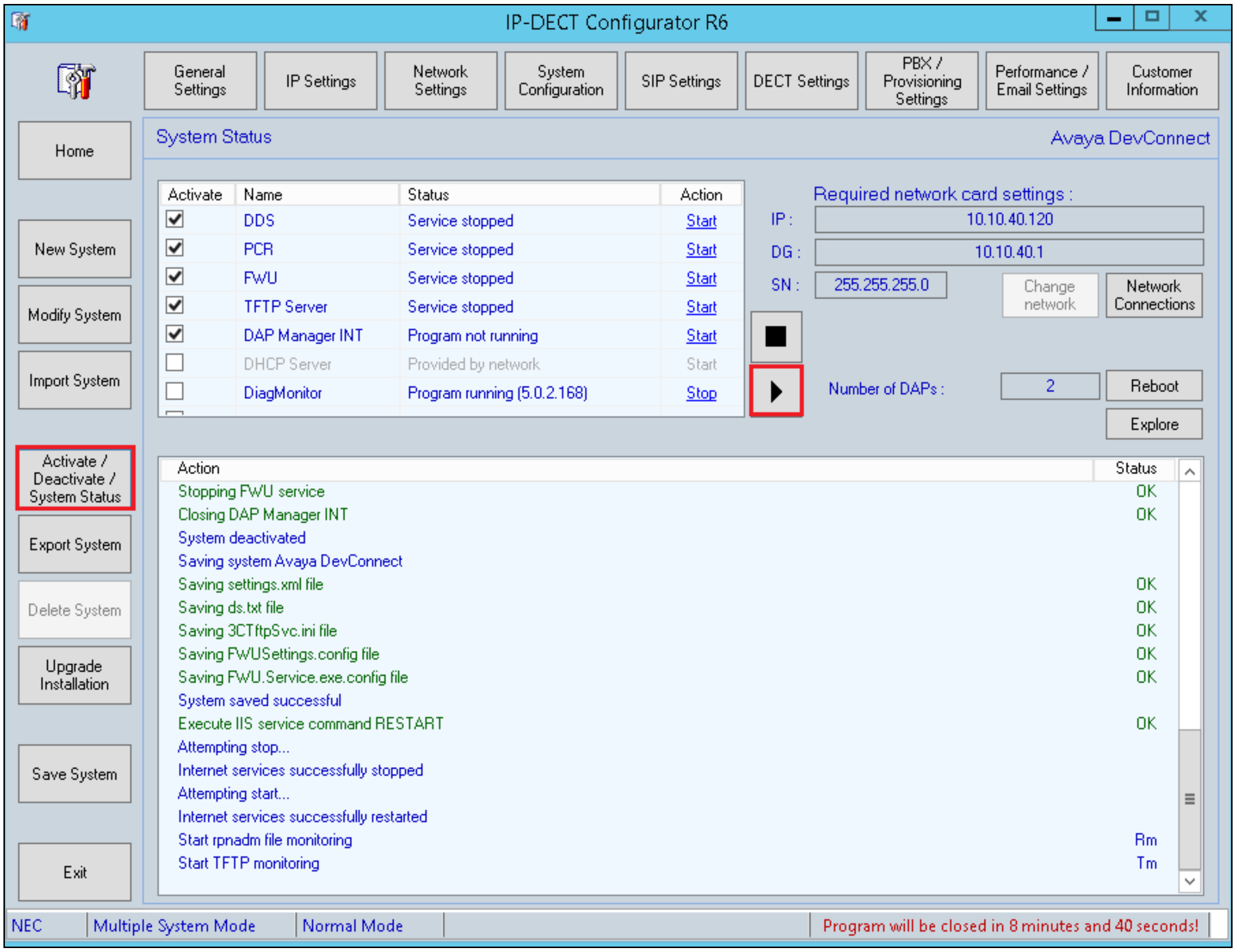
NEC | Multiple System Mode | Normal Mode | Ready

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**.



```
Action                                                                                Status
Reading settings.xml                                                                  OK
Reading customer.xml                                                                  OK
Reading rpnadm.txt                                                                    OK
Number of DAPs in rpnadm.txt file: 2
Reading rpn_dev.txt
Optional file rpn_dev.txt not present in C:\ProgramData\NEC\DAP Controller\Avaya DevConnect\
Reading sm.xml                                                                        OK
Reading alarms.xml                                                                    OK
Start rpnadm file monitoring                                                          Rm
Start TFTP monitoring                                                                 Tm
Start rpnadm file monitoring                                                          Rm
Start TFTP monitoring                                                                 Tm
Start rpnadm file monitoring                                                          Rm
Start TFTP monitoring                                                                 Tm
Deactivate System Avaya DevConnect
Stopping DAP-DDS service                                                              OK
Stopping 3CTftpSvc service                                                            OK
Stopping DAP-PCR service                                                              OK
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
```

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.



System Status — Avaya DevConnect

| Activate | Name | Status | Action |
|---|---|---|---|
| ☑ | DDS | Service stopped | Start |
| ☑ | PCR | Service stopped | Start |
| ☑ | FWU | Service stopped | Start |
| ☑ | TFTP Server | Service stopped | Start |
| ☑ | DAP Manager INT | Program not running | Start |
| □ | DHCP Server | Provided by network | Start |
| □ | DiagMonitor | Program running (5.0.2.168) | Stop |

Required network card settings :

IP : 10.10.40.120

DG : 10.10.40.1

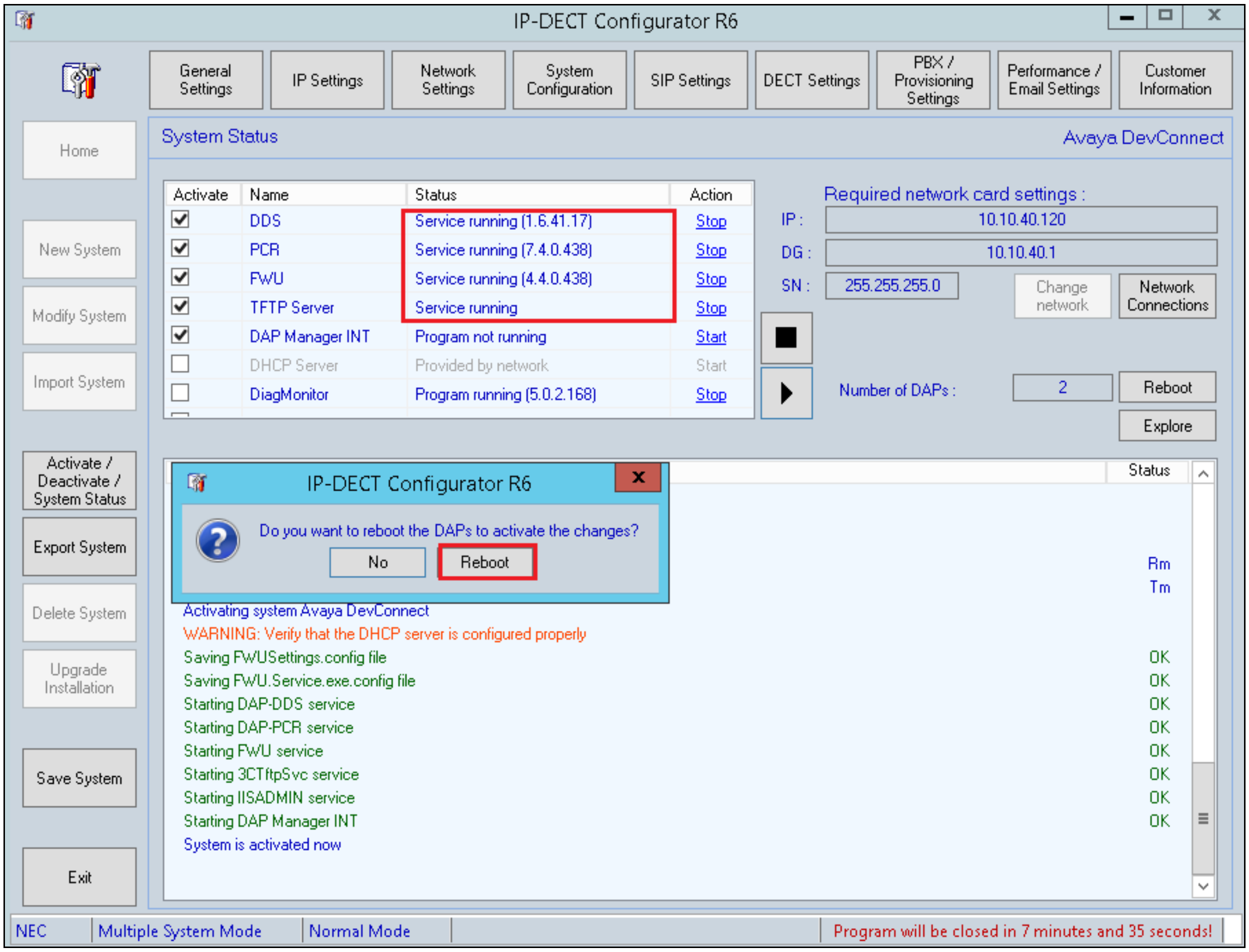
SN : 255.255.255.0

Number of DAPs : 2

| 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.



| Activate | Name | Status | Action |
|---|---|---|---|
| ☑ | DDS | Service running (1.6.41.17) | Stop |
| ☑ | PCR | Service running (7.4.0.438) | Stop |
| ☑ | FWU | Service running (4.4.0.438) | Stop |
| ☑ | TFTP Server | Service running | Stop |
| ☑ | DAP Manager INT | Program not running | Start |
| □ | DHCP Server | Provided by network | Start |
| □ | DiagMonitor | Program running (5.0.2.168) | Stop |

Required network card settings :

IP : 10.10.40.120

DG : 10.10.40.1

SN : 255.255.255.0

Number of DAPs : 2

IP-DECT Configurator R6

Do you want to reboot the DAPs to activate the changes?

No | Reboot

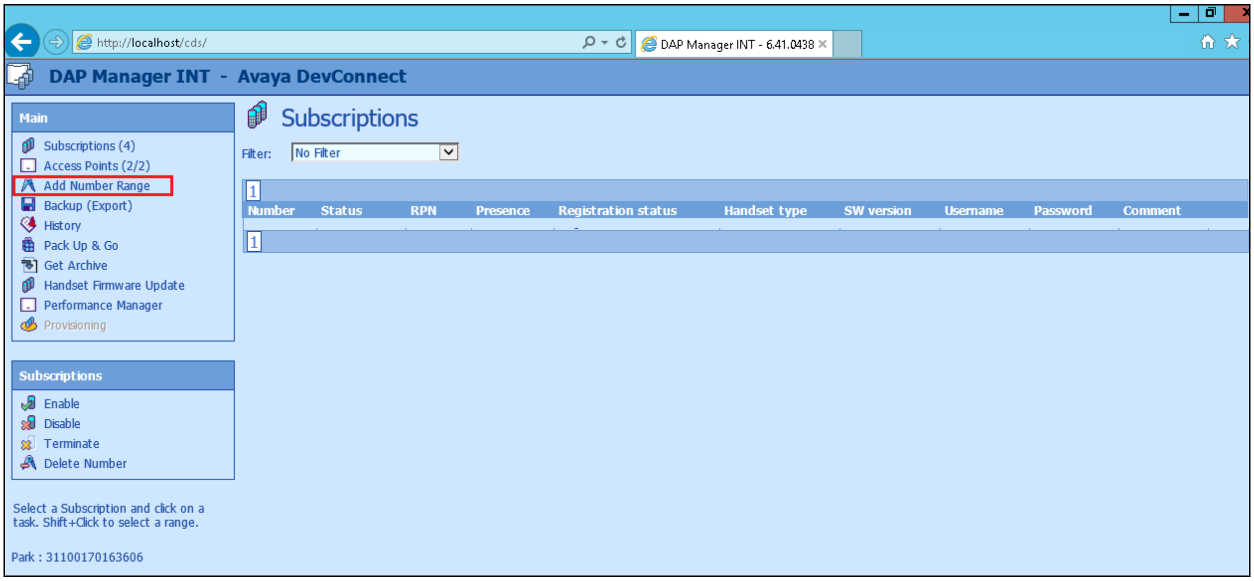
```
                                                          Rm
                                                          Tm
Activating system Avaya DevConnect
WARNING: Verify that the DHCP server is configured properly
Saving FWUSettings.config file                            OK
Saving FWU.Service.exe.config file                        OK
Starting DAP-DDS service                                  OK
Starting DAP-PCR service                                  OK
Starting FWU service                                      OK
Starting 3CTftpSvc service                                OK
Starting IISADMIN service                                 OK
Starting DAP Manager INT                                  OK
System is activated now
```

NEC | Multiple System Mode | Normal Mode | Program will be closed in 7 minutes and 35 seconds!

## 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.

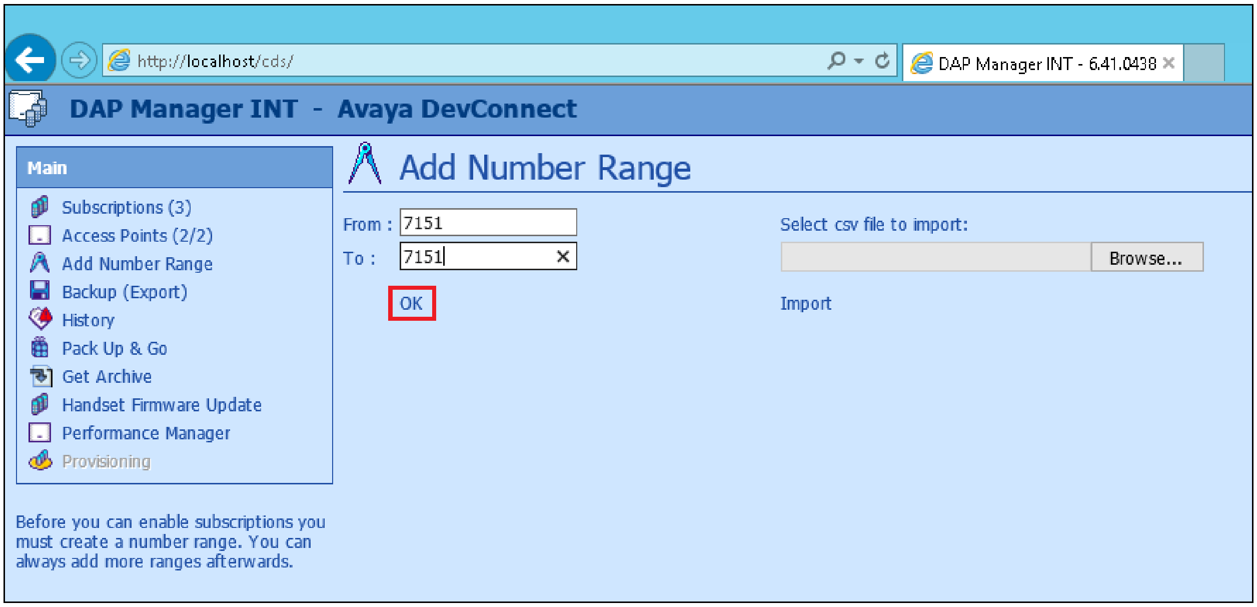
Click on **Add Number Range** in the left window.



Select a Subscription and click on a task. Shift+Click to select a range.

Park : 31100170163606

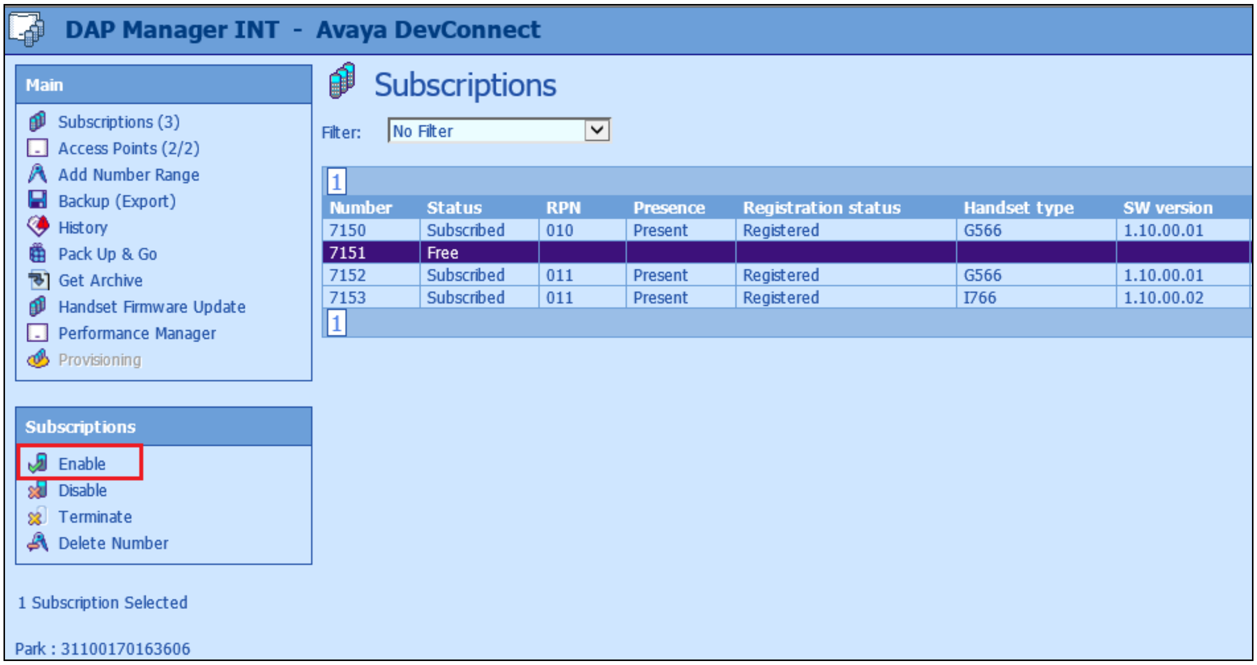
Enter the number range or the number of the extension(s) to be added and click on **OK**.



From : 7151
To : 7151

Before you can enable subscriptions you must create a number range. You can always add more ranges afterwards.

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



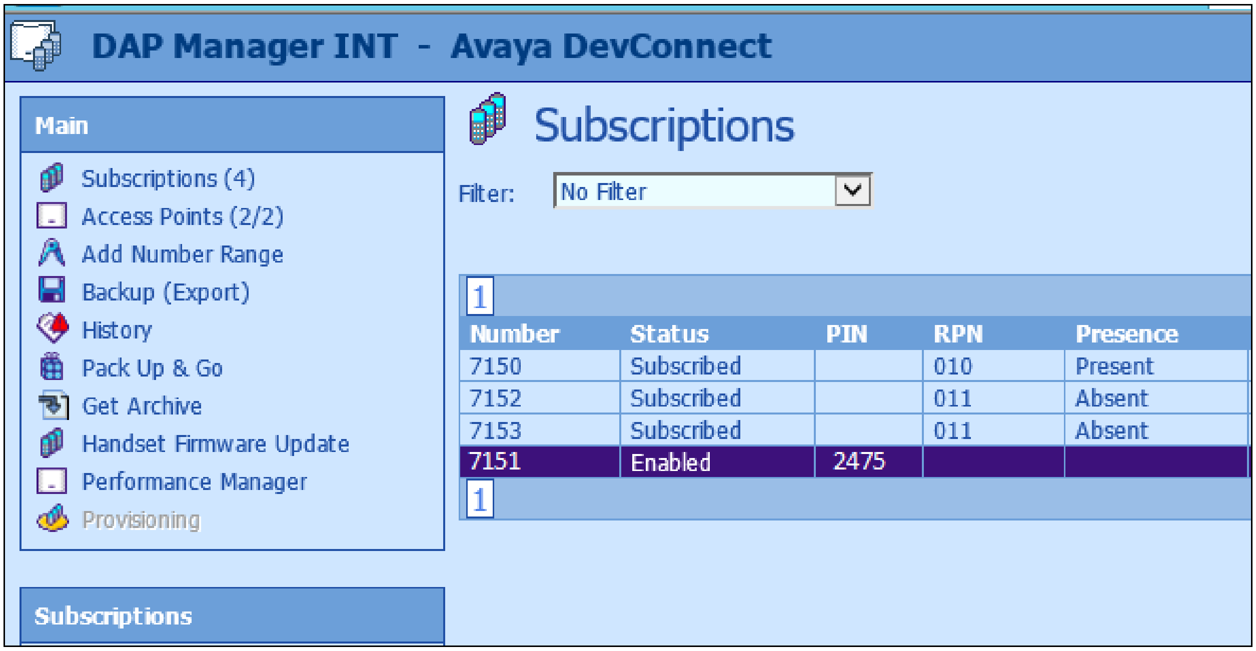
Filter: No Filter

| 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 |

1 Subscription Selected

Park : 31100170163606

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

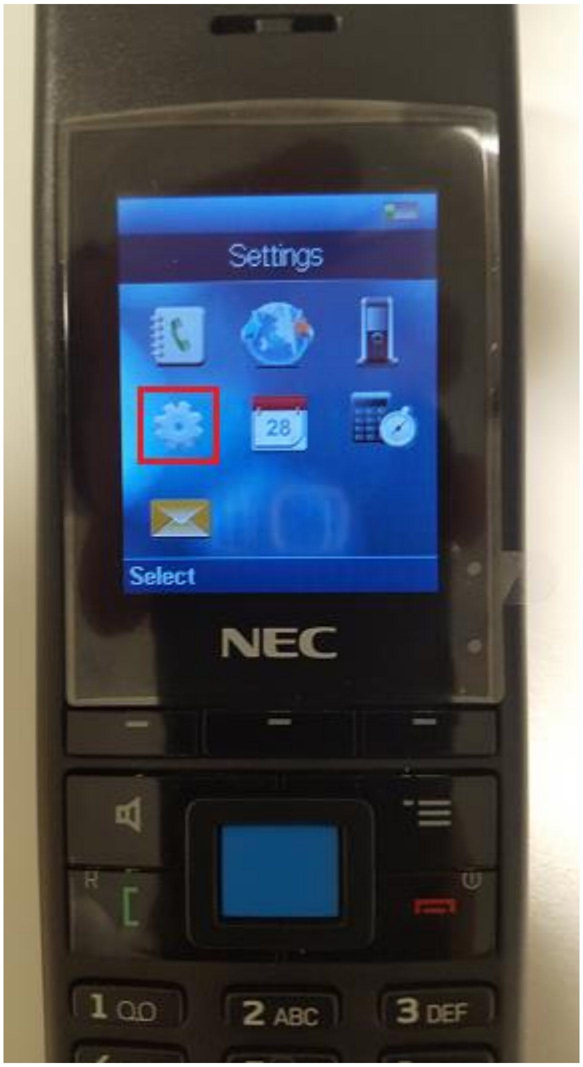


Filter: No Filter

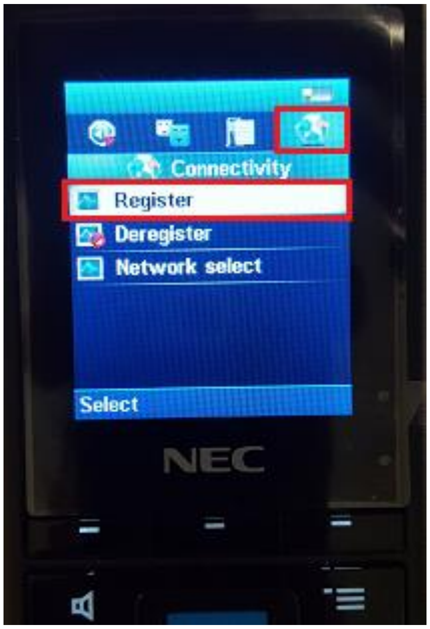
| Number | Status | PIN | RPN | Presence |
|---|---|---|---|---|
| 7150 | Subscribed | | 010 | Present |
| 7152 | Subscribed | | 011 | Absent |
| 7153 | Subscribed | | 011 | Absent |
| 7151 | Enabled | 2475 | | |

## 6.3. How to Subscribe the DECT Handset

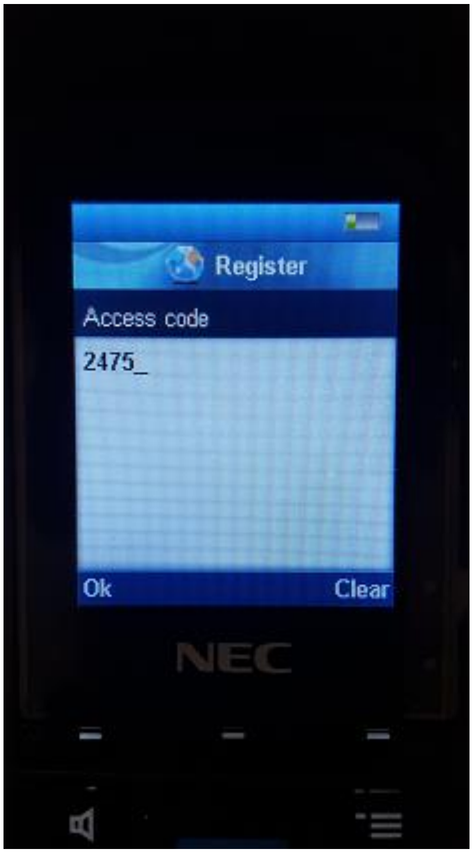
From the DECT handset click on the menu button (on top of the power button) and select **Settings** as highlighted below.



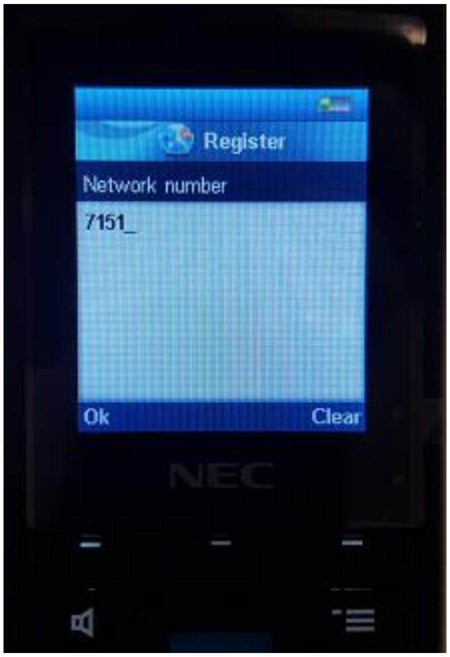
Scroll right to **Connectivity** and select **Register** as shown below.



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**.



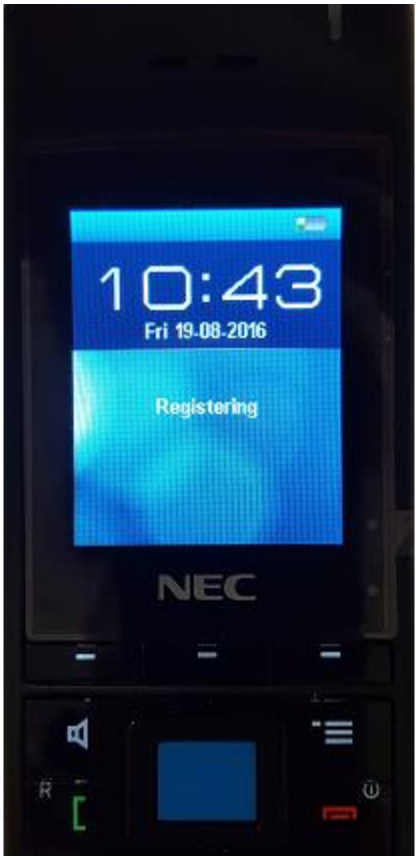
Enter the extension number for the **Network number** as shown below for extension **7151**.



Network number

7151_

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



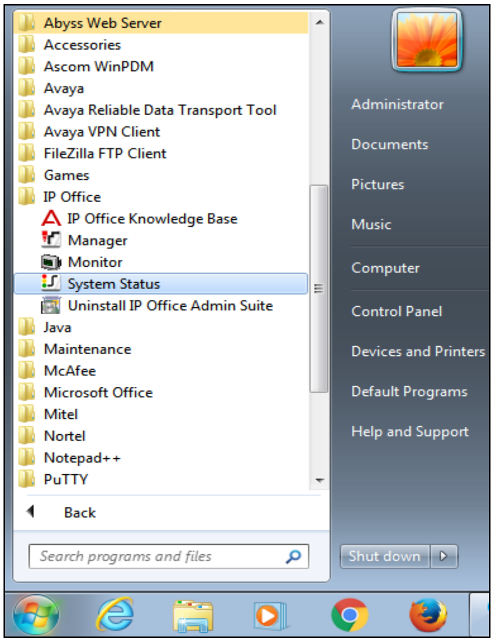
Registering

# 7. Verification Steps

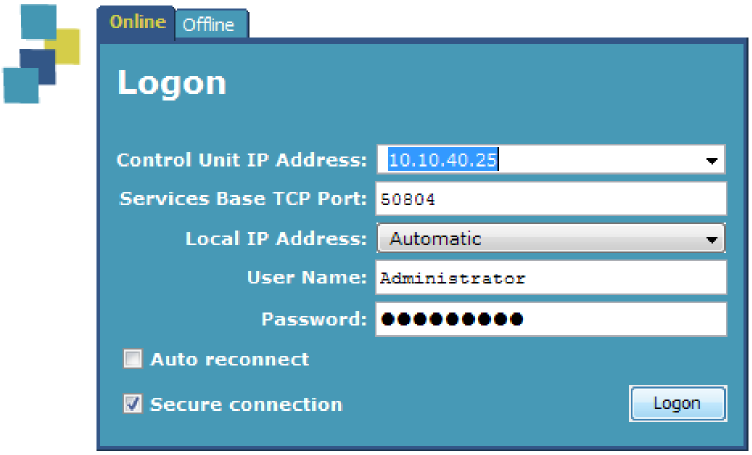
The ultimate test is to make and receive calls between the NEC DECT handsets and to and from the Avaya phones. This will verify that the NEC DECT handsets are connected correctly with the Avaya solution. The following steps can be taken to ensure that connections between NEC DECT handsets and IP Office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



Logon

Control Unit IP Address: 10.10.40.25

Services Base TCP Port: 50804

Local IP Address: Automatic

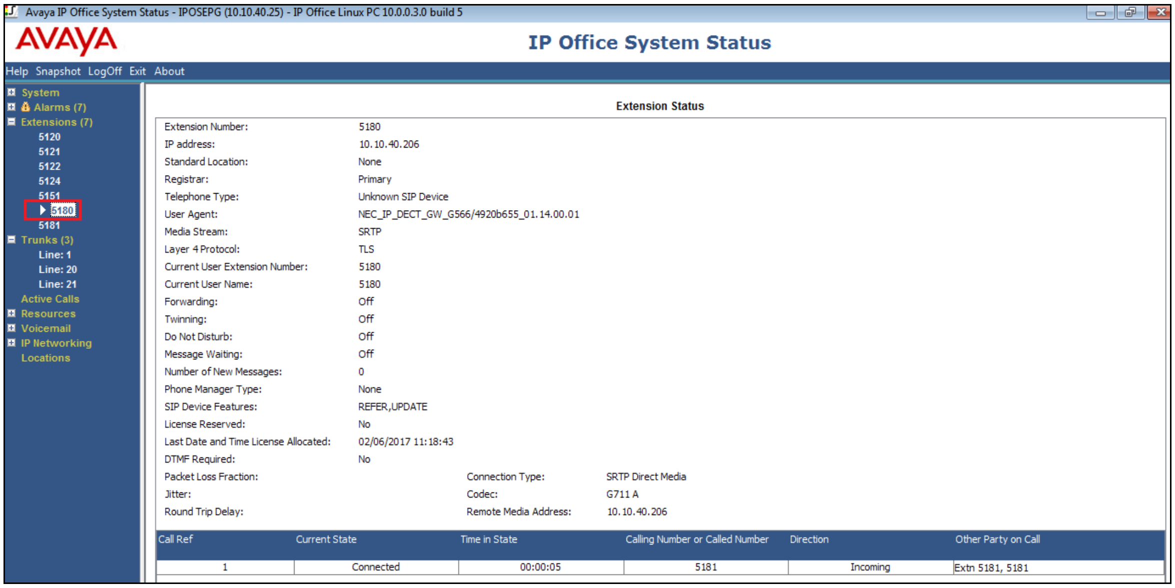
User Name: Administrator

Password: ●●●●●●●●●

□ Auto reconnect

☑ Secure connection

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.

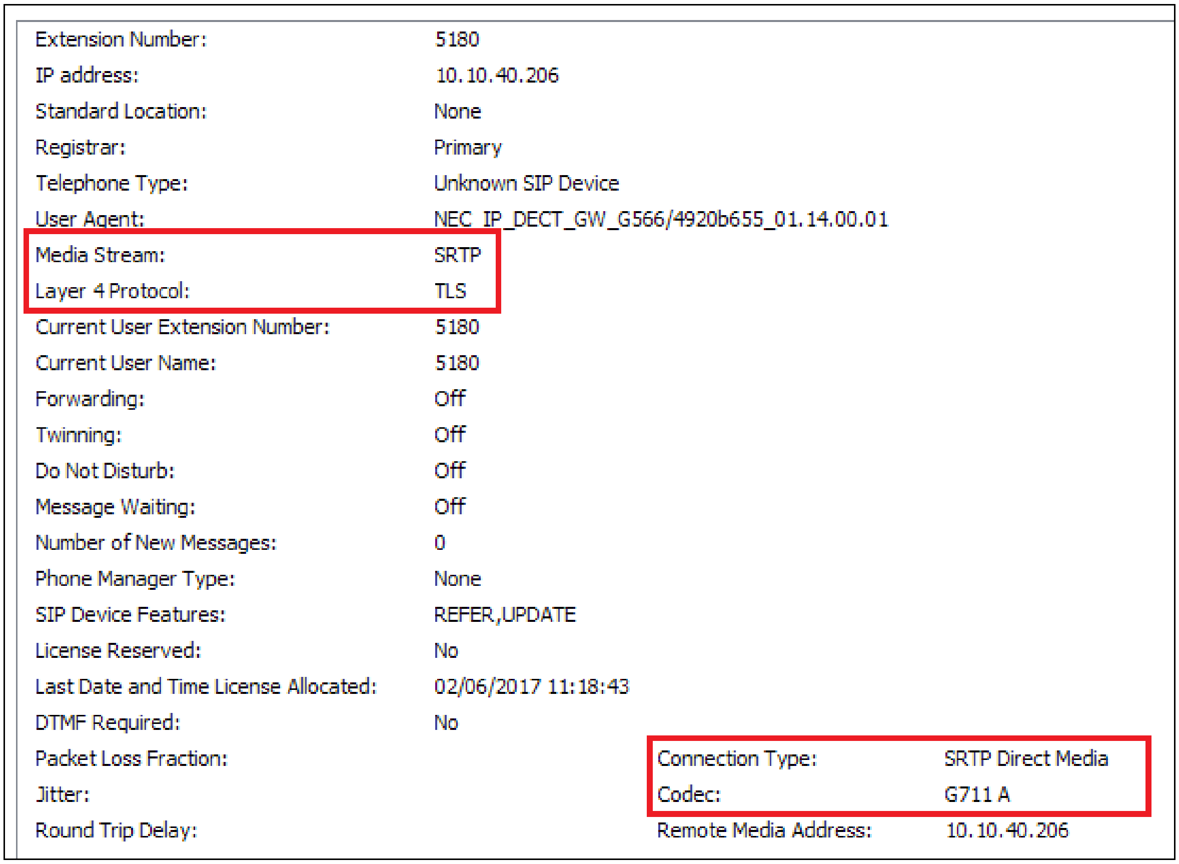


Extension Status

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: SRTP
Layer 4 Protocol: TLS
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 11:18:43
DTMF Required: No
Packet Loss Fraction: Connection Type: SRTP Direct Media
Jitter: Codec: G711 A
Round Trip Delay: Remote Media Address: 10.10.40.206

| Call Ref | Current State | Time in State | Calling Number or Called Number | Direction | Other Party on Call |
|---|---|---|---|---|---|
| 1 | Connected | 00:00:05 | 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 **SRTP** and **TLS**.



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: SRTP
Layer 4 Protocol: TLS
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 11:18:43
DTMF Required: No
Packet Loss Fraction: Connection Type: SRTP Direct Media
Jitter: Codec: G711 A
Round Trip Delay: 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

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.