Orchestrating a brighter world NEC

# InDECT

## Additional Information Manual

Version 1.2

For InDECT 1.3.1

# Contents

## Revision History

| Version | Author | Date | Changes |
|---|---|---|---|
| 1.0 | Stewart Hayles | 01/09/2019 | Initial release of InDECT v1.3.1 |
| 1.1 | Nigel Witts | 17/09/2019 | Correct typo for PBX in place of SV9100 |
| 1.2 | Nigel Witts | 20/01/2020 | Update the license details for IPDECT handsets (p13) |
| | | | |
| | | | |
| | | | |
| | | | |

# Preface

This manual is valid for the installation of the InDECT software Release 1.3.1.

**IMPORTANT:**

This manual gives information for setting up an InDECT IP DECT system. However, the Business Mobility IP DECT is normally part of an IP network. The success of the installation depends on the structure and components in the IP network. Make sure that you have sufficient knowledge of the customers IP network.

The InDECT IP DECT is also a wireless data communication system. This requires knowledge of radio signal propagation. The radio signal propagation in InDECT IP DECT system requires a different approach than for the traditional DECT systems. The success of the installation also depends on the radio signal propagation. Make sure that you have sufficient knowledge about this subject as well.

*No legal rights can be obtained from information in this manual.*

# PRODUCT DISPOSAL INFORMATION (EN)

**For countries in the European Union**

**The symbol depicted here has been affixed to your product in order to inform you that electrical and electronic products should not be disposed of as municipal waste.**

Electrical and electronic products including the cables, plugs and accessories should be disposed of separately in order to allow proper treatment, recovery and recycling. These products should be brought to a designated facility where the best available treatment, recovery and recycling techniques is available. Separate disposal has significant advantages: valuable materials can be re-used and it prevents the dispersion of unwanted substances into the municipal waste stream. This contributes to the protection of human health and the environment.

Please be informed that a fine may be imposed for illegal disposal of electrical and electronic products via the general municipal waste stream.

In order to facilitate separate disposal and environmentally sound recycling arrangements have been made for local collection and recycling. In case your electrical and electronic products need to be disposed of please refer to your supplier or the contractual agreements that your company has made upon acquisition of these products.
At https://www.nec-enterprise.com/Support/WEEE-934 you can find information about separate disposal and environmentally sound recycling.

**For countries outside the European Union**

Disposal of electrical and electronic products in countries outside the European Union should be done in line with the local regulations. If no arrangement has been made with your supplier, please contact the local authorities for further information.

# InDECT System

## What is InDECT

InDECT is a toolset that can be integrated to either NEC's UNIVERGE SV9100 or SL2100 communication servers. It allows for easy installation, deployment and maintenance of a small scale IP DECT system with no additional IT servers required.

InDECT minimises the installation effort by automatically retrieving settings such as regional, tone plan, SIP settings etc. from the PBX configuration, whilst enabling access points to download configuration files from the on-board file server with minimal intervention by the installation engineer to the end users network.

The user interface of InDECT consists of web pages that can be accessed by means of a web browser, so not requiring a dedicated PC configurator tool for installing or upgrading a system.

InDECT is part of the family of NEC's easy to use 'InApps' range of applications and future versions will include additional functionality as the application is developed further.

An external DHCP Server is preferred. E.g. a DHCP Server in a (small) Router in combination with IP Switch functionality.

## Characteristics

The IP DECT InDECT system has the following characteristics:

- Applicable for PBX platforms:
    - SIP on SV9100 (CP10/CP20)/SL2100
- Maximum 32 DAPs (DECT Access Points)
- Maximum 64 handsets.

One of the main differences between the full DAP Controller and the InDECT system is that you can do the subscription management (subscribing handsets or removing handsets) via a WEB interface in the DAPs, instead of via the DAP Controller. Please note that the number of DAPs and handsets are limited, as mentioned above.

## System Overview

The InDECT IP DECT system is an easy to install, relatively small IP DECT system.

The implementation of IP DECT InDECT is a standalone DECT system that is connected to one of the supported PBX types via a TCP/IP connection. This means that in the PBX, the extension numbers that you will use on the InDECT System must be prepared.

InDECT also supports iSIP, however the functionality is only available when the handsets and the PBX support it as well. The figure below shows an example IP DECT InDECT system configuration. All connections are IP connections over Ethernet. The following components are distinguished:

## Handsets

Handsets must be the type of DECT handsets that are supported on this type of IP DECT system. Supported handsets are the following models G266/G277/G566/G577/G577h/i766.

## DAPs

A DAP (DECT Access Point) is the actual transceiver.
The DAPs support up to 11 simultaneous calls and are for indoor applications. However, a dedicated outdoor box can be ordered, which allows you to install a DAP outdoors. The following DAP types are supported:

**AP400E**

This type of DAP is similar to the AP400 (generic) but is equipped with SMA antenna connectors, to connect an external antenna. It is deliverable from January 2013 onwards. The total number of DAPs is limited to either 10, in case of a mix with AP400S, or 32 in case of a mix with AP400C or generic AP400.

**AP400C**

This type of DAP is the standard DAP type delivered from January 2013 onwards. A maximum of 32 x AP400C is allowed in InDECT Release 6.6.x.
When a mix with other types, the total number of DAPs is limited to either 10, in case of a mix with AP400S, or 32 in case of a mix with AP400C or generic AP400..

**AP400S**

This type of DAP is available for small InDECT systems. A mix with other DAP types is possible. However, the overall maximum number of DAPs in the system is limited to 10.

DAPs are powered by means of PoE. We strongly recommend you to use “Power-Over-Ethernet” capable Switches.

### IP Switch

The IP Switch connects the Ethernet connections together. Only use an IP Switch that is supported for this DECT solution, preferably an un-managed IP Switch, because they are normally transparent for IP Multicast. In case of using a managed IP Switch, please make sure that the following settings in the IP Switch are correct:

- The IP Switch must support forwarding “IP Multicast”.
- ***“IGMP snooping” must be disabled***.
- The ports should be set to “Auto Negotiate”.
- The ports should be set to “Fast Forward”.
- The IP Switch should support PoE.

### Router (optional)

There can be a router in the IP network to have access to/from the external network. Please note that the router can be equipped with a DHCP server. In particular in small systems, the router most likely will be equipped with a DHCP server (default) for this IP segment only. This is important info because this may mean that you must use that DHCP server, also for your IP DECT system.

***Note:*** *All DAPs must be in one IP Subnet, which supports IP Multicast. Also the PBX must be in the same IP Subnet as the DAPs.*

### PBX

This is one of the PBX types mentioned in Section 0 Characteristics.

### Laptop PC (or Desktop computer)

The Laptop PC or Desktop computer is needed for initial configuration only by means of the InDECT web interface.

# DAP Planning

## Requirements

The position of the DAPs depends on two factors:

- DAPs must provide radio coverage for the handsets, in such a way that the sound quality of the handsets is good or excellent.

- The DAPs for the IP DECT Lite system should be installed in such a way, that one DAP can see at least two other DAPs with a signal strength of -80 dBm or better. After the installation, you can check this signal strength in the WEB page of the DAPs, because there the RSSI value should be 3 or better.

- All DAPs should see each other directly or indirectly and should form one cluster of DAPs with seamless handover.

## Simple DAP Planning

Before you determine where DAPs are needed, make sure that you have a map of the area/building to be covered.
Mind the following items:

- In an average office building the radiation around a DAP is about 20 meters where you will have good sound quality. . This depends of course on the building materials and the size of the rooms in the buildings. Mind toilets and elevators, which give a higher loss in signal radiation. In open space, the radiation around the DAPs is of course (much) more.

- Try to position the DAPs in open space rather than in rooms.

- Also mind metal objects and metal (inside) walls, which may cause quite some loss and reflection.

- Please note, that by means of an estimation of coverage of the DAPs, you run a risk that you need more DAPs after the installation is finished, or that you order more DAPs than strictly needed. If you want to be sure about the number and the position of the DAPs, you should perform a Site Survey with the special tool kit, the Site Survey kit.

## Licensing

For any operational IP DECT system you must have a unique system identifier called PARI (Primary Access Right Identifier). This is an 8 digit hexadecimal number. Prophix generates a PARI when you order an InDECT system.

License Code 3518 is required to run InDECT on the SV9100 or SL2100 communication servers, it can also run if the 60 day license is enabled. The following LMS licenses are available for InDECT:

| PBX | Part Number | Description |
|---|---|---|
| **SV9100** | BE118719 | SV9100 OnBoard App. InDECT Lic. |
| **SL2100**[1] | BE118720 | SL2100 OnBoard App. InDECT Lic. |

*[1]An EU917108 Gx66 Memory Card is also included with the SL2100 InDECT license for additional file storage space. This memory card that was originally selected for DECT handsets is delivered along with an adapter that enables it to fit in to the SL2100 CPU memory card slot.*

# DHCP Server

The IP addressing is based on DHCP. There can be a DHCP server in the network (e.g. in the Router) as “External DHCP server” or there can be the “Internal DHCP Server in IP DECT (built-in DHCP server that comes with the DAP Configurator software).

## Using “External DHCP” Server (e.g. in the Router).

**Characteristics:**

- DHCP Server is part of the network segment where IP DECT is installed.
- DHCP Server can be part of the Router. In particular the smaller Routers with built-in Switch functionality can be equipped with DHCP.
- DHCP server must issue IP addresses and Subnet mask and Gateway (router) address.
- DHCP Server should NOT issue option 66/67!

**IP data stored in the DAPs.**

The issued IP Address, together with Subnet mask and default Gateway address, are stored in the DAPs, even when the lease time is shorter than infinite. When DAPs reboot and there is no External DHCP server, they will reboot with the stored IP Addresses. In During reboot, the DAPs will check on duplicate IP addresses.

## Provisioning

The DAPs need to be provided with firmware and a configuration file. This is done by means of the file server built in the InDECT software running on the PBX.

There is only one possibility for provisioning server and that is using the InDECT PBX file server.

## DHCP and Provisioning Configuration Overview

The DHCP and Provisioning configuration is as follows:

- DHCP server
  Preferred DHCP Server is an external DHCP server!

- Provisioning
  Automatically, the built-in file server is used on the PBX.

# PBX PREPARATION

The PBX must be prepared to work in combination with InDECT.

***Note*:** Prepare the PBX for InDECT, before setting up the InDECT Configuration.

The PBX setup for IP DECT is the same standard procedure used for setting up SIP extensions on the system. The process consists of three sub-procedures:

-Setting up the IPLE configuration (IP addressing etc.)
-Setting up IP extensions
-Setting up IP extension features

In the following sections, examples are given on how to setup the PBX. If the information is not sufficient, please also consult the PBX documentation for further details.

***Note**: Ensure that the extension numbers you want to use as IP DECT extensions have not been used already as other IP devices in the PBX. Also make sure the IP DECT extensions are either not yet setup in the IP DECT configuration or are switched off. If not, there may be registration data in the PBX which causes the handsets to register or perform improperly.*

## Licensing

For IP DECT extensions, PBX device licenses will be required to be installed on the PBX.
The following table provides license details for the standard SIP/iSIP IP DECT extensions.

| License Code | Applied Device | License Capacity & Type |
|---|---|---|
| SV9100 EU901001 / BE114054<br>SL2100 EU909388 / BE116746[3] | G266, G566, I766, G277, G577, G577h | Per standard SIP / iSIP device registered[2] |
| SV9100 BE114497<br>SL2100 EU909388 / BE116746[3] | G566[1], I766[1,] G277, G577[1], G577h[1] | Per iSIP Device registered |

*[1]The G566, I766, G577, G577h handsets can use either standard SIP or iSIP protocol if running compatible handset firmware and the IP DECT system is configured to support iSIP on these devices.*

*[2]The Standard SIP license will support either Standard SIP or iSIP operation for the DECT handset. Prophix will configure this license code EU901001 as this gives the choice of either mode.*

*[3]The SL2100 has a single IP device license that supports either Standard SIP or iSIP mode.*

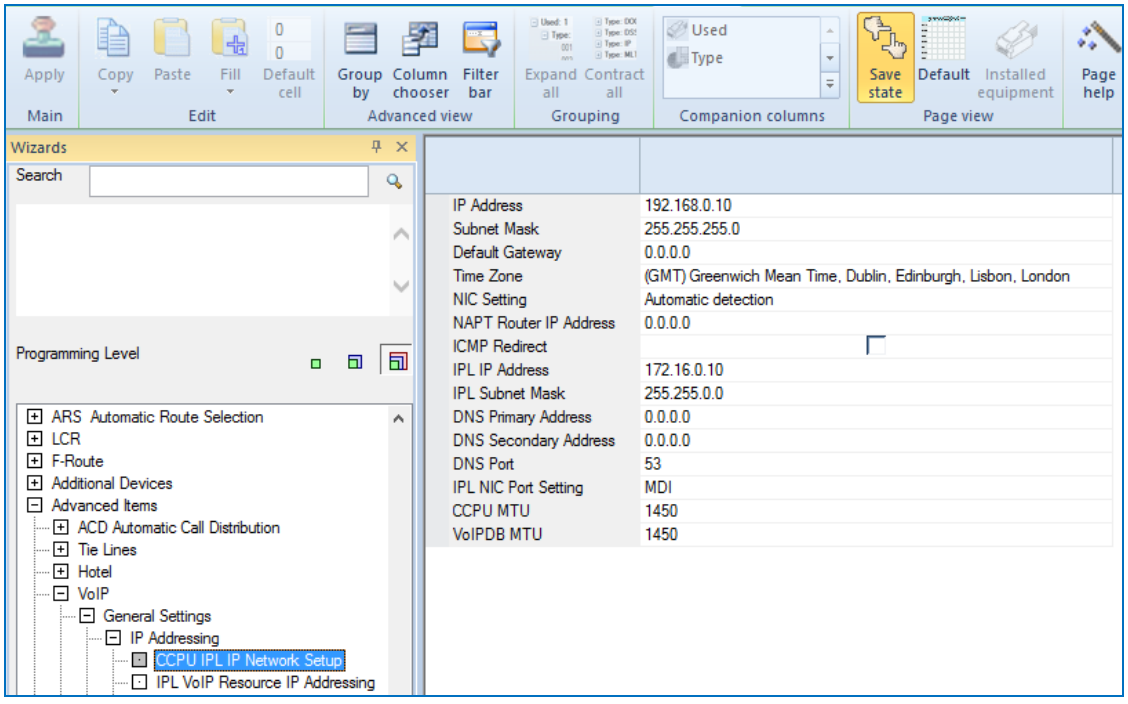
## IP Configuration Settings

The default IP DECT configuration assumes the default PBX network settings are used as given in the below table. These can be:

| DEVICE | IP Addresses |
|---|---|
| PBX IPLE IP Address | 172.16.0.10 |
| IPLE VoIP Gateway IP Address | 172.16.0.20 |
| Management PC | 172.16.0.5 |
| DAPs | 172.16.0.100 – 172.16.0.150 (Addresses are assigned) |

## Configure PBX VoIP IP Addressing

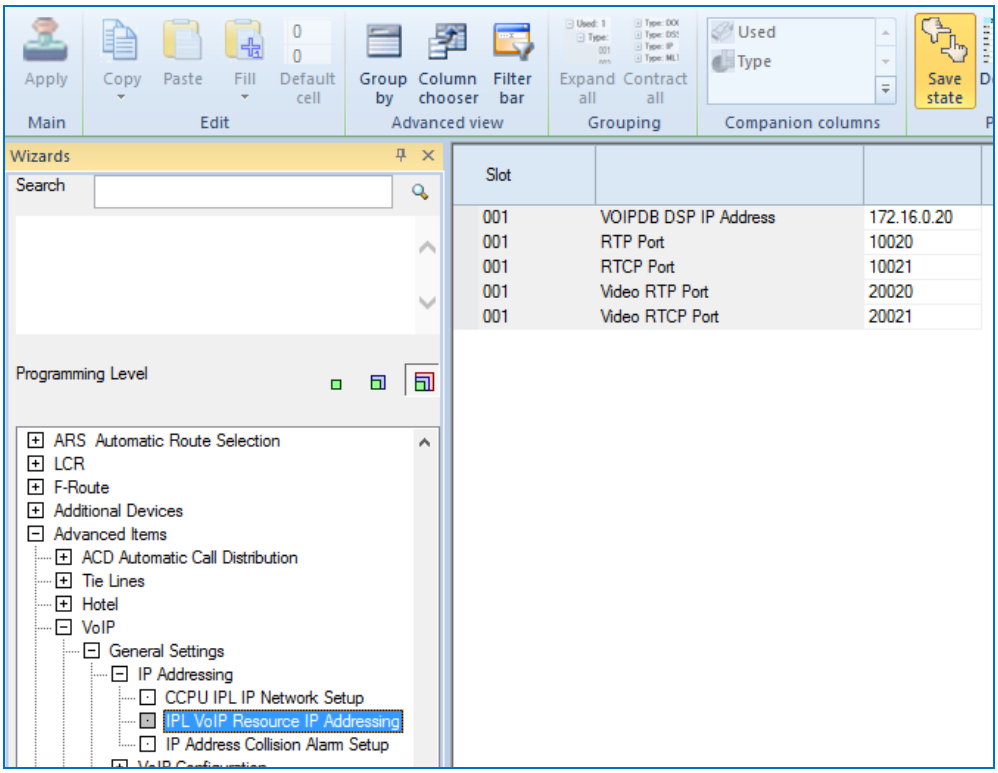
1. Ensure that the relevant PC Programming tool for offline programming of your PBX is running on your management PC. If not already, start the application and connect to the PBX.
2. Take a full download of the PBX configuration.
3. Go to ***Easy Edit > Advanced Items > VoIP > General Settings > IP Addressing > CCPU IPL IP Network Setup*** or if using the system data commands then go to PRG***10-12***.




4. Set the IPL IP address and subnet mask (PRG items ***10-12-09*** and ***10-12-10***) to the required settings for the customers network along with the default gateway address (PRG item ***10-12-03***) if required.
5. Click **Apply** when finished.

## Configure PBX VoIP Gateway IP Addressing

1. Go to ***Easy Edit > Advanced Items > VoIP > General Settings > IP Addressing > IPL VoIP Resource IP Addressing*** or if using the System Data commands then go to PRG ***84-26***.



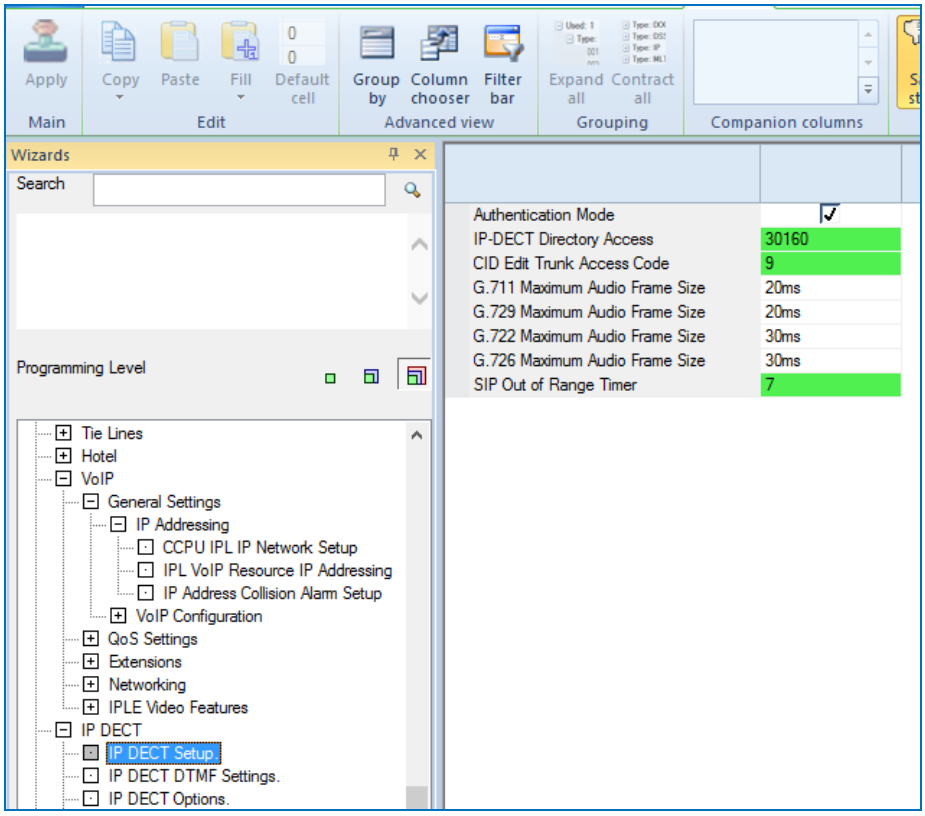

2. Set the IPL VoIPDB DSP IP address (PRG **84-26-01**) information to the required settings for the customer's network.

3. Generally the port numbers can be left as the default values and start from 10020 for RTP and 10021 for RTCP.

4. Click **Apply** when finished.

# Configure Standard SIP IP DECT Settings (Gx66/i766/Gx77/G577h)

1. Go to ***Easy Edit > Advanced Items > IP DECT > IP DECT Setup***.




2. Configure the recommended standard SIP IP DECT settings as per your installation requirements.

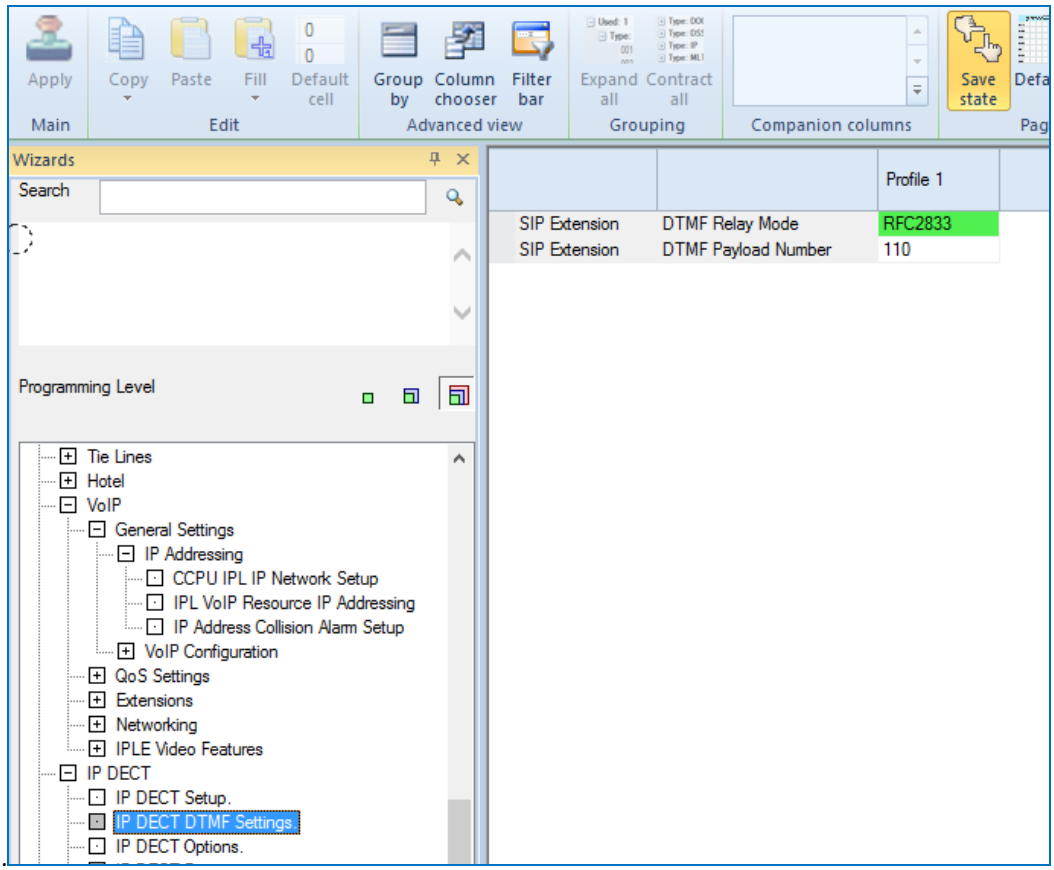
| **Program Name** | **Program Number** | **Input Data** | **Default Value** | **Recommended Settings** |
|---|---|---|---|---|
| Authentication Mode | 10-33-02 | 0=Disabled<br>1=Enabled | 1=Enabled | 1=Enabled |
| IP DECT Directory Access | 10-20-01<br>Device 14 | 0-65535 | 0 | 30160 |
| Trunk Access Code[1] | 10-02-05 | 0-9,*,# | Blank | 9 or 0 |
| G.711 Maximum Audio Frame Size | 84-19-01 | 10ms - 40ms | 20ms | 30ms |
| G.729 Maximum Audio Frame Size | 84-19-07 | 10ms – 60ms | 20ms | 30ms |
| G.722 Maximum Audio Frame Size | 84-19-33 | 10 – 40ms | 30ms | 30ms |
| G.726 Maximum Audio Frame Size | 84-19-38 | 10 – 40ms | 30ms | 30ms |

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| SIP Out of Range Timer | 24-02-15 | 0 – 64800 | 4 | 7 |

[1]*This item is required for the correct operation of call back from the SIP/iSIP IP DECT extensions using the handsets call history lists.*

3. Click the **Apply** button when finished.

4. Go to ***Easy Edit > Advanced Items > IP DECT > IP DECT DTMF Settings***

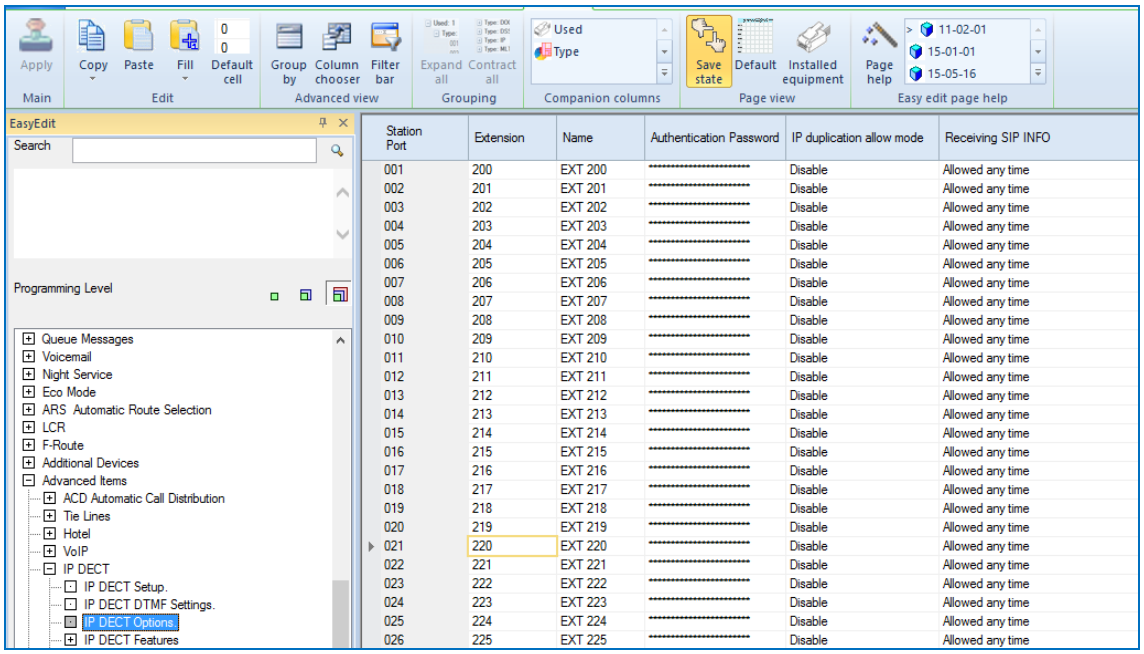



5. Enter the recommended standard SIP IP DECT DTMF Settings as per your installation requirements.

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| DTMF Relay Mode | 84-34-01<br>(04 – SIP Extension) | 0=Disabled<br>1=Enabled | 0=Disabled | 1=Enabled |
| DTMF Payload Number | 84-34-02 | 0-65535 | 110 | 110 |

6. Click **Apply** when finished.

7. Go to ***Easy Edit > Advanced Items > IP DECT > IP DECT Options***.




8. Determine a port range that is unallocated to existing extension cards or IP terminals and are available for IP DECT devices.

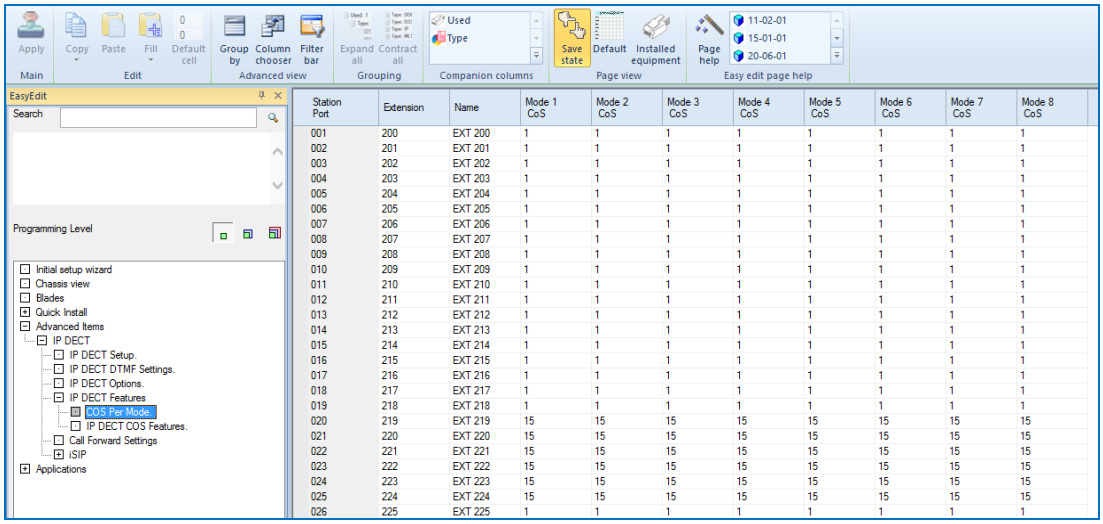
9. Assign extension numbers the IP DECT to the relevant ports.

10. If Authentication Mode (PRG ***10-33-02***) is used between the PBX and IP DECT for added security, then assign an 'Authentication Password' (PRG ***15-05-16***) to the relevant ports here. The password should be secure but the password should be the same for all standard SIP IP DECT extensions.

11. Check that the IP Duplication Allowed Group (PRG***15-05-18***) is set to 'not used' for all standard SIP IP DECT extension numbers. This field will automatically update when standard SIP IP DECT extensions complete registration with the PBX.

12. Click **Apply** when finished.

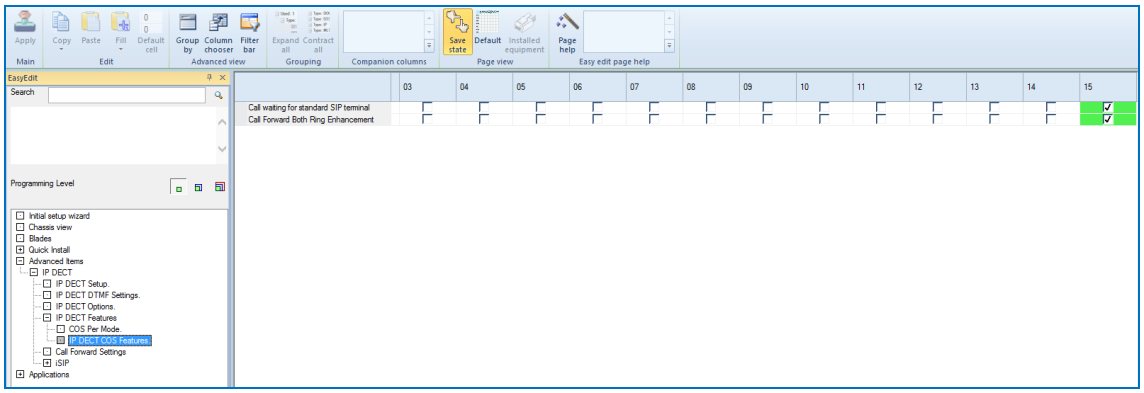
13. Go to ***Easy Edit > Advanced Items > IP DECT > IP DECT Features > COS per Mode***.




14. Assign the standard SIP IP DECT extensions to a class of service group between the values of 1 – 15. By default all station ports are members of class of service group 1.

15. Click **Apply** when finished.

16. Go to Easy Edit > Advanced Items > IP DECT > IP DECT Features > IP DECT COS Features.

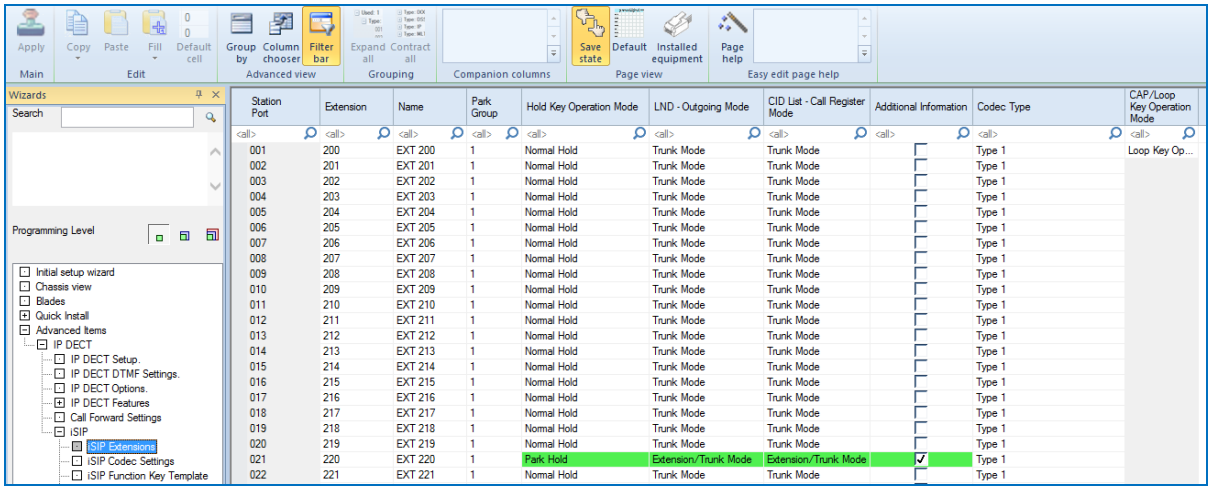



17. If the users of the IP DECT system require using either Call Waiting or Call Forward Both Ring features of the PBX. Then enable these items on this screen for the relevant class of service group the standard SIP IP DECT extensions were assigned to previously at step 12.

18. Click **Apply** when finished.

# Configure iSIP IP DECT Device Settings (G566/i766/G577/G577h)

1. Go to ***Easy Edit > Advanced Items > IP DECT > iSIP > iSIP Extensions***.




2. Determine a port range that is unallocated already to existing extension cards or IP terminals and are available for IP DECT devices.
3. Assign extension numbers for the iSIP IP DECT devices to the relevant ports.
4. Configure the recommended iSIP IP DECT settings as per your system requirements.

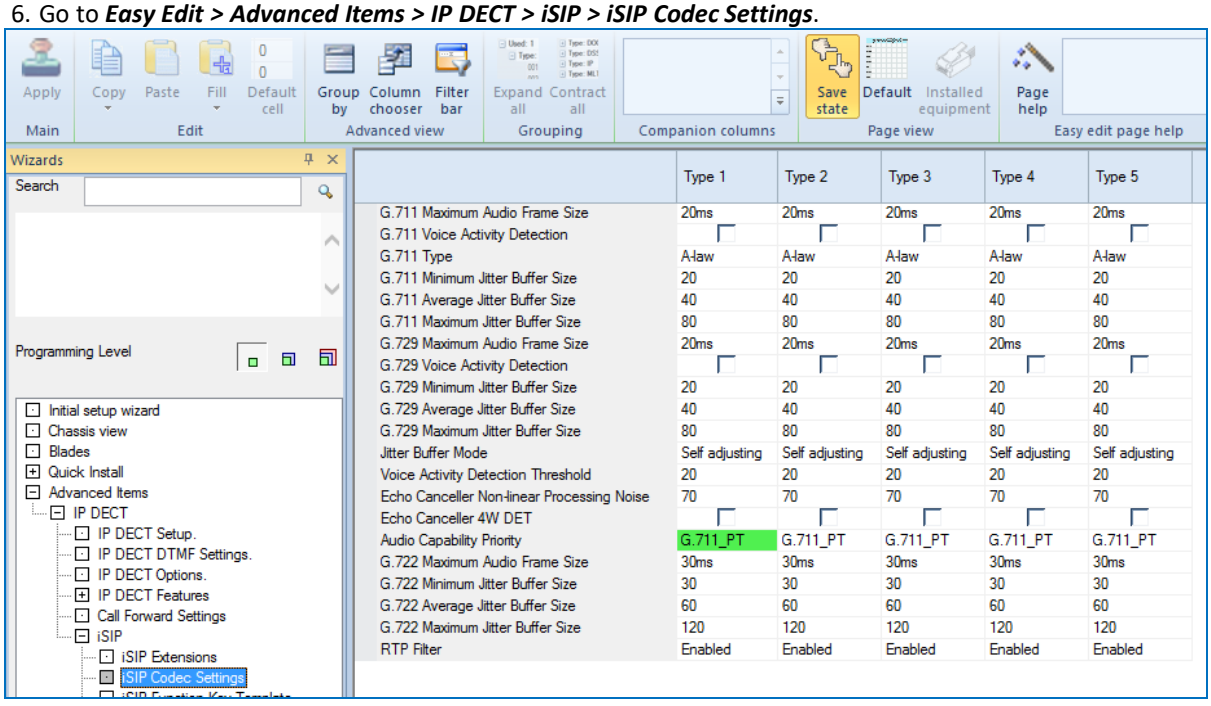
| **Program Name** | **Program Number** | **Input Data** | **Default Value** | **Recommended Settings** |
|---|---|---|---|---|
| Extension | 11-02-01 | 0-9<br>(up to 8 digits) | | |
| Name | 15-01-01 | Up to 12 characters | | |
| Park Group[2] | 24-03-01 | 1-64 | 1 | 1 - 64 |
| Hold Key Operation[1] Mode | 15-02-06 | 0=Normal Hold<br>1= Exclusive hold<br>2=Park Hold | 0 = Normal Hold | 2=Park Hold |
| LND – Outgoing Mode | 15-02-13 | 0=Extension/Trunk Mode<br>1=Trunk Mode | 1=Trunk Mode | 0=Extension/Trunk Mode |
| CID List – Call Register Mode | 15-02-34 | 0=Extension/Trunk Mode<br>1=Trunk Mode | 1=Trunk Mode | 0=Extension/Trunk Mode |
| Additional Information | 15-05-28 | 0=Disable<br>1=Enable | 0=Disable | 1=Enable |
| CODEC Type | 15-05-15 | 1=Type 1<br>2=Type 2 | 1=Type 1 | |

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| | | 3=Type 3<br>4=Type 4<br>5=Type 5 | | |
| CAP/Loop Key Operation Mode | 20-02-23 | 0=CAP Key Operation Mode<br>1=Loop Key Operation Mode | 1=Loop Key Operation Mode | |

[1] *The iSIP IP DECT extension(s) is recommended to be configured to use Park Hold instead of Normal Hold. This means that when the extension uses the Hold function, internal and external callers are held on the Park Hold key and can be retrieved easily.*

[2]*Optionally the extension can be added to a separate Park Hold Group if the same Park Hold orbits are being used by devices elsewhere. There are 64 Park Hold Groups, and each group contains 64 Park Hold orbits which can be distributed over iSIP IP DECT devices.*

5. Click the **Apply** button when finished.
6. Go to ***Easy Edit > Advanced Items > IP DECT > iSIP > iSIP Codec Settings***.




7. Configure the recommended iSIP IP DECT settings as per your system requirements.

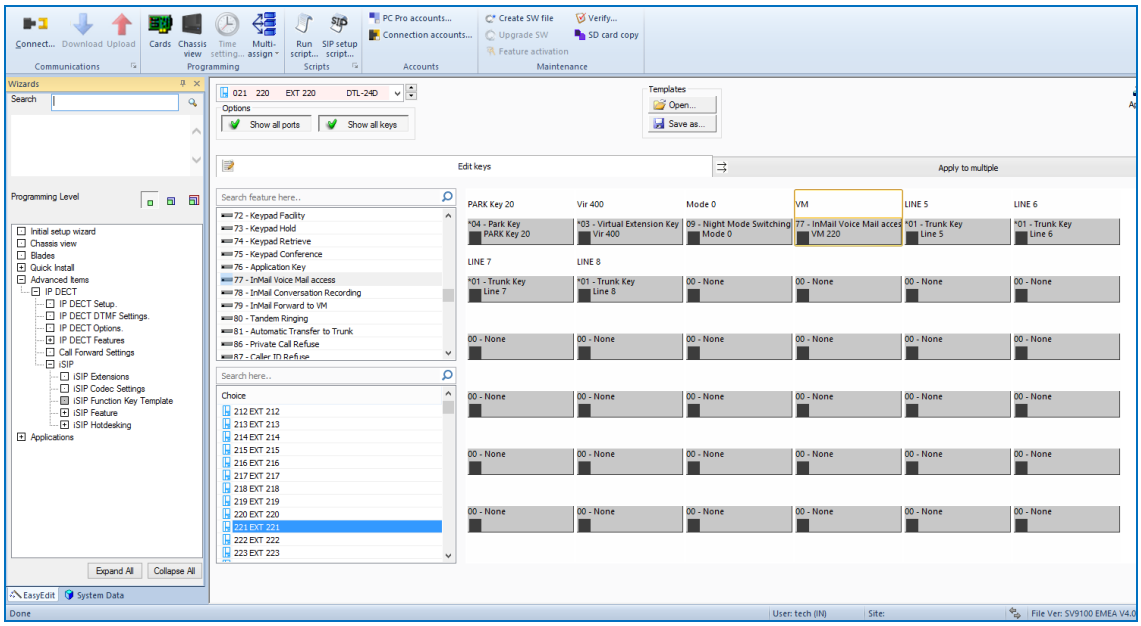
| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| G.711 Maximum Audio Frame Size | 84-24-01 | 1=10ms | 2=20ms | 2=20ms |

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| | | 2=20ms<br>3=30ms<br>4=40ms | | |
| G.711 Type | 84-34-02 | 0=A-Law<br>1=u-Law | 0=A-Law | |
| Audio Capability Priority | 84-24-28 | 0=G.711<br>1=G.729<br>2=G.722 | 0=G.711 | 0=G.711 |

8. Click the **Apply** button when finished

# Configure iSIP IP DECT Programmable Keys

1. Go to ***Easy Edit > Advanced Items > IP DECT > iSIP > iSIP Function Keys*** or if using the System Data commands then go to PRG areas ***11-02***, ***15-07***, ***15-20***.




2. Assign and configure function keys for the iSIP IP DECT extension. Keys 1 – 4 can be programmed. It is recommended the following template be used for programming of these keys;

   Key 1 = Park Key (for on Hold call operation)*

   Key 2 = User defined

   Key 3 = User defined

   Key 4 = User defined

* *The number of required function keys can be reduced from two to one using a unique Park key for controlling Hold operation instead of an ICM/CAP key combination. See*

*Configure iSIP IP DECT Device* Settings *for more details on setting the extensions to use Park Hold operation mode.*

*The key is programmed as a Park Hold (*03) key. A unique Park Hold Orbit should be assigned to each iSIP IP DECT extension for exclusive use. Shared Park Hold orbits across the system should not be used at the same time on these devices.*

*It is possible to add multiple Park Hold keys if the handset user is required to manage multiple calls at once.*

### Supported iSIP Programmable Function Keys

Programmable Function Keys can be used to assign features to an iSIP handsets 4 line keys. For certain functions, you can append data to the keys basic function number. For example, a Function key 26 appended by data **1** makes a Group Call Pickup key for Pickup Group 1. You can also program Function Keys using Service Codes. For full details on these programmable function keys usage please refer to the NEC Telephone Systems Features and Specifications manual.

To clear any previously programmed key, press **000** to erase any displayed code.

| Function Number | Function Description | iSIP DECT Support |
|---|---|---|
| 00 | Not Defined | OK |
| 01 | DSS/One-Touch | OK |
| 02 | Microphone | - |
| 03 | Do Not Disturb (DND) Key | OK |
| 04 | Background Music (BGM) | - |
| 05 | Headset | - |
| 06 | Transfer | OK |
| 07 | Conference | OK |
| 08 | Incoming Caller ID List | - |
| 09 | Night Mode Switching | OK |
| 10 | Call Forward – Immediate | OK |
| 11 | Call Forward – Busy | OK |
| 12 | Call Forward – No Answer | OK |
| 13 | Call Forward – Busy/No Answer | OK |
| 14 | Call Forward – Both Ring | OK |
| 15 | Call Forward – Follow Me | OK |
| 16 | --- Not Used --- | - |
| 17 | --- Not Used --- | - |
| 18 | Text Message Setup | - |
| 19 | External Group Paging | OK |
| 20 | External All Call Paging | OK |
| 21 | Internal Group Paging | OK |
| 22 | Internal All Call Paging | OK |
| 23 | Meet-Me Answer to Internal Paging | - |
| 24 | Call Pickup for Own Group | OK |
| 25 | Call Pickup for Another Group | OK |
| 26 | Call Pickup for Specified Group | OK |
| 27 | Speed Dial – Common/ Private | OK |

| Function Number | Function Description | iSIP DECT Support |
|---|---|---|
| 28 | Speed Dial – Group | OK |
| 29 | Redial | - |
| 30 | Saved Number Redial | OK |
| 31 | Memo Dial | - |
| 32 | Meet – Me Conference | - |
| 33 | Off-Hook Signaling (Call Waiting) | OK |
| 34 | Barge – In | OK |
| 35 | Camp On/Callback | OK |
| 36 | Department Group Step Call | OK |
| 37 | Do Not Disturb/Call Forward Override | OK |
| 38 | Message Waiting | OK |
| 39 | Room Monitoring | - |
| 40 | Handset Transmission Cut-off | OK |
| 41 | Secretary Call (Buzzer) | - |
| 42 | Secretary Call (Manager) | - |
| 43 | Series Call | - |
| 44 | Common Hold | - |
| 45 | Exclusive Hold | - |
| 46 | Department Group Logout | OK |
| 47 | Reverse Voice Over | - |
| 48 | Voice Over | - |
| 49 | Call Redirect | OK |
| 50 | Account Code | - |
| 51 | General Purpose Relay | - |
| 52 | Incoming Call Queuing Message Setup | OK |
| 53 | Queuing Message Starting | - |
| 54 | External Call Forward by Doorphone | OK |
| 55 | Change Extension Name | - |
| 56 | General Purpose LED Operation | - |
| 57 | General Purpose LED Indication | - |
| 58 | Automatic Transfer to Department Group | OK |
| 59 | Delayed Transfer to Department Group | OK |
| 60 | DND Transfer to Department Group | OK |
| 61 | --- Not Used --- | - |
| 62 | Flash Key | OK |
| 63 | ISDN Outgoing Call Without Caller ID | OK |
| 64 | --- Not Used --- | - |

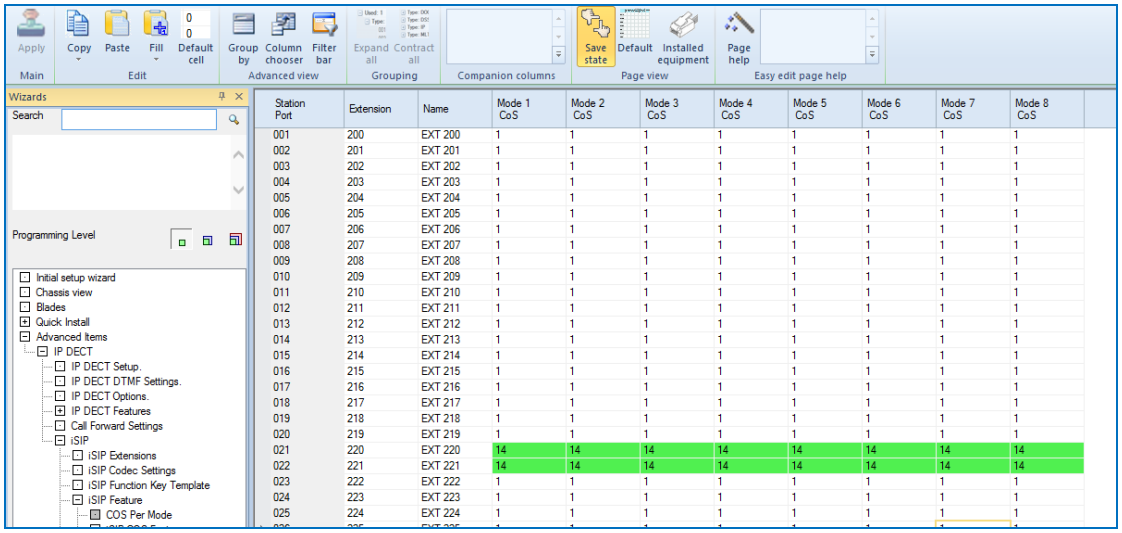
| Function Number | Function Description | iSIP DECT Support |
|---|---|---|
| 65 | --- Not Used --- | - |
| 66 | --- Not Used --- | - |
| 67 | --- Not Used --- | - |
| 68 | --- Not Used --- | - |
| 69 | ACI Conversation Recording | - |
| 70 | --- Not Used --- | - |
| 71 | --- Not Used --- | - |
| 72 | Keypad Facility | - |
| 73 | Keypad HOLD | - |
| 74 | Keypad RETRIEVE | - |
| 75 | Keypad Conference | - |
| 76 | Application Key (3rd Party CTI) | - |
| 77 | InMail Voice Mail access | OK |
| 78 | InMail Conversation Recording | OK |
| 79 | InMail Forward to VM | - |
| 80 | Tandem Ringing | - |
| 81 | Automatic Transfer to Trunk | - |
| 82 | --- Not Used --- | - |
| 83 | --- Not Used --- | - |
| 84 | --- Not Used --- | - |
| 85 | --- Not Used --- | - |
| 86 | --- Not Used --- | - |
| 87 | Caller ID Refuse | - |
| 88 | Dial Mode Switching | - |
| 89 | Do-Not-Call Setup | - |
| 90 | Do-Not-Call Registration | - |
| 91 | Live Monitor | - |
| 92 | --- Not Used --- | - |
| 93 | --- Not Used --- | - |
| 94 | Call Attendant | - |
| 95 | --- Not Used --- | - |
| 96 | --- Not Used --- | - |
| 97 | Doorphone Access | OK |
| 98 | --- Not Used --- | - |
| 99 | --- Not Used --- | - |

| Function Number | Function Description | iSIP DECT Support |
|---|---|---|
| #04 | Change Restriction Class | OK |
| #06 | Power Saving for Eco Mode Group | OK |
| #07 | Fixed Operation Mode | OK |
| #08 | Bluetooth Connect | - |
| #09 | Bluetooth Path | - |
| #10 | Conference Record | - |
| #11 | Major Alarm | - |
| #12 | Minor Alarm | - |
| #13 | Calling Party Number Notification | - |
| #14 | Multi Device Support | - |
| *00 | ICM Key | OK |
| *01 | Trunk Key | OK |
| *02 | Trunk Group Key | OK |
| *03 | Virtual Extension Key | OK |
| *04 | Park Key | OK |
| *05 | Hybrid/Loop Key | OK |
| *06 | Trunk Access Via Networking | OK |
| *07 | Station Park Hold | OK |
| *08 | CAP Key | OK |
| *09 | --- Not Used --- | - |
| *10 | ACD Log-In/Log-Out | - |
| *11 | --- Not Used --- | - |
| *12 | ACD Emergency Call | - |
| *13 | ACD Off-duty Mode | - |
| *14 | ACD Operation Start/End | - |
| *15 | ACD Terminal Speech Monitor | - |
| *16 | ACD Waiting | - |
| *17 | ACD Work Wrap-up Time | - |
| *18 | ACD Overflow Control | - |
| *19 | ACD Queue Status Display | - |
| *20 | --- Not Used --- | - |
| *21 | --- Not Used --- | - |
| *22 | --- Not Used --- | - |
| *23 | --- Not Used --- | - |
| *24 | --- Not Used --- | - |
| *25 | --- Not Used --- | - |
| *26 | --- Not Used --- | - |

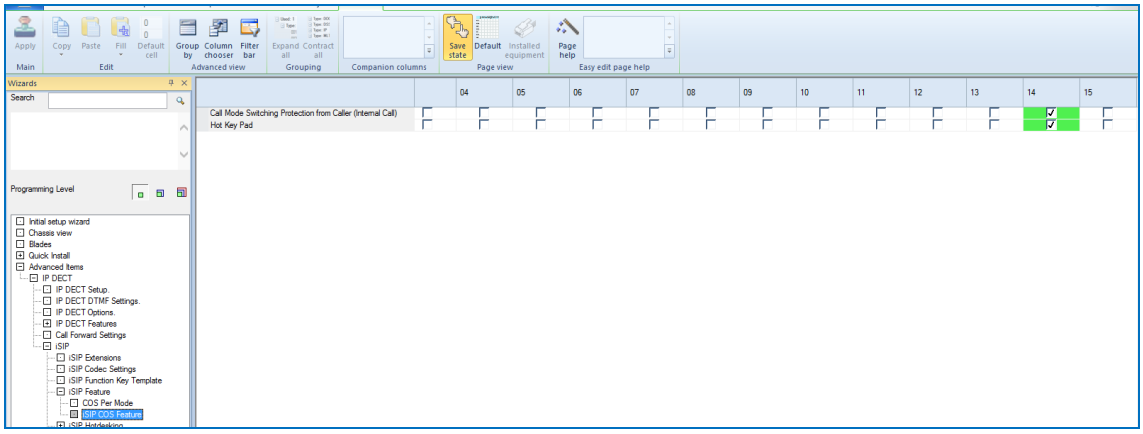
| | | |
|---|---|---|
| *27 | --- Not Used --- | - |
| *28 | --- Not Used --- | - |
| *29 | --- Not Used --- | - |
| *30 | --- Not Used --- | - |
| *31 | --- Not Used --- | - |
| *32 | Warning Message | OK |
| *33 | Sensor Mode | OK |
| *34 | ACD Caller ID Marking Setup | - |
| *35 | System Call History | - |
| *36 | ACD Whispering | - |
| *37 | ACD Queue Alarm | - |

## Configure iSIP IP DECT Features

1. Go to ***Easy Edit > Advanced Items > IP DECT > iSIP > iSIP Feature > COS per Mode*** or if using the System Data commands then go to PRG areas ***11-02***, ***15-01***, ***20-06***.




2. Assign the iSIP IP DECT extension numbers to an unused class of service group between the values 1 – 15. By default all system extensions are members of class of service group 1.
3. Click the **Apply** button when finished.
4. Go to ***Easy Edit > Advanced Items > IP DECT > iSIP > iSIP Feature > iSIP COS Feature*** or if using the System Data commands then go to PRG ***20-08***.




5. Configure the recommended iSIP IP DECT settings as per your system requirements.

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| Call Mode Switching Protection from Caller (Internal Call)[1] | 20-08-11 | 0=Disabled<br>1=Enabled | 0=Disabled | 1=Enabled |

| Program Name | Program Number | Input Data | Default Value | Recommended Settings |
|---|---|---|---|---|
| Hot Key Pad[2] | 20-08-20 | 0=Disabled<br>1=Enabled | 0=Disabled | 0=Disabled |

[1] *iSIP IP DECT extensions do not fully support the voice announce calls feature of the PBX. To protect the devices from this feature being used, this COS option is recommended to be enabled.*

[2] *iSIP IP DECT extensions do not fully support Hot Keypad feature of the PBX. To protect the devices from this feature being used this COS option should be disabled.*

6. Click the **Apply** button when finished

The above procedures are applicable for a common installation of standard SIP/iSIP IP DECT extensions in the PBX. There are additional settings in the PBX that can be changed to fine-tune the behavior of the SIP/iSIP IP DECT extensions.

# Backup and Restore Data

InDECT does not offer a feature for making a Backup or doing a Restore.

In an InDECT system, the primary configuration data is held on the PBX file server and the subscription data is held on the DAPs.

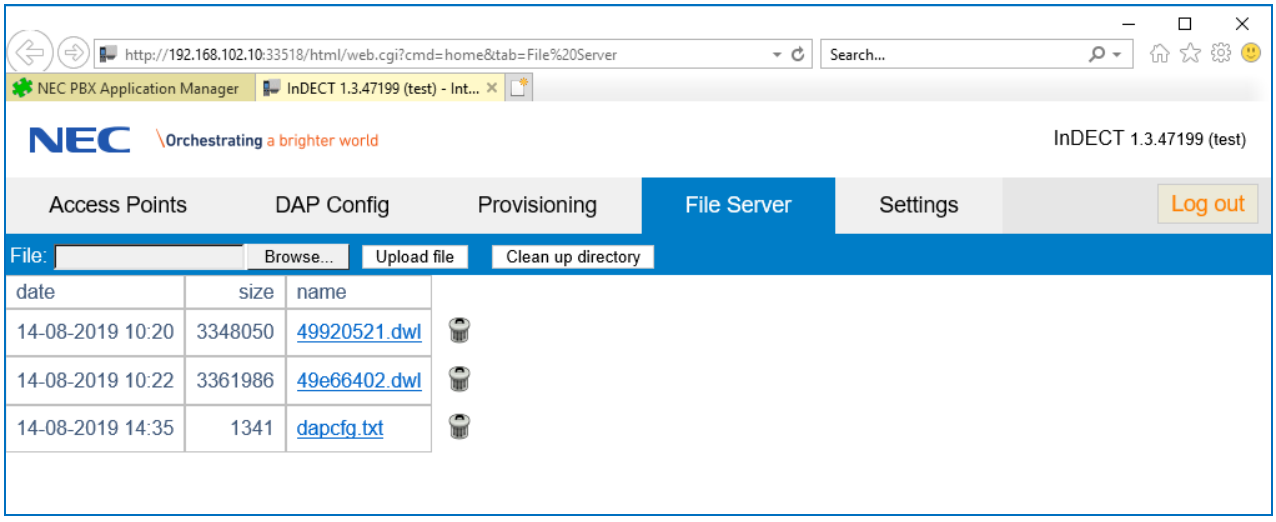
You can make a simple backup of the configuration data but not the subscription data from the DAPs. So if the system was lost for any reason, the configuration could be restored but the handsets would need to be re-subscribed to the system.

## Backup Configuration Data

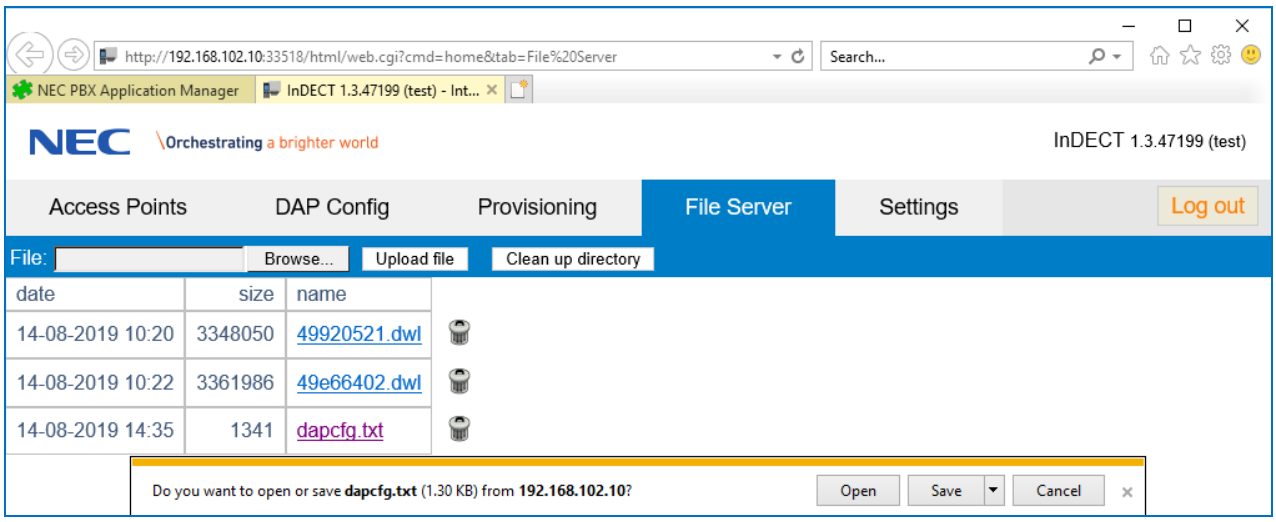
Open the InDECT web interface using the **Configure** button 

and go to the **File Server** screen.

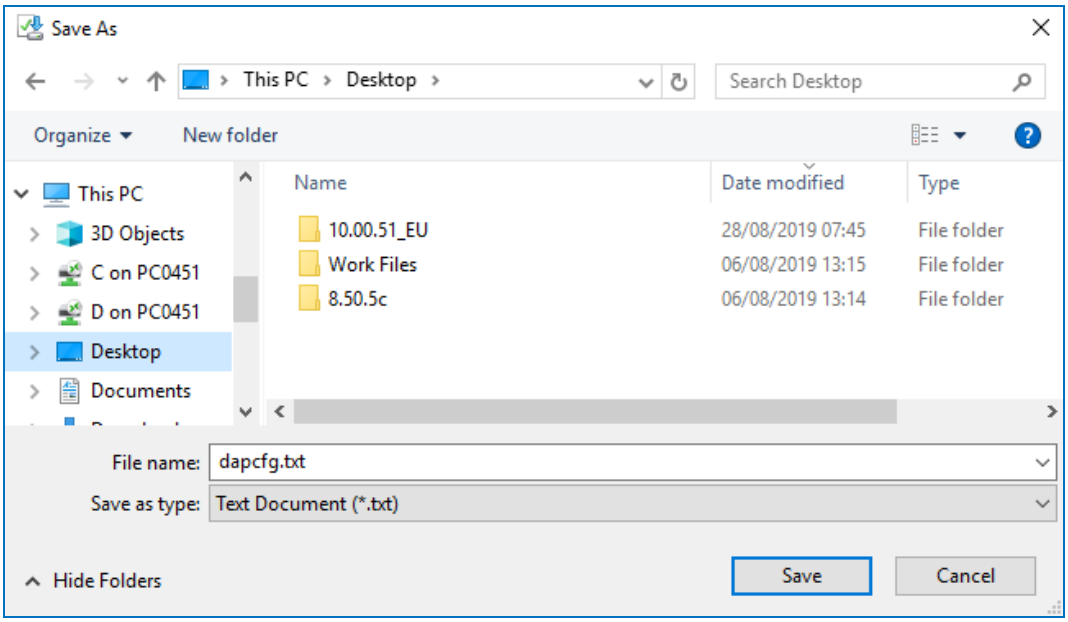
The system files will be listed on this screen.



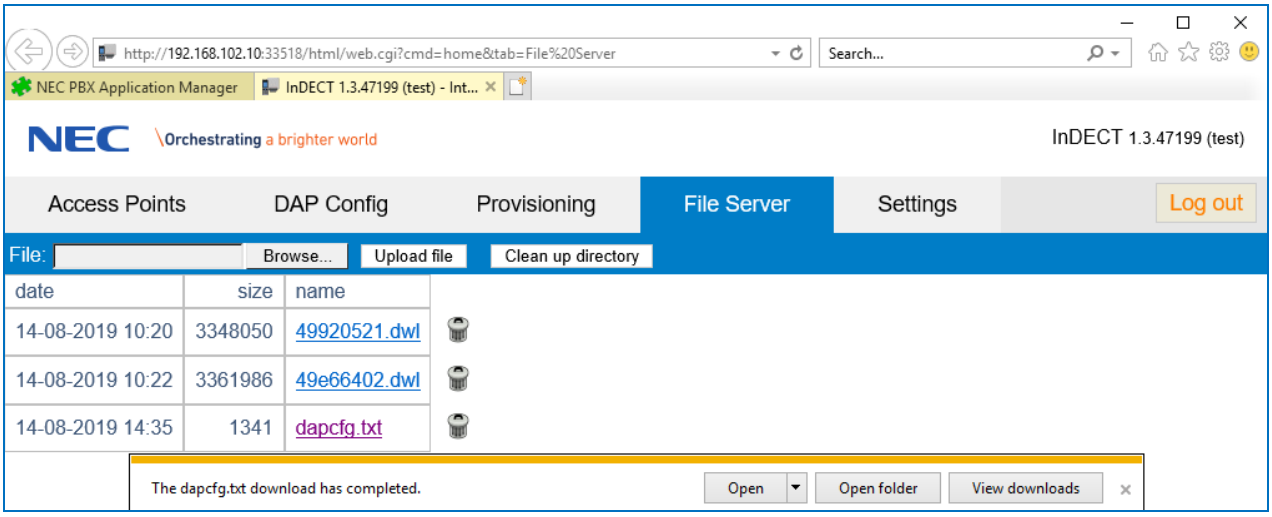

Click the name of the file to download to the device you are using. The InDECT configuration file is called dapcfg.txt.




Save the file to a safe location.



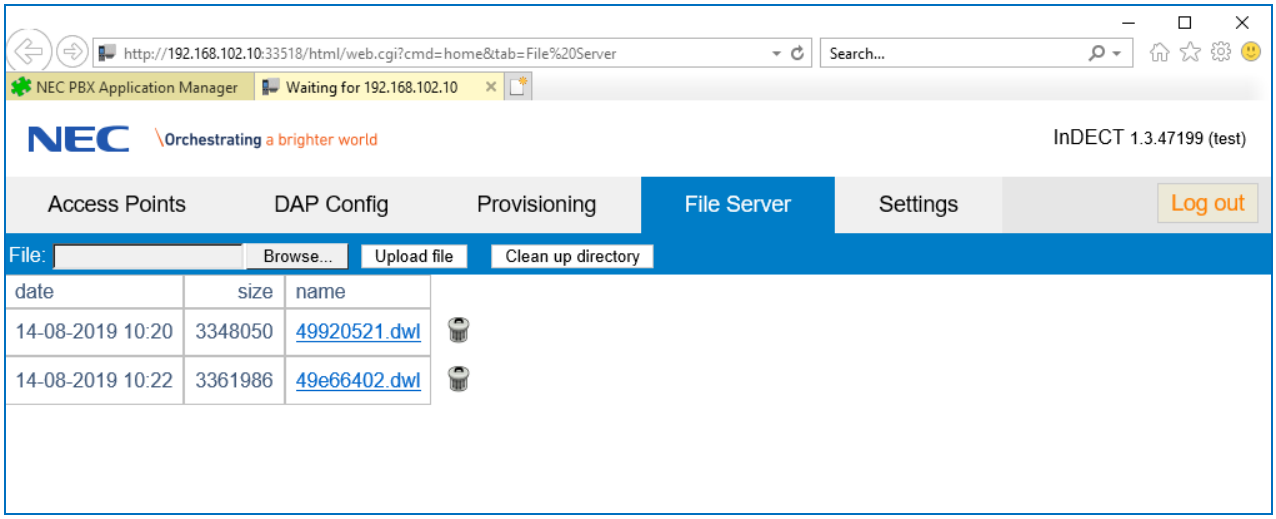

You can now open the file to the view the system configuration if you want to.



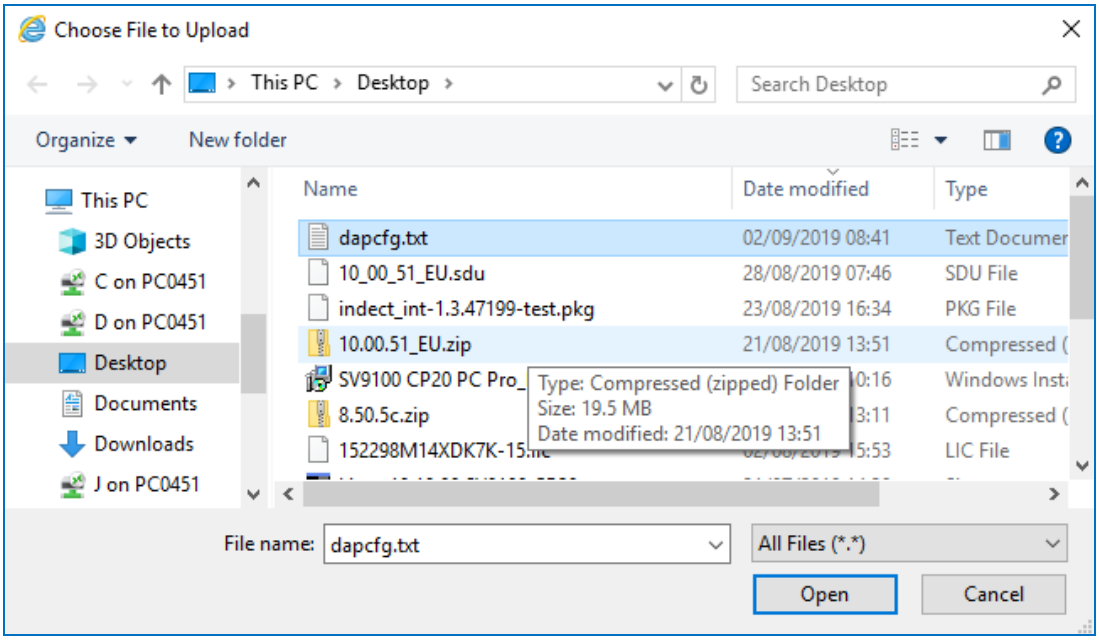
## Restore Configuration Data

Open the InDECT web interface using the **Configure** button 

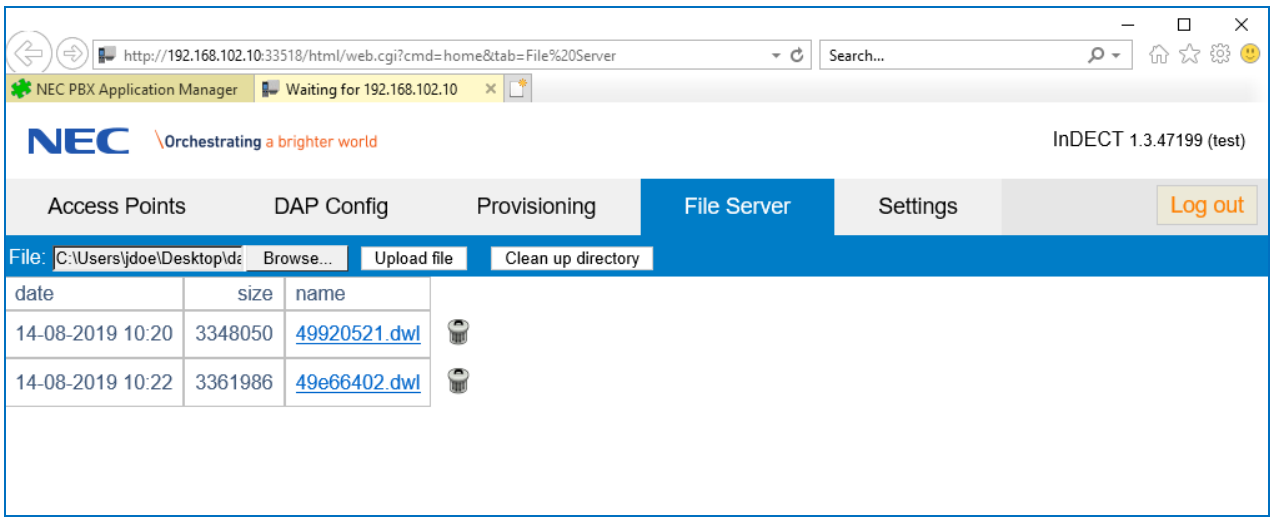
and go to the **File Server** screen.



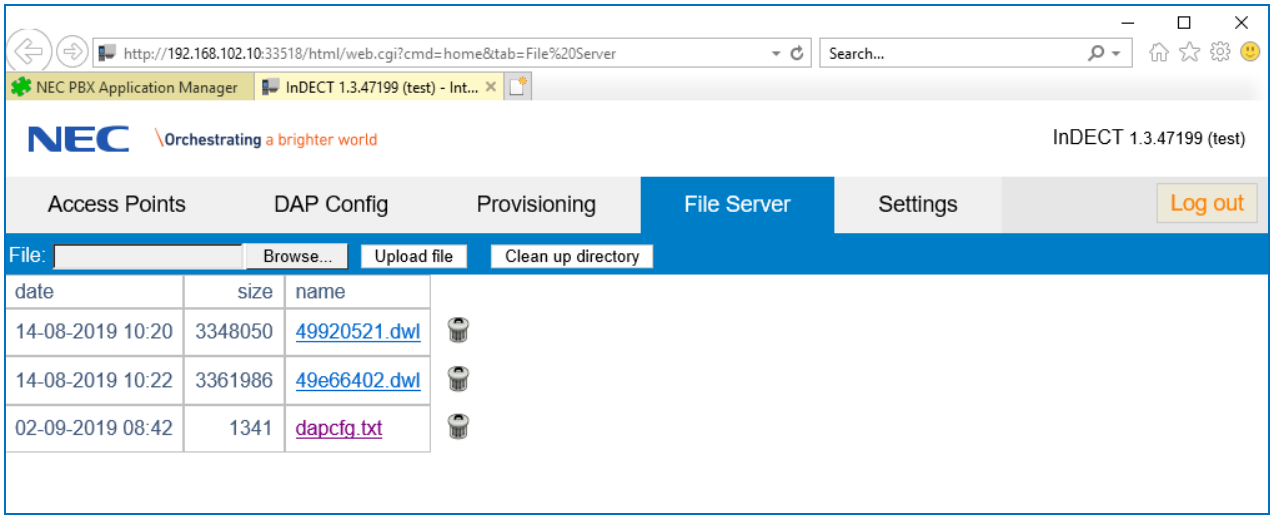

To restore an InDECT system configuration file, press the **Browse** button first and locate the dapcfg.txt file of the InDECT configuration you want to restore. Then press the **Open** button.



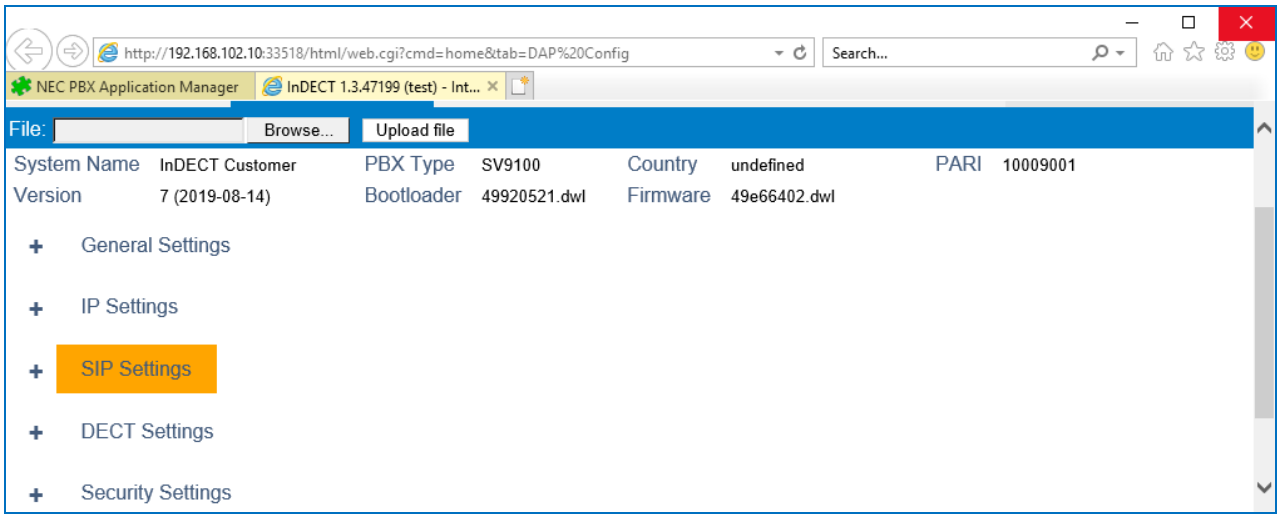

You can when ready upload the file to the PBX file server using the **Upload** button.




The file will be uploaded and appear in the list of files on the **File Server** screen.




You can check the configuration has been restored successfully then by going to the **DAP Config** screen.



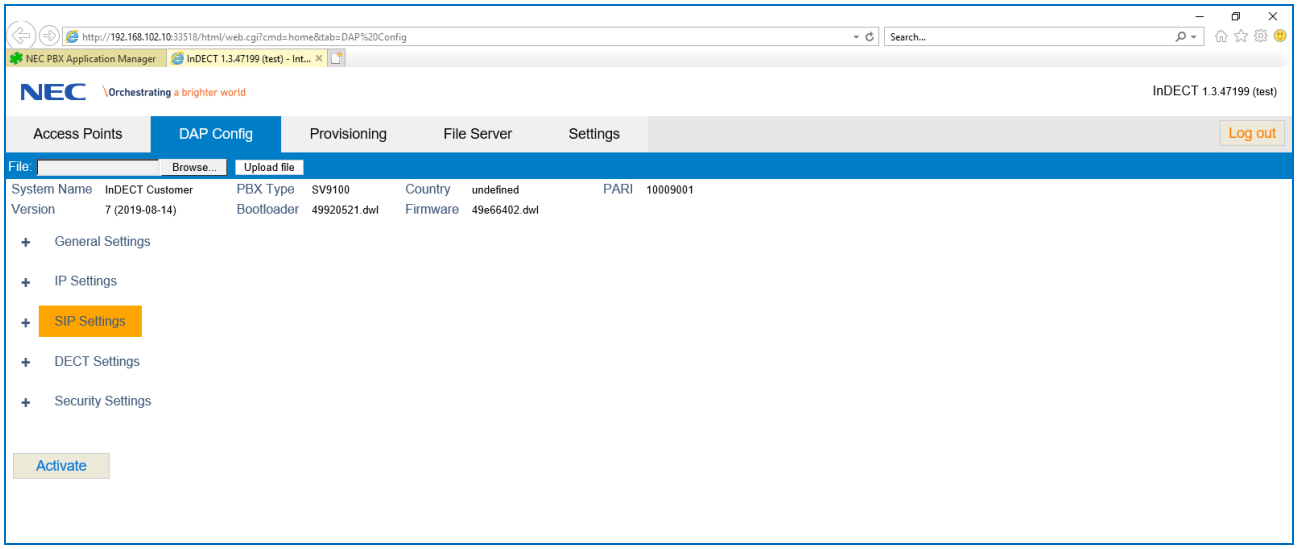

Using the same process, you can also upload DAP bootloader and firmware packages here.

# DAP Web Page Security

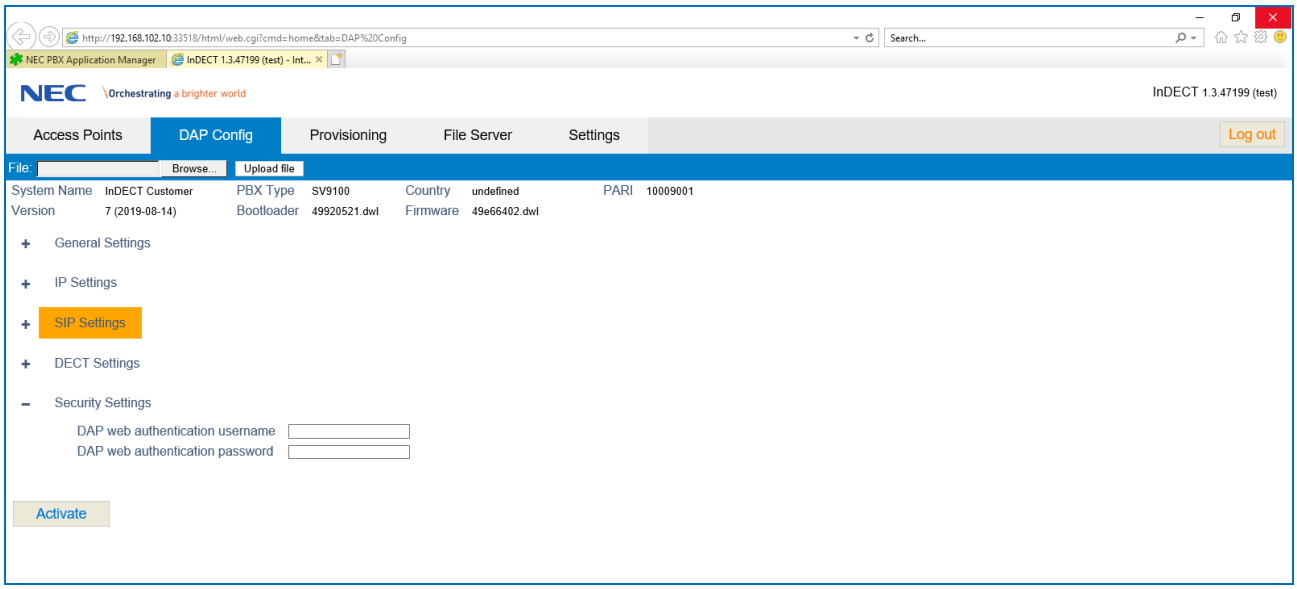
You can easily protect the DAP WEB page with a user name and password. Use the following procedure to do this:

Open the InDECT web interface using the **Configure** button 

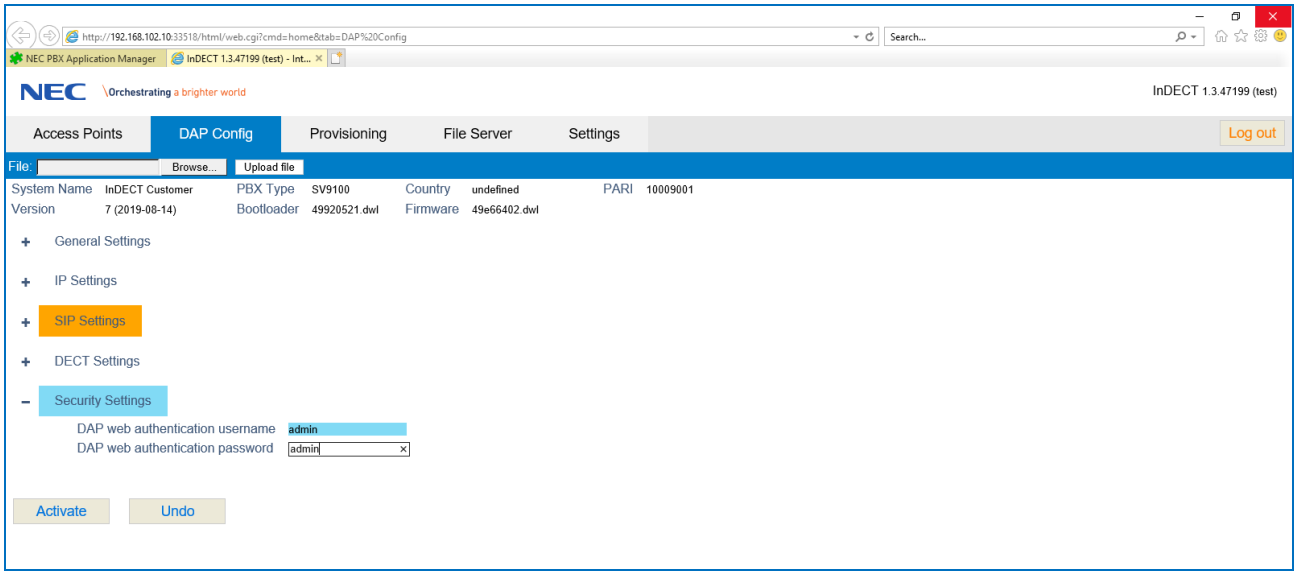
and go to the **File Server** screen.



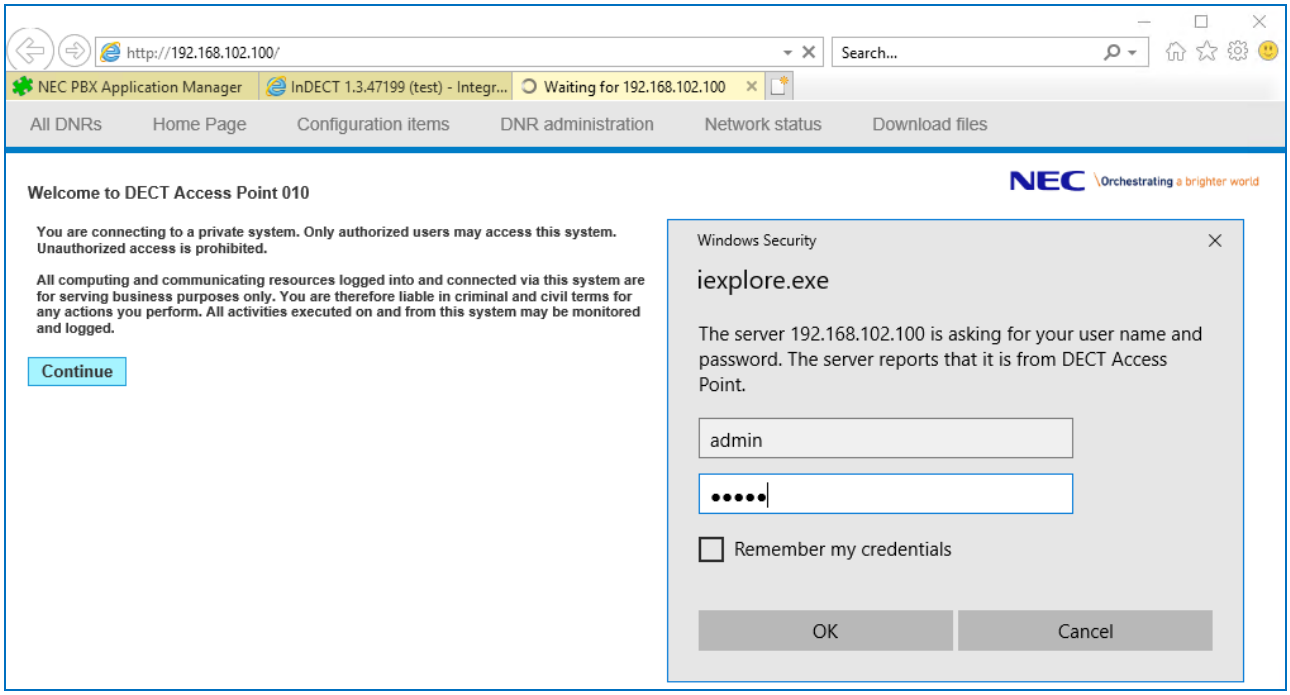

Expand the **Security Settings** section.



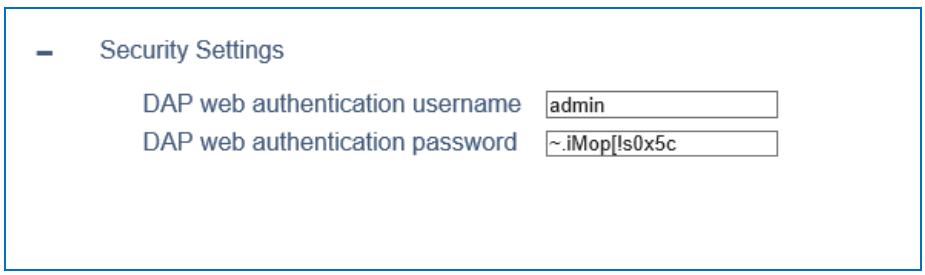

Fill in the user name and the password that you want to use on the DAP WEB Pages.




Click the **Activate** button and then **OK** button at the prompt asking if you want to reboot the DAPs for them to detect the configuration changes. After the reboot, the Login on the DAPs is active.




Please note that the password that you have entered in the DAP Configurator is encrypted in the DAP Configurator.



# Synchronisation

***Note:*** *This chapter is not applicable for the Hotspot mode. In Hotspot mode, DAPs do not synchronize.*

## What about Synchronisation

DAPs must be synchronized with each other to allow handset handover between DAPs during a call. This means that each DAP should “see” two or more other DAPs in the air.

Each DAP has a cell around it, in which you can make and receive phone calls. The minimum signal strength must be -72 dBm. However, for synchronization a DAP should receive signal from at least one other DAP with a signal strength of at least -80 dBm (down to -85 dBm.) See Figure. Coverage for Synchronisation

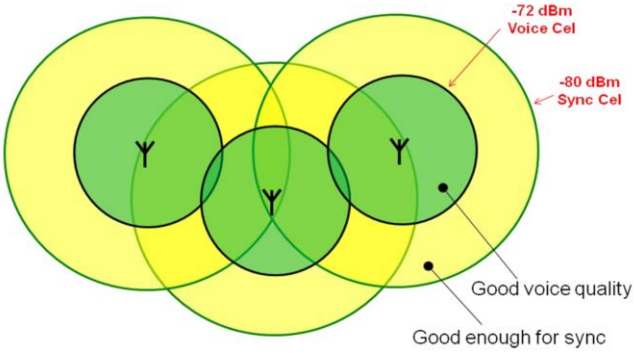



Figure. Coverage for Synchronisation

When DAPs try to synchronize to each other, there must be a hierarchy structure. The system arranges this itself to a certain extend.

However, when you have started the system for the first time, you should use the “Optimize” feature to make sure that the synchronization structure is setup efficiently. After that the synchronization structure will not change, unless you move DAPs or make changes in the DAPs (adding DAPs etc.). When you have made changes, you must run the “Optimize” feature again.

Each DAP has its own unique identifier, the RPN (Radio Part Number). The RPN is a hexadecimal three digit number in the range 000 – 01F. The DAP with the lowest RPN will be the synchronization master/source. The other DAPs will try to synchronize to a DAP that has the shortest path to the synchronization master/source. Normally, the master/source will be more or less in the middle of the IP DECT System. But that is determined by the Optimize Feature. See Figure. Synchronisation Hierarchy.

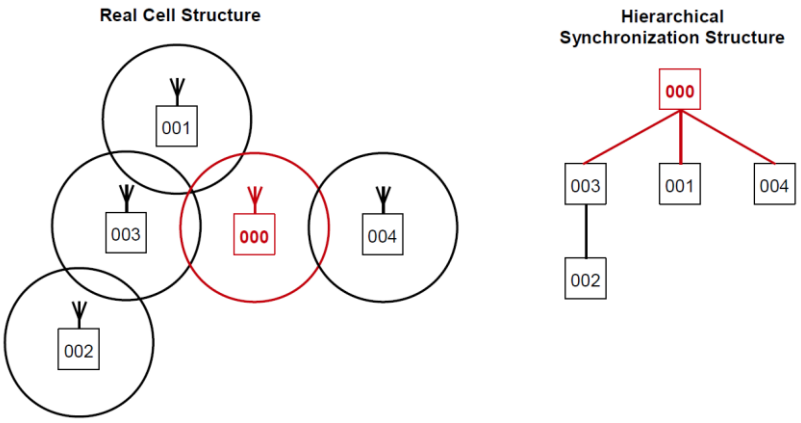



Figure. Synchronisation Hierarchy.

## How to Check the Synchronisation Structure

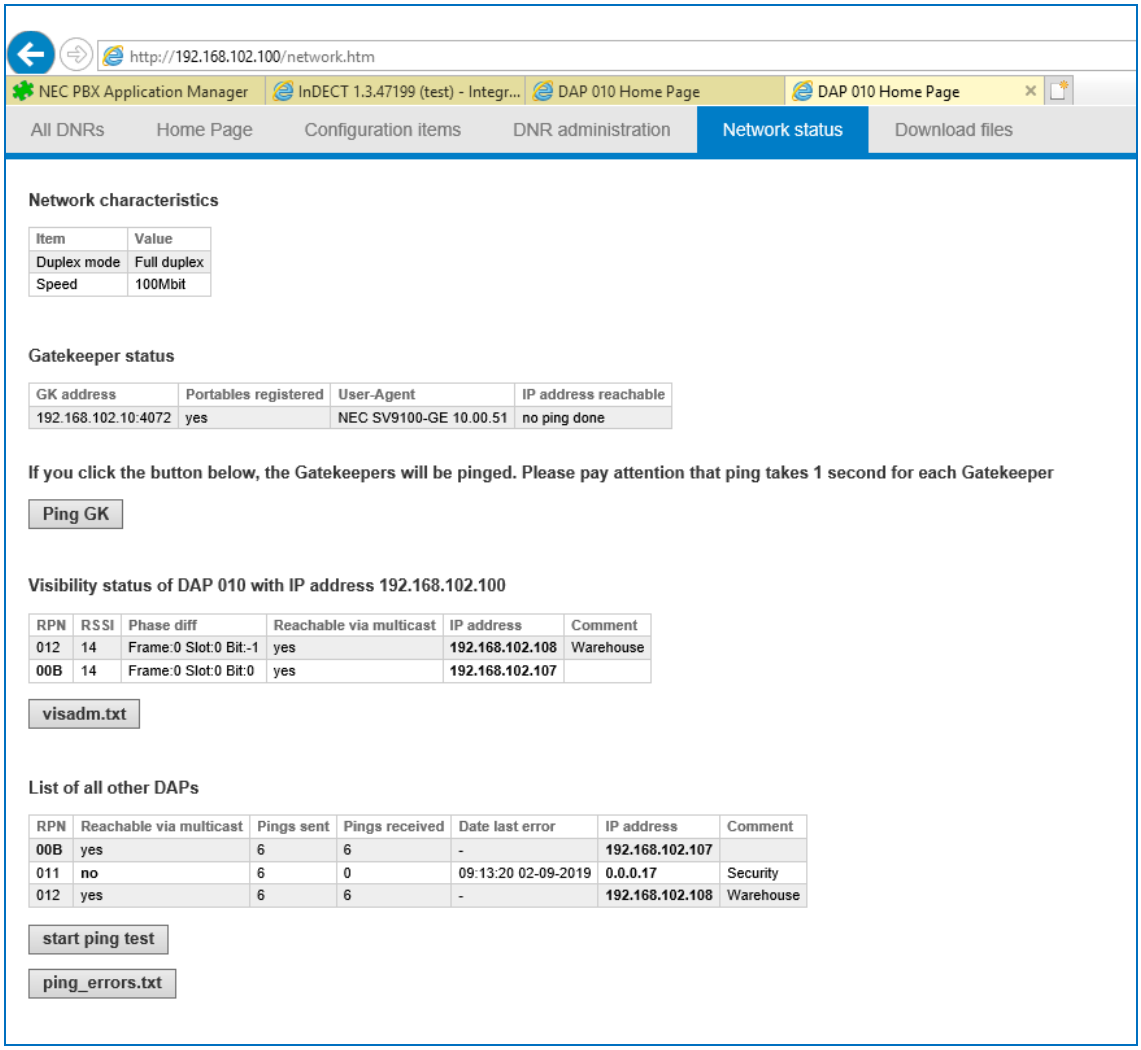
After you have done an installation, it is necessary to do a quick check of the synchronisation structure.

You can simply check the synchronisation structure by means of the information in the DAP WEB Page.

Make sure that the system is running *for at least 5 minutes*.

Open the WEB Page of one of the DAPs from the **Access Points** screen.

Click to view the **Network Status** screen. You will see the following window displayed.




Check the part "*Visibility status of DAP 000 with IP Address*".

Here you see an overview of the DAPs that are seen by this DAP.

Check that:

- *There is at least one DAP with an RSSI value (signal strength) of "3" or higher!*
- *All shown DAPs have a Phase Diff in the Bit range -7 to 7. (Frame and Slot must both be "0".)*

If the above mentioned requirements are not met, you must change the position of one or more DAPs.

Repeat step 1 to 4 for all other DAPs.

Please note that you can download the synchronisation information by means of clicking the button `visadm.txt`. Check that all DAPs are directly or in-directly connected to the Master DAP via the hierarchical structure (see Figure. Synchronisation Hierarchy.

## RSSI and Phase Diff (More Insight)

In the DAP Web interface, on the **Network status** screen, there are two important items that gives information about the synchronisation between the DAPs:

- **RSSI**

  The RSSI is Radio Signal Strength Indication. It gives a signal Strength value of the received signal from another DAP. This value is in the range 0 ...14. However, for synchronisation, the minimum signal strength should be 3 from at least one other DAP. However, it is strongly recommended to position the DAPs in such a way that all DAPs see at least two other DAPs with a signal strength of 3 or higher.

- **Phase Diff**

  The phase difference gives information about the actual synchronisation. It shows the difference between the clock signals between DAPs. There are three indications: *Frame, Slot and Bit*.
  The "*Frame"* indication must always be "0".
  The "*Slot"* indication should also always be "0".
  The "*Bit"* value ***must be*** in the range -7 to 7 for ALL DAPs.
  When the value of one of the DAPs is not in this range, synchronisation is not established and handset handover is not possible.

  When the Phase Difference is out of range, the following three items could be the cause:

  - Not sufficient signal strength between the DAPs.
  - Multicast problems on the IP network.
  - Too many reflections in the environment (due to too much metal in the environment).

# Time Provisioning

The handsets in an InDECT IP DECT system must show the correct date and time in the display. This date and time comes from the DAPs. This means that the DAPs should have the correct time. There are several sources available. In the next overview you see the time source selection according to their priority.

| Priority | Source | Remarks |
|---|---|---|
| 1 | SV9100 or SL2100 PBX | Only when the PBX issues the time and date in the interface protocol, either SIP or iSIP.<br>When SIP, see RFC3261. |
| 2 | NTP (Network Time Protocol) Server (Not currently supported by InDECT but will be in a future release for now the DHCP NTP server options can be configured) | Priority **5 a**<br>The DAPs must know where to find the NTP, in other words, it must know one or more NTP IP addresses. The DAPs can get their NTP addresses via DHCP option 42 and option 100 (POSIX). The DHCP Server can issue up to 5 NTP IP addresses. However, the DAPs will only store maximum 2 NTP IP Addresses: a Primary and Backup. When the DHCP server does not provide the NTP IP addresses and you want to use an NTP, you can enter these addresses manually in the DAP Configurator, see cell below. |
| | | Priority **5 b**<br>When the DHCP server does not provide the NTP IP Address via option 42 and if necessary option 100 for the POSIX time, and you want to use NTP, you can enter the IP address of the NTP server in the DAP Configurator. |
| 3 | DAP | When the DAP cannot find any of the Time sources mentioned above, it will try to get the date and time from another DAP. Each DAP issues the date and time at least every 20 seconds. |

## DHCP Option 42 and Option 100.

A DHCP Server offers two options that can be used for date and time settings:

- **Option 42**
  This option can be used to send one or two NTP Server IP addresses to the DAPs. The DAPs will contact the NTP Server regularly (every 1024 seconds).

- **Option 100**

  This option can be used to send the POSIX date and time location to the DAPs. It consists of a special text string that defines the time zone offset from UTC, along with information on Daylight Saving Time. An example of this definition for the Eastern time zone in America is ”EST5EDT4,M3.2.0/02:00,M11.1.0/02:00”.

  See RFC 4833 “Timezone Options for DHCP.

For your info:

The **Unix epoch** (or **Unix time** or **POSIX time** or **Unix timestamp**) is the number of seconds that have elapsed since January 1, 1970 (midnight UTC/GMT), not counting leap seconds. The “epoch” is *Unix time 0* (midnight 1/1/1970), but 'epoch' is often used as a synonym for 'Unix time'.

# Hotspots

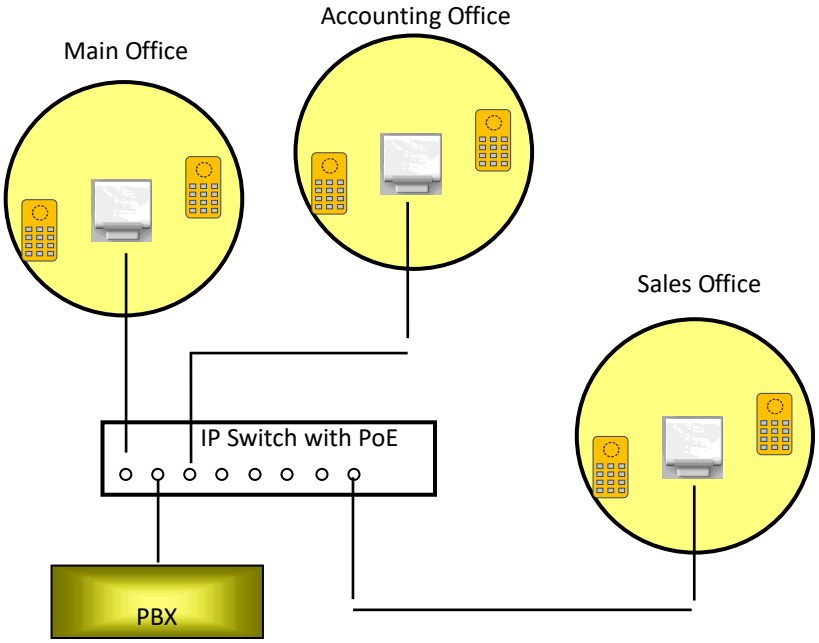
InDECT supports the option of hotspots. When enabled, the DAPs will not synchronize to each other anymore and they don't "see" each other anymore via the air. Each DAP will behave as a stand-alone cell.

This means that:

- there is ***no*** "handover" possible between the DAPs.
- "Roaming" is possible with a disconnection from current Hotspot DAP.

***Note:*** *There should not be any overlap between cells. This means that the distance between the hotspots must be such, that a handset never "sees" two DAPs.*

***Note:*** *in Hotspot mode, the output of the DAPs is reduced to 12 dBm. (Normal operation is 24 dBm).*




When the handset moves to another hotspot (DAP), the subscription record of the handset will move with it to the other hotspot.

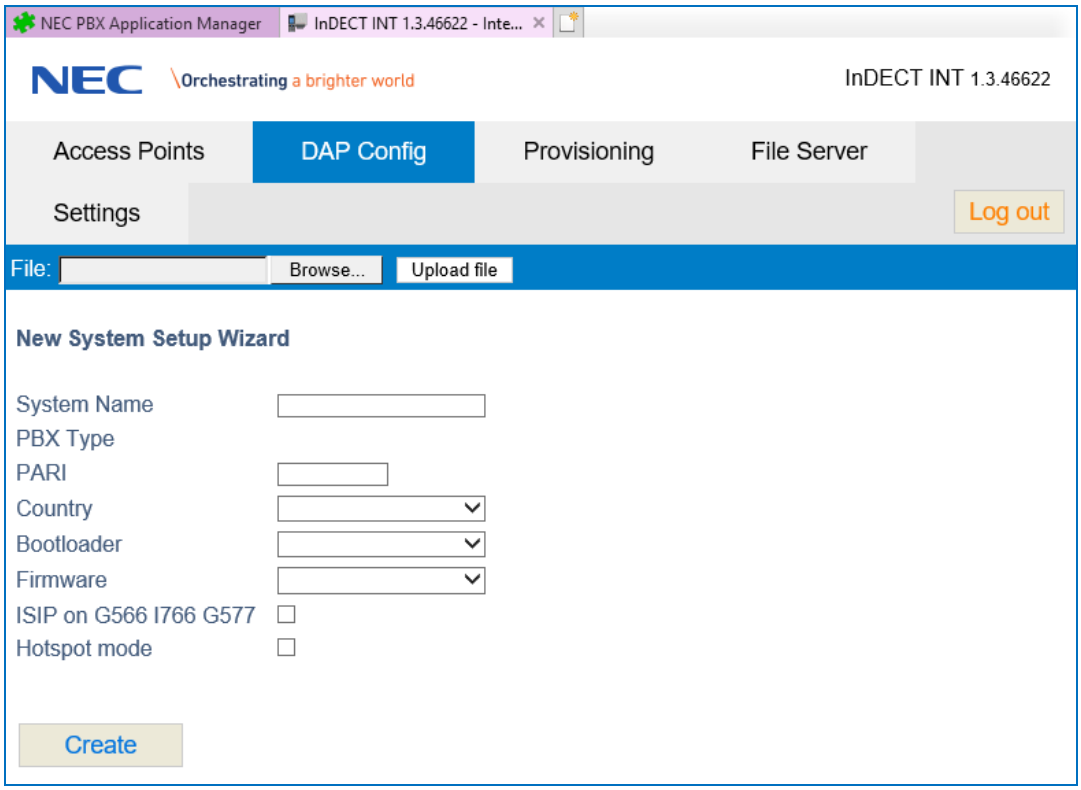
Please note that the distance between the individual DAPs must be such that the handset can never see more than one DAP. In open area, this will be around 200 meters between the DAPs. In office environment, the distance between the DAPs could be around 100 meters. However, you can only be sure about the distance when you measured it in advance.

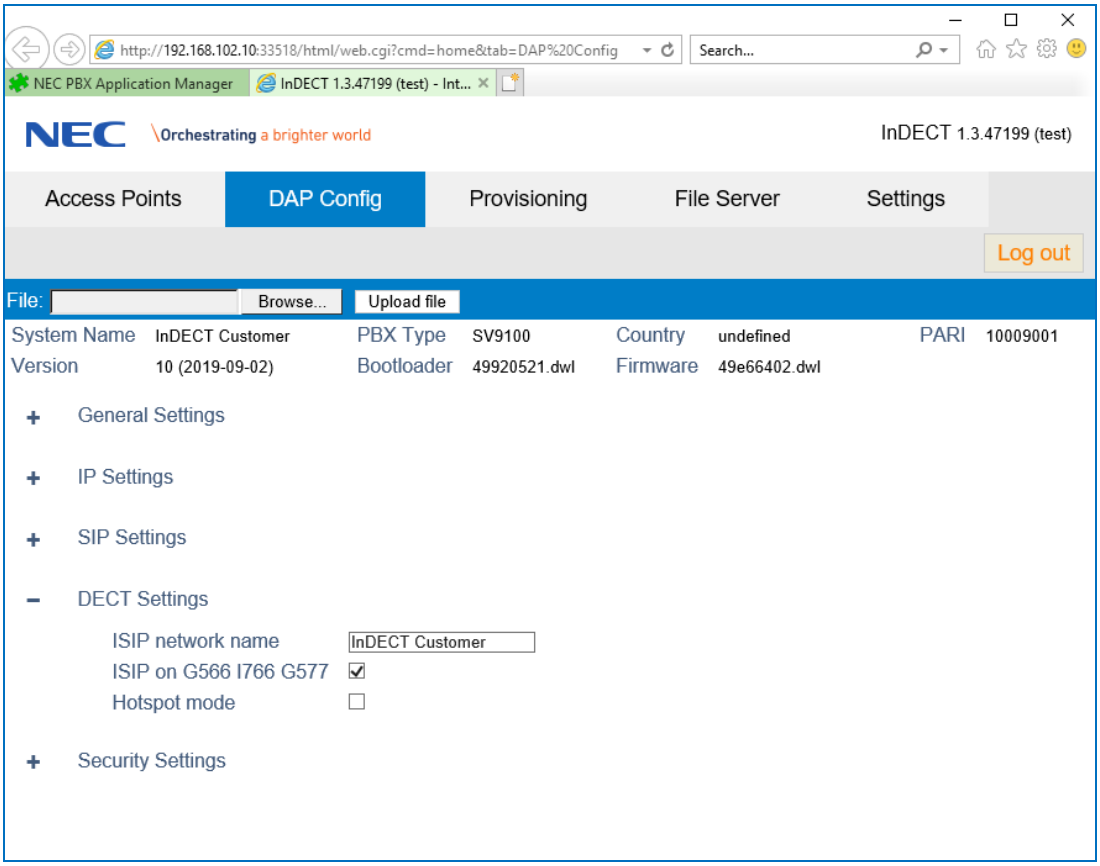
It is advised to have all DAPs together with the DAP Configurator PC (when present) in one IP subnet. In case of having DAPs in different IP Subnets, you must make sure that IP Multicast is supported over the routers.

- **How to enable Hotspot mode?**

  You can enable the hotspot mode during setting up of a new system configuration or from the **DAP Config** screen.

Also see the screens below.



# Troubleshooting

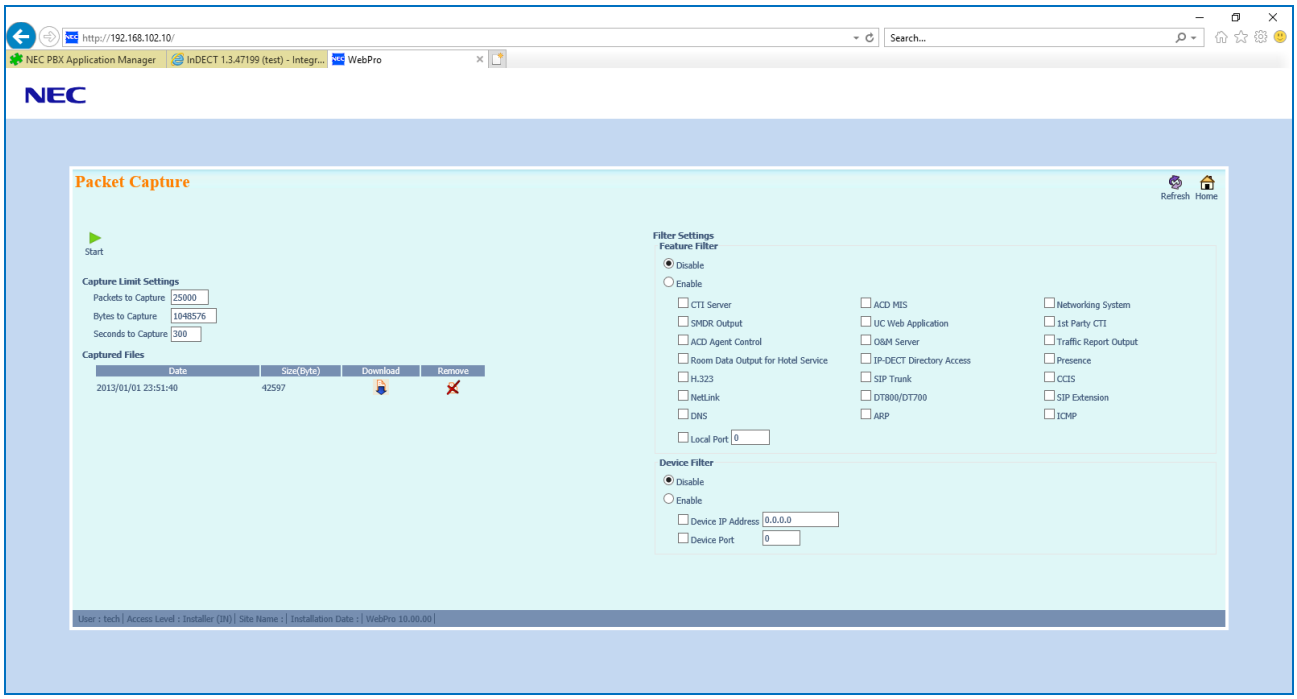
## Making Traces

When there are problems at the interface level between the DAPs and the PBX, you will probably need to make a network protocol trace. Please note that for making a trace, you need to have a laptop PC or other PC that can be installed with an application such as Wireshark in order to look at the capture files further.

To create the capture file. Access WebPro on the PBX and go to the Packet Capture function (SL2100 screens will differ from the SV9100 but function is similar)

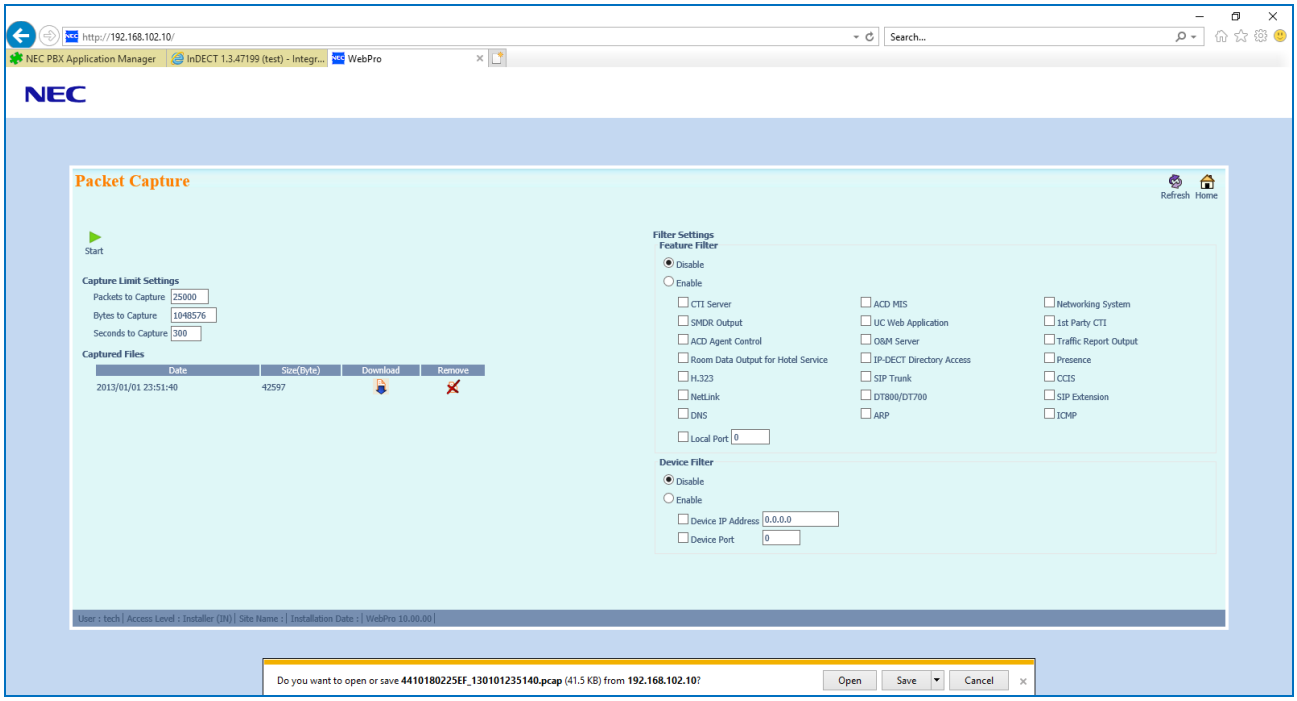
Begin capturing network traffic by pressing the **Start** button 

.

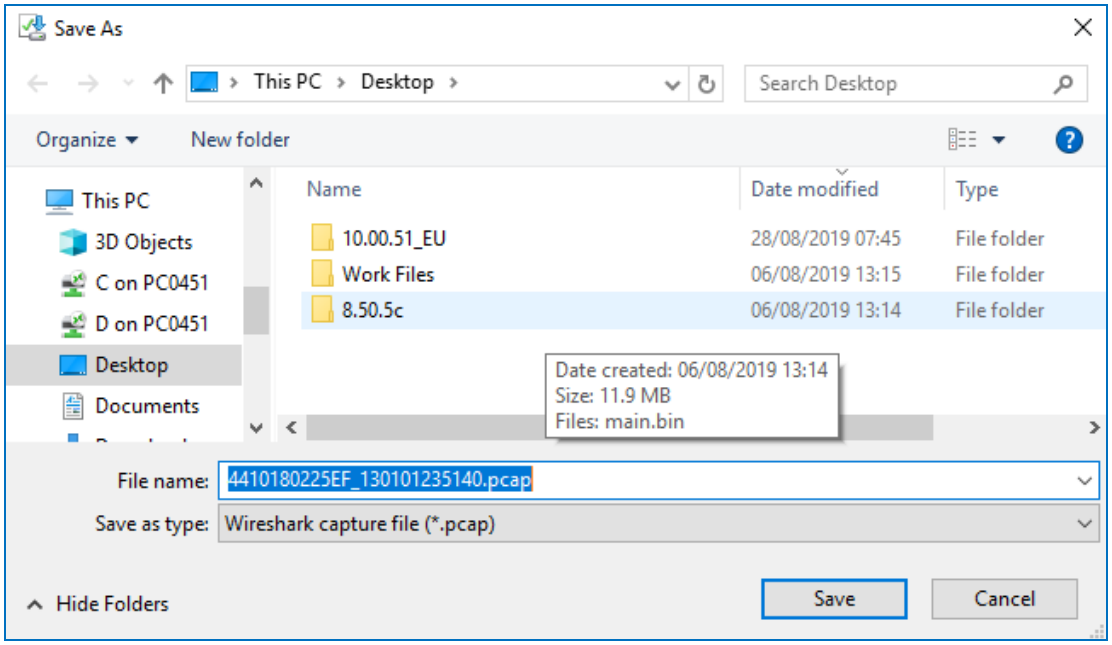



Perform the problem operation to recreate a specific issue and capture the network traffic. Once this is recreated press the **Stop** button 

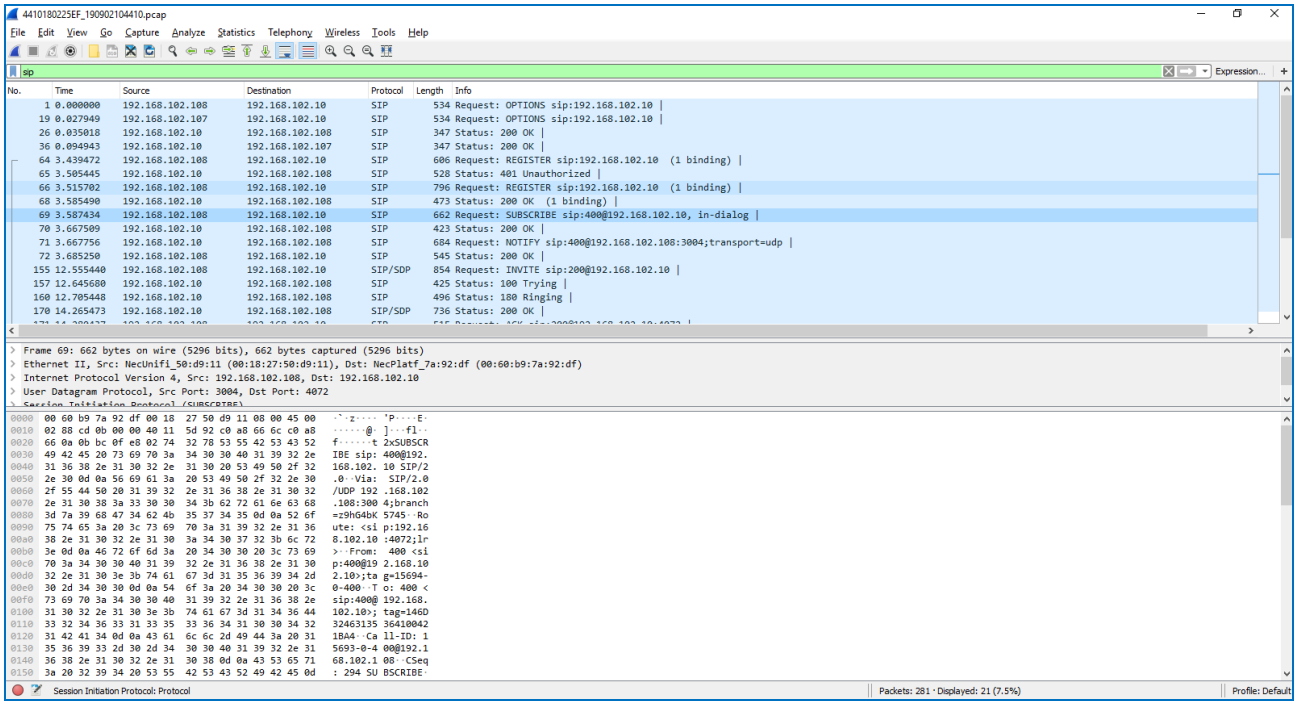
to end the packet capture and download the capture file from the PBX using the **Download** button 
.




Save the file to a save location on your computer.

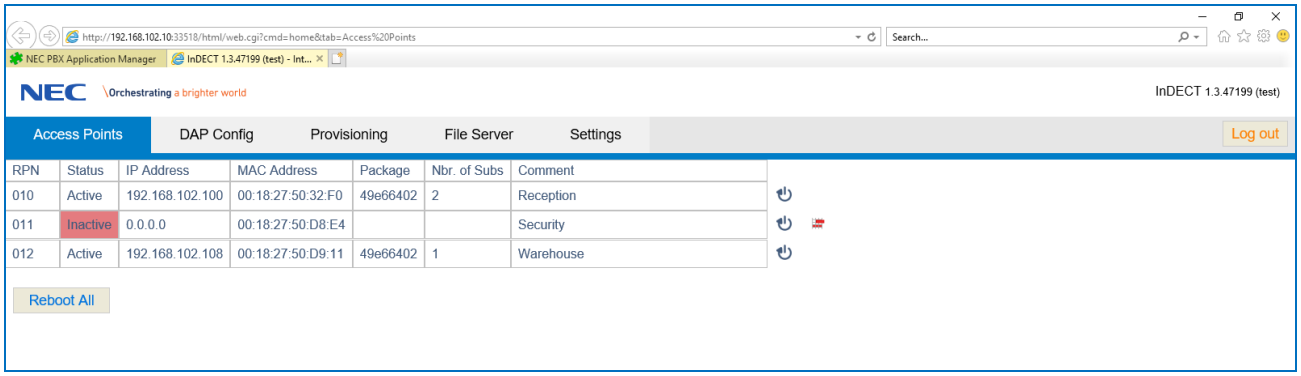



This file can now be opened and analysed further using Wireshark or simlar packet capture analysis tool.



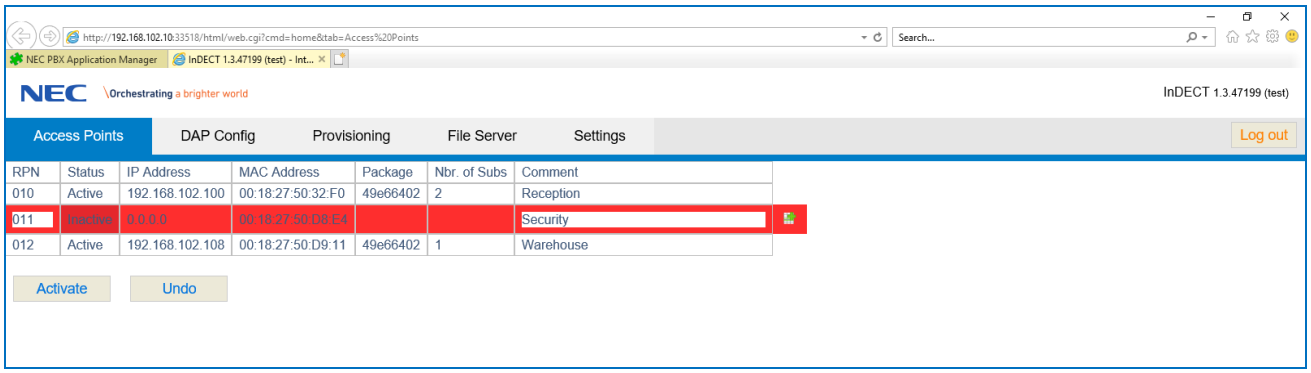
# How To Replace A DAP

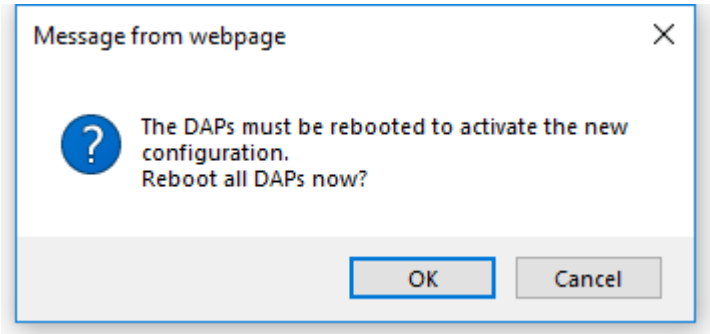
When a DAP is not operating as expected with InDECT, it will be displayed with a status as ‘Inactive’ on the **Access Points** screen. At this point disconnect the DAP that must be replaced.




To remove the DAP from InDECT press the **Remove DAP** button  next to the row listed as ‘Inactive’. The row will change to be RED highlight.

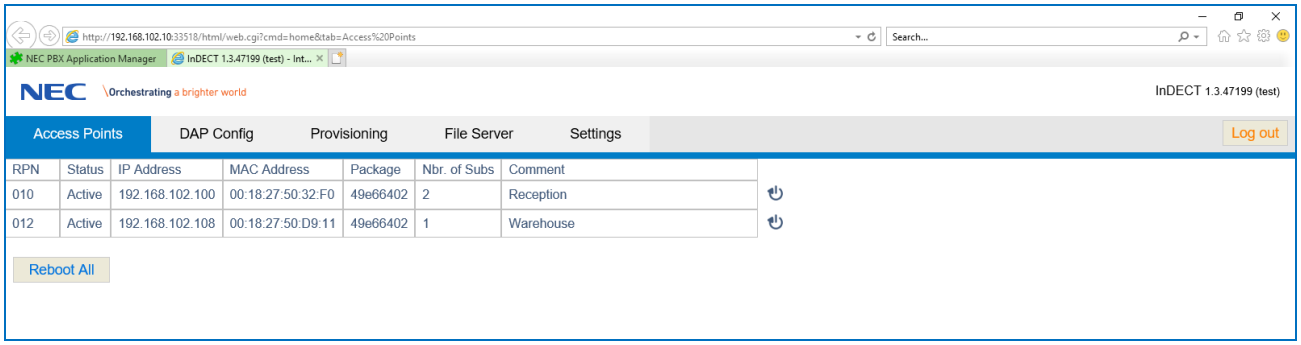
Send the changes to the DAPs by pressing the **Activate** button and then the **OK** button at the prompt asking if you want to reboot the DAPs for them to detect the configuration changes.



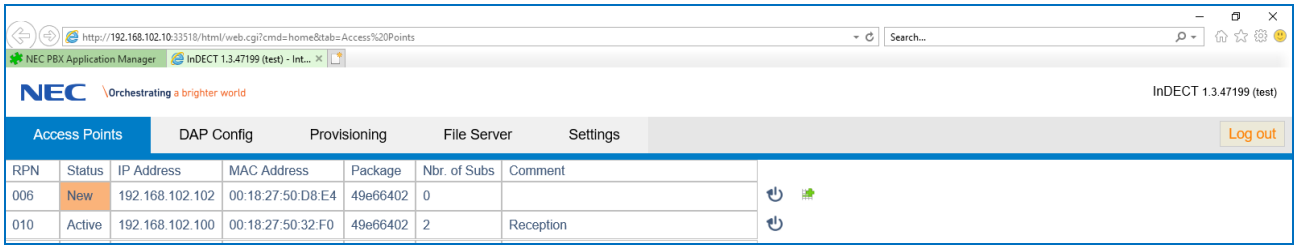



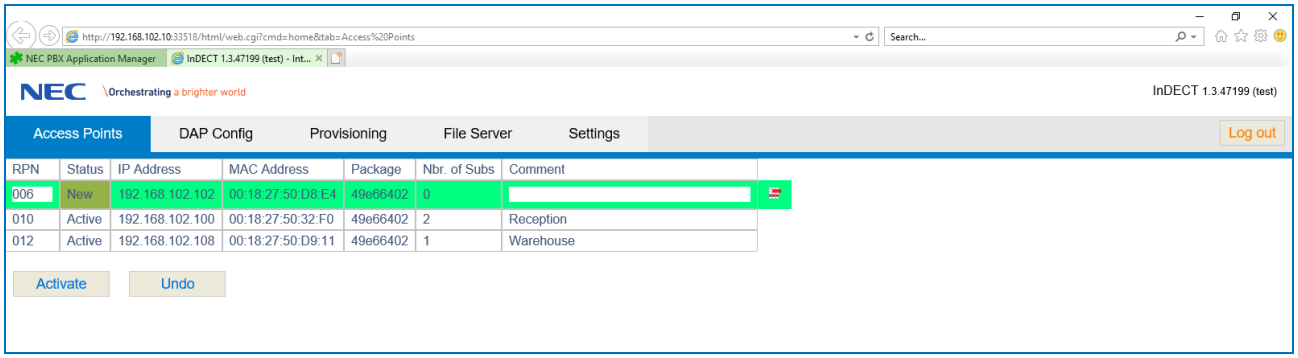
Once the ‘Inactive’ DAP has been removed from the InDECT system. The new DAP can be connected the system.

Connect the new DAP to the PBX network.

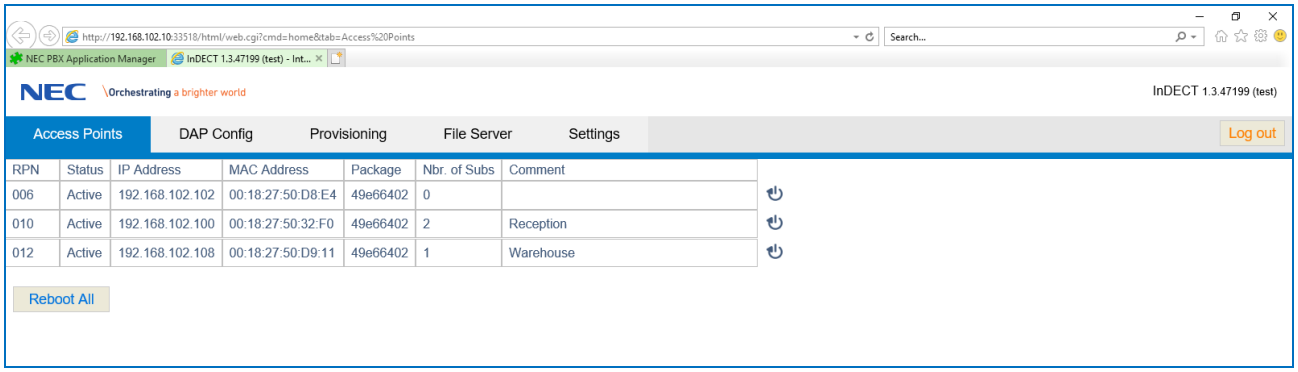



InDECT will detect the new DAP on the network and show it as ‘New’. To add detected access points to your InDECT system press the **Add** button  next to each access point.. The selected access point row should change to green highlight.




When ready to continue, press the **Activate** button and the system asks for a reboot of all DAPs. Press **OK** to reboot all DAPs.



# Provisioning Handset Firmware

## General

InDECT supports handset firmware updates over the air. This is done by means of the **Provisioning** screen.

Uploading the firmware to the handsets has the following characteristics:

- Upload time per handset can be as much as 4 hours.
- Handset remains fully operational during the upload process. Updating does not disturb the normal operation of the handset.
- The user will NOT notice that firmware uploading is taking place.
- Only when the new firmware package has been uploaded successfully and the handset is in the charger for more than one minute, the new firmware is activated.
- Upload process is fail-safe. Even when the handset goes down as a result of an empty battery, the upload process will resume when the handset is back again.
- While the upload takes place, one channel on a DAP is occupied.

  **Important** – Due to DAP channel occupation during FW uploading, the number of simultaneous uploads should be limited, by default InDECT has it set to 6 simultaneous updates.

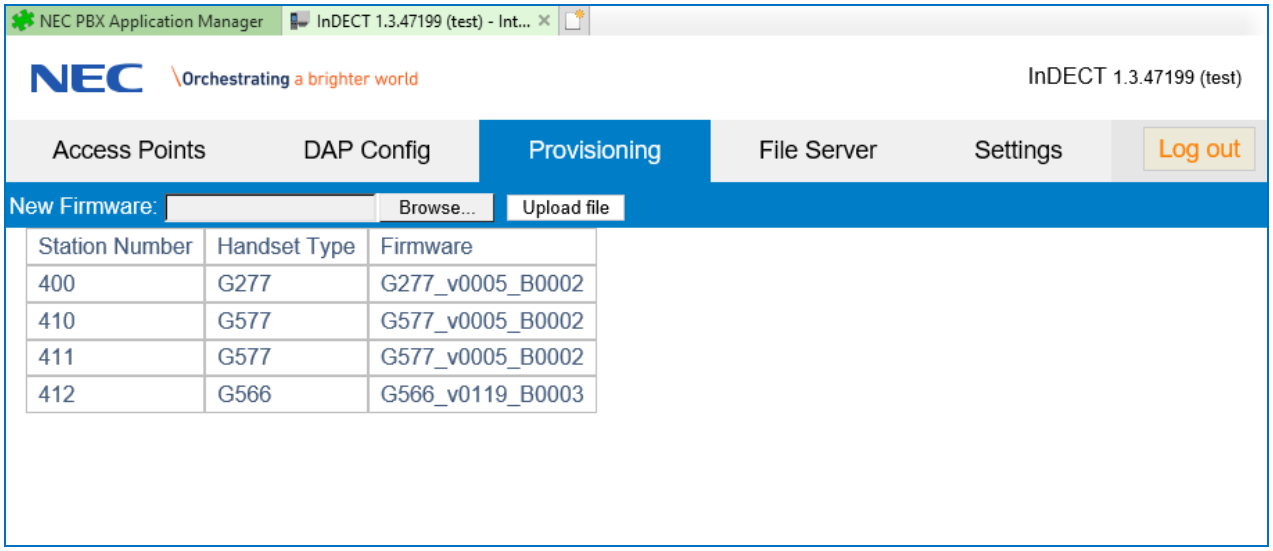
## Supported Handsets

Handset Firmware Upload is available for the following handsets:

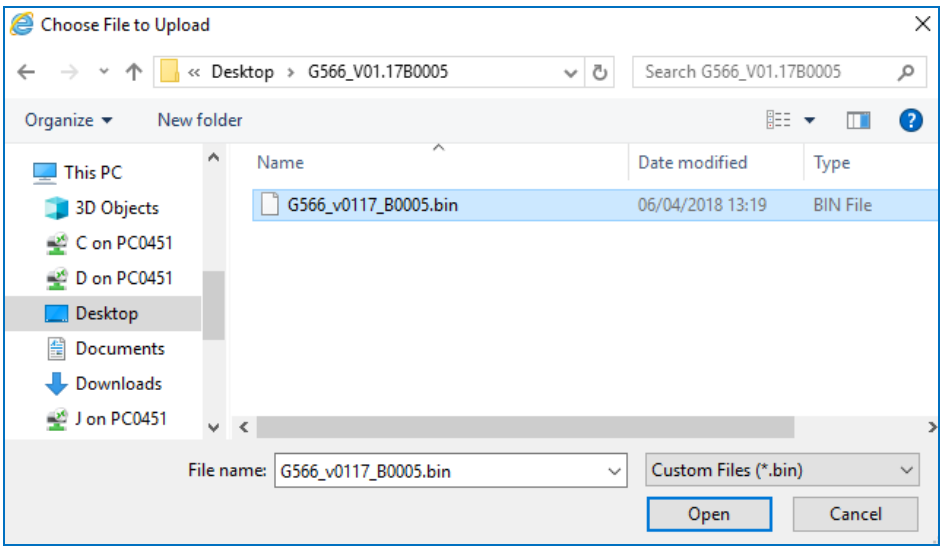
- G266
- G277
- G566
- G577/G577h
- I766

## Firmware Update Procedure

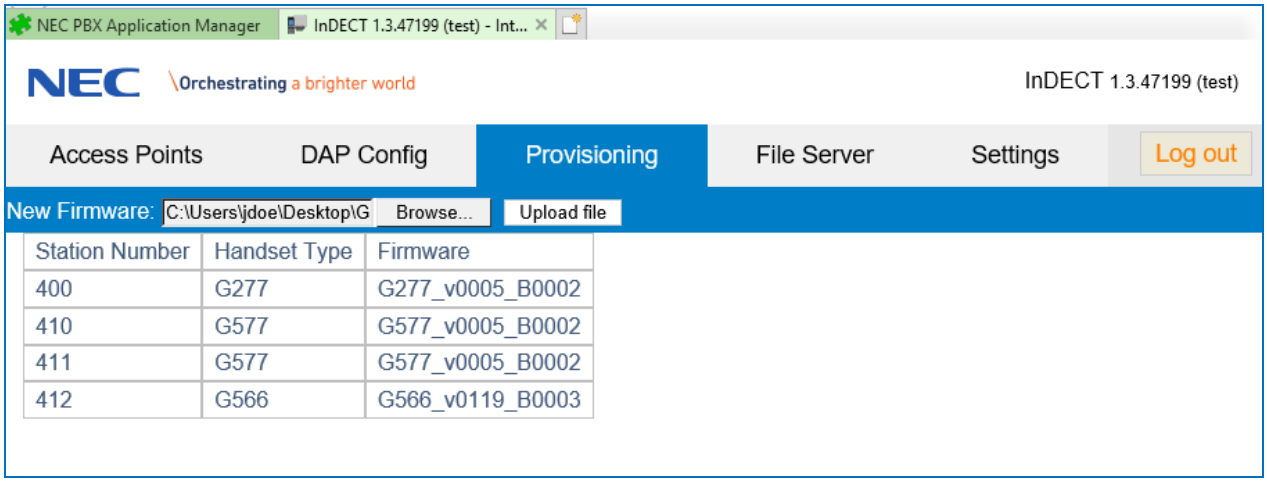
Go to the **Provisioning** screen. Handsets subscribed to the InDECT system will be displayed here along with their current firmware running on the device.



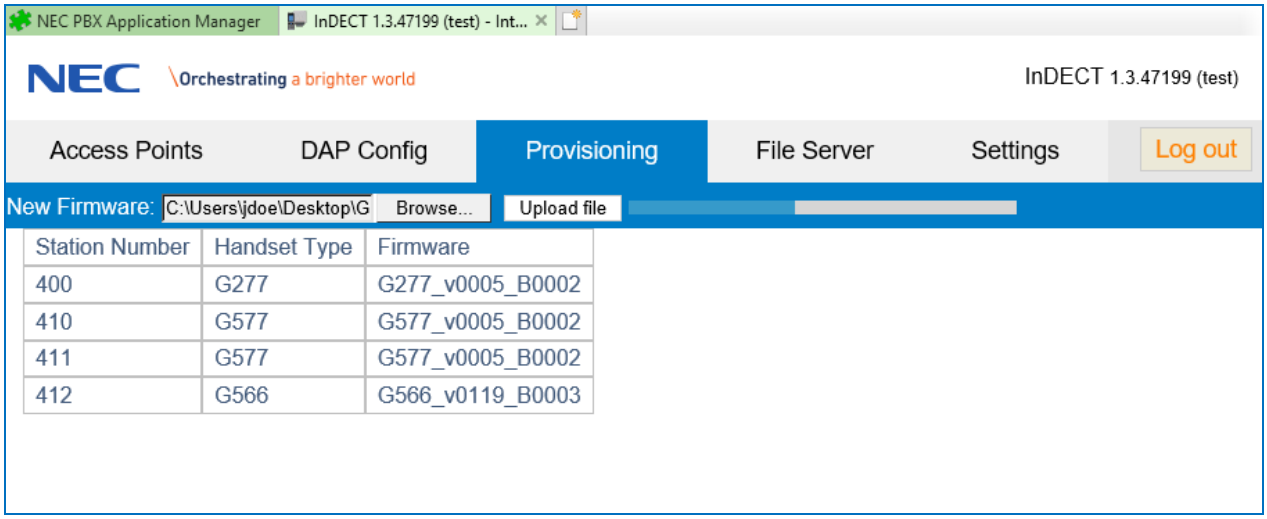

Press the **Browse** button and locate a valid firmware package for the handset type you want to update the firmware to. Press the **Open** button to select the file.



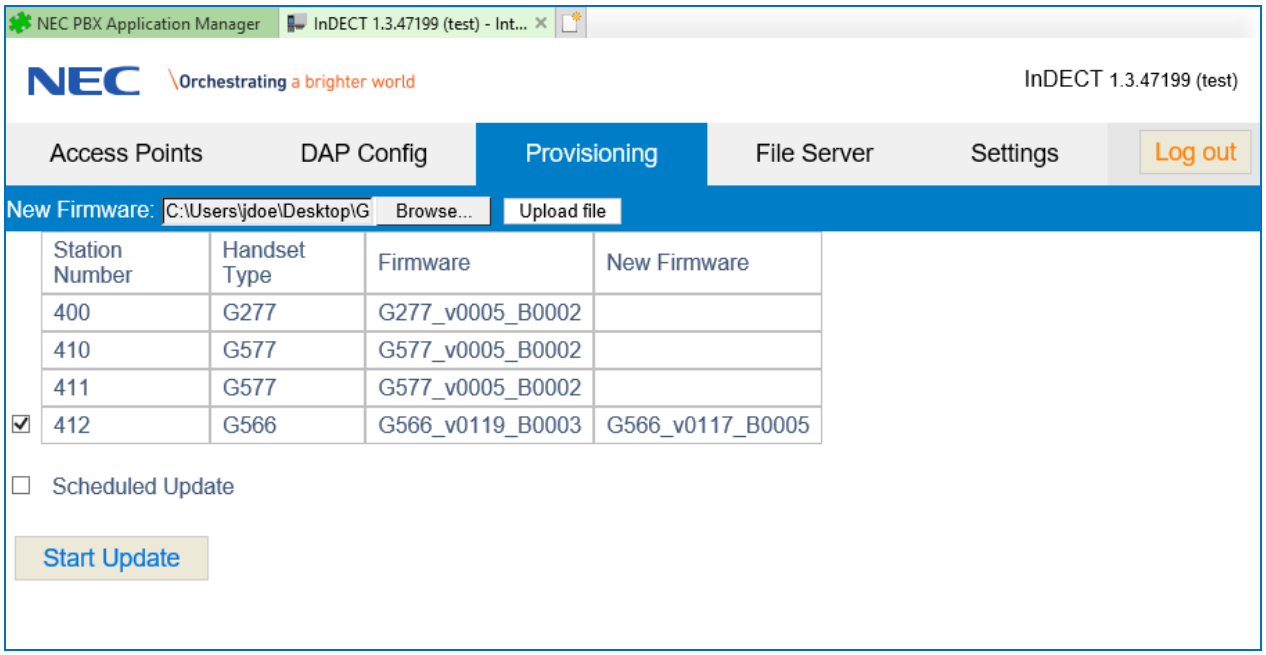

Press the **Upload File** button to transfer the file to the PBX file server.



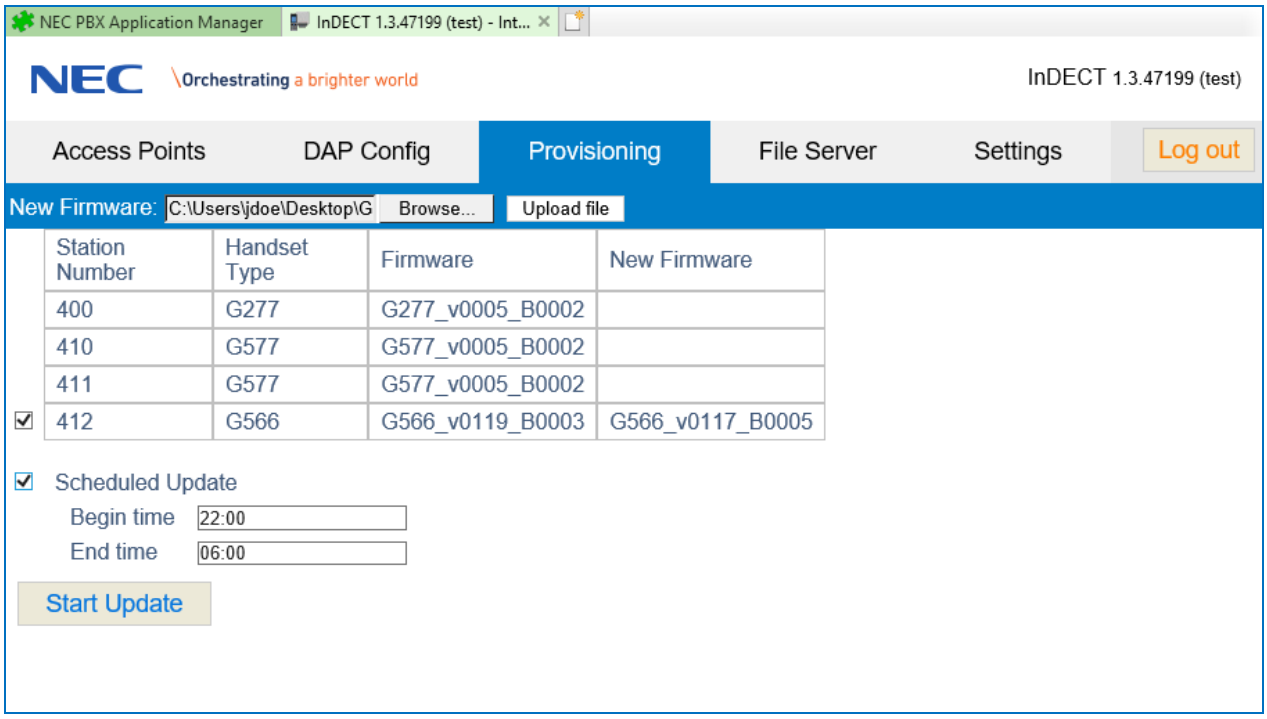

Wait until the blue progress bar is filled and the new package is listed next to the supported handset type.



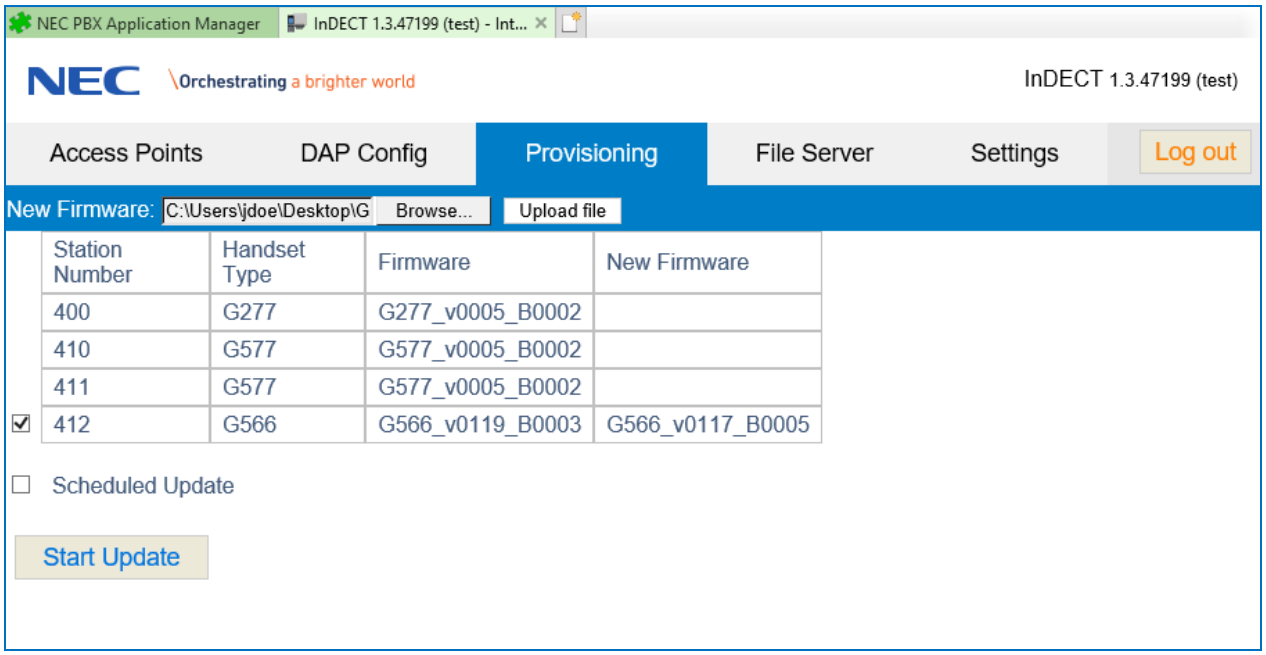

If multiple handets are available of the same type for the firmware package uploaded, then check the tick box of the devices you want to update down the left hand side of the screen next to the handsets Station Numbers.



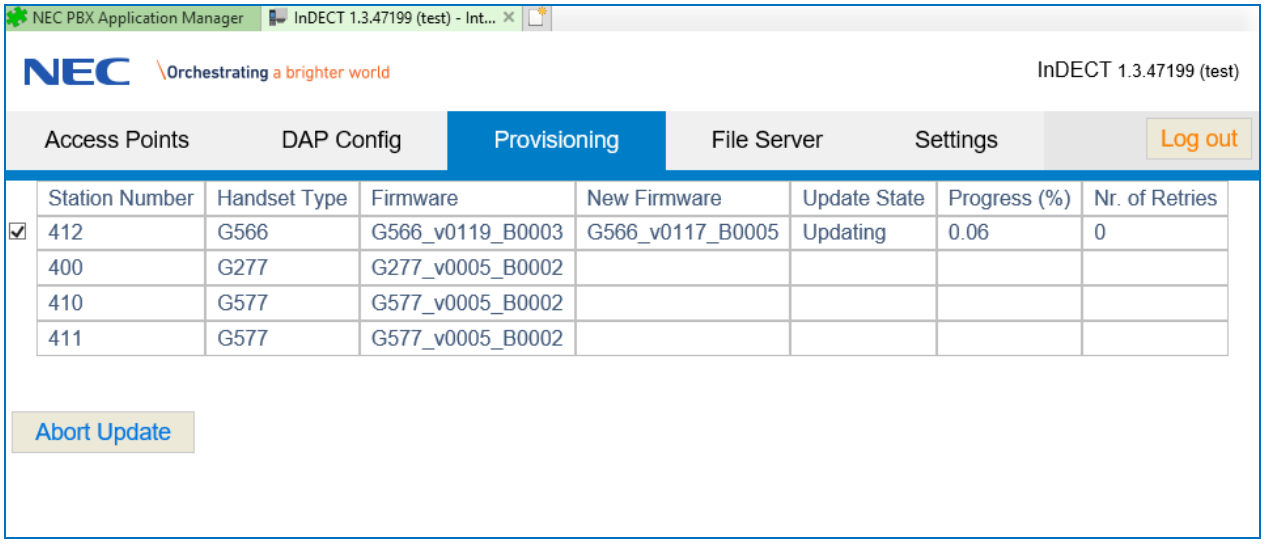
You can enable a schedule if you want to for the update to be performed automatically between a Start Time and End Time if entered. This schedule will operate on a daily basis.




To begin either a schedule update or manual update immediately press the **Start Update** button.




The update process will begin. If a scheduled update was set then the update will begin at the designated time.




Once the update has completed successfully, the handset will need to be first placed in it's charging cradle for the new firmware to be applied to the device.

# Settings Screen – User Configuration

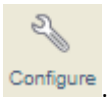
The **Settings** screen in InDECT can be used to configure additional users for the system if required.

You can create additional users in InDECT, so you do not always have to use the default installer user. The default installer username and password is tech/12345678

There are different user characteristics (roles) that can be applied to each user. These are detailed below.

| Characteristic | Typical User Type | Description | Screens Accessible |
|---|---|---|---|
| **VIEW** | End-user | Is enabled to inspect the state of the system, but is not allowed to make any changes. | [Access Points], [DAP Config] (read-only), [Provisioning] |
| **CHANGE** | IT Admin at customer site | Next to being enabled to inspect the state of the system, this user can changes the current DAP configuration; add/remove DAPs, change DAP settings, upload/download files. This user can not create or remove a DAP configuration, nor change the settings of InDECT itself through the Settings screen. | [Access Points], [DAP Config], [Provisioning], [File Server] |
| **CONFIG** | PBX Service Engineer | This engineer installs InDECT and is allowed to change its settings later on. This engineer can also create and remove DAP configurations all together. | [Access Points], [DAP Config], [Provisioning], [File Server], [Settings] |

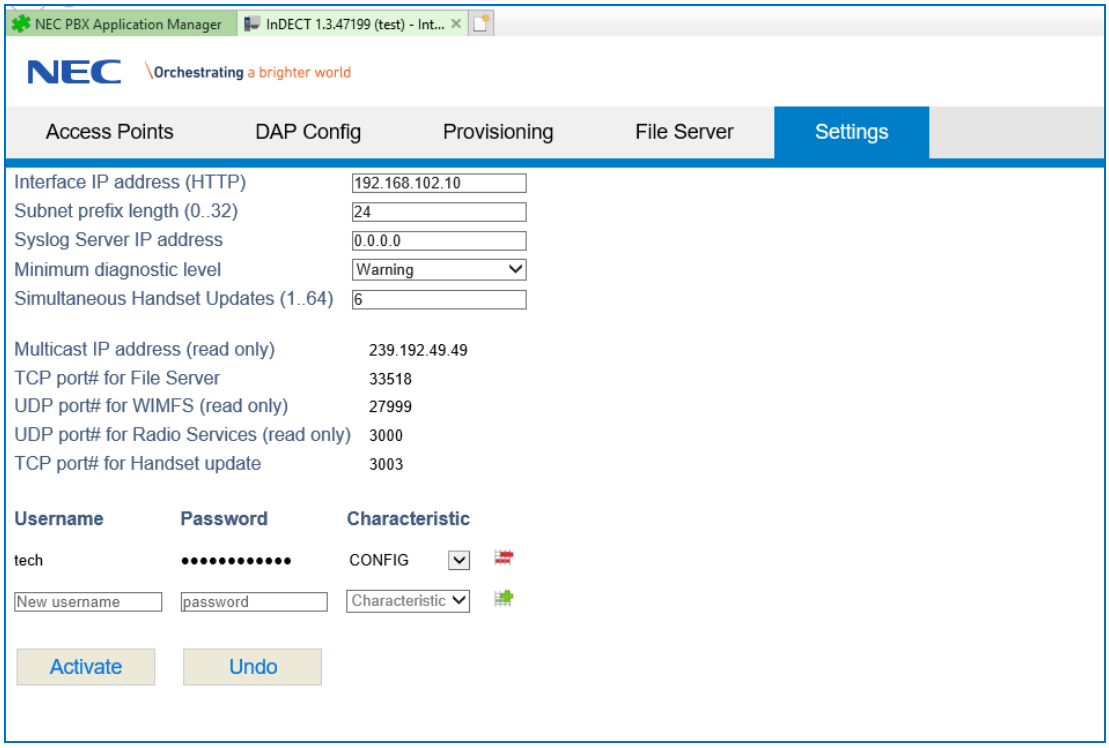
A user with VIEW or CHANGE characteristic can only access InDECT using the **InDECT INT** button 

. Users with CONFIG characteristic can access InDECT using the **Configure** button 

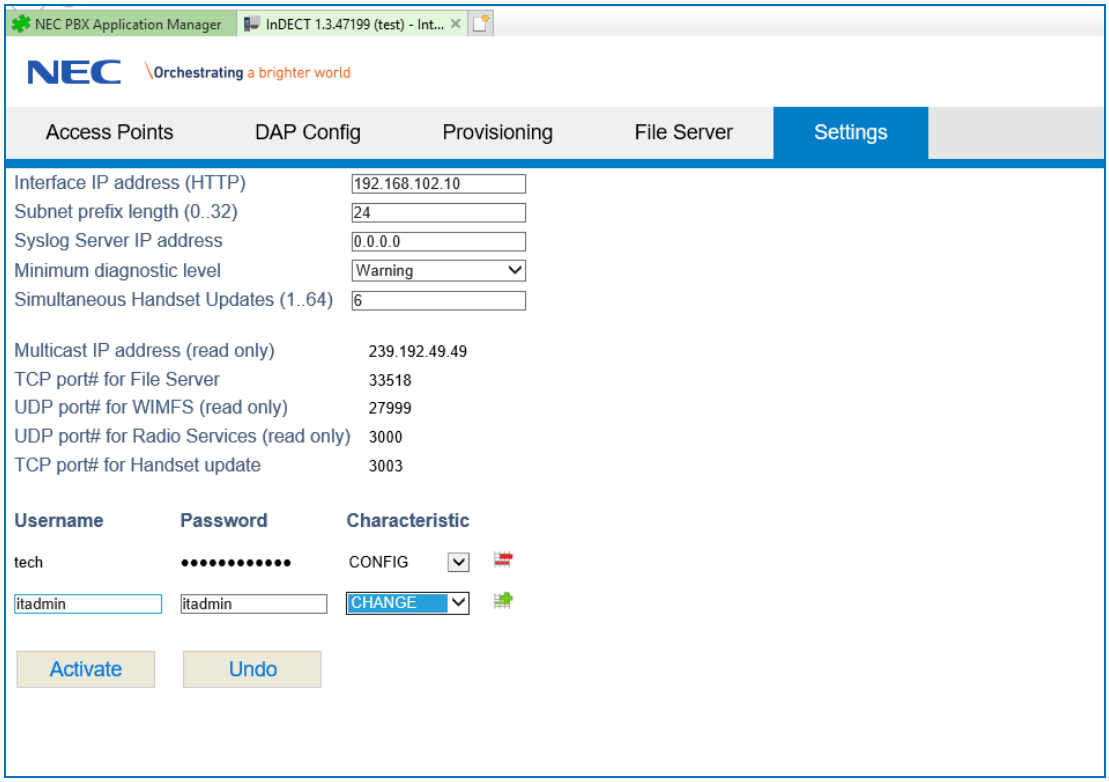
.

## Adding a new user

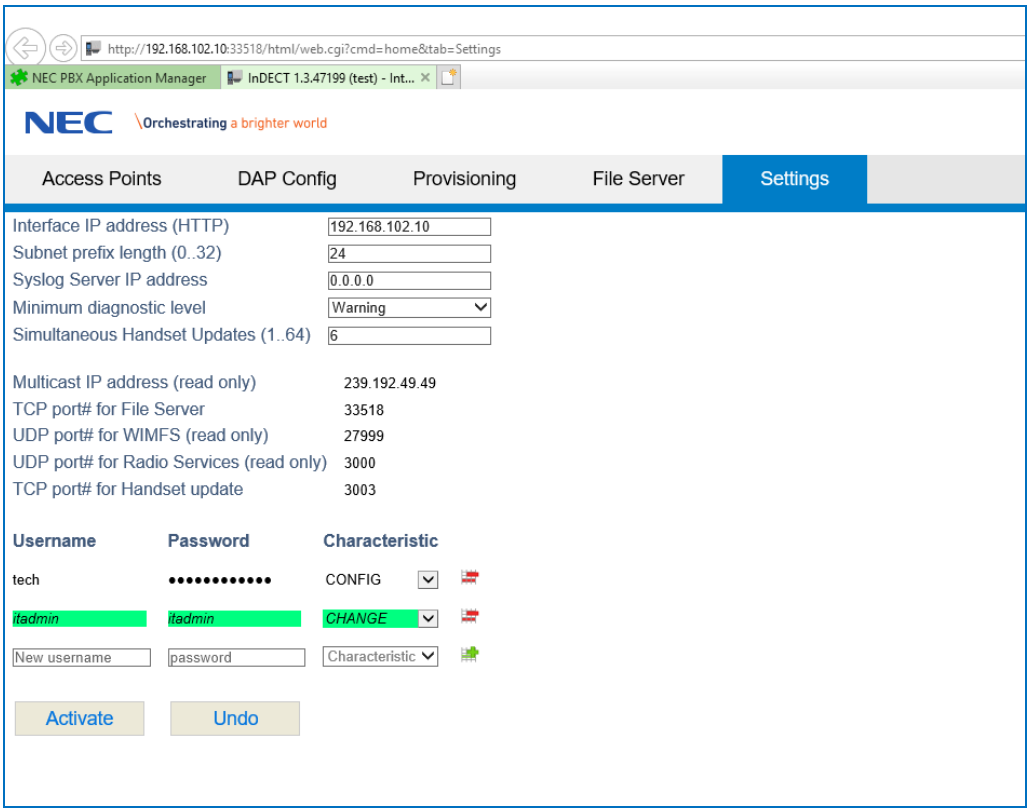
Open the **Settings** screen.



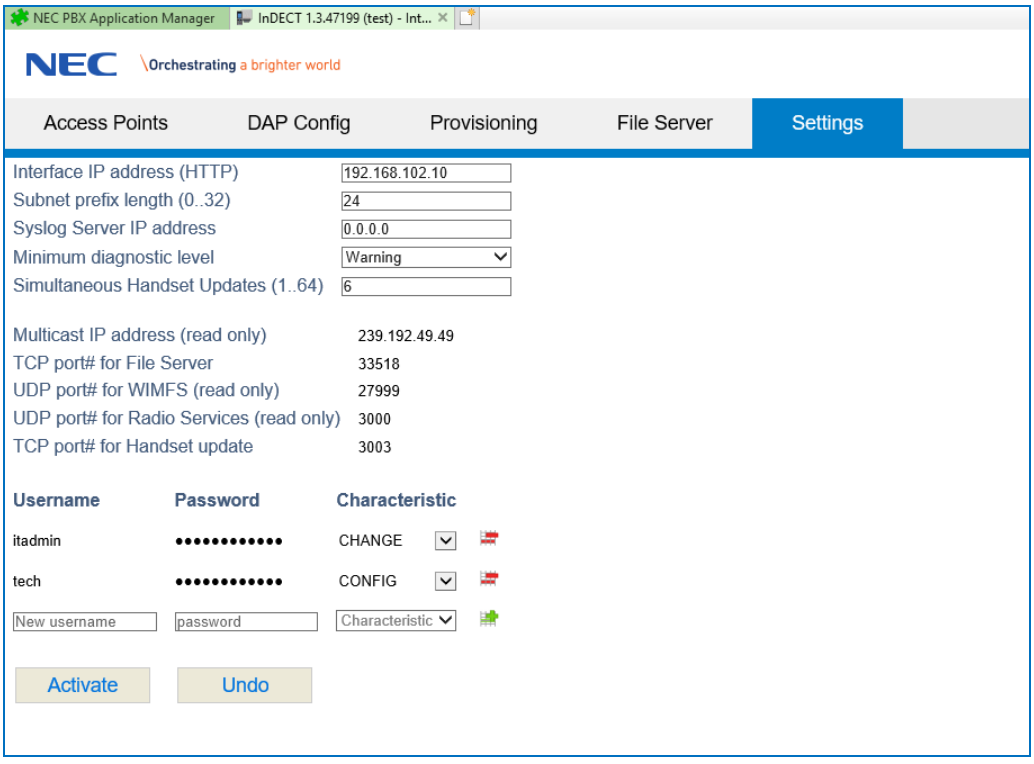

Enter a username and password and select the characteristic for the user.



To add the user press the **Add** button  next to the username entered The selected user row should change to green highlight.

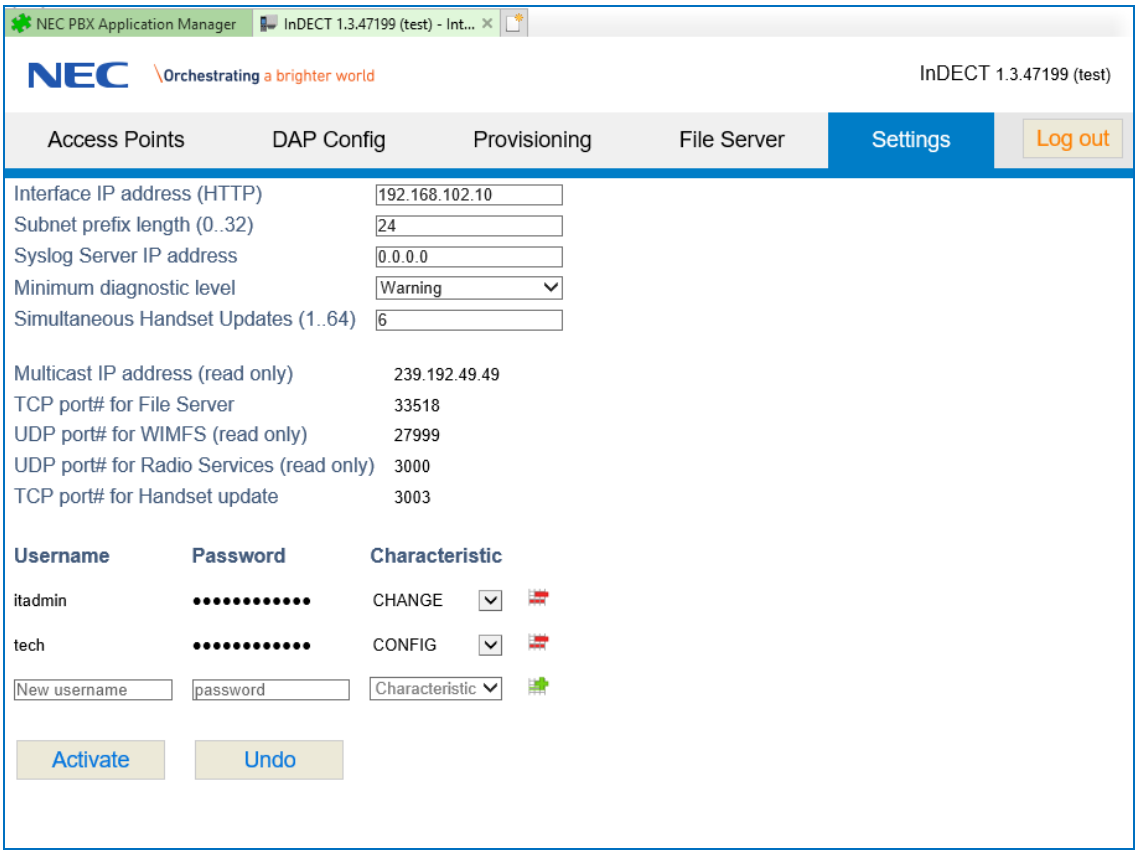



When ready to continue, press the **Activate** button and the system will add the new user. You can now access InDECT user the entered username/password using the relevant application icon depending on the characteristic set.

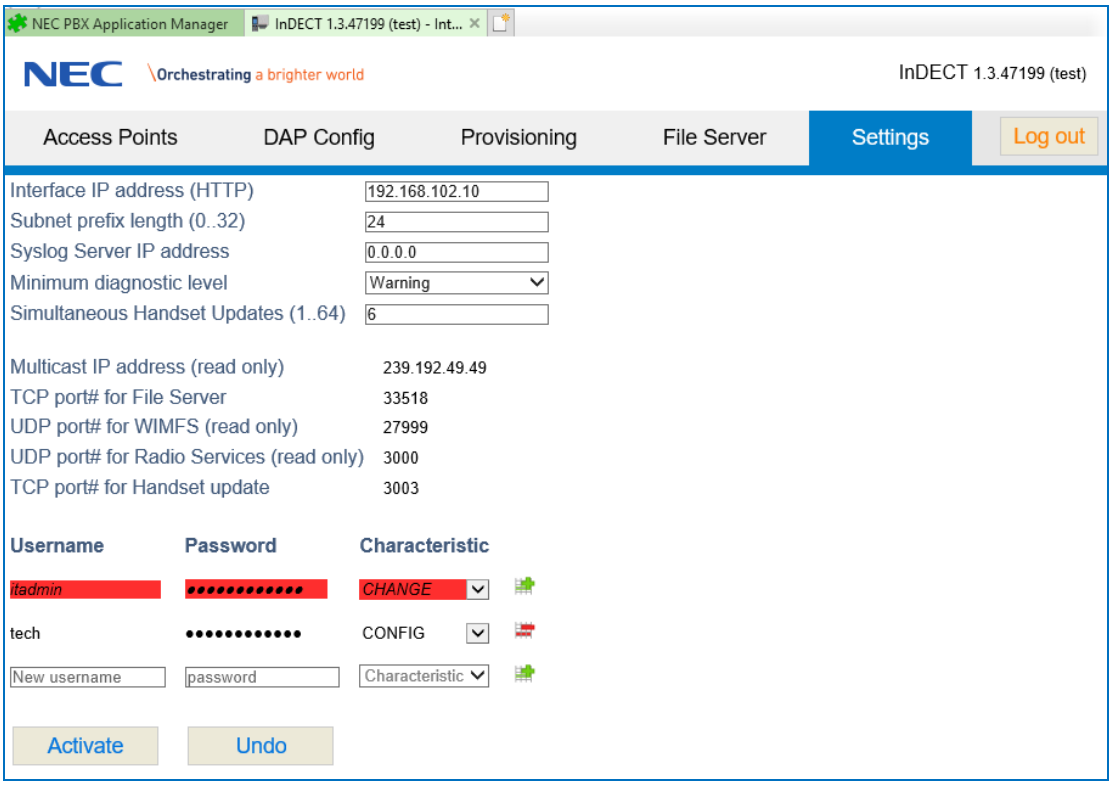


## Deleting a User

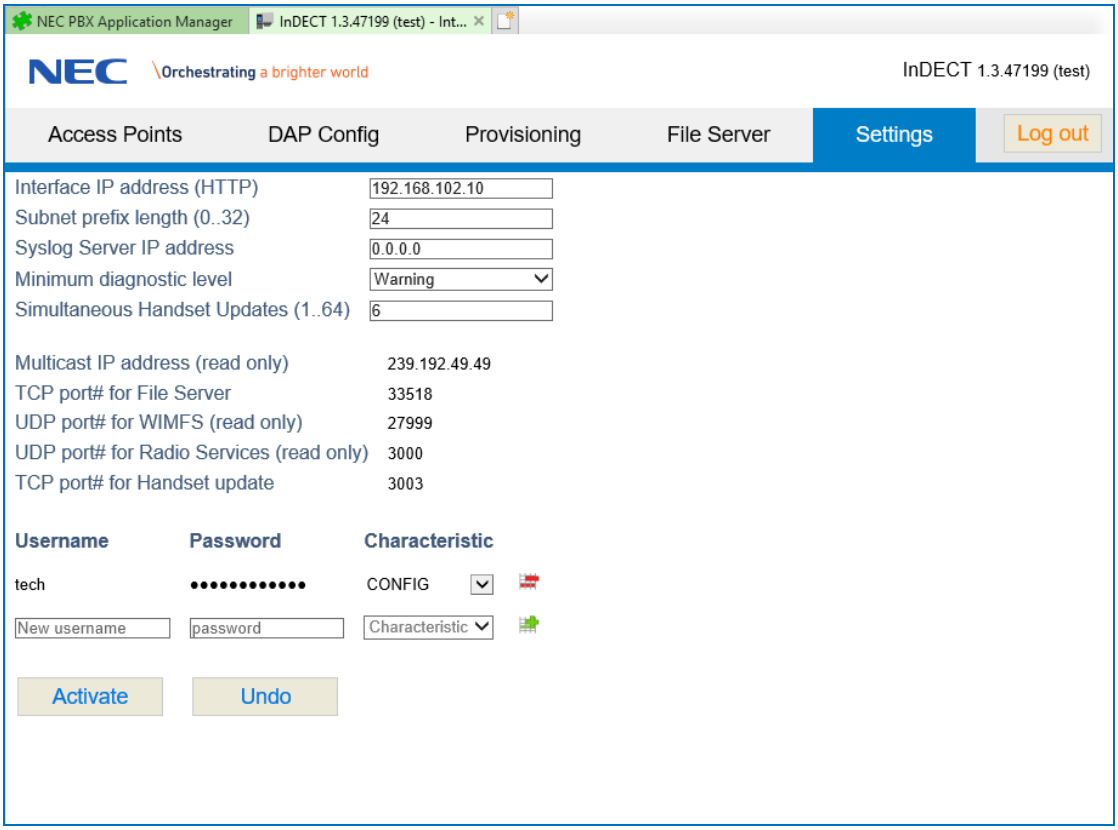
Open the **Settings** screen.




To remove a user from InDECT press the **Remove DAP** button  next to the username you want to remove. The row will change to be RED highlight.




When ready to continue, press the **Activate** button.




The user should now be removed from the system and you can no longer logon to InDECT using the username and password.

# InDECT – Software Licence Agreement

**PLEASE READ THIS SOFTWARE LICENCE AGREEMENT ("LICENCE") CAREFULLY BEFORE USING THE INDECT SOFTWARE. BY USING THE INDECT SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENCE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENCE DO NOT USE THE SOFTWARE.**

## 1. The Definitions

1.1. “Licence” means this Software Licence.

1.2. “Customer” means Software User.

1.3. “Software” means all InDECT Software, the subject of this Licence, including (a) the accompanying documentation and any Updates and (b) any Upgrades purchased by the Customer or provided by NEC at no cost pursuant to §5.2 below.

1.4. “Update” means minor Software release the primary purpose of which is to remove incompatibilities, apply corrections, enhance the stability or remedy technical faults in the Software.

1.5. “Upgrade” means major Software release the primary purpose of which is to add new functionality or enhance the performance of the Software.

## 2. The Licence

2.1. NEC grants the Customer a limited, non-exclusive, non-transferable, non-sub licensable Licence to use the Software, subject to the following conditions:

2.1.1. The Software may only be used on the System upon which it is first installed. Consent must be obtained beforehand if the Software is to be used on a different System.

2.1.2. The Software may not be copied except for internal back-up purposes.

2.1.3. The Software may not be modified, de-compiled, disassembled, reverse engineered, merged or de-coded in any manner whatsoever.

2.1.4. The Software shall be maintained in safe custody. Any unauthorised use, reproduction, distribution or publication of the Software must be prevented. If the Software comes into the possession of a third party NEC must be notified immediately.

2.1.5. This Licence is personal to the Customer. The Software or a copy thereof shall not be loaned, rented, leased, licensed, assigned or otherwise transferred. The Customer acknowledges NEC’s proprietary rights to the Software. No title or ownership to the Software is transferred. The Software shall not be used in any manner that would derogate from NEC’s proprietary rights in the Software. The Software is protected by applicable copyright laws and international treaty provisions.

2.1.6. The Software, including documentation relating thereto, contains confidential information. Such information shall not be disclosed to any third party, other employees or authorised agents of the Customer, without NEC’s prior written consent.

2.1.7. The use of the Software shall be supervised and controlled in accordance with the terms of this Licence. The Customer shall ensure that its employees, subcontractors or agents who have authorised access to the Software are made aware of the terms of this Licence and comply therewith. The Customer shall maintain safe custody of the Software.

2.1.8. The Customer shall permit NEC during NEC normal business hours to audit use of the Software and verify its compliance with the above conditions.

### 3. Copyright

3.1. The Customer acknowledges that the Software and documentation are protected by European and International copyright laws. The Customer shall not, during or at any time after the expiry or termination of this Licence, permit any act that infringes that copyright. The Customer expressly agrees that it shall not copy the Software except for back-up purposes pursuant to §2.1.2, or distribute, modify, publicly display or publicly perform the Software.

3.2. Ownership: This is a Licence to use the Software. It is NOT an agreement for the sale of the Software. All worldwide ownership of and all rights, title and interest in and to Software, and all copies and portions thereof, including without limitation, all copyrights, patent rights, trademark rights, trade secret rights, inventions and other proprietary rights therein and thereto, are and shall remain exclusively in NEC and its licensors. The Customer's rights to use the Software are specified in this Licence, and NEC retains all rights not expressly granted to the Customer in this Licence.

### 4. Limited Warranty

4.1. Subject to §4.2 through 4.6, NEC warrants that for ninety (90) days from the purchase date of the Software, it will perform according to its specifications.

4.2. NEC shall repair or replace Software subject to a valid warranty claim made within the warranty period, either on-site or off-site, at NEC's discretion and during normal business hours. If the Customer asks NEC to provide services outside its normal business hours, it shall be charged for such services at NEC's standard after-hours rates. If it is not possible to repair or replace the Software, the Software licence fee shall be refunded. The remedies described in this §4.2 shall be NEC's sole obligation and the Customer's sole remedy in the event Software fails to perform according to its specifications during the warranty period. For support purposes, the Customer shall permit remote access to the Software, during normal business hours, upon request for support. The Customer recognises that NEC's ability to support the Software is dependent upon the Customer providing this remote access.

4.3. Because there is such a diverse range of telecommunications environments, NEC cannot warrant that the Software will be compatible in every operating environment. It is the Customer's responsibility to ascertain whether its own operating environment is compatible with the Software.

Any Software modifications which NEC may agree to make to achieve compatibility shall be at its prevailing rates and charges. NEC does not warrant that the Software will meet the Customer's requirements or that its operation will be uninterrupted or error-free. NEC does not warrant that the Software is free of errors or defects. The existence of such Software errors or defects shall not constitute a breach of this warranty. Notwithstanding the foregoing NEC shall provide the Customer with Software corrections for known errors that also affect NEC's other licensees. NEC excludes, and expressly disclaims, all express and implied warranties of merchantability or fitness for any particular purpose. NEC shall not be responsible for external factors affecting the performance of the Software, including without limitation, telecommunications and network breakdowns, power surges or interruptions and other "Acts of God".

4.4. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL NEC BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES ARISING OUT OF OR RELATED TO YOUR USE OR INSTABILITY TO USE THE NEC SOFTWARE, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF NEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.5. Some jurisdictions do not allow the exclusion of certain implied warranties or conditions, so the above exclusions may not apply to the Customer. This Licence does not exclude any implied warranties or conditions that may not under applicable law be excluded. In no event shall NEC total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of seventy five pounds (£75). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.



4.6. This Licence does not impose any obligations upon NEC to provide support and Software Assurance ("SA") services outside of the warranty period. Should the Customer require such services, they shall be obtained by arrangement with NEC Technical Services.

5. Other Services

5.1. If NEC provides services outside the coverage of its limited warranty or after it has expired, the Customer shall pay for such services at NEC's standard rates and charges, plus travel and accommodation if applicable.

5.2. To fix an error in the Customer's Software, it may be necessary to install an Upgrade containing both version enhancements and bug fixes. During the warranty period, NEC shall provide such Software Upgrade at no cost. After the warranty period, NEC shall provide such Upgrade at its standard price. In addition to the price of such Upgrade, the Customer shall pay us for any services that NEC provides pursuant to §5.1.

## 6. Termination/Cancellation

6.1. NEC may Terminate/Cancel this Licence if the Customer breaches any condition thereof. If the breach is capable of remedy, NEC shall give the Customer thirty (30) days written notice within which to do so. Otherwise, Termination/Cancellation shall take effect immediately upon the Customer's receipt of NEC's notice.

6.2. The Customer may Terminate/Cancel this Agreement upon forty five (45) days prior written notice to NEC. Upon the date of Termination/Cancellation, the Customer's Licence to use the Software shall be deemed revoked, the customer will no longer be bound by the terms of this Agreement. Payment for the Software remains unaffected by this clause; this clause does not grant any free period of usage.

## 7. Term of Licence

7.1. This Licence commences upon the Customer's acceptance hereof. It shall continue, in perpetuity, subject to termination by NEC in the event that the Customer breaches any term herein, or by the Customer with written notice as stipulated in §6.2.

7.2. Upon termination/cancellation the Customer or its representatives shall immediately stop using the Software and documentation and shall return, or destroy all copies of the Software and documentation in a manner directed by NEC.

## 8. Other Clauses

8.1. If NEC foregoes or delays enforcing an obligation or remedy under this Licence, such forbearance or delay shall not result in a waiver or variation of such obligation or remedy. No failure by NEC to insist upon strict performance of any term or condition in this Licence shall constitute a waiver or

variation of such term or condition. Such failure shall not prevent NEC from claiming default or seeking a remedy under this Licence.

8.2. This is the entire agreement between NEC and the Customer. Upon agreeing to the terms of this Licence the Customer agrees that this Licence supersedes prior licensing agreements, both written and verbal for NEC Software.

8.3. This Agreement shall be governed by and construed in all aspects in accordance with the Laws of the jurisdiction in which NEC as the supplier of the Software is geographically based and each party submits to the non-exclusive jurisdiction of the courts in that geographic location.

8.4. The Customer acknowledges that a breach of this Agreement may cause irreparable and continuing damage to NEC for which money damages may be insufficient, and NEC shall be entitled to injunctive relief and/or a decree for specific performance and such other relief as may be proper (including money damages if appropriate). In the event of litigation between NEC and the Customer concerning Software or any other item which is subject to this Agreement, the prevailing party in the litigation will be entitled to recover legal fees and expenses from the other party.

8.5. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the balance of the Agreement, which shall remain valid and enforceable according to its terms.

8.6. Acknowledgement. **BY INSTALLING SOFTWARE, THE CUSTOMER ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS.**

NEC Enterprise Solutions reserves the right to change the specifications, functions, or features at any time without notice.

NEC Enterprise Solutions has prepared this document for use by its employees and customers. The information contained within this manual is the property of NEC Enterprise Solutions and shall not be reproduced without prior written approval of NEC Enterprise Solutions.



**NEC Nederland**

**B.V.**

**Olympia 4**

**1213 NT Hilversum**

**The Netherlands**

**www.nec-enterprise.com**