ADDSECURE®

NGP Ultimate

Installation Guide

For a safer and smarter world

Contents

Introduction

Introduction

Product description

NGP Ultimate is a dual path alarm signalling unit with its own built in hub. It is set up to work with a dedictaed broadband service for transmitting alarm signals from a customer's alarm panel, via the AddSecure private network, to an Alarm Receiving Centre (ARC) using pass-through mode of operation. Once connected to the platform the unit uses a poll and response check to determine path status. When the primary path fails the secondary path will take up the polling and reporting parameters of the primary path. Individual path fails are transmitted over the remaining path. Dual path failure is platform generated.

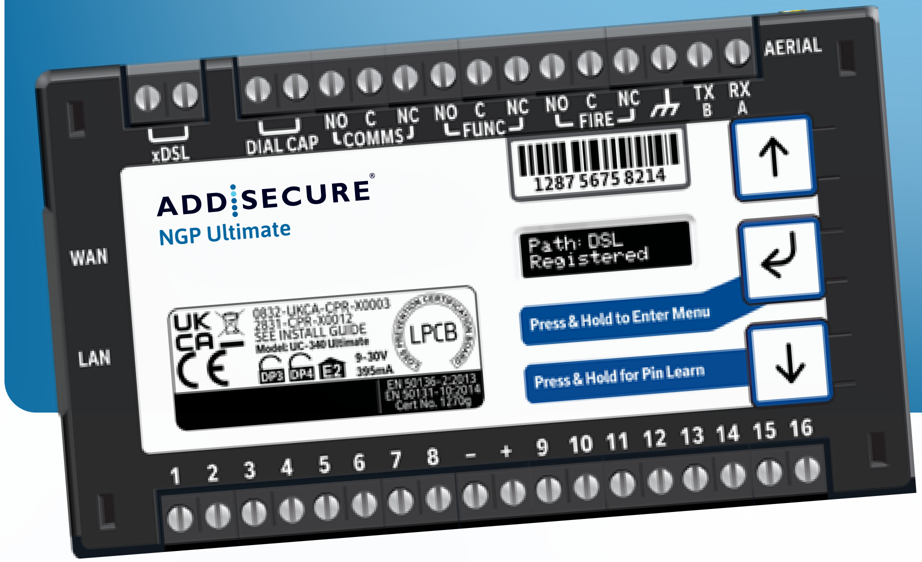


Figure 1 – NGP Ultimate unit (not to scale)

The NGP Ultimate services comes with a dedicated AddSecure broadband service using the latest technology available.

All services need to be in an Openreach served area.

NGP Ultimate uses an IP primary path with dual SIM 4G/2G mobile technology as the backup path.

The unit is designed for use in both Security and Fire systems.

A valid TA (Terminal adapter) account must exist for the unit to communicate. The TA account will have been populated with the serial number of the unit.

The unit has 16 general purpose alarm inputs, and 3 outputs, making it suitable for connection to most common alarm panels. The unit is supplied already fitted with two AddSecure enabled SIM cards, one an EE UK fixed SIM and a UK Roaming SIM.

Specifications

	NGP Ultimate
Primary path fail reporting	90 secs
Secondary path fail reporting	60 mins
Both paths fail concurrent	3 mins
Catastrophic failure (both paths together)	3 mins
Alarm Transmission category EN Standards / PD6669 (UK)	DP4
PD6669, EN50131 (2017) Grade	4
Grade option (Table 10 EN50131-1 2020)	4C
Previous grade (Pre June 1st 2019)	4
Environmental class	II
Information and Substitution security	AES256
Size	114mm x 67mm x 20mm
Weight	149g
Power	9V – 30V

Current	Average Normal Operation
IP/4G unit @12V	308mA
IP/4G unit @24V	150mA
Alarm inputs	16 General purpose inputs 1–16. (-0.5V – 30V)
Alarm threshold	High >2V, and Low <1.3V
Outputs	3 x Relay NO C NC (Comms, Func, Fire). Max rating 1A @ 30V DC
RS232 port	Remote panel access (UDL) and signalling to some intruder panel types
RS485 port	Remote panel access (UDL) and signalling to some intruder panel types
Configuration	Using onboard configuration buttons, web portal or app
Processor	STM32
Wireless module	ELS61
GSM/GPRS/EDGE	Dual band 900/1800MHz, maximum transmit power +34.5dBm
LTE	Penta-Band 700 (Bd28)/800 (Bd20/900 (Bd8)/1800 (Bd3)/2100 MHz (Bd1),maximum transmit power +24dBm
Operating range	-10 to +50 degrees Celsius, average 90% non-condensing humidity

Safety notes

Work area safety

- Keep work area clean, well lit and free of obstacles.
- Keep floor and walkways clear of cables and materials to avoid trip hazards.
- Keep children and bystanders away while performing installation and maintenance work.
- Remove any left over materials when finished and keep all items away from children and pets.

Personal safety

- Stay alert and attentive. A moment of inattention may result in personal injury.
- Do not perform installation or maintenance work when tired or under the influence of medication, drugs or alcohol.
- Upon commencing work on security system enclosures and components, ensure the item is securely fixed to the wall and that no components or contents such as the battery can fall and cause personal injury.

Electrical safety

- Exercise care when working inside security system enclosures:
- Metallic tools, fingers, body parts or jewellery coming into contact with mains wiring and terminals may cause electric shock.
- Metallic tools or jewellery coming into contact with battery terminals may cause sparks, personal injury or create a fire risk.
- Exercise care when drilling into, or inserting fasteners into walls. Pipes and wiring may be present in the wall and contact with tools or fasteners may provide risk of electric shock, damage to premises services, or create a fire risk. Locate wiring, pipes and services first to avoid accidents.

WARNING!
Read all safety warnings and instructions. Failure to heed warnings and follow instructions may result in electric shock, fire risk and/or personal injury.

Mounting and wiring

Mounting and wiring

Removal of cover

The top cover can be removed by gently releasing each of the 4 clips on the base of the unit by pushing the clips outward with a screwdriver blade.

Regular access to the inside of the unit should not be required, although occasional access may be required to access the SIM cards.

Mounting

The unit should be mounted inside the alarm panel, or inside a separate powered housing, using the sticky mounting pads supplied.

For security installations the enclosure must meet or exceed the protection requirements of the particular security grade for the whole installation as per EN 50131-1. For Grade 4 intrusion alarm systems the NGP Ultimate SPT must be located within the intrusion alarm panel enclosure. Alternatively, the NGP Ultimate SPT can be housed within a separate enclosure meeting the applicable protection requirements of EN 50131-10 and that is directly coupled to the intrusion alarm panel enclosure.

For all installations access to the unit needs to meet EN50131-1 installer access level 3.

For fire alarms it is recommended the signalling unit is mounted within an enclosure separate from the fire alarm panel or fire alarm power supply.

Caution: mounting the signalling unit within fire alarm panel or fire alarm power supply enclosure might invalidate their compliance with EMC regulatory requirements.

The separate enclosure must meet the requirements of EN 54-2 and EN 54-21 associated with access restriction to installer level 3, ingress protection to IP30 or above and power supply integrity. The transmission of fire alarm signals and the state of the fault and acknowledge outputs on the signalling unit shall be displayed at the separate enclosure or at the fire alarm panel.

If the fire panel and the separate enclosure are some distance apart (i.e. not within line of sight) then the indications should be at the panel.

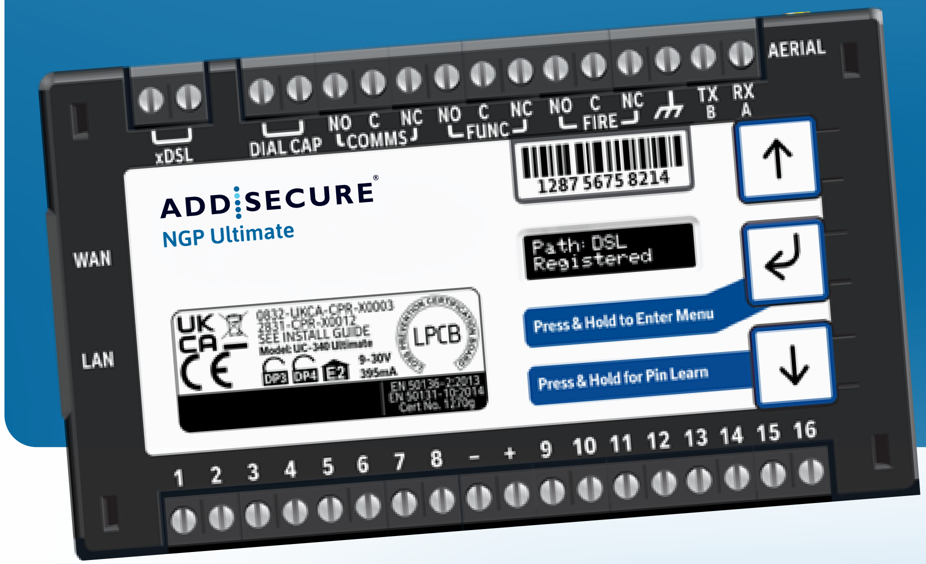


Figure 2 – Layout of terminals (not to scale)

For optimum performance the supplied aerial should be mounted vertically outside of and away from, the housing by removing the adhesive backing. Ideally the aerial should not be mounted on a metal surface. The aerial should be installed a distance of 20cm or greater away from any user or bystander.

Connection terminals

All screw terminals are suitable for use with a standard 3mm blade terminal screwdriver.

xDSL connections

Connection to the DSL service is by the two screw connections top left of the unit labelled xDSL. When the xDSL connection is used, pass the cable through the supplied ferrite twice (two turns), using the minimum wire length around the ferrite. Connect to the screw terminals of the xDSL port so that the ferrite is within 60mm of the terminals. See section on DSL connections.

WAN connection

The WAN port is for connection to the AddSecure broadband service delivered over a FTTP service. The unit monitors the valid presence of a 10/100 Mbit ethernet link. When the WAN connection is used, pass the cable through the supplied ferrite twice (two turns), using the minimum wire length around the ferrite. Crimp the RJ-45 plug within 60mm of the ferrite and plug into the WAN port.

LAN connection

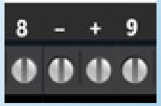
The LAN port is for future developments but can be used to connect a laptop to the device to access the web server.

Power connections

Power to the unit is via 2 screw terminals at the centre, with positive to the right nearest Pin 9.

The supply voltage range is 9V to 30V. The unit is designed to be connected to the auxiliary power output on an associated alarm panel, or separate powered enclosure. For use with intruder alarm panels the power supply must meet the requirements of EN 50131-6.

For use with Fire alarm panels the signalling unit must be powered from a supply meeting the requirements of EN 54-4. Ensure the power source is sufficient to power all devices connected. See the power requirements in the specification section for more information. The account at the Alarm Receiving Centre (ARC) should be put ‘on test’ before power up, as signals will be sent following initialisation.

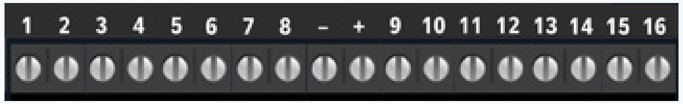


Alarm inputs

The unit has 16 alarm inputs which are presented on screw terminals along the bottom of the unit. These are labelled as Pin 1–8 and 9 –16.

By default the 16 alarm inputs require a positive condition to be presented to send an alarm. (Default = Positive applied).

This can be changed using the Pin Learn button or through the configuration menu. *See later section on configuration.*



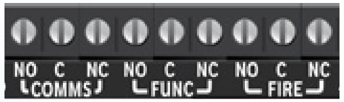
Input (Pin)	**Use**
1	Fire alarm (When programmed Fire NAK and ACK outputs operate in conjunction with pin 1)
2	Fire Fault or Hold up alarm
3	Intruder alarm
4	Open / Close (Set / Unset) (Func out put can be set up as RPS in conjunction with pin 4)
5 – 10	General alarm
11	ATS input (BSIA F175 mode) (Can be reprogrammed as a normal alarm pin)
13	AC Fail alarm (has a 7 minute delay which can be altered in programming)
14-16	General alarm

Outputs

Three relay outputs are provided on screw terminals at the top of the unit. Output 1 is Comms, Output 2 is Func, and Output 3 is Fire.

For fire alarm installations the indication of 'acknowledgement of fire alarm' and 'SPT fault' messages must be provided by the fire panel into which the SPT is mounted. System fault indications which are notified by the line fault output (Output 1) must be latched by the fire panel as required by EN 54-21.

See the further sections on outputs for a full explanation.

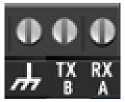


Serial data connections

The serial data connection labelled TX, RX, B and A is configurable for RS485 or RS232 connection depending on the panel.

This is done in the configuration menu. These ports allow serial alarm panel connection. See Panel Upload Download section.

See the Panel Upload-Download section.



Dial capture

The dial capture (Dial Cap) terminals enable interfacing with an alarm panel's digital communicator. The alarm panel can then send SIA, CID or Fast Format messages through the unit to the Alarm Receiving Centre.

Dial capture can also be used for upload download UDL allowing remote access with some types of alarm panel.

Aerial connection

Connect the supplied aerial to the MMCX connectors on the top right of the unit. The aerial should be placed in a vertical position and slightly away from the housing to ensure a good wireless coverage. The aerial should be installed a distance of 20cm or greater away from any user or bystander.

Carry out a survey to establish the best location.

If necessary, a selection of high gain and extension aerials can be available via your ARC.

Programming

Programming

Unit initialisation

The unit will immediately attempt to connect to the AddSecure platform over the configured paths. The unit will typically complete path establishment in the following times from power up. The xDSL/FTTP Path takes longer as the DSL modem needs to train up with the broadband service.

xDSL/FTTP	240s
4G/2G	120s

Figure 4 – time to commission paths after unit power up

Status display

The performance category can only be determined by the unit while in contact with the platform. The unit will not show the performance category until at least one path is registered and the profile can be retrieved from the platform. If the unit is configured and connected to an FTTP service then the display will show:

Path: Ethernet
Registered

The unit clearly displays its status on the OLED. In its normal working state, the unit will cycle its display depending on the dsl configuration.

Alarms GPI Alarm
3

Pin status – any outstanding alarm pins will be shown. If no pins are in the alarm state, then pin status will not be shown.

Alarms Battery
Low Battery

The unit may also show Low Battery if the supply voltage is below the supply threshold.

Path: DSL
Registered

IP Path and if registered with the platform For ADSL and VDSL connections.

DSL
20MB / 400KB

If the DSL path is synced it will show downstream and upstream speeds. Whilst syncing this will show the unit handshaking or training up depending on the type of broadband service.

Path: Mobile
Registered

Pin status – any outstanding alarm pins will be shown. If no pins are in the alarm state, then pin status will not be shown.

Signal Strength
4G[▪■] [-103]

Signal strength – network type (4G or 2G) received wireless signal strength in dBm and signal strength indicator bars. 2 Bars or more is the recommended signal level required.

Mobile Operator
EE

Shows which network the Mobile path is connected to.

Service Grade
Redcare DP4

Service Grade – shows the EN Performance category.DP4 for NGP Ultimate.

Signal strength

That is:

- On 2G below -90dBm = X will be displayed
- On 2G between -90 and -85, 1 bars will be displayed
- On 2G between -85 and -80, 2 bars will be displayed
- On 2G between -80 and -75, 3 bars will be displayed
- On 2G above -75dBm, 4 bars will be displayed

That is:

- On 4G below -120dBm = X will be displayed
- On 4G between -120 and -110, 1 bars will be displayed
- On 4G between -110 and -100, 2 bars will be displayed
- On 4G between -100 and -90, 3 bars will be displayed
- On 4G above -90dBm, 4 bars will be displayed

Guide to signal strength

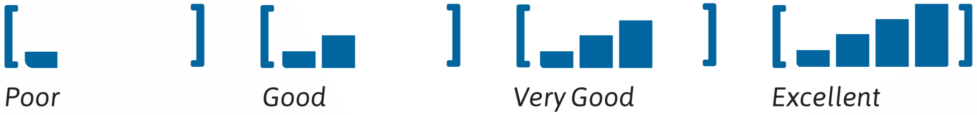
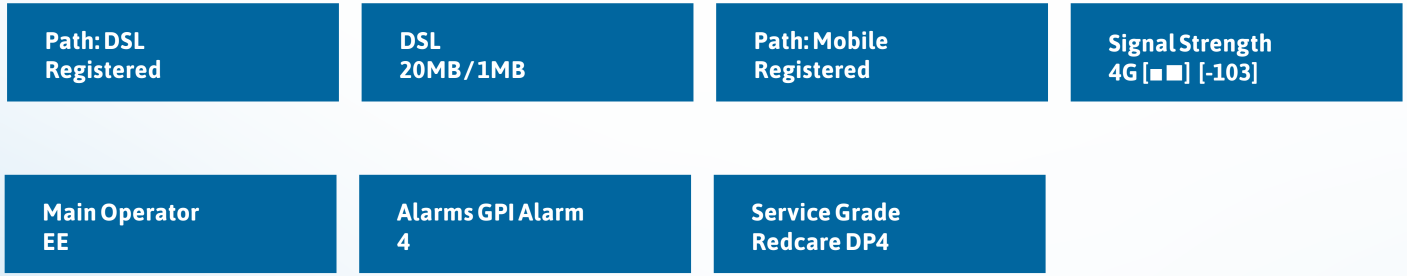


Figure 5 – Signal strength chart



Path: DSL
Registered

DSL
20MB / 1MB

Path: Mobile
Registered

Signal Strength
4G [▪■] [-103]

Main Operator
EE

Alarms GPI Alarm
4

Service Grade
Redcare DP4

Figure 5 – Typical display cycling on a fully commissioned unit with a good signal strength and pin 4 in the alarm or open state

Path status

The state of the communication paths is indicated by the OLED display, both the xDSL/FTTP and mobile path have the following possible path status:

- **Up No Reg** – path is up but not registered with the platform.
- **Registered** – has contacted the platform and successfully registered.
- **Alarm/ACK** – Alarm is being transmitted and awaiting acknowledgement.
- **Down** – the path has lost connectivity to the platform and is trying to reconnect.

NOTE: When fully commissioned over both paths, then both paths should be registered.

Pin inputs

Of the 16 alarm pin inputs, all behave as general purposes inputs with the following exceptions:

- Pin 1 must be used for Fire alarm when ACK NAK outputs are used for Fire panels. The signalling unit, when configured, provides an acknowledge and not acknowledged indication via use of outputs 2 (Func) and 3 (Fire).
- Pin 4 can have an RPS output associated with it. (See output 2 RPS (N/A for Fire config)).
- Pin 11 acts as an ATS input as per the requirements of the BSIA form 175 document. This applies only when output 1 is set to BSIA mode. N/A when configured for Fire.
- Pin 13 acts as an AC fail input and therefore has a default 7 minute delay before a pin 13 alarm is transmitted. It also has a 7 minute delay before a reset is sent. On presenting an alarm condition to pin 13, the units display will show the alarm immediately but 7 minutes of constant alarm condition needs to elapse before transmission. Similarly, restoring pin 13 will immediately remove pin 13 from the display, but 7 minutes of constant restore condition needs to elapse before transmission of pin 13 restore.
- The 7 minute time delay can be configured through the web portal or app by typing a new value up to 99 (mins) in the “Mains Fail delay” field. If the “Mains Fail delay” is set to 0, then pin 13 can be used as a general purpose alarm input. (Subject to ARC acceptance).
- Pins 1 – 16 can be set up for End of Line and Dual End of Line interconnection monitoring see descriptions on end of line monitoring.

Default outputs

Output 1 (COMMS)

Output 1 acts as the Communications fail output.

The mode of operation can be selected through the configuration menu *(see Configuration section).*

1. **BSIA form 175 output**
   This allows the alarm panel to interrogate path faults as single path or dual path. By default the relay output will switch, following either path fail, once the relevant timer has expired.
   If ATS input (pin 11) is toggled during the fail period, e.g. (panel interrogation) then Output 1 will either switch back to indicate a single path failure, or remain operated to indicate a dual path failure.
   The unit also supports inverted mode BSIA175 operation by learning pin 11 to be positive removed.
2. **Single path fault**
   Will operate when either path is in fault.
3. **Dual path fault**
   The relay will operate when both the IP and Mobile path are in fault.
4. **Mobile 1 Path fault**
   To be used in conjunction with Output 2 for the mobile path.

Output 1 operation as follows:

Condition		Relay Terminal
Power Off	Output	C <-> NC
Power On (no comms fault)	Output	C <-> NO
Comms fault	Output	C <-> NC

Output 2 (FUNC)

Output 2 has a number of configuration options:

1. **Dual path fault:**
   User operated output
   Can be operated remotely with the customer app.
2. **Dual path fault**
   Will operate when both paths are in fault.
3. **Mobile path fault output**
   In this case Output 1 is set as the IP path fault output, and Output 2 as the Mobile path fault output.
4. **RPS output for Pin 4**
   The output will operate when input pin 4 is triggered. It will return to normal when an acknowledge signal is returned from the ARC. The output has a minimum operation time of 1s. When the acknowledgement is received in less than 1 second after pin 4 is triggered then the output will remain operational for 1s.
5. **Fire NAK output**
   When configured in this way Output 2 will activate after a pin 1 alarm is sent and no acknowledgement from the platform is received for 80s.
6. **Keyswitch**
   To be able to set/unset the alarm panel with the customer app.

By default Output 2 is set to Dual path fault.

The NAK and ACK relay operate in the following mode:

Condition	Fire ACK	Relay Terminal
Power Off	Output 3	C <-> NC
Not in ACK (idle)	Output 3	C <-> NO
ACK	Output 3	C <-> NC
	Fire ACK	**Relay Terminal**
Power Off	Output 2	C <-> NC
Not in ACK (idle)	Output 2	C <-> NO
NAK (no ACK for 80 seconds)	Output 2	C <-> NC

Output 3

1. **User operated:**
   The default setting for output 3. This can be operated through the web portal or the app.
2. **Fire ACK output**
   When configured in this way, output 3 will activate when an acknowledgment to a pin 1 alarm is received. It will de-activate when pin 1 resets.
3. **Keyswitch**
   To be able to set/unset the alarm panel with the customer app.

Keyswitch Mode

- *Momentary* – momentary pulse to allow set and unset of alarm panel with customer app.
- *Latched* – Latched output option to allow set and unset of panel with customer app.

Used in conjunction when setting output 2 as Keyswitch.
Default Outputs 1, 2 and 3:

- *Output 1* is set to BSIA 175 and will operate if either path is in fault.
- Output 2 is set to Dual path fault. This allows a choice for simple installations for PD6669 without reprogramming.
- Output 3 is set to User operated.

Fire output settings:

To ensure that NGP Ultimate can inform the fire alarm panel of status as per the requirements of EN 54, the outputs need to be configured as follows.
Output 1:
COMMS – Single Path fail – Will operate when either signalling path fails.
Output 2:
FUNC – Fire NAK – Will operate after a pin 1 alarm is sent and no acknowledgement from the Alarm Receiving Centre (ARC) is received for 80s.
Output 3:
FIRE – Fire ACK – Will operate when an acknowledgment to a pin 1 alarm is received from the ARC. It will return to normal when pin 1 is reset.

Output 1 will be operated in the normal state. This ensures that, in the unlikely event of a total failure of the unit, the fire panel will still detect a state change on its fault input.

Configuration

Configuration

Pin Learn

For speed of installation a single button press Pin Learn is available. All pins to be used should be wired in and all the pins should be in the non alarm state. No tampers should be active (if wired in) and Pin 4 (open/close) should represent the system being set/closed.

When ready press and hold the down arrow for 3s, Notice – Done! is displayed when finished. This has completed the Pin Learn. There is also an option to learn the pins within the configuration menu.

Press & Hold for Pin Learn ↓

Notice – Done!

Configuration menu programming

The unit is supplied pre-configured with factory default values. For most installations no changes to the configuration are required.

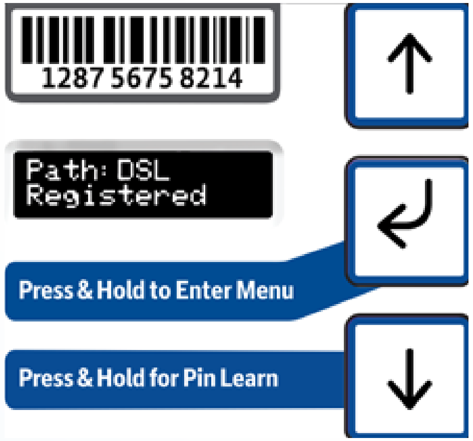
The unit can either be configured by using the on-board configuration menu driven by the buttons, or through the installer app or web portal. Some configurations are only available through the app or web portal. For use of the app or web portal remotely, written authorisation is required from a Level 2 user.

A minority of sites may require minimal configuration changes at installation, and most of these will be achievable through the button configuration, e.g:

- Change the individual Pin status.
- Enable dual end of line for interconnection monitoring.
- Change the comms fail output type etc.

Button configuration

The button configuration mode is entered by holding down the centre configuration button (Enter) for 3s.



When in the main menu, each press of ↓ will step to the next menu item down.

Use ↑ to step back up and eventually return to the top of the menu.

See figure 7 for the full main menu options.

The unit will then display 'Configuration'.

Configuration
↵

Press the Enter button again and the display will show the first menu option.

Inputs
↵

Pressing the Enter button on any menu item will enter the sub-menu and take you into edit mode. This will allow the function to be changed. Depending on the menu item will depend on the structure of the sub-menu.

Output Type 1*
Single Path Fault

You know you are in edit mode and that changes can be made by a * next to the menu title.

Some menu items have more options. e.g. Output 2 has 5 options to set the comms fault output type. On such menus, press the Enter button to enter the sub menu, then use the down and up arrows to increment through the options with each press. Holding the Enter button for 5s will save changes. Display will show Notice – Saved!

Some more complex menu items use the Enter button to also step through additional items in the sub menu. E.g. Network IP addresses to be input.

Notice -
Saved!

Typically, many menu items simply have two options, use the down and up arrow to switch between the two. Press and hold the Enter button to save changes. Display will show 'Notice – Saved!'

Edit mode can be exited at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Main menu display

Main menu display

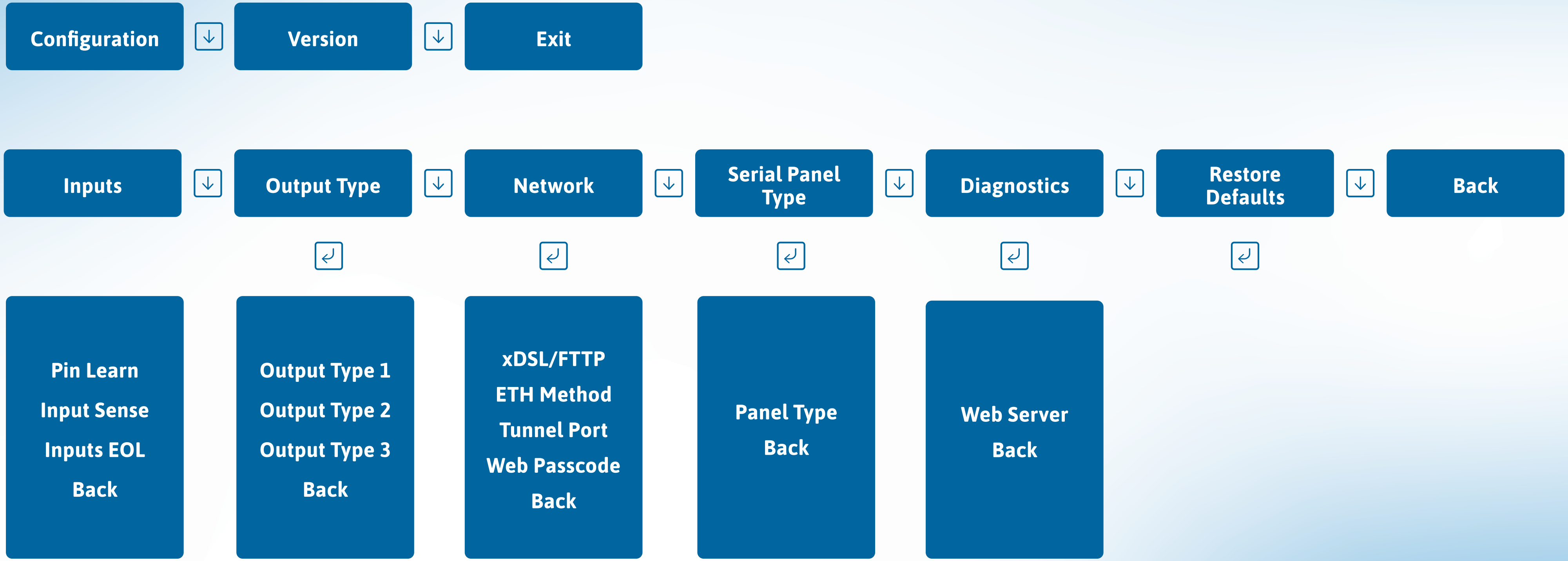


Figure 6 – Button configuration main menu options

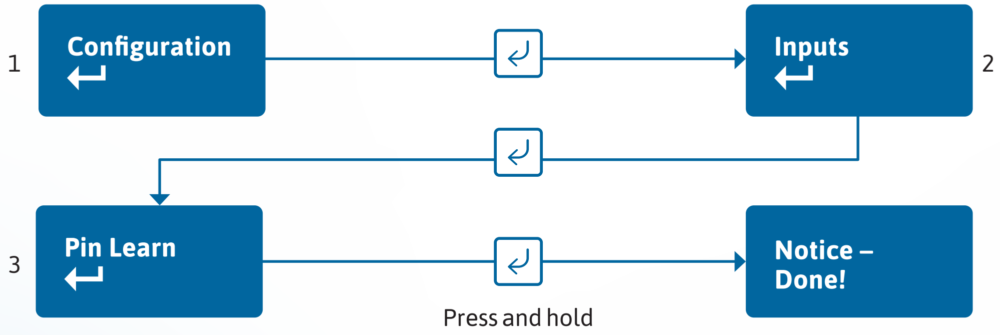
Additional network menus will become available depending on xDSL/FTTP and ETH Method. See Ethernet Mode page 29.

Inputs

Pin Learn

The unit can learn the polarity of pins by pressing and holding the down arrow for five seconds. The display will read 'Notice – Done!'. You can also carry out Pin Learn through the configuration menu.

Example – to learn the pin polarity in the configuration menu:



- Access the button configuration menu by holding the Enter button. Configuration is displayed.
- Press the Enter button again – the display now reads Pin Learn.
- Press and hold the Enter button – the display shows 'Notice – Done!'.

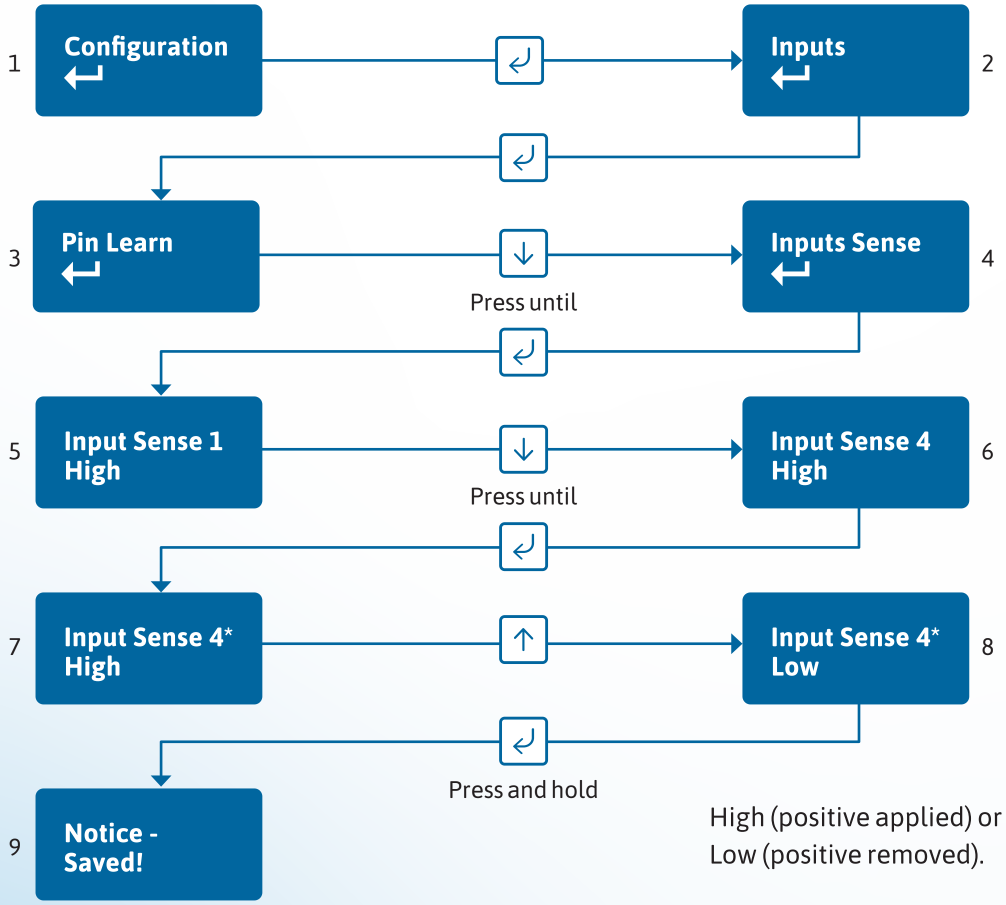
You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Input Sense

You can also manually configure the polarity of the pins. This is in addition to the Pin Learn function described earlier.

Example – to configure Pin 4 to be positive removed:



High (positive applied) or Low (positive removed).

- Access the configuration menu by holding Enter button for three seconds, then press the Enter button again – the display will read
  Pin Learn. Press the down arrow. The display will show Input Sense. Press the Enter button again to enter Input Sense. Pin 1 and status will be shown.
- Use the down arrow to scroll through the pins. Once you reach the desired pin, press the Enter button. * will be displayed.
- Use down or up arrow to change to High or Low – High (positive applied) or Low (positive removed).
- Once selected, hold the Enter button down until 'Notice – Saved!' is displayed. Then it will return to the position in the menu for you to select another pin, or you can use the down arrow to scroll through all the pins to return to the Back option.

You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

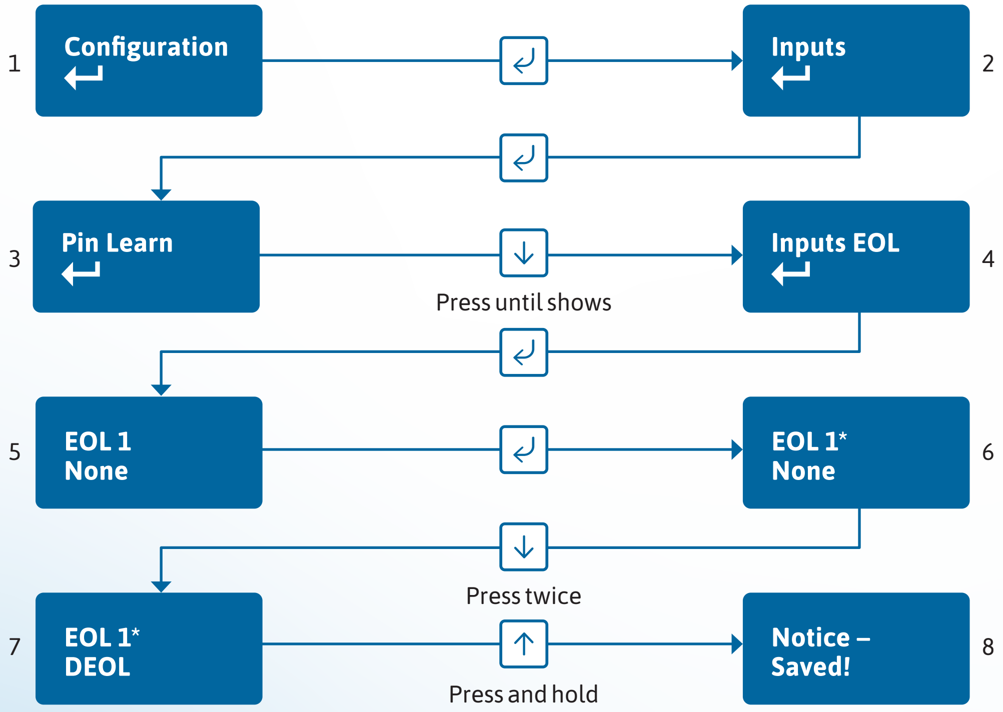
Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Inputs EOL (End of Line mode)

You can set the alarm inputs to the following modes:

- **None** – (Alarm and Restore)
- **EOL** (Single End of Line mode) – (Alarm, Restore and Cut)
- **DEOL** (Dual End of Line mode) – (Alarm, Restore, Cut and Short)

Example – configure Pin 1 for DEOL:



This allows the unit to monitor the wiring to the alarm panel contacts.

- Access the configuration menu by holding the Enter button for three seconds. Press the Enter button again – the display will read ‘Pin Learn’. Press the down arrow twice. The display will read ‘Inputs EOL’. Press the Enter button again to enter Input EOL. ‘EOL 1 = None’ will be shown.
- Use the down arrow to scroll through the pins. Once you reach the desired pin, press the Enter button. * will be displayed. Use the down or up arrow to change to None, EOL or DEOL.
- Once selected, hold the Enter button down until ‘Notice – Saved!’ is displayed.
- You’ll then be returned to the same position in the menu to either select another pin, or use the down arrow to scroll through all the pins to get to the Back option. Use the down arrow to step through all pins to get to the Back option.

You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Outputs

The three relay outputs can be configured as follows:

1. Output type 1 (COMMS):

- ***BSIA 175 Mode*** – operates when either path is in fault but in conjunction with Pin 11 ATS allows the panel to interrogate the device to determine a single or dual path fault (default).
- ***Single path fault*** – operates when either path is in fault.
- ***Dual path fault*** – operates when both paths are in fault.
- ***IP path fault*** – operates when the IP Path is in fault.

2. Output type 2 (FUNC):

- ***Dual path fault*** – operates when both paths are in fault (default).
- ***User*** – allow the relay to be operated remotely via the app or portal (default).
- ***Mobile path fault*** – operates when the mobile path is in fault.
- ***RPS*** – return path signal operates in conjunction with pin 4.
- ***Fire NAK*** – Fire pin not acknowledged. Operates in conjunction with Pin 1.
- ***Keyswitch*** – allows panel to be set/unset via the customer app.

3. Output type 3 (Fire):

- ***User*** – allow the relay to be operated remotely via the app or portal.
- ***Fire NAK*** – Fire pin acknowledged. Operates in conjunction with Pin 1 (default).
- ***Keyswitch*** – allows panel to be set/unset via the customer app (Coming soon).

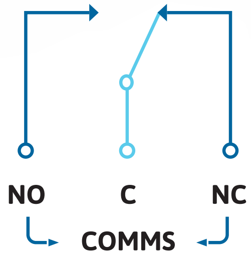
Keyswitch mode:

- ***Momentary*** – allow the Func relay, when set to Keyswitch, to be operated remotely via the app or portal by one pulse of the relay (default).
- ***Latched*** – allow the Func relay, when set to Keyswitch, to be operated remotely via the app or portal by latching the relay.

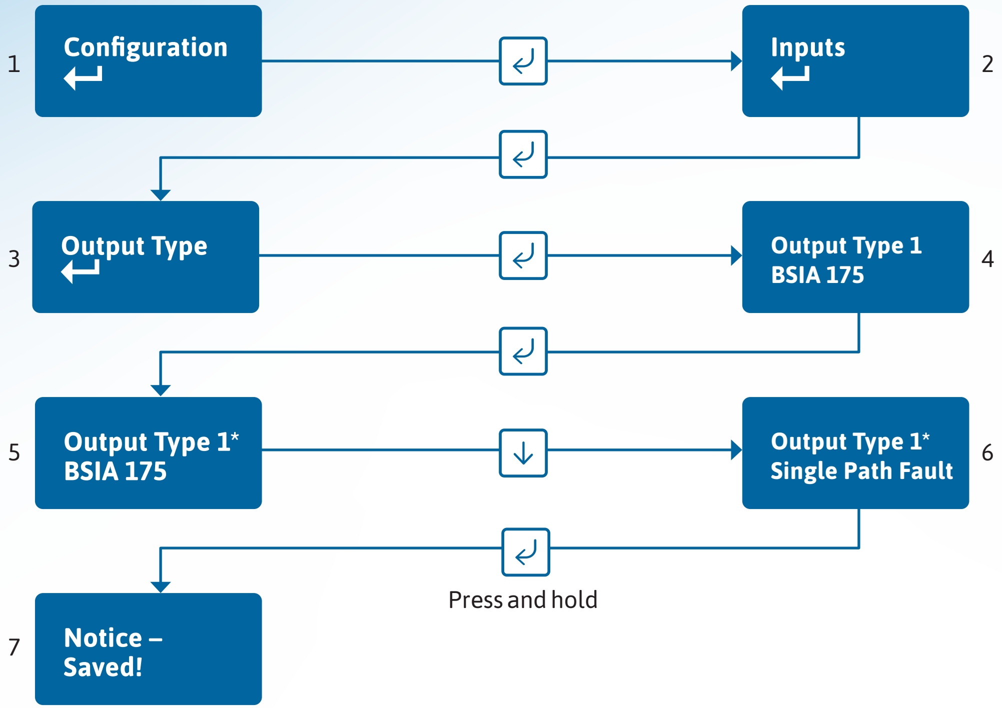
Output 1 operation as follows:

Condition		Relay Terminal
Power Off	Output	C <-> NC
Power On (no comms fault)	Output	C <-> NO
Comms fault	Output	C <-> NC

Relay status with path fail in operation



Example – configure Output 1 (Comms) for a single path fault



- Access the configuration menu by holding Enter button for 3 seconds, press the Enter button again, the display will show Pin Learn. Press the down arrow until Output Types is displayed. Press the Enter button again. The display will show the default setting for Output type 1. Use the down arrow to step through the Output types. Once the desired output is reached press the Enter button. * will be displayed. Use down or up arrow to change to the required configuration for that output.
- Once selected hold the Enter button down till Notice – Saved! is displayed.
- Then it will return to the same position in the menu for you to select another output or use the down arrow to step through all outputs to get to the Back option.

Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing ↓ for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing ↑ for 5s. This will take you back to the scrolling status display.

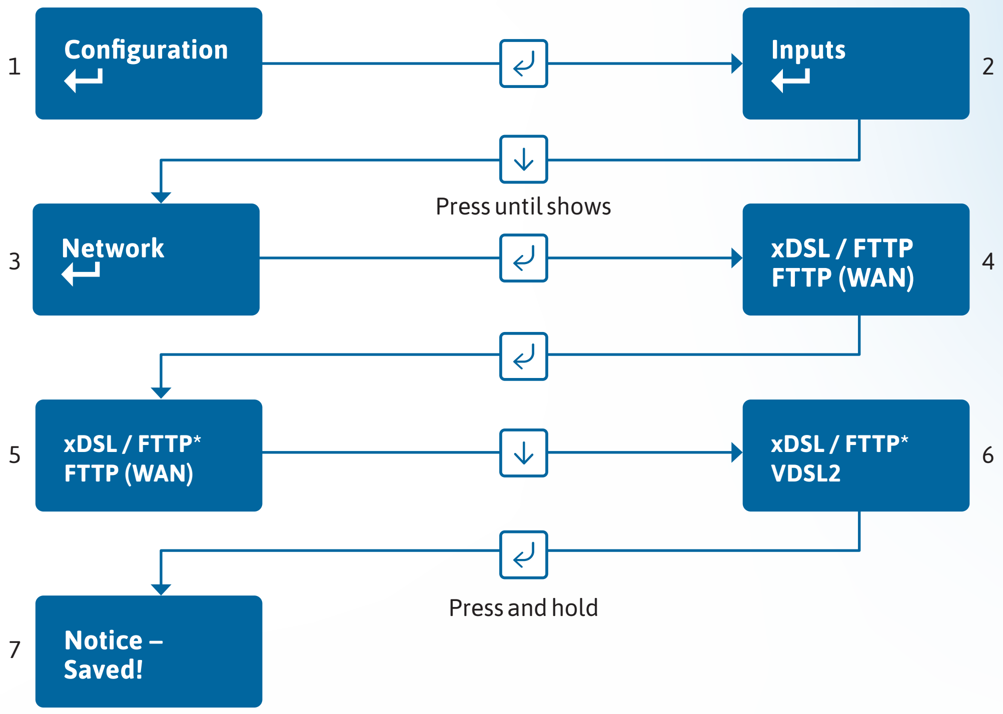
Network

The programming options under the network sub menu are:

1. xDSL/FTTP

Allows the unit to be changed between dynamic (DHCP client) or Static mode.
Default setting is enabled. The Ethernet port will attempt to obtain an IP address from a DHCP server on the LAN.

- FTTP (WAN) use when connecting to a FTTP service.
- ADSL2 used when connecting to an ADSL2+ service.
- VDSL2 used when connecting to an FTTC service.



AddSecure will advise if it is either an ADSL2+ or VDSL service that has been supplied.
If ADSL2+ or VDSL2 is selected the next menu option under network will be Tunnel Port.

- Access the configuration menu by holding the Enter button for 3 seconds, press the Enter button again, the display will show inputs. Press the down arrow until Network is displayed. Press the Enter button again. xDSL/FTTP is displayed. Press the Enter button . * will be displayed. Use down arrow to change to VDSL2.

- Once selected hold the Enter button down till Notice – Saved! is displayed.

You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

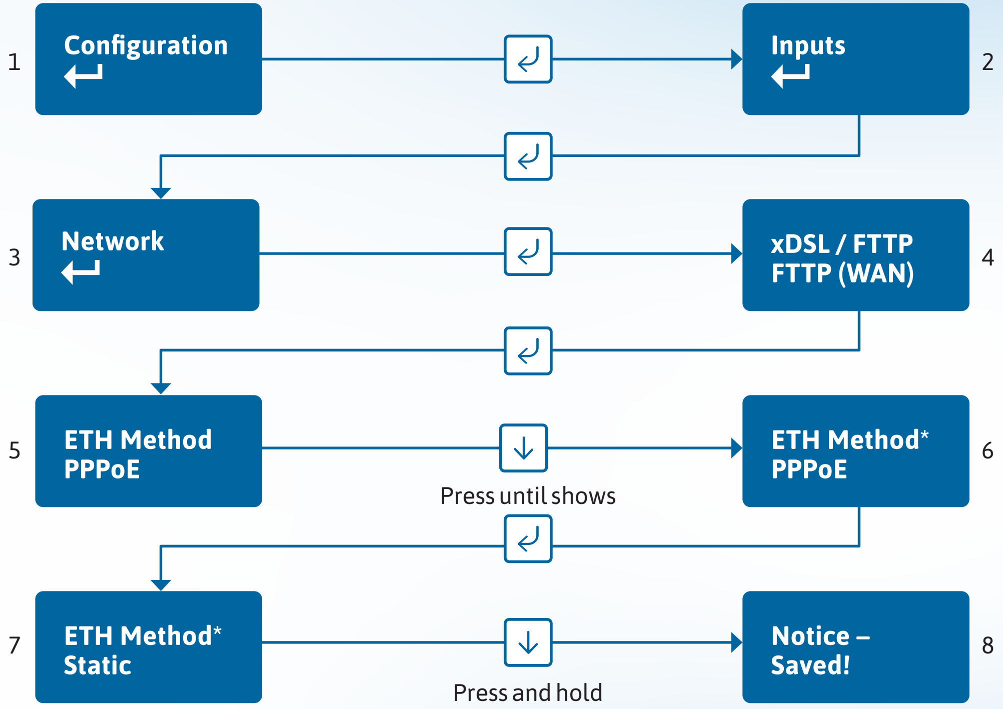
Ethernet Mode

PPPoE

Default it is set as PPPoE for connecting to the AddSecure broadband service and should not be changed unless the device is being used temporarily on a customer network or broadband. If being used on a customer Network or Broadband service the unit can be set to DHCP or Static. This allows the unit to be changed between dynamic (DHCP client) or Static mode.

The Ethernet port will attempt to obtain an IP address from a DHCP server on the LAN.

- ETH IP address – shows current IP Address but can also be configured for a static IP address.
- ETH Subnet mask address – shows current subnet address but can also be configured for a customer's subnet address.
- ETH Gateway address – shows current gateway address but can also be configured for a customer's gateway address.
- ETH DNS Address 1 – 1.1.1.1 or can be configured to use specific DNS servers.
- ETH DNS Address 2 – 8.8.8.8 or can be configured to use specific DNS servers.
- Tunnel Port – Port 443 is default but there is an option to use 10443.
- Web passcode – used in conjunction with Installer and Customer apps.



- Access the configuration menu by holding the Enter button for 3 seconds, press the Enter button again, the display will show inputs. Press the down arrow until Network is displayed. Press the Enter button again. xDSL/FTTP is displayed. Press the Enter button.

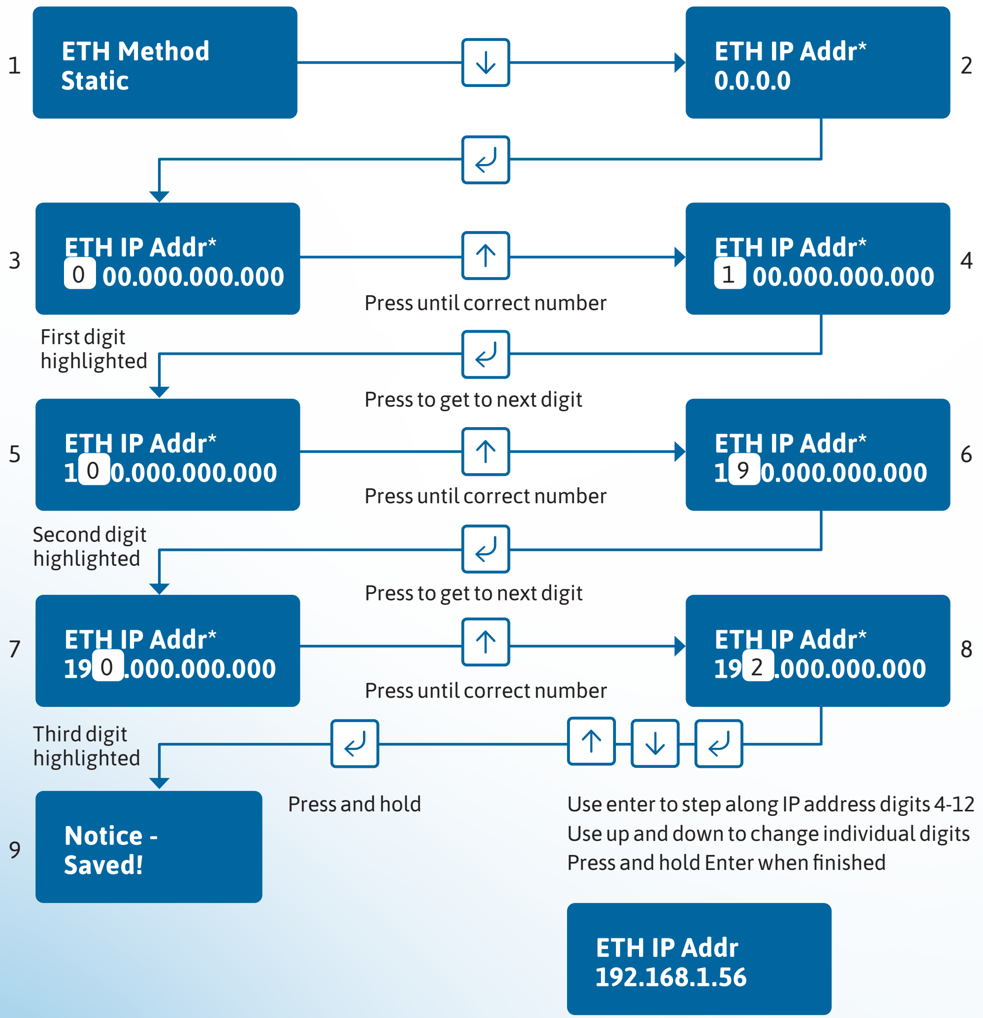
  * will be displayed. Use down arrow to change to VDSL2.
- Once selected hold the Enter button down till Notice – Saved! is displayed.

Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing ↓ for 5s. This will return you to the sub menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing ↑ for 5 seconds. This will take you back to the scrolling status display.

Setting a static IP address, netmask and gateway address

If the unit is to be connected to a LAN that requires the unit to have a static IP address (e.g. no DHCP server on the LAN) then this can be configured as follows after setting DHCP to Disabled.



1 ETH Method Static

↓

2 ETH IP Addr* 0.0.0.0

↲

3 ETH IP Addr* 000.000.000.000

First digit highlighted

↑ Press until correct number

4 ETH IP Addr* 100.000.000.000

↲ Press to get to next digit

5 ETH IP Addr* 100.000.000.000

Second digit highlighted

↑ Press until correct number

6 ETH IP Addr* 190.000.000.000

↲ Press to get to next digit

7 ETH IP Addr* 190.000.000.000

Third digit highlighted

↑ Press until correct number

8 ETH IP Addr* 192.000.000.000

↑ ↓ ↲

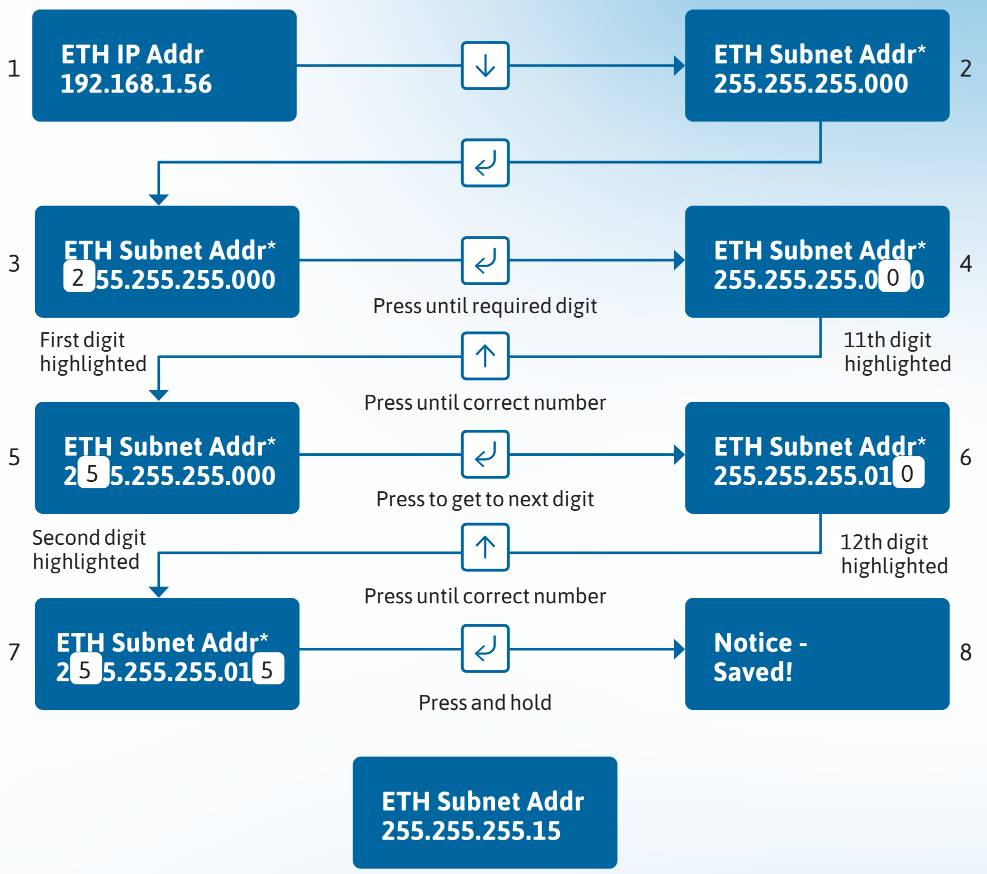
Use enter to step along IP address digits 4-12
Use up and down to change individual digits
Press and hold Enter when finished

↲ Press and hold

9 Notice - Saved!

ETH IP Addr 192.168.1.56

Then use ↓ to step to subnet address and use the same process as above to set the subnet address.



1 ETH IP Addr 192.168.1.56

↓

2 ETH Subnet Addr* 255.255.255.000

↲

3 ETH Subnet Addr* 255.255.255.000

First digit highlighted

↲ Press until required digit

4 ETH Subnet Addr* 255.255.255.000

11th digit highlighted

↑ Press until correct number

5 ETH Subnet Addr* 255.255.255.000

Second digit highlighted

↲ Press to get to next digit

6 ETH Subnet Addr* 255.255.255.010

12th digit highlighted

↑ Press until correct number

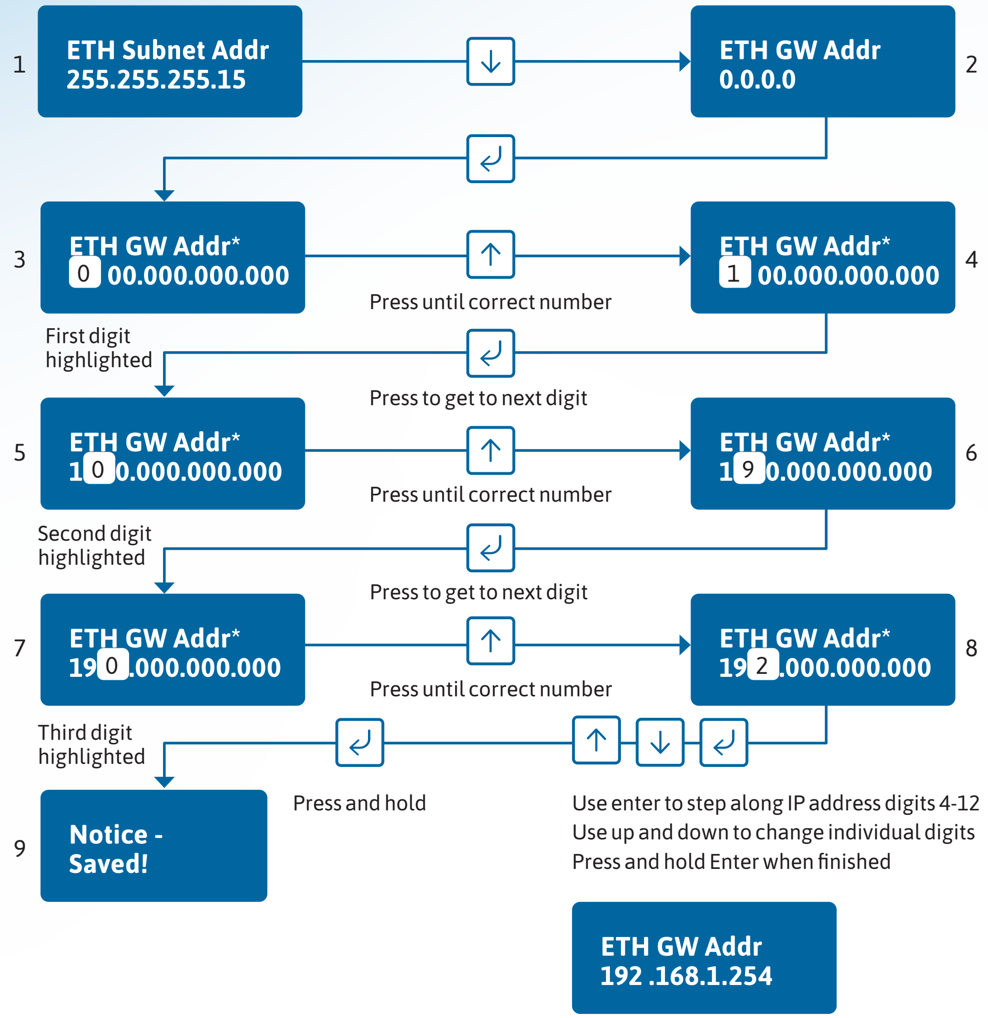
7 ETH Subnet Addr* 255.255.255.015

↲ Press and hold

8 Notice - Saved!

ETH Subnet Addr 255.255.255.15

Then use ↓ to step to gateway address, and use the same process as above to set the subnet address.



Note that IP addresses are made up of 12 digits in four batches of three, separated by dots. You must enter addresses through the buttons as 12 digit numbers, with zeros used to the left of each batch where necessary to pad out the addresses – as follows:

- IP Address = 192.168.001.056
- Subnet mask = 255.255.255.015
- Gateway = 192.168.001.254

The display will show the full address for each of the above.

You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

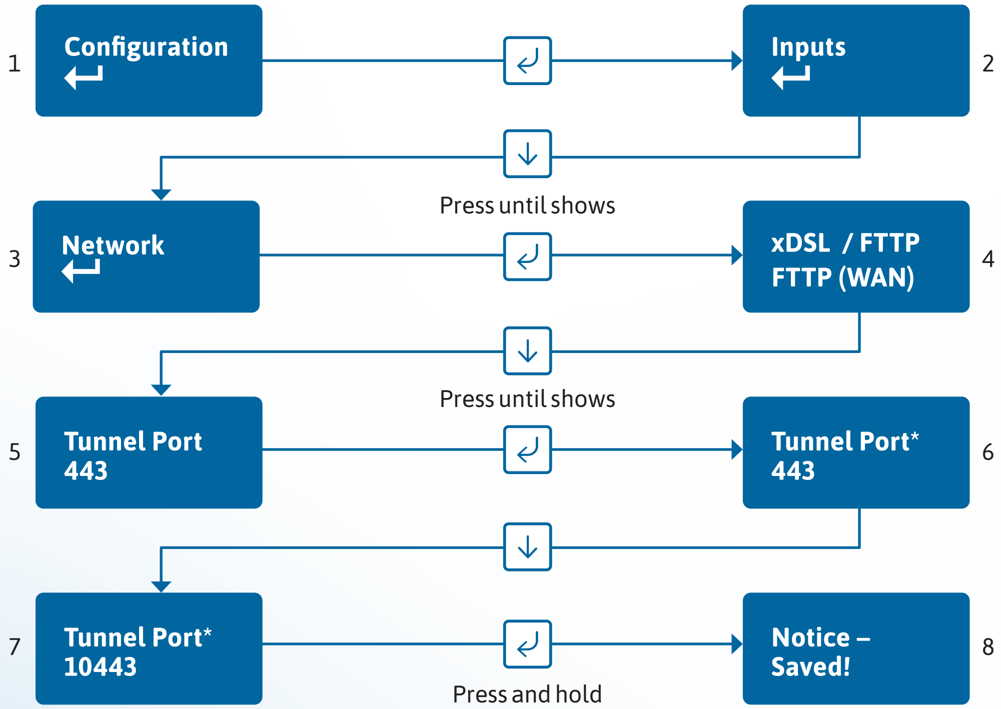
Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Tunnel port

The alternative tunnel port can be selected by accessing the Tunnel Port menu under network

- 443 (default)
- 10443

Example – changing the unit to use Port 10443:



When used in Ethernet Static or DHCP mode, the unit will attempt to establish a connection to the AddSecure servers by signalling on IP Port 443.

For most LANs this will function correctly, but on some advanced LAN configurations the network manager may not allow outgoing access on port 443 but 10443 may have outgoing access. Where this is the case then the unit can be configured to use the alternative port 10443. The AddSecure servers are set to accept both ports and so no changes are required other than on the unit's configuration.

- Access the configuration menu by holding the Enter button for 3 seconds, press the Enter button again, the display will show Pin Learn. Press the down arrow until Network is displayed. Press the Enter button again. The display will show xDSL/FTTP. Use the down arrow to step through to, Tunnel Port 443 is displayed. press the Enter button. * will be displayed. Use down arrow to change to 10443.
- Once selected hold the Enter button down till Notice – Saved! is displayed.

DNS Addr 1
1.1.1.1 Required to convert host names that are used to contact the server.

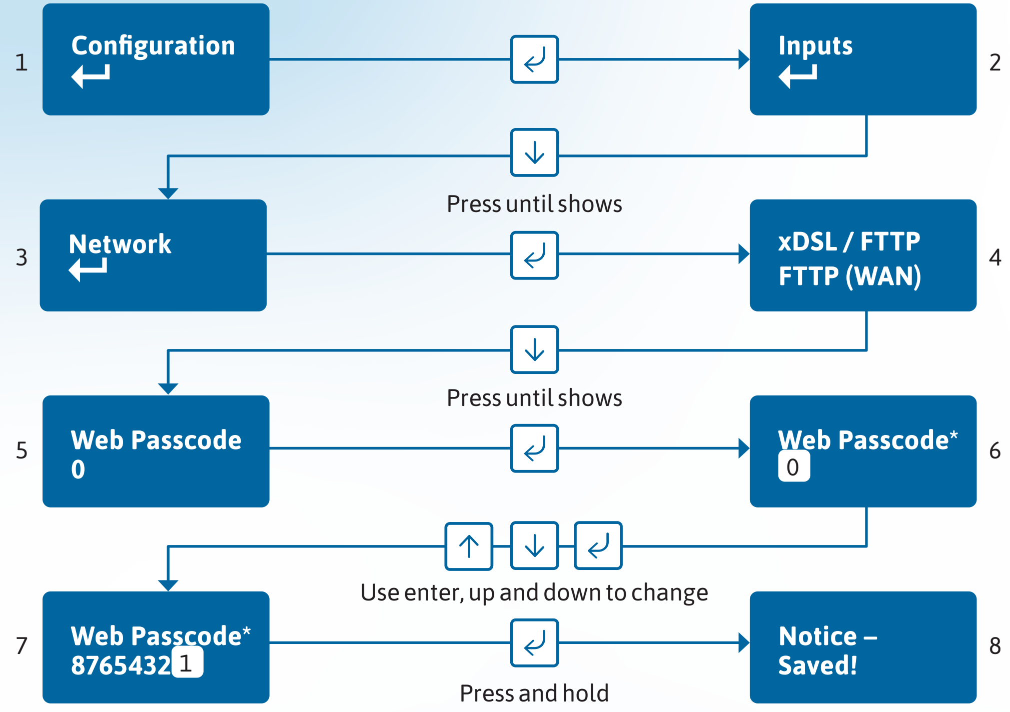
DNS Addr 2
8.8.8.8 Alternative DNS addresses

You can exit Edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to the sub-menu that you were making changes in.

Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds. This will take you back to the scrolling status display.

Web passcode

This code is used to set up both the installer and customer app. The passcode will need to be entered by you and can be any 8 digits.



This passcode can be changed any time, if required, via this menu within settings.

For best practice, mobile app access requires the Installer to set up a Web passcode and pin in the device and then advise and show the end customer how to change the PIN.

Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing ↓ for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing ↑ for 5s. This will take you back to the scrolling status display.

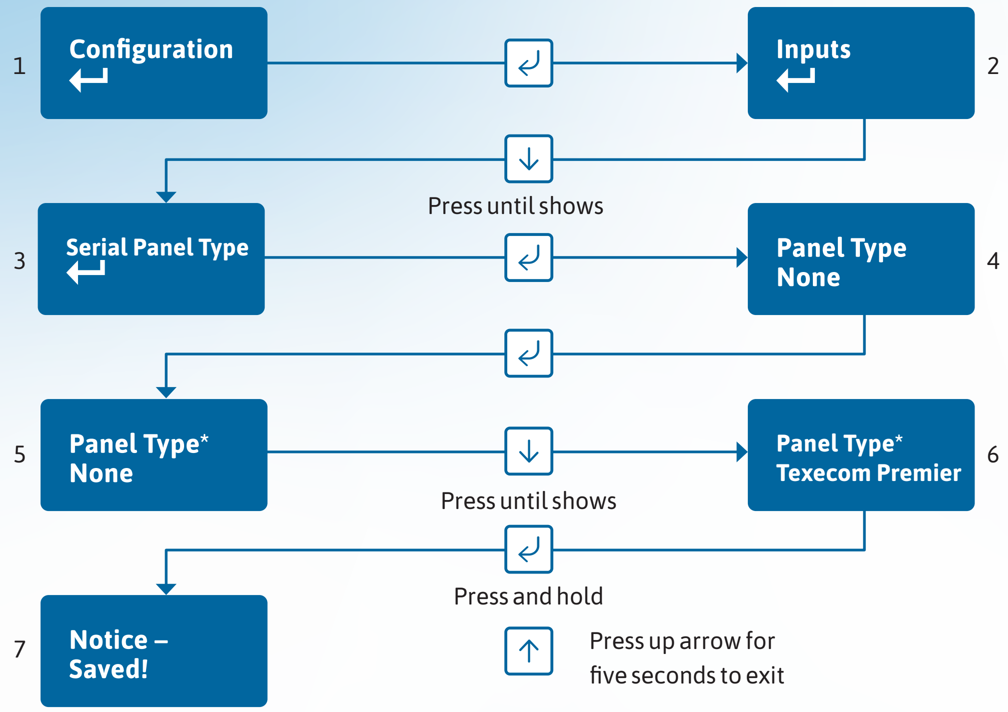
Serial connection panel type

This menu selects the panel connection type for serial connected panels (RS232 or RS485).

Settings:

- None
- Dimension GD 232 (Galaxy Dimension 48/96/264/520 (RS232 9600 8n1))
- Dimension GD 485 (Galaxy Dimension 48/96/264/520 (RS485))
- Galaxy G3 232 (G3 48/144/520 (RS232 9600 8n1))
- Galaxy G3 485 (G3 48/144/520 (RS485))
- Galaxy G2 485 (G212/20/44 (RS485))
- Galaxy Classic 485 L (Classic 8/18/60/128 (RS485))
- Galaxy Classic 485 H (Classic 500/504/512 (RS485))
- Galaxy Flex 485
- Texecom 816 (Texecom 412/816/832 (RS232 19200 8n2 inv))
- Texecom 48 88 (Texecom 48/88/168 Com - IP (RS232 19200 8n2 inv))
- Texecom Premier(Texecom Premier Elite 48 Com-IP (RS232 19200 8n2 inv))
- Bespoke Panel
- Pyronix RS232
- Contact IP (RS232 9600/2400/1200 8n1)
- Contact IPv2
- Eaton I-on
- Panel RS232 UDL

Example – changing the unit to connect to a Texecom Premier Elite panel via RS485:



- Access the configuration menu by holding Enter button for 3 seconds, press the Enter button again, the display will show Pin Learn. Press the down arrow until serial panel type is shown. Press the Enter button again to enter serial panel Type. Default status = None will be shown.
- Use the down arrow to step through the available panel. Once the desired Panel is reached press and hold the Enter button down till Notice – Saved!
  is displayed.
- Then it will return to the same position in the menu for you to select a different panel or use the down arrow to step through all pins to get to the Back option.

If panel types are changed the unit will reboot for the changes to take effect.

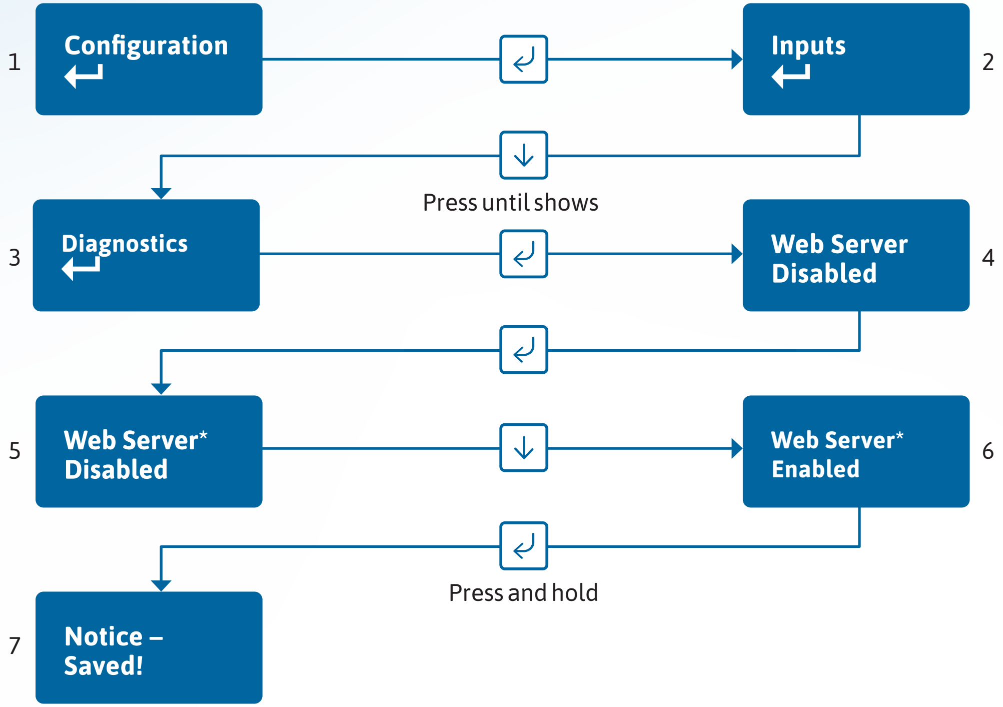
Edit mode for that part of the menu can be exited at any time, without saving changes, by pressing ↓ for 5s. This will return you to the sub-menu that you were making changes in.

The configuration menu can be exited at any time without saving any changes by pressing ↑ for 5s. This will take you back to the scrolling status display.

Diagnostics

Web server

To allow access to program the unit via a lap top, the web server needs to be set to enabled. Access to the web server is then allowed.



You will then need to plug in your laptop and login to the device.

Open your web browser and enter http://192.168.33.1.

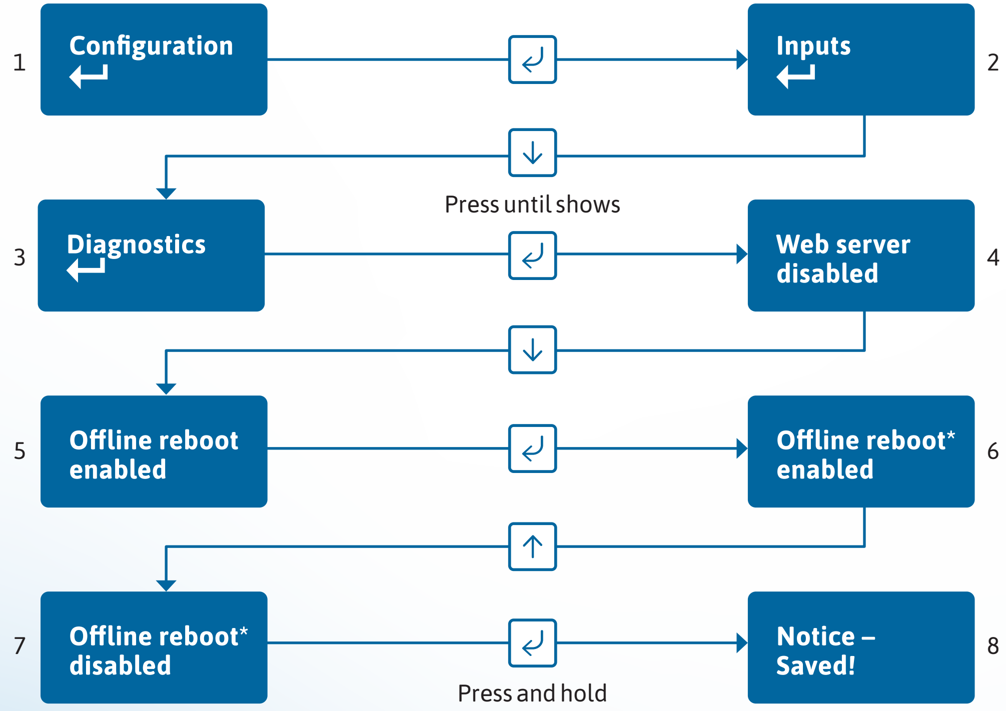
You can get the username and password from your AddSecure account manager. The unit will now have a static IP address of 192.168.33.1 for the duration that the web console is enabled. To access the Web Server a PC needs to be connected to the Ethernet port.

- Web Server will automatically exit after 20 minutes.
- Web Server can be disabled at any time by the installer.
- Web server will revert to disabled if the unit is restarted.
- To access the Web Server a PC needs to be connected to the Ethernet LAN port.
- Access the configuration menu by holding Enter button for 3 seconds, press the Enter button again, the display will show Pin Learn. Press the down arrow until diagnostics is shown. Press the Enter button again to enter diagnostics. Web Server, Disabled is displayed. Press Enter button again, * is displayed, press down arrow enabled is shown, hold Enter button to save changes.

Offline Reboot

Device will automatically reboot if offline for approx. 2 hours (time will vary between 2 and 3 hours)

This feature can be disabled as follows:



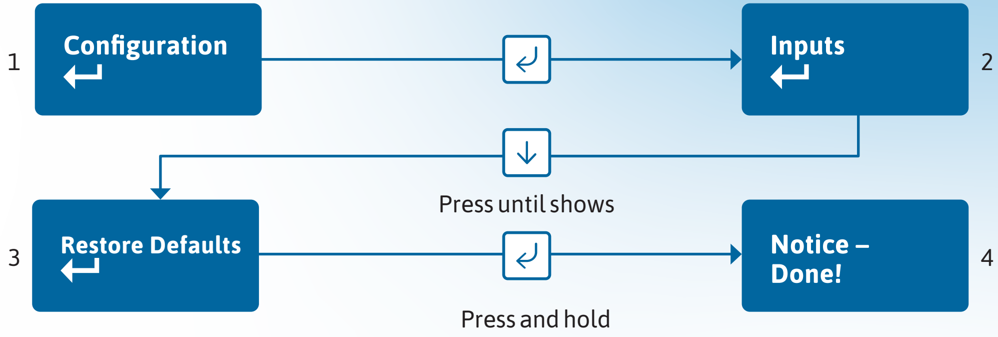
You can exit edit mode at any time, without saving changes, by pressing ↓ for five seconds. This will return you to sub-menu that you were making changes in.

Exit configuration menu at any time without saving any changes by pressing ↓ for five seconds. This will take you back to the scrolling status display.

Restore defaults

The Restore defaults option on the menu can be used to set the unit back to factory default. That is all settings will be reset to their standard values.

Example – setting the unit back to factory default:

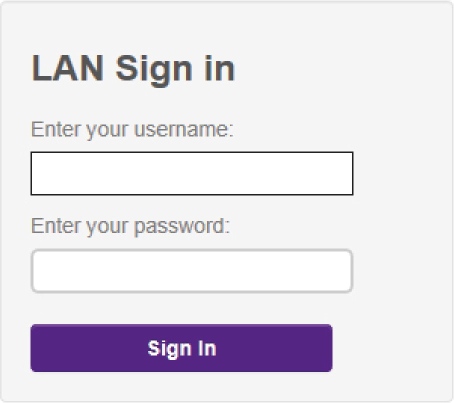


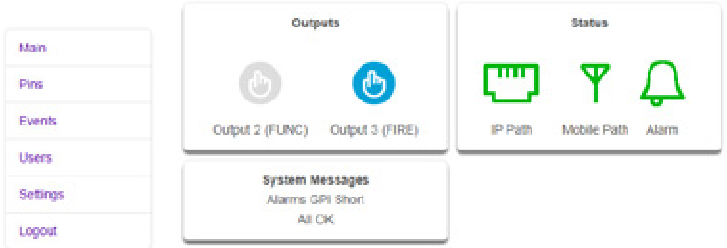
Exit the configuration menu at any time without saving any changes by pressing ↑ for five seconds.

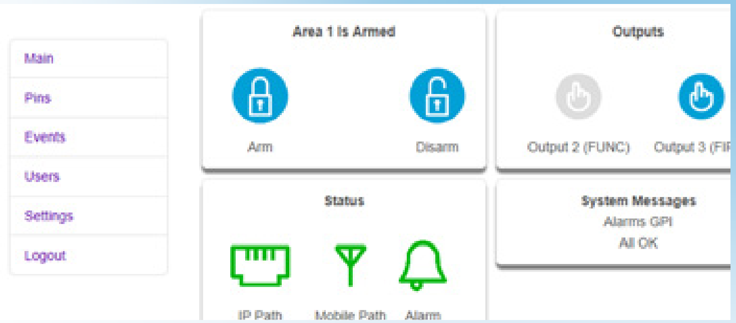
This will take you back to the scrolling status display.

Web server

Web server







Descriptions that follow are when directly connecting to the Ethernet port of the unit. The same menu options are available via the web portal or AddSecure installer app.

The Webportal displays the license agreement and privacy agreements on first login and the user must accept the T&Cs before continuing. The date and time when the user accepts the license agreement is captured. The Installer should obtain the End Customers consent should they wish to use any personal information.

Log in with the AddSecure username = xxxxx, password = xxxxxxxx

This is available from the AddSecure Technical Helpdesk or your AddSecure account manager.

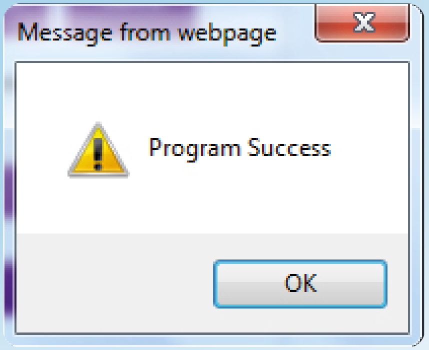
To comply with EN 50136-2 Clause 5.2 Access levels, the PIN code access must be set to 6-digits. You can change the access PINs in the user settings.

This applies for all types of access to the device.

Main status display

When you first login you are presented with the main status page, you can return to this page at any time by clicking Main on the menu bar.
The status page shows the User operated outputs. Output 2 (FUNC), which can be renamed in the settings menu, can be operated by clicking on the interactive icon if Output 2 (FUNC) is set up as USER. When operated the interactive icon turns orange from blue and back to blue when pressed again.
Output 3 (FIRE) can be operated in the same way when Output 3 (FIRE) is set to USER. If the Output Icon is grey it means that the Output is not set up as User operated.

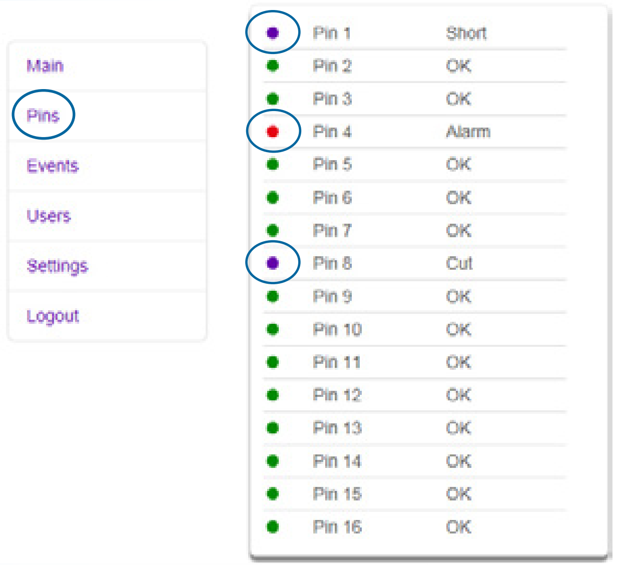
In the example above Output 2 is not configured to be user operated. Output 3 is configured. The main status page will be different if a keyswitch option is selected.



Message from webpage

Program Success

The above will be shown when changes have been saved. Click OK to continue.



●	Pin 1	Short
●	Pin 2	OK
●	Pin 3	OK
●	Pin 4	Alarm
●	Pin 5	OK
●	Pin 6	OK
●	Pin 7	OK
●	Pin 8	Cut
●	Pin 9	OK
●	Pin 10	OK
●	Pin 11	OK
●	Pin 12	OK
●	Pin 13	OK
●	Pin 14	OK
●	Pin 15	OK
●	Pin 16	OK

Pins shows the Name (if changed) and status of each of the PIN alarms. OK with green dot shows the pin is not in alarm and Alarm with the red dot if in alarm. It will also show if a PIN is in a cut or short state, with a blue dot and cut or short.

Status

These icons show the status of the signalling paths and if there are any outstanding alarms. Green for the signalling path icons indicates signalling paths are successfully connected to the platform. Red indicates that a path is down.

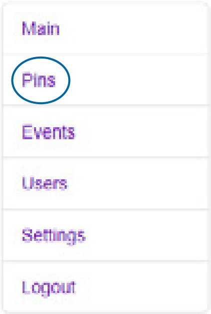
The bell icon is green in the example on the previous page as we have no alarms showing in the system messages box, which you would expect to see as the system will be set. If PIN inputs are in alarm the bell icon will be red.

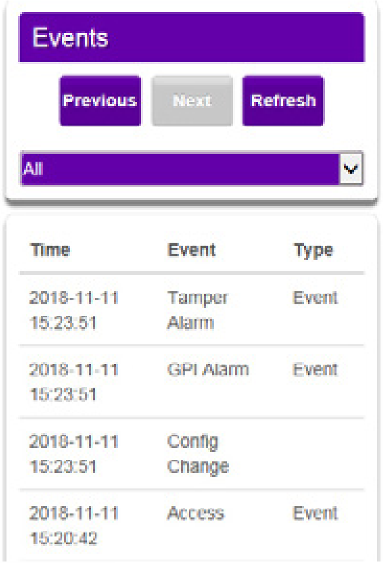
System messages

The system messages box will scroll though the key messages:

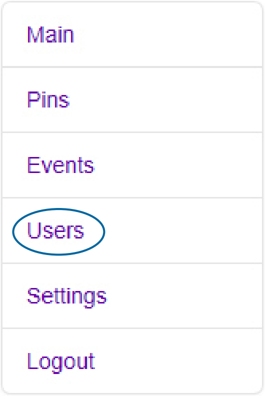
- ***Battery*** – will indicate if supply is low.
- ***Alarms GPI Cut*** – any PIN inputs that are in the cut state (EOL or DEOL).
- ***Alarms GPI short*** – any PIN inputs that are in the short state (DEOL).
- ***Alarms GPI*** – any PIN inputs in alarm.
- ***Signal strength*** – signal strength in dBm and the name of the mobile network operator.

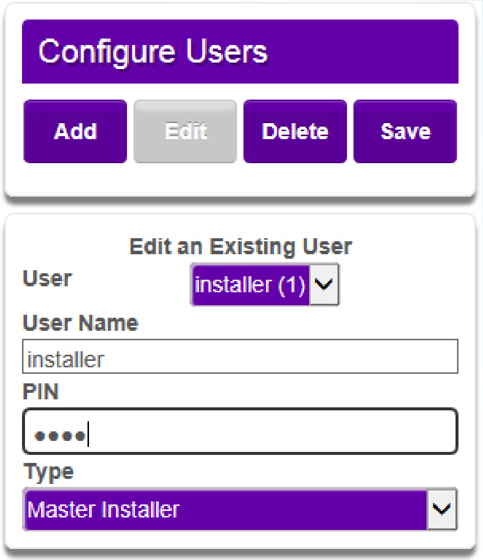
The menu bar on the left hand side can take you to any of the menu options described below. Should you need to make any changes in the following menu options click on save. This will save your changes to the unit.





Time	Event	Type
2018-11-11 15:23:51	Tamper Alarm	Event
2018-11-11 15:23:51	GPI Alarm	Event
2018-11-11 15:23:51	Config Change	
2018-11-11 15:20:42	Access	Event





Edit an Existing User

User: installer (1)

User Name: installer

PIN: ••••

Type: Master Installer

The abow shows the most recent events. If you click on the drop down you are able to filter the events by type. e.g. Alarms, System, Configuration or Connection.

In the event log on the app or on the unit web page ** indicates a non-reportable event. If a single * is displayed by an event this indicates no acknowledgement has been received.

This menu allows you to set up additional installer and end customer app access to the unit and change log in pin numbers.

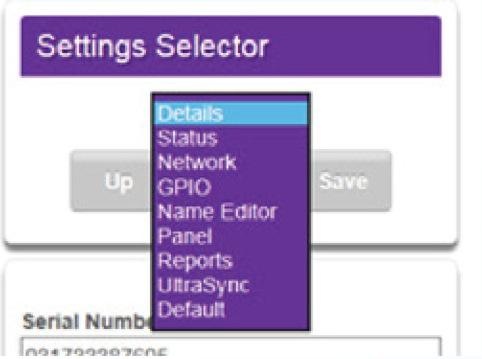
To comply with EN 50136-2 Clause 5.2 Access levels, the PIN code access must be set to 6-digits. You can change the access PINs in the user settings.

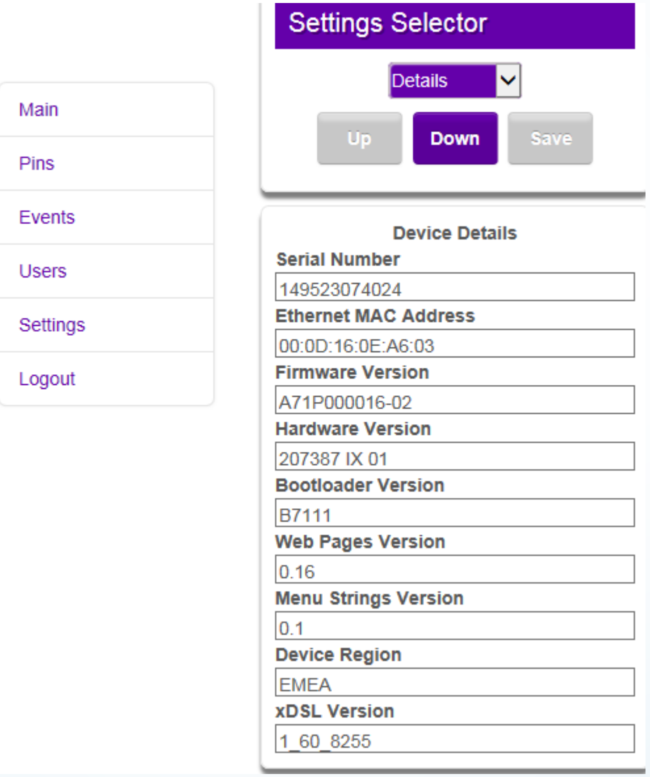
This applies for all types of access to the device.

For best practice, mobile app access requires the Installer to set up a Web passcode and pin in the device and then advise and show the end customer how to change the PIN.

For passcode/pin recovery the End Customer needs to contact their Installer. For PIN resets you can use the reset pin function in the AddSecure portal.

The settings menu has sub menus to be able to program the unit. The first screen gives you details of the device including MAC address and firmware version. Use the down button to step to the first sub menu option or use the drop down to access the sub menus.





Device Details

Serial Number
149523074024

Ethernet MAC Address
00:0D:16:0E:A6:03

Firmware Version
A71P000016-02

Hardware Version
207387 IX 01

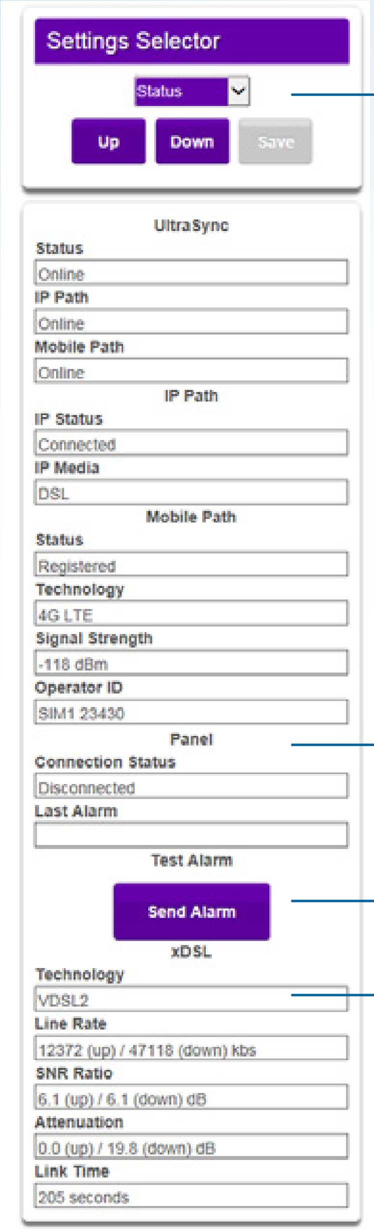
Bootloader Version
B7111

Web Pages Version
0.16

Menu Strings Version
0.1

Device Region
EMEA

xDSL Version
1_60_8255



Status

UltraSync

Status: Online

IP Path: Online

Mobile Path: Online

IP Path

IP Status: Connected

IP Media: DSL

Mobile Path

Status: Registered

Technology: 4G LTE

Signal Strength: -118 dBm

Operator ID: SIM1 23430

Panel

Connection Status: Disconnected

Last Alarm:

Test Alarm

xDSL

Technology: VDSL2

Line Rate: 12372 (up) / 47118 (down) kbs

SNR Ratio: 6.1 (up) / 6.1 (down) dB

Attenuation: 0.0 (up) / 19.8 (down) dB

Link Time: 205 seconds

The status sub menu shows the status of the IP path. It also shows the mobile path status, if it's using 2G or 4G, the signal strength, which SIM and operator.

- 23410 – O2
- 23415 – Vodafone
- 23420 – Three
- 23430 – EE

Panel – if the panel is connected serially then this will show the status of that connection.

By clicking the test alarm button this will send a test alarm over both paths.

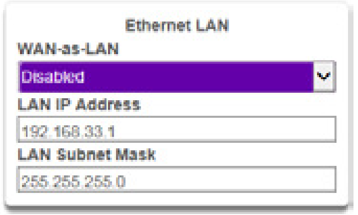
xDSL shows the technology (ADSL2+ or VDSL2) the sync rate – up and down speeds and link up time.

Network

The Network menu allows you to change the broadband service type between Ethernet (FTTP), VDSL (FTTC) and ADSL. When set to ADSL2 or VDSL2 no other changes should be made as this could affect the service operation. If you wish to use this unit temporarily as an Advanced unit on a customer network or broadband, then select Ethernet as the WAN interface and the method to DHCP.

When you connect back to the AddSecure broadband service you will need to change these back.

The Web Access passcode should be entered if setting up app access. Enter an 8 digit number and save changes. Make your changes and then click the save button. Program Success will be displayed.

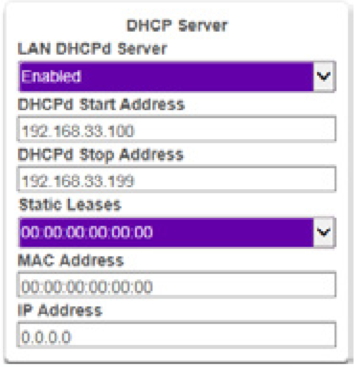


Ethernet LAN

WAN-as-LAN
Disabled

LAN IP Address
192.168.33.1

LAN Subnet Mask
255.255.255.0



DHCP Server

LAN DHCPd Server
Enabled

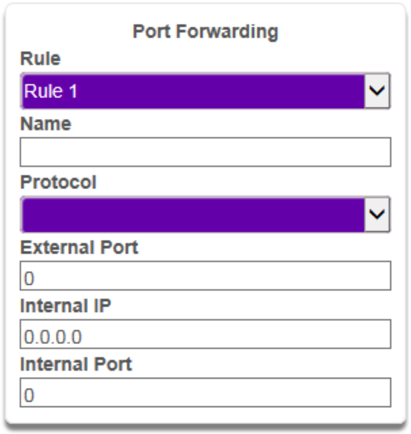
DHCPd Start Address
192.168.33.100

DHCPd Stop Address
192.168.33.199

Static Leases
00:00:00:00:00:00

MAC Address
00:00:00:00:00:00

IP Address
0.0.0.0



Port Forwarding

Rule
Rule 1

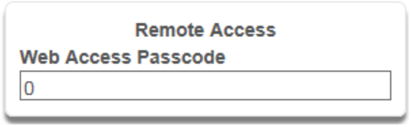
Name

Protocol

External Port
0

Internal IP
0.0.0.0

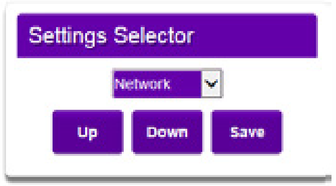
Internal Port
0

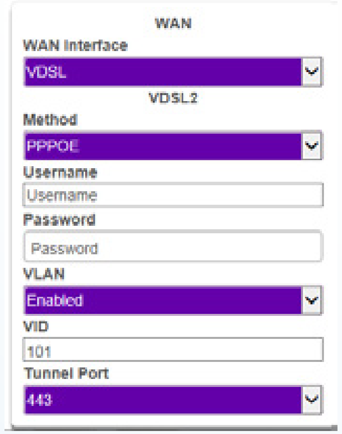


Remote Access

Web Access Passcode
0

WAN as LAN, DHCP Server and port forwarding are for future developments.





WAN

WAN Interface
VDSL

VDSL2

Method
PPPOE

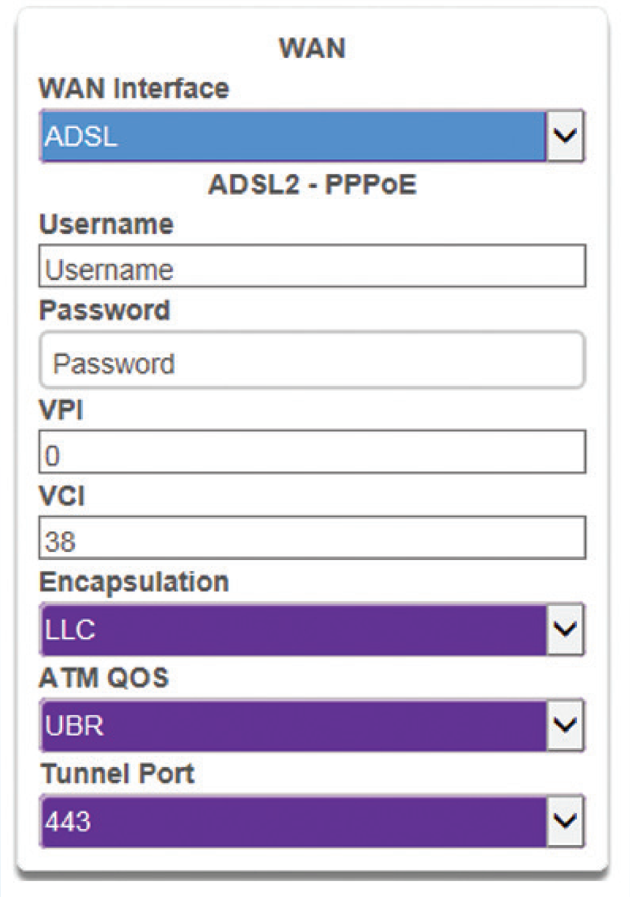
Username
Username

Password
Password

VLAN
Enabled

VID
101

Tunnel Port
443



WAN

WAN Interface: ADSL

ADSL2 - PPPoE

Username: Username

Password: Password

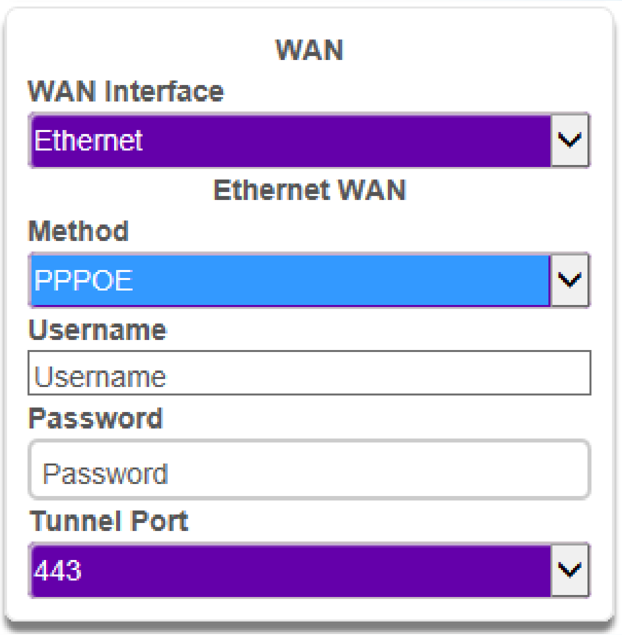
VPI: 0

VCI: 38

Encapsulation: LLC

ATM QOS: UBR

Tunnel Port: 443



WAN

WAN Interface: Ethernet

Ethernet WAN

Method: PPPOE

Username: Username

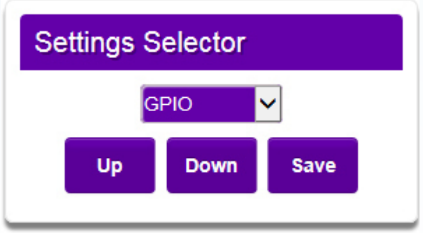
Password: Password

Tunnel Port: 443

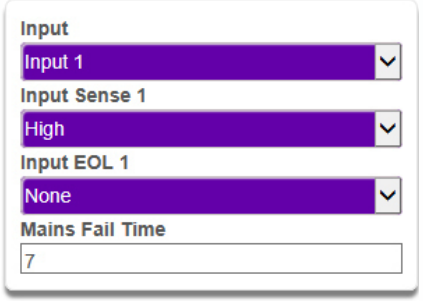
For ADSL and FTTP (WAN) the settings are as follows.
These should not be changed.

GPIO

In this menu, by using the drop down arrows on each section, you can change any of the PIN input status from High (positive removed) to Low (positive removed). You can set up either end of line (EOL) or dual end of line (DEOL) for each PIN as required. Mains fail time for Pin 13 can be adjusted. If set to Zero, PIN 13 becomes a normal alarm pin. Each of the 3 Outputs can be configured as described earlier in this guide.


Settings Selector

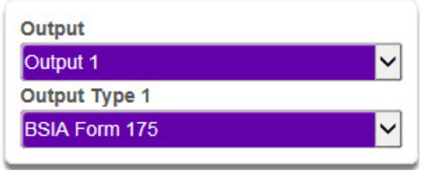
GPIO


Input: Input 1

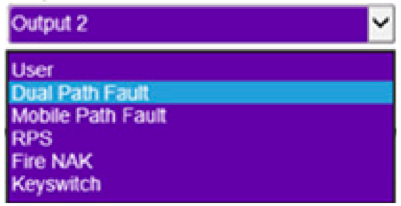
Input Sense 1: High

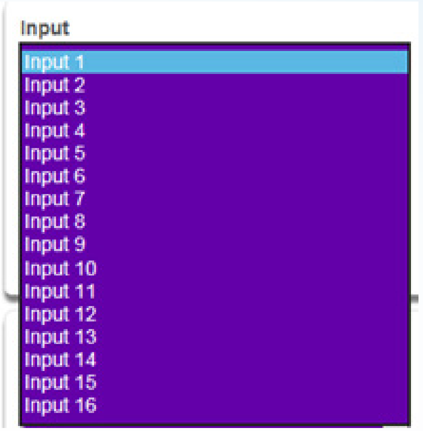
Input EOL 1: None

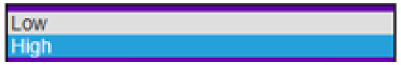
Mains Fail Time: 7

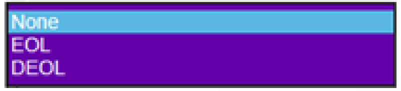

Output: Output 1

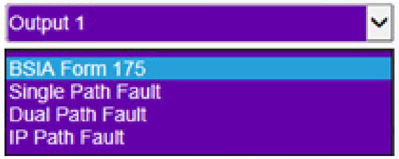
Output Type 1: BSIA Form 175


Output 2

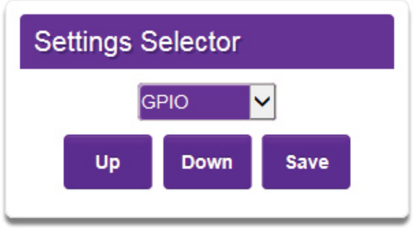




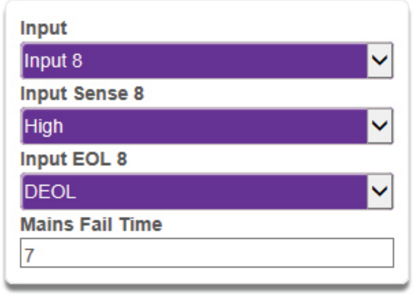



Output 1

When Output 2 is set to keyswitch you will need to go to the Keyswitch section to select the correct settings.


Settings Selector

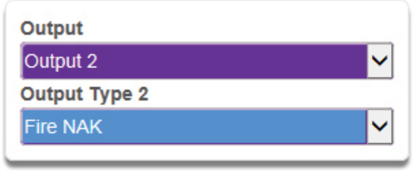
GPIO


Input: Input 8

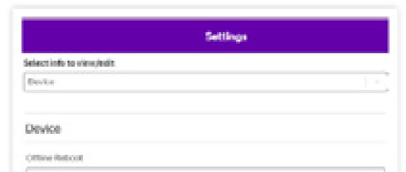
Input Sense 8: High

Input EOL 8: DEOL

Mains Fail Time: 7


Output: Output 2

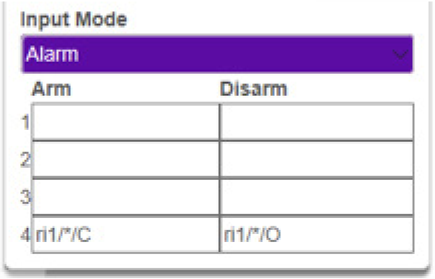
Output Type 2: Fire NAK


Settings

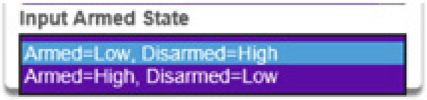
Select info to view/edit: Device

Device

Offline Reboot

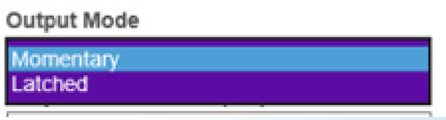

Input Mode: Alarm

	Arm	Disarm
1		
2		
3		
4	ri1/*/C	ri1/*/O


Input Armed State

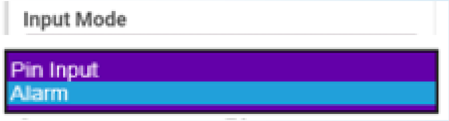
Armed=Low, Disarmed=High

Armed=High, Disarmed=Low


Output Mode

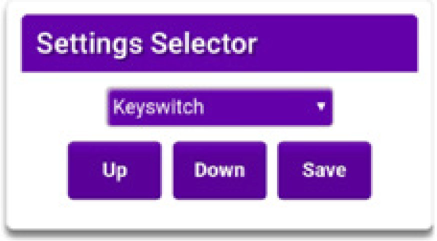
Momentary

Latched

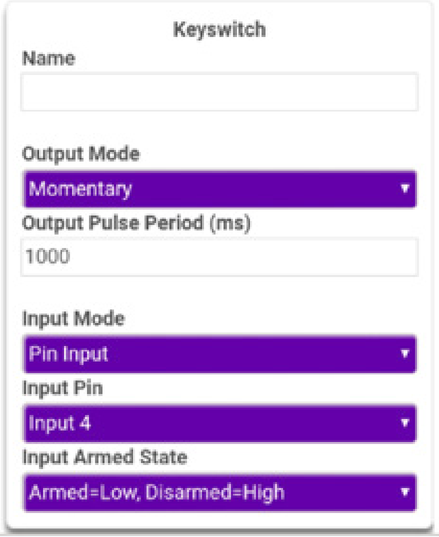

Input Mode

Pin Input

Alarm


Settings Selector

Keyswitch


Keyswitch

Name:

Output Mode: Momentary

Output Pulse Period (ms): 1000

Input Mode: Pin Input

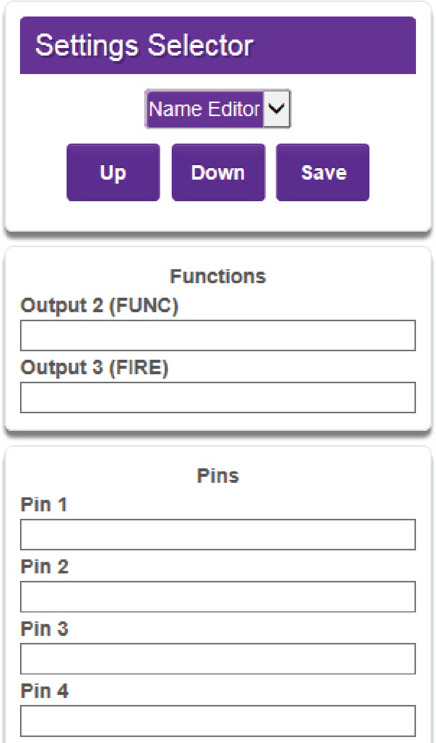
Input Pin: Input 4

Input Armed State: Armed=Low, Disarmed=High

In the example above, we show PIN 8 as Active High, with DEOL monitoring. Output 2 is set to operate as a Fire NAK output (operates if an acknowledgement on a PIN 1 alarm is not received within 80 seconds).
Make all the changes to the PIN inputs and outputs then click the save button to store your changes in the unit. Program success will be displayed.

A keyswitch can be set up to operate in conjunction with the AddSecure App. Any pin can be used, but will typically be Pin 4. It can be Latched or Momentary and armed low or high.

There is also the option to set up Keyswitch with extended format signalling.



Settings Selector

Name Editor

Functions

Output 2 (FUNC)

Output 3 (FIRE)

Pins

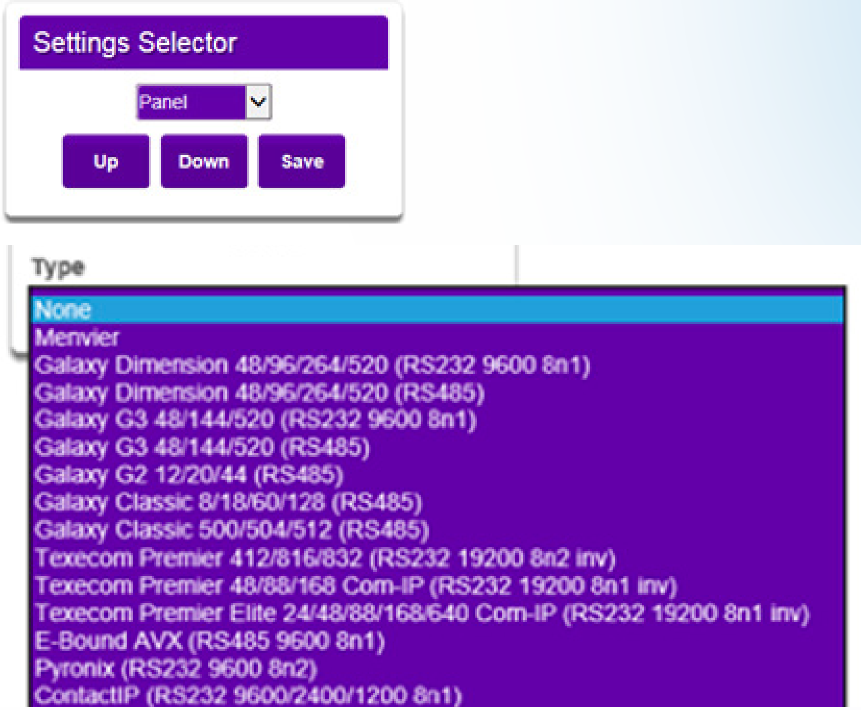
Pin 1

Pin 2

Pin 3

Pin 4

It is possible to add names to the PIN inputs. This will then show up on the customer app and notifications. You can choose a description for the USER relay outputs. Click save when you have entered all the information.



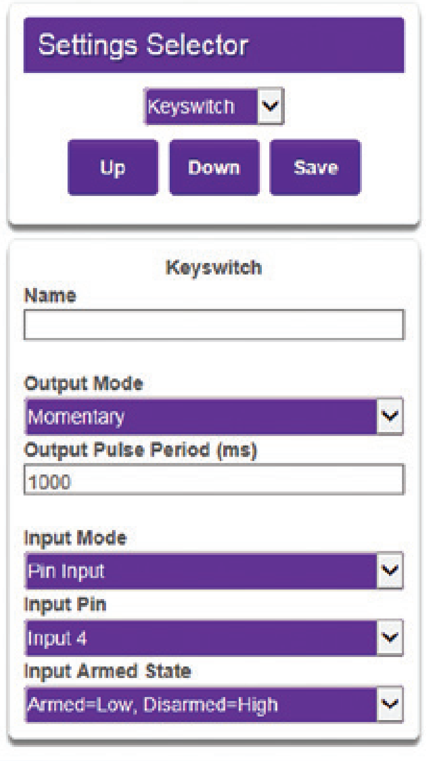
Settings Selector

Panel

Type

- None
- Menvier
- Galaxy Dimension 48/96/264/520 (RS232 9600 8n1)
- Galaxy Dimension 48/96/264/520 (RS485)
- Galaxy G3 48/144/520 (RS232 9600 8n1)
- Galaxy G3 48/144/520 (RS485)
- Galaxy G2 12/20/44 (RS485)
- Galaxy Classic 8/18/60/128 (RS485)
- Galaxy Classic 500/504/512 (RS485)
- Texecom Premier 412/816/832 (RS232 19200 8n2 inv)
- Texecom Premier 48/88/168 Com-IP (RS232 19200 8n1 inv)
- Texecom Premier Elite 24/48/88/168/640 Com-IP (RS232 19200 8n1 inv)
- E-Bound AVX (RS485 9600 8n1)
- Pyronix (RS232 9600 8n2)
- ContactIP (RS232 9600/2400/1200 8n1)

Allows selection of the Serial connection for specific panel types. Select the drop down next to Type and you will get a list of panel types. Select the required panel type and connection type and then click save. Program success will be displayed.



Keyswitch

Keyswitch

Name

Output Mode: Momentary

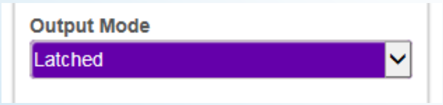
Output Pulse Period (ms): 1000

Input Mode: Pin Input

Input Pin: Input 4

Input Armed State: Armed=Low, Disarmed=High

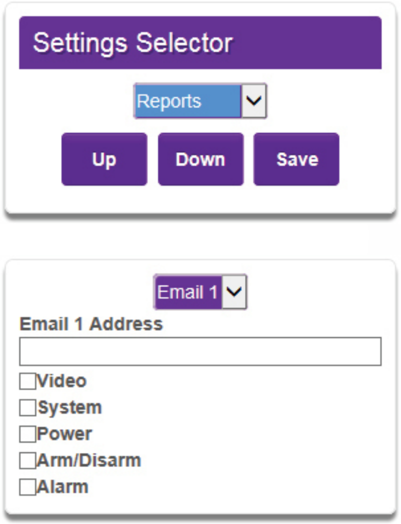
Output pulse period can be changed if required. (milliseconds)



Output Mode: Latched

There is an option to change the output mode to Latched.

Reports



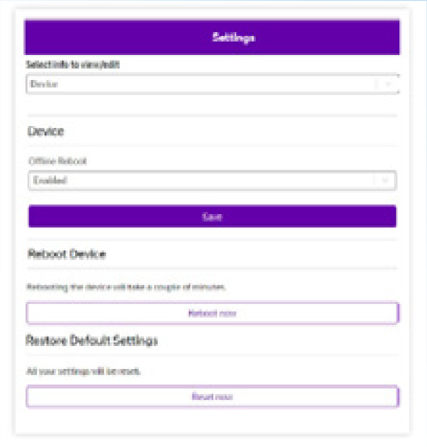
Reports

Email 1

Email 1 Address

□Video
□System
□Power
□Arm/Disarm
□Alarm

This allows you to set up a number of email addresses that could receive emails on the various options. e.g. Alarms and System messages.



Select info to view/edit: Device

Device

Offline Reboot: Enabled

Reboot Device

Rebooting the device will take a couple of minutes.

Restore Default Settings

All your settings will be reset.

The **Default sub-menu** gives you the option to disable auto reboot. This is where the device will auto reboot to try to restore the connection after approximately two hours of losing that connection to the platform. Use the drop down arrow next to enabled, change to disabled and click save. This will stop the device auto rebooting.

Reboot device allows you to reboot the device remotely. Click reboot now.

You will have to re-connect to the device as rebooting will lose the connection. Try reconnecting after a couple of minutes. To restore the unit to factory settings click Reset now.

Logout

Clicking Logout will take you back to the sign in screen.

Should the web server enablement time out, you will not be able to save changes. You will need to re-enable the Web Server through the programming buttons.

Web portal and AddSecure app

The device menus are accessible via the AddSecure web portal and app.

AddSecure App Password

To change an existing known password on the AddSecure App

- Go to Settings and turn off the app lock (password) by toggling the button.
- You will need to enter your current password,
- When you re enable app Lock (password) it will ask you to create a new password.
- If you forget your App password you will need to un install and re install the app.
- When using the web portal and app remotely after installation is completed then the following will apply.

Compliance with the user access level requirements of EN 50136

Access to the configuration options by an installer must be authorised by a level 2 user e.g. site owner. For the Next Generation alarm transmission equipment compliance is achieved at installation by requiring a one-time authorisation agreed as part of a service level agreement.

It is recommended the signed authorisation is retained with the 'as fitted' documentation. An example authorisation form is provided in the Appendix. To comply with EN 50136-2 Clause 5.2 Access levels, the PIN code access must be set to 6-digits. You can change the access PINs in the USER settings.

This applies for all types of access to the device.

Firmware updates

During the installation process or annual maintenance visit, it's important to check to see if there are any firmware updates available for the device.

You should apply any firmware updates at that point – either from the AddSecure web portal, or by the AddSecure Helpdesk under the instruction of an on-site engineer.

There'll be firmware updates for security updates, bug fixes and additional functions. Once you've installed a device, you can check for firmware updates and apply them at any time, using the AddSecure web portal.

It's your responsibility to update the firmware, as a reboot of the device will take place.

Notification of software updates is via the web portal. If the update is critical, then the installer will receive an email indicating the risks mitigated by the new version. The release notes and relevant documentation will also provide details on the period of service disruption should

the user initiate the upgrade.

Relevant upgrade documentation is saved as part of the Webportal for the installers.

You will need to login to find the latest information.

It is the responsibility of the installer to communicate with the end-customer before changes are made to the communicators.

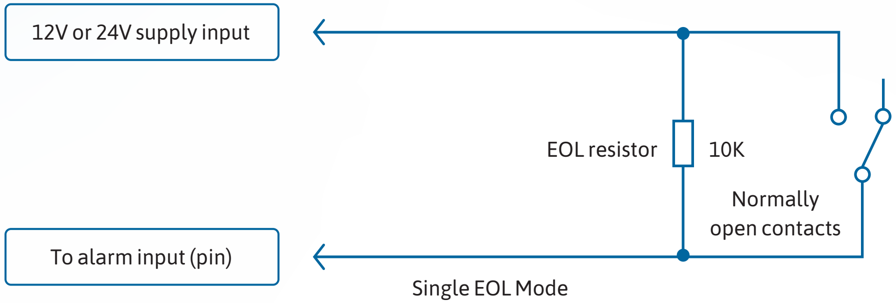
Interconnection monitoring

Interconnection monitoring

If the enclosure housing the unit is not next to, or close coupled to, the fire panel e.g. right next to the fire panel enclosure or perhaps a very short (<25mm/1”) section of cable conduit coupling the enclosures together, then there is a requirement in EN54-21 to detect open or short circuits on the interconnection wiring between the fire panel and the unit, as well as an indication back to the fire panel of an issue.

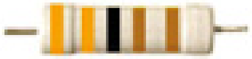
The power connections need to meet EN54-21 7.5.2 when the unit is fitted in an enclosure remote from the Fire control panel.

To enable the interconnection monitoring you will need to program the unit via the config menu, app or web portal.



You will need 1 x 3K3 and 1 x 10K resistors for each PIN with interconnection monitoring.

3.3KΩ 1%



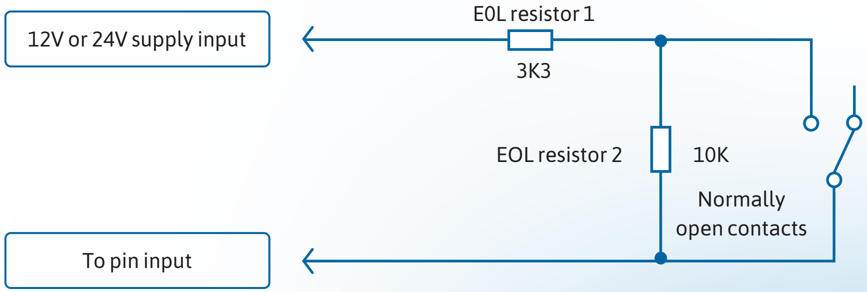
orange, orange, black, brown, brown

10KΩ 1%

brown, black, black, red, brown

Wiring for interconnection monitoring

Each of the pins required will need to be wired as shown below.



What happens when pins are configured and wired in this way

The dual resistor EOL mode is able to detect four states:

- Alarm event
- Restore
- Wire cut
- Wire shorted

The OLED display will show Pin cut 1 through 16 to indicate the wire cut condition for any of PINs 1–16, which are presently in the wire cut state.

Alarms GPI Cut
6

Above, example Cut on Pin 6.

The OLED display will show Short 1 through 16 to indicate the wire shorted condition for any of PINs 1–16, which are presently in the wire shorted state.

Alarms GPI Cut
8

Above, example Short on Pin 8.

Example configuration and wiring for connection to fire panel with interconnection monitoring

Ensure that the required pins have Dual EOL enabled in the config menu. In the example Pin 1 and Pin 8 have been enabled for this.

Note it is available on pins 1 – 16

- Output 1 = Single path fail
- Output 2 = Fire NAK
- Output 3 = Fire ACK

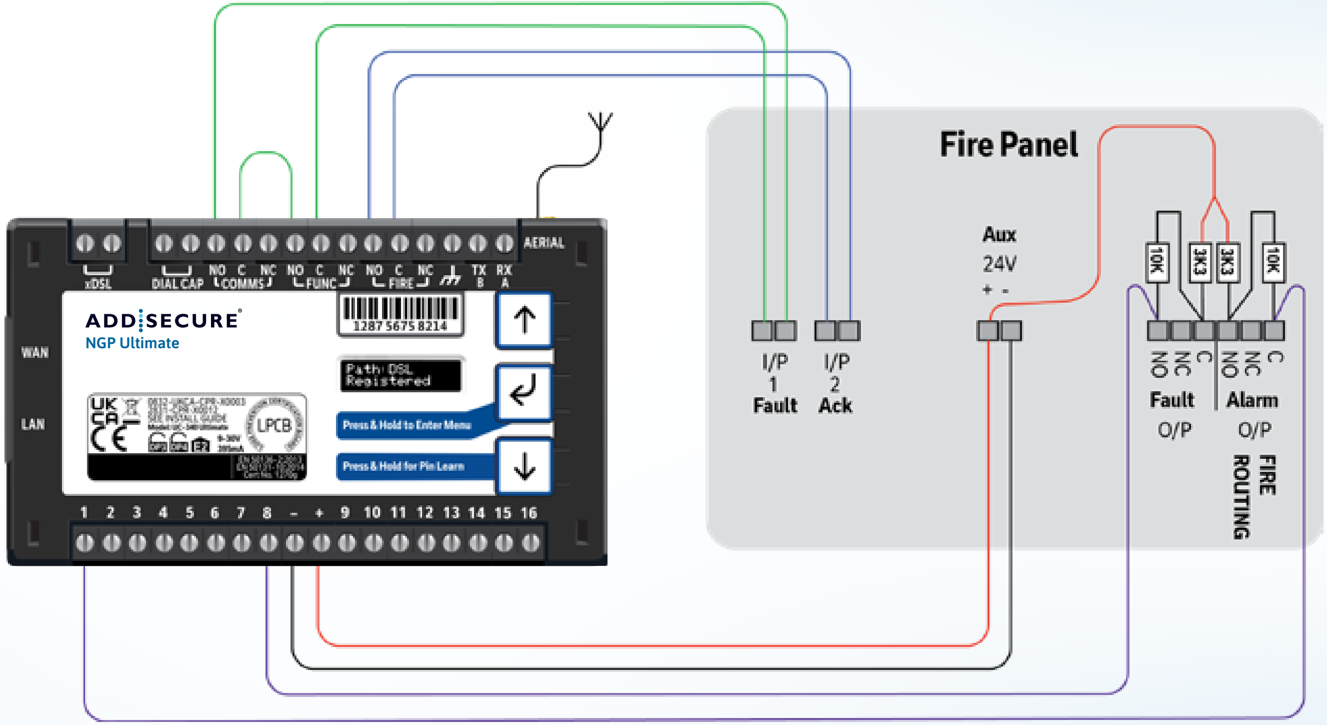


Figure 7 – Typical fire alarm connections for panel with 2 inputs and unit with interconnection monitoring

Roaming SIMs

The unit has two SIMs.

- SIM 1 – EE network sim with 4G and 2G
- SIM 2 – A UK roaming sim with 4G and 2G network access

The unit uses smart roaming to determine which network to use. Should network connectivity be lost the unit will try different networks, 4G and 2G and will also swap SIMs if required.

Should the unit lose connectivity with the AddSecure platforms, or lose registration with the current base station, then the unit will roam onto the next available 4G or 2G network.

Panel upload Download and Enhanced format signalling (SIA/CID)

Remote access to the alarm panel can be achieved using the AddSecure UDL facility. Additional panel set up information is also available for enhanced format signalling. Contact your AddSecure representative for further details.

Dial capture

The dial capture pins present a 'phone line' to the panels on-board digital communicator Connect the alarm panel's digital communicator line connections to the terminals marked Dial Cap on the unit. The terminals are not polarity conscious.

Configure the alarm panel digital communicator to dial 29 and use the last 4 digits of the TAID as the account number.

The dial capture board will auto detect the panel protocol as events are sent from the alarm panel. SIA, CID or FF.

Please check current panel compatibility listing.

If there are any issues you can easily spot them and put them right by connecting a test phone, or listening device to the Dial Capture inputs. The dial capture pins with a test phone connected and line seized (as if making a phone call) will provide a continuous tone (dialling tone). The dial capture pins will also have a voltage on there of 45V.

Serial panel connections

Select the required panel via the serial panel type menu option via the buttons, app or web portal.

Please contact your AddSecure representative for the latest information on panel compatibility for Upload download and enhanced format signalling via serial connections.

Then wire in the panel using the GND, TX/B and RX/A terminals.

Example below shows connection via RS 485 to a Galaxy Dimension panel:

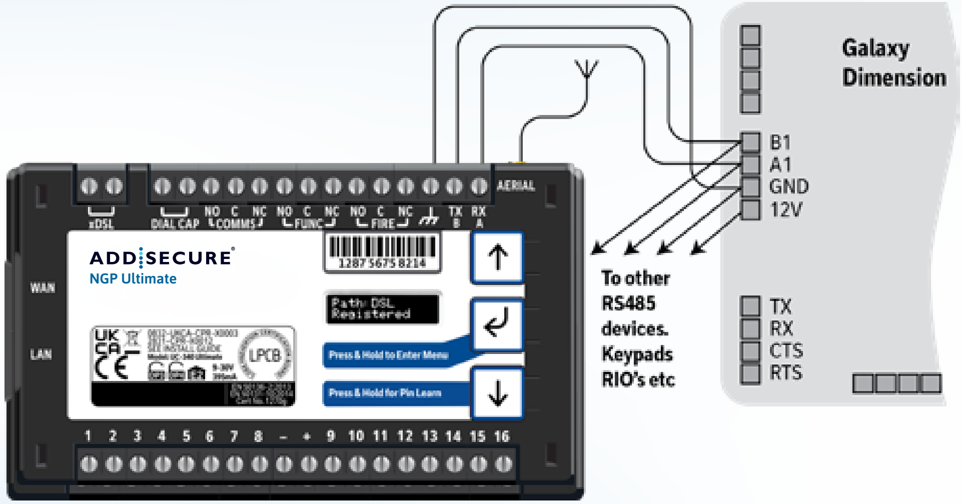


Figure 8 (not to scale).

Connection advice

The unit should be connected to the Honeywell Galaxy panel as shown in figure 11, RS485A to A1 and RS485B to B1. Do not use the secondary data line (if your panel has one – A2/ B2) as it will not work. Ensure that the GND of the unit is connected to the GND terminal on the panel.

It is recommended that good quality screened cable (Belden type, CAT5e or equivalent) is used in all wiring of this type to avoid interference on the panel's data bus. A 680Ω resistor should be used at the end of the 'daisy chain' line of devices in the normal way, taking care not to exceed the maximum number of devices allowed on that data line. If the unit is fitted less than 5m from the alarm panel then an additional termination resistor is generally not required.

The Unit does not have a terminating resistor.

Alarm list

Description	Pin	CID (zone)
Inputs 1-16	1-16	323 (901-16)
Low Battery	985	302 (999)
Unit reboot	984	305 (995)
Panel dial fail	983	314 (999)
Software changed	979	304 (999)
Panel message error	958	311 (997)
Panel Connection (RS485)	n/a	356 (997)
BSIA 175 Test	n/a	354 (998/999)
Inputs 1-16 cut alarm	n/a	325 (901-16)
Inputs 1-16 Short Alarm	n/a	324 (901-16)
IP Path	1023	351 (999)
Mobile Path	1022	351 (998)
Total Comms Fault	n/a	350 (999)

Figure 9 – alarms signals as delivered to your ARC

IMPORTANT NOTE: If intending to use dial capture or serial for sending alarms, please confirm beforehand with your ARC that their automation software is capable of differentiating correctly between PIN alarms (NGP Ultimate or AddSecure Platform generated alarms) and alarm panel generated ZONE alarms.

If used temporarily as an Advanced on a customers Network or broadband then the following applies:

IP specification notes

IP Protocol: TCP
Port: 443 or 10443

Data usage/requirements

IP polling is every 30 seconds. A poll and response results in 288 total bytes transferred (incl IP headers). A small number of alarms will also typically be generated per day and these result in 296 bytes transferred. Overall this generates approximately 800K bytes per day, per site.

Traffic direction

The Advanced and Advanced Extra establishes an outgoing TCP connection from your network to the AddSecure platform. Once this outgoing TCP connection has been established, traffic over that connection is 2 way.

Additional protocols

Only TCP is required from your network.

Port forwarding

No ports need to be forwarded in the incoming direction. The outgoing TCP connection connects to port 443 or 10443 on the AddSecure network, so you would need to allow outgoing access to port 443 or 10443 if you block that by default.

NAT

Not required.

4G/2G requirements

You do not need to route mobile traffic. The mobile connection from the communicator through to the AddSecure platform and on to the ARC is entirely independent of your network.

DHCP and static addressing

The communicators can be configured as either DHCP clients or with specific static IP addresses on your internal network as you prefer.

DNS server

The device uses host names for establishing connection to the servers so DNS addresses will be required.

Personal Data

Personal information consent
Installers should obtain the End Customers consent should they wish to include any personal data in the app or portal.

End of Service
The End Customer needs to follow the standard process to cease the service with their installers. The following steps should be followed by the installer when disabling a service. The Installer should cease the service with the Alarm Receiving Centre. AddSecure will then cease the entry on the portal within 3 months (this allows for re instatement of any cease in errors) **The communicator needs to be recovered from site by the installer or defaulted to restore its configuration to factory defaults.** The installation quick start guide provides steps to set the unit back to factory defaults. The unit should then be powered down so that it will not attempt connection to the network. All personal data associated with the unit will be deleted from the device. However, historical event information will remain in the system archives for 7 years as part of compliance requirements.

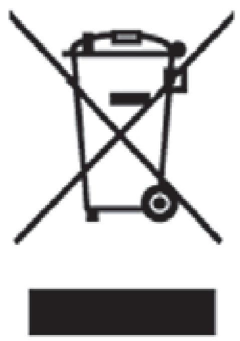
Withdraw of End Customer Consent
The only way for an End Customer to withdraw consent of personal data processing by AddSecure is to deactivate the service. Please refer to the End of Service section above for more details. The End Customer will need to remove the APP from their personal smart device using standard methods. Installers will need to delete the Site from their APP using standard site deletion method.

AddSecure privacy policy can be found here https://www.addsecure.com/alarm-signalling/uk/ which includes what to do if you are unhappy about how we have handled personal information.

Disposal

The symbol shown here and on the product means that it’s classed as Electrical or Electronic Equipment, and should not be disposed of with other household or commercial waste at the end of its working life.

The Waste Electrical and Electronic Equipment (WEEE) Directive (2002/96/EC) has been put in place to recycle products using the best available recovery and recycling techniques, to minimise the impact on the environment, treat any hazardous substances and avoid increasing landfill.



Product disposal instructions for users

Please dispose of the product as per your local authority’s recycling processes. For more information please contact your local authority or retailer where the product was purchased. You can return the product to the freepost address below:

BT Supply Chain
Darlington Road
Northallerton
North Yorkshire
DL6 2PJ

Disclaimer

The manufacturer or his agents disclaim responsibility for any damage, financial loss or injury caused to any equipment, property or persons resulting from any use of this equipment. The manufacturer is not liable for any purely economic loss arising from any use of this equipment. All responsibility and liability in the use of AddSecure products are assumed by the user.

This unit is designed to be used in customer premises. Use of this equipment in other locations may void warranty.

This unit is not intended for use in marine environments or water borne vessels.

AddSecure may make changes to features and specifications at any time without prior notification in the interest of ongoing product development and improvement.

Glossary

ADSL
Asymmetric digital subscriber line (Broadband)

ARC
Alarm Receiving Centre

BSIA
British Security Industry Association

CSQ
Carrier Signal Quality (RSSI,BER)

DHCP
Dynamic Host Configuration Protocol

DNS
Domain Name System

F175
Form 175 as issued by BSIA

FTTC
Fibre To The Cabinet

FTTP
Fibre To The Premise

GMT
Greenwich Mean Time

IP
Internet Protocol

LAN
Local Area Network

MMCX
Micro Miniature Coaxial Connector

OLED
Organic Light Emitting Diode

RSSI
Received Signal Strength Indicator

RPS
Return Path Signalling
(An output that confirms delivery of Pin 4 to the ARC)

RX
Receive

SID
Serial Identity number – 12 digit unique identity number of a unit

SIM
Subscriber Identity Module (sim card)

TTL
Transistor Transistor Logic

TX
Transmit

VDSL
Very high speed digital subscriber line

WAN
Wide Area Network

Approvals

BT Redcare,
British Telecommunications plc 2024.
Registered office: 1 Braham Street,
London E1 8EE.
Registered in England
No. 1800000.

November 2024

NGP Ultimate is suitable for use in systems installed to conform to PD 6662:2017 at Grade 4 (DP4) and environmental class 2.

EN 54-21:2006
Alarm transmission and fault warning routing equipment for fire alarm systems.
Constancy of performance certificate for Construction Products Regulation.
2831-CPR-X0012
0832-UKCA-CPR-X0003
NGP Ultimate

LOSS PREVENTION CERTIFICATION BOARD
LPCB
EN 50136-2: 2013
EN 50131-10: 2014
Cert No. 1270g

Product	Fire Product	Transmission time Classification	Transmission time Max. Values	Reporting time Classification	Substitution Security	Information Security	Network Availability
NGP Ultimate	EN 54-21 Type 1	D4	M4	T5	S2	13	A4

The Ultimate unit meets the following performance parameters as per EN 54-21 Annex A.

Technical Data: see www.addsecure.com/alarm-signalling/uk/

Technical support:
AddSecure Ltd
Phone: +44 20 461 431 70
Email: support.smartalarms.uk@addsecure.com

Support
For assistance with your AddSecure installation, please contact the AddSecure Helpdesk.
If there is a problem with the service and/or communicator the End Customer should contact the alarm installer. The alarm installer can contact AddSecure Helpdesk M-F 9 till 5.

bsi Internet of Things - Commercial KITEMARK™ Secure Digital Applications KITEMARK™

KM 742188
In respect of: Internet of Things (IoT)
Security of a device against common vulnerabilities for use in a commercial environment (includes Residential environment)

bsi Internet of Things - Commercial KITEMARK™ Secure Digital Applications KITEMARK™

KM 742187
In respect of: OWASP ASVS and MASVS
Secure Digital Applications
Mobile Applications (OWASP MASVS Ver 1.3 Level 1):
AddSecure Mobile Application Android version 2.18.0 Build 0363
AddSecure Mobile Application iOS version 2.18.0 Build 0463
Web Application (OWASP ASVS 4.0.2 Level 1)
The AddSecure Portal Application

Secured by Design
SBD
Police Preferred Specification

LPCB certification

- Extensive testing by BRE has independently validated the performance of Advanced/Advanced Extra and demonstrated compliance with the applicable EN 50131 and EN 50136 standards.
- Regular on-going surveillance of the manufacturing facilities by BRE, ensures the high quality of the Next Generation range is maintained through the life of the products.
- LPCB certification provides prescribers and owners of intrusion alarm systems with assurance that the signalling equipment will respond rapidly and continue function reliably, a prerequisite for any monitored alarm system.

BSI 'Kitemark' accreditation for IoT devices, app and portal

- The Kitemark is designed to help consumers confidently and easily identify IoT devices, apps and portals that they can trust to be safe, secure, and functional.
- Once the BSI Kitemark is achieved the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained the BSI Kitemark will be revoked until any flaws are rectified.
- The IoT Kitemark assessment process involves a series of tests that help ensure the device is fully compliant to the requirements. Before being awarded the Kitemark the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing scanning for vulnerabilities and security flaws.
- An app that has been awarded a BSI Kitemark™ for Secure Digital Applications has demonstrated that it has appropriate robust security controls in place for the information it is handling. To achieve the BSI Kitemark, an app must undergo rigorous and independent testing.

Police CPI 'Secured By Design' (SBD) accreditation

- Police Crime Prevention Initiatives (Police CPI) is a police-owned organisation which delivers a wide range of crime prevention and demand reduction initiatives across the UK.
- The extensive Police CPI portfolio covers a variety of crime prevention initiatives, of which Secured by Design is the most well-known, with all initiatives designed to keep the public safe from crime.
- Secured by Design (SBD) operates an accreditation scheme on behalf of the UK Police Service for products or services that have met recognised security standards. These products or services, which must be capable of deterring or preventing crime, are known as being of a 'Police Preferred Specification'.

Appendix

Example authorisation form

For the purposes of on-going maintenance and configuration

Company name

Authorises

Installer company name

Remote access to AddSecure Next Generation Supervised Premises Transceiver

Serial No. *number*	
Installed at: *premises address*	
Date	*Signature*

ADDSECURE