iris touch

Alarm over IP

IRIS Touch 2 NG SERIES
Engineering Manual

Version 1.2

CE EN 50131/6 Independently certified VdS

Contents

1. Introduction

The IRIS Touch 2 offers cost effective Alarm over IP (AoIP) for the commercial and residential sectors.

All IRIS Touch 2 diallers are certified as suitable for all Grade 4 systems with an Alarm Transmission System (ATS) configuration up to SP6 for single path, or ATS configuration DP4 for dual path (IRIS Touch 240NG only).

The IRIS Touch 2 is based on Chiron's successful IRIS Touch range of AoIP diallers with the same hardware and software used in all IRIS diallers; with the same level of security and features provided to military, governments, banks and commercial industry markets.

The IRIS Touch 2 offers a touch screen as standard for configuration, local alerts, and allows diagnostic and tests to be performed by the engineer.

Polling and alarm transmission are performed via the Ethernet or GPRS/3G communication paths (4G and CDMA on request) to the monitoring centre using the IRIS Secure Apps monitoring software.

2. IRIS Communication Mechanism (Polling / Alarms)

The polling / alarm mechanism used on the Chiron IRIS system is highly secure and flexible, and uses the IRIS Secure Apps monitoring software (installed at the monitoring centres) with the IRIS Touch diallers.

It has been independently certified as compliant to the Grade 3, ATS6 - within the EN50131 standard for alarm systems.

The IRIS system is unique in its ability for the polling frequency to be varied which means that the polling profile can be adjusted as necessary to take into account the grade of security required and the traffic bandwidth available.

Key features are:

- Independently certified as compliant with EN50131-1 Grade 3 ATS configuration SP6 over Ethernet and ATS – SP5 over GPRS for single path Ethernet and DP4 for dual path communications.
- After initial installation all backup or alternate IP address for the Polling engines (main & backup) are downloaded to the IRIS Touch dialler over the polling communications.
- All polling and alarms are authenticated by the receiver (Polling Engine) using the secure and sophisticated 'Challenge Handshake' mechanism as used in military and credit card applications. Each remote IRIS dialler proves its authenticity using a 256 bit security key. A new random number generated by the receiver (Polling Engine) is used for every poll so it is not possible to substitute the dialler using playback or sequence prediction.
- Unlike other systems each dialler can have a unique security key which can be changed at the monitoring centre any time as required. For additional security the installer never needs to load the key or be aware of what it is.
- Also unlike other systems, the polling frequency is not fixed and can be varied by the monitoring centre at any time, from a period of 10 seconds for high security systems down to once a week for low security systems. This means that polling rates can be optimised to deliver the grade of service required and minimise the bandwidth required.
- Polling and alarms are carried over the TCP/IP protocol that gives end-to-end error protection. This removes the possibility with other protocols such as UDP that data packets are lost or re-sequenced in the network leading to false alarms.
- All polling and alarms are outbound from the dialler location to the monitoring centre and do not require the IP address of the dialler to be known. No special set-up is required at the customer's router, such as port mapping for incoming calls. This feature is essential for operation with networks with dynamic addressing and standard GPRS/3G networks.
- Background communication path polling is also configurable at the monitoring centre and enables the IRIS dialler to periodically poll over the backup communication path, and any faults with this communication will be reported back to the IRIS Secure Apps system.
- Each poll transaction is very small and with the authentication protocol is only about 500 bytes of data, including all traffic in both directions. For fixed line IP networks there are no traffic costs.

Total traffic is proportional to the polling frequency. For example, at 10 second poll 180K bytes per hour and at 3 minutes polling this would reduce substantially to only 10K bytes per hour.

Even with tariffed networks such as GPRS/3G, and when running at a polling rate suitable for the highest level of security, a typical cost is only a few Euros per month. For GPRS/3G in many cases the level of traffic falls within the free bandwidth that comes with the SIM card contract and will effectively be at no cost.

3. Product Features

Features	IRIS Touch		
	200NG	220NG	240NG
Fire retardant enclosure	●	●	●
Touch screen	●	●	●
Ethernet	–	1	1
GPRS/3G	●	–	●
Dial capture	●	●	●
Relays	3	3	3
Inputs (Pins)	4	4	4
Serial RS485	●	●	●
Serial TTL	●	●	●
RS232 (Basic or Full)	Basic		
Text messaging	●	–	●
Multi language menus	●	●	●
VoIP & SIP services	●	●	●
Option available on request	4G / CDMA		

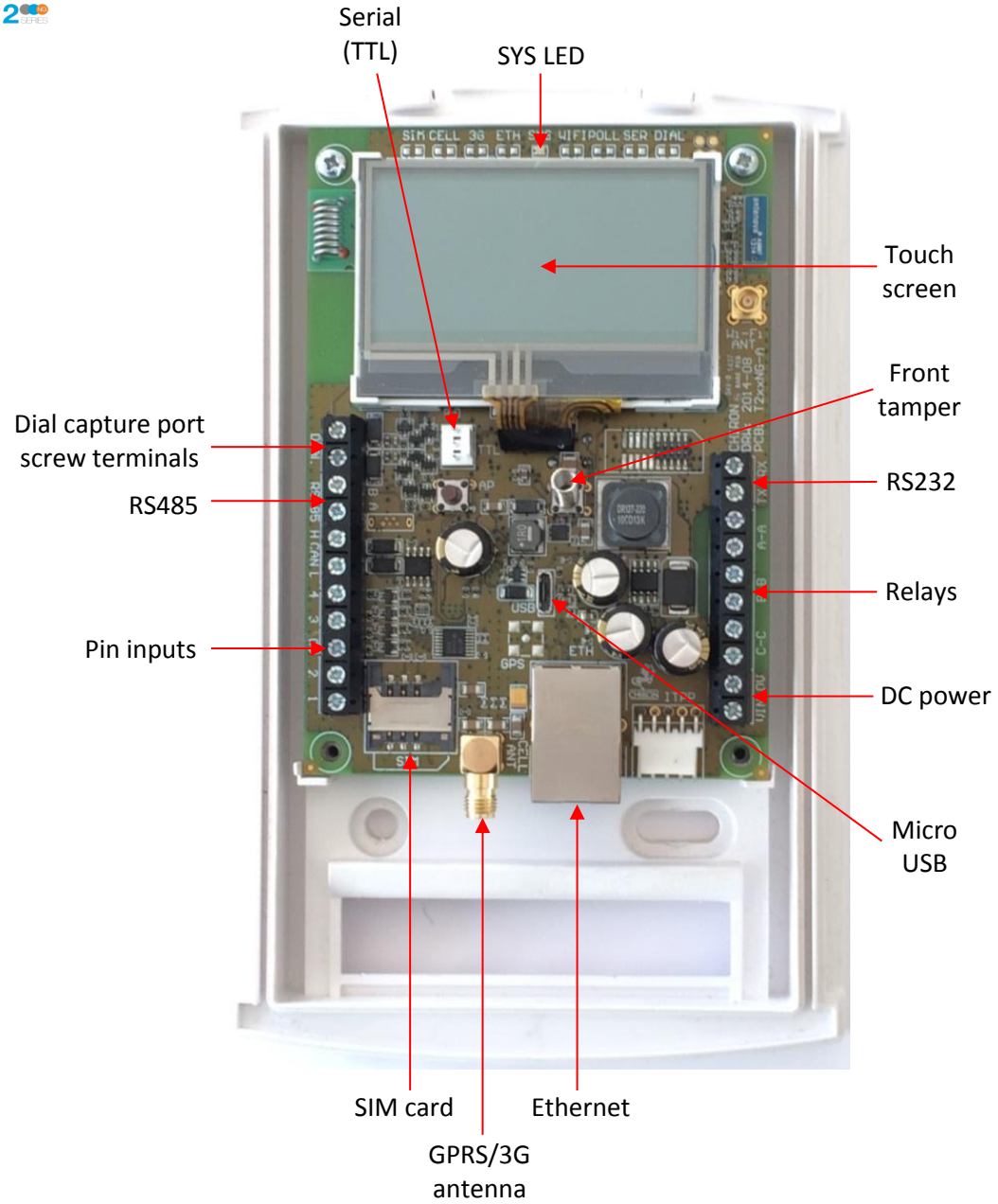
4. Package Contents

Contents dependent on model type:

- Dialler board in plastic housing
- Ethernet cable (IRIS Touch 220NG & 240NG)
- GPRS/3G antenna (IRIS Touch 200NG & 240NG)
- Stylus
- 18k Ohms sense resistor

5. Board Configuration

IRIS Touch 2



SYS LED

LED Colour	Indication
Yellow flashing	Not currently configured or indicating that there are some current faults outstanding. See Section 9 "Trouble report".
Yellow constant	Communicating and no current faults (flickers on every poll).

6. Before You Start

Monitoring Centre (ARC)

Make sure that the monitoring centre to which the IRIS Touch device will send alarm signals is equipped with the appropriate IRIS Secure Apps receiving system. The following information should be obtained from the monitoring centre.

Dialler account number	
Monitoring centre IP address	

Ethernet Connection Details

The customer's Ethernet (LAN) network details are required in order to connect the IRIS Touch. The following information should be obtained from the customer.

Fixed IP address or DHCP	Fixed ☐	DHCP ☐
	If using DHCP then the following information will not be required as it will be assigned by the network.	
IP address		
Gateway address		
Subnet mask address		

GPRS/3G SIM Card and Access Point Name

If the installation uses GPRS/3G then a SIM card will be required. The IRIS Touch will also need to be given a GPRS/3G 'Access Point Name' (APN) and other possible configurations as shown below. These can be obtained from the SIM card provider.

Access Point Name (APN)	
User Name (USR)	
Password (PWD)	
SIM Pin	

7. Installing the IRIS Touch Dialler

Use the following procedure to install your IRIS Touch dialler:

7.1. Mounting

Choose a suitable location, taking into consideration the routing of cables: power, panel dialler interface cable. Remove the two case fixing screws under the slide cover and open the unit, remove the two PCB fixing screws and remove the PCB.

Position the housing on the wall and drill three holes. Feed the cables through the opening at the base of the plate, or via the 'knockouts', and secure the plate to the wall with the three screws supplied.

7.2. Power

The IRIS Touch dialler can be powered from a separate or Aux 9-28V DC power supply specified to delivery up to 1A current using the screw terminals indicated in Section 5 "Board Configuration".

Note: For Radio & Telecoms Terminal Equipment Directive compliance the power cable must be no longer than 3 meters in length.

Fit the power cable. DO NOT APPLY POWER TO THE DIALLER UNTIL INDICATED.

7.3. Connections

Connect cables to the PCB for your system as shown on in Section 5 "Board Configuration".

- Ethernet enabled systems (IRIS Touch 220NG & 240NG): Ethernet socket ETH.

  Connect the Ethernet cable from 'ETH' to the local IP router/switch or socket that has been allocated for the LAN/WAN network IP connection.
- GPRS/3G enabled systems (IRIS Touch 200NG & 240NG): Cell Ant. Fit the supplied T-bar GPRS/3G antenna but do not fix in place until after performing the GPRS/3G network scan.

  Note: An external GPRS/3G antenna can be fitted if required.
- Dial capture port (optional and for more information see section below).
- 4 x Pin Inputs.

Optional serial connection

The following 3 connections are optional and depend on the panel connection method to be used.

By default the IRIS Touch RS485 connection is for Honeywell Galaxy panels. For alternative selections for other panel manufactures use the touch screen on the IRIS Touch Installers menu – settings to select the option required.

- RS485 currently available for Honeywell Galaxy data bus (Alarms and Upload/download) or Risco ProSys bus (Upload/download) connections (optional).
- Serial TTL (optional).
- RS232 screw terminal (optional).

For more details on the cable requirements / connections please see details below.

RS485 connections (Honeywell Galaxy or Risco ProSys)

IRIS Touch to Honeywell Galaxy panels

IRIS RS485 screw terminal	To	Galaxy Data Bus terminal
0V (Power)	← →	Galaxy (-)
VIN (Power)	← →	Galaxy (+)
A	← →	Galaxy (A)
B	← →	Galaxy (B)

IRIS Touch to Risco ProSys panels

IRIS RS485 screw terminals	To	Risco Bus1 terminal
0V (Power)	← →	COM
VIN (Power)	← →	AUX
A	← →	YEL
B	← →	GRN

7.4. GPRS/3G SIM card (IRIS Touch 200NG or 240NG)

DO NOT FIT SIM card until after you have performed the GPRS/3G Network Scan detailed in the Section 7.9 "Configuration" you will be prompted when to insert the SIM card.

7.5. Dial Capture

Dial capture enabled systems: Connect the dial port screw terminals with the alarm panel dialler telecoms line connections.

Note: Polarity is not important in this instance.

Fit the supplied 18K sense resistor in parallel with the dialler output of the alarm panel, at the alarm panel end of the cable.

Note: This resistor enables the dialler to detect cable faults and/or tampers and must be fitted at the alarm panel end of the cable to function correctly, the monitoring centre will also need to enable the dial port monitoring from the IRIS Secure Apps software to receive alarm notifications.

7.6. Pin Inputs

The IRIS Touch dialler has 4 Pin inputs that can be used to generate alarm messages. These can be:

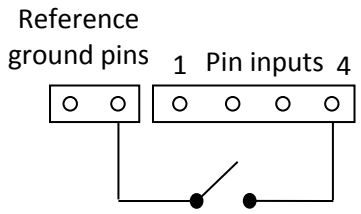
- Text messages via SMS *(GPRS/3G)*.
- SIA, Contact ID or Fast Format alarm messages over IP to the monitoring centre.

Note: These pin alarm inputs can also be used when the dialler is directly connected to an alarm panel via the dial capture, serial or RS485 connections.

Via Open/Close Contact Source

Each pin input is designed to be connected in a loop via an open/close contact source from an alarm panel, or other device, to a reference ground pin available on the IRIS dialler, as shown opposite.

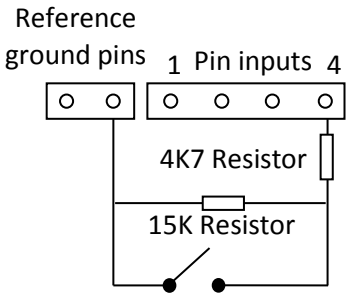
Opening the contact (i.e. loop is open circuit) generates an alarm signal. Closing the contact generates the equivalent restore signal.



Via Sense Resistors

It is also possible to link the contacts to the IRIS dialler via sense resistors so that an open or short circuit tamper on the loop can be detected and the monitoring centre alerted. In this case, the connections should be made as shown opposite.

Note: For this feature to work correctly it is essential that the resistors are connected at the contact end of the loop and not the dialler end. The monitoring centre must also enable the monitoring of this facility on the dialler within the IRIS Secure Apps receiving system.



7.7. Switch On and Test

To confirm power is applied, look for the indicator SYS LED flashing yellow on the IRIS Touch dialler board.

7.8. Configuration

To configure your dialler, use any of the following methods:

- Touch screen.
- Alarm panel integration e.g. Honeywell Galaxy (RS485 connection). Please refer to Section 7.9 "Panel Configuration".

  Note: For connections to Honeywell Galaxy on the serial integration ensure you configure the alarm panel first as this will transmit configuration to the IRIS Touch dialler.

  For more details on the alarm panel integration download the full panel installation manual from http://www.chironsc.com/downloads_security.html.
- Connect the board's Micro USB connector to a laptop / PC running the IRIS Toolbox software.

  Download the IRIS ToolBox user guide from http://www.chironsc.com/downloads_security.html.

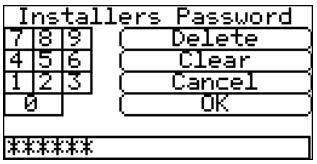
Defaulting

If at any point you want to completely default the dialler you can use the following procedure:

1. Enter the Installer menu on the dialler touch screen and enter the installer password.
2. Go to the 'Settings' option and scroll down with the scroll bar on right until you see option for 'Default All'.
3. Enter the 'Default All' and confirm that the dialler is to be defaulted.

Configuration via Touch Screen

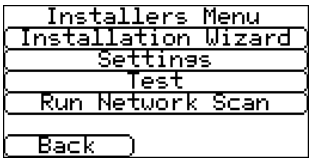
IRIS Touch 2 can be configured directly using the on board touch screen with the supplied stylus.



Enter the default installer code: 111111 and then click 'OK'.

You will be prompted to change the password, please record the new password.

Enter and confirm a new password and press 'Save'.



The *Main Menu* is displayed.

IRIS Touch 200NG or 240NG with GPRS/3G connection:

GPRS/3G Network Scan

Select the 'Run Network Scan'.

The scan must be carried out **without** the SIM card fitted.

The dialler listens for every base station in range, requests operator name and records the signal strength. This will take a few minutes to complete.

For a reliable GPRS/3G connection it is recommended that for the chosen network (SIM card) used there should be at least two base stations with signal strength (CSQ) of 10 or more.

If the signal strength is below or close to minimum then try to reposition the antenna/IRIS Touch dialler in a different location or you can use an external building or high gain antenna (if necessary), and rerun the network scan to check signal strength.

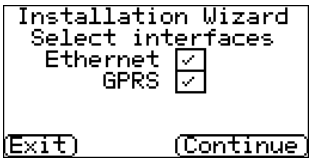
Once you have the required GPRS/3G signal strength power down the dialler and insert the SIM card into the SIM card holder, then power the dialler back up.

Go back into the 'Installers Menu' and enter in the installer code that you had setup beforehand and then select the Installation Wizard as indicated next.

IRIS Touch 220NG or 240NG without GPRS/3G or after network scan completed:

Installation Wizard

Select the Installation Wizard and follow the on screen prompts, if you require further information on this process then please check Section 8.2 “Installation Wizard”.

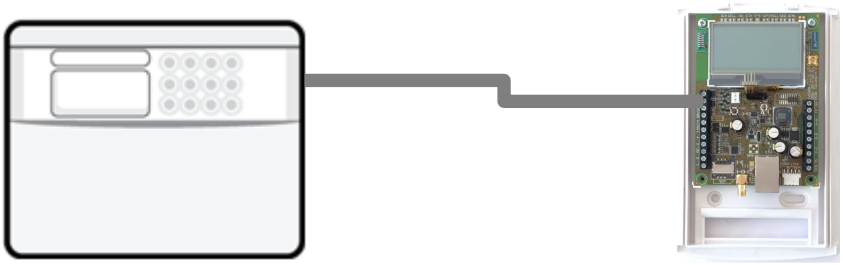


Once you have completed the Installation Wizard and setup any additional panel interface configuration via the settings menu you will need to check / configure the panel for the connection method you are using:

7.9. Panel Configuration

Panel configuration for dial capture

If you are connecting the IRIS Touch dialler via the dial capture method which is connecting the Telecoms module to the dial port of the IRIS Touch, you will need to configure the following options:



Alarm Panel IRIS Touch dialler

Alarm Panel Configurations:

Dial Type	=	Tone dial.
Telephone Number	=	The 12 digit format of the monitoring centre IP address e.g. 192.168.0.34 would become 192168000034.
Account Number	=	4 – 6 digit account number allocated by the monitoring centre.
Alarm Format	=	Fast Format (DTMF), Contact ID, SIA (level 1 to 3), or Robofon alarm format.

Note: If the ‘Alarm Override’ mode is selected, the IRIS Touch dialler replaces the phone number and the account number used by the alarm dialler with the IP address of the monitoring centre and account number entered during configuration, so there is no need to change any settings on the alarm panel.

You can now perform the alarm signals commissioning and sign off required by the monitoring centre (ARC).

Configuration from Honeywell Galaxy Panel via RS485

The IRIS Touch dialler can simulate a Galaxy Ethernet Module (Comm's Mod 4) and remote keypad, for both Alarms and Remote Service Suite upload/download connection.

Note: If you want to use the SMS messaging function from the Galaxy panel then you will need to emulate the external PSTN module, and setup the Galaxy External PSTN module settings see the IRIS Honeywell Galaxy Installation manual.

For further information on both the Galaxy installation and Remote Service Suite upload/download connection please refer to the IRIS Honeywell Galaxy Installation Manual or IRIS Remote Service App Client User Guide for Honeywell Galaxy range available from http://www.chironsc.com/downloads_security.html.

Connect the IRIS Touch dialler to the Galaxy Data bus as indicated in Section 7.3 "Connections", then power up the Galaxy control panel, if not already powered up.

The configuration menu on the Galaxy panel for the Ethernet card is found at location 56 (Communications) entry 4 (Ethernet), please enter the required information as indicated below.

You must enter Engineer Mode on the Galaxy to access these options.

56 = Communication

- 4 = Ethernet
  - 01= Module Config
    - 1 = IP Address - Program in the IP address for the IRIS e.g. 192.168.0.10
    - 2 = Site Name - Leave blank
    - 3 = Gateway IP - Enter the network gateway IP address e.g.192.168.0.1
    - 4 = Network Mask - Enter the subnet mask e.g. 255.255.255.240

Note: If you are using a DHCP address then leave all "Module Config" addresses blank

  - 02 = Alarm Reporting
    - 1 = Format - Set to SIA level 3
    - 2 = Primary IP
      - 1 = IP Address - Set this to the IP address of the monitoring centre e.g. 80.176.196.135

Note: Secondary IP address not required as the backup IP address will be download by the IRIS Secure Apps system to the dialler.

    - 4 = Account No. - Enter in the account number allocated by the monitoring centre.
  - 03 = Remote Access
    - 1 = Access Period - Set to 4 'Any Time'
    - 2 = Mode - Set to 'Direct Access' if making calls into site from Honeywell Remote Service Suite (RSS) for remote access directly or via the IRIS Remote Service App client.
    - Set to 'MGR Authorise' if making the remote access calls out from site to the Honeywell RSS, and then set the 'call IP1' IP address to the IP address for the Honeywell RSS communication server e.g. 80.176.196.135

Note: The IRIS Touch does not support the Honeywell Encryption as uses its own encryption so please ensure the following 2 options are turned off.

  - 9 = Encrypt
    - 1 = Alarm Report - Set to Off
    - 2 = Remote Access - Set to Off

After you have entered in the relevant information exit Engineer Mode and the panel should now detect 2 new RS485 modules (Comms Mod 4 & Keypad 15).

If the new modules are not detected then you may need to power off the Galaxy panel, check the dialler connections, and power back on.

Now go back into Engineer Mode and select the menu option sequence 56.04.05 'ENGINEER TEST' and send the test alarm. Check to see if this test alarm has been received by the monitoring centre (ARC).

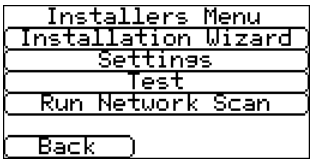
Note: If you are required to default the IRIS Touch dialler and start again you can do this by setting the primary IP address within the Galaxy menu 56.04.02.02 to an IP address of 127.0.0.1.

You can now perform the alarm signals commissioning and sign off required by the monitoring centre (ARC).

7.10. Testing

Once all configurations are complete, perform a full commissioning test with the monitoring centre. This will normally involve testing normal alarm transmissions over all communication paths from the alarm panel to the monitoring centre, and verifying that these are successfully received.

8. Main Menu



The IRIS Touch dialler has a number of options under the main menu and below we will go through each section explaining their functions and uses.

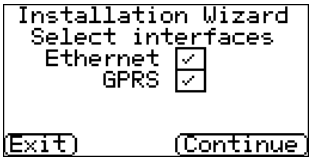
8.1. Installation Wizard

The Installation wizard guides you through the set up process for the IRIS Touch dialler and if there is a problem you will be told what it is and will not be allowed to continue until it is solved.

Note: During the Installation Wizard process you may find that some configurations are already setup, when the panel is using an integrated serial / RS485 connection. These configurations would have been downloaded from the alarm panel setup and if these are incorrect you would need to correct them first in the alarm panel.

Select the Installation Wizard and follow the on screen prompts.

Select interfaces

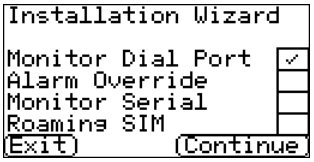


The first options within the Installation wizard are the network paths settings.

The IRIS Touch dialler has Ethernet and GPRS/3G options for single or dual communications.

Select the paths required and then click ‘Continue’.

Additional options



The next screen will give you a number of options to enable or disable. Please look at the reference below for more details:

Monitor Dial Port

Sets the IRIS Touch unit to monitor the dial port using the 18K resistor (as supplied in box) being fitted across the A & B terminal of the 2-wire analogue interface (telecoms module), and reports any status change back to the monitoring centre (ARC).

This resistor enables the dialler to detect cable faults and/or tampers and must be fitted at the alarm panel end of the cable to function correctly, the monitoring centre will also need to enable the dial port monitoring from the IRIS Secure Apps software to receive alarm notifications on this status.

Alarm Override

Allows the IRIS dialler to override / replace the phone number and account number used by the alarm panel dialler with the IP address of the monitoring centre and account number entered during configuration. This can be used for dial port or serial / RS485 connection to alarm panels where you may not have access or are unable to change the account / phone number in the alarm panel. This can be useful when converting some old alarm panel sites to work with the IRIS Touch dialler solution.

Monitor Serial

Set the IRIS dialler to monitor the serial port for activity and report any status change back to the monitoring centre (ARC), the monitoring centre will also need to enable the serial port monitoring from the IRIS Secure Apps software to receive alarm notifications on this status.

Roaming SIM

This option enables an enhanced roaming feature when used with a Roaming SIM. Standard Roaming SIMs will always attach to the preferred provider even if this has the weakest signal.
Enabling this option forces the GPRS/3G attachment to attach to the strongest signal base station. This allows the IRIS Touch dialler to be even more resilient with the GPRS/3G network.

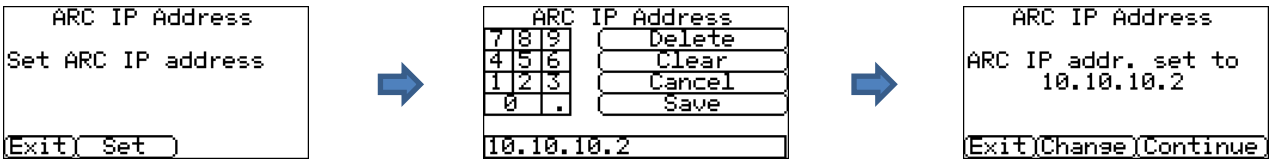
Account Name/Number

Now you are asked to enter the account (name / number) reference allocated by the monitoring centre which can be alphanumerical and up to 32 characters long, but normally you would expect a 4 or 6 digit numerical account number.

Press the 'Set' button and enter in the account name/number and then click the 'Save' button. Now confirm that the account is entered correctly and press 'Continue'.

ARC IP Address

Next you will be asked to enter in the ARC (Alarm Receiving Centre) IP address for the monitoring centre. This can be obtained from the monitoring centre and would normally be the external IP address for their IRIS Secure Apps system.



Press the 'Set' button and enter in the ARC IP address and then click the 'Save' button. Now confirm that the IP address is entered correctly and press 'Continue'.

Note: Only the primary/main ARC IP address needs be entered on the dialler as all backup or alternative IP addresses, for the ARC are downloaded to the IRIS Touch dialler on the first polling communications.

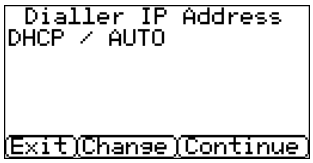
Ethernet (IRIS Touch 220NG or 240NG)

Checking Ethernet

The IRIS Touch dialler will now confirm if an Ethernet connection has been made to another piece of Ethernet equipment like a router or switch, if no connection is being seen this will display as 'Ethernet Disconnected' and the cable between the 2 pieces of equipment will need to be checked.

If the connection is good you will see 'Ethernet Connected' and can press 'Continue'.

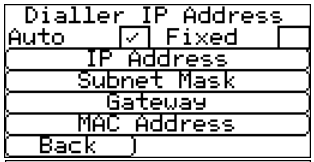
Dialler IP Address



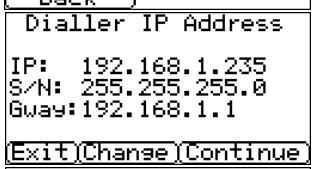
Now you are asked to setup the Dialler IP address for the network to which you are connecting the IRIS Touch dialler.

By default the IRIS Touch dialler is set for DHCP (Dynamic Host Configuration Protocol) which means that the network will allocate an IP address and other related settings gateway and subnet. If you are using a DHCP network connection then press 'Continue'.

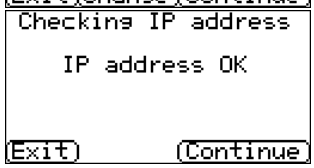
If the customer has requested that a fixed IP address is assigned then press 'Change'.



You will need to tick the fixed box at the top right and then enter the IP address, subnet mask and gateway information for the customer network.



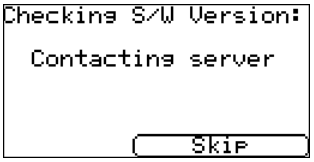
Once entered press 'back' and confirm the information has been entered correctly then press 'Continue'.



The IRIS Touch dialler will then perform a quick check on the validity of the IP address and confirm if this is ok. If not then please check the IP information entered.

Checking Software Version

Note: If using an IRIS Touch 400NG or 440NG with GPRS/3G and no Ethernet selected then this check will be done after the GPRS/3G settings.



The IRIS Touch dialler will now check with Chiron's global reflash server to see if a new version is available. If it is you will be presented with the option to 'Reflash now'.

The Reflasher option has a separate password to the Installation password and if this is the default '111111' you will be requested to change this password as required for EN50136-2.

Note: If there is a newer version available we recommend reflashing the IRIS Touch dialler to the latest version before completing the installation.

The IRIS Touch dialler will now perform various tests depending on which communication paths have been selected.

Ethernet Tests

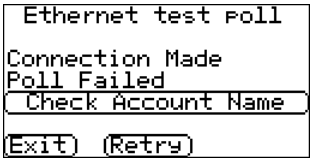
Next the dialler will send a test poll and alarm message to the monitoring centre to check the Ethernet connection.

Please ensure that both of these are successful and if not the dialler will indicate the possible issues and the configuration to check as shown below:

Note: The normal sequence of sending test alarms from the alarm panel must still be carried out.

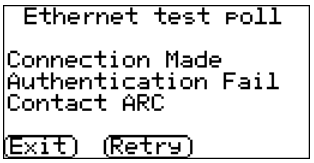
This indicates that the poll call did not reach the IRIS Secure Apps system and could be caused by one of the following:

- Check that the ARC IP Address entered is correct for the monitor centre.
- Check the LAN IP address setup for the IRIS Touch dialler, and confirm with the customer's IT department that you have the correct addresses for their network.
- Ensure that the alarm and polling port is not being blocked outbound by the customer's firewall. The required ports are 53165 TCP.



This indicates that the test poll call has reached the IRIS Secure Apps system but the account number is not valid.

- Check that the account number is programmed correctly.
- Check with the monitoring centre that the account in IRIS Secure Apps is setup.



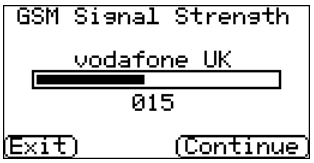
This indicates that the test poll call has reached the IRIS Secure Apps system but the security keys do not match.

The security key is a feature designed to prevent substitution attacks against both dialler and monitoring centre. When enabled, a randomly generated 32 byte key is transmitted to the dialler. This key must be used for all future polling authentication. Both the dialler and the Polling Engine authenticate each other, thus ensuring that a replacement dialler cannot be used to fool a Polling Engine into thinking its status is unaffected during malicious tampering; it also ensures that the dialler will be aware if its IP traffic has been maliciously redirected to a different IRIS Polling Engine.

- If the installer has recently replace or defaulted the IRIS Touch dialler then the IRIS Secure Apps operator will need to re-load the security key into the IRIS Touch dialler using the Allocator App.

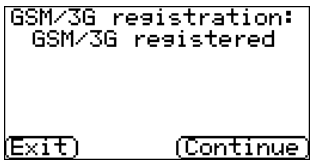
After checking each of the configuration options the IRIS Touch dialler will then reattempt to test the connection.

GPRS/3G (IRIS Touch 200NG or 240NG)

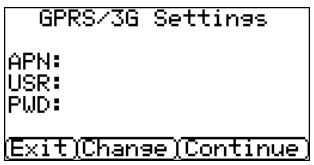


If you selected connection via GPRS/3G, the dialler will display the current operator / signal strength for the base station to which it is currently attached.

Note: You will require a signal strength of 10 CSQ or higher for a reliable connection. Click Continue.



Next the unit will check if it has GSM/3G registration and if it does it will report GSM/3G registerted. If this screen shows GSM/3G not registered then please check the SIM card is inserted correctly and contact the SIM provider to confirm it is enabled.



All GPRS/3G networks require the Access Point Name (APN) to be set. A few also require User Name (USR) and Password (PWD).

Now enter in the information you have from the SIM provider for this SIM card by clicking ‘Change’.

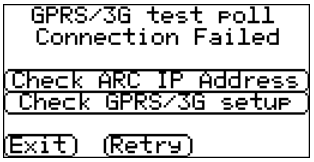
This will result in the following menu which allows you to enter in the settings for APN, User Name, Password and Pin (Scroll down) with which you may have been supplied.

Once you have confirmed that the information entered in is correct, click ‘Continue’.

The IRIS Touch dialler will make a test poll and test alarm transmission over GPRS/3G.

Note: The normal sequence of sending test alarms from the alarm panel must still be carried out.

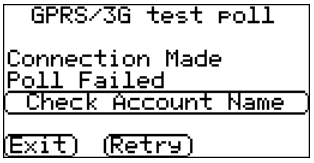
Please ensure that both of these transmissions are successful. If not successful the dialler will indicate the possible issues and the configuration to check as shown below:



This indicates that the poll call did not reach the IRIS Secure Apps system and could be caused by one of the following:

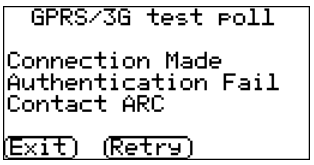
- Check ARC IP Address entered is correct for the monitor centre.

  Note: if using Ethernet on a VPN for example then the ARC IP would be for this connection and not the correct one for GPRS/3G. In this case please have the ARC operator check the Allocator setup for this account and try a Reload Parameters.
- Check GPRS/3G settings are correct for APN, User name, Password and Pin.
- Ensure SIM card is setup for GPRS/3G Machine to Machine data.



This indicates that the test poll call has reached the IRIS Secure Apps system but the account number is not valid.

- Check that the account number is programmed correctly.
- Check with the monitoring centre that the account in IRIS Secure Apps is setup.



This indicates that the test poll call has reached the IRIS Secure Apps system but the security keys do not match.

- If the installer has recently replace or defaulted the IRIS Touch dialler then the IRIS Secure Apps operator will need to re-load the security key into the IRIS Touch dialler using the Allocator App.

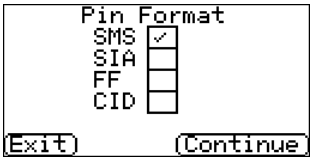
After checking each of the configuration options the IRIS Touch dialler will then reattempt to test the connection.

Pin Alarms

Now you have the option to use pin alarms which are the IRIS Touch pin inputs which can be used for SMS messaging or alarm signalling.

Select 'Yes' if you want to use the pin alarms or 'no' to continue.

Pin Format



You will now be asked to select which pin alarm format you wish to use.

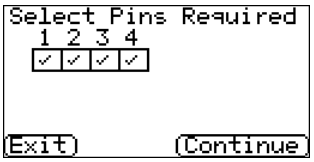
Note: SMS only available on IRIS Touch 400NG & 440NG diallers.

Select the format you wish to use and press 'Continue'.

A warning will then be given to advise that all current pin input settings will be lost, click "Continue" and then click "Continue" again.

For more information on each format and additional configurations for the pin alarms please go to the Section 8.2 "Settings – Pin Inputs".

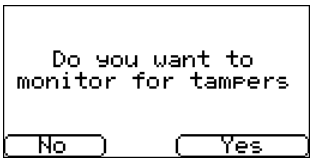
Pins Required



You will now be asked to select the pins you wish to enable and use if you have selected SIA, FF or CID for the alarm format.

Unselect pins you wish to disable from sending alarms and leave ticked only the pins / you want to use for alarm transmission, and then click 'Continue'.

Monitor for tampers



You will now be asked if you want to monitor for tamper on the pin alarm inputs, which is done using the sense resistors as detailed in Section 7.6 "Pin Inputs".

Select 'Yes' or 'No' depending if you want to use this function.

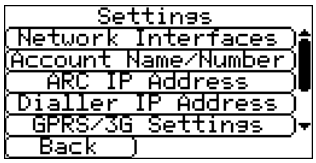
Setup Complete

The Initial setup is now complete. Click 'Finish' to exit the Installation Wizard and return back to the main menu.

For advanced settings select the 'Settings' menu.

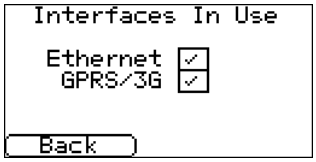
Once you have completed the Installation Wizard and setup any additional panel interface configuration via the settings menu you will need to check / configure the panel for the connection method being used if not already configured.

8.2. Settings



The **Settings** option is used to configure additional settings required for installation or additional options that may be added at a later date. Below is a detailed description of all of these options.

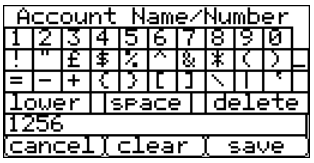
Network Interfaces



This section allows the user to select the communication paths to be used for polling / alarms on a multipath IRIS Touch dialler. There are up to 2 options as detailed below, depending on which version of IRIS Touch dialler:

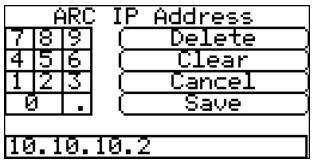
- Ethernet
- GPRS/3G (Machine to machine data 'M2M')

Account Name/Number



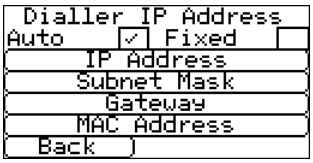
Set the account name/number for the IRIS Touch unit on site, as allocated by the monitoring centre.

ARC IP Address



Set up the external IP address for the monitoring centre receiver (polling engine).

Note: Only the primary/main ARC IP address needs be entered on the dialler as all backup or alternative IP addresses, for the ARC are downloaded to the IRIS Touch dialler on the first polling communications.



Dialler IP Address (IRIS Touch 220NG or 240NG)

Allows the user to setup the IP address of the dialler to either automatic (DHCP) or a fixed IP address. The settings below will either show the IP address received (DHCP mode) or, if fixed, allow the user to set the IP address, subnet and gateway:

- IP Address
- Subnet Mask
- Gateway
- Mac Address (view only)

GPRS/3G Settings (IRIS Touch 200NG or 240NG)

This section allows the user to enter or view the GPRS/3G settings.

Signal Strength

This option shows the provider and signal strength for the base station to which the dialler is connected.

Run Network Scan

Performs a network scan for all providers in the local area, and gives a chart of the best 3 base stations per provider.

To perform this the dialler should be powered down and the SIM card removed.

For the chosen GPRS/3G SIM provider CSQ values with a minimum of 10 (ideally 12) are required for at least 2 of the 3 base stations for reliability.

APN

GPRS/3G Access Point Name for the SIM card used.

User Name

If none required then leave blank otherwise set the GPRS/3G user name for the SIM card.

Password

If none required then leave blank otherwise set the GPRS/3G password for the SIM card.

SIM PIN

If the SIM card used has a PIN number set please enter here, normally this is disabled/blank.

Call Barring

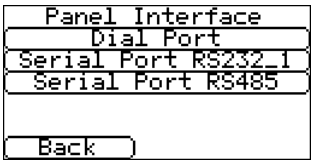
Incoming calls can be rejected to helps prevent any possibility of blocking the GSM/GPRS/3G communication paths.

Roaming SIM

This option enables an enhanced roaming feature when used with a roaming SIM.

A standard roaming SIM will always attach to the preferred provider even if this has the weakest signal.

Enabling this option forces the GPRS/3G attachment to connect to the strongest signal identified by the IRIS dialler. This allows the IRIS Touch dialler to be even more resilient with the GPRS/3G networks when using roaming SIM.



The IRIS Touch dialler has a number of panel interface options that allow connection too many different systems. Below are the settings available for each connection type and their function:

Dial Port

- **Monitor Cable**

  Sets the IRIS Touch dialler to monitor the dial port using the 18K resistor (as supplied in box) fitted across the A & B terminals of the 2-wire analogue interface (telecoms module). Reports any status changes back to the monitoring centre (ARC).

  This resistor enables the dialler to detect cable faults and/or tampers and must be fitted at the alarm panel end of the cable to function correctly. The monitoring centre will also need to enable the dial port monitoring from the IRIS Secure Apps software to receive alarm notifications on this status.

- **Report Poll Fail**

  Tick to enable the dialler to drop the line voltage on the dial port connection if unable to poll over any configured path to the monitoring centre. This allows the panel to detect and report locally on the keypad of the alarm panel that it has a line fault, so the site has local indication of a communication failure (for EN standards).

- **Enable Ringtone**

  This feature is to allow the user to enable or disable the IRIS unit simulating the PSTN ring tone to the dial port while the connection is being made. In most case this can be left as the default setting but if you are having issues with alarms or remote service app connection (Upload/download), then you can try turning this off.

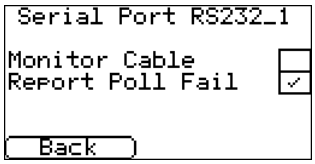
- **Ring**

  If the alarm panel is expecting European or UK ring cadence to detect an incoming call, you can change the IRIS Touch dialler to simulate either from Euro ‘ticked’ to UK ‘unticked’ (controls ring and ring tone cadence).

- **Only PSTN & GSM/3G**

  Forces alarm calls from the panel telecoms module to the IRIS dial port to go over the GSM/3G communication paths. This is done by using the number dialed by the panel telecoms module.

Serial Port RS232_1



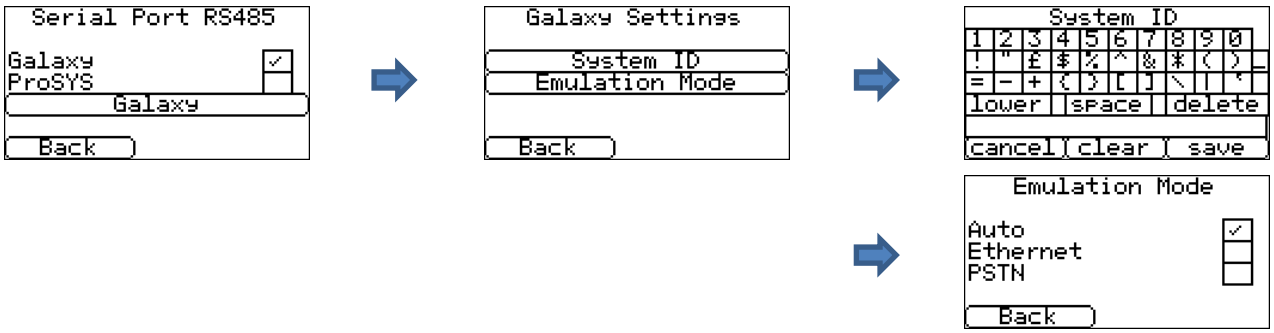
- **Monitor Cable**

  Set the IRIS dialler to monitor the serial port for activity and report any status change back to the monitoring centre (ARC). The monitoring centre will also need to enable the serial port monitoring from the IRIS Secure Apps software to receive alarm notifications on this status.

- **Report Poll Fail**

  Set the IRIS dialler to stop responding to the serial commands if polling has failed. This will then indicate the failure back to the alarm panel. This allows the site to have local indication of a communication failure (for EN standards).

Serial Port RS485



- **Galaxy**

  Set the RS485 bus for Honeywell Galaxy mode where the IRIS Touch will simulate one of 3 external modules in the following order (Ethernet, External Telecoms, and External RS232).

- **ProSYS**

  Set the RS485 bus for the Risco ProSYS bus to allow Upload/Download connections but not alarms, the panel alarm will need to be either on the dial port, or pin inputs.

- **Galaxy**

  The Galaxy Bus emulation mode has some additional option available for configuration and these are detailed below:

  - **System ID**

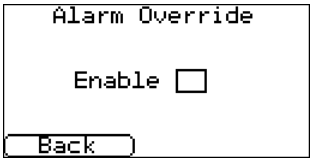
    Can override or enter a system ID independent from the panel.

  - **Emulation Mode**

    This option allows you to select the Honeywell Galaxy RS485 bus module that is emulated to the Galaxy control panel. By default this is set to AUTO (Automatic assigned) which will try the external Ethernet module first and if this is not seen then the external PSTN, and finally the external serial modules. This allows for backwards compatibility to older Galaxy panel software versions that do not support the Honeywell Ethernet module (Galaxy Classic below version 4.00).

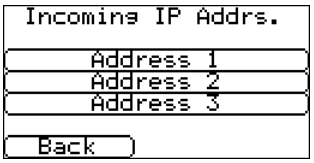
    You can also pre fix the module emulated to be either Ethernet or PSTN if required; this may be needed if for instance you already have a Honeywell Ethernet module fitted.

Alarm Override



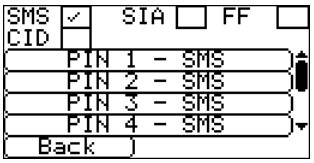
Allows the IRIS unit to override the alarm panels account number and dialled number with those set in the IRIS Touch dialler.

Incoming IP Addrs



As a security feature allows the user to define a list of 3 source IP addresses that are allowed to connect to the IRIS serial port. If all addresses are left blank then all calls are allowed.

Pin Inputs



Setup the Inputs (Pins) function between SMS messaging, SIA Alarm format, Fast format or Contact ID alarm format.

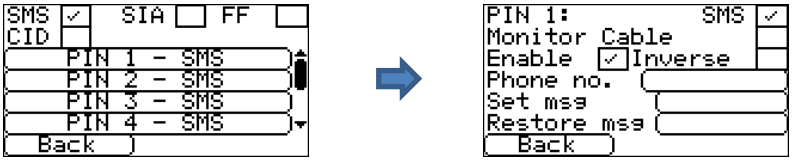
Note: You are able to select one alarm format for the Pins (SIA, FF or CID) and then setup individual pins to be SMS messaging if required.

When changing the pin format between one of the alarm formats (SIA, FF or CID) you will receive a warning message indicating that all pins will be setup for this alarm format and returned to the default allocation shown below, as pins cannot be setup to different alarm formats.

SMS (IRIS Touch 200NG or 240NG)

On input 'Set' (open circuit) and input 'Restore' (close circuit) the IRIS Touch will send the configured SMS message for the 'Set' or 'Restore' text, to the configured phone number.

Selecting SMS for the input format will display the following options to configure for each pin as shown.



Monitor Cable

The option to monitor the input for tamper will also be given. See Section 7.6 "Pin Inputs".

Enable

Enable/disable each pin input with the 'Enable' tick box.

Inverse

The function of the inputs 'Set' and 'Restore' can also be inverted to be the opposite way round by ticking the 'Inverse' tick box. This will mean that the 'Set' is now the closed circuit and the 'Restore' is open circuit.

Phone no.

Phone number used to send the SMS messages.

Set msg / Restore msg

Setup the 'Set' and 'Restore' messages to be sent to the entered phone number. The maximum length for the text message is 24 characters.

SIA

Selecting SIA for the Inputs means that the inputs will send specific SIA alarm protocol messages on the set event and restore for that input, the options available as shown.

SMS

One input can be setup to be SMS by ticking the 'Set as SMS' and this will allow setup of the SMS option as shown above.

Monitor Cable

You also have the option to monitor the input for tamper which is detailed in Section 7.6 "Pin Inputs".

Enable

Enable/disable each pin input with the 'Enable' tick box.

Inverse Polarity

The function of the inputs 'Set event' and 'Restore event' can be inverted to be the opposite way round by ticking the 'Inverse' tick box. This will mean that the 'Set event' is now the closed circuit and the 'Restore event' is open circuit.

Set msg / Restore msg

Setup the 'Set / Restore' message sent on the relevant event using the correct format as defined in SIA Format protocol SIA DC-03-1990.01(R2003.10). At default this is pre-set to a specific SIA code and a zone number (see table below). This can be modified for any event code and a text description added for each event which will be sent with the SIA alarm code as with SIA level 3 alarm protocols. These can be no longer than 15 characters in total.

To add a text description to the Set / Restore msg use the following format applying ^ before and after to indicate the text description:

Set msg SIA code	Set msg text description	Entry into the Set msg via the Touch screen
NFA01	FIRE	NFA01^FIRE^

Default SIA Set/Restore event codes for Pin inputs:

Pin Number	Set message SIA code	Restore message SIA code	SIA event Description
1	NFA01	NFR01	Fire alarm zone 1
2	NPA02	NPR02	Panic alarm zone 2
3	NBA03	NBR03	Burglary alarm zone 3
4	NOP04	NCL04	Open/Close zone 4

FF (Fast Format)

Selecting FF for the Inputs means that the inputs will send a specific Scancom fast format alarm protocol messages on the event and restore for that input, the options available are shown below:

SMS

One input can be setup to be SMS by ticking the 'Set as SMS' and this will allow setup of the SMS option as shown above.

Monitor Cable

There is also the option to monitor the input for tamper which is detailed in Section 7.6 "Pin Inputs".

Enable

Enable/disable each pin input with the 'Enable' tick box.

Alarm

Sets the input to be an alarm triggered input which will send the following states of the channel according to the following:

Signal	Event Type	Description
5	Not in alarm	The alarm triggering input is at its quiescent state.
1	New alarm	The alarm triggering input is at its active state and it has not previously been reported.
6	In alarm	The alarm triggering input is at its active state and it has previously been reported.
3	New restore	The alarm triggering input has just returned to its quiescent state from the alarm state.

O/C (open / close)

Sets the input to be an open/close input which will send the following states of the channel according to the following:

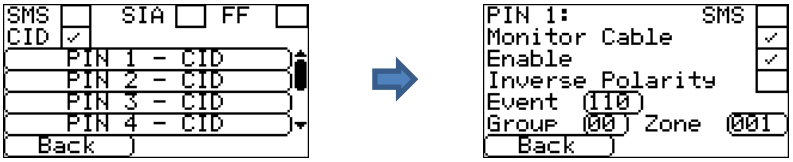
Signal	Event Type	Description
2	New opening	The alarm triggering input is at its alarm state, the intruder alarm system has been unset.
4	New closing	The alarm triggering input is at its quiescent state, the intruder alarm system has been set.
5	Premises closed	The alarm triggering input is at its quiescent state and it has previously been reported.
6	Premises open	The alarm triggering input is at its alarm state and it has previously been reported.

Inverse Polarity

The function of the inputs 'Event' and 'Restore' can be inverted to be the opposite way round by ticking the 'Inverse' tick box. This will mean that the 'Event' is now the closed circuit and the 'Restore' event is open circuit.

CID (Contact ID)

Selecting CID for the inputs means that the inputs will send a specific Ademco® alarm protocol messages which will include an event code, zone and group number, on the event and restore for that input. The following options available are shown below:



SMS

One input can be setup to be SMS by ticking the 'Set as SMS' and this will allow setup of the SMS option as shown above.

Monitor Cable

There is also the option to monitor the input for tamper which is detailed in Section 7.6 "Pin Inputs".

Enable

Enable/disable each pin input with the 'Enable' tick box.

Inverse Polarity

The function of the inputs 'Event' and 'Restore' can be inverted to be the opposite way round by ticking the 'Inverse' tick box. This will mean that the 'Event' is now the closed circuit and the 'Restore' event is open circuit.

Event

Enter the Event code (3 digits 0-9) for this input for example: 110 = Fire.

To determine which event code is to be used please refer to the Digital Communication Standard -

Ademco® Contact ID Protocol - for Alarm System Communications SIA DC-05-1999.09

Group

Group or Partition number (2 digits 0-9).

Use 00 to indicate that no specific group or partition information applies.

Zone

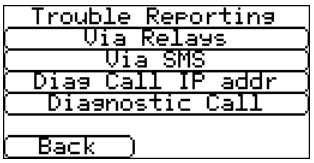
Zone number (Event reports) or User # (Open / Close reports) (3 digits 0-9).

Use 000 to indicate that no specific zone or user information applies.

Default CID Set/Restore event codes for Pin inputs:

Pin Number	Contact ID event code	Group number	Zone number	Contact ID event description
1	110	00	001	Fire alarm zone 1
2	120	00	002	Panic alarm zone 2
3	130	00	003	Burglary alarm zone 3
4	400	00	004	Open/Close zone 4

Trouble Reporting

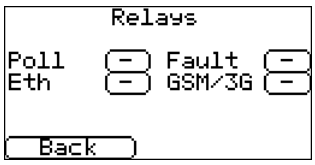


Trouble reporting allows setup of the reporting of communication faults via relays or SMS and making diagnostic calls over an IP communication path (Ethernet or 3G/GPRS).

The remote diagnostic call allows an outbound TCP/IP call using TCP/IP port number 51292 to a senior technician with a PC/laptop running the IRIS Toolbox software. This will then allow them to check setup and run diagnostics remotely to investigate any issues.

Below is a breakdown of these individual setup options:

Via Relays

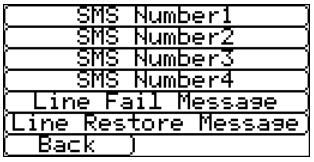


It is possible to enable or disable the IRIS Touch dialler toggling the state of the relays to indicate communication path failures. This is intended to signal failures back to the panel inputs so the site has local indication of a communication failure (for EN standards). The IRIS Touch dialler allows the selection of which relay is to be used for the poll fail indication or communication path fail.

If you click on the box you can toggle through which relay you wish to assign for this fault report and note the same relay can be used for multiple path fault indication.

The option for 'Fault' reporting allows reporting of system fault indications via the selected relay, for a list of these faults please check the Section 9 "Trouble Reporting".

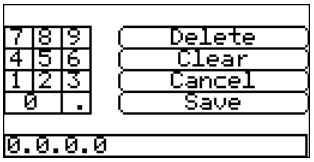
Via SMS



The IRIS Touch dialler can send SMS messages to indicate communication / line faults via the GSM/3G network.

There are 4 SMS phone number that can be set up for sending SMS messages, for line fail/restore reporting.

Diag Call IP addr



This menu allows the IP address of the PC/laptop running the IRIS Toolbox software to be entered in order to make an outbound TCP/IP diagnostics call for remote diagnostics.

Diagnostic Call

This option allows you to make a diagnostics call back to the IP address entered above for remote diagnostics to the IRIS Toolbox software.

On first entry this will show the one time password for this remote connection which may need to be passed on to the operator of the IRIS Toolbox software.

Press the 'Diagnostic Call' button once the password has been passed onto the operator and they are ready to receive the call.

Relay SMS activation (IRIS Touch 200NG or 240NG)

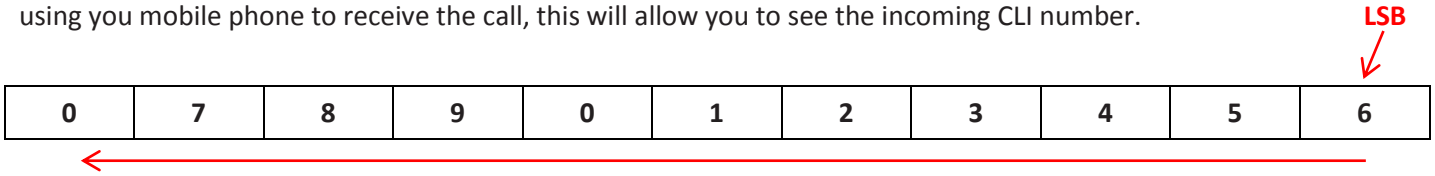
The IRIS Touch dialler allows each relay to be activated or deactivated by a predefined SMS message from a mobile phone.

Phone no

Sets which calling device (mobile phone) is allowed to control the relay with the relevant SMS message. This is done by using the Calling line number (CLI) on the SMS and comparing this with the number entered.

The dialler will start the comparison from the least significant digit and then work backwards as shown below:

For the example we will use the phone number 07890123456, please confirm what CLI number is being received by using you mobile phone to receive the call, this will allow you to see the incoming CLI number.



Starting from the LSB '6' you can work backwards to compare the CLI number so for example you can enter a number of 56. This will allow all phone numbers with a CLI ending in 56.

Leaving the source number blank will allow any mobile number to set or restore the relay as long as the SMS text matches.

Activation msg

Sets the SMS text message required to open the relay, note this is case sensitive.

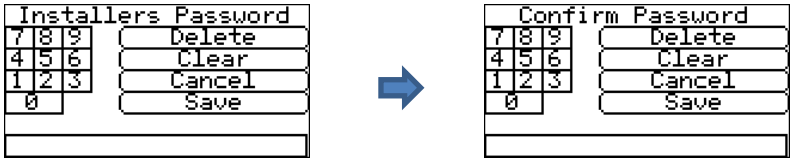
Deactivation msg

Sets the SMS text message required to close the relay, note this is case sensitive.

Language

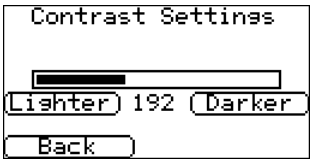
The IRIS Touch dialler supports a number of languages that you can select here.

Installers Password



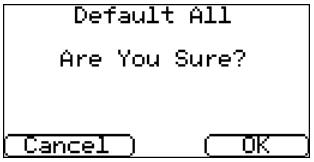
When the user first accesses the Installer menu, the Installers password is required, which is defaulted to '111111'. During installation you will be required to change the password as required for EN50136-2.
This password can be changed again if required with this setting and you will be asked to enter and then confirm the new password.

Contrast



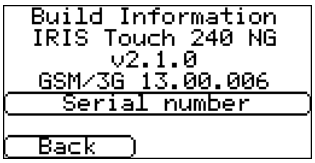
This setting allows you to alter the contrast on the Touch screen.

Default All



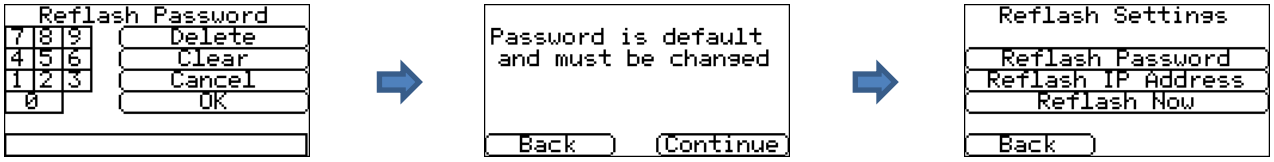
Completely resets the IRIS Touch dialler to manufacturing defaults.

Build Information



IRIS Touch software version, GPRS/3G software version and dialler serial number are displayed.

Reflash



The option will be given to reflash the unit to the latest version available from the Chiron reflash server.

On first entry to the reflash option, which could be during installation or maintenance, the password will need to be changed as required for EN50136-2.

Otherwise you will be asked to enter the reflash password that has been configured for this unit.

A reflash to update the IRIS Touch dialler to the latest software version can be initiated and the options are shown below:

Reflash Password

This password can be changed again if required with this setting.

Reflash IP Address

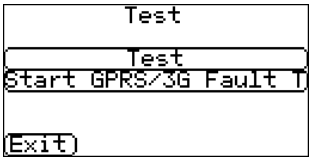
The default reflash IP address is the Chiron reflash server setup on an IP address 195.59.117.164 which is available 24/7 for connections, and kept up to date with the latest software available.

There are cases where a customer will only open their network to communicate back to the monitoring centre (network/IP address), and in some cases the monitoring centre has their own reflash server installed. This option allows the sending of a reflash request to an alternate IP address.

Reflash Now

Initiate the reflash to the reflash IP address and will bring up a status window to indicate progress.

8.3. Test



The test menu allows checking of all current enabled communication paths, and will test both polling and alarms. There are two options here and these are detailed below:

Test

This will start the polling and alarm tests over the enabled communication path or paths.

Once the tests are complete the following possible outcomes are available as shown in the table on the next page.

Start GPRS/3G Fault Test (IRIS Touch 200NG or 240NG)

This option enables an engineer to simulate a GPRS/3G fault so the monitoring centre can check that the report is presented properly to the operators.

Note: This mode stays operational for 1 minute and is then automatically switched off, to prevent a situation where the installer forgets to switch it off thereby disabling GPRS. It can be switched off earlier if required.

Testing	Results and explanations
Checking Ethernet	**Connected**: Confirms the dialler is connected to the Ethernet network. **Not Connected**: The dialler is currently not connected to the Ethernet network; check the Ethernet cable and cabling all the way through to the other end (Router / Switch).
Checking IP address	The IRIS Touch dialler will check the dialler IP address is valid as set either by DHCP or manually.
Ethernet test Poll	**Successful**: Dialler successfully polled to the monitoring centre (ARC) IRIS Secure Apps system over the Ethernet network. **Polling disabled**: Configured not to poll over the Ethernet network; check ARC IP address and account number are still entered. **Connection failed**: Failed to connect to ARC over the Ethernet network; check the ARC IP address is correct, confirm Ethernet router external WAN connection and firewall setup. **Connection made, poll fail**: Connected to the ARC IRIS Secure Apps but was rejected; check correct account number has been setup at ARC IRIS Secure Apps and that correct account number is entered in dialler. **Connection made, authentication failed**: Connected to the ARC IRIS Secure Apps but was rejected due to invalid security key; check correct account number entered in dialler. If a replacement dialler was installed the ARC will need to perform a 'Reload Parameters' on the IRIS Secure Apps web interface.
Ethernet test alarm	**Successful**: Ethernet SIA level 3 test alarm reported successfully to ARC. **Connection failed**: Failed to send alarm to ARC over Ethernet network; check with ARC.
GSM/3G registration	**Registered**: Dialler is connected to the GSM/3G network. **Not registered**: The dialler is not registered to the GSM/3G network; check SIM card is enabled and inserted correctly into the SIM card holder, also check antenna and signal strength are connected and above minimum signal strength.
Signal strength	Indicates current signal strength, which is recommended to be above 10 for reliable communications; if below the minimum required either move the dialler or antenna to gain better coverage or fit an external high gain GPRS/3G antenna.
GPRS/3G test poll	**Successful**: Dialler successfully polled to the monitoring centre (ARC) IRIS Secure Apps system over the GPRS/3G network. **Polling disabled**: Configured not to poll over GPRS/3G network; check ARC IP address and account number are still entered. **Connection failed**: Failed to connect to ARC over GPRS/3G network; check the ARC IP address is correct, and confirm SIM card is enabled for GPRS/3G machine to machine data (M2M) with the SIM card provider. **Connection made, poll fail**: Connected to the ARC IRIS Secure Apps but was rejected; check correct account number has been setup at ARC IRIS Secure Apps and that correct account number entered in dialler. **Connection made, authentication failed**: Connected to the ARC IRIS Secure Apps but was rejected due to invalid security key; check correct account number entered in dialler, and if a replacement dialler was installed the ARC will need to perform a 'Reload Parameters' on the IRIS Secure Apps web interface.
GPRS/3G test alarm	**Successful**: GPRS/3G SIA level 3 test alarm reported successfully to ARC. **Connection failed**: Failed to send alarm to ARC over GPRS/3G network; check with ARC.

8.4. Run Network Scan

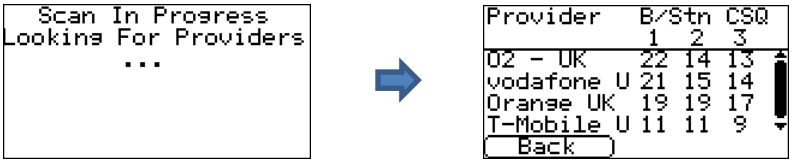
IRIS Touch 400NG or 440NG with GPRS/3G connection:

The GPRS/3G network scan function allows you to get overall feedback of signal strength from all providers in the area. This should be performed on installation as detailed in Section 7 “Installing the IRIS Touch Dialler” and also after installation, for example during maintenance, as location signal stregnth can change e.g. new building in the area or cosmetic changes in the current location (storage racking etc).

The scan must be carried out **without** the SIM card fitted.

The dialler listens for every base station in range, requests operator name and records the signal strength.

This will take a few minutes to complete.

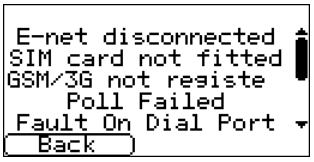


For a reliable GPRS/3G connection it is recommended that for the chosen network (SIM card) used there should be at least two base stations with signal strength (CSQ) of 10 or more for reliability.

If the signal strength is below or close to minimum then try to reposition the antenna or use an external high gain antenna (if necessary), and rerun the network scan.

Once you have the required GPRS/3G signal strength power down the dialler and insert the SIM card into the SIM card holder, then power the dialler back up.

9. Trouble report



When the SYS LED is flashing yellow the dialler has some trouble events being reported. These can be viewed in more detail by accessing the welcome screen, then 'Status – Trouble' and finally 'View Trouble Report' option.

The Trouble Report Menu indicates what the current system troubles are and below is an explanation of all possible events.

Trouble Reported	Explanation
E-net disconnected	The dialler is currently not connected to the Ethernet network; check the Ethernet cable and cabling all the way through to the other end (Router / Switch).
E-net polling fail	Unable to poll via the Ethernet network to the monitoring centre's (ARC) IRIS Secure Apps system; check ARC IP address, confirm Ethernet router external WAN connection and firewall setup.
GSM/3G not registered	Not able to register to the GSM/3G network; normally means the SIM card has been disabled, check with SIM provider.
GPRS/3G Polling fail	Unable to Poll via the GPRS/3G network to the monitoring centre's (ARC) IRIS Secure Apps system; check ARC IP address, SIM card is enabled for GPRS/3G machine to machine data (M2M).
SIM Card not fitted	SIM card not being seen in the IRIS unit; check SIM fitted and that connection is ok.
SIM PIN required	SIM card has been setup for a PIN number and no SIM PIN entered in configuration; Confirm the correct SIM PIN with the SIM provider and enter.
SIM PIN error	Current SIM PIN entered in the configuration is invalid; confirm correct SIM PIN with SIM provider and confirm entered correctly.
Poll Failed	The dialler is unable to poll over any path; check correct ARC IP address entered, and communication paths setup.
Fault On Dial Port	Dial port configured to monitor dial port and sense resistor not being detected (18K). Check cable/resistor connections.
Pin Fault on pin**	Indicates that the dialler has been set to monitor for tampers and is in an open or short circuit tamper condition. Check cable/resistors connections.
Serial port fault	The dialler is setup to monitor serial but is seeing no activity on the serial connection; check setup of the dialler / panel and physical connection.
Fail to communicate	A dialler input has been triggered and this event has failed to be communicated to the ARC. Check all communication paths are working and configuration is correct; also check with the ARC that they have no known issues with received alarms (E.G. IRIS Poll engine IP link down).
Eeprom	The dialler has a possible hardware issue and is unable to see the Eeprom. The Eeprom stores all local parameters for protection against power failure.

10. Maintenance

There is no requirement for any onsite maintenance on the IRIS Touch 2.

If engineers want to carry out a maintenance inspection please perform the following:

- Confirm the status of the IRIS Touch unit.
- Clear any faults on the dialler.
- Reflash IRIS Touch software to latest version.
- Test the configured communication paths (Ethernet / GPRS / 3G).
- Perform full test of alarms from the alarm panel and confirm these are received at the monitoring centre.

The IRIS Touch dialler will give a visual indication of the current system status via the SYS LED. If this is yellow constant the current setup of the dialler is reporting OK, yellow flashing means the dialler is reporting some trouble events.

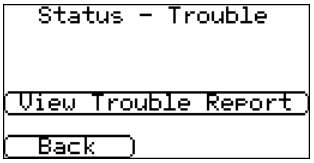
To further investigate any faults or to perform checks, the IRIS Touch dialler gives engineers the option via the touch screen, to see current faults, reflash to latest software and perform communication path checks.

Engineers will need to touch the screen to exit the screen saver mode and should now be presented with the welcome screen. Engineers will now see the option indicating status and the option to enter the installer menu. The engineer will now be able to perform the following checks:

10.1. Confirm Current Status

The IRIS Touch dialler will indicate “Status – ok” if the current dialler setup is all working correctly, and if the status is showing “Status – Trouble” the dialler has a trouble reported.

To view the reported trouble click on the “Status – Trouble” option then “View Trouble Report”.

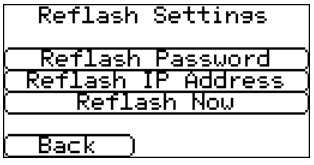


Engineers can now see the current system troubles that are being reported and then look to resolve these issues. For further information please refer to the Section 9 “Trouble Report”.

10.2. Check Software Version / Reflash

The engineer will need to go into the settings menu and then select the ‘Reflash’ option. On first entry to the reflash option which could be during installation or maintenance, the engineer will be required to change the password as required for EN50136-2 compliance. Please record the password on the installation documentation.

Enter the correct reflash password and you will then have the following options.



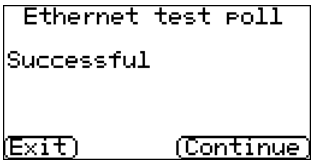
The Chiron Reflash server IP address will already be setup under the ‘Reflash IP Address’ but if using an alternative Reflash IP address then change the IP address.

Once you have the correct reflash IP address entered press the ‘Reflash Now’ to connect to the server and check if there is a later version, and if there is, it will start to reflash.

The reflash will take up to 15 minutes if via GPRS/3G and approximately 2 minutes with the Ethernet connection. Once completed the dialler will reboot and switch to the new software. All configurations are saved and there is no need to reconfigure the IRIS Touch.

Note: During the reflash process please do not remove power until dialler has completed and reset.

10.3. Communication Paths Checks



The engineers can test the communication paths for both polling and alarm communications using the ‘Test’ option in the Main installer menu, this will test all configured communication paths.

Please refer to Section 8.3 “Test” for more details.

10.4. Test Alarm Panel Alarms and Communication to ARC

Depending on the monitoring centre (ARC) engineers will now be required to perform alarm test and possibly other tests to the ARC. Before the engineer leaves site get confirmation from the ARC that all is working correctly.

11.Specifications

Transmission paths		200NG	220NG	240NG
Ethernet	Standard	–	UTP 10/100 Base T with auto-negotiation	
	Connection	–	RJ45 socket for CAT5 cabling	
	IP addressing	–	Dynamic (DHCP) or fixed	
	Connection fault detection	–	Loss of Ethernet synchronisation	
GPRS/3G (4G/CDMA optional on request)	Standard	Dual band GSM 900/1800 MHz Dual band UMTS 900/2100 MHz	–	Dual band GSM 900/1800 MHz Dual band UMTS 900/2100 MHz
	Connection	SMA socket for GPRS/3G antenna connection	–	SMA socket for GPRS/3G antenna connection
	Connection fault detection	Loss of registration with network	–	Loss of registration with network
IP				
TCP ports (outbound)		53165 (Alarms & Polling), 51292 (Diagnostic & Reflashing), 10001 (Upload/Download)		
Alarm transmission				
Interface to monitoring centre		IRIS Secure Apps or IRIS Management Suite via EN 50136-2 pass-through mode		
Dial capture interface to alarm panel		Two wire interface via the dial port terminal block		
Serial interface to alarm panel		RS485, TTL, RS232 **Note: RS232 cabling must not exceed 30 meters**		
PIN Inputs interface to alarm panel		Maximum input voltage range 0V to +24V		
		Input 'low' (alarm) threshold < 1V		
		Input 'high' (restore) threshold > 2V		
		Internal pull-up impedance 10K to 3.3V supply		
Alarm protocols		SIA (level 1 to 3) reference SIA DC-03-1990.01(R2003.10)		
		Contact ID reference SIA DC-05-1999.09		
		Fast format (Scancom)		
		Robofon (Dial capture only)		
Tamper detection reporting to monitoring centre		Dial capture interface, Serial interface, Pin inputs		
Fault reporting to monitoring centre		Transmission interface/path fault		
Relay outputs				
Maximum operating voltage		24V DC		
Maximum current rating		100mA DC		
Power supply				
Supply voltage		9V to 28V DC		
Typical current		124mA @ 12V DC	138mA @ 12V DC	140mA @ 12V DC
Maximum current		1A @ 12V DC		
Recommended external PSU		12V DC 1A 12 Watt **Note: For Radio & Telecoms Terminal Equipment Directive the power cable must be no longer than 3 meters in length**		
Environmental				
Operating temperature range		-10°C to 55°C		
Operating humidity range		95% max, non-condensing		
Weights and dimensions				
Physical dimensions		19 cm x 13 cm x 4 cm		
PCB weight		550 grams		
Fully packaged weight		750 grams		

Safety

Care should be taken when connecting telecommunications equipment to ensure only like interfaces are connected to avoid safety hazards.

SELV: SELV (Safety Extra-Low Voltage) is defined as a secondary circuit which is so designed and protected that under normal and single fault conditions the voltage between any two accessible parts does not exceed a safe value (42.4V peak or 60V dc maximum)

The interfaces on the IRIS Touch have the following safety classifications:

- Dial capture interface: SELV suitable for connection to the TNV interface of single line telecommunications equipment such as telephones, alarm panels, etc.
- Power Interface: SELV for connection to a DC supply
- Inputs: SELV for connection to alarm output pin.

Conformance

European Directives

The IRIS Touch complies with the following European Directives:

- 1999/5/EC (Radio & Telecoms Terminal Equipment Directive)
- 2006/95/EC (Low Voltage Directive)
- 2004/108/EC (Electromagnetic Compatibility Directive)

EN50131, EN50136 (VdS Certified)

The dialler is compliant with the requirements of European Standards:

EN50131-1: 2006 & EN50131-10: 2014
EN50136-1: 2012 & EN50136-2: 2013
Security Grade 3
ATS-SP6 over Ethernet, ATS-SP5 over GPRS/3G, ATS-DP4 (IRIS Touch 240NG)
Environmental Class II

The future of security, secured

IP by security professionals, for the professional security industry

Installation and Service Engineer Support Telephone: +44 871 977 1133
(Calls are charged at 10p a minute from a BT landline. Calls from mobiles or other providers may be higher)

Sales Enquiries: +41 435 080 870

Email: sales@chironsc.com
www.chironsc.com

CHIRON SECURITY COMMUNICATIONS AG
BAARERSTRASSE 19
6300 ZUG
SWITZERLAND