IRIS-4 Terminals

Technical Reference Manual

7/7/2026

Table of Contents

1 About this manual 8
1.1 Target group 8
1.2 Scope 8
2 About the IRIS-4 product range 9
3 Circuit board layouts 10
3.1 DS2220/IRIS-4 50 10
3.1.1 Sys LED Indications 10
3.2 IRIS-4 160 11
3.2.1 Sys LED indications 11
3.3 IRIS-4 2xx 12
3.3.1 Sys LED indications 12
3.4 IRIS-4 4xx 13
3.4.1 Sys LED indications 13
3.4.2 Expansion boards 13
3.5 IRIS-4 6xx 14
3.5.1 LED indications 14
4 Basic setup 15
4.1 Before you begin 15
4.1.1 ARC 15
4.1.2 Ethernet connection details 15
4.1.3 Cellular SIM card and Access Point Name 15
4.2 Recommended installation sequence 16
4.2.1 Installing the Extension boards on the 4xx 16
4.2.1.1 Expansion boards 17
4.2.2 Mount the terminal 17
4.2.2.1 Mounting the 50 (DS2220/IRIS-4 50) 17
4.2.2.2 Mounting the 160 17
4.2.2.3 Mounting the 2xx 18
4.2.2.4 Mounting the 4xx & 6xx 18
4.2.3 Position the antenna 18
4.2.4 Connect cables 18
4.2.4.1 Cables 18
4.2.4.2 Serial connections 18
4.2.4.3 Power Supply 19
4.2.5 Power up 20
4.2.5.1 Using the terminal touchscreen 20
4.2.5.2 Using the virtual touchscreen 20
4.2.6 Welcome menus 20
4.2.6.1 Language selection 20
4.2.6.2 Installer's password 20
5 Configuring the terminal 21
5.1 Accessing the Installation Wizard 21
5.2 Initial configuration settings 21
5.2.1 Select interfaces 21
5.2.2 Alarm Transmission Protocol 21
5.2.3 Account name/number 21
5.2.4 ARC IP address (Iris protocol only) 22
5.2.5 DC-09 settings menus (DC-09 protocol only) 22
5.2.6 Encryption 23
5.3 Communication configuration 23
5.3.1 Communication tests 24
5.3.1.1 Connection failed 24

5.3.1.2 Connection made, Poll failed 24
5.3.1.3 Authentication failed 24
5.3.2 Checking S/W version 24
5.3.3 Ethernet setup and test 25
5.3.3.1 Checking Ethernet connection 25
5.3.3.2 Dialler IP Address 25
5.3.3.3 Ethernet communications tests 25
5.3.4 Wi-Fi setup and test 26
5.3.4.1 Wi-Fi settings 26
5.3.4.2 Checking Wi-Fi connection 26
5.3.4.3 Wi-Fi communication tests 26
5.3.5 Cellular setup and test 26
5.3.5.1 Cellular registration 26
5.3.5.2 Cellular signal strength 27
5.3.5.3 Cellular settings 27
5.3.5.4 Cellular communication tests 28
5.3.6 PSTN Setup & test 28
5.3.6.1 PSTN connection test 28
5.4 Further configuration settings 28
5.4.1 Additional options 28
5.4.2 Dial port check 29
5.4.3 Battery backup 29
5.4.4 Pin alarms 29
5.4.4.1 PSTN: Alarm Setup 29
5.4.4.2 Pin format 29
5.4.4.3 Pins required 29
5.4.4.4 Monitor for tampers 30
5.4.5 Setup complete 30
5.5 Configuring the 160 using the Installer App: 30
6 Settings 31
6.1 Network interfaces 31
6.2 Alarm Tx protocol 31
6.2.1 ARC IP address (for Iris protocol) 31
6.2.2 DC-09 transmitter settings (for DC-09 protocol) 31
6.2.3 ATS category 31
6.2.4 DC-09 receiver 32
6.2.5 Encryption 32
6.2.6 Poll period and Reporting delay 32
6.2.7 Account prefix 33
6.2.8 Receiver number 33
6.2.9 Date format 33
6.3 Account name/number 33
6.4 Eth 1: For terminals with Ethernet capability 33
6.5 Eth 2: For terminals with dual Ethernet capability 33
6.5.1 Cellular Bridge 34
6.5.1.1 DHCPSRV or Fixed 34
6.5.1.2 Cell/Client IP 34
6.5.1.3 Subnet mask 34
6.5.1.4 Gateway 34
6.5.2 Cellular Routed 34
6.5.2.1 DHCPSRV or Fixed 34
6.5.2.2 Eth 2 IP/Gateway 34
6.5.2.3 Subnet mask 34
6.5.2.4 Cellular IP 35

6.5.2.5 Forwarded IP 35
6.5.3 Vanderbilt SPC 35
6.5.4 DC-09 35
6.6 Wi-Fi: For terminal with Wi-Fi capability 35
6.6.1 Network 35
6.6.2 Password 35
6.6.3 Wi-Fi network scan 35
6.6.4 Wi-Fi signal strength 35
6.6.5 IP address 35
6.7 Cellular Settings: For terminals with cellular capability 36
6.7.1 Signal strength 36
6.7.2 Run network scan 36
6.7.3 APN 36
6.7.4 Username 36
6.7.5 Password 36
6.7.6 SIM PIN 36
6.7.7 Call barring 36
6.7.8 SMS transport 36
6.7.9 Mode 37
6.8 Battery backup: 37
6.9 Panel interface 38
6.9.1 Dial port: 38
6.9.1.1 Monitor cable 38
6.9.1.2 Report polling fail 38
6.9.1.3 Enable Ringtone 39
6.9.1.4 Voice call alarm 39
6.9.1.5 Ring 39
6.9.1.6 Dial tone 39
6.9.1.7 PSTN Only 39
6.9.1.8 Telim conversion 39
6.9.2 COM 39
6.9.2.1 Monitor cable 39
6.9.2.2 Report poll fail 39
6.9.2.3 Emulation mode 39
6.9.2.4 Serial settings 39
6.9.3 RS232 (1) 40
6.9.3.1 Monitor cable 40
6.9.3.2 Report poll fail 40
6.9.3.3 Emulation mode 40
6.9.3.4 Serial settings 40
6.9.4 RS232 (2) 40
6.9.4.1 Monitor cable 40
6.9.4.2 Report polling fail 41
6.9.4.3 Emulation mode: For 4xx and 6xx 41
6.9.4.4 Serial settings 41
6.9.5 Serial port RS485 41
6.9.5.1 Galaxy 41
6.9.5.2 ProSYS 42
6.9.5.3 ESMI 42
6.9.6 Eth 2 42
6.10 Alarm override 42
6.11 Extra features 42
6.11.1 Normal 42
6.11.2 Set / unset 42
6.11.2.1 Set / unset pin 42
6.11.2.2 Exit delay 43

6.11.2.3 Entry Pin 43
6.11.2.4 Entry delay 43
6.11.2.5 Set status relay 43
6.11.2.6 Alarm status relay 43
6.11.3 ENS4-21 Fire 43
6.11.4 VdS 2463 Intruder 43
6.11.5 VdS 2463 Fire 43
6.11.6 ILKA mode + PSU 43
6.11.7 ILKA mode 43
6.11.8 Tamper detection 43
6.11.9 INCERT 2+/3 43
6.11.10 Test alarm 44
6.11.11 Add SIA Timestamp 44
6.11.12 Limotec ..... Error! Bookmark not defined.
6.12 Incoming TCP 44
6.13 Pin inputs 45
6.13.1 Common options 45
6.13.1.1 Monitor cable 45
6.13.1.2 Enable 45
6.13.1.3 Inverse polarity 45
6.13.2 Alarm format SMS 46
6.13.2.1 Phone number 46
6.13.2.2 Set msg and Restore msg 46
6.13.3 Alarm format SIA 46
6.13.3.1 Set msg and Restore msg 46
6.13.4 Alarm format FF 46
6.13.4.1 Alarm 46
6.13.4.2 O/C (open/close) 47
6.13.5 Alarm format CID 47
6.13.5.1 Event 47
6.13.5.2 Group 47
6.13.5.3 Zone 47
6.13.5.4 Default CID Set/Restore event codes 47
6.14 Relays 48
6.14.1 Relay input follower 48
6.14.2 Relay SMS activation 48
6.14.2.1 Phone number 48
6.14.2.2 Activation msg 48
6.14.2.3 Deactivation msg 48
6.14.3 Relay invert 49
6.15 Time 49
6.16 Trouble reporting 49
6.16.1 Via relays 49
6.16.2 Via SMS 50
6.16.3 Diagnostic call IP address 50
6.16.4 Diagnostic call 50
6.17 PSTN Settings 50
6.17.1 PSTN Alarm Setup 50
6.17.2 Audio 50
6.17.3 Tone Detect 50
6.18 Language 51
6.19 Installers password 51
6.20 Display 51
6.20.1 Touchscreen calibration 51
6.21 Default 52

6.21.1 For terminals with an AP or SW button (this is not part of Settings menu) 52
6.22 Build information....52
6.23 Reflash 52
6.23.1 Reflash Access Password 52
6.23.2 Reflash IP address 52
6.23.3 Reflash now 53
7 Installation for EN54-21:2006 compliance....54
7.1 Introduction....54
7.2 General description of the equipment....54
7.2.1 Technical specification....54
7.3 Installation, configuration, and commissioning....54
7.3.1 Monitoring requirements....54
7.3.2 Requirements for the installation 54
7.3.3 Configuration requirements....55
8 Installation for VdS 2463 Compliance 58
8.1 Introduction....58
8.2 Installation 58
8.3 VdS mode operation 59
8.4 VdS Intruder Applications 59
8.5 VdS Fire Applications....60
8.6 Conformance to VdS2463....61
9 Trouble reporting and test....62
9.1 Trouble report 62
9.2 Test....63
9.2.1 Test 63
9.2.2 Disable Cellular....64
10 Maintenance 65
10.1 Checking for faults....65
10.2 Checking battery status 65
10.3 Upgrading software....65
10.4 End to end tests....65
11 Technical specifications....66
12 Conformance 68
Appendix 1: Setting up the IRIS Toolbox....69
Starting the IRIS Toolbox 69
Appendix 2: Abbreviations used by AddSecure 70
Appendix 3: Enclosure T-NG-ENC2 71
Specification:....71
Accessories 71
Installation instructions 71
Appendix 4: Panel Specific Protocol Handling (Emulation Mode)....73
A4.1 ESPA....73
A4.1.1 Enabling the ESPA interface....73
A4.1.2 Connection to the fire panel....73
A4.1.3 Conversion of ESPA display messages to SIA format alarms....74
A4.1.4 Setting SIA/XSIA 74
A4.1.5 Setting TEF Mode 74
A4.1.6 Setting E2E Ack (End to End Acknowledgement) Mode 75
A4.1.7 Trouble Reporting 75

A4.2 Alarm Panels Using SIA DC-09 Protocol....76
A4.2.1 IP Addressing....76
A4.2.2 Panel Account Number....77
A4.2.3 Encryption....77
A4.2.4 Poll Period....77
A4.2.5 IP Port....77
A4.2.6 Operation with an Alphatronics UNii Panel....78
A 4.3 Operation with a Vanderbilt SPC Panel....79
A4.3.1 IP Addressing....79
A4.3.2 Panel polling....79
A4.3.3 Web access to the panel....80
Appendix 5: Default Alarm Messages Generated by the Terminal....81
A5.1 Pin Input Alarms....81
A5.2 Voice call alarm....81
A5.3 General Alarms....82
A5.4 Alarms generated when using DC-09 as the transmission protocol.....82

1 About this manual

This Technical Reference manual applies to the complete range of IRIS-4 models, see chapter 2 “About IRIS-4 product range”.

1.1 Target group

This document is intended as a technical reference for engineers and for anybody that needs technical information about the IRIS-4 range of terminals.

1.2 Scope

This document has all the technical information about the IRIS-4 range of terminals running software version 4.29.3. Many of the features described are also available in earlier software versions. More information about connecting to proprietary alarm panels is in the separate documents.

The manual has these chapters:

1	About this manual	Describes the range and scope of the manual.
2	About the IRIS-4 product range	Presents the terminals in the IRIS-4 range.
3	Circuit board layouts	Presents the Printed Circuit Boards (PCB) for each terminal.
4	Basic Setup	Explains how to install the terminals.
5	Configuring the terminal	Explains how to configure the terminals for their purpose.
6	Settings	Explains how to configure all the settings.
7	Installation for EN54-21:2006 Compliance	Installation instructions for complying with this standard.
8	Installation for VdS 2463 Compliance	Installation instructions for complying with this standard.
9	Trouble reporting and test	Explains how the terminal reports problems and how to test an installation.
10	Maintenance	Explains maintenance procedures.
11	Technical Specifications	Lists all the technical specifications for the products.
12	Conformance	Lists the standards to which the products conform.
A1	Setting up the IRIS Toolbox	Explains how to install the IRIS Toolbox.
A2	Abbreviations used	Lists and explains all abbreviations used in the document.
A3	T-NG-ENC2 enclosure.	Description and installation instructions for the enclosure for the IRIS-4 4xx and 6xx terminals.
A4	Panel Specific Protocol Handling (Emulation Mode)	Explains how settings for specific alarm panel types can be used to enable alarms to be sent based on serial messages from the panel.
A5	Default alarm messages generated by the terminal	Some input and fault related alarms are generated directly by the terminal and sent to the ARC. This section lists the default settings.

2 About the IRIS-4 product range

Below are the IRIS-4 models and their functions:

	Touchscreen	Ethernet	Cellular (2/3/4G)	Dial capture	Wi-Fi	Pin inputs	Relays	Serial RS485	Serial TTL	Serial RS232	Enclosure	Bluetooth	Battery	Enclosure (optional)
DS2220/ IRIS-4 50			✔	✔ [5]		2	2			1	✔			
IRIS-4 160		✔	✔	✔	✔	4	3	✔	✔	1	✔	✔	✔	
IRIS-4 200	✔		✔	✔		4	3	✔		1	✔			
IRIS-4 220	✔	✔		✔		4	3	✔		1	✔			
IRIS-4 240	✔	✔	✔	✔		4	3	✔		1	✔			
IRIS-4 240AP	✔	✔	✔ [4]	✔		4	3	✔		1	✔			
IRIS-4 400	✔		✔	✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 400G[3]	✔		✔	✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 420	✔	2		✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 420G[3]	✔	2		✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 440	✔	2	✔	✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 440G[3]	✔	2	✔	✔		4[1]	4	✔	✔	2[2]				ENC 2
IRIS-4 620		✔				6	4	✔	✔	2				ENC 2
IRIS-4 620D		2				6	4	✔	✔	2				ENC 2
IRIS-4 640		✔	✔			6	4	✔	✔	2				ENC 2
IRIS-4 640D		2	✔			6	4	✔	✔	2				ENC 2

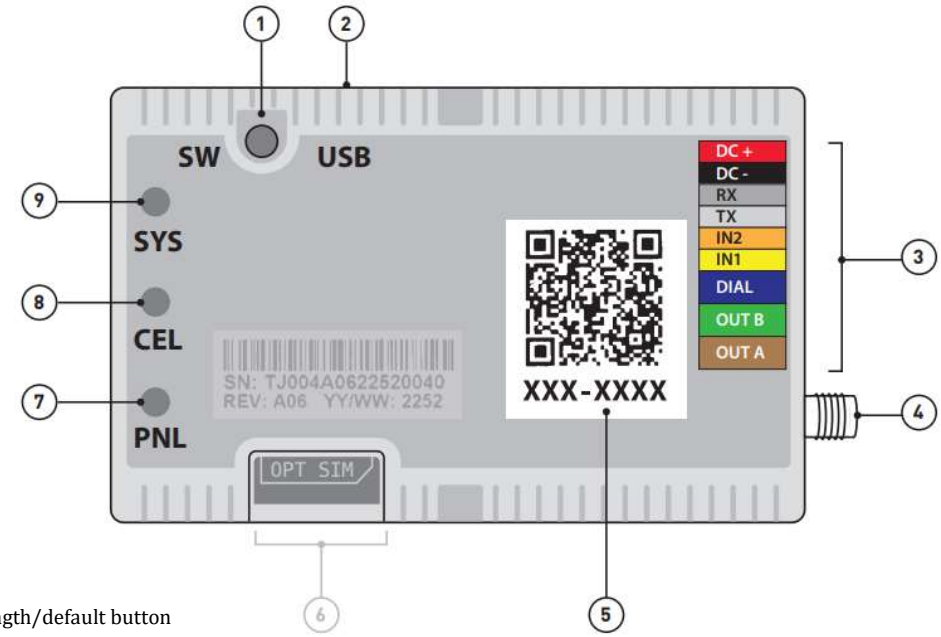
Notes:

1) The number of pin inputs on the 4xx can be extended by 12 using an Extension (EXT) board, providing a total of 16 pin inputs.
2) The two basic serial RS232 ports on the 4xx can be converted to a single full port if required.
3) The 4xxG are virtually identical to the 4xx, except that:
   - Ethernet and Cellular will not work/power up, without external power being supplied. They are disabled when only powered by USB and show a fault message on the touchscreen accordingly. USB is for programming only.
   - Serial port RS232(2) no longer supports 1200 baud.
   - There is an AP button, like the 6xx series, so you can default the terminal on power up.
4) The 240AP has only 3 & 4G with frequencies required for Asia Pacific.
5) The DS2220/IRIS-4 50 is also fitted with an eSIM. Please contact AddSecure if you wish to use this instead of a plastic SIM card.

A metal enclosure (T-NG-ENC2) is available for the IRIS-4 4xx and IRIS-4 6xx terminals.

3 Circuit board layouts

3.1 DS2220/IRIS-4 50

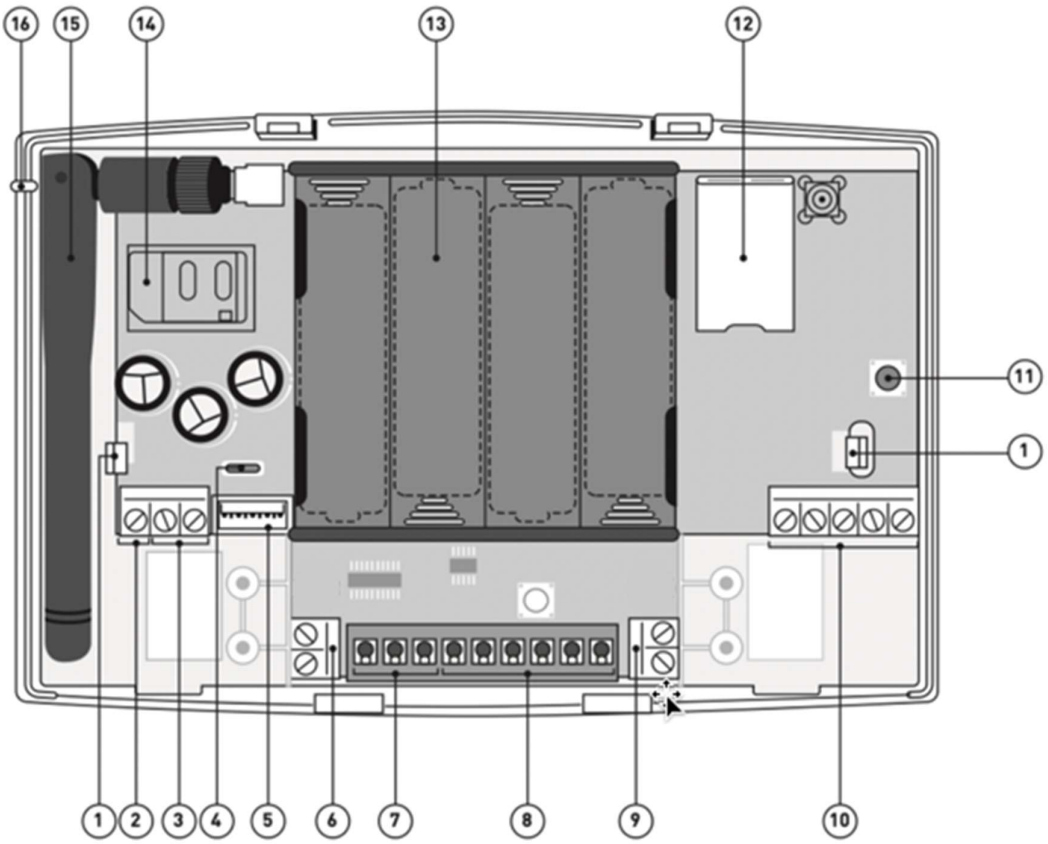


① = Signal strength/default button
② = USB micro connector
③ = Cable harness loom, with colour coded identification
④ = Cellular antenna connection
⑤ = Terminal Activation Code (TAC)
⑥ = Plastic SIM card (optional)
⑦ = Panel interface status indicator (red)
⑧ = Cellular status indicator (yellow)
⑨ = Terminal status LED indicator (green)

3.1.1 Sys LED Indications

LED color	Light	Indication
🟢	Flashing	Fault.
🟢	Constant	Communicating, no current faults.
🟡	Off	Cellular not registered.
🟡	Flickers on	Cellular registered but no data connection.
🟡	Flashing	Cellular connected but not polling to ARC.
🟡	Constant	Successfully polling over cellular to ARC (flickers on every poll).
🔴	Flashing	Panel interface fault, either Dial Capture, tamper, pin input tamper or no serial activity. Note each of these fault notifications are disabled by default
🔴	Constant	Panel interface – no faults.
All 🟢 🟡 🔴		Will flash together for a short period when the terminal has been defaulted. Will blink together for a short period if the terminal is installing new software which it has received.

3.2 IRIS-4 160



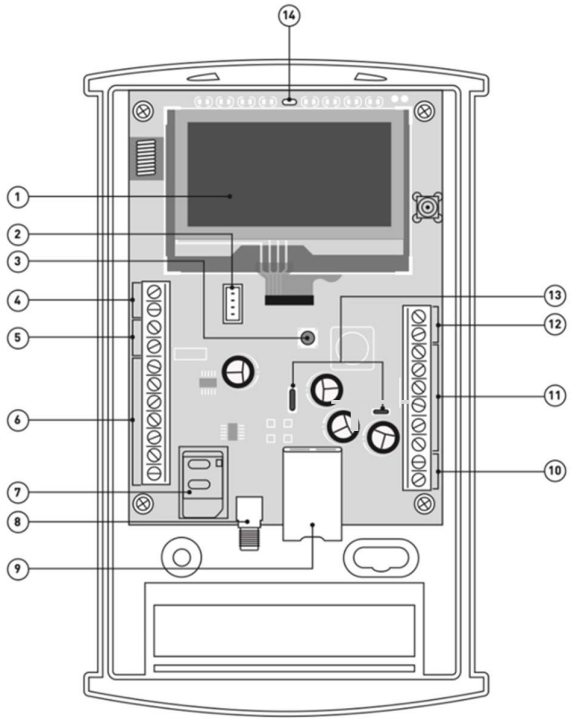
①= Release clip
②= Sense screw terminal
③= DC power screw terminals
④= Micro USB connector
⑤= Serial (TTL) connector
⑥= RS485 screw terminals
⑦= RS232 screw terminals
⑧= Relay outputs screw terminals
⑨= Dial capture port screw terminals
⑩= Pin input screw terminals
⑪= Bluetooth button
⑫= Ethernet connector
⑬= Battery case
⑭= SIM card holder
⑮= Cellular antenna
⑯= Sys LED

3.2.1 Sys LED indications

LED color	Light	Indication
	Flashing	Default state not currently configured.
	Constant	Successfully connected, but still outstanding faults. See section 9.1, “Trouble report”.
	Flashing	Bluetooth mode, but no active connection.
	Constant	Bluetooth mode with an active connection.
	Constant	Communicating, no current faults (flickers on every poll).

3.3 IRIS-4 2xx

① = Touchscreen
② = Serial (TTL) (not supported)
③ = Case tamper switch
④ = Dial capture port screw terminals
⑤ = RS485 screw terminals
⑥ = Pin input screw terminals
⑦ = SIM card holder
⑧ = Cellular antenna socket
⑨ = Ethernet connector
⑩ = DC power screw terminals
⑪ = Relay outputs screw terminals
⑫ = RS232 screw terminals
⑬ = Micro USB connectors
⑭ = Sys LED

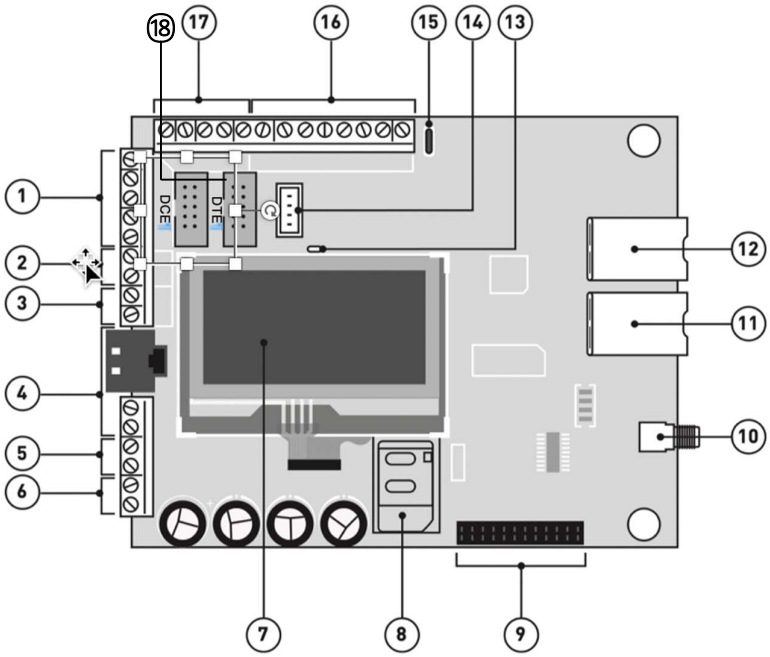


3.3.1 Sys LED indications

LED Color	Indication
• Yellow flashing	Not configured or indicating there are current faults outstanding. See section 9.1, “Trouble report”.
• Yellow constant	Communicating and no current faults (flickers on every poll).

3.4 IRIS-4 4xx

① = 2 x RS232 screw terminals
② = CAN bus (not supported)
③ = RS485 screw terminals
④ = Dial capture port, RJ45 & screw terminals
⑤ = External tamper screw terminals
⑥ = DC power screw terminals
⑦ = Touchscreen
⑧ = SIM card holder
⑨ = Expansion board connector
⑩ = Cellular antenna socket
⑪ = Ethernet 1 connector
⑫ = Ethernet 2 connector
⑬ = Sys LED
⑭ = Serial (TTL) connector
⑮ = Micro USB connector
⑯ = Relay outputs screw terminals
⑰ = Pin input screw terminals
⑱ = 10-way headers for full RS232 connection



3.4.1 Sys LED indications

LED Color	Indication
• Yellow flashing	Not currently configured or indicating there are current faults outstanding. See section 9.1, “Trouble report”.
• Yellow constant	Communicating and no current faults (flickers on every poll).

3.4.2 Expansion boards

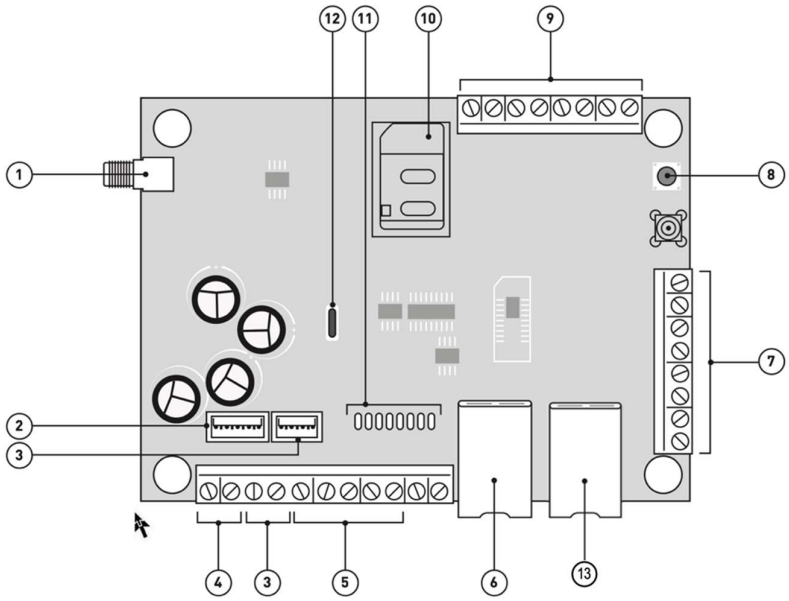
An expansion board can be added to the 4xx main board. There are 3 variants:

- EXT1: provides additional 12 pin inputs.
- EXT2: provides additional 12 pin inputs and a standard PSTN analog line interface (PSTN) as an outbound transmission path for alarms.
- EXT3: provides an additional 12 pin inputs and 3 mechanical relays (EXT3 not supported on 4xxG boards)

See section 4.2.1 “Installing the Extension boards on the 4xx” for installation instructions.

3.5 IRIS-4 6xx

① = Cellular antenna socket
② = Serial (TTL) connector
③ = RS485 connector and screw terminals
④ = DC power screw terminals
⑤ = 2 x RS232 screw terminals
⑥ = Ethernet 1 connector
⑦ = Pin input screw terminals
⑧ = AP button
⑨ = Relays screw terminals
⑩ = SIM card holder
⑪ = LEDs
⑫ = Micro USB connector
⑬ = Ethernet 2 connector



3.5.1 LED indications

LED status		Indication
SYS	On	Terminal is operational and all systems ok.
	Flashing	Not currently configured or indicating there are current faults outstanding. See section 9.1, “Trouble report”.
SIM	On	Terminal can see the SIM card (IRIS-4 640D).
	Off	Terminal cannot see the SIM card (IRIS-4 640D).
GSM	On	GSM connected / registered (IRIS-4 640D).
	Off	GSM Not connected / registered (IRIS-4 640D).
GPRS/3G	On	Terminal has network connection (IRIS-4 640D).
	Off	Terminal has no network connection (IRIS-4 640D).
Ethernet	On	ETH connected / synchronized.
	Off	ETH disconnected / not synchronized.
Serial	Flashing 0.2s on/ off	Not communicating with panel.
	Flashing 1.5s on/off	Terminal not configured.
	Flashing 0.1s on/0.9s off	Normal communication.
Poll	On (flickers per poll)	Successfully polling with ARC.
	Off	Not polling with ARC.

4 Basic setup

4.1 Before you begin

4.1.1 ARC

Make sure that the Alarm Receiving Center (ARC) to which the terminal will send alarm signals has the appropriate IRIS Secure Apps (ISA) receiving system. The following information should be obtained from the ARC.

Terminal account no: .....

For IRIS protocol:

ARC IP address (for IRIS protocol) .....

For DC-09 protocol:

ARC Main receiver IP address .....

ARC Main receiver TCP port .....

ARC Backup receiver IP address .....

AC Backup receiver TCP port .....

4.1.2 Ethernet connection details

If the installation uses Ethernet, the customer's Ethernet network (LAN) must be connected to the terminal. Obtain the following information from the customer.

Will the terminal be required to use either:

Fixed IP address ☐ or Dynamic Host Configuration Protocol (DHCP) ☐

Note: If using Fixed IP Address, then the following additional information will be required.

IP address: .....

Gateway address: .....

Subnet mask: .....

4.1.3 Cellular SIM card and Access Point Name

If the installation uses cellular then a SIM card will be required. The terminal will also need to be given a cellular Access point name (APN) and other possible configurations. Obtain the information from your SIM card provider.

APN: .....

Username (USR): .....

Password (PWD): .....

SIM pin code: .....

4.2 Recommended installation sequence

We recommend that you follow this installation sequence:

- Add Extension board (if required)
- Mount the terminal
- Position the antenna
- Connect cables to the terminal
- Power up
- Use Touchscreen menus

Note: that the term “touchscreen” as used in this document refers to both the physical touchscreen on a terminal PCB and the virtual touchscreen provided in the IRIS Toolbox.

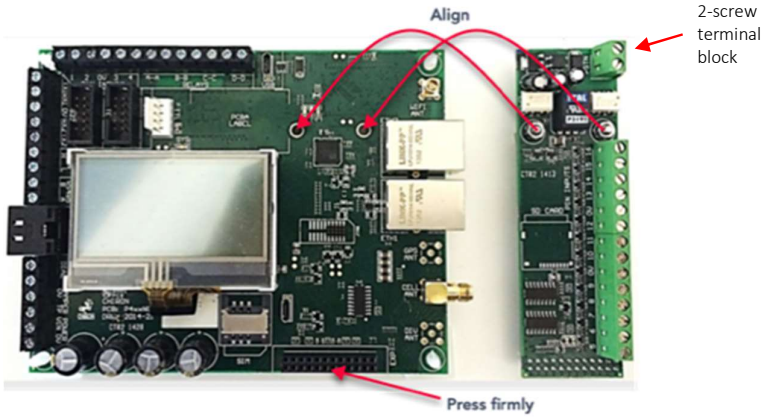
4.2.1 Installing the Extension boards on the 4xx

Expansion boards plug directly into the terminal with no additional wiring.

Use the following procedure to install your expansion board:

1 Power down the terminal.

2 Remove the PCB from its casing.

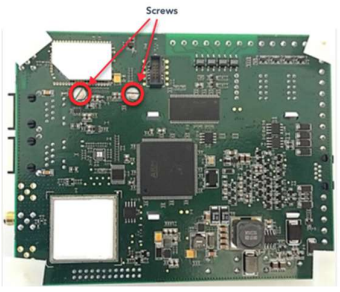


3 Align the expansion board over the expansion socket and mounting holes.

4 Slowly, but firmly, push down the module onto the PCB until the expansion pin header is fully inserted into the EXP header.

5 Turn over the PCB and secure the two expansion pillars with the screws and washers supplied.

6 Now turn the PCB over again and mount it back into the casing.



4.2.1.1 Expansion boards

An expansion board can be fitted to the main terminal to provide additional functionality.

4.2.1.1.1 Pin Inputs

The EXT1 expansion board provides 12 additional pin inputs

4.2.1.1.2 PSTN and input pins

The EXT2 expansion board provides 12 additional pin inputs and a PSTN Dial-out for a PSTN connection via the 2-screw terminal block (see Figure 4).

Connect the PSTN line to the PSTN screw terminals, which are not polarity sensitive.

Figure 4



4.2.1.1.3 Relays and input pins

The EXT3 expansion board provides 12 additional pin inputs and 3 mechanical relay outputs. This board is not supported on the 4xxG.

4.2.2 Mount the terminal

4.2.2.1 Mounting the 50 (DS2220/IRIS-4 50)

The terminal is intended to be mounted within the existing tamper protected alarm panel enclosure which means that the interfaces between the terminal and the alarm panel do not need to be separately protected against tamper:

1. Identify a location within the enclosure from which the interface cables provided with the terminal will reach their required destination on the panel. The position of the cellular antenna must also be taken into account, and this is best located externally to the enclosure.
2. Fix the terminal into the position chosen using either the Velcro pads, adhesive mounting pad, cable tie provided, or some combination of these.

4.2.2.2 Mounting the 160

Choose a suitable location, considering the routing of both power and terminal interface cables. Follow this procedure:

1. Remove the cover by removing the two screws accessible through the cover.
2. Once released, lift the lid slightly and push until lid comes off.
3. Remove the terminal PCB (retained by two clips to left and right off the board).
4. Position the housing on the wall and drill three holes.
5. Feed the cables through the opening at the base of the plate, or via the ‘knock-outs’, and secure the plate to the wall with the three screws supplied.
6. Slide the PCB back into the top retainers and within the side pillar and then gently secure the terminal back in place using the release clips.
7. Continue with installation and configuration of the terminal.
8. When finished, re-attach the cover with the two screws. This also affixes the PCB in place.

4.2.2.3 Mounting the 2xx

Choose a suitable location, considering the routing of cables for both power and the panel terminal interface. Remove the two case fixing screws under the slide cover and open the unit. Now release the two clips on the base holding the PCB in place.

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 'knock-outs', and secure the plate to the wall with the three screws supplied.

Continue with installation and configuration of the terminal.
When finished, re-attach the cover with the two screws and re-position the slide cover.

4.2.2.4 Mounting the 4xx & 6xx

Choose a suitable location, considering the routing of both power and terminal interface cables, within the alarm panel or in a separate enclosure. Secure the terminal within the enclosure using the fitted standoffs or the alternative self-adhesive feet.

Note: For EN50131-10 compliance, you must use the supplied standoff and not the self-adhesive feet.

4.2.3 Position the antenna

Place the antenna appropriately to obtain a strong cellular signal. It is advised to keep the antenna away from large metal structures.

You can check the signal strength during the configuration process as described in chapter 5. You may have to reposition the antenna to improve signal reception.

4.2.4 Connect cables

DO NOT INSERT THE SIM CARD into its holder until you have made all the connections and carried out a network scan. See section 6.7.2 “Run network scan”.

4.2.4.1 Cables

Depending on which type of communications are to be used, connect these cables to the PCB:

Ethernet enabled systems	Connect the ETH 1 connector using the Ethernet cable to the local IP router/switch or socket allocated for the LAN/WAN network IP connection. ***Note – The terminal can be adversely affected by significant amounts of broadcast traffic on an Ethernet connection. Therefore mitigations such as use of network segmentation and VLANs should be consider in these situations.***
Cellular enabled systems	Fit the supplied T-bar cellular antenna to the cellular antenna connector but do not fix in place until after performing the network scan. If needed, the antenna on the 160 can be repositioned outside the plastic housing using knockouts in the top cover.
Dial port	This is a two-wire connection to the PSTN output of the panel.
Pin Inputs	For pin input connections, see section 6.13 “Pin inputs”.

4.2.4.2 Serial connections

These connections are for panels using serial communication to the terminal.

Note: For alternative selections for third-party panels, use the Settings option in the Installers Menu.

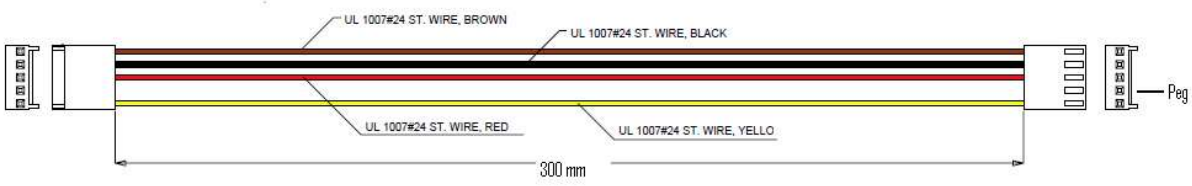
4.2.4.2.1 RS485 connections (Honeywell Galaxy or Risco ProSys)

Where fitted, you can use the screw terminal blocks or the 4-pin header. The connections for the screw terminals are:

I RS485 screw terminals	Honeywell Galaxy Data Bus terminal	Risco ProSys Bus1 terminal
0V (Power)	Galaxy (-)	Com
VIN (Power)	Galaxy (+)	AUX
A	Galaxy (A)	YEL
B	Galaxy (B)	GRN

4.2.4.2.2 Serial TTL connections

The requisite cable, Texecom RS232 Lead, part no. Tex600, can be ordered from AddSecure



4.2.4.2.3 RS232 connections

These are used with several panels such as HHL, ESPA fire panels, Notifier, Protec, EBL Talk, and CTEC. The actual panel for your installation can be selected in Settings, see section 6.9 “Panel Interface”.

RS232 screw terminals	HHL com port	DB9 Male connector
TX2	2 (RX)	Pin 2 (RX)
RX2	3 (TX)	Pin 3 (TX)
0V	1 (GRD)	Pin 5 (GRD)

4.2.4.3 Power Supply

The terminal can be powered using a separate 9-28V DC power supply specified to deliver at least 1A current to the screw terminals or receive power directly via the RS485 or Serial TTL connectors.

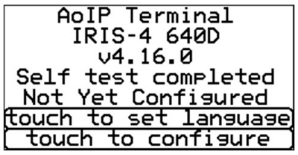
Note: to comply with the Radio Equipment Directive, the power cable must be no longer than 3 meters in length.

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

4.2.5 Power up

4.2.5.1 Using the terminal touchscreen

If you are going to use the touchscreen on the terminal, power up the terminal. This screen will be displayed.



If the terminal has a physical touchscreen, it is supplied with a stylus intended to be used with the screen.

4.2.5.2 Using the virtual touchscreen

Alternatively, and for terminals without a physical touchscreen, once the terminal is powered up, you can access the terminal's 'virtual' touchscreen on a PC using the IRIS Toolbox software. For details on how to set up the toolbox, see "Appendix 1: Setting up the IRIS Toolbox".

4.2.6 Welcome menus

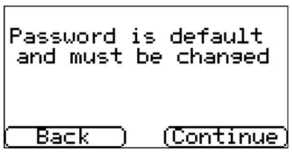
4.2.6.1 Language selection

English is the default language.
To change the touchscreen language, click <<touch to set language>, and select your desired language.

4.2.6.2 Installer's password

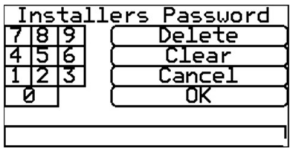
Click <<touch to configure>> and then you will need to set your own password to comply with EN50136-2. Follow the procedure below:

1 Enter the default password, "111111", and click «OK».

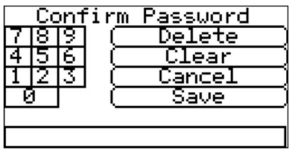


2 Click «Continue» to enter your own password.

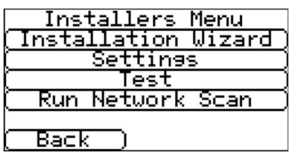
3 Now enter your own password, 6 to 12 digits, then click «OK».



4 Re-enter the new password to confirm it, then click «Save». It is recomended that you store this password separately in a safe place.



5 The Installers Menu will then be displayed.



For the next and any following times you select "Installers Menu" from the Welcome screen, simply enter your password and click «OK».

5 Configuring the terminal

IRIS-4 terminals need to be configured the first time they are used. All terminals can be configured with the Installation Wizard on the physical or virtual touchscreen. The 160 can also be configured using the Installer app, see section 5.5 “Configuring the 160 using the Installer App”.

The Installation Wizard presents configuration options in predetermined sequences. Once one option is completed, the wizard automatically moves on to the next option. Sequences vary depending on the terminal type and the choices you make as you go through the sequence.

5.1 Accessing the Installation Wizard

Access the Installer’s menu as described in section 4.2.4 and 4.2.5.

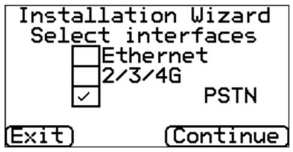
5.2 Initial configuration settings

If options described in this manual are not visible on the screen, it is because they are not supported on the terminal type you are using.

Once you have entered your password, see section 4.2.5 “Installer’s password”. the main menu is displayed. Click “Installation Wizard” to start the Installation Wizard.

5.2.1 Select interfaces

As the terminal can use Ethernet, Wi-Fi, cellular communication and PSTN, the sequence of options that the installation wizard automatically displays varies to suit the chosen communication mode:



The first task presented by the Installation Wizard is to select the network interfaces to be used.

For single path communications, the terminal can use Ethernet, Wi-Fi or cellular paths.
For dual path communications, select cellular and one of the other paths.

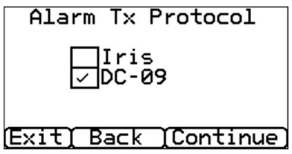
If you have installed a PSTN expansion board (EXT2), then the PSTN communication path will be available, allowing triple path communication.

If you are configuring a 160, Wi-Fi is presented as an option.
Only Ethernet or Wi-Fi can be selected, not both.



5.2.2 Alarm Transmission Protocol

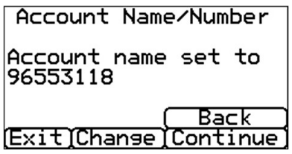
Select the alarm transmission protocol required and click «Continue».



5.2.3 Account name/number

The Account Name/Number screen is then automatically displayed.

To change, click «Change». The format required differs between Iris and DC-09, so the format of the display for each protocol is different.



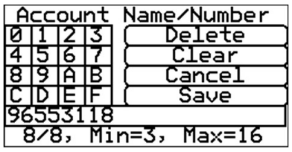
Enter the account (name/number) provided by the ARC.



For Iris this can be alphanumerical and up to 32 characters long. It is normal to have a simple 4- or 6-digit numerical account name.

For DC-09, the account name can be between 3 and 16 hexadecimal characters.

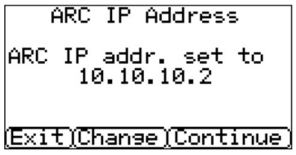
Click «Save» and then click «Continue».



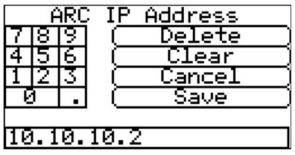
If Iris is selected, the next menu is for the setting of the ARC IP address and the ARC will configure the communications settings required by the terminal when the terminals connects to it. If DC-09 is selected, the transmission settings must be set in the terminal as they cannot be set by the ARC. A series of menus is displayed.

5.2.4 ARC IP address (Iris protocol only)

The ARC IP address screen is displayed. This address is obtained from the ARC and would normally be the external IP address for their ISA system.



To change the IP address, click «Change» and enter the ARC IP address, then click «Save». Confirm that the IP address is correct, then click «Continue».

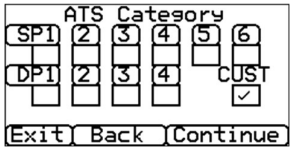


Note: Only the primary/main ARC IP address needs to be entered on the terminal, all backup or alternative IP addresses are downloaded from the ARC to the terminal on the first polling communication.

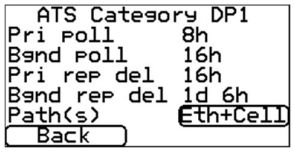
5.2.5 DC-09 settings menus (DC-09 protocol only)

For DC-09 setup, a sequence of menus is used.

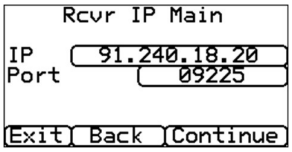
The EN50136-1 ATS Category is selected from the first menu. Unless Cust (Custom) is selected, this automatically sets the Poll Periods and Reporting Delays. A menu showing the settings and where the path(s) used can be set is accessed using the category buttons shown.

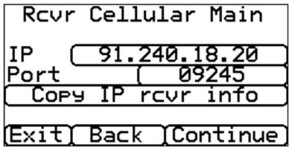


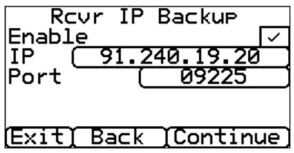
If Custom is selected, then the Paths are those selected in the Interfaces menu (see above) and the Polling Periods and Reporting Delays are set later in the wizard.

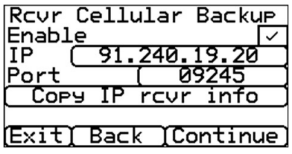


The IP addresses and the port numbers to be used should be obtained from the ARC. If the ARC does not have a backup receiver, this setting can be disabled.



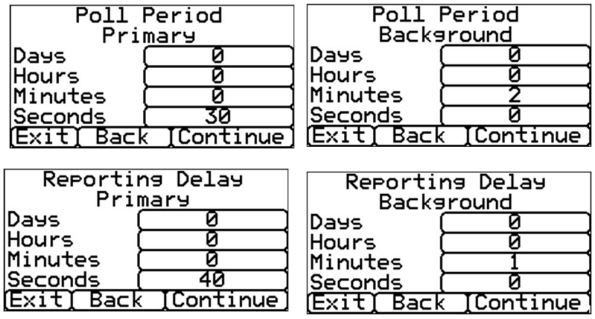






The next Polling Period and Reporting Delay menus described below are bypassed if an ATS category other than Custom is selected.

The Primary Poll Period and Reporting Delay determine the Primary ATP Reporting Time as required by EN50136-1. These settings are used on one of the connections as set up in the receiver addresses set up above. The particular one used is the first one that the terminal is able to communicate with in order



- IP Main
- IP Backup
- Cellular Main
- Cellular Backup

The Background Poll Period and Reporting Delay determine the Alternative ATP Reporting Time as required by EN50136-1 and apply to the receiver connections which are not identified by the terminal as the Primary.

When the terminal identifies a fault with a connection, it waits for the time defined by the Reporting Delay before reporting the fault to the ARC. This brings the reporting time in line with EN50136-1.

Suggested settings for the different ATS configurations defined in EN50136-1 are:

Configuration	Primary poll rate	Primary reporting delay	Background poll rate	Background reporting delay
SP1	1 day	30 days	1 day	30 days
SP2	8 hours	16 hours	8 hours	24 hours
SP3	9 minutes	20 minutes	8 hours	24 hours
SP4	60 seconds	110 seconds	8 hours	24 hours
SP5	30 seconds	50 seconds	8 hours	24 hours
SP6	6 seconds	10 seconds	8 hours	24 hours
DP1	8 hours	16 hours	16 hours	30 hours
DP2	9 minutes	20 minutes	8 hours	16 hours
DP3	60 seconds	110 seconds	8 hours	16 hours
DP4	30 seconds	50 seconds	99 minutes	3 hours

5.2.6 Encryption

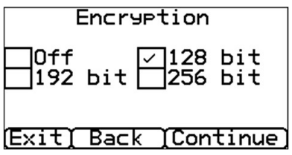
One of four different encryption levels can be selected. If appropriate the key can also be set. The key is made up of Hex characters (0 to 9 and A to E) and the length required depends on the level of encryption selected:

128 bit – 32 characters

192 bit – 48 characters

256 bit – 64 characters





5.3 Communication configuration

The Installation Wizard now goes through a sequence of setup and test options for each communication path chosen, in this order; Ethernet, Wi-Fi, Cellular and PSTN. The sequences can vary depending on the combination of paths chosen and the type of terminal being configured.

The sections immediately below (Test failure messages and Checking S/W version) describe items common to more than one path.

5.3.1 Communication tests

Each communication path is tested by sending a test poll and test alarm. If these tests fail, the failure is displayed together with possible measures that can be taken to solve the problem.

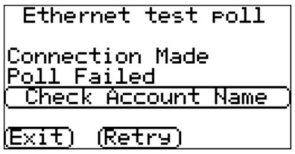
5.3.1.1 Connection failed



If the call did not reach the ISA system, these are the remedies for the possible causes:

- Check that the ARC IP address entered is correct for the ARC.
- Check the LAN IP address setup for the terminal and confirm with the customer IT department that you have the correct addresses for their network.
- If using Ethernet on a Virtual Private Network (VPN), the ARC IP would be defined for that VPN but not correct for cellular connections which will not be on the VPN. If this is the case, please have the ARC operator check the ISA setup for this account to have a separate address for the cellular connection.
- Ensure the alarm and polling port (TCP Port 53165) is not blocked outbound by the customer's firewall.
- For cellular connections, ensure the SIM card is set up for cellular Machine-to-Machine data and configured with the correct Access Point (APN) details.

5.3.1.2 Connection made, Poll failed



This indicates that the test poll or alarm call has reached the ISA system, but the account number is not valid.

- Check that the programmed account number is correct.
- Check with the ARC that the account in ISA is correctly set up.

5.3.1.3 Authentication failed



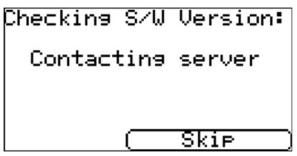
This indicates that the test poll call has reached the ISA system, but the security keys do not match.

Check if the terminal has recently been replaced or defaulted. If so, the ISA operator will need to reload the security key into the terminal using the Allocator App.

The security key is a feature designed to prevent substitution attacks against both the terminal and the ARC. When enabled, the ARC and terminal use an agreed private key. This key must be used for all future polling authentication. Both the terminal and the Polling Engine authenticate each other, thus ensuring a replacement terminal cannot be used to fool a Polling Engine into thinking its status is unaffected during malicious tampering; it also makes sure the terminal will be aware if its IP traffic has been maliciously redirected to a different ISA system.

If the installer has recently replaced or defaulted the terminal, the ISA operator must reload the security key, e.g., by using the Allocator App.

5.3.2 Checking S/W version

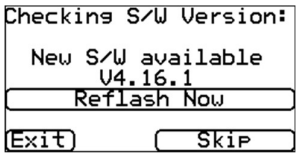


Once the terminal has established its first connection path, it will check its software version with an external server operated by AddSecure.

The Checking S/W Version screen is displayed.

Note: If you have selected cellular as the only interface, this check will be done after the cellular settings.

The terminal will now check with the AddSecure server to see if a new version is available. If a new version is available, the «Reflash now» option will appear and can be clicked, see section 6.22 “Reflash”.



5.3.3 Ethernet setup and test

5.3.3.1 Checking Ethernet connection

If Ethernet is being used, the Checking Ethernet screen is displayed.

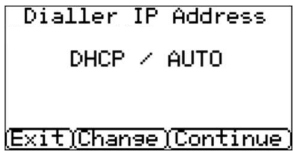


The terminal will now confirm if an Ethernet connection has been made to the premise’s network equipment, such as an Ethernet router or switch. If no connection can be seen, “Ethernet Disconnected” will be displayed and the cable between the terminal and the premise’s network equipment will need to be checked.

If the connection is good, you will see ‘Ethernet Connected’ and can click «Continue».

5.3.3.2 Dialler IP Address

The Terminal IP address screen is then displayed.



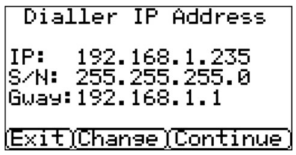
This shows or allows you to set up the Terminal IP address for the network to which the terminal is to be connected. The terminal is setup for DHCP by default, so the network will allocate an IP address, subnet mask and gateway.

If you are using a DHCP network connection, click «Continue». If the customer has requested that a fixed IP address is assigned, then click «Change».



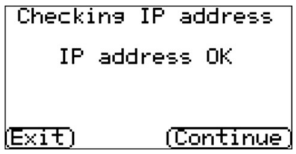
Click the «Fixed» box.

Using these menu options, enter the IP address (IP), Subnet Mask (S/N) and Gateway information (Gway) for the customer network.



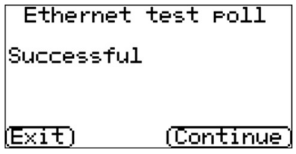
Then click «Back» and check that the information was entered correctly, then click «Continue».

The terminal will then check the validity of the IP address and confirm if this is OK. If "IP address OK" is displayed, click «Continue». If not, go back and check and correct the information.

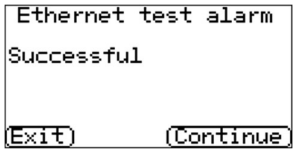


5.3.3.3 Ethernet communications tests

The terminal will send a test poll and test alarm message to the ARC to check the Ethernet connection.



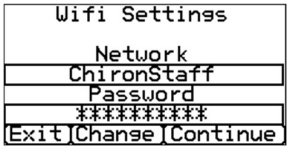
If these are not successful, the terminal will display the failure and possible reasons. See section 5.3.1.



5.3.4 Wi-Fi setup and test

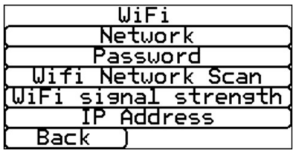
5.3.4.1 Wi-Fi settings

If you selected Wi-Fi as the communication method, this screen shows the name of the current Wi-Fi network and the current password. Click <<Change>> if you need to make changes.

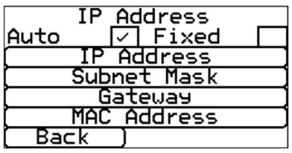


You can then change the parameters required, such as network SSID and access password.

The Wi-Fi network scan allows you to see all the networks that the terminal can see and select the one you want to use.



The IP address setting allows you to set a fixed Wi-Fi IP address in the terminal, should the network being used require it.



When done, click on <<Continue> to continue.

5.3.4.2 Checking Wi-Fi connection

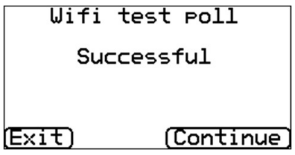
The Wi-Fi connection will now be checked.

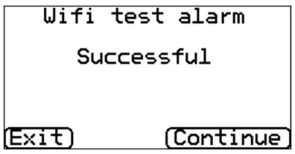


5.3.4.3 Wi-Fi communication tests

The terminal will send a test poll and test alarm message to the ARC to check the Wi-Fi connection.

If these are not successful, the terminal will display the failure and possible reasons. See section 5.3.1.



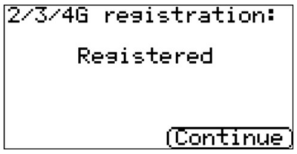


5.3.5 Cellular setup and test

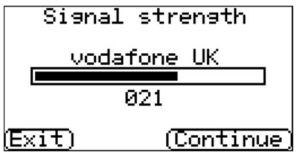
If the cellular interface was selected, the terminal will now perform cellular communication checks and tests.

5.3.5.1 Cellular registration

if the cellular network is registered, it will display "Registered". If "Not registered" is displayed, check that the SIM card is inserted correctly and contact the SIM provider to confirm it is enabled.



5.3.5.2 Cellular signal strength



The terminal then displays the current operator and signal strength for the base station with which it is communicating.

Note: A signal strength of 010 CSQ or higher is recommended for a reliable connection.

If the signal strength is below or close to minimum then try to reposition the antenna or use an external high gain antenna to improve signal strength (if necessary). Re-run the signal strength test and reposition again if necessary to gain best signal strength possible.

When the signal strength is as good as you can get it, click «Continue».

5.3.5.2.1 For the 50 (DS2220/IRIS-4 50)

On this terminal you can press and hold the "SW" button for 3s which will let you see the current signal strength indicated across the LEDs:

- Strength too low
- Strengh adequate
- Strength high

5.3.5.2.2 For the 6xx with cellular connection

Use the LEDs on the 6xx to perform a signal strength check.On the 6xx you can press and hold the "AP" button which will let you see the current signal strength indicated across the LEDs. The SYS LED remains flashing and the signal strength is indicated from the POL LED.

For a reliable cellular connection, a signal strength that lights three or more of the indicating LEDs is recommended:

Strength too low | Minimum strength | Maximum strength

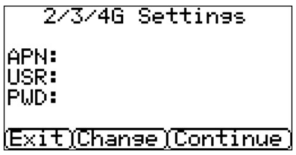


5.3.5.3 Cellular settings

5.3.5.3.1 APN, USR and PWD input

All cellular networks require the Access Point Name (APN) to be set. A few also require Username (USR) and Password (PWD).

Click «Change» to enter new settings for APN, USR, PWD and PIN (scroll down) that the SIM provider has given you.



A network scan can also be run. See section 6.7.2 for more information.

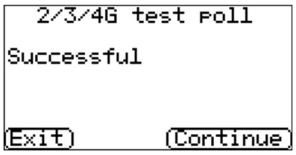


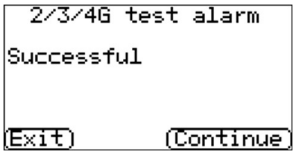
Once the information has been entered, click <<Back>> and it is presented on the screen. Click «Continue» to enter the next piece of information.

5.3.5.4 Cellular communication tests

The terminal will send a test poll and test alarm message to the ARC to check the Ethernet connection.

If these are not successful, the terminal will display the failure and possible reasons. See section 5.3.1.

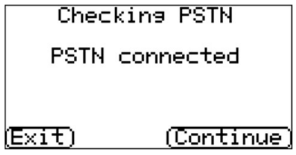




5.3.6 PSTN Setup & test

5.3.6.1 PSTN connection test

If the PSTN expansion board (EXT2) is fitted and the PSTN network interface is selected, the terminal will now check the PSTN connection by checking the line voltage.

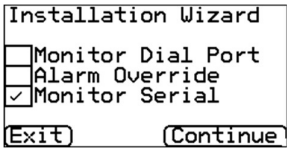


If PSTN is not connected, please check the cable and connection to the PSTN line. After reconnecting, it can take up to 30 seconds to detect.

5.4 Further configuration settings

5.4.1 Additional options

Depending on your terminal type, these additional options are available.



Monitor Dial Port

This sets the terminal to monitor the dial port using the 18K resistor (as supplied in the box). This resistor should be fitted across the A & B terminal of the 2-wire analog interface at the alarm panel and allows the terminal to indicate any status change to the ARC. This setting must be enabled if compliance with EN50136 is required and the interface to the alarm system is via the dial port.

The resistor must be fitted at the alarm panel end of the cable to enable the terminal to detect cable faults and/or tampers correctly. The ARC will also need to enable the dial port monitoring (Panel) on the ISA receiver software to receive alarm notifications on this status.

Alarm override

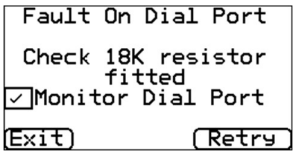
This allows the terminal to override and replace the phone and account numbers used by the alarm panel with the IP address of the ARC and account number entered during configuration. It can be used for dial port, serial or RS485 connection to alarm panels where you may not have access or cannot change the account or phone number in the alarm panel itself. This can be useful when converting older alarm panel sites to work with the IRIS-4 terminal.

Monitor serial

This sets the terminal to monitor the serial ports for activity and report any status changes back to the ARC. The ARC will also need to enable the serial port monitoring on the ISA receiver software to receive alarm notifications on this status.

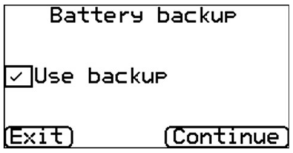
5.4.2 Dial port check

If Monitor Dial Port has been selected at the start of the wizard, the terminal will perform a check to see if the 18K ohm resistor has been fitted. If Monitor Dial Port has been enabled in error, the terminal will report this. In that case, uncheck the "Monitor Dial Port" checkbox.



5.4.3 Battery backup

For terminals with integral battery backup, the menu 'Battery backup' will now be shown. Tick the box to automatically use the battery backup when needed.



5.4.4 Pin alarms

This provides the option to use pin alarms which are the Pin inputs, and which can be used for SMS messaging or alarm signaling.

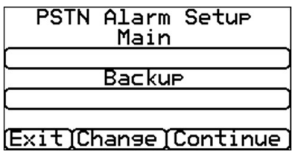
Click «Yes» to use the pin alarms or «No» to continue.



5.4.4.1 PSTN: Alarm Setup

If you have selected to use the PSTN interface, you will be asked to enter the telephone numbers of the PSTN receiver(s) at the ARC.

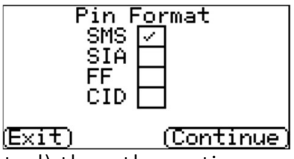
Click <<Continue>> when done.



5.4.4.2 Pin format

The Pin format screen is then displayed.

Click the appropriate tick-box to select which pin alarm format to use. SMS is only available on terminals with cellular capability.



Note: If you have selected PSTN network interface (EXT2 expansion board fitted) then the option for SIA will not be available as this is not currently available over PSTN.

When done, click «Continue».

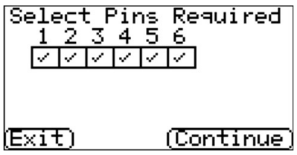
If you change the setting, you will be presented with a warning that all current pin input settings will be lost, click «Continue» and then click «Continue» again.

For more information on each format and additional configurations for the Pin alarms see section 6.13, "Pin inputs".

5.4.4.3 Pins required

If you have selected SIA, FF or CID for the alarm format, you will now need to select the pins you wish to enable and use.

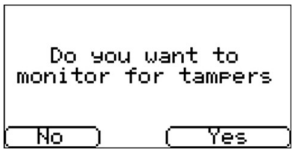
How many pins are displayed depends on which product you are working with:



Deselect 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'.

5.4.4.4 Monitor for tampers

Click «Yes» to monitor for tamper on the pin alarm inputs, otherwise select "No". Monitoring for tamper requires that the sense resistors are installed, see section 6.13 "Pin inputs".



5.4.5 Setup complete

The Installation Wizard has now been completed and the terminal is now configured. Click 'Finish' to exit and return to the main menu.



5.5 Configuring the 160 using the Installer App:

The IRIS Installer app is available from Apple Store or Google Play. Ensure that Bluetooth is enabled on your mobile device, download the Installer app and start it.

When the 160 is enclosed in its case and no user buttons are accessible, the Bluetooth operation can be started by tapping twice on its case lid. Use a metal object, such as a screwdriver, to "tap-tap" upon the lid. The LED will turn blue, and the 160 will begin broadcasting its Bluetooth existence.

On the App, click on "Connect" and wait until the terminal has been found. Enter the installer's password. The first time you do this, use the default password "111111". You will then be asked to enter your own password.

Enter a new password, 6 - 10 digits. The app menu, as follows, is then presented

Information	Action
Current Status	Console
Settings	Security

Now simply follow the instructions in the app.

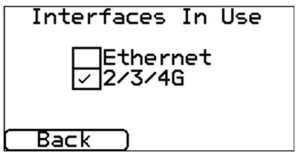
6 Settings

The options in the Settings menu vary for the different product types. Each option can be selected individually (there is no sequence as in the Installation Wizard),

6.1 Network interfaces

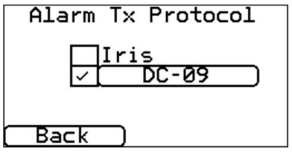
This option lets you select the communication paths to be used for polling and alarms on a multipath IRIS-4 terminal. There are several options:

- Ethernet
- For 160: Wi-Fi
- Cellular (Machine-to-machine data (M2M))
- For 4xx: PSTN (PSTN expansion board required)



6.2 Alarm Tx protocol

This allows the alarm transmission protocol to be selected. Related settings are available in sub menus by clicking on the button against the tick box selected.



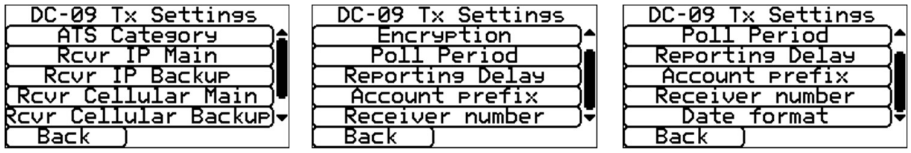
6.2.1 ARC IP address (for Iris protocol)

The IP address is obtained from the ARC and would normally be the external IP address for their ISA receiver system. This option lets you change it if needed.

Enter the external IP address for the ARC receiver and click «Save».

Note: Only the primary, or main ARC IP address, needs to be entered, all backup or alternative IP addresses are downloaded from the ARC to the terminal in the first polling communication.

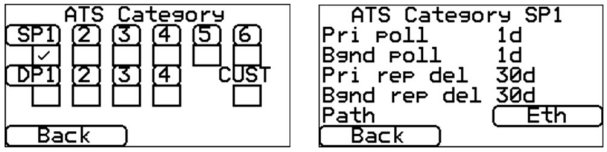
6.2.2 DC-09 transmitter settings (for DC-09 protocol)



6.2.3 ATS category

This menu allows the poll period and reporting delay to be set automatically, depending on the EN50136-1 ATS Category required.

Selecting the category button causes the setting values to be displayed. The Path(s) required can be selected on this menu by selecting the paths button, which will cycle around the paths available.

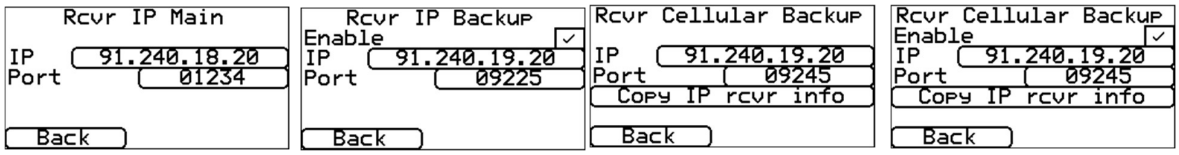


Selecting 'Cust' (Custom) allows the settings to be done manually using the Poll Period and Reporting Delay menus. In this case, the paths required can be set in the Network Interfaces menu.

When Custom is not selected, the Poll Period and Reporting Delay menus are hidden.

6.2.4 DC-09 receiver

The terminal can support up to four ARC connections, two via IP (Ethernet) and two via Cellular. Each connection can have different IP addresses and TCP port numbers.



If the same receiver is used for both IP and Cellular, the information entered for the IP connection can be quickly copied to the cellular settings.

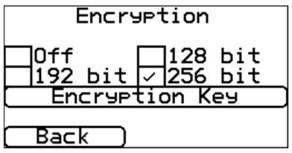
6.2.5 Encryption

One of four different encryption levels can be selected. If appropriate the key can also be set. The key is made up of Hex characters (0 to 9 and A to E) and the length required depends on the level of encryption selected:

128 bit – 32 characters

192 bit – 48 characters

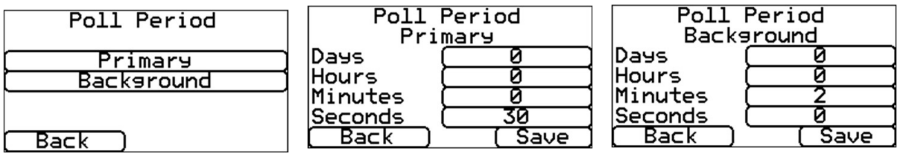
256 bit – 64 characters

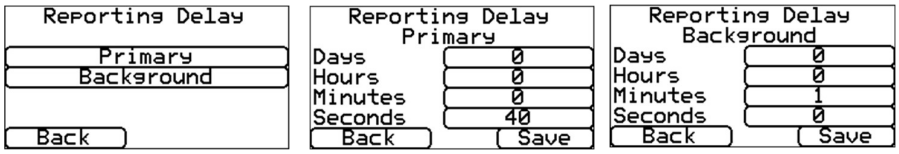




6.2.6 Poll period and Reporting delay

These menus are only displayed when the ATS Category 'Custom' is selected.





The terminal has two polling periods:

Primary – this is equivalent to the Primary ATP as described in EN50136-1 The terminal uses one of its ARC connections as the primary, starting with Main via IP and rotating to the others if a path is not operational in the order of Backup via IP, Main via Cellular and Backup via Cellular.

Alternative – the connections not used as Primary.

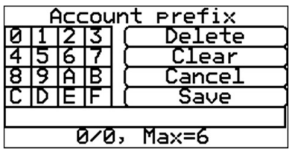
Polling can be disabled by setting the period to 0.

When the terminal identifies a fault with a connection it waits for the time defined by the Reporting Delay before reporting the fault to the ARC. This brings the reporting time in line with EN50136-1.

Suggested settings are shown in the Wizard DC-09 section earlier in this guide.

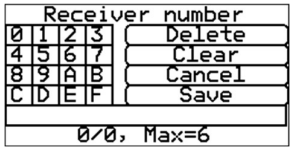
6.2.7 Account prefix

This is additional information that the terminal can send to the ARC that may may be required by the ARC to uniquely identify the account.



6.2.8 Receiver number

This is also additional information that the terminal sends to the ARC that may be required by the ARC to uniquely identify the account. This can also be left blank unless specified by the ARC.

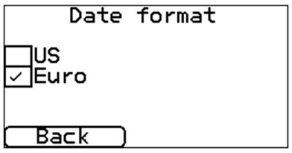


6.2.9 Date format

This sets the date format used by the receiver:

US (default): MM-DD-YYYY

Euro: DD-MM-YYYY



It is important to get this right as otherwise the real-time clock in the terminal may get set incorrectly and alarm transmissions may be ignored by the receiver.

6.3 Account name/number

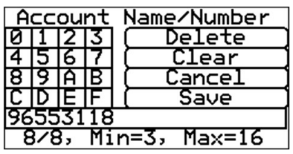
This option lets you change the account name/number for the terminal, as allocated by the ARC.

For Iris this can be alphanumerical and up to 32 characters long. It is normal to have a simple 4- or 6-digit numerical account name.

For DC-09, the account name can be between 3 and 16 hexadecimal characters.

Enter the account (name/number) provided by the ARC. Click «save».





6.4 Eth 1: For terminals with Ethernet capability

If your terminal has one Ethernet connector, this will be called “Dialler IP Address”. This allows you to set up the IP address of the terminal to use either automatic (DHCP) or a fixed IP address. The settings below will show the IP address either received (DHCP mode) or, if fixed will, let you set the IP address, Subnet Mask and Gateway:

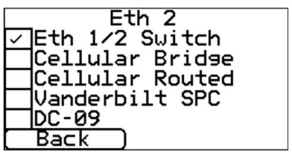


- IP Address
- Subnet Mask
- Gateway
- Mac Address (view only)

6.5 Eth 2: For terminals with dual Ethernet capability

By default, the Eth 2 connector is a shared Ethernet port with Eth 1 acting like a switch.

If you require the Eth 2 connection to be separate to Eth 1, make sure “Eth 1/2 Switch” is not ticked.



6.5.1 Cellular Bridge



Cellular Bridge creates a bridge between Eth2 and the terminal's cellular interface for UDP and TCP traffic. The IP address of the connected device should be set to be the same as the IP address for data connections allocated by the SIM card as shown in the "Cell/Client IP" sub-menu.

Note that there is potentially a security risk of unauthorized access to the device connected to Eth2 and to minimize this risk the SIM card should use a private APN (see Cellular Settings section below), such as that provided by the AddSecure Link service.

6.5.1.1 DHCPSRV or Fixed

Click on «DHCPSRV» if you want the terminal to assign the IP address to the device attached to Eth 2 automatically.

6.5.1.2 Cell/Client IP

This is the IP address that must be assigned to the device attached to Eth 2 and called from the cellular network when a remote connection to this device is required. This address is the address the cellular network assigns to the SIM card and cannot be changed.

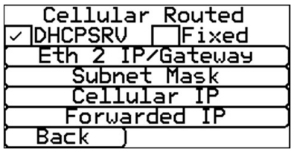
6.5.1.3 Subnet mask

This setting is fixed and is the subnet mask that should be set on the device attached to Eth 2.

6.5.1.4 Gateway

This is the gateway IP address that should be set on the device attached to Eth 2. It is preset and fixed and is derived from the cell/client IP address.

6.5.2 Cellular Routed



Cellular Routed routes UDP and TCP traffic between Eth2 and the terminal's cellular interface. The terminal converts the IP address of traffic received on the cellular interface to an address configured on the terminal for the device connected to Eth2, and vice-versa.

The default for Cellular Routed mode is set to the Forwarded IP address (i.e., the address of the attached device) of 192.168.1.1 and the Gateway IP address (i.e., the address of the Eth2 connection on the terminal) set to 192.168.1.254. The DHCP server is on by default.

Note that there is potentially a security risk of unauthorized access to the device connected to Eth2 and to minimize this risk the SIM card should use a private APN (see Cellular Settings section below), such as that provided by the AddSecure Link service.

6.5.2.1 DHCPSRV or Fixed

Click on «DHCPSRV» if you want the terminal to assign the IP address to the device attached to Eth 2 automatically.

6.5.2.2 Eth 2 IP/Gateway

This is the gateway IP address that should be set on the device attached to Eth 2.

6.5.2.3 Subnet mask

This setting is fixed and is the subnet mask that should be set on the device attached to Eth 2.

6.5.2.4 Cellular IP

This is the IP address that should be called from the cellular network when a remote connection to the device attached to Eth 2 is required. It is the address that the cellular network assigns to the SIM card and cannot be changed.

6.5.2.5 Forwarded IP

This is the IP address that has been assigned to the device attached to Eth 2.

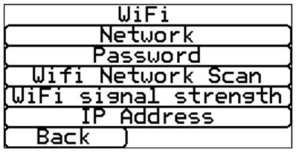
6.5.3 Vanderbilt SPC

This allows you to set up the second Ethernet port for the Vanderbilt (Siemens) SPC integration. See the Appendices of this document for more information.

6.5.4 DC-09

This allows you to set up the second Ethernet port for an alarm panel that supports the SIA DC-09 alarm communication protocol. See the Appendices of this document for more information.

6.6 Wi-Fi: For terminal with Wi-Fi capability



If you selected Wi-Fi communication, this screen would now display.

This will display the name of the current Wi-Fi network and the current password. Click on either to change them, then click «save»

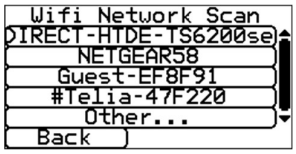
6.6.1 Network

This will display the name of the current Wi-Fi network and allow you to change it.

6.6.2 Password

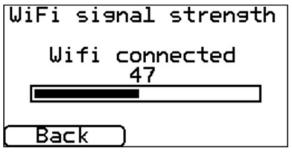
This will display the name of the current Wi-Fi password and let you change it.

6.6.3 Wi-Fi network scan



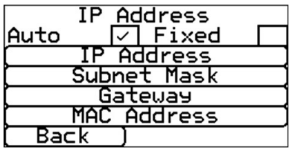
This option scans all available Wi-Fi networks and presents the results. If you select one, you will be asked for that network password.

6.6.4 Wi-Fi signal strength



The terminal now checks the current Wi-Fi network strength and presents the result.

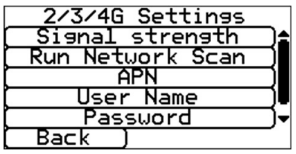
6.6.5 IP address



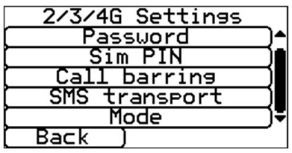
Set “Auto” (DHCP) to view the allocated IP address, or “Fixed” to set a fixed address, a subnet mask and a gateway. The MAC address is not changeable and given as reference, to allow the configuration of MAC filtering by the premise’s network. When done, click «Back» to return to the Settings menu.

6.7 Cellular Settings: For terminals with cellular capability

This option lets you view and change the cellular (2/3/4G) settings.



1



2

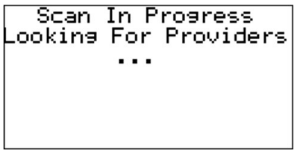
6.7.1 Signal strength

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

6.7.2 Run network scan

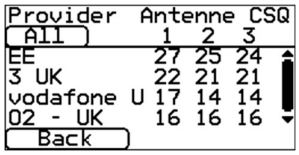
This option performs a scan of all providers in the local area and presents a chart of the best three base stations per provider.

This scan cannot be performed if the SIM card is fitted. Remove the SIM card by powering down the terminal, removing the SIM card and then powering the terminal up.



The terminal scans for providers and base stations and reports the results with signal strengths for eac. This can take a few minutes.

You can view each network technology by clicking through them with the button near the top left corner.



For a reliable cellular connection, there should be at least two base stations with signal strength (CSQ) of ten or more for the network to be used. If the signal strength is below that, try to reposition the antenna or the terminal or swap the current antenna for a high gain antenna. Then run the network scan again to check signal strength.

6.7.3 APN

This option lets you enter the cellular Access Point Name (APN) for the SIM card used.

6.7.4 Username

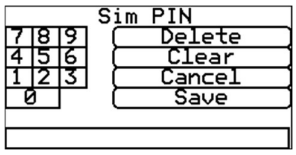
If no username is required, leave it blank. Otherwise, set the cellular username for the SIM card.

6.7.5 Password

If no password is required, leave it blank. Otherwise set the cellular password for the SIM card.

6.7.6 SIM PIN

If the SIM card used has a Pin number, enter it here. If it does not, leave it blank.

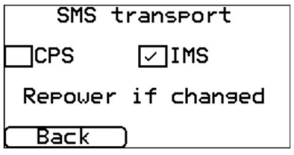


6.7.7 Call barring

To prevent any possibility of blocking the cellular communication paths, incoming calls can be barred.

6.7.8 SMS transport

The SMS transport mode can be set to Cellular Packet Switched (CPS) for use with SIM cards that support 4G but do not support sending SMS messages over 4G. Otherwise, click IP Multimedia Core Network Subsystem (IMS).



If you change this setting, you must power down the terminal and then restart it.

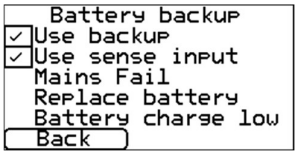
6.7.9 Mode

Allows you to select the desired cellular technology for the terminal. For most circumstances, it is recommended to use the Auto setting.

The options available are:

Auto	The terminal will automatically select the technology depending on the SIM card configuration and the network operator.
Best signal	The technology with the highest signal strength will automatically be selected.
4G	Locked to 4G only. **Note:** that if there is no 4G available, cellular communication will not be possible.
4G preferred	4G is selected if available and above the set minimum signal strength. If there is no 4G available the terminal will revert to 3G or 2G, if available.
3G + 4G	2G will not be used. **Note:** that if there is no 3G or 4G available, cellular communication will not be possible.
2G + 4G	3G will not be used. **Note:** that if there is no 2G or 4G available, cellular communication will not be possible.
2G + 3G	4G will not be used. **Note:** that if there is no 2G or 3G available, cellular communication will not be possible.
3G	Locked to 3G only. **Note**: If there is no 3G available, cellular communication will not be possible.
3G preferred	3G is selected if available and above the set minimum signal strength. If there is no 3G available the terminal will revert to 2G, if available
2G	Locked to 2G only. **Note**: If there is no 2G available, cellular communication will not be possible.
2G preferred	2G is selected if available and above the set minimum signal strength.
Enhanced roaming	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 cellular attachment to connect to the strongest signal identified by the terminal.

6.8 Battery backup:



For terminals with battery backup, the menu ‘Battery backup’ will be shown. Tick the box to automatically use the battery backup when needed.

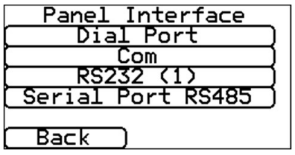
The sense input can be used to prevent the terminal taking power from an external source. For example, if power is taken from an external alarm panel that is itself battery backed, this input can be connected to the DC input of the panel that has been derived from mains power and prevent the terminal taking power from the panel’s own battery.

This screen also shows faults with the battery backup (main fail, batteries need replacing or low battery charge), if present

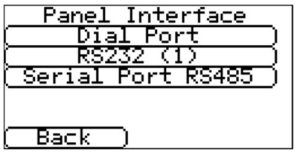
6.9 Panel interface

The range of panel interface options differ for the different products series:

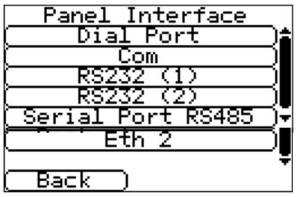
160:



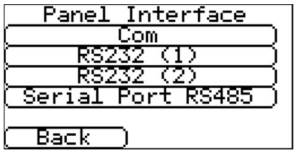
2xx series:



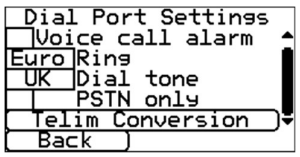
4XX series:



6XX series:

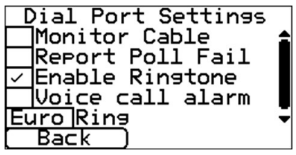


The range of settings that each option has is described below.



6.9.1 Dial port:

The Dial Port sub-menu has several options:



6.9.1.1 Monitor cable

Sets the terminal to monitor the dial port using the 18K resistor (as supplied in the terminal package box). This should be fitted across the A & B terminal of the 2-wire analog interface (alarm panel telecoms module) and allows the terminal to report any status change back to the ARC. Note that this must be fitted at the panel end of the connection to be effective. . This setting must be enabled if compliance with EN50136 is required and the interface to the alarm system is via the dial port.

The ARC will also need to enable the dial port monitoring (Panel) from the ISA software to receive alarm notifications on this status.

6.9.1.2 Report polling fail

Click to enable the terminal to drop the line voltage on the dial port connection if it cannot poll over any configured path to the ARC. This lets the panel 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).

6.9.1.3 Enable Ringtone

This feature lets you enable or disable the terminal simulating the PSTN ring-back tone to the dial port while the connection is being made. Usually this can be left as the default setting but if you are having issues with alarm panels not sending alarms, try turning this off.

6.9.1.4 Voice call alarm

This causes the terminal to send an alarm to the ARC if a call is made via the dial port connection. This alarm is pre-coded as shown in the Default Alarm Message appendix and is in either SIA or Contact ID format depending on the Pin Inputs setup.

6.9.1.5 Ring

If the alarm panel is expecting a ring cadence (pattern of rings and pauses) to detect an incoming call, you can set this to «Euro» or «UK».

6.9.1.6 Dial tone

If the alarm panel is expecting a dial tone when it makes an outgoing call, set this to «Euro» or «UK».

6.9.1.7 PSTN Only

Sets the terminal to route all calls into the Dial Capture port to be routed directly to the PSTN interface, if the EXT2 extension board is fitted. The number dialed is used for the external PSTN connection.

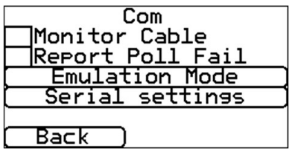
6.9.1.8 Telim conversion

The terminal can support the Telim protocol on the dial capture interface. This screen lets you modify the default Telim to SIA alarm conversion by selecting through the presets or to set to Custom and entering the required SIA code.



6.9.2 COM

Several options can be set for the Com (TTL) connection.



6.9.2.1 Monitor cable

This sets the terminal to monitor the serial port for activity and report any status change back to the ARC.

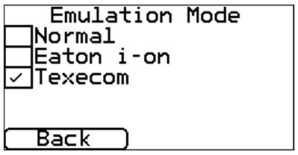
For this to work, the ARC must enable the “serial port monitoring” on the ISA receiver software in order to receive alarm notifications on this status.

6.9.2.2 Report poll fail

This sets the terminal to stop responding to the serial commands if polling has failed. This will then indicate the failure back to the alarm panel thus locally indicating a communication failure (for EN standards).

6.9.2.3 Emulation mode

This sets up the serial port for Normal, Eaton I-ON (Coopers) or Texecom connections. The default is Texecom emulation. For more information on the connection and setup, please refer to separate alarm panel interface documents.

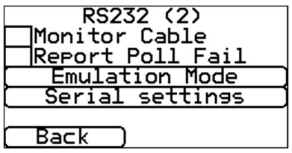


Note: For the Eaton I-ON panel, you will need to use the IRIS-4 CT-interface board separately. Please contact the sales team for further information.

6.9.2.4 Serial settings

This option lets you modify the baud rate and parity of the connection.

6.9.3 RS232 (1)



6.9.3.1 Monitor cable

This sets the terminal to monitor the serial port for activity and report any status change back to the ARC.

For this to work, the ARC must enable the “serial port monitoring” on the ISA receiver software in order to receive alarm notifications on this status.

6.9.3.2 Report poll fail

This sets the terminal to stop responding to the serial commands if polling has failed. This will then indicate the failure back to the alarm panel. This lets the site locally indicate communication failures (for EN standards).

6.9.3.3 Emulation mode

This option lets you select which emulation mode should be used for the RS232 (1).

The DCE and DTE sockets allow for a converter cable for a D-type connector either as a Data Communications Equipment type (DCE), equivalent to that on a modem or as a Data Terminal Equipment type (DTE), equivalent to that on a PC. Cables to convert the header to a 9way D-type can be obtained from AddSecure.

Note: enabling Full (DCE) or Full (DTE) modes will disable the other serial port RS232 (2).

6.9.3.3.1 Normal

This sets the serial port RS232 (1) to basic mode which only uses the TX1, RX1 and 0V screw terminals

6.9.3.3.2 Full (DCE)

This means the Serial Port RS232_1 will now be in full RS232 mode (all control signals) using the DCE header. Please contact the sales team for the relevant cable requirements.

6.9.3.3.3 Full (DTE)

This means the Serial Port RS232_1 will now be in full RS232 mode (all control signals) using the DTE header. Please contact the sales team for the relevant cable requirements.

6.9.3.3.4 Espa

See Emulation Mode Appendix in this document.

6.9.3.3.5 Espa settings

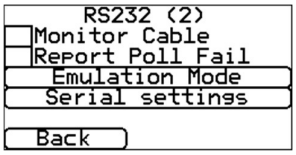
This lets you change the format of the alarms transmitted.

6.9.3.4 Serial settings

This option lets you modify the baud rate and parity of the connection.

6.9.4 RS232 (2)

This is the configuration setting for the second RS232 serial port connections (TX2 & RX2) and has the following configuration options.



6.9.4.1 Monitor cable

This sets the terminal to monitor the serial port for activity and report any status change back to the ARC.

For this to work, the ARC must enable the “serial port monitoring” on the ISA receiver software in order to receive alarm notifications on this status.

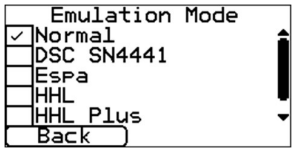
6.9.4.2 Report polling fail

This sets the terminal to stop responding to the serial commands if polling has failed. This will then indicate the failure back to the alarm panel. This lets the site locally indicate communication failures (for EN standards).

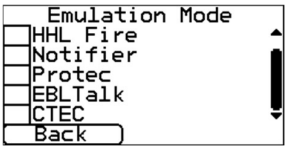
6.9.4.3 Emulation mode: For 4xx and 6xx

This allows you to set up the RS232 (2) port for several connection options for alarm panel specific communications. For ESPA, see Emulation Mode Appendix in this document. For others, panel specific documentation is available from AddSecure.

1



2



6.9.4.4 Serial settings

This option lets you modify the baud rate and parity of the connection.

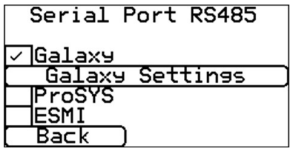
6.9.5 Serial port RS485



The configuration setting for the RS485 serial port has these options:

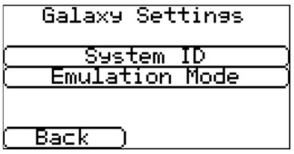
Choose the one you need.

6.9.5.1 Galaxy



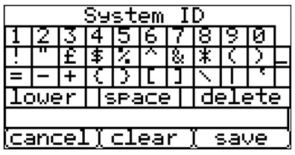
This sets the RS485 bus for Honeywell Galaxy mode where the terminal will automatically emulate one of the galaxy communication modules in the following order: Ethernet, PSTN, External RS232.

6.9.5.1.1 Galaxy Settings



This opens the Galaxy settings screen with two more configuration options:

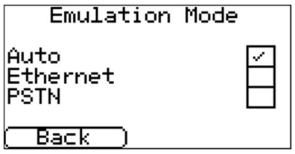
System ID



This lets you enter a system ID independently from the panel that will override the current ID sent by the panel.

To enter the ID, which will override the existing ID, click «clear», enter the ID, then click «save».

Emulation mode



This option lets you select the Honeywell Galaxy RS485 bus communication module emulated.
This provides backwards compatibility with older Galaxy panel software versions that do not support the Honeywell Ethernet module (Galaxy Classic below version 4.00).

The default is Auto (Automatically assigned). This will try the external Ethernet module first. If this is not found, it will try the external PSTN, and finally the external serial modules.

You can also preset the emulated module to be Ethernet or PSTN by clicking the relevant box. This may be needed if, for example, there is already a Honeywell Ethernet module fitted.

6.9.5.2 ProSYS

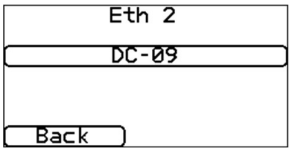
This sets the RS485 bus for the Risco ProSYS bus to allow Upload/Download connections but not alarms. For this to be useable for alarm transmission from the panel, the panel alarm must be connected to the dial port, or to the “pin input” signals.

6.9.5.3 ESMI

This option displays the “ESMI Settings” submenu where you can change settings for ESMI Fire Panel serial interfaces on the RS485 port.

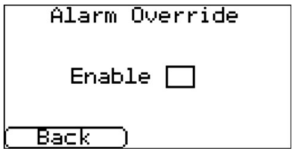
6.9.6 Eth 2

This allows you to set up the terminal for alarm panels connected via Eth2 that communicate using the SIA DC-09 protocol. For more information see the Appendices of this document.



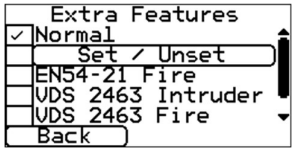
6.10 Alarm override

This lets you set the terminal to override the alarm panel's account number and dialed number with those set in the terminal.

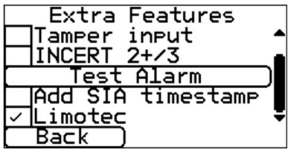


6.11 Extra features

This allows you to set up the special options for the terminal.

1


2

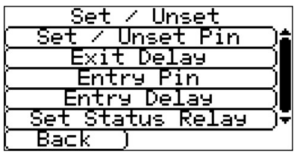

3


6.11.1 Normal

This is the default mode for a terminal.

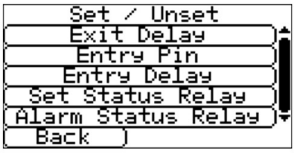
6.11.2 Set / unset

In a normal alarm installation, the terminal is used with an attached alarm panel. However, if the requirements for monitoring are simple, requiring only a few alarm events like set & unset or entry / exit alarms (e.g., ATM monitoring), the terminal can be set up to be a simple alarm panel using the pin inputs.

1


6.11.2.1 Set / unset pin

Configuration options for the Set/Unset pin.

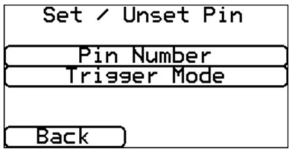
2


6.11.2.1.1 Pin number

Allocate which pin is for the set and unset signals.

6.11.2.1.2 Trigger mode

This sets the trigger mode to “normal”, which means that the unit is unset when the input pin is “open circuit”. This method is suitable for an external physical switch such as a key-switch.



The trigger mode can be set to “pulse”, which means that a pulse on the set/unset input toggles the set/unset status. This is suitable for an external device such as a proximity tag reader.

6.11.2.2 Exit delay

This option lets you set the exit delay timer. The default is 10 seconds.

6.11.2.3 Entry Pin

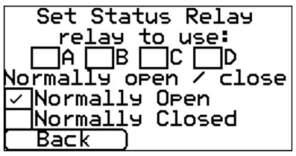
This option lets you allocate which pin is to be used for the entry signal.

6.11.2.4 Entry delay

This option lets you set up the entry delay timer. The default is 10 seconds.

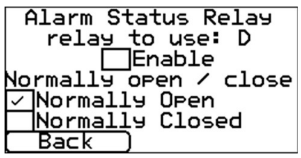
6.11.2.5 Set status relay

This option lets you allocate which relay output is to be the set/unset status indicator and to set the default state to “Normally open” or “Normally closed”. The default is “Normally open”.



6.11.2.6 Alarm status relay

This option lets you enable relay D as the alarm status indicator. This means that if any (enabled) pin Inputs are in an alarm state, the relay will change state according to what the default state is set to (default is normally open).



6.11.3 ENS4-21 Fire

Sets the IRIS-4 4xx to EN54-21 Fire conformances. For further details, see chapter 7 “Installation for EN54-21 conformance”.

6.11.4 VdS 2463 Intruder

Sets the terminal to VdS 2463 Intruder conformances. For further details, see chapter 8 “Installation for VdS 2463 Compliance”.

6.11.5 VdS 2463 Fire

Sets the terminal to VdS 2463 Fire conformances. For further details, see chapter 8 “Installation for VdS 2463 Compliance”.

6.11.6 ILKA mode + PSU

Sets the terminal to customer specific PSU monitoring with predefined threshold and dial port settings.

6.11.7 ILKA mode

Sets the terminal to customer specific PSU monitoring with predefined threshold and dial port settings.

6.11.8 Tamper detection

Enables or disables tamper detection on the terminal, which lets you connect an external tamper switch, for example, for the cover of the terminal enclosure.

6.11.9 INCERT 2+/3

Enables terminals that support dual path IP communications to support Belgian INCERT T015

The INCERT standard T015 requires Grade 2+ and Grade 3 installations to signal alarms over both paths.

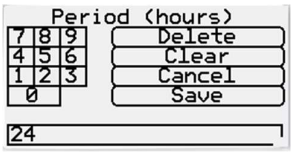
When the alarm format is SIA, the terminal will also insert a SIA Path modifier (pt) on test alarms (event codes RX and RP) to show the path over which the alarm is sent:

- 01 = Ethernet
- 02 = Wi-Fi
- 03 = Cellular

Note: This function only works over Ethernet and cellular and not PSTN.

6.11.10 Test alarm

Where the IRIS terminal is not connected to an alarm panel that can itself generate a regular test alarm (e.g., when inputs are used), it can be convenient for the terminal to generate a regular test alarm. This gives the ARC a consistent way to monitor end-to-end connectivity across many installations.



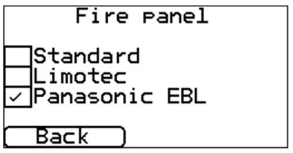
6.11.11 Add SIA Timestamp

This option causes the terminal to append the date and time to any SIA format messages generated internally, including those generated from activity on the Pin Inputs. The date and time will be correct only if the terminal is connected to an ISA 4 system at the ARC as this can send the date and time to a terminal.

Note: The timestamp cannot be enabled if the PSTN transmission path is selected, likewise the PSTN transmission path cannot be selected if timestamp is already enabled.

6.11.12 Fire panel

This menu sets up operation for specific types of Fire panel. The following will be set:



Limotec

- EN54-21 Fire mode (this setting cannot be changed while in this mode).
- Input zone numbers from 9901 9916 instead of 01 to 16.
- Espa End to end Acknowledge mode (this setting cannot be changed while in this mode).

Panasonic EBL

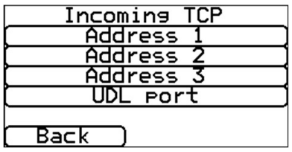
- EN54-21 Fire mode (this setting cannot be changed while in this mode).
- Input events for inputs 1 and 2 set to UA/UR rather than FA/FR and FT/FJ.
- Espa End to end Acknowledge mode off.

Standard

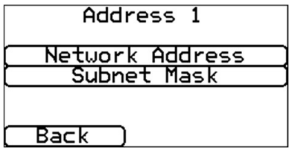
- Input events are restored to SIA factory default settings.
- Espa End to end Acknowledge mode off.

6.12 Incoming TCP

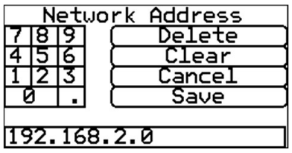
This lets you limit incoming TCP calls to the terminal serial port to up to three source IP addresses. If all the addresses are left blank, all calls are allowed.



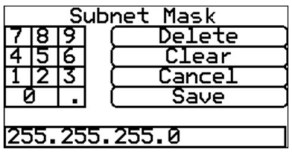
Each source also has an associated Subnet mask, so a range of addresses from sources on the same subnet can also be allowed to connect. This can be helpful if you have several computer systems that may need to make remote connections at different times, rather than having to use just one system every time.



The example shown shows where IP addresses 192.168.2.0 to 192.168.2.255 are allowed to connect. The network address should be set to the lowest IP address in the range.



If you want just a single IP address to be allowed to connect, set the Network Address to this and the Subnet Mask to 255.255.255.255.



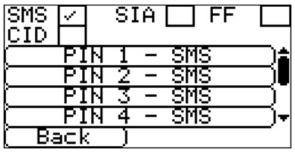
This menu also allows you to set the TCP port number to be used for incoming Upload/Download (UDL) calls. These calls are routed to attached alarm panels through the appropriate interface (serial, RS485 etc.), depending on the alarm panel type attached and the terminal settings.

6.13 Pin inputs

This lets you set the alarm format for the pin inputs to SMS, SIA, Fast Format (FF) or Contact ID (CID).

Note: You can select one alarm format, see subsections below, for the pin inputs (SIA, FF or CID) and then also setup individual pins to be SMS messaging if required.

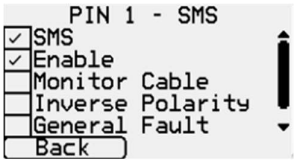
When changing the alarm format, you will receive a warning message indicating that all current pin inputs will be setup for this alarm format and returned to the default settings shown below, as they cannot be set up to different alarm formats.



6.13.1 Common options

These options are available for all pins for all alarm formats.

6.13.1.1 SMS



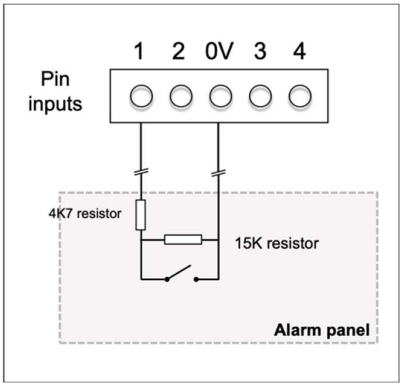
Selects SMS format for this pin input when ticked.

6.13.1.2 Enable

Enables this pin input when ticked.

6.13.1.3 Monitor cable

Monitors tamper detection when ticked. This requires resistors to be fitted at the alarm panel end of the cable to enable the terminal to detect cable faults and/or tampers.



Wire the alarm outputs from the panel to the position in the diagram marked as a switch – open is the alarm condition and closed is the restore condition.

6.13.1.4 Inverse polarity

When ticked, this reverses the function of the inputs “Set” and “Restore”. This will mean that the “Set” will be a closed circuit and the “Restore” will be an open circuit.

6.13.1.5 General Fault

When ticked, the pin’s fault condition is indicated on the General Fault relay. Messages can also be sent to notify the ARC.

When in EN54-21 fire mode, this option is labelled Power Fault, for use with the optional DC Combiner board wired to pins 3 and 4, as required when the power supply is external to the terminal’s enclosure. When

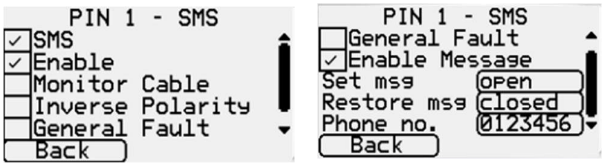
ticked, the DC Combiner power fault will be indicated on the General Fault relay. Messages can also be sent to notify the ARC.

6.13.1.6 Enable Message

When ticked, the transmission of the messages is enabled.

6.13.2 Alarm format SMS

Selecting SMS format for all pins or ticking this box for a specific pin will mean that on input “Set” (open circuit) and input “Restore” (closed circuit), the terminal will send the configured SMS text for the set or restore message to the configured phone number.



6.13.2.1 Phone number

This option lets you enter the phone number to which the SMS message will be sent.

6.13.2.2 Set msg and Restore msg

Enter the Set and Restore text messages to be sent. No message is sent for an entry that is blank.

6.13.3 Alarm format SIA

On input “Set” (open circuit) and input “Restore” (closed circuit), the terminal will send SIA alarm protocol messages for that input.



6.13.3.1 Set msg and Restore msg

Here you can input the “Set” and “Restore” messages in the correct format as defined in SIA format protocol SIA DC-03-1990.01(R2003.10). The default "Set" and "Restore" event codes are in the table below.

These defaults can be changed and text descriptions to be sent with the SIA alarm code (under SIA level 3 alarm protocols) can be added. If you exceed the maximum number of characters for the combined set and restore messages supported by the terminal, a warning will be shown.

Text descriptions can be added by adding ^ before and after the text. For example, to add the text "Fire" to the message SIA code "NFA01", input "NFA01^FIRE^" into the touchscreen.

These alarms are pre-coded as shown in the Default Alarm Message appendix.

6.13.4 Alarm format FF

Selecting FF for the inputs means that the inputs will send a specific Scancom FF alarm protocol message on the event and restore for that input.



6.13.4.1 Alarm

Signal	Event Type	Description
1	New alarm	The alarm triggering input is active and has not yet been reported.
3	New restore	The alarm triggering input has returned to its quiescent state from the alarm state.

This sets the input to be an alarm triggered by an input.

5	Not in alarm	The alarm triggering input is quiescent.
6	In alarm	The alarm triggering input is active and has been reported.

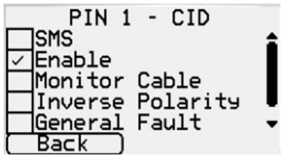
6.13.4.2 O/C (open/close)

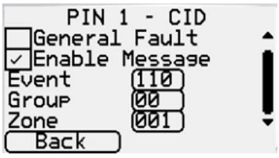
This option sets the input to be an O/C input.

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

6.13.5 Alarm format CID

This setting means that the pin inputs will cause a specific Ademco® Contact ID format alarm protocol message to be sent. This message includes an event code, a zone number and a group number.





6.13.5.1 Event

Here you can input the 3-digit event code for this input, e.g., 110 = Fire.

To determine which event code is to be used, refer to the digital communication standard "Ademco® Contact ID Protocol - for Alarm System Communications SIA DC-05-1999.09"

6.13.5.2 Group

Here you can input your pre-defined 2-digit group or partition number.

Use the value 00 if no specific group or partition information applies.

6.13.5.3 Zone

Here you can input your pre-defined 3-digit zone number (event reports) or user number (Open / Close reports). Use the value 000 if no specific zone or user information applies.

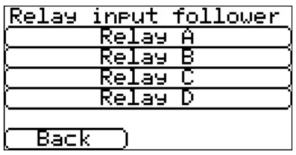
6.13.5.4 Default CID Set/Restore event codes

These alarms are pre-coded as shown in the Default Alarm Message appendix.

6.14 Relays

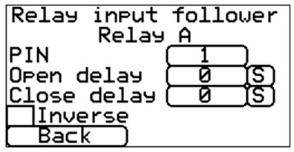
This option lets you configure the relays.

6.14.1 Relay input follower

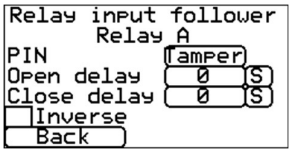


This feature lets the terminal relay outputs be set to follow a pin input, with a delay if required. Normally a relay will open if the associated input goes open circuit, and vice-versa, but this can be inverted if required.

Touch on the PIN number to select the pin required. If 'Tamper' is selected, the relay will follow the state of the case tamper. A setting of '0' switches this feature off.



Note: Do not use this feature for a relay with another purpose, e.g., communications path trouble reporting.



6.14.2 Relay SMS activation

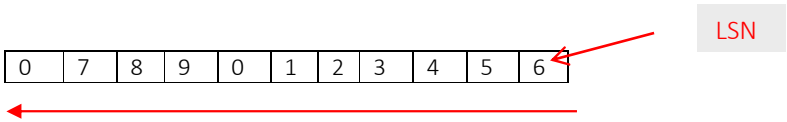


The terminal lets each relay be activated or deactivated with a predefined SMS message from a mobile phone.

6.14.2.1 Phone number

This option sets which calling device (mobile phone) may 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 comparison begins at the least significant number (LSN) and then works backward as shown in the example below using the phone number 07890123456:



Starting from the LSN 6, you can work backward to compare the CLI number. For example, you can enter "56" which will allow all phone numbers with a CLI ending in 56.

You need to confirm which CLI number is being received, by using your mobile phone to receive the call, thereby displaying the incoming CLI number.

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

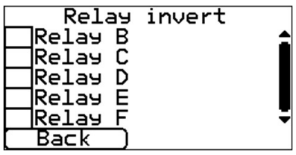
6.14.2.2 Activation msg

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

6.14.2.3 Deactivation msg

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

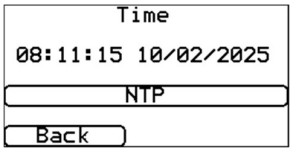
6.14.3 Relay invert

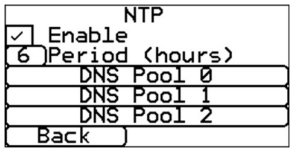


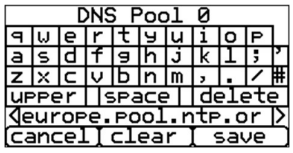
This option lets you reverse the way relays work so you can reverse the normal state of a relay from open to closed and vice versa.

This might be required depending on the external equipment being connected.

6.15 Time





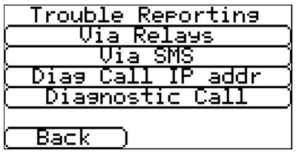


The terminal contains a Real Time Clock (RTC) that needs to be synchronized after every power up or repower. In a normal situation this will be done when the terminal connects either to an IRIS Secure Apps receiver or a DC-09 receiver. However, before this is possible, the terminal will synchronize time with a pool of NTP servers.

By default, the pool uses is “europe.pool.ntp.org”, but this can be changed, for example if this pool is not reachable from the current terminal location, or it is not appropriate for some other reason.

Note that once time has been received from an IRIS Secure Apps or a DC-09 receiver, synchronisation with this pool l is disabled.

6.16 Trouble reporting

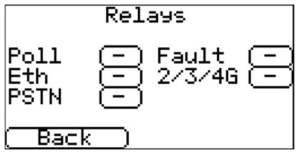


Trouble reporting allows setup of the reporting of communication faults via relays or SMS and diagnostic calls to be made over an IP communication path (Ethernet or cellular).

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

Below is a breakdown of these individual setup options:

6.16.1 Via relays



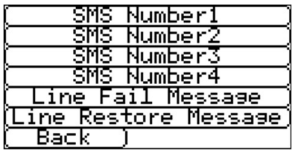
It is possible to enable or disable the terminal toggling the state of the relays to indicate communication path failures. This is intended to signal failures back to the panel inputs, so the site has local indication of a communication failure (for EN standards). The terminal allows the choice of which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

Click on the relevant box for the relay to be used for indicating this failure.

Note: Each relay can be used for multiple path fault indications.

The «Fault» option allows reporting of system fault indications via the selected relay. For a list of these faults, see section 9.1. “Trouble report”

6.16.2 Via SMS

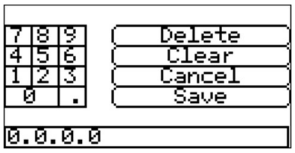


The terminal can send SMS messages via the cellular network to indicate communication or line faults.

There are 4 SMS phone numbers that can be set up as destinations for these SMS messages.

Click on the relevant option and enter the phone numbers, then click «Save», then «Back».

6.16.3 Diagnostic call IP address



This menu allows the IP address of the PC/laptop running the IRIS Toolbox software to be entered so outbound TCP/IP diagnostic calls for remote diagnostics can be made.

6.16.4 Diagnostic call

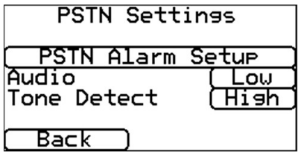


This option lets you make diagnostics calls back to the IP address entered above for remote diagnostics to the IRIS Toolbox software.

The first time this is used, the one-time password for this remote connection will be displayed. Take note of this password, as it may need to be passed on to the operator of the IRIS Toolbox software.

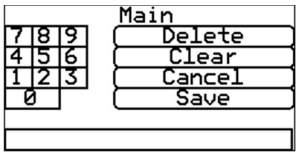
Click «Diagnostic Call» once the password has been passed onto the operator and they are ready to receive the call.

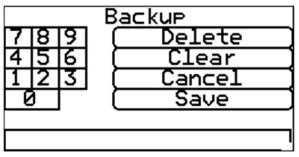
6.17 PSTN Settings



If PSTN was selected, the PSTN Settings menus lets you adjust how alarms are handled over a PSTN connection.

6.17.1 PSTN Alarm Setup





This lets you change the phone numbers of a main and backup receiver the terminal will use to send alarms overa PSTN line.

6.17.2 Audio

Sets the audio level of alarms sent over PSTN and the expected level of alarms received over PSTN.

6.17.3 Tone Detect

This lets you adjust the audio level of tones received over PSTN.

6.18 Language

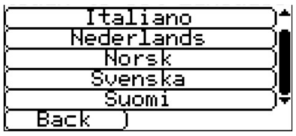
The terminal supports several languages.

Select your preference.

1



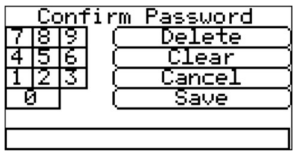
2



6.19 Installers password

To comply with EN50136-2, you had to change the default installers password, 111111, when you first accessed the Installers Menu. This option lets you change the password again.

Follow this procedure:

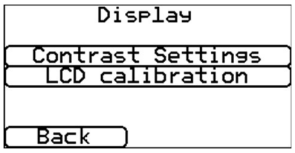


1 Input the new password and click «Save».
You will be asked to confirm the password.

2 Confirm the password, then click «Save».

6.20 Display

For terminals with a physical touchscreen, this option lets you alter the contrast and recalibrate the touchscreen if required.

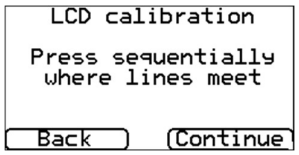


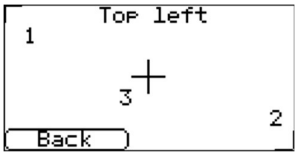
Click «Contrast Settings» or «Touch Calibration» and follow the on-screen prompts.

6.20.1 Touchscreen calibration

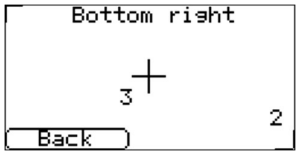
This can be done only on a physical touchscreen, not a virtual one. Follow this procedure:

1 You will be presented with three screens in sequence. In each screen, click on the center of the crosshairs:

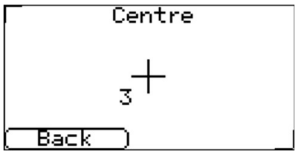




1

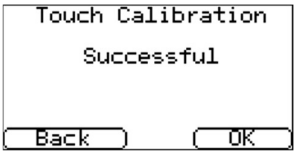


2

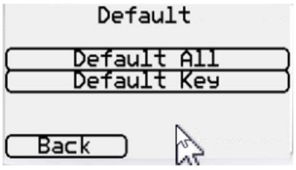


3

2 The screen will then display “Successful”.



6.21 Default



If at any point a default of the terminal is required, use these options.

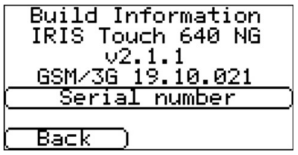
To reset the terminal to manufacturing defaults, click «Default All» and confirm that the terminal is to be defaulted.

To only reset the security key used by the ARC, click «Default Key». Then request the ARC to re-synchronize which will create a new key.

6.21.1 For terminals with an AP or SW button (this is not part of Settings menu)

1. Power down the terminal.
2. Press and hold down the button.
3. Re-apply power while still holding down the button for another 10 seconds. This resets the terminal to manufacturing defaults.

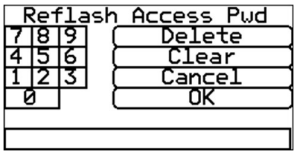
6.22 Build information



Displays the product name, the IRIS-4 software version and the cellular module version.

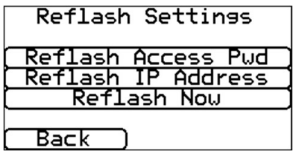
Click on various items to see the information.

6.23 Reflash



This menu controls the reprogramming of the terminal to the latest software.

To enter this menu, you must enter the reflash password. By default, this is '111111' and in this case it must be changed, to comply with EN50136-2.

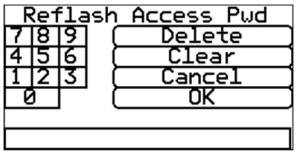


Note: If required, the ARC can run a reflash remotely.

6.23.1 Reflash Access Password

To change your password, follow this procedure:

1. Enter your new password.
   If you need to redo your typing, click «Clear» and start again. When you are done, click «Save».
2. Confirm your password and click «Save». This will return you to the "Reflash Settings" screen.



6.23.2 Reflash IP address

The default reflash IP address is 195.59.117.164 and links to the AddSecure reflash server. This server is available 24/7 and is kept constantly up to date with the latest software.

This option lets you enter a different IP address when required. For example, when a customer will only allow their network to communicate back to the ARC (network/IP address), and/or when the ARC has their own reflash server installed.

6.23.3 Reflash now

This immediately starts a reflash and then displays a status window indicating progress.

7 Installation for EN54-21:2006 compliance

7.1 Introduction

Some of the IRIS-4 range of terminals are certified as compliant with the European standard EN54-21:2006 – Fire detection and fire alarm systems - Alarm transmission and fault warning routing equipment". To comply with this standard there are conditions to which the installation must comply. These conditions apply both to the terminal and to the fire CIE. This guide describes these conditions.

Note: if these conditions are not complied with, then the installation will not be compliant with EN54-21:2006.

All other aspects of the installation are covered in the other sections of this document.

7.2 General description of the equipment

IRIS-4 terminals are used to take alarms from fire CIE and transfer these reliably over IP telecommunication networks such as broadband and cellular. The interface of the CIE uses inputs to the terminal and outputs from the terminal.

Depending on the terminal type, backup communication over 4G/3G/2G or PSTN is also provided.

All communications paths can be constantly monitored (supervised) so any failures are reported to the ARC.

The terminals comply with both transmission system types defined in Annex A of EN54-21:2006:

Type 1: signaling path is Ethernet (e.g., broadband), cellular or Ethernet with 4G/3G/2G backup.

Type 2: one of the signaling paths is PSTN (e.g., PSTN only, cellular with PSTN backup or Ethernet with PSTN backup).

7.2.1 Technical specification

Please refer to chapter 11 “Technical Specifications” for details on the appropriate IRIS-4 terminal.

7.3 Installation, configuration, and commissioning

7.3.1 Monitoring requirements

The ARC should set up the monitoring reporting times (i.e., poll period + poll overdue period) of the site, as follows:

For Type 1	80 seconds or less.
For Type 2	24 hours or less

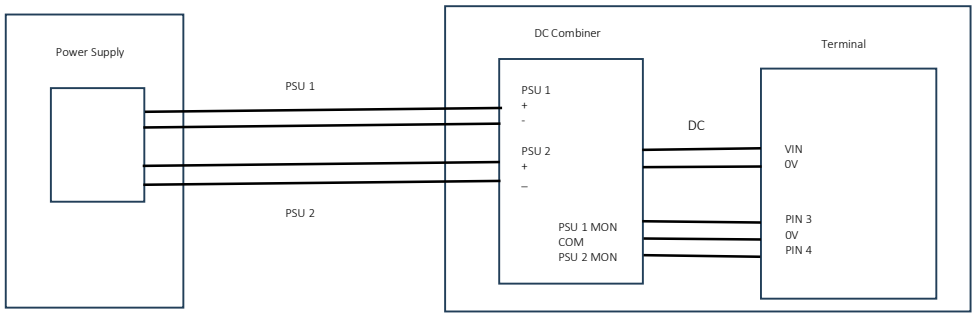
7.3.2 Requirements for the installation

General installation instructions are in sections 4 “Basic setup” and 5 “Configuring the terminal”. The following additional requirements are for EN54-21:2006 compliance:

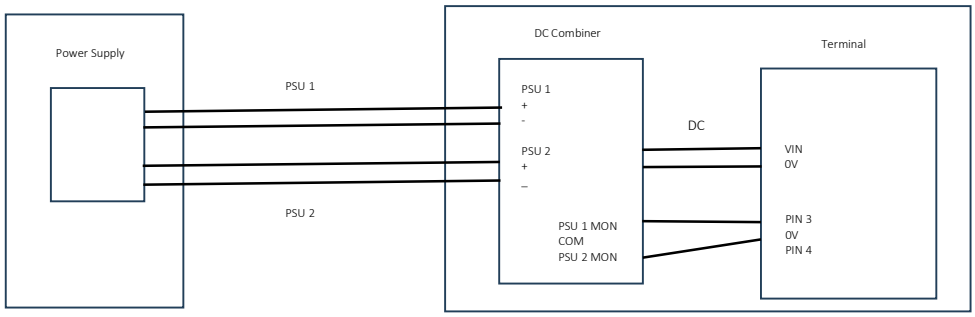
- The Fire CIE must be able to indicate fire signal acknowledgments and fault conditions as visual indications driven by the outputs from the terminal, as described below. These indicators must comply with EN54-21:2006.
- The terminal should be powered from an EN54-4 compliant power source, such as a model from the Elmdene ST range.
- The terminal must be mounted in an Access Level 3 protected enclosure compliant with the requirements of either EN54-2 (Fire detection and fire alarm systems – CIE) or EN54-4 (Fire detection and fire alarm systems – Power supplies).

If there is not sufficient space to mount the terminal within the existing CIE or power supply cabinet, an alternative is to use a separate EN54-4 compliant power supply cabinet. A model from the Elmdene ST range is recommended.
If the terminal enclosure used is not actually used to house the power source, then the terminal enclosure must be mounted against the power source enclosure so the power cable between the two cannot be the subject of tamper or accidental damage.

If the terminal enclosure and power supply enclosure are separated, the optional DC Combiner board must be housed within the terminal enclosure to accept the power supply wiring which must be externally protected against tamper or accidental damage between the enclosures. The Power Fault function of pins 3 & 4 must be selected to indicate the power supply fault conditions, as detected by the DC Combiner board.



For situations where pin 4 is required for other purposes, a simplified arrangement can be used which indicates a power fault without identifying explicitly whether PSU 1 or PSU 2 is in fault. In this case, only pin 3 must be configured for the Power Fault function.



- The interface to the fire control equipment should be via terminal inputs (pins) and relay outputs, as described below. The terminal's "Dial Capture" interface that emulates a PSTN line should not be used as it does not provide adequate status signaling back to the control equipment. Serial communication lines can be used for more information but must not be the primary signaling method.

7.3.3 Configuration requirements

Run through the Installation Wizard, see chapter 5 "Configuring the terminal" in the normal way. Make sure that for pins 1 and 2, the Pin input alarms are configured for SIA or CID and are enabled. If a separate enclosure for the fire panel is being used, monitoring for tampers must also be enabled.

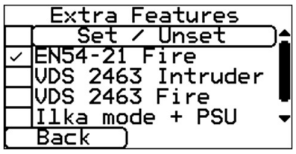
If an IRIS-4 4xx EXT1/EXT2 Expansion board is installed, you must use pins 9 & 12 for monitoring of the PSU. Confirm these are ticked in the Installation Wizard, see section 5.6.3 "Pin Alarms".

Other alarm inputs can also be enabled if required from the Settings menu, but do not change the above settings for inputs 1 or 2 or inputs 9 and 12 (if used).

Note: After the EN54-21 Fire mode is selected, it is essential that no other changes are made to the settings for Pin 1 or Pin 2 or to the Relay A or B outputs as this may invalidate conformance to EN54-21:2006.

Use the Settings «Extra Features» menu to set the 'EN54-21 Fire' mode.





When this mode selected, input pins allocated for the fire application are as follows:

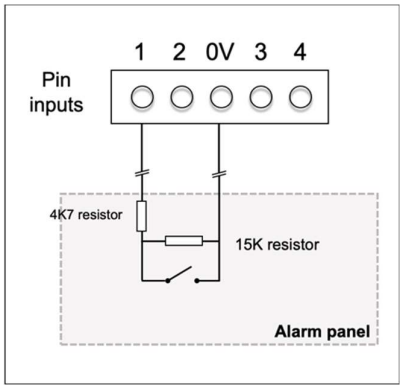
- Input pin 1 – Fire Alarm/Restore – open circuit = alarm
- Input pin 2 – Fire Alarm Fault/Restore – open circuit = fault
- Input pin 9 – AC Power Trouble/Restore – open circuit = fault
- Input pin 12 – System battery Trouble/Restore – open circuit = fault

Note: For inputs 9 & 12 you will need the expansion board EXT1 (12 pins) or EXT2 (12 pins + PSTN) fitted.

The alarm codes generated by these inputs are:

SIA:	Pin 1 FA01/FR01
	Pin 2 FT02/FJ02
	Pin 9 AT09/AR09
	Pin 12 YT12/YR12
	If Limotec mode is selected, the zone numbers are changed to 9901 etc.
Contact ID:	Pin 1 Event 110 group 0 zone 1
	Pin 2 Event 300 group 0 zone 2
	Pin 9 Event 301 group 0 zone 9
	Pin 12 Event 302 group 0 zone 12

If the terminal is not mounted within the fire panel, tamper detection on the inputs must be enabled and end of line resistors should be fitted for detection of open circuit or short circuit faults:



Wire the alarm outputs from the panel to the position in the diagram marked as a switch – open is the alarm (pin 1) or fault (pin 2) condition and closed is the restore condition.

The terminal provides relay outputs for these indications which should be wired to corresponding inputs to the CIE.

1. Relay B – Indicates that an acknowledgment to a fire alarm signal has been received from the ARC. This relay is normally open and closes when the acknowledgment is received. It will be opened when the fire alarm restore signal is sent.
2. Relay A – Fault indication, including no acknowledgment received, loss of power to terminal, transmission network fault, software watchdog restart or configuration memory fault. This relay is normally closed and opens if any of the above fault conditions are present.

Confirm receipt by the ARC for these events: Test alarms, fault activations, and restores events.

When installation has been completed and correct operation confirmed, please confirm that either the enclosure is appropriately marked, or a label that indicates EN54-21 compliance and product type is fixed to the outer surface of the enclosure and is clearly visible.

8 Installation for VdS 2463 Compliance

8.1 Introduction

AddSecure IRIS-4 alarm over IP terminals have been tested and certified by VdS in Germany to comply with the VdS2463 (2007) standard, “Alarm Transmission for alarm signals (ATE)” and have been given a “G” approval rating.

The IRIS-4 models certified to VdS2463 and for which this guide is applicable include IRIS-4 400, 420 and 440. For compliance with this standard, the installer must set the terminal to operate in one of:

- VdS Intruder mode
- VdS Fire mode.

8.2 Installation

AddSecure provides a special VdS compliant enclosure and wiring kit that includes:

- Mounting points for the terminal.
- A tamper proof enclosure.
- A tamper detection switch.
- Termination connector blocks and sense resistors for the connection and monitoring of the inputs from the alarm system.
- An external relay for fire applications.
- Cable ties for strain relief.

The IRIS-4 terminal **must** be used with this enclosure and powered from the Intruder Alarm System Alarm Control and Indicating Equipment (IAS-CIE). This additional power consumption must be considered when calculating the standby duration.

Note: If these conditions are not followed, then the installation will not comply with VdS2463.

For VdS 2463 compliant installations, the terminal must be set to use only the pin inputs. The dial capture (2 wires) interface cannot be used as it is not compatible with the VdS terminal protocols.

The terminal can be set to operate in conformance to VdS 2463 in either VdS Intruder or VdS Fire mode.

Follow this procedure to set the pin inputs for these modes:

1 Follow the instructions in chapter 4 “Basic Setup” and chapter 5 “Configuring the terminal” to configure the terminal.

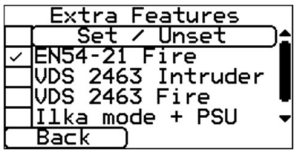


2 Go to Settings «Extra Features» menu.

3 Tick «VdS 2463 Fire» or «VdS 2463 Intruder» as required.

4 Go to Settings Pin Inputs.

5 Enter the appropriate messages and configurations for the pins to be used, see section 6.13 “Pin inputs”.



6 Enable tamper detection on all used input pins, except pin 1, to enable monitoring of the inputs with the end of line resistors (see section 6.13).

7 Disable unused pins, then click «Back».

Note: To conform to the VdS standard, shielded cables shall not be used for interconnection with the Intruder IAS-CIE.

8.3 VdS mode operation

In VdS modes, these changes are made to the way the terminal functions:

- Voltage thresholds on the inputs that determine the alarm and restore detection levels are changed to conform to VdS2463 requirements.
- Tamper detection parameters on the inputs are changed to conform to VdS2463 requirements.
- Ethernet failure detection de-bounce time is 20s (normally 30s).
- The polling period over Ethernet or cellular is fixed at 8s, despite the rate requested by the ARC.
- Relay A indicates an ATE fault, such as a transmission path failure, by going open circuit.
- Relay B indicates a transmission failure of an input pin alarm by going open circuit.
- Relay C indicates an ATE fault, such as a transmission path failure, by going closed circuit (Intruder mode) or open circuit (Fire mode).
- In the VdS Fire mode only, Relay D indicates successful transmission of alarms on inputs 2 and 10 (which is designated for Fire) by going open circuit.

8.4 VdS Intruder Applications

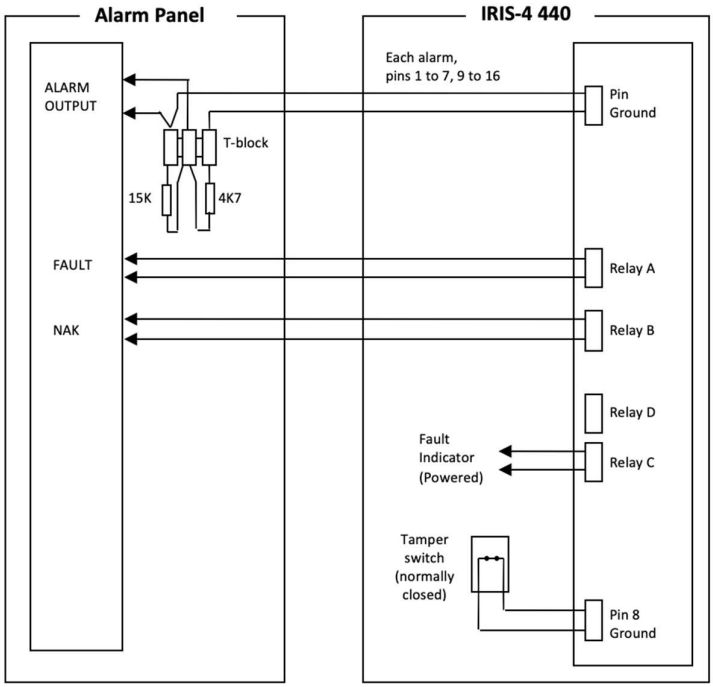
The relays are assigned as follows:

Relay A:	ATE fault (normally closed)
Relay B:	NAK (normally closed)
Relay C:	Fault indicator (normally open) – to be connected to the indication device selected for this installation.
Relay D:	User defined

The input pins are assigned as follows:

Pins 1 to 7, 9 to 16:	User definable
Pin 8:	Tamper switch

The intruder alarm signaling shall be connected as illustrated below:



8.5 VdS Fire Applications

The relays are assigned as follows:

Relay A:	ATE fault (normally closed)
Relay B:	NAK (normally closed)
Relay C:	Fire ATE fault (normally closed)
Relay D:	Fire Alarm Receiving Equipment (ARE) ack (normally closed)

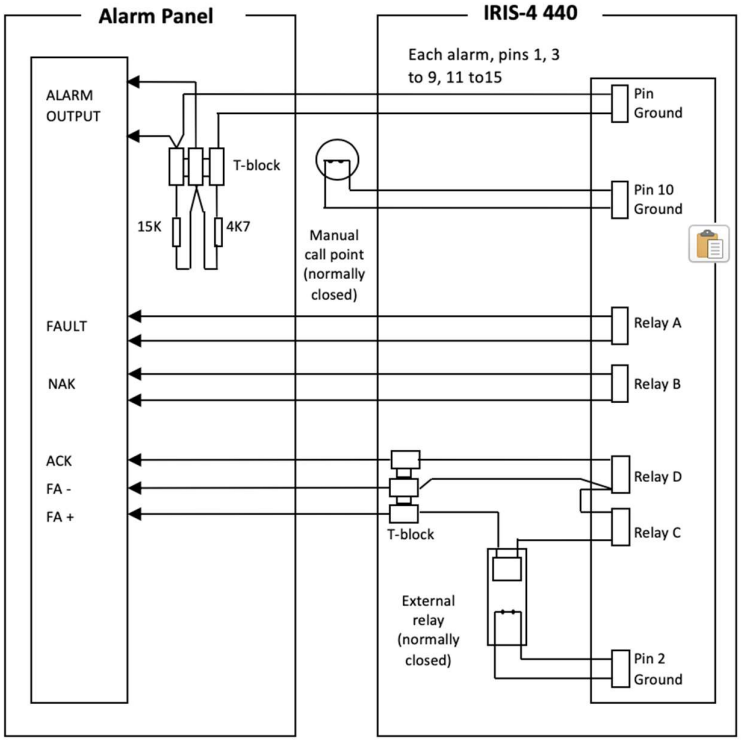
The input pins are assigned as follows:

Pins 2 to 16:	User definable
Pin 1:	Fire

An additional external relay with a voltage rating that matches the voltage of the FASCIE equipment is required:

For 12V equipment:	relay item = OMRON G2R-1-T 12VDC
For 24V equipment:	relay item = OMRON G2R-1-T 24VDC

The fire alarm signaling shall be connected as illustrated below:



8.6 Conformance to VdS2463

For conformance to the VdS2463 standard, the following must apply:

1. Installation should conform to the instructions set out above.
2. Access to all configuration parameters on the terminal, including the addresses of the Alarm Receiving Equipment (ARE) is restricted by use of an installer password. A default installers password (111111) is set as a factory default. This must be changed to another 6-digit number, preferably during installation, or later.
3. Shielded cables should not be used for interconnection with the IAS-CIE.
4. Faults on the inputs to the terminal that act as interfaces to the alarm system will be reported to the alarm receiving equipment as SIA code NT9107, and a restore as SIA code NR9107. Note these codes can be modified on the alarm receiving equipment if so required.
5. If the terminal shares IP transmission facilities with other systems, this should be arranged so that routing of messages to and from the terminal is given priority higher than other messages.
6. The status of the terminal inputs that act as interfaces to the alarm system is sent to the ARE whenever the terminal is started or restarted. These are indicated as either “activated” or “not activated” and can be viewed by the operator of the ARE as required.
7. The serial communication lines must not be the primary signaling method. They may, however, be used for additional information.

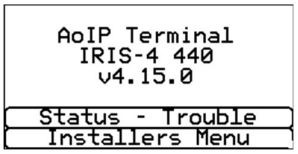
Remote activation of relays via the ISA receiver at the ARC is prohibited when in VdS mode.

.

9 Trouble reporting and test

9.1 Trouble report

If there are problems with the terminal installation, these will be shown under the option “Status - Trouble” on the welcome screen as trouble reports. This chapter explains the possible trouble reports that can be displayed.

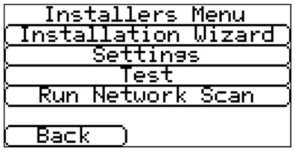


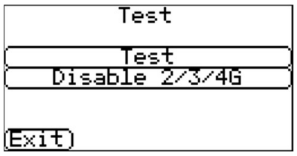
Trouble Report	Explanation
Ethernet disconnected	Not connected to the Ethernet network. Action: check the Ethernet cable and cabling all the way through to the other end (Router / Switch).
Wi-Fi disconnected	Not connected to the Wi-Fi network. Action: check that the Wi-Fi router is working satisfactorily.
Ethernet polling fail	Unable to poll via the Ethernet network to the ARC’s ISA receiver system. Action: check ARC IP address, confirm Ethernet router external WAN connection and firewall setup.
Wi-Fi polling fail	Unable to poll via the Wi-Fi network to the ARC’s ISA system. Action: check the Wi-Fi router is working satisfactorily and that it connects to the Internet.
PSTN not connected	Not connected to the PSTN network. Action: check all the connections in the PSTN wiring.
Not registered	Not able to register to the cellular network which normally means the SIM card has been disabled. Action: check with SIM provider.
2/3/4G Polling fail	Unable to Poll via the cellular network to the ARC’s ISA receiver system Action: check ARC IP address, SIM card is enabled for cellular machine-to-machine data (M2M) and Access Point Name (APN) is correct.
SIM card not fitted	SIM card not being seen in the IRIS-4 4xx unit Action: check that the SIM card is correctly fitted, and that the connection is OK.
SIM pin number required	SIM card has been setup for a Pin number and no SIM PIN entered in configuration Action: Confirm the correct SIM PIN with the SIM provider and enter.
SIM Pin number error	Current SIM PIN entered in the configuration is invalid Action: confirm correct SIM PIN with SIM provider and confirm entered correctly.
Poll failed	The terminal cannot poll over any path Action: check correct ARC IP address entered, and communication paths setup.
Pin Fault on pin**	Indicates that the terminal has been set to monitor for tampers and is in an open or short circuit tamper condition. Action: check cable/resistors connections.
Fault on serial port	The terminal is setup to monitor serial but is seeing no activity on the serial connection Action: check setup of the terminal / panel and physical connection.
Fault on dial port	The dial port is showing a fault, either open or short circuit. Action: check that the 18K sense resistor is correctly fitted across the two-wire connection to the alarm panel.
Fault on RS485	The RS485 connection is not working satisfactorily. Action: check the RS485 connection to the panel.

Fail to communicate (FTC)	A terminal input change has occurred, and this event failed to communicate to the ARC. Action: 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 receiver fault).
EEPROM	The terminal has a possible hardware issue and cannot see the EEPROM. The EEPROM stores all local parameters for protection against power failure.
Tamper detection	Tamper switches or case tamper input has been activated. Action: check enclosure for incorrect fitting.
Replace batteries	The batteries have failed the load/health test, performed automatically by the terminal, indicating a lack of storage capacity. Action: replace batteries
Low battery	The batteries are discharged and will soon cease to power the terminal. Action: Ensure mains power is restored and start a full battery charge.
Mains fail	The mains power supply has failed. Action: troubleshoot the mains power supply and switch back on.

9.2 Test

This option tests communication paths and is available directly from the Installers Menu. Click «Test» to access the test options.





9.2.1 Test

The Test option checks polling and alarms on the enabled communication paths. The table below explains the tests that can be carried out and possible errors. Click «Test» to start these tests.

Tests	Results and explanations
Checking Ethernet	Connected: Confirms that the terminal is connected to the Ethernet network. Disconnected: Means that the terminal is not connected to the Ethernet network Action: check the Ethernet cable and cabling all the way through to the other end (Router/Switch).
Checking IP address	IP address OK; Confirms the terminal has a valid IP address No IP address: Check whether DHCP/fixed IP is correctly configured.

Tests	Results and explanations
Test polls	These can be carried out for Ethernet, cellular and Wi-Fi network interfaces. Successful: The terminal successfully polled the ARC ISA receiver system over the network. Polling disabled: Configured not to poll over the network; check ARC IP address and account number entered. Connection failed: did not connect to ARC. Action: check that the ARC IP address is correct and confirm that the router's external WAN connection and firewall are set up. Connection made, poll fail: Connected to the ARC ISA but rejected. Action: check that the correct account number has been configured at the ARC ISA receiver and that the correct account number is entered in the terminal. Connection made, authentication failed: Connected to the ARC ISA but rejected due to invalid security key. Action: check that the correct account number was entered in the terminal. If a replacement terminal was installed, the ARC will need to perform a «Reload Parameters» on the ISA receiver interface.
Test alarms	These can be carried out for Ethernet, cellular and Wi-Fi network interfaces. Successful: Test alarm reported successfully to the ARC. Connection failed: not able to connect to the ARC over the network interface Action: check with the ARC.
Checking Wi-Fi	Connected: Confirms that the terminal is connected to a Wi-Fi network. Disconnected: The terminal is not connected to a Wi-Fi network. Action: check that the Wi-Fi router is working. Restart the router.
Cellular registration	Registered: The terminal is connected to the cellular network. Not registered: The terminal is not registered to the cellular network. Action: check that the SIM card is enabled and inserted correctly into the SIM card holder, that the antenna is connected, and the signal strength is above the minimum signal strength.
Checking PSTN	Connected: Confirms that the PSTN connection is OK. Disconnected: Means that the PSTN connection is not OK.
Dial Port	OK: Dial port monitoring is working correctly. Fault: Dial port monitoring is not working. Action: Check that the sense resistor wiring is correct.

9.2.2 Disable Cellular

This option lets you simulate a cellular fault so the ARC can check that the operators receive the path fault event.

Note: To prevent a situation where the installer forgets to switch it off, which would disable cellular communications, this mode stays operational for 1 minute and then automatically switches off.

10 Maintenance

There is generally no requirement for any onsite maintenance on the IRIS-4 product range, except those that contain batteries, where the battery status should be checked yearly (see below). However, all the procedures described below are advisable.

10.1 Checking for faults

Check that the SYS LED is steady and not indicating a fault - see chapter 3 “Circuit board layouts” for the SYS LED status indications. If the SYS LED indicates that there is a fault, then further information can be obtained from the touchscreen as described in section 9.1. “Trouble Report”. Identify and correct the fault. Communications tests can be carried out as described in section 9.2 “Test”.

10.2 Checking battery status

The terminal will report battery problems via the fault reporting as above. This will indicate batteries should be replaced or the charge is low.

10.3 Upgrading software

Upgrade the software in the terminal if there is a later version available. The availability of updated software can be found by running the Installation Wizard up to “Checking S/W Version”. The software can be updated at this point if required by clicking on <<Reflash Now>>.

10.4 End to end tests

Carry out end-to-end alarm tests from the alarm panel to the ARC to check that the complete system is operational.

If the terminal is using multiple paths, check that alarm transmission is still operational when just one path is connected. Repeat the test for each path. Note that a cellular path fault can be simulated as described in section 9.2.2 “Disable Cellular”.

11 Technical specifications

Wi-Fi (if applicable)		
Standard	IEEE 802.11 b/g	
Connection	2.4GHz b/g/n with internal PCB chip antenna	
Fault detection	Loss of association/data	
Ethernet (if applicable)		
Standard	UTP 10/100 Base T with auto-negotiation	
Connection	RJ45 socket for CAT5 cabling	
IP addressing	Dynamic (DHCP) or fixed	
Fault detection	Loss of Ethernet synchronization	
Cellular (if applicable)		
IRIS-4 models (from REV A25)		
LTE (4G) Cat1	B28A(700MHz), B20(800MHz), B8(900MHz) B3(1800 MHz), B1(2100MHz), B7(2600MHz)	
UMTS (3G)	B8(900MHz), B3(1800MHz), B1(2100 MHz)	
GPRS (2G)	B8(900MHz), B3(1800MHz)	
IRIS-4 240AP		
LTE (4G) Cat1	B28(700MHz), B5/B26/B18/B19(800MHz) B8(900MHz), B3/B9(1800MHz), B1(2100MHz)	
UMTS (3G)	B5/B6/B19(800MHz), B8(900MHz), B1(2100MHz)	
IRIS-4 models (up to REV A24)		
LTE (4G) Cat4	B20(800MHz), B8(900MHz), B3(1800 MHz) B1(2100MHz), B7(2600MHz)	
UMTS (3G)	B8(900MHz), B1(2100 MHz)	
GPRS (2G)	B8(900MHz), B3(1800MHz)	
Connection	SMA socket for antenna	
Fault detection	Loss of registration with network	
IP		
TCP ports (outbound)	53165 (Alarms and Polling) 51292 (Diagnostic and Reflashing) 10001 (Upload/Download)	
Alarm transmission		
Interface to Monitoring Center	ISA or IRIS Management Suite via EN 50136-2 pass-through mode	
Dial capture interface to alarm panel	Two-wire interface via terminal block	
Serial interface to alarm panel	RS485, TTL, RS232, RS232 **Note**: cabling must not exceed 3 meters	
PIN Inputs interface to alarm panel	Maximum input voltage range 0V to +24V	**Note: Cabling must not exceed 3 meters**
	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	
	FF (Scancom)	
	Robofon (Dial capture only)	
	Telim (Dial capture only)	
	CESA (Dial capture only)	
Tamper detection reporting to Monitoring Center	Dial capture interface Serial Interfaces Pin inputs Lid & back tamper (cased units, apart from IRIS-4 50)	

	Tamper input (where fitted)
Fault reporting to Monitoring Center	Transmission interface/path fault
Relay outputs	
Maximum operating voltage	24V DC
Maximum current rating	100mA DC
Power supply	
Supply voltage	
IRIS-4 160	9V to 15V DC
others	9V to 28V DC
Typical current	
IRIS-4 50 (DS2220)	At 12V DC: 80mA At 24V DC: 40mA
IRIS-4 160	At 12V DC: 83mA
IRIS-4 200/220/240	At 12V DC: 138mA / 110mA / 153mA
	At 24V DC: 78mA / 63mA / 86mA
IRIS-4 400/420/440	At 12V DC: 157mA / 120mA / 160mA
	At 24V DC: 87mA / 68mA / 89mA
IRIS-4 400/420/440G	At 12V DC: 122mA/130mA/137mA
	At 24V DC: 63mA/69mA/73mA
IRIS-4 620/640	At 12V DC: 68mA / 89mA
	At 24V DC: 55mA / 76mA
IRIS-4 620D/640D	At 12V DC: 134mA /142mA
	At 24V DC: 58mA / 81mA
Maximum current	At 12V DC and 24V DC: 1A
Recommended external PSU	⎓ 12V DC 1A 12 Watt **Note:** The Radio Equipment Directive states that the length of the power cable may only be a maximum of 3 meters long.
Environmental	
Operating temperature range	-10°C to 55°C
Operating humidity range	95% max., non-condensing
Weights and dimensions: IRIS-4 50 (DS2220)	
Physical dimensions	87mm x 55mm x 16mm
PCB weight	85 grams (with wire harness)
Fully packaged weight	200 grams
Weights and dimensions: IRIS-4 160	
Physical dimensions	11 cm x 17.5 cm x 4.5 cm
PCB weight	400 grams
Fully packaged weight	600 grams
Weights and dimensions: IRIS-4 2xx	
Physical dimensions	19 cm x 13 cm x 4 cm
PCB weight	550 grams
Fully packaged weight	750 grams
Weights and dimensions: IRIS-4 4xx	
Physical dimensions	14 cm x 11.5 cm x 1.5cm
PCB weight	300 grams
Fully packaged weight	500 grams
Weights and dimensions: IRIS-4 6xx	
Physical dimensions	12 cm x 9 cm x 2cm
PCB weight	60 grams
Fully packaged weight	160 grams

12 Conformance

The European standards that each terminal is compliant to are listed in the Quick Installation manual included in the terminal packaging. They can also be found on our website ‘AddSecure.com’.

Appendix 1: Setting up the IRIS Toolbox

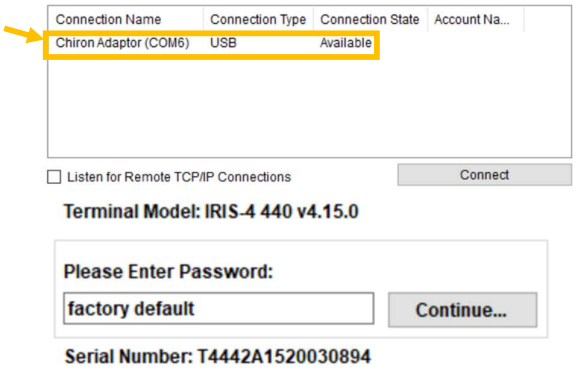
The IRIS Toolbox lets you use a PC to configure or change settings on a terminal. One of the features offered is access to a terminal's 'virtual' touchscreen so the instructions in this manual can be followed on a terminal that does not have a physical touchscreen. IRIS Toolbox is compatible with Windows 10.

Starting the IRIS Toolbox

Begin by downloading the toolbox from AddSecure (use this URL "https://www.addsecure.com/product/iris-toolbox"). Install the toolbox. Connect the terminal to the PC using a USB cable with a micro-USB connector. Now open the toolbox.

IRIS Toolbox immediately scans to see if it can connect to a terminal and shows the results on this screen:

Click on the connection, then click «Connect».

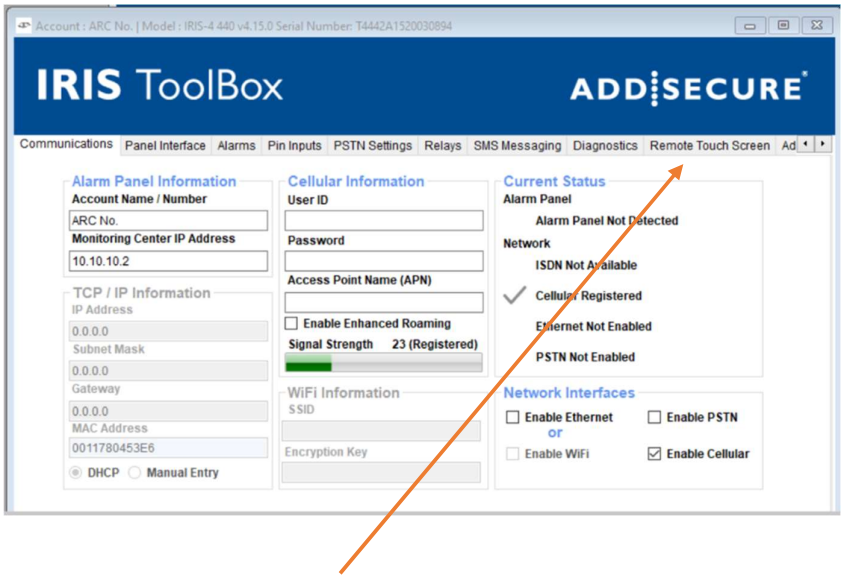


The toolbox now asks for a password with this screen:

The default password is "factory default" so simply click «Continue» and this screen is displayed showing the details of the terminal.

Click on "Remote Touchscreen" in the top menu bar.

This displays the virtual terminal touchscreen:



Click on the touchscreen and the terminal Welcome screen will be displayed.

You can now proceed as described in the main sections in this document from 4.2.4 onwards.

Appendix 2: Abbreviations used by AddSecure

Abbreviation	Description
AOIP	Alarm over IP
APN	Access point name
ARC	Alarm receiving center
ARE	Alarm receiving equipment
ATE	Alarm transmission equipment
ATS	Alarm transmission system
AUTO	Automatic
CID	Contact ID (An alarm format engineers will know as CID)
CIE	Control and indicating equipment
ComIP	A Texecom product reference
CSQ	Cellular signal quality
DCE	Data Communications Equipment
DHCP	Dynamic Host Configuration Protocol
DTE	Data Terminal Equipment
EN	A reference to standards published by the CENELEC, the European Committee for Electrotechnical Standardization
ESPA	European Selective Paging Manufacturer's Association, publishers of pager related standards
EXP	Expansion circuit board for IRIS terminals
FF	Fast format (alarm format)
FTC	Failure to communicate
HHL	A panel manufacturer
IAS-CIE	Intruder Alarm System Alarm Control and Indicating Equipment
IP	Internet protocol
ISA	IRIS Secure Apps (a receiver system for IRIS terminals used by ARCs)
IT	Information technology
LAN	Local area network
PCB	Printed circuit board
PIN	Personal identification number
ProSYS	Type of alarm panel
PSTN	Public Switched Telephone Network
PSU	Power supply
PWD	Password
RP	A SIA alarm format event code
RX	RS232 signal reference
SIA	Security Industry Association, publishers of standards for alarm communication
SIM	Subscriber Identity Module (ETSI GSM technical specification)
TCP	Transmission Control Protocol used over IP
TTL	Serial communication electrical level
UDP	User Datagram Protocol used over IP
USR	Username
VdS	German standards organization
VPN	Virtual private network
WAN	Wide area network
XSIA	A proprietary alarm format based on SIA but extended

Appendix 3: Enclosure T-NG-ENC2

This enclosure is suitable for installations using the IRIS-4 4xx or IRIS-4 6xx terminals that need to comply with EN standards for Fire and Intruder applications. A variant (T-NG-ENC2A) is available which also has an antenna included.

Specification:

Height	25.5 cm
Width	25.5 cm
Depth	10.1 cm
Weight	1450 grams (additional 215 grams for the antenna and bracket for the T-NG-ENC2A)
Colour	AL9003 (White)

Accessories

The enclosure comes with the following accessories:

Qty	Item
10	Soft rubber grommets with membrane, to fit in knockouts
2	Plastic insulating bushes for use with antenna
20	Resistors 15K for terminating inputs (see Settings -> Pin inputs section) to detect tampering
20	Resistors 4.7K for terminating inputs (see Settings -> Pin inputs section) to detect tampering
1	Tamper switch with 35cm wires attached.
1	Tamper arm (long)
1	Tamper arm (short)
1	Grounding cable (already installed)
1	Pack of 4 x 14mm wall spacers
5	8x60 screws and plugs
8	Cable ties
1	Antenna with cable and bracket (T-NG-ENC2A)

Installation instructions

There are two methods for wall mounting the enclosure:

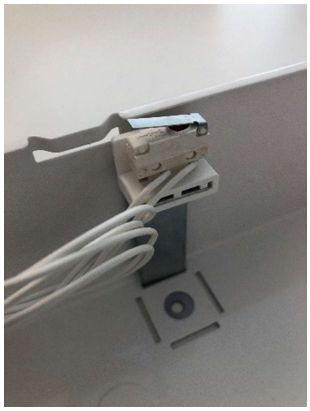
- Using wall spacers provided to give space behind the enclosure. The long tamper arm is provided for this option.
- Without the wall spacers. The short tamper arm is provided for this option.

Remove those knockouts required for external access for cables to the terminal to be fitted within the enclosure. Fit rubber grommets to the holes where the knockouts have been removed. **Knockouts must not be used in the vicinity of the Ethernet and antenna connections on the terminal, to prevent unplugging of the related connectors.**

Fix the enclosure in the location required using the screws and plugs provided, using either method as above.

Fix the terminal within the enclosure using the stand-offs provided with the terminal and the pre-punched holes within the enclosure. **Do not use the self-adhesive feet provided with the terminal.** Connect the terminal as required (see Basic Setup section).

Fit the tamper switch with bracket (either long or short depending on whether the wall spacers have been used). As shown below, and connect to the tamper inputs of the terminal.



For the T-NG-ENC2A the antenna can either be mounted with the bracket provided or removed from the bracket and fitted to the enclosure using the knockout on the top of the enclosure. When installed on the enclosure fit the insulating bushes supplied.

All cables (e. g. tamper switch, Ethernet, antenna) must be secured with cable ties, to prevent easy capture and tampering of the wires. Use the cable ties provided and the cable tie clip points in the base of the cabinet.

Once the terminal is installed and working, close and lock the cabinet lid.

Appendix 4: Panel Specific Protocol Handling (Emulation Mode)

A4.1 ESPA

IRIS-4 4xx series Alarm over IP terminals have been tested and certified to conform to the EN54-21 standard for fire alarm transmission systems. This is in addition to conformance to intruder alarm standard EN50136.

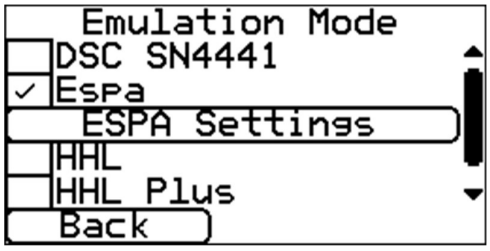
To complement this functionality for fire alarm systems, the terminals also support the ESPA 444 protocol on their serial RS232 interfaces. This protocol is commonly used by fire alarm panels for communications with pager and other text transmission systems. In this mode, display messages sent by the panel over the ESPA protocol are transmitted by the terminal to the IRIS Secure Apps receiver at the ARC as SIA formatted messages.

The installer can also embed standard SIA format events and zone numbers within the text message so that the ARC has precise event and location information on which to act as well as the text string.

Please note: Any installation of the IRIS Touch 4xx for fire alarm transmission that is required to comply with EN54-21 should be installed in accordance with the instructions in the 'Installation for EN54-21:2006 compliance' section of this document. ***This requires that 'Fire' and 'Fault' inputs should be wired from the panel to the terminal with acknowledge and fault signals wired back from the terminal. This is necessary as the ESPA protocol does not provide any alarm transmission acknowledgement signal back from the terminal to the alarm panel.***

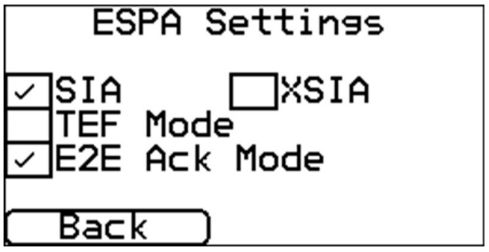
A4.1.1 Enabling the ESPA interface

The ESPA functionality on the serial interfaces of the terminal is enabled via the touch screen settings menus, Panel Interface->RS232 (x)->Emulation mode, where x can be '1' or '2'.



Note that ESPA cannot be set for both serial ports simultaneously. If ESPA is selected for port 2 whilst it is enabled for port 1, then port 1 is set to 'Normal' and vice-versa.

When 'ESPA' is selected, button 'ESPA Settings' gives access to additional ESPA specific settings.



A4.1.2 Connection to the fire panel

The connection to the alarm panel is from the 3-wire RS232 interface header on the terminal. The connection at the alarm panel end depends on the panel itself. The baud rate for the terminal must be set to the same as that used by the panel.

A4.1.3 Conversion of ESPA display messages to SIA format alarms

When the terminal receives an ESPA message from the panel, it extracts the Display Message (identified by the ESPA Data Identifier '2'). It converts it to 2 x SIA format messages which are sent to the ARC. As default the first message is a SIA Event Code 'FS99' (Fire Supervisory zone 99). The second message is the display text identified as a SIA 'Ascii' message. For example:

ESPA Display message: "Detector Fault"

SIA messages: "NFS99", followed by "ADetector Fault"

If required, a SIA event message can be embedded at the start of the text by surrounding the event string with '#'….'#'. This replaces the default 'FS99'. For example:

ESPA Display message: "#FA222#Elevator switch room"

SIA messages: "NFA222", followed by "AElevator switch room"

Note that as SIA messages can be a maximum of 63 characters, each string should be a maximum of 63 characters long. Any messages longer are truncated to 63 characters.

A4.1.4 Setting SIA/XSIA

If 'XSIA' is selected, the format of messages (as in the sample above) is changed to a single message:

ESPA Display message: "Detector Fault"

SIA messages: "NFS99*'Detector Fault'NM"

A4.1.5 Setting TEF Mode

This setting is for use with TEF Fire alarm panels. With this setting enabled, the terminal extracts from the ESPA message the Call Address (identified by the ESPA Data Identifier '1') and the Beep Coding (identified by the ESPA Data Identifier '3'). These are used to determine the SIA Event Code and Zone Number sent to the ARC, as follows:

Call Number	SIA Event Code and Zone Number
999	FA000
998	UX000
997	FT000
996	QA000
995	Depends on Beep Coding, as below

.

Beep Coding	SIA Event Code and Zone Number
1	FA000
2	UX000
3	FT000
4	QA000
5	FB000
6	YO000
7	FI000
8	YO000

A4.1.6 Setting E2E Ack (End to End Acknowledgement) Mode

In this mode, messages from the panel are not acknowledged with an ACK until they have been sent to the ARC and receipt has been acknowledged. If for any reason the messages cannot be sent to the ARC, or transmission fails, then a Negative Acknowledge (NAK) is returned to the panel.

In this mode the terminal operates with a window size of 1, so the panel must not send another message until the previous one has been responded to with an ACK or a NAK.

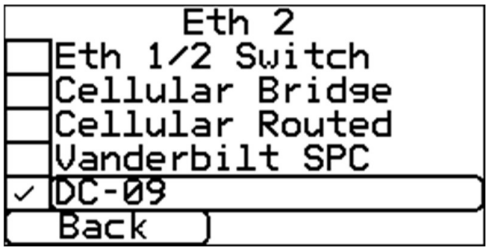
If Limotec mode is selected, this mode is set automatically and cannot be changed.

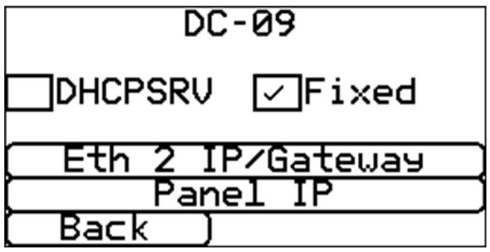
A4.1.7 Trouble Reporting

The terminal monitors the ESPA Interface and if no poll is received from the panel for 30s a ‘serial interface’ trouble report is sent to IRIS Secure Apps receiver at the ARC. This requires the tick box ‘Serial’ to be ticked for this terminal on IRIS Secure Apps.

A4.2 Alarm Panels Using SIA DC-09 Protocol

Terminals with dual Ethernet connections can support alarm panels that use the SIA DC-09 protocol (SIA Digital Communication Standard – Internet Protocol Event Reporting, SIA-DC-09-2021) over an Ethernet connection. This is achieved by connecting the alarm panel to the Eth2 connection on the terminal and configuring the terminal appropriately, using the Settings->Eth 2 menu.

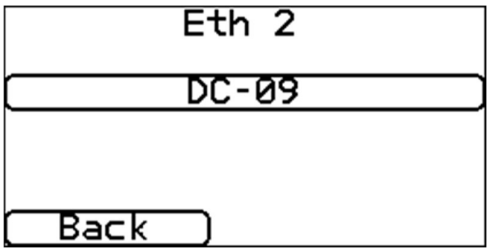


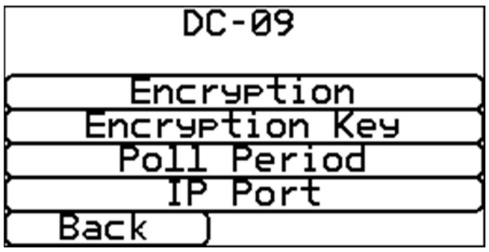


In this mode the terminal will:

- Receive SIA or Contact ID format alarms from the DC-09 panel and forward them to an IRIS Secure Apps receiver, in the same way as alarms received from an alarm PSTN dialler via the terminal's Dial Capture port. This includes transmission over a backup cellular path if the IRIS terminal is set to do this.
- Respond to polls (NULL messages) from the DC-09 alarm panel.
- Monitor activity from the DC-09 panel and report a fault to the IRIS Secure Apps receiver if communications from the panel stops.
- Handle encrypted messages from the DC-09 panel, as defined in the DC-09 specification.

Various options are available for compatibility with the panel connected, using the Panel Interface->Eth 2 menu:





These settings ***must*** match the settings in the panel.

A4.2.1 IP Addressing

When this mode is enabled, by default, the terminal Eth2 port is allocated IP address 192.168.1.254, so this is the address of the Alarm Receiving Centre as far as the alarm panel is concerned. DHCP is enabled and the panel will be allocated address 192.168.1.2.

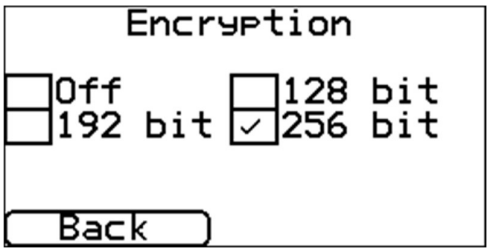
If these IP addresses overlap with the IP address range of the IP network to which the terminal's Ethernet 1 is connected, the address of Ethernet 2 must be changed.

If the panel has been given a fixed IP address, this should be configured in the terminal so that it knows where to send packets it forwards.

A4.2.2 Panel Account Number

The alarm account number set in the panel should be the site account number set up at the ARC in which the IRIS Secure Apps is located.

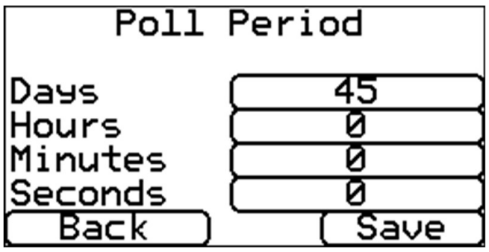
A4.2.3 Encryption





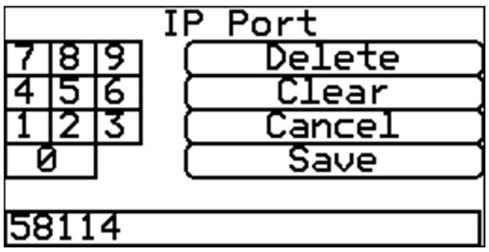
AES encryption, as defined in the DC-09 standard, can be configured as Encryption off, key length 128 bit, 192 bit or 256 bit. The key must be set up with the appropriate number of characters, depending on the number of bits 128 bits = 32, 192 bits = 48, 256 bits = 64. Note that because of the length of the key, which cannot be displayed completely on the Touch screen, using the IRIS Toolbox provides an easier method of setting the key.

A4.2.4 Poll Period



The terminal expects the panel to communicate, either with an alarm or a “NULL” message at the rate configured here. If the terminal does not see a message within the time specified it will report a Peripheral Serial Interface fault.

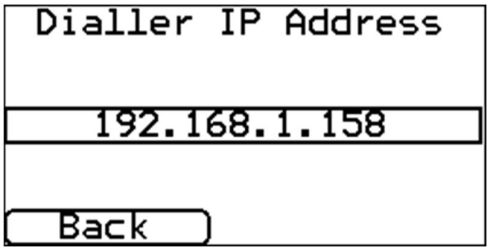
A4.2.5 IP Port

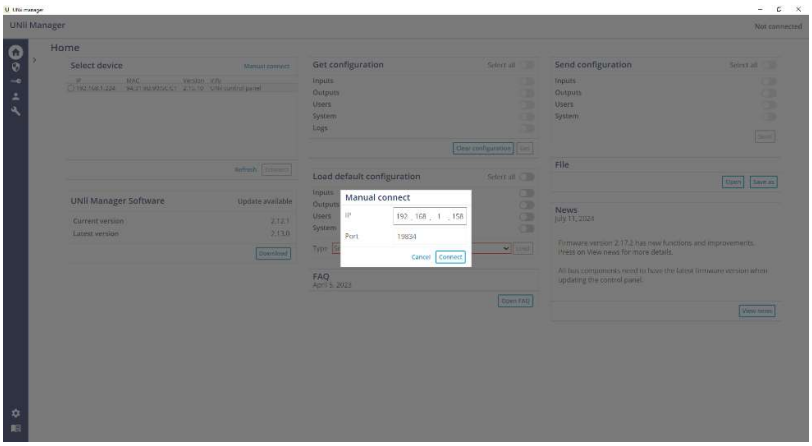


This setting defines the IP port used for communications between the panel and the terminal, either using TCP or UDP.

A4.2.6 Operation with an Alphatronics UNii Panel

The UNii Manager configuration software can be connected to the alarm panel by manually connecting to the IP address of the Eth 1 connection of the terminal.

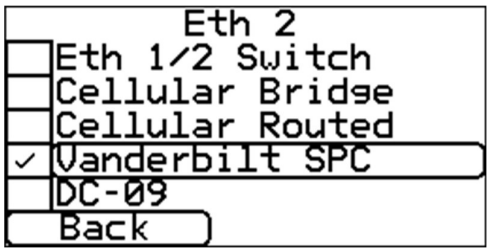


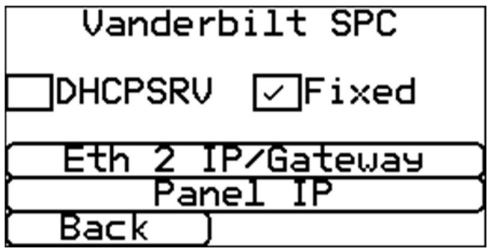


Traffic between the panel and the mySmartControl App will automatically be routed by the terminal between the panel and the external IP network, via the Eth 1 connection with the cellular connection as backup if the Eth 1 connection is not available.

A 4.3 Operation with a Vanderbilt SPC Panel

Terminals with dual Ethernet connections can support Vanderbilt SPC alarm panels using the EDP protocol over an Ethernet connection. This is achieved by connecting the alarm panel to the Eth2 connection on the terminal and configuring the terminal appropriately, using the Settings->Eth 2 menu.





In this mode the terminal will:

- Receive SIA format alarms from the SPC panel and forward them to an IRIS Secure Apps receiver, in the same way as alarms received from an alarm PSTN dialler via the terminal's Dial Capture port. This includes transmission over a backup cellular path if the IRIS terminal is set to do this.
- Respond to polls from the SPC alarm panel.
- Monitor activity from the SPC panel and report a fault to the IRIS Secure Apps receiver if communications from the panel stops.

A4.3.1 IP Addressing

When the Vanderbilt SPC mode is enabled, by default, the terminal Eth2 port is allocated IP address 192.168.1.254, so this is the address of the Alarm Receiving Centre as far as the alarm panel is concerned. DHCP in the Terminal is enabled and the panel will be allocated address 192.168.1.2. DHCP should also be enabled in the alarm panel.

If these IP addresses overlap with the IP address range of the IP network to which the terminal's Ethernet 1 is connected, the address of Ethernet 2 must be changed, and this will result in a new IP address being given to the panel. The panel should be restarted to ensure it gets this address.

The Network Protocol should be set to TCP/IP and the Alarm Receiving Centre port should be set to 58212 in the SPC panel.

If the panel has been given a fixed IP address, this should be configured in the terminal so that it knows where to send packets it forwards.

A4.3.2 Panel polling

The IRIS Terminal checks every 30s that the panel is communicating with it, so the panel poll rate should be set faster than this, for example every 10s.

A4.3.3 Web access to the panel

The panel web page can be accessed by using a PC on the same LAN segment as the terminal Eth1 connection. Direct the browser to the IP address of the terminal Eth1 connection and the request will be forwarded to the panel on Eth2., with the panel responses on Eth2 forwarded back to the browser.



Appendix 5: Default Alarm Messages Generated by the Terminal

A5.1 Pin Input Alarms

Pin no.	Event description	SIA Format Alarm Message	SIA Format Restore message	Contact ID Event Code	Group no.	Zone no.
1	Fire alarm zone 1	NFA01	NFR01	110	00	001
2	Panic alarm zone 2	NPA02	NPR02	120	00	002
3	Burglary alarm zone 3	NBA03	NBR03	130	00	003
4	Open/Close zone 4	NOP04	NCL04	400	00	004
5	Equipment fault zone 5	NIA05	NIR05	300	00	005
6	Burglary bypass zone 6	NBB06	NBU06	573	00	006
7	Burglary verified zone 7	NBV07	NBR07	139	00	007
8	Tamper alarm zone 8	NTA08	NTR08	137	00	008
9	AC Power trouble zone 9	NAT09	NAR09	301	00	009
10	Fire trouble zone 10	NFT10	NFJ10	380	00	010
11	Emergency alarm zone 11	NQA11	NQR11	101	00	011
12	System battery trouble zone 12	NYT12	NYR12	302	00	012
13	Medical alarm zone 13	NMA13	NMR13	100	00	013
14	Untyped alarm zone 14	NUA14	NUR14	323	00	014
15	Untyped alarm zone 15	NUA15	NUR15	323	00	015
16	Untyped alarm zone 16	NUA16	NUR16	323	00	016

A5.2 Voice call alarm

Event	SIA Format Alarm Message	SIA Format Restore Message	Contact ID Event Code	Group no.	Zone no.
Voice call alarm	SC93^Voice call^	None	140	00	093

A5.3 General Alarms

The alarms shown below are generated by the terminal. Some other alarms that relate to the terminal are generated and sent by the IRIS Secure Apps system to which the terminal is reporting. These include communication and interface status events. See IRIS Secure Apps documentation for more information. However, if the terminal is reporting using the DC-0 protocol, these are generated by the terminal itself.

Event	SIA Format Alarm Message	SIA Format Restore Message	Contact ID Event Code	Group no.	Zone no.
Battery fault	NYT96^Battery low^	NYR96^Battery restore^	302	0	96
Battery test failure	NYP96^Battery test fail^	NYQ96^Battery test OK^	309	0	96
Engineer access	NLB97^Iris engineer^	NLX97^Iris engineer^	627	0	97
Engineer test alarm (via Cellular)	NRX98^Cellular test alarm^	N/A	602	0	98
Engineer test alarm (via Ethernet)	NRX99^Ethernet test alarm	N/A	602	0	99
Engineer test alarm (via WiFi)	NRX94^Wifi test alarm^	N/A	602	0	94
Mains fail	NYP95^Power fail^	NYQ95^Power restore^	301	0	95
Pin fault (tamper)	NETxx (xx = pin number 01 to 16)	NERxx (xx = pin number 01 to 16)	330	0	Pin number 1-16
Regular test alarm	NRP92^Iris test alarm^	N/A	602	0	92
SIP registration over Cellular	NLT87^SIP registration over Cellular fail^	NLR87^SIP registration over Cellular restore^	350	0	87
SIP registration over Ethernet	NLT89^SIP registration over Ethernet fail^	NLR89^SIP registration over Ethernet restore^	350	0	89
SIP registration over WiFi	NLT88^SIP registration over Wifi fail^	NLR88^SIP registration over Wifi restore^	350	0	88
Tamper input	NTA99^Iris tamper^	NTR99^Iris tamper^	137	0	99

A5.4 Alarms generated when using DC-09 as the transmission protocol.

Event	SIA Format Alarm Message	SIA Format Restore Message	Contact ID Event Code	Group no.	Zone no.
Ethernet connection fault	NNT101^Ethernet Trouble - not connected to network^	NNR101^Ethernet Restore - connected to network^	350	0	110
Cellular loss of regisration	NNT102^Cellular Trouble - not registered with network^	NNR102^Cellular Restore - registered with network^	350	0	102
Wi-Fi connection fault	NNT103^WIFI Trouble - not connected to network^	NNR103^WIFI Restore - connected to network^	350	0	103
Dial port fault	NNT111^Dial port Trouble - with connection to panel^	NNR111^Dial port Restore - with connection to panel^	350	0	111
Serial RS232 (1) connection fault	NNT112^RS232 1 Trouble - no comms from panel^	NNR112^RS232 1 Restore - comms from panel^	350	0	112
Serial COM connection fault	NNT113^Com port Trouble - no comms from panel^	NNR113^Com port Restore - comms from panel^	350	0	113
Serial RS232 (2) connection fault	NNT114^RS232 2 Trouble - no comms from panel^	NNR114^RS232 2 Restore - comms from panel^	350	0	112
RS485 connection fault	NNT110^RS485 Trouble - no comms from panel^	NNR110^RS485 Restore - comms from panel^	350	0	110
DC-09 IP Main channel trouble	NLT86^DC09 Tx IP main failure^	NLR86^DC09 Tx IP main restore^	356	0	86
DC-09 Cellular Main channel trouble	NLT85^DC09 Tx Cellular main failure^	NLR85^DC09 Tx Cellular main restore^	356	0	85
DC-09 IP Backup channel trouble	NLT84^DC09 Tx IP backup failure^	NLR84^DC09 Tx IP backup restore^	356	0	84
DC-09 Cellular Backup channel trouble	NLT83^DC09 Tx Cellular backup failure^	NLR83^DC09 Tx Cellular backup restore^	356	0	83