SPCS310

SPC Pro Installation & Configuration Manual

3.6

A6V10216077
01.10.2015

Vanderbilt

Copyright

Technical specifications and availability subject to change without notice.

Edition: 01.10.2015

Document ID: A6V10216077

Table of contents

1 Meaning of symbols

There are several symbols in the document:

Symbol	Description
	Not available for SPC42xx, SPC43xx.
	Only available for SPC controller with IP interface (SPC43xx/SPC53xx/SPC63xx).
	Not available for installation type Domestic.
	Only available in unrestricted mode.
	Find further information about Security Grade, Region or Mode in text.
	See Appendix for further information.

2 Technical data

Communication protocol	● Proprietary (via RS232, USB, TCP/IP on Ethernet, PSTN, GSM) ● Data transfer from/to SPC Fast Programmer
System compatibility	● Single PC solution ● Running on PCs with Windows XP/Vista ● Fully supports SPC42xx/SPC43xx/SPC52xx/SPC53xx/SPC63xx
Memory	Min. 1 GB required
Database	Local file storage in compressed format.

3 Software description

The SPC Pro is a PC based software application that provides the user with the ability to program and configure SPC systems on either a local or a remote connection. All of the programming features accessible through the SPC embedded browser interface are also provided by SPC Pro.

3.1 Operational modes

SPC Pro provides the user with the ability to create multiple installation profiles. Each profile consists of the installation name, ID and connection details which will be listed in turn on the SPC Pro installation page.

Once an installation profile has been created, it can be configured by entering configure mode. In configure mode, all of the programming features (zones, outputs, timers, etc.) can be configured as required and saved.

3.1.1 Offline mode

You can create new installation profiles, edit or delete existing profiles without ever connecting to an installation. In this mode of operation each of the installations can be configured off-line and the configuration saved for future downloads if required.

When SPC Pro is not connected to a panel the icon  will be displayed in the Configuration Mode Toolbar [→ 19].

The text **offline** will be presented at the top of each programming window to remind you that you have not yet connected to an installation site. All status refresh buttons will be disabled when offline.

3.1.2 Online mode

When you enter configure mode for an existing installation, the option to connect to a panel is presented. In this mode a direct connection to the panel is established allowing you to read and configure all of the programming features of the selected installation.

When SPC Pro is connected to a panel the icon  will be displayed in the Configuration Mode Toolbar [→ 19].

The text **online** will be presented at the top of each programming window to remind you that you are connected to an installation site. Refresh and status programming buttons (such as zone isolate, inhibit, etc.) will be enabled when online.

3.2 Connectivity

The SPC Pro can connect to the SPC controller via the following interfaces.

3.2.1 Ethernet interface

IP

Your PC must have an Ethernet network card to connect locally via a Local Area Network (LAN), remotely via a Wide Area Network (WAN) or directly to the Ethernet Port on the controller using a crossover cable.

For details on how to connect to the controller using an IP connection see page [→ 219].

3.2.2 Direct USB

A direct connection to the controller via the USB port of your PC is supported. The SPC USB drivers must be installed on your PC. These drivers are contained on the SPC CD.

For details on how to connect to the controller using a USB connection see page [➞ 220].

3.2.3 Direct serial

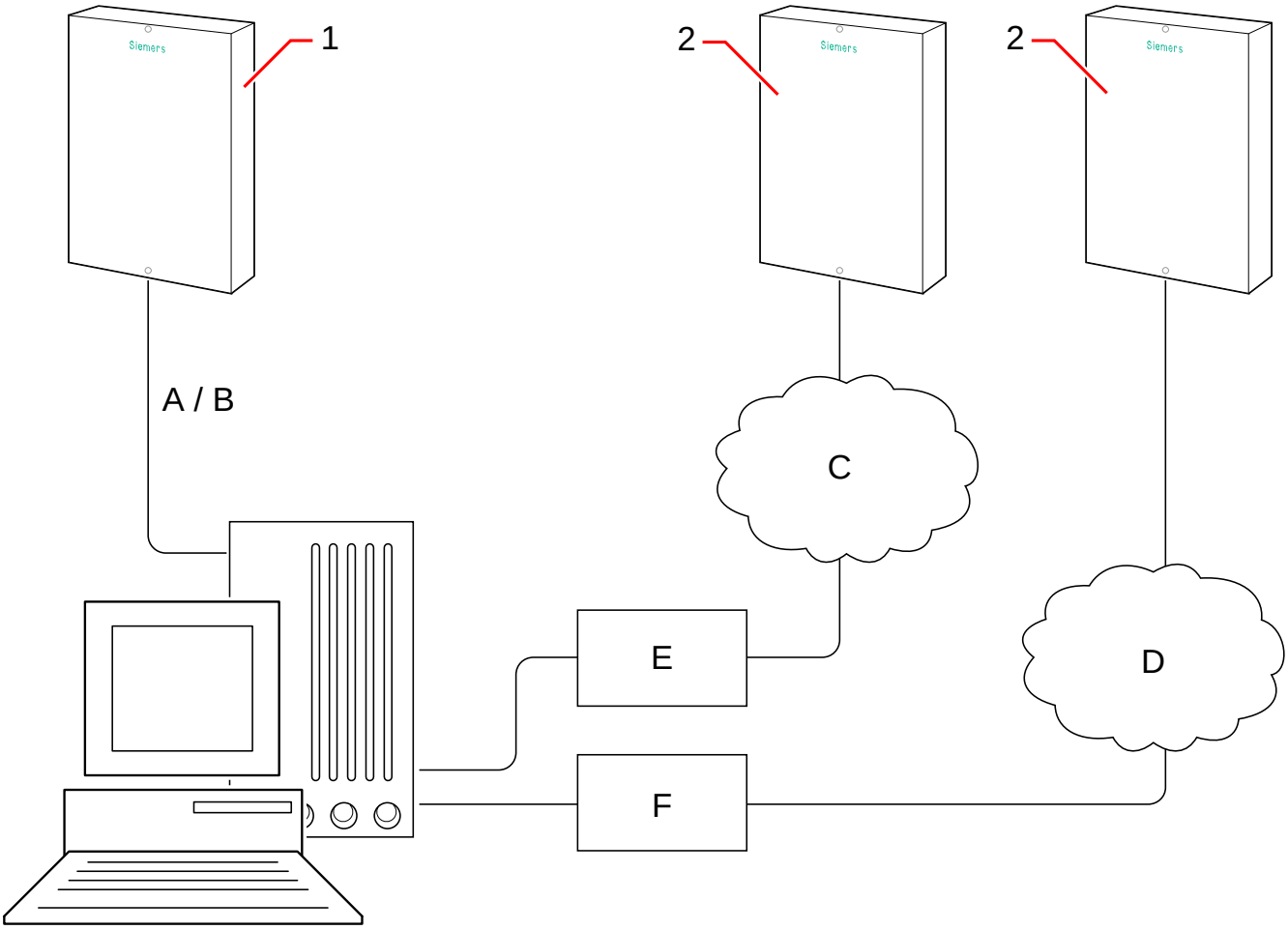
A direct connection from the serial port on your PC to the serial port on the controller is supported by SPC Pro.

For details on how to connect to the controller using a serial connection see page [➞ 221].

3.2.4 Modem

A remote connection to the controller via a PSTN or GSM modem is also supported. Your PC must have a functioning PSTN/GSM modem installed for a connection to be established. For a PSTN connection a functioning PSTN line must be connected to the modem. The remote the controller must also have a PSTN/GSM modem installed and configured to answer incoming calls.

For details on how to remotely connect to the controller see page [➞ 224].



1	Local SPC connectivity
A	Ethernet
B	USB

2	Remote SPC connectivity
C	IP network
D	PSTN / GSM network
E	Router
F	Modem

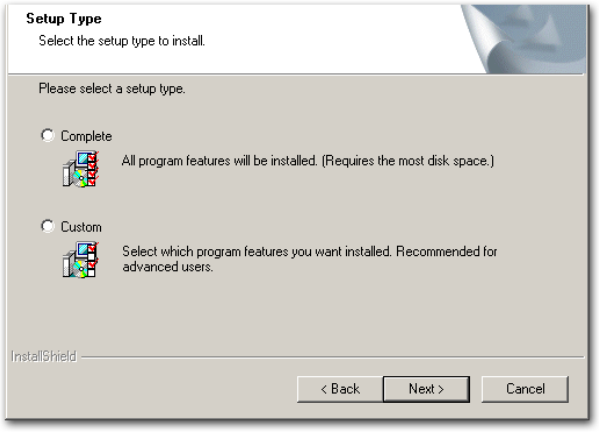
4 Installation

4.1 Installing new SPC Pro software

	⚠ **WARNING**
	Before installing the latest version of SPC Pro, you must uninstall any older versions.

The latest versions of SPC Pro setup program is located on the SPC support CD which comes with the control panel.

1. Click on **setup.exe**.
   ⇨ The setup wizard is displayed.
2. Click **Next**.
3. Enter a user name and a company name.
4. Click **Next**.
   ⇨ The following window is displayed:



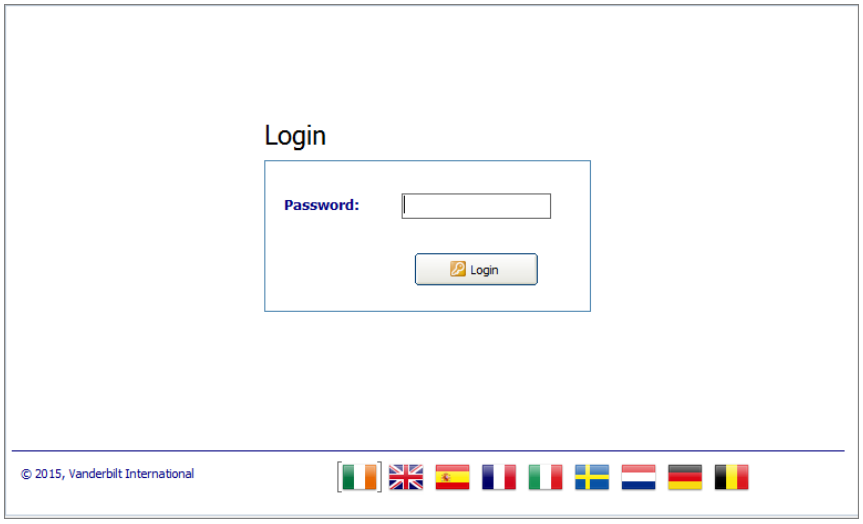
5. Choose the installation type.
6. Click **Next**.
7. Click **Install**.
   ⇨ SPC Pro will be installed.
8. Click **Finish**.

	⚠ **WARNING**
	If using SPC Remote Maintenance with Windows 7 (32 bit & 64 bit) or Windows Vista, you must install SPC Pro and Remote Maintenance into a folder other than *Program Files* or *ProgramFiles(x86).*

5 Getting started

5.1 Login

1. Click the icon SPC Pro in the Windows programs menu bar.
   ⇨ The following window is displayed:



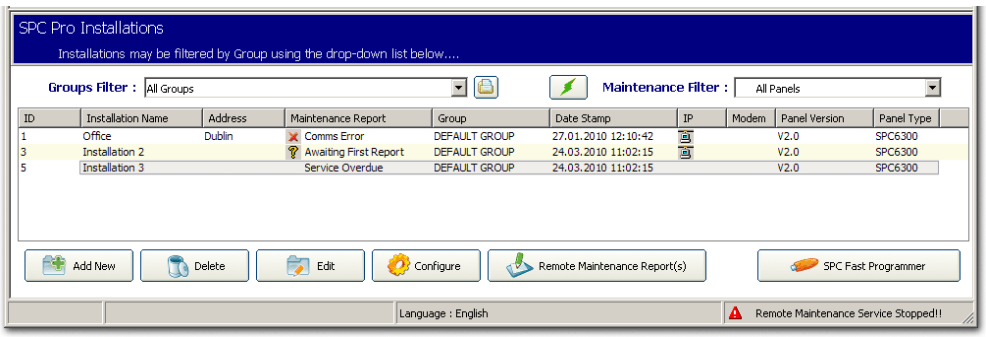
2. Click on the appropriate flag to change the language.

The language flags only change the language used in the application. To change the language for the keypads, web interface and event logs see page [→ 78]. Note that if you change the system language from SPC Pro, the system log language will only update after a disconnect and reconnect to panel.

3. Enter the default password (1111) in the field **Password**.

The password for logging on to the application is not related to the password for connecting to the panel (see page).

4. Click the button **Login**.
   ⇨ The following window will be displayed.
   ⇨ The window lists all of the installation profiles created on the system.



ID	This number uniquely identifies the installation (1 – 999999).
Installation Name	The name of the installation.
Address	The installation address.

Panel Type	The type of control panel.
Group	Each installation may be categorised into distinct groups, allowing the user to readily recognize installation sites by customer.
Date Stamp	The last time that the installation was configured with SPC Pro.
IP	The IP address of the installation.
Modem	The modem associated with the installation.
Panel Version	Displays the firmware version in the panel.

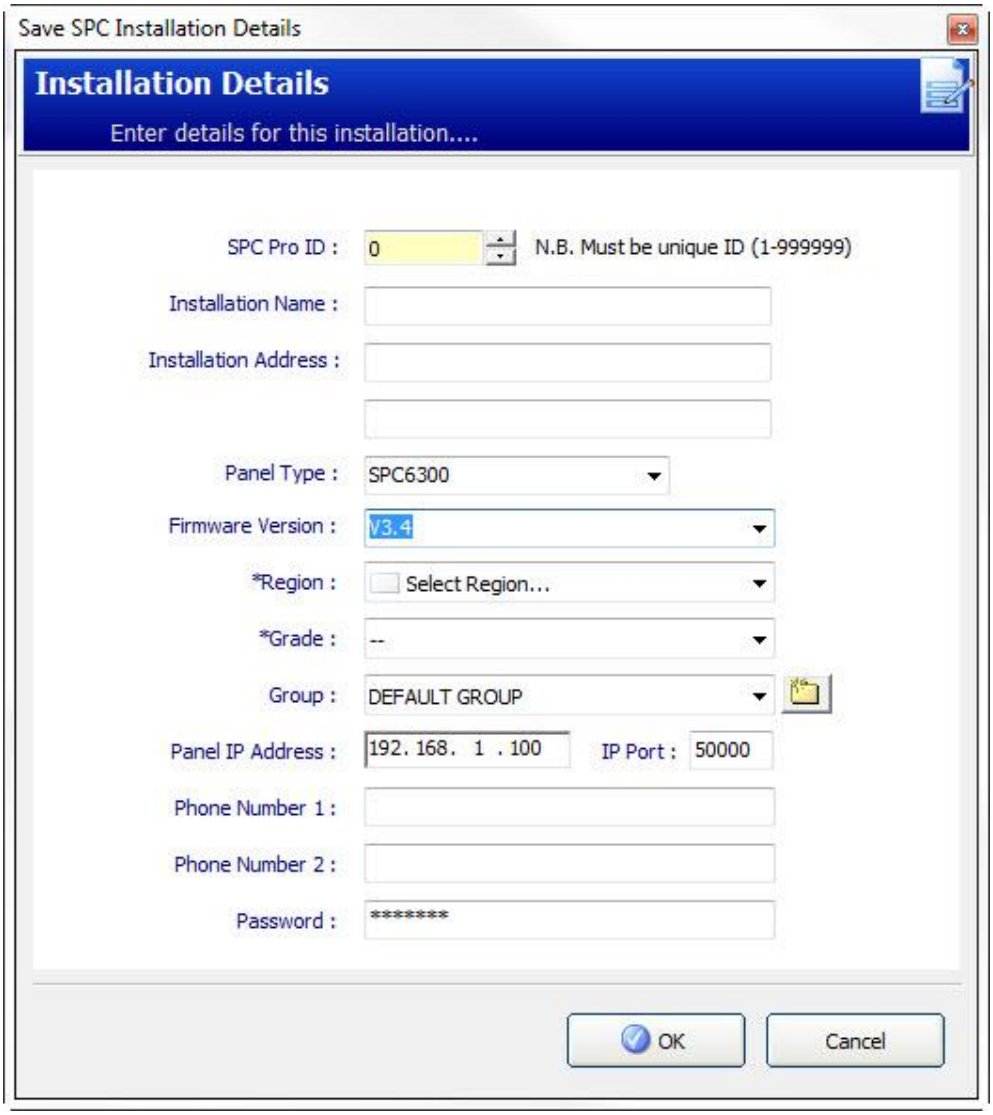
On entering this page for the first time the list will be empty and you will be required to create an installation profile in order to proceed (see page [→ 15]).

5.2 Installations

5.2.1 Adding an Installation

A SPC Pro connection must be enabled in Engineer programming on the control panel before a connection can be established (see page [→ 26]).

1. Click the button **Add New**.
   ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.
3. Click **OK**.

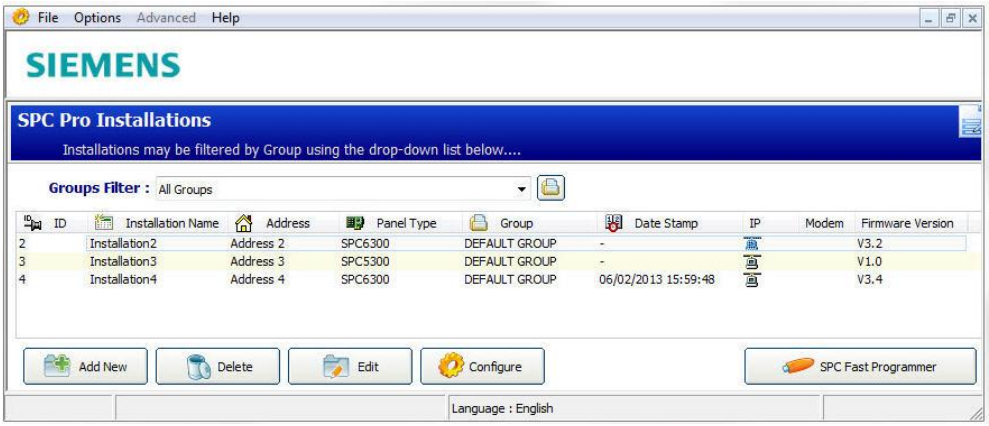


SPC Pro ID	Enter a unique number for each installation. This number uniquely identifies the SPC Pro installation (1- 999999). **Note:** This is not the same value as the **Installation ID**, displayed in the Panel Status\Summary, which uniquely identifies the panel.
Installation Name	Enter an installation name before the installation is saved on the system.
Installation Address (optional)	Enter an address to act an aid to identify individual sites.
Panel Type	Select a type of panel from the dropdown list.
Firmware Version	Select the firmware version from the dropdown list.
Region	Select the region from the dropdown list.
Grade	Select the grade from the dropdown list.
Group	Each installation may be categorised into distinct groups, allowing the user to readily recognize installation sites by customer.
Panel IP Address IP	Enter an IP address for the installation.
IP Port IP	Enter an IP Port for the installation.
Phone Number 1	Enter a telephone number that is associated with the PSTN Line or GSM number assigned to the primary modem on the SPC controller. SPC Pro will attempt to make a call on this number when remotely connecting via a

	modem. If this connection does not succeed, Telephone Number 2 will be dialled
Phone Number 2	Enter a telephone number that is associated with the PSTN line or GSM number connected to the backup modem on the controller. SPC Pro will only dial this number if a connection on telephone number 1 did not succeed
Password	Enter a password to enable the connection to the panel. **Note**: This password must match the SPC Pro password programmed in the controller

Date Stamp

In addition to the basic installation parameters a field Date Stamp is displayed.



This field displays the following:

- The last time an installation configuration was uploaded from, or saved to a panel.
- The last time an installation configuration was saved locally on the PC.

Date stamp fields that are displayed as blank (–) indicate that these installations were added to the system without ever being configured or sent to a panel (i.e. only the basic site initialisation details were configured and saved).

Although SPC Pro allows you to add a large number of installations (1 – 999999), you can only connect to one installation at a time. Any attempt to simultaneously connect to more than one configuration will be rejected.

5.2.2 Configuring an installation

1. Click an installation from the list.
2. Click the button **Configure**.

⇨ The Configuration window [→ 18] will be displayed.

5.2.3 Copying an Installation

Installation profiles can be copied and edited to create a new profile. This is a convenient method of creating a number of similar profiles.

1. Click on an existing profile.
2. Right click and select **Copy/Create New Installation** from the dropdown menu.

⇨ The **Installation Details** window display for editing.

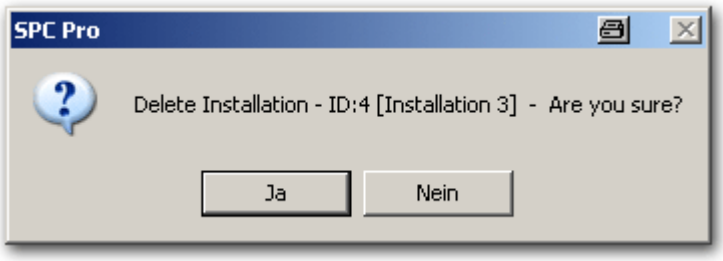
5.2.4 Deleting an installation

It is good practice to note the details of an installation you are about to delete. Once an installation has been deleted from SPC

Pro all information for that installation can not be retrieved.

When you delete an installation, the ID number for that installation will also be deleted. This number is free to be used again for a new installation.

1. Click an installation from the list.
2. Click the button **Delete**.
   ⇨ The following message will be displayed:



3. Click **Yes**.

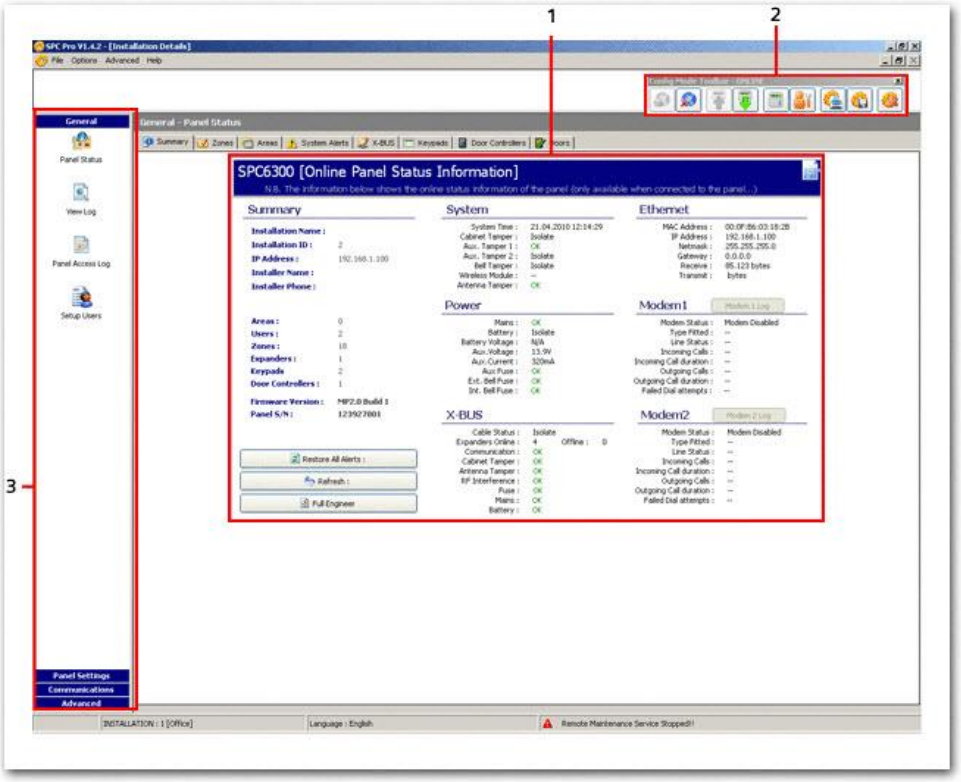
⇨ The installation is deleted.

5.2.5 Editing installation details

1. Click an installation from the list.
2. Click the button **Edit**.
   ⇨ The **Edit Installation Details** window is displayed. The **Edit Installation** Details window is identical to the new **Installation Details** window, except it is not possible to edit the **Region** or **Grade** of an existing installation in SPC Pro.
3. Enter the new data.
4. Click **Save New Configuration**.

5.3 Configuration window

Once an installation has been added to SPC Pro it may be configured as required in the following window:



1 SPC4xxx	Online Status information (only when SPC Pro connects to the panel).
2	Configuration Mode Toolbar
3	Program Menu Headings

5.3.1 Online status information

System summary	Summary of the panel tampers, Wireless RXR and time.
Power	Summary of the controller electrical parameters (voltages, currents) and the status of the fuses (auxiliary & bell).
X-BUS	Summary of X-BUS status and online expanders.
Ethernet	Summary of Ethernet parameters on the panel.
Modem 1	Summary of the modem parameters for Modem 1 (Primary slot).
Modem 2	Summary of the modem parameters for Modem 2 (Back-up slot).

5.3.2 Configuration mode toolbar

Button	Function	Description
	Connect to panel	This button is displayed when the SPC Pro is offline. To connect to the SPC panel click this button. The window **Select Comms Path** will be displayed prompting you to select from one of the connection modes that were

Button	Function	Description
		programmed for this installation (IP, USB, Serial, Modem 1, Modem 2).
	Disconnect from panel	This button is displayed when the SPC Pro is online (already connected to a panel). To disconnect from the SPC panel click this button. SPC Pro will prompt you to confirm that you wish to disconnect from the panel. Click on the button Yes to proceed with disconnection.
	Send Config File to panel	Click this button to send the current configuration to the panel. All programming settings will be transferred to the panel. Ensure that you have correctly configured the installation before clicking this button. This feature is only available in the full engineer mode
	Get Config file from panel	Click this button to load the panel configuration file in to your configuration file. All programming settings will be loaded on to your configuration file. Any configuration data that is different from the panel configuration will be over written.
	Keypad Emulation	Click this button to activate a virtual SPC keypad on your PC. This keypad behaves exactly as if you were operating a physical keypad. It allows you to view information on the keypad display and to enter Engineer or User programming by clicking on the keypad buttons (see page [➞ 217]).
	Select Soft or Full engineer mode	Click this button to toggle between Soft- and Full Engineer modes. In Full Engineer mode all alarm activations and reporting is de-activated. **Note:** If the default PIN 1111 is enabled, for example, a new SPC installation, you must change the engineer PIN at the panel. If you do not change your PIN, you will get an information message forcing you to change your default PIN before logging out of full engineer mode. The “Soft Engineer” mode provides fewer programming functionality and is used for system operation. However, programming in “Soft Engineer” mode allows arming and testing procedure on the system. All alarms remain active. **Note:** If ‘Engineer Exit’ option is enabled in System Options, the engineer is allowed leave Full Engineer mode with alerts active but must acknowledge all alerts listed before switching from Full Engineer mode to Soft Engineer mode.
	Save Config File changes	Click this button to save the configuration that you have programmed.
	Exit Config Mode	Click this button to exit the configuration mode. If you wish to save your configuration changes before exiting click the button **Save Config file changes**.

5.3.3 Program menu headings

General	Panel Settings	Communications	Advanced
 Status	 System Settings	 Serial Ports	 Cause & Effect
 System Log	 Controller Inputs &		

General	Panel Settings	Communications	Advanced
	Outputs	Modems	Calendars
 Panel Access Log	 Expanders & Keypads	 ARC Settings	 Triggers
 Setup Users	 All Zones	 EDP Settings	 Mapping Gates
	 Wireless	 SPC Pro/SPCSafe*	 X-10
	 All Doors	 RM Settings	 Advanced Output
	 Areas	 CEI-ABI	 Logo Configuration
		 Network Settings	 Audio Configuration
			 Verification

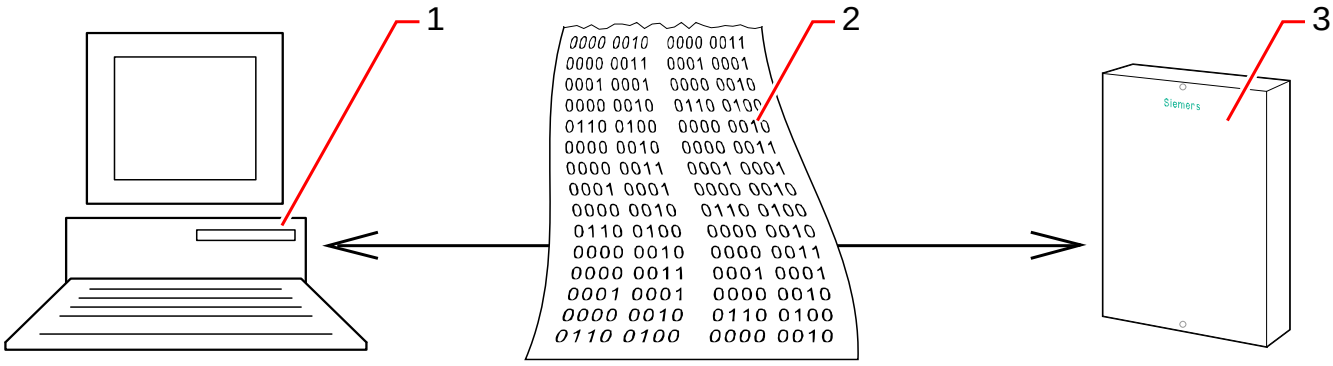
* See SPC Remote Maintenance and SPC Safe Configuration Manual.

6 Programming overview

6.1 Configuration files

6.1.1 Storing and retrieving to the panel

Programming data is exchanged between SPC Pro and the panel by means of a configuration file. When you upload or download a configuration file to the panel ALL of the configuration settings are sent or received. It is therefore important that you check all of the configuration data (not just the data you are currently viewing), before sending a file to the panel.



1	SPC Pro
2	Config File
3	SPC Panel

Every configuration file is stored with a time and date stamp. When the SPC Pro connects to the panel, a check is made to determine if your PC configuration file has the same time and date stamp as the configuration file of the panel. See page [➞ 208].

If the time and date stamps match, then the configuration data is the same in both SPC Pro and the panel (see note below). If the time and date stamps do not match, a warning message will be displayed to inform you that your local configuration data is not the same as the configuration of the panel.

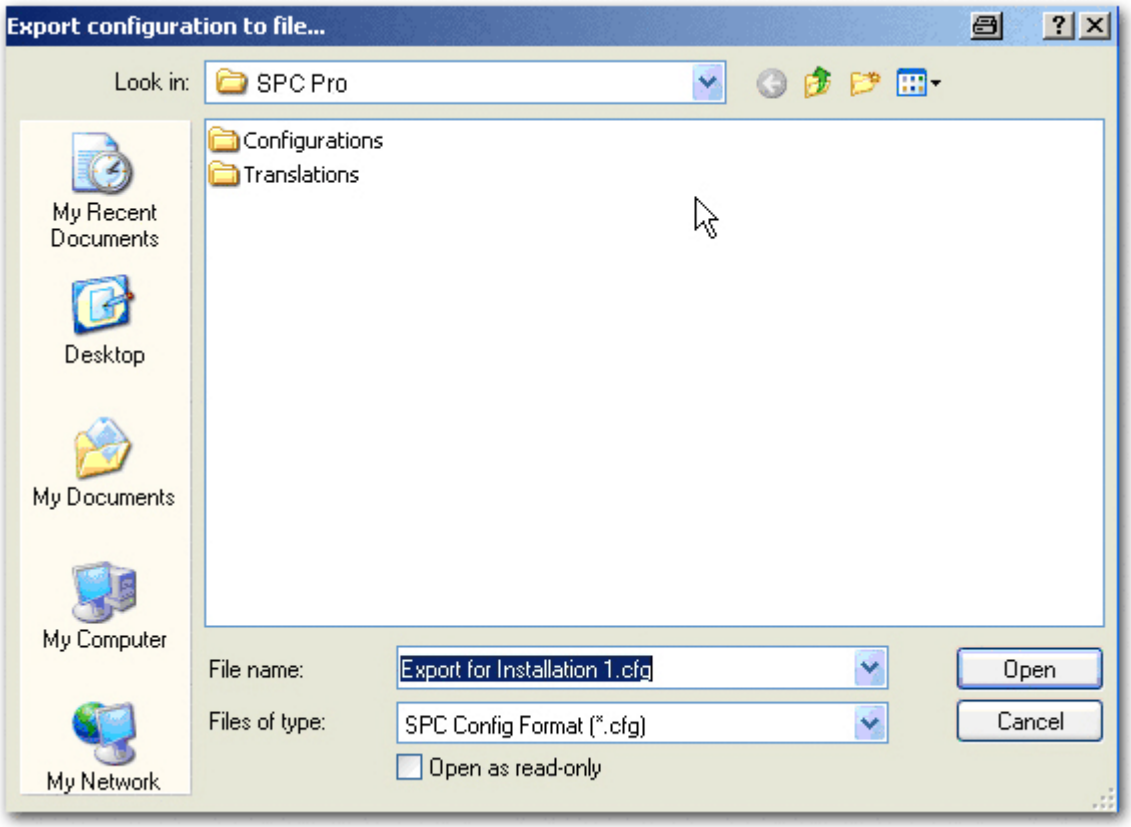
By uploading configuration settings from the panel and then saving them to a file on your PC (without making any changes), the time and date stamp will be altered. You will receive a warning message to this effect if you attempt to save the same unchanged configuration file back to the panel.

6.1.2 Exporting

A SPC configuration file (.cfg) contains all of the configuration information for a panel in a portable format that can be stored, attached in an email or imported to SPC Pro again for editing or downloading. The embedded browser on the panel and the Fast Programmer both store and retrieve configuration information in this format.

1. Open the window SPC Pro Installations.
2. Highlight the installation you wish to export.
3. Right click.

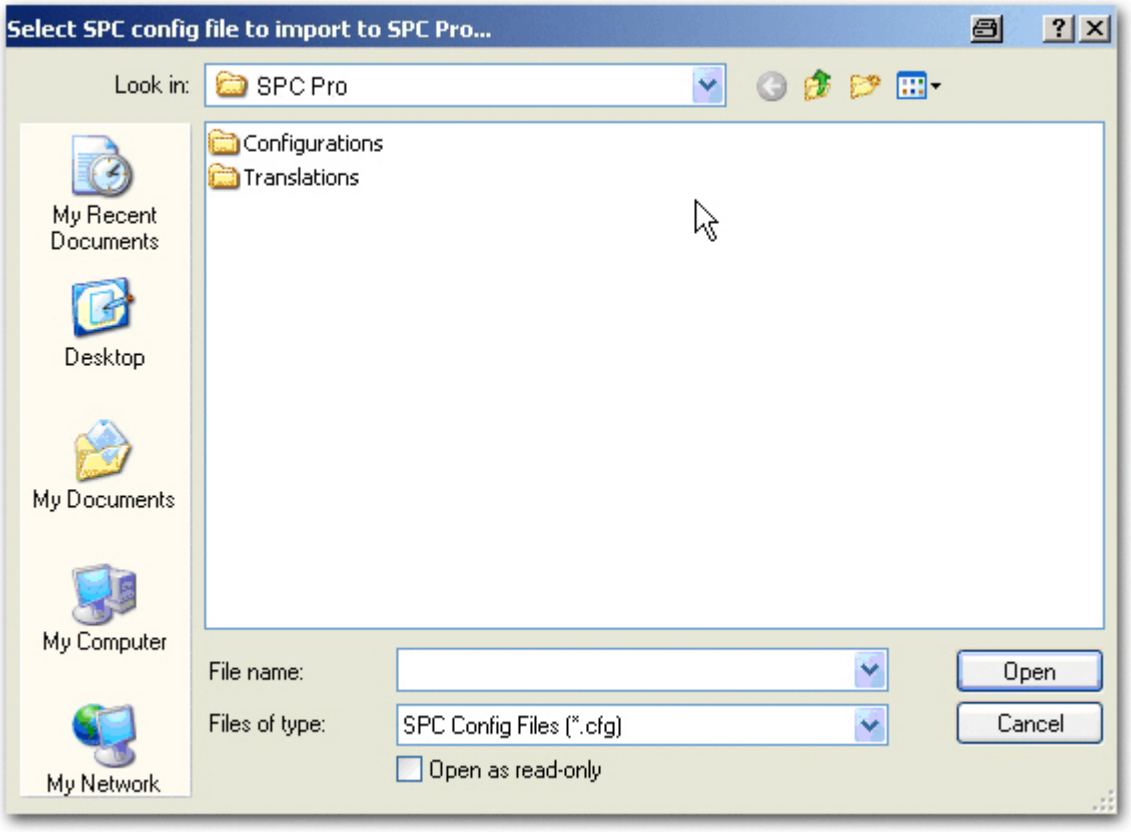
4. Select **Export Installation to File**.
   ⇨ The following window will be displayed:



5. Enter the file name.
6. Click **Save**.

6.1.3 Importing

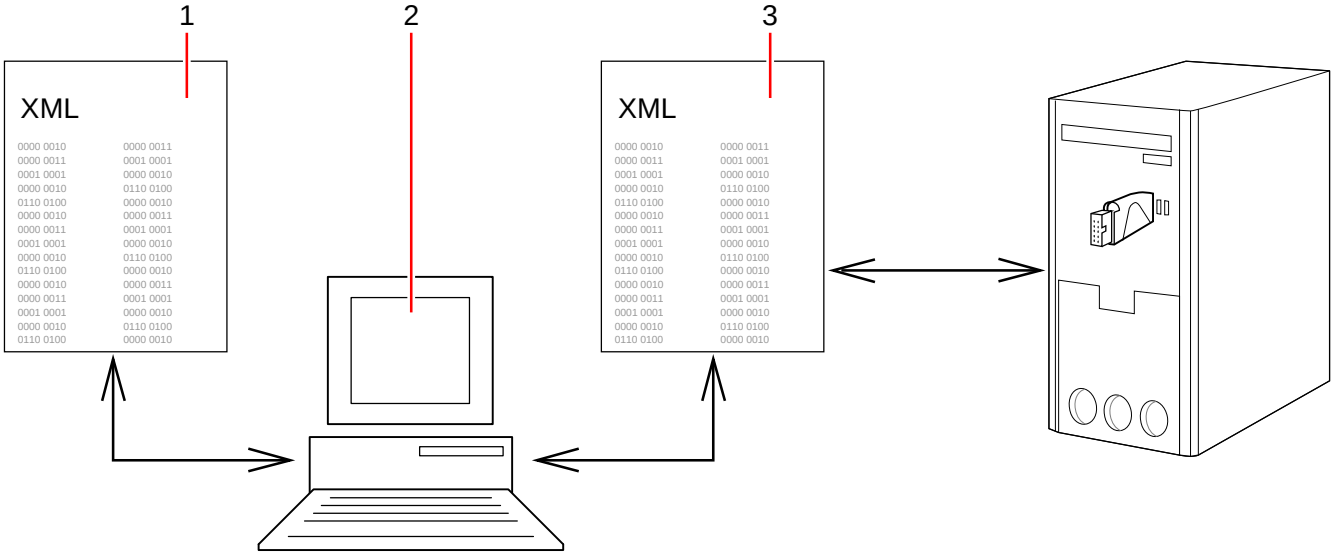
1. Open the window SPC Pro installations.
2. Select the menu **File > Import Installation from File**.
   ⇨ The following window will be displayed:



3. Select the .cfg file.
4. Click **Open**.

6.2 Programming configurations offline

SPC Pro provides the user with the ability to create, configure and store configuration files without ever connecting to a SPC panel. In this mode of operation you can create and configure an installation as required and store that configuration until such time as a connection to an actual installation is required.



1	Saved Config File
2	SPC Pro

3	Exported Config File

6.2.1 Saving

- Click the button  **Save Config File changes** in the config mode toolbar.

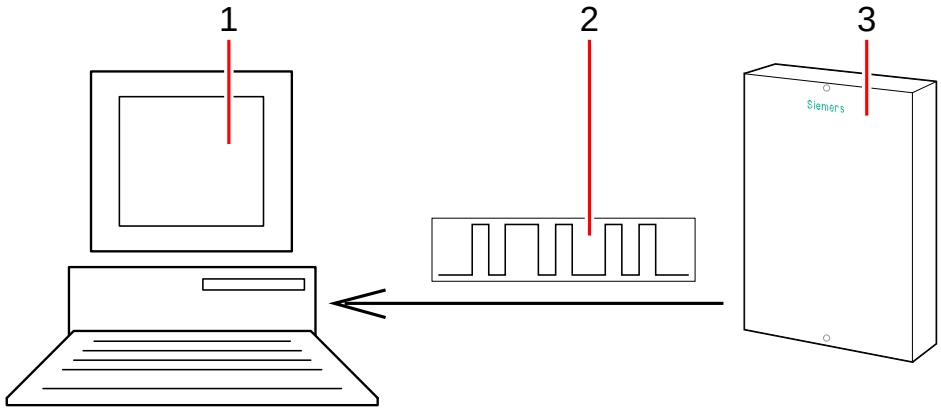
⇨ The file is saved locally on your hard disk and is automatically loaded when you access the configuration via SPC Pro.

6.2.2 Exporting

Installation configurations can be exported in a portable format for use by a Fast Programmer device or for emailing to remote sites etc.

These .config files can be saved directly to your hard disk under a programmable name for easy access. To load these files into SPC Pro use the Import Configuration option.

6.3 Connecting to the panel



1	SPC Pro
2	Status Data
3	SPC Panel

1. Connect to a target installation.
2. Select the local installation configuration on the SPC Pro.
3. Enter the configure mode.
4. Connect to the panel via one of the connection modes (see page [→ 10]).

On successfully connecting to the panel, the following status information is sent from the panel to SPC Pro:

- Firmware Version
- Configuration file time & date stamp
- Hardware overview: Modem status, wireless receiver status, power, system tampers
- X-BUS status
- Ethernet status
- System Alert status
- Zone status

- Areas status
- Door status

This status information provides the user with an overview of the essential panel configuration data without having to upload the complete configuration from the panel.

SPC Pro will not allow you to connect to a version of panel firmware that is not compatible with it. You must ensure that you have the correct SPC firmware release.

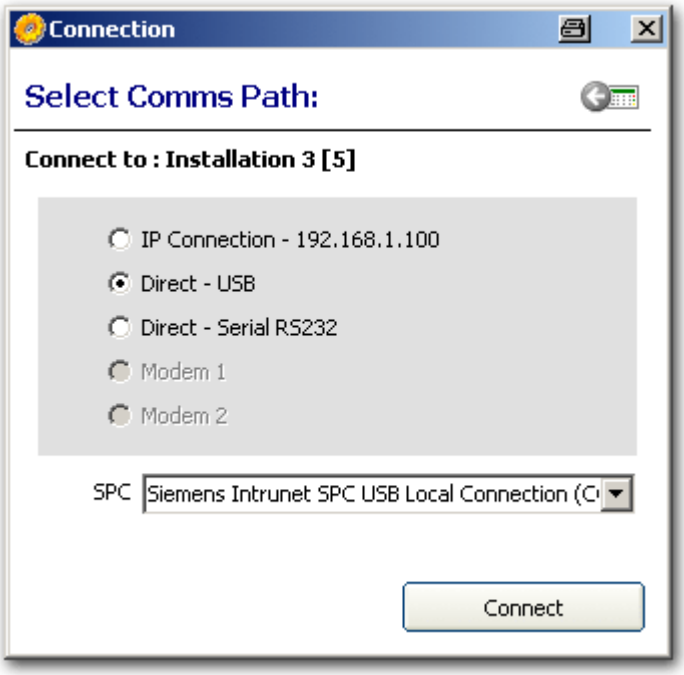
6.3.1 Enabling a connection on the panel

To enable a SPC Pro connection to a panel you must program the panel to accept a connection:

1. Enter the Full Engineer mode from a keypad connected to the panel.
2. Enter **Full Engineer**.
3. Select **Utilities**.
4. Select **SPC Pro**.
5. Select **Enable SPC Pro**.
6. Select **Enabled**.
7. Select **Engineer Access**.
8. Select **Enabled**.
9. Select **Password**.
10. Program the password that will be required for a connection (default password: password).

6.3.2 Establishing a connection to the panel

1. Click the icon  in the Config Mode Toolbar.
   ⇨ The following window will be displayed:27



Only the connection modes that were programmed for that installation when it was added or edited will be displayed. See page [→ 15].

2. Select the appropriate connection mode.
3. Click **Connect**.

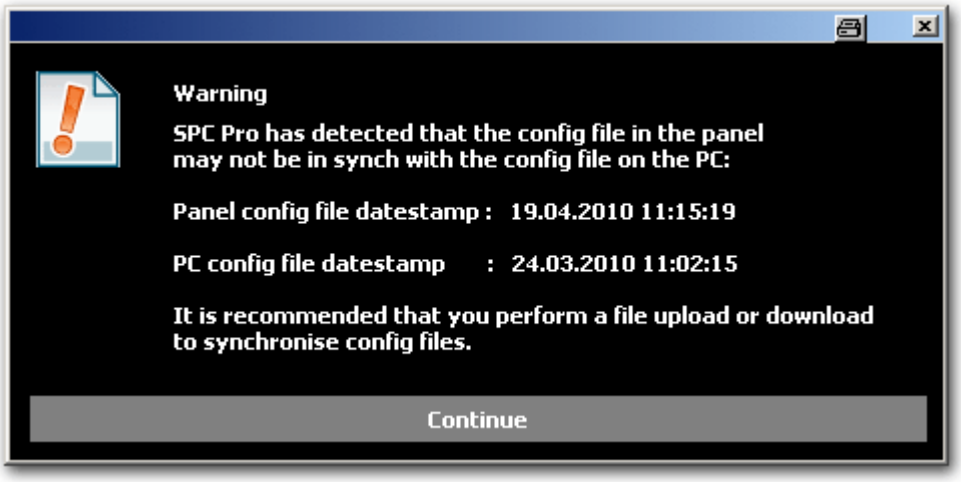
Firmware version

SPC Pro will read the status information on connecting to the panel and display a warning if the version of firmware detected in the panel is not supported by SPC Pro.

If the firmware version of the panel is not supported by SPC Pro please contact Vanderbilt for the latest panel firmware upgrade quoting the version number of your X Pro program.

Configuration file Synchronisation

If the configuration information detected in the panel does not match the configuration programmed in SPC Pro the following window will be displayed:



Before you can send or receive configuration data you must synchronize the configuration file on your PC with the panel configuration file. You can do this by overwriting one file with the other.

Vanderbilt recommend that you get the configuration file from the panel BEFORE you send you configuration changes to the panel. This ensures that BEFORE you make any configuration changes, you are working with an exact copy of the current installation configuration.

To synchronize the PC and the panel configuration files:

1. Click the button **Continue**.
2. Click on one the following options:
   - Get Config file from panel: uploads panel configurations from panel to PC.
   - Send Config file to panel: downloads panel configurations to panel.

Get Config file from panel

Any configuration changes made from a keypad on site while SPC Pro is connected will be overwritten when you send your configuration file to the panel.

If you have not uploaded the configuration from the panel, then it is recommended that you do so. You may then program your configuration changes on top of the downloaded information. When you have completed your changes send it to the panel. Only those configuration settings you have changed are changed on the panel.

Send Config file to panel

You may wish to send your configuration file to the panel without ever loading configuration data from the panel. In this case it is important that you have a comprehensive and accurate knowledge of the panel configuration before you send your configuration file.SPC Pro will not allow you to send expander configuration information that does not match the actual expander configuration on the panel. See page [→ 91].

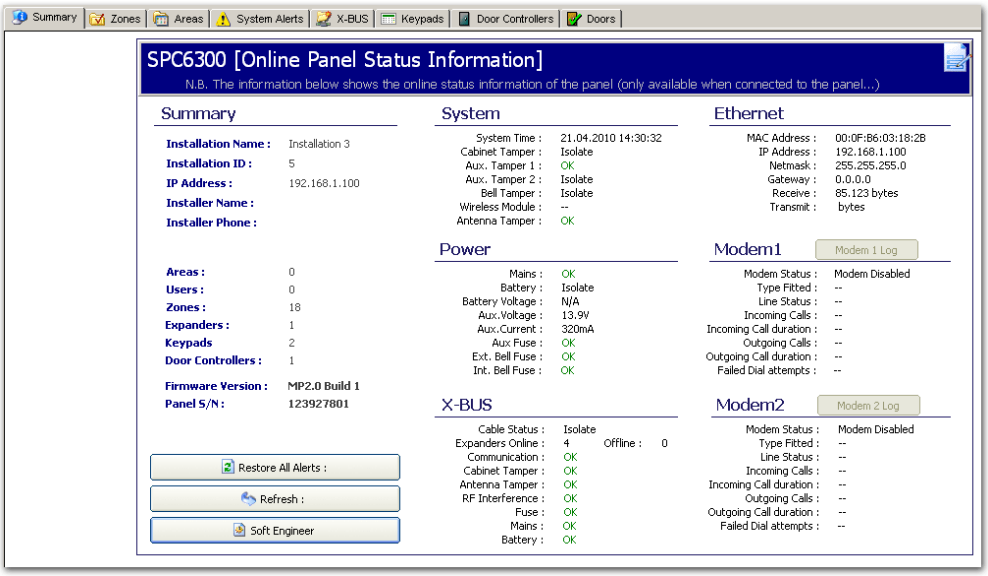
7 Panel status

7.1 Status

This page displays the status and summary of the main SPC components, including system, power, X-BUS and communications.

Panel Status

1. Click the tab **Summary**.
2. See tables below for further information.



Offline\Online Panel Status Information	Displays the parameters programmed for the installation when it was created (Installation name, ID, etc.). This data will be updated by the panel data when you connect to the panel. The firmware version and panel S/N fields are also displayed as soon as a connection is made to the panel.

Performable actions

The following actions are only possible if a connection has been established.

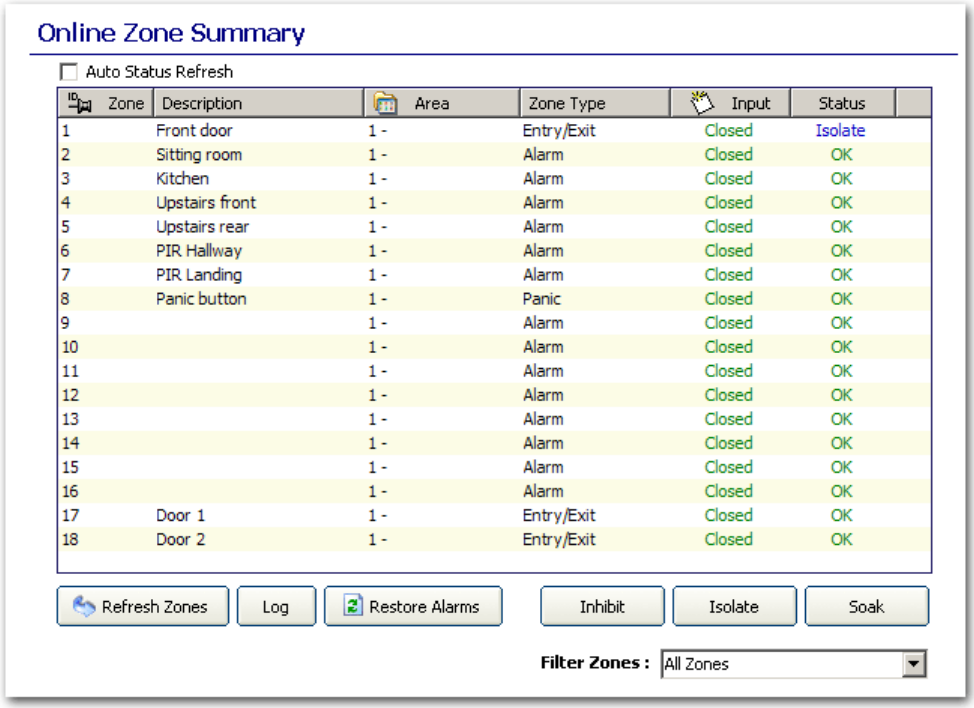
Restore All Alerts	Restores all active alerts on the panel. These alerts messages are displayed in red text opposite the relevant item.
Refresh	Updates any changes in panel status. You must refresh the status window to display the actual panel status at any particular moment.
Full Engineer / Soft Engineer	To toggle between Soft- and Full Engineer modes. Full Engineer mode disables alarms and prevents reporting of events to a central station.

7.2 Zones

For configuration see page [➞ 120].

Panel Status

1. Click the tab **Zones**
2. See tables below for further information.



Auto Status Refresh	Tick this button to activate an automatically refreshing of the zone summary. This can only be done for all zones, and not for filter zones.
Zone Description	Text description of the zone (max. 16 characters).
Area	Areas to which this zone is assigned.
Zone Type	The type of zone (Alarm, Entry/Exit, etc.).
EOL Quality	Displays the EOL quality for the zone state resistance range. Possible values are: ● Good — Nominal value +/-25% of the defined range. ● OK — Nominal value +/- 50% of the defined range. ● Poor — Nominal value +/- 75% of the defined range. ● Unsatisfactory — any other value. ● Noisy — indicates a problem detecting the signal. The cabling may be in close proximity to a mains cable or other source of interference. This column is only visible in Engineer mode. For more information on nominal resistance values and their defined ranges, see Wiring the zone inputs.
Input	The detected input state of that zone (Unknown, Open, Closed, Disconnect, Short, Pulse, Gross, Masked, Fault, Out of bounds, Unstable, DC Sub, Noisy). DC Sub is an input tamper alert. DC substitution performs a periodic check to ensure that no external voltages are being applied to that circuit. Unstable: An unstable state occurs when the zone input resistance value is not stable over a defined sampling period. Noisy: A Noisy state occurs when an external interference is induced onto the input circuit over a defined sampling period. Out Of Bounds: An Out of Bounds state will occur when the resistance value on the zone input does not come within accepted tolerances of the present EOL values.

Status	The programmed status of that zone. A status value of Normal means that the zone is programmed to operate normally. The following is a complete list of possible values: Isolate, Soak, Inhibit, Tamper, Alarm, Fire Exit, Warning Fault, Holdup Fault, Detector Fault, Line Fault, Panic, Hold Up, Tech, Medic, Lock, Fire, Trouble, PIR Masked, Normal, Actuated, Tamper , Post Alarm. A zone is in the post alarm status if an alarm occurred and the confirmed alarm timed out. This reinstates the zone, however it also flags that an alarm did occur.

Performable actions

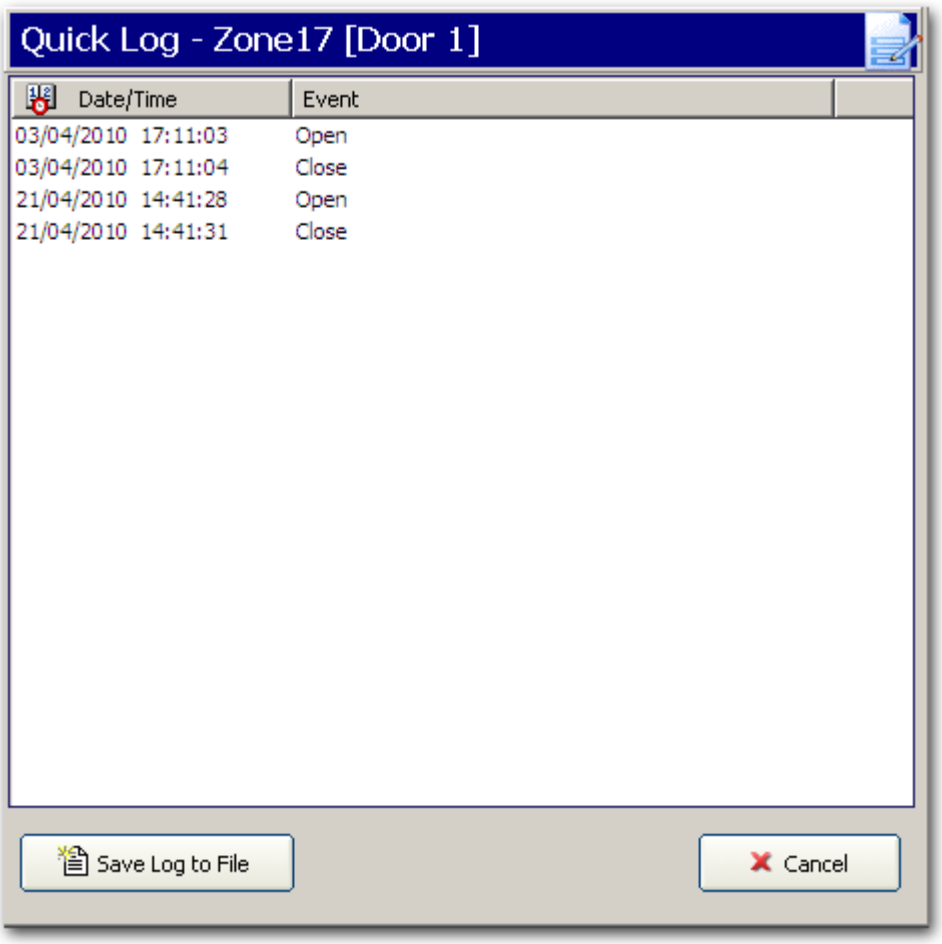
Refresh Zones	Updates the status information displayed for the panel.
Log	Highlight a zone and click on the Log button to view a log of the input status of that zone. [→ 31]
Inhibit ⓘ	Click this button to inhibit a fault or open zone. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Restore Alarms	Click this button to restore the alarm condition of the panel.
Isolate	Zone Description . Isolating a zone will deactivate that zone until such time as the zone is explicitly deisolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.
Soak	Highlight a zone and click this button to perform a Soak test on that zone.
Seismic Test	Click this button to initiate a test of the selected seismic sensor. For more information on seismic sensors, see Seismic Sensors [→ 246].
Hide Closed	Click this button to hide all closed inputs.
Filter Zones	Select a zone type from the dropdown menu. Only the summary of this zone type will be displayed.

7.2.1 Quick log - Zone X

To view a quick log of the input status of a zone:

1. Highlight the zone.
2. Click the button **Log**.

⇨ The following window will be displayed:



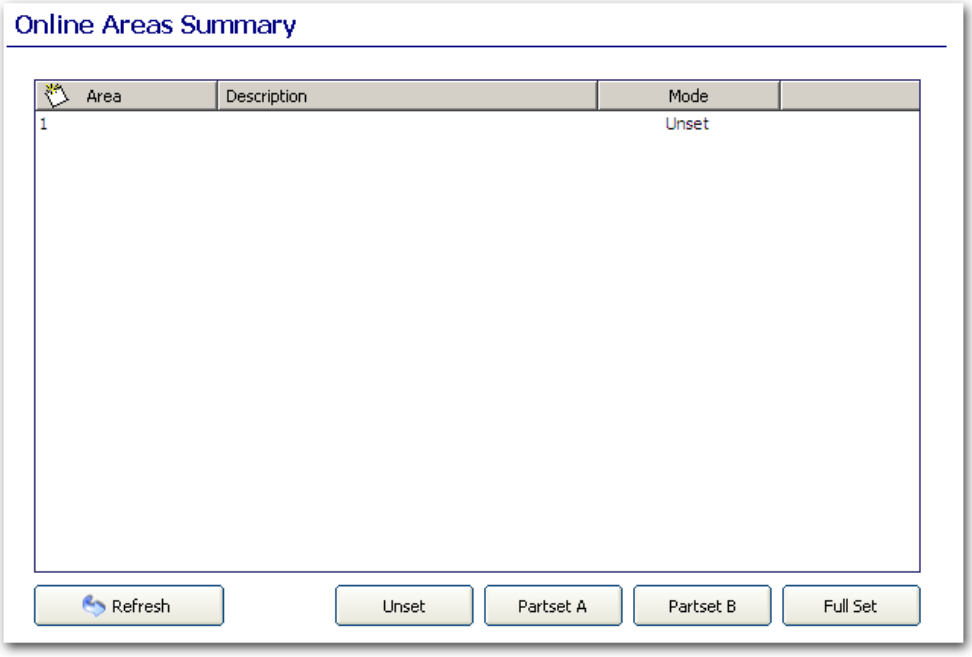
The most recent event is displayed at the bottom of the list.

7.3 Areas

Each area defined on the system and its status is revealed here.
For configuration see page [→ 122].

Panel Status

1. Click the tab **Areas**.
   ⇨ The following window will be displayed.
2. See table below for further information.
3. Click **Refresh**.



Area	Area number.
Description	Text description of the area (max. 16 characters).
Mode	The current armed mode of the area.

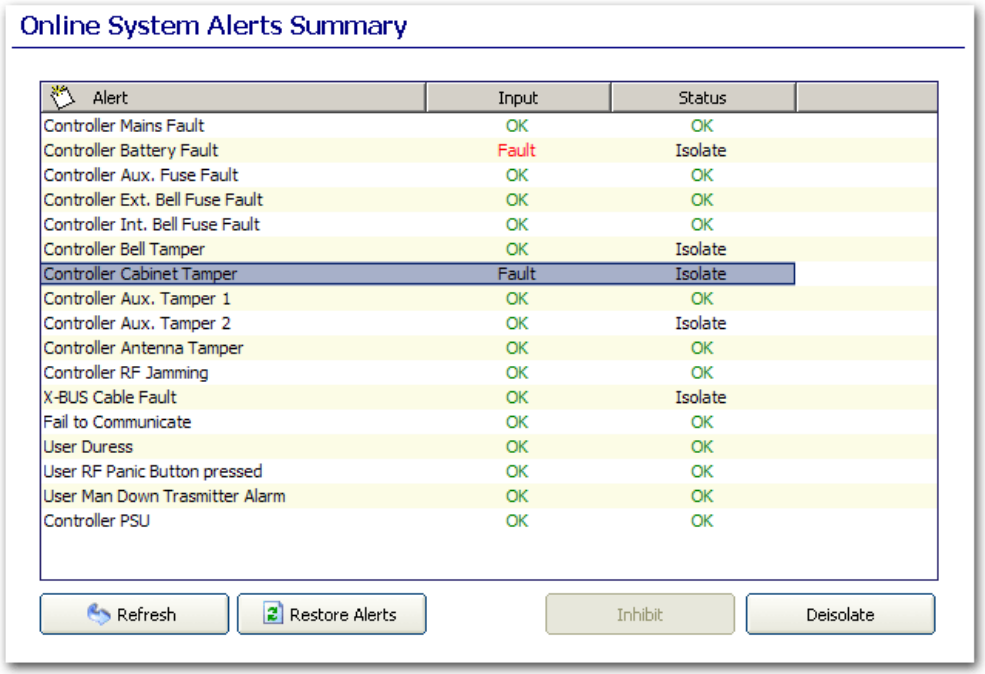
To change the mode of the area:

1. Click the button  **Soft Engineer Mode** in the Config Mode Toolbar.
2. Select an area from the list.
3. Select a mode for this area by clicking on the relevant button (Unset, Partset A, Partset B, Full Set).

7.4 System alerts

Panel Status

1. Click the tab **SystemAlerts**.
2. See tables below for further information.



Alert	Description of the system alert.
Input	The actual state of the alert that was detected on the panel (OK, Fault).
Status ⚠	The programmed status of the system alert, i.e. whether the alert has been isolated or inhibited. A status value of OK is displayed if the alert condition has not been disabled in any way (see page).

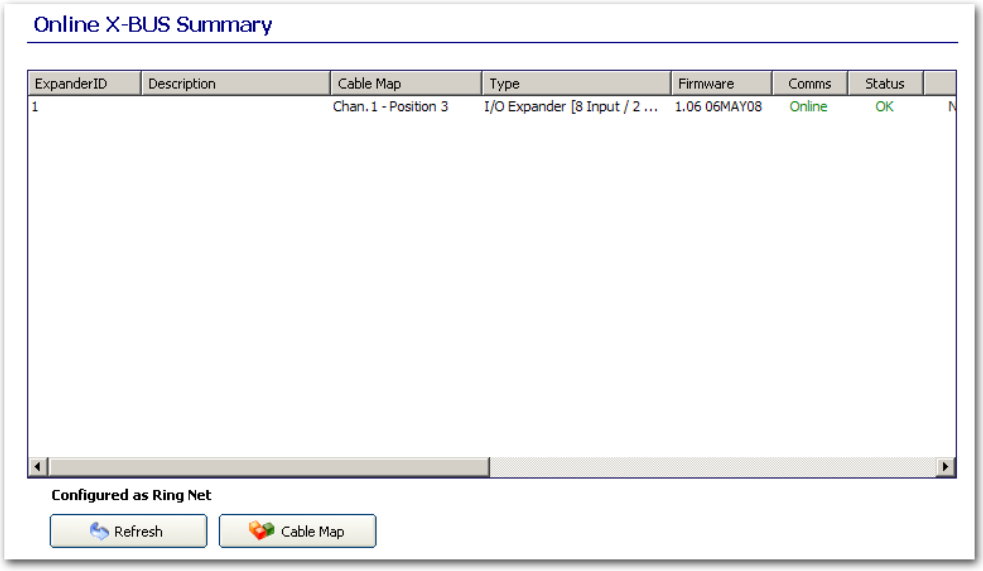
Performable actions

Refresh	Click this button to update the status of the system alerts.
Restore Alarms	Click this button to restore ALL alerts on the panel
Inhibit ⓘ	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security EN 50131 Grade 3.
Isolate	Click this button to isolate the zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

7.5 X-BUS

Panel Status

1. Click the tab X-BUS.
2. See tables below for further information.



Expander ID	This ID number is a unique identifier for the expander.
Description	Text description of the expander. This text will also appear on the browser and keypad.
Cable Map	The order that the system sees the expanders on the X-BUS.
Type	The type of expander detected (I/O, PSU, keypad etc.).
Firmware version	The firmware version of the expander.
Comms	The status of the expander (online or offline).
Status	The status of the expander (OK, Fault).
PSU	Type and version of PSU, if fitted.
Wireless	Model of wireless module, if fitted.

Performable actions

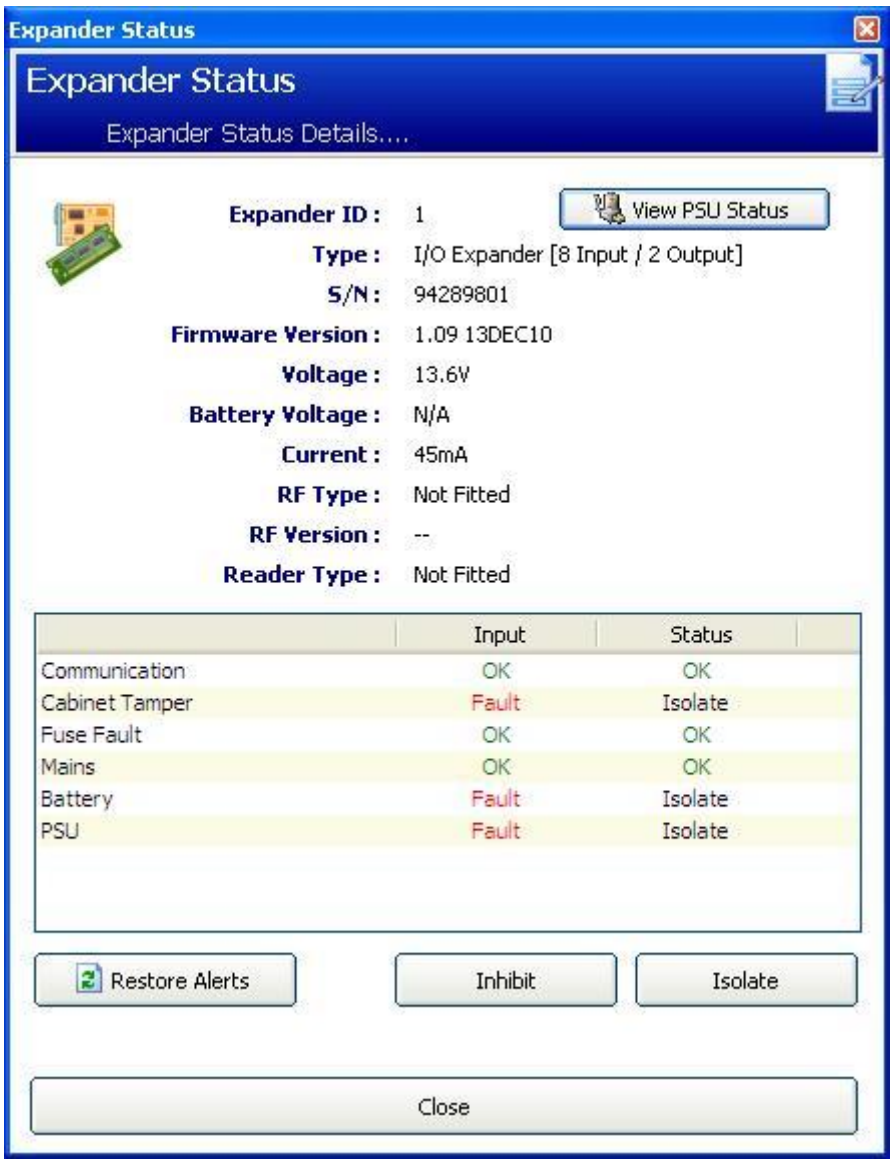
Refresh	Click the button to update the status of the X-BUS.
Cable Map	Click the button to get a list of expanders/keypads that are physically connected to the panel.

On first connecting to the panel this information will be displayed providing you with a comprehensive overview of the X-BUS configuration without requiring you to upload the configuration file from the panel. This information is particularly useful if you are attempting to add/configure expanders on a panel. See page [→ 91].

Expander status

To view the online status of an expander connected to the X-BUS:

1. Click an expander from the list.
2. See tables below for further information.



Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the X-BUS cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
Fuse fault	The physical and programmed status of the expander fuse.
Mains	The physical and programmed status of the mains power.
Battery	The physical and programmed status of battery.
PSU	The physical and programmed status of the connected PSU. To view more detailed status on the PSU, click on the **View PSU Status** button. (See PSU status)

Performable actions

Restore Alerts	Click the button to restore ALL alerts on the panel.
Inhibit ⓘ	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

The expander status data will vary depending on the type of expander selected, i.e. the window displayed shows the physical and programmed status of a number of parameters for an expander.

7.5.1 PSU Status

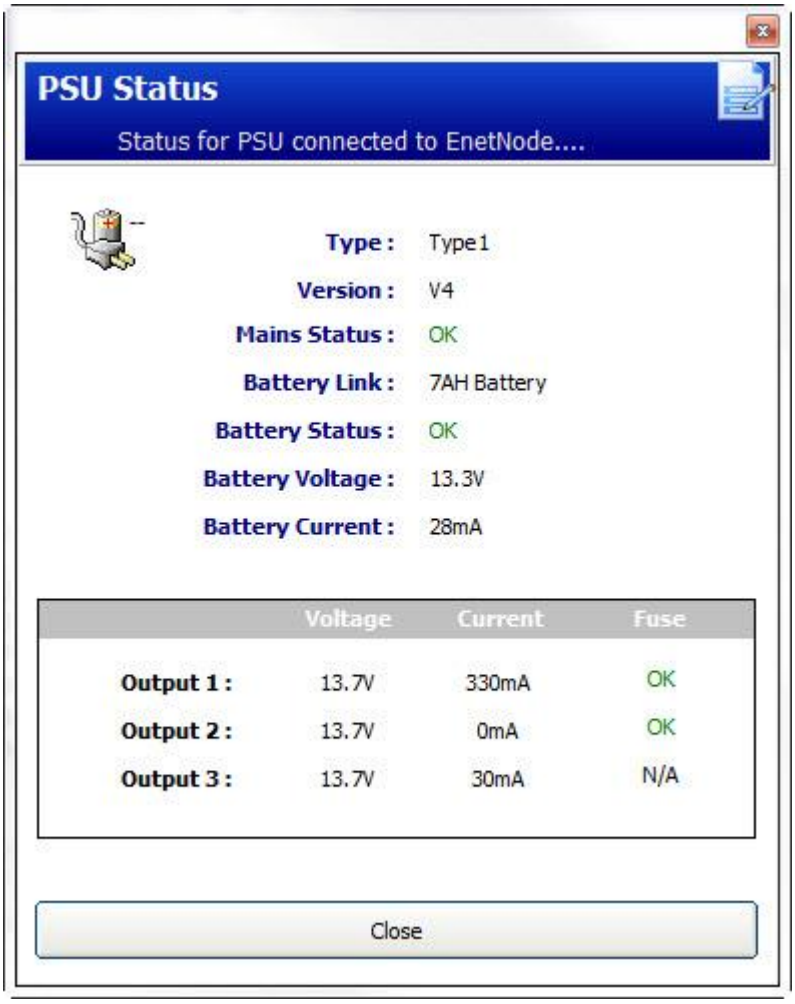
The **PSU Status** window displays details of the current status of the PSU and its outputs in addition to the status of any connected batteries.

The following PSU types are supported:

- SPCP 332/333 Smart PSU (referred to as Smart PSU)
- SPCP 355 Smart PSU

Smart PSU Status

The following image shows the Smart PSU status:

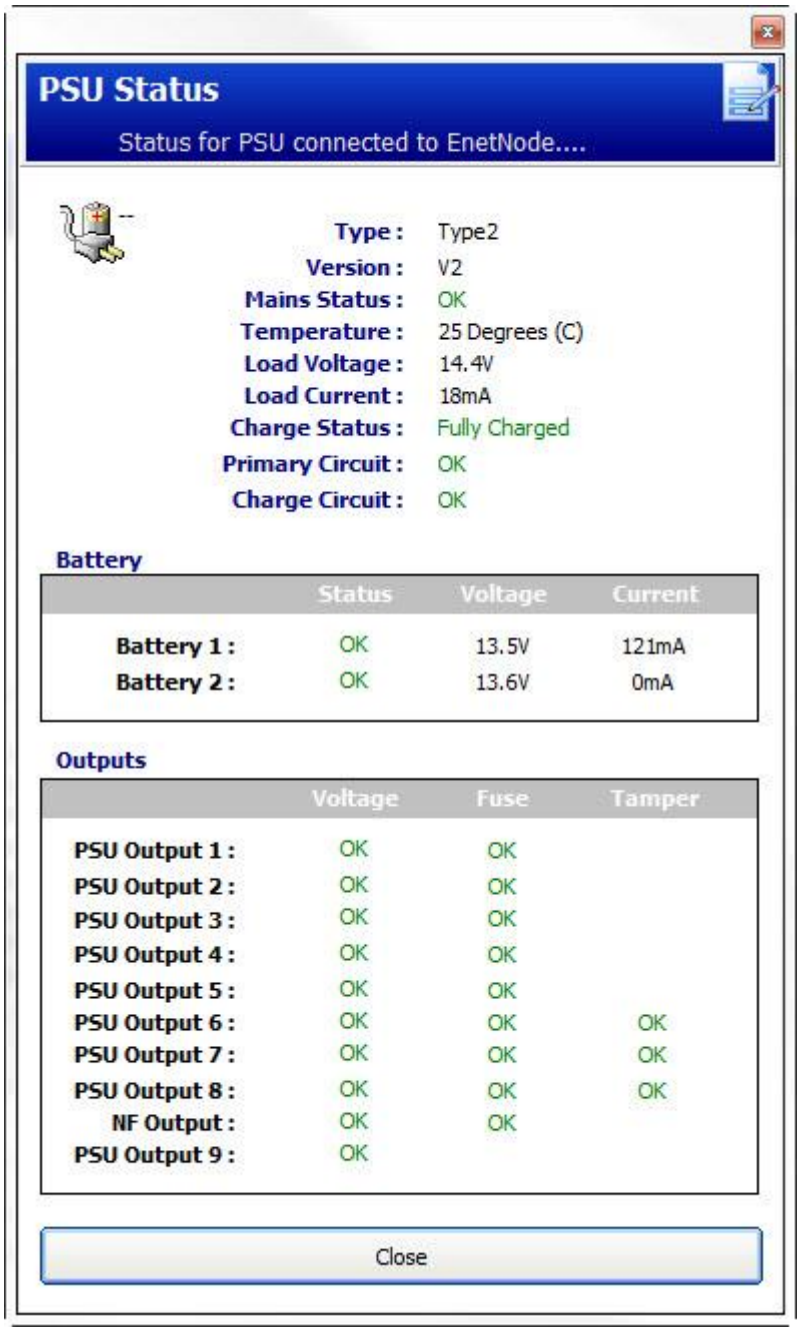


Name	Description
Type	The type of power supply unit (PSU).
Version	The version of the PSU.
Mains Status	Displays the condition of the mains connection. Possible values are Fault or OK.
Battery Link	Displays the type of battery connected.

Name	Description
Battery Status	Displays the condition of the battery connection. Possible values are Fault or OK.
Battery Voltage	Displays the voltage reading of the battery.
Battery Current	Displays the current taken from the battery.
Outputs	Displays the voltage on the outputs, the current drawn by the output and the condition of the fuse on the output.

SPCP355 Smart PSU Status

The following image shows the SPCP355 PSU status.



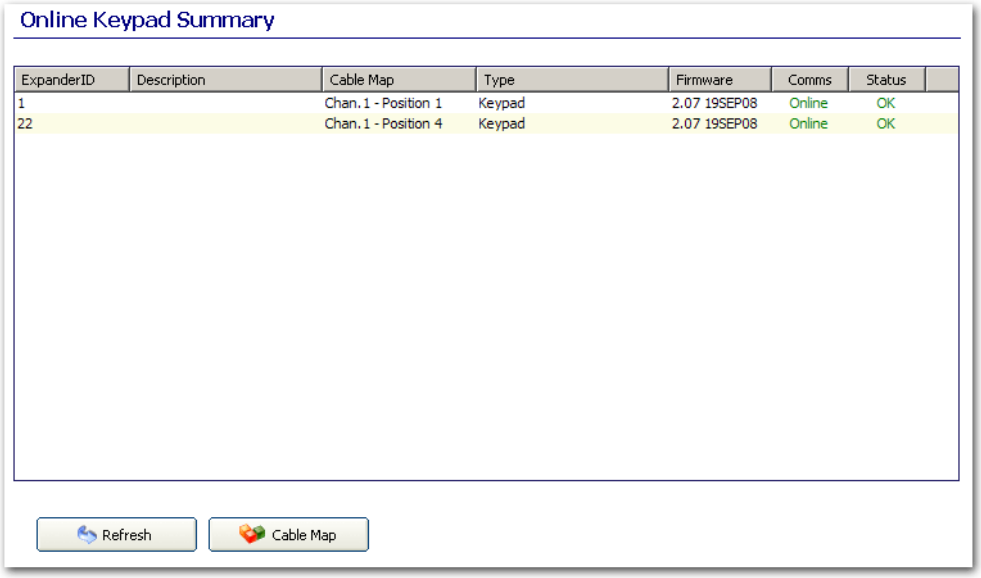
Name	Description
Type	The type of power supply unit (PSU).
Version	The version of the PSU.
Mains Status	Displays the condition of the mains connection. Possible values are Fault or OK.
Temperature	Displays the temperature of the PSU.
Load voltage	The voltage on the PSU
Load Current	The current drawn by the PSU.
Charge Status	Displays the condition of the battery charge.
Primary Circuit	Displays the condition of the primary circuit which supplies power when the mains is connected..
Charge Circuit	Displays the condition of the charge circuit which charges the batteries when the mains is connected..
Battery	Displays the charge status, voltage and current available from the batteries.
Outputs	Displays the voltage, fuse condition and tamper condition of the PSU outputs.

7.6 Keypads

For configuration see page.

Panel Status

1. Click the tab **Keypad**.
2. See tables below for further information.



Expander ID	This ID number is a unique identifier for the keypad.
Description	Text description of the keypad (max. 16 characters).
Cable Map	The position of the keypad on the X-BUS.
Type	The type of expander detected (=keypad).
Firmware version	The firmware version of the keypad.
Comms	The status of the keypad (online or offline).
Status	The status of the keypad (OK, Fault).

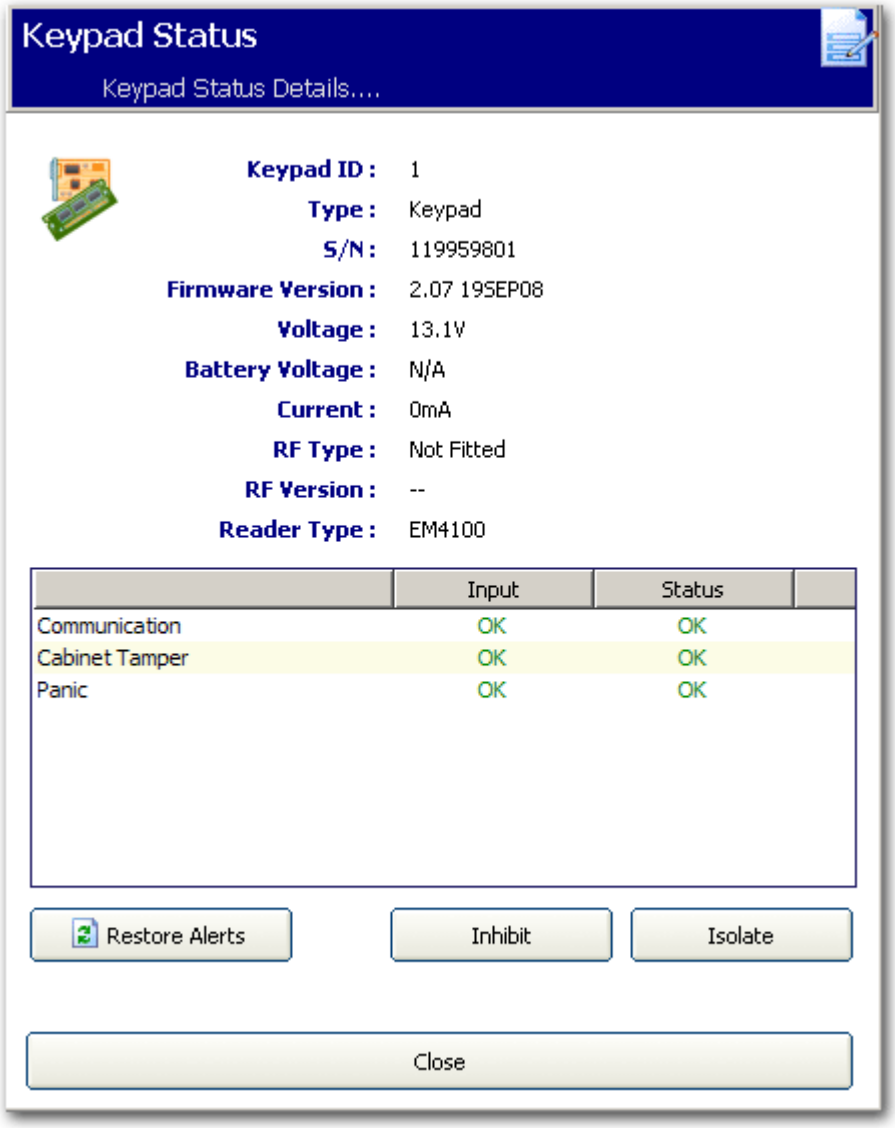
Performable actions

Refresh	Click on the refresh button to update the status of the system alerts.
Cable Map	Click the button to get a list of expanders/keypads that are physically connected to the panel.

Keypad status

To view the online status of a keypad:

1. Click a keypad from the window Online Keypad Summary (see page [→ 39]).
2. See tables below for further information.



Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
PACE	Applies only to Keypads with a PACE receiver installed.
Panic	Keypad Panic Alarm status revealed.

Performable actions

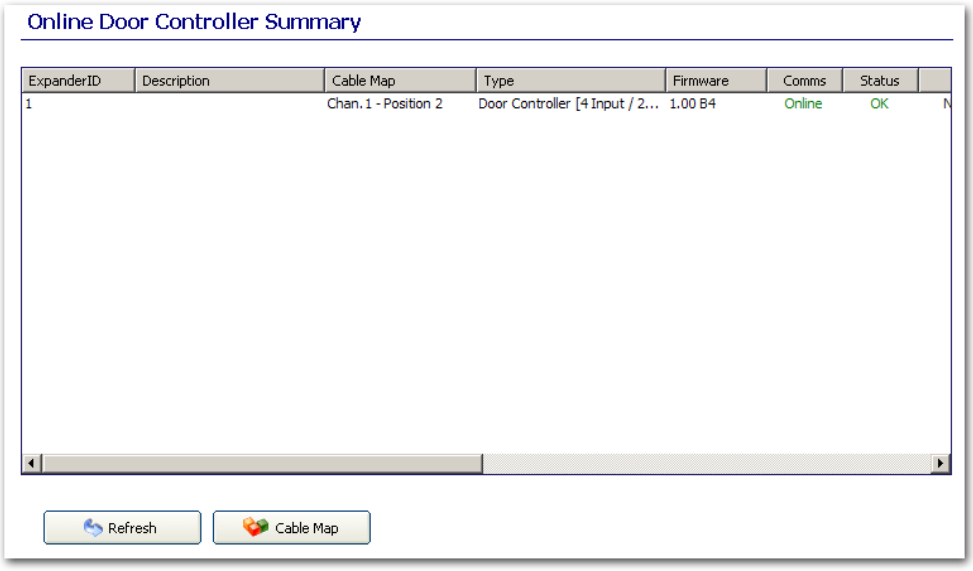
Restore Alerts	Click the button to restore all alerts on the panel.
Inhibit (!)	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

7.7 Door Controllers

General

Panel Status

1. Click the **Door Controllers** tab.
2. See table below for further information.



Expander ID	This ID number is a unique identifier for the door controller.
Description	Text description of the door controller (max. 16 characters).
Cable Map	The position of the door controller on the X-BUS.
Type	The type of expander detected (=door controller).
Firmware version	The firmware version of the door controller.
Comms	The status of the door controller (online or offline).
Status	The status of the door controller (OK, Fault).
PSU	Specifies if the door controller has a PSU.

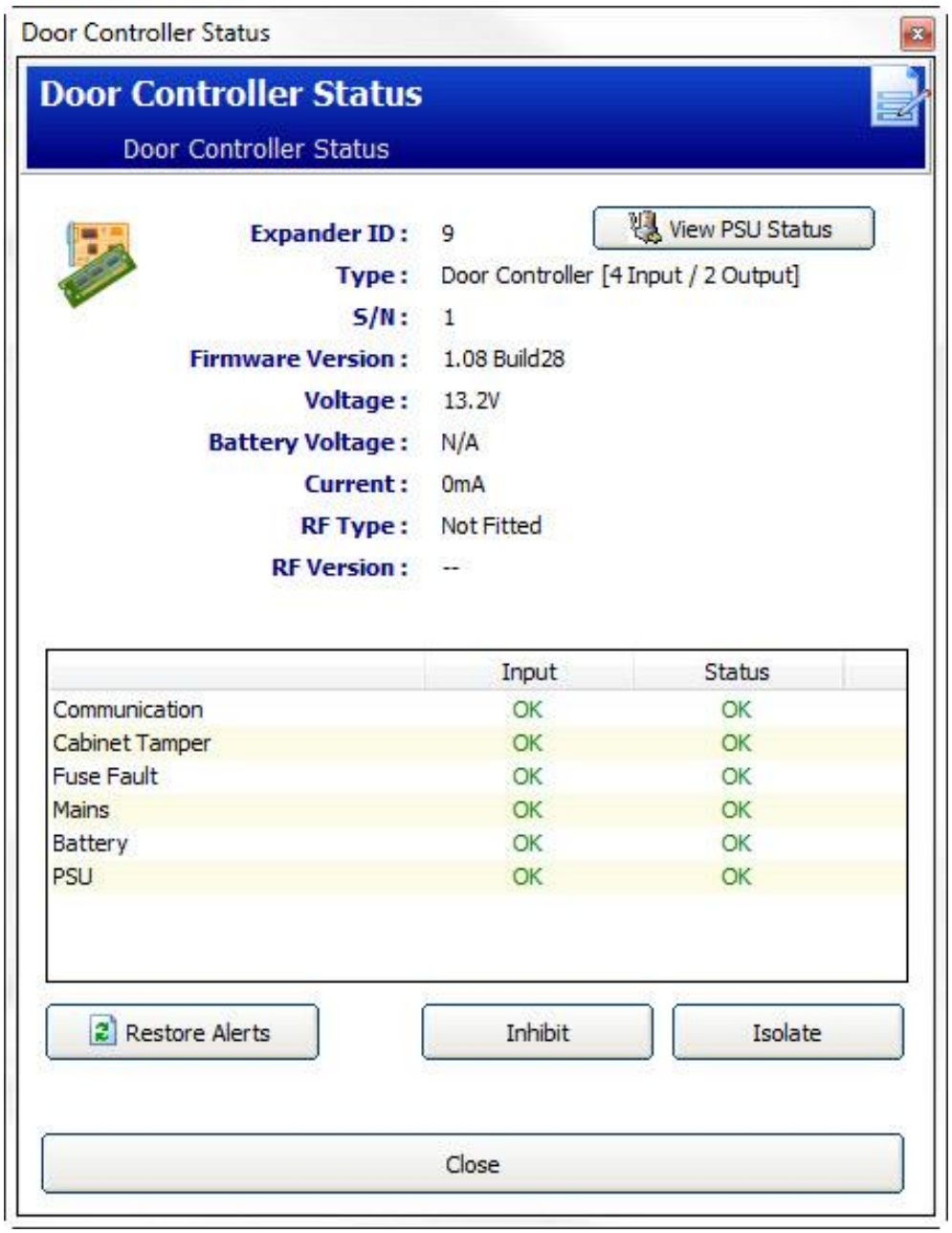
Performable actions

Refresh	Click on the refresh button to update the status of the system alerts.
Cable Map	Click the button to get a list of expanders/keypads that are physically connected to the panel.

Door controller status

To view the online status of a door controller:

1. Click a door controller from the list.
2. See tables below for further information.



Communication	The physical status (OK, Fault) and the programmed status (OK, Isolated, Inhibited) of the keypad cable connection to the expander.
Cabinet Tamper	The physical and programmed status of the expander cabinet tamper.
Fuse Fault	The physical and programmed status of the door controller fuse.

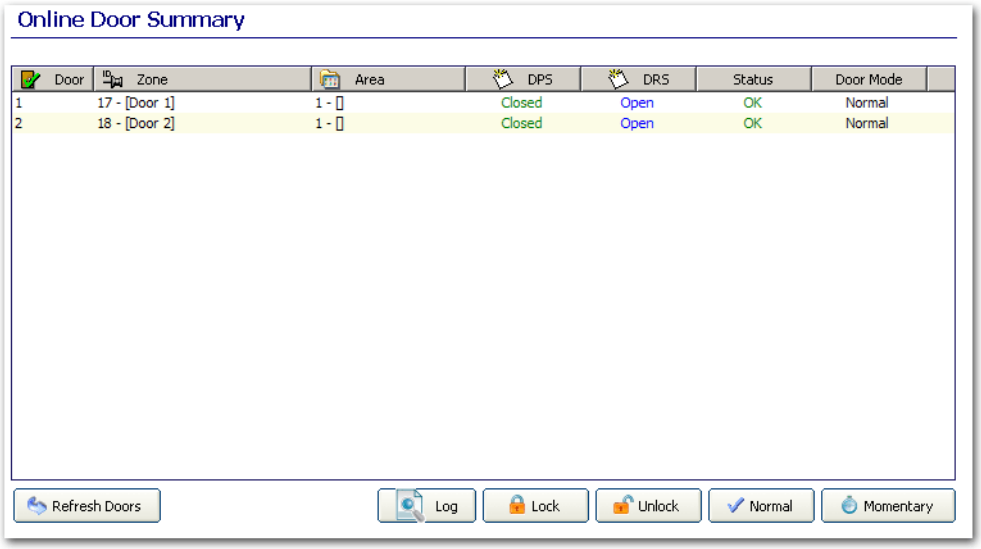
Performable actions

Restore Alerts	Click the button to restore all alerts on the panel.
Inhibit (!)	Click this button to inhibit a fault condition. The inhibit operation will disable that fault or zone for one arming period only. Inhibit operation is not available in Security Grade EN 50131 Grade 3.
Isolate	Click this button to isolate that zone. Isolating a zone will de-activate that zone until such time as the zone is explicitly de-isolated again. It is recommended that you exercise caution when isolating zones as those zones will not be active every time the system is SET.

7.8 Doors

Panel Status

1. Click the **Doors** tab.
2. See tables below for further information.



Door	This ID number is a unique identifier for the door.
Zone	The zone number the door position sensor is attached to (only if the door position sensor input is also used as intrusion zone).
Area	The area the door position sensor input and the card reader are assigned to.
DPS	Status of the door position sensor.
DRS	Status of the door release switch.
Status	The status of the door (OK, fault).
Door Mode	Specifies the door operate mode.

Performable actions

Refresh	Updates the door summary.
Log	Displays a log of events for the selected door.
Lock	Locks the selected door.
Unlock	Unlocks the selected door.
Normal	Returns the door to normal system control.
Momentary	Unlocks the door for one timed interval.

7.8.1 Access log - Door X

To view a quick log of the status of a door:

▷ SPC Pro is connected to a panel.

1. Click a door from the list.

2. Click the **Log** button.

The most recent event is displayed at the bottom of the list.

3. Click the **Save Log to File** button to save the current event log to a file (e.g. *.txt).

⇨ You can open this log file after disconnecting from the panel.

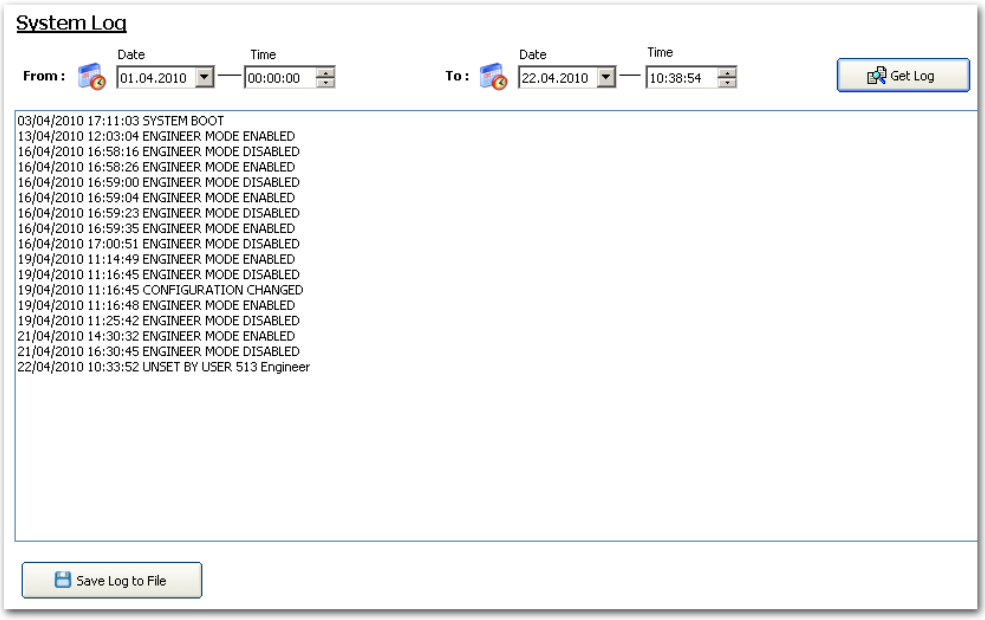
7.9 System Log

This log displays all the system events of the SPC system.

System Log

▷ SPC Pro is connected to a panel.

- Click the **System Log** tab.
  ⇨ The following window will be displayed:



To view events that occurred over specific time periods:

1. Enter the start date and time for the log in the **From: Date & Time** dropdown menu.
2. Enter the end time and date for the log in the **To: Date & Time** dropdown menu.
3. Click the button **Get Log**.
   ⇨ The current system log of events will be downloaded from the panel.
   ⇨ The system log of events between these time and dates will be listed in following order: Date, Time, Event and Description.

In order to avoid multiple events from the same source filling the log, the SPC system, in accordance with standards, permits the logging of only 3 activations of the same zone in one set period.

4. Click the button **Save Log to File** to save the current event log to a file (e.g. “log.txt”).

⇨ You can open this log file after disconnecting from the panel.

If you use SPC Pro to change the system language on the panel, the system log language will only update after you disconnect and reconnect to panel.

7.10 Access Log

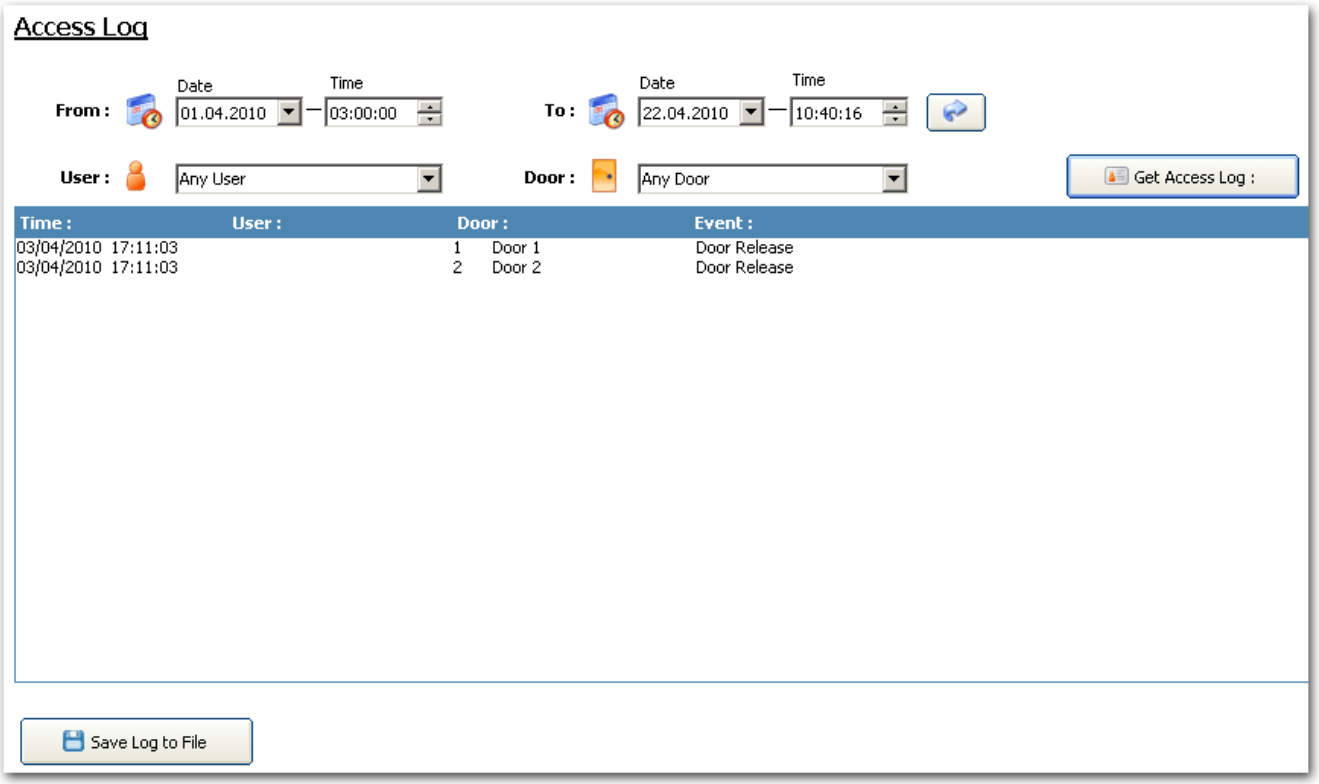
The log provides all the access events of the SPC system.

Panel Access Log

▷ SPC Pro is connected to a panel.

In order to avoid multiple events from the same source filling the log, the SPC system in accordance with standards, permits the logging of only 3 activations of the same zone in the one set period.

- Click the **Panel Access Log** tab.
  ⇨ The following window will be displayed:



To view access events that occurred over specific time periods:

1. Enter the start date and time for the log in the From: Date & Time dropdown menu.
2. Enter the end date and time for the log in the To: Date & Time dropdown menu.
3. Enter the user name from the User dropdown menu.
4. Enter the door name from the Door dropdown menu.
5. Click the **Get Access Log** button.
   - ⇨ The current system log of access events will be downloaded from the panel.
   - ⇨ The system log of access events between these time and dates will be listed in following order: Date, Time, User, Door and Event.
6. Click the button **Save Log to File** to save the current event log to a file (e.g. .txt).

⇨ You can open this log file after disconnecting from the panel.

8 Users

The following table shows the maximum number of users, user profiles and user devices for the panel:

Maximum No.	SPC4xxx	SPC5xxx	SPC6xxx
Users	100	500	2500
User Profiles	100	100	100
User Profiles per User	5	5	5
PACE Devices	32	250	250
SMS IDs	32	50	100
Web Passwords	32	50	100
RF Fobs	32	50	100
MDT Devices	32	32	32

⚠ WARNING

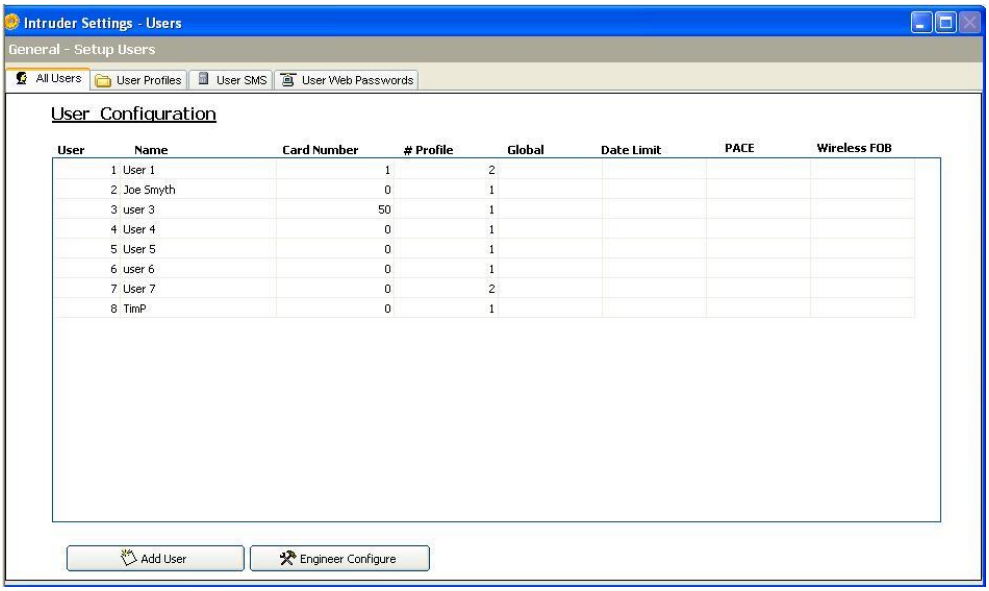
If upgrading from a firmware version prior to version 3.3, please note the following:
- The Engineer web password, if configured, is deleted and must be reentered after upgrade.
- All existing users will be assigned to new user profiles corresponding to their previous user access levels. If max. number of user profiles is exceeded, no profile is assigned (see User Profiles [→ 51]). Please review all user configuration after a firmware upgrade.
- The default Engineer ID is changed from 513 to 9999.

8.1 Adding / Editing a User

For general information on max. number of users and max. number of areas please refer to the Installation & Configuration Manual of the appropriate SPC control panel.

Setup Users

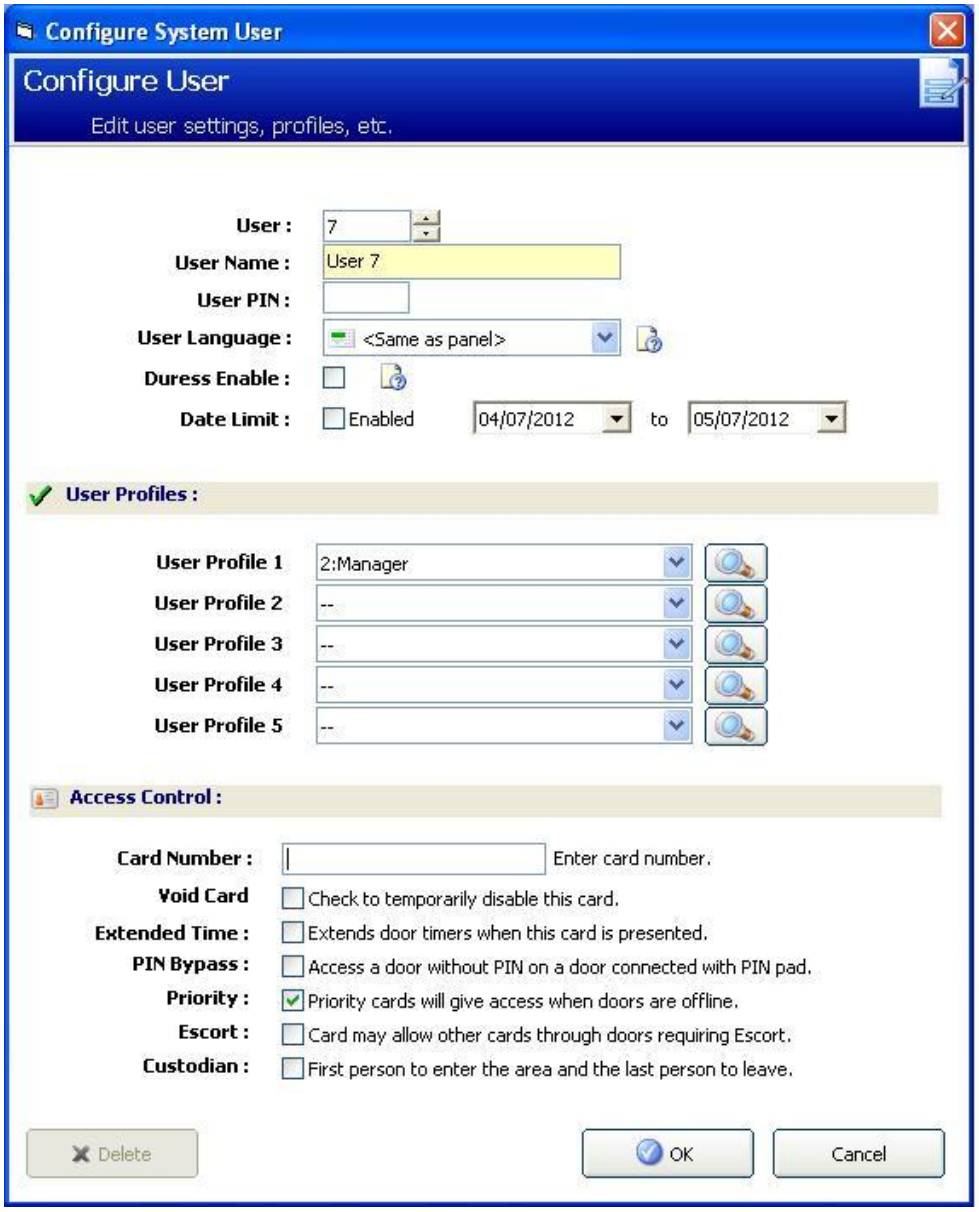
1. Click the tab **All Users**.
2. See table below for further information.



Add User	Click this button to add a user to the panel.
Engineer Configure	Click on this button if you wish to change the PIN and web password for Engineer access. See Configuring Engineer Settings [→ 60].

Add user

1. Click the button **Add User** to add a new user –OR–
   Click on a user from the user list to edit the user.
2. Configure the fields as described in the table below.



User	Select a user ID from the available IDs on the system.
User Name	Enter a unique name for this user (max. 16 characters and case sensitive).
User PIN	Enter the user access PIN. **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
Language	You can select a language other than the default panel language which will display the keypad menus in that language when you enter the PIN for this user. If the selected language is not available on the panel, the menus display in the panel default language. If SPC Pro is offline (not connected to the panel) a list of all possible panel languages is displayed. The actual languages available in the particular panel firmware are only displayed when SPC Pro is online (connected to the panel) In addition, when SPC Pro is offline, 'Custom' is displayed instead of the actual name of a custom language.
Duress Enable	Enable Duress for this user if required. The number of PINs allocated for duress (PI +1 or PIN+2) is set in System Options [→ 66]. **Note:** Duress option only available on this screen if 'User Duress' is enabled for the system in System Options. If Duress is enabled for this user, then consecutive user PINs for other users (i.e. 2906, 2907) are not permitted, as entering this PIN from the keypad would activate a user duress event.

Date Limit	Click on the Enable check box to restrict this user's access to a time period within the specified dates.
User Profiles	Select user profiles to assign to this user from the dropdown lists.
Access Control	See table in following section.

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign this card.
Void Card	Check to temporarily disable this card.
Extended Time	Extend door timers when this card is present.
PIN bypass	Access a door without PIN on a door with PIN reader.
Priority	Priority cards are stored locally in the door controllers and will grant access in case of a technical fault where the door controller cannot communicate with the control panel. The maximum number of priority users is: ● SPC4xxx – all users ● SPC5xxx – 512 ● SPC6xxx - 512
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is enabled on a door, a card with the "escort" right has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Custodian	The custodian feature enforces a card holder with custodian privilege to always be inside a room (door group) when other card holders are inside. The custodian must be the first to enter the room. Only if a custodian is in the room other cardholders are allowed to enter. The cardholder with the custodian right will not be allowed to exit until all non-custodian cards left the room. Identifies this card holder as a custodian. The user with the custodian attribute has to be the first who enters a door group which requires a custodian card holder and has to be the last that is leaving this door group.

See also

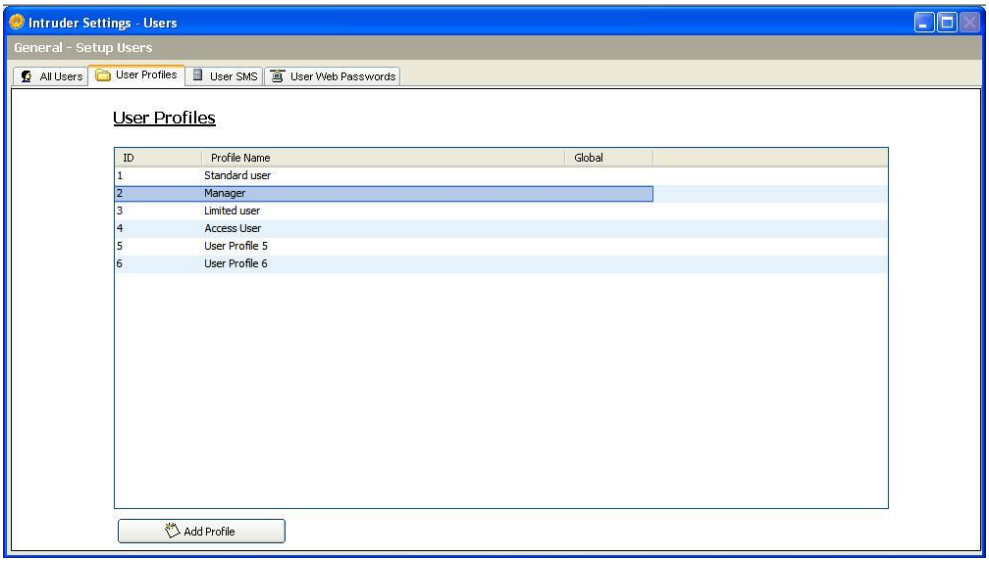
Configuring SMS [→ 56]

8.2 Adding / Editing User Profiles

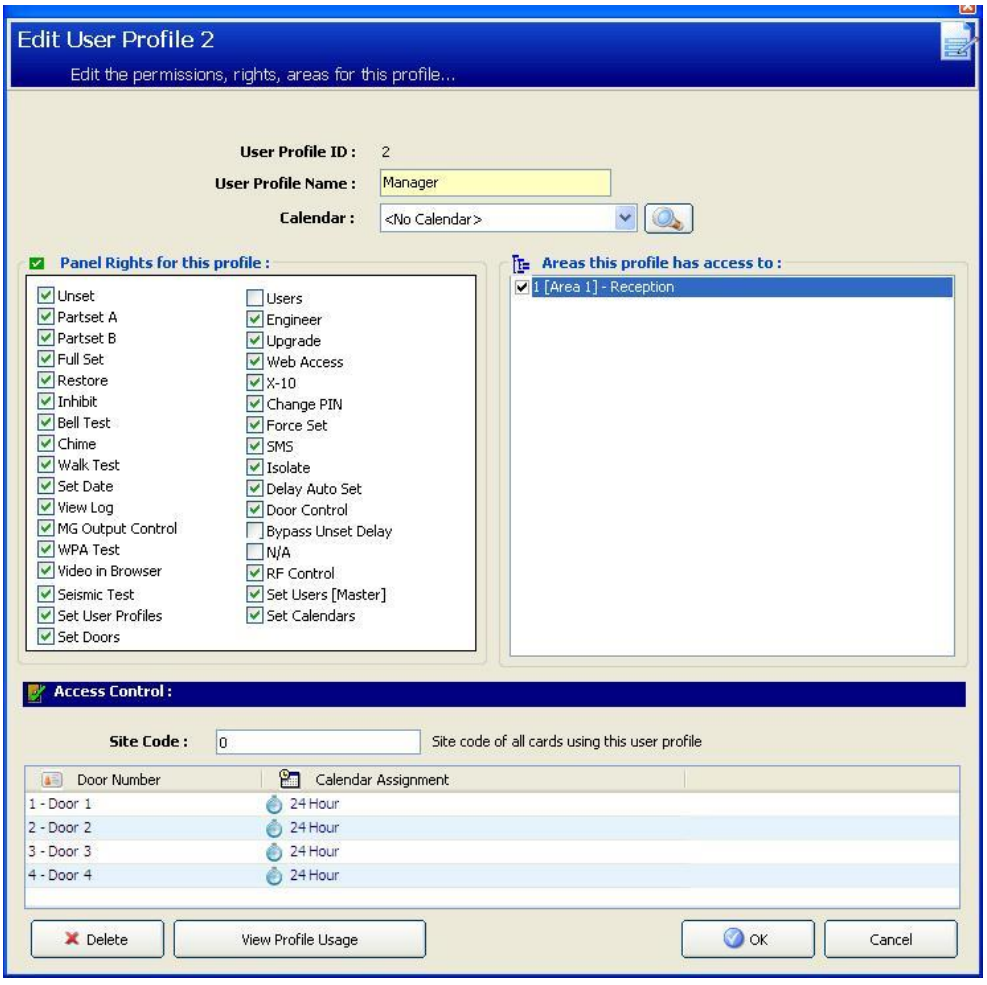
!	*NOTICE*
	Global user profiles cannot be edited in the browser or SPC Pro and must be edited in SPC Manager

Setup Users

1. Click the tab **Users Profiles**.
   ⇨ A list of existing user profiles is displayed.



2. Select **Add Profile** or click on a profile to edit.



General Settings

1. Enter a **User Profile ID** that is not currently being used. If you enter an ID that is already used, an 'ID Unavailable' message is displayed.
2. Provide a **User Profile Name** (maximum 16 characters and case sensitive).
3. Select all **Areas** that will be controlled by this user profile.
4. Select a **Calendar** to set the time limitations of this profile on the system.

User/Panel Rights

- Select the required user rights that are to be assigned to this user profile.

User rights

Right	User Profile Type Default	Description
User Rights - Intruder		
Fullset	Limited Standard Manager	The FULLSET operation fully sets the alarm system and provides full protection to a building (opening of any alarm zones activates the alarm). On selecting FULLSET, the buzzer sounds and the keypad display counts down the exit time period. Exit the building before this time period has expired. When the exit time period has expired, the system is set and opening of entry/exit zones starts the entry timer. If the system is not Unset before the entry timer expires, the alarm is activated.
Partset A	Standard Manager	The PARTSET A option provides perimeter protection to a building while allowing free movement through the access areas. Zones that have been classified as EXCLUDE A remain unprotected in this mode. By default, there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset A timed variable.
Partset B	Standard Manager	The PARTSET B option applies protection to all zones except those that have been classified as EXCLUDE B. By default there is no exit time; the system sets instantly on selection of this mode. An exit timer can be applied to this mode by enabling the Partset B timed variable.
Forceset	Standard Manager	The FORCESET option is presented on the keypad display when an attempt is made to set the system while an alarm zone is faulty or still open (the top line of the display shows the open zone). Selecting this option sets the alarm and inhibits the zone for that set period.
Unset	Limited Standard Manager	The UNSET operation unsets the alarm. This menu option is only presented on the keypad after an Entry/Exit zone has been activated and a valid user code has been entered.
Delay Auto Set	Standard* Manager	User can delay or cancel autosetting..
Bypass Delay	Standard Manager	User can automatically override the Unset Delay. Only available for Financial installations. See Setting/Unsetting [→ 128]
Restore	Standard Manager	The RESTORE operation restores an alert condition on the system and clears the alert message associated

Right	User Profile Type Default	Description
		with that alert condition. An alert condition can only be cleared after the zone(s) or fault(s) that triggered the alert condition have been restored to their normal operating state and the CLEAR ALERT option in user programming is selected for that zone.
Inhibit	Standard Manager	Inhibiting a zone deactivates that zone for one alarm set period. This is the preferred method of deactivating a faulty or open zone as the fault or open condition is displayed on the keypad each time the system is being set to remind the user to attend to that zone.
Isolate	Standard* Manager	Isolating a zone deactivates that zone until such time as the zone is de-isolated. All zone types on the controller can be isolated. Use of this feature to deactivate faulty or open zones should be considered carefully; once a zone is isolated, it is ignored by the system and could be overlooked when setting the system in the future, compromising the security of the premises.
User Rights - System		
Web Access	Standard* Manager	User can access panel through web browser.
View Log	Standard Manager	This menu option displays the most recent event on the keypad display. The event log details the time and date of each logged event.
Users	Manager	User can create and edit other users on the panel but with only the same or less rights than this user.
SMS	Standard* Manager	This feature allows users to set up the SMS messaging service if a modem is installed on the system.
Set Date	Standard Manager	Use this menu option to program the time and date on the system. Ensure the time and date information is accurate; these fields are presented in the event log when reporting system events.
Change PIN	Standard Manager	This menu option allows users to change their user PINS. **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
View Video/Video in Browser	Standard Manager	User can view video images via the web browser. Note: The Web Access right must also be enabled for this function.
Chime	Standard Manager	All zones that have the CHIME attribute set generate a short burst of audible tone on the keypad buzzer when they are opened (while the system is unset). This menu option allows for enabling or disabling of the chime feature on all zones.
Engineer	Manager	This option allows users to grant access to engineer programming. For Swiss CAT 1 and CAT 2 regional requirements, when Engineer Access is granted, all areas must be unset otherwise the engineer will be denied access.
Upgrade	Manager	User can grant manufacturer access to panel to perform firmware upgrade.
User Rights - Control		

Right	User Profile Type Default	Description
Outputs	Standard Manager	User can activate/deactivate configured outputs (mapping gates). See Editing an Ouput [→ 85].
X-10	Standard Manager Access Control	User can activate/deactivate configured X-10 devices. **Note:** X-10 is in maintenance. The functionality remains in the system for backward compatibility.
Door Control	Standard* Manager Access Control	User can lock/unlock doors.
RF Control	Standard Manager Access Control	User can control RF output
User Rights - Test		
Bell Test:	Standard Manager	User can perform a bell test to test the external bells, strobe, internal bells and buzzer to ensure their correct operation.
Walk Test	Standard Manager	User can perform a walk test to allow for testing of the operation of all alarm sensors on a system.
WPA Test	Standard Manager	User can test a WPA.
Seismic Test	Standard Manager	User can test the seismic detector.
User Rights – Service Engineer		
Set Users (Master)		User can create and edit other users on the system with no restriction on user rights.
Set User Profiles		User can create and edit user profiles on the system.
Set Calendars		User can configure calendars.
Set Doors		User can edit doors.
* Functions not enabled by default for this user but can be selected.		

Access Control

1. Enter **a Site Code**, if required, for all cards assigned to this user profile. Refer to the appendix section on Card Readers and Formats.
2. Select the **Access** rights of this user profile for the doors configured on the system. Options are:
   - No access
   - No time limit (i.e. 24 hour access)
   - Calendar (if configured)

Users

Click on the **View Profile Usage** button at the bottom of the dialog box to display a list of users that are assigned to this profile.

You can create a new user profile based on an existing profile by clicking **Replicate**. A new User Profile page is displayed.

See also

Adding / Editing User Profiles [→ 53]

Adding / Editing an area [→ 122]

8.3 Configuring SMS

The SPC system allows remote (SMS) messaging on systems with installed modems.

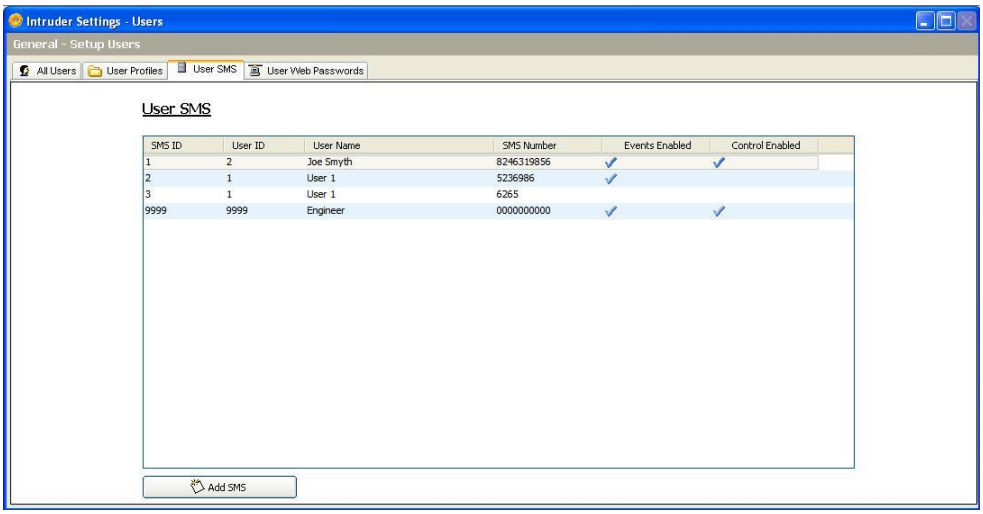
Setup Users

▷ A modem is installed and identified by the system.

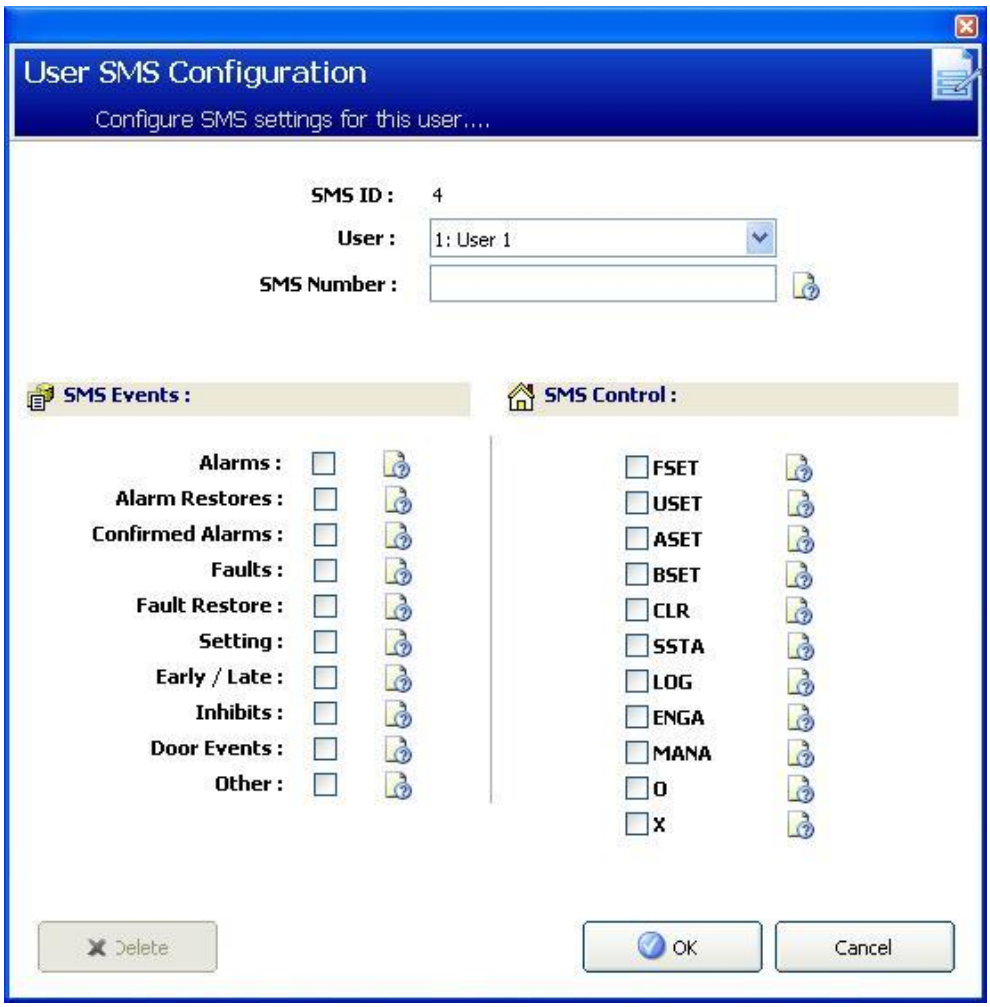
▷ The function **SMS Authentication** is activated. See page [→ 66].

1. Select the **User SMS** tab.

   ⇨ The Engineer SMS ID and a list of user SMS IDs with corresponding SMS details are displayed.



2. Click on the **Add SMS** button to add a new SMS ID or click on an SMS entry to edit it.



3. Configure the SMS details as follows:

SMS ID	System generated ID.
SMS Number	Enter the number to which the SMS will be sent (requires three-digit country code prefix). **Note:** Engineer SMS number can deleted by resetting it 0. User SMS numbers cannot be deleted.
User	Select a new user for this SMS ID if required.
SMS Events	Select the panel events which the user or engineer will receive via SMS.
SMS Control	Select the operations that the user or engineer can perform remotely on the panel through SMS. See SMS Commands [→ 58]

!	*NOTICE*
	HOLDUP alarm events are not transmitted via SMS.

If the phone line is connected to the PSTN network via a PBX, the appropriate line access digit should be inserted before the called party number. Ensure that **C**alling **L**ine **I**dentity (CLI) is enabled on the line selected to make the call to the SMS network. Consult the PBX administrator for details.

8.4 SMS Commands

When the SMS setup and configuration is complete, SMS features may be activated. Commands, depending on SMS configuration, are sent using a PIN or caller ID. The type of PIN depends on what is set for SMS Authentication.

The table below provides all available SMS commands. Subsequent action and response are also provided.

SMS Commands are sent as texts to the phone number of the SIM card on the controller.

For commands using a PIN, the format of the text is:

****.command or **** command

where **** is the PIN and “command” is the command i.e. the PIN followed by either a space or a full stop. For example, the command “FSET” is entered as: **** FSET or ****.FSET. The full version of the command, where listed, can also be used. For example, ****.FULLSET.

If the user does not have sufficient rights to perform a command, the system returns ACCESS DENIED.

If Caller ID is enabled, and the sender’s SMS number is configured, the PIN prefix is not required.

COMMANDS (**** = code)			
Using Code	**Using Caller ID**	**Action**	**Response**
**** HELP ****.HELP	HELP	All available commands displayed	All available commands
**** FSET ****.FSET ****. FULLSET	FSET FULLSET	Sets all areas the user has access to.	Time/date of system set. If applicable, responds with open zones/force set zones
**** USET ****.USET ****. UNSET	USET UNSET	Unsets all areas the user has access to.	System Unset
**** SSTA ****.SSTA ****. STATUS	SSTA STATUS	Retrieves the status of areas.	Status of system and applicable areas ● For a single area system, system and mode are returned, where mode is the set status of the system ● For a multi-area system, the status of each area is returned.
**** XA1.ON (X10) ****.XA1.ON		Where X10 device is identified as “A1”, it is triggered on.	Status of “A1”
**** XA1.OFF ****.XA1.OFF		Where X10 device is identified as “A1”, it is triggered off.	Status of “A1” .
**** LOG ****.LOG		Up to 10 recent events displayed	Recent events
**** ENGA.ON	ENGA.ON	Enable Engineer access	Allow Engineer

(ALLOW ENGINEER) ****.ENGA.ON			
**** ENGA.OFF ****.ENGA.OFF	ENGA.OFF	Disable Engineer access	Revoke Engineer
**** MANA.ON ****.MANA.ON		Enable Manufacturer access	Manufacturer status
**** MANA.OFF ****.MANA.OFF		Disable Manufacturer access	Manufacturer status
**** O5.ON ****.O5.ON ****. OUTPUT		Where mapping gate is identified as “O5”, it is triggered on.	Status of “O5” For example: ● Output O5 on. ● Output heating on (where heating is the name of the output.)
**** O5.OFF ****.O5.OFF		Where mapping gate is identified as “O5”, it is triggered off	Status of “O5” For example: Output O5 off
****.ASET (PARTSET A)		Allows Partset A of alarm by SMS It is also possible to specify the custom name defined in the PARTSET rename field of the Options window. See Options [➙ 66]	System set.
****.BSET PARTSET B)		Allows Partset B of alarm by SMS It is also possible to specify the custom name defined in the PARTSET rename field of the Options window. See Options [➙ 66] For example: ****.ASET NIGHT	System set.
****.CLR ****. RESTORE		Allows clear alerts by SMS	

For SMS recognition, mapping gate identification uses the format ONNN, where O stands for mapping gate, and NNN are the numeric placeholders, of which not all are necessary.
(Example: O5 for mapping gate 5)

For SMS recognition, X-10 device uses the format: XYNN, where X stands for X-10; Y stands for the alphabetic identity and NN are the available numeric placeholders. (Example: XA1)

The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN, the following criteria are required:

- Caller ID needs to be enabled on the telephone line.
- Direct telephone line – not through PABX or other communications equipment.
- Please also note that most Service Providers only allow SMS to a telephone registered in the same country. (This is due to billing issues)

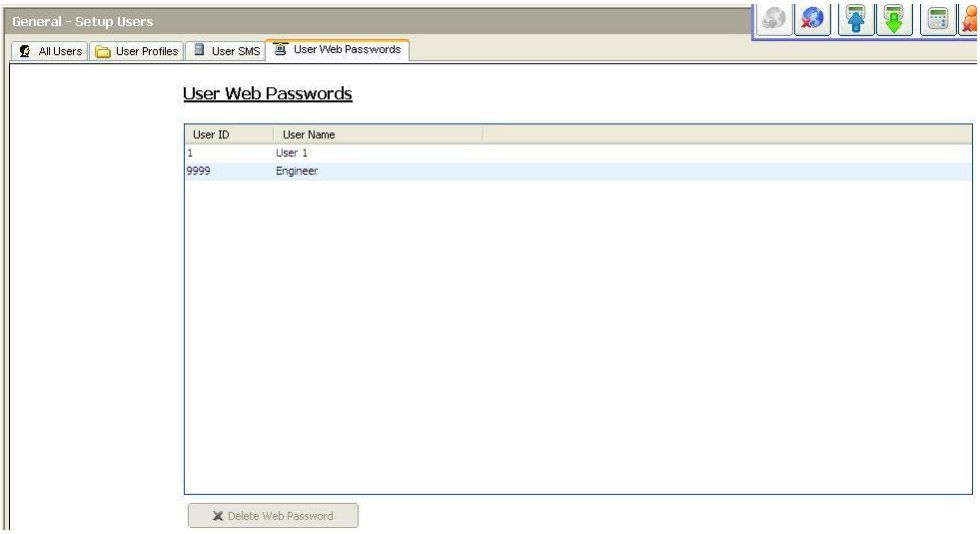
8.5 Deleting Web Passwords

This screen lists the engineer and any user and Engineer password that has been created for accessing the Web browser.

General

Setup Users

1. Select the **User Web Passwords** tab.
2. Click the button **Engineer Configure**.

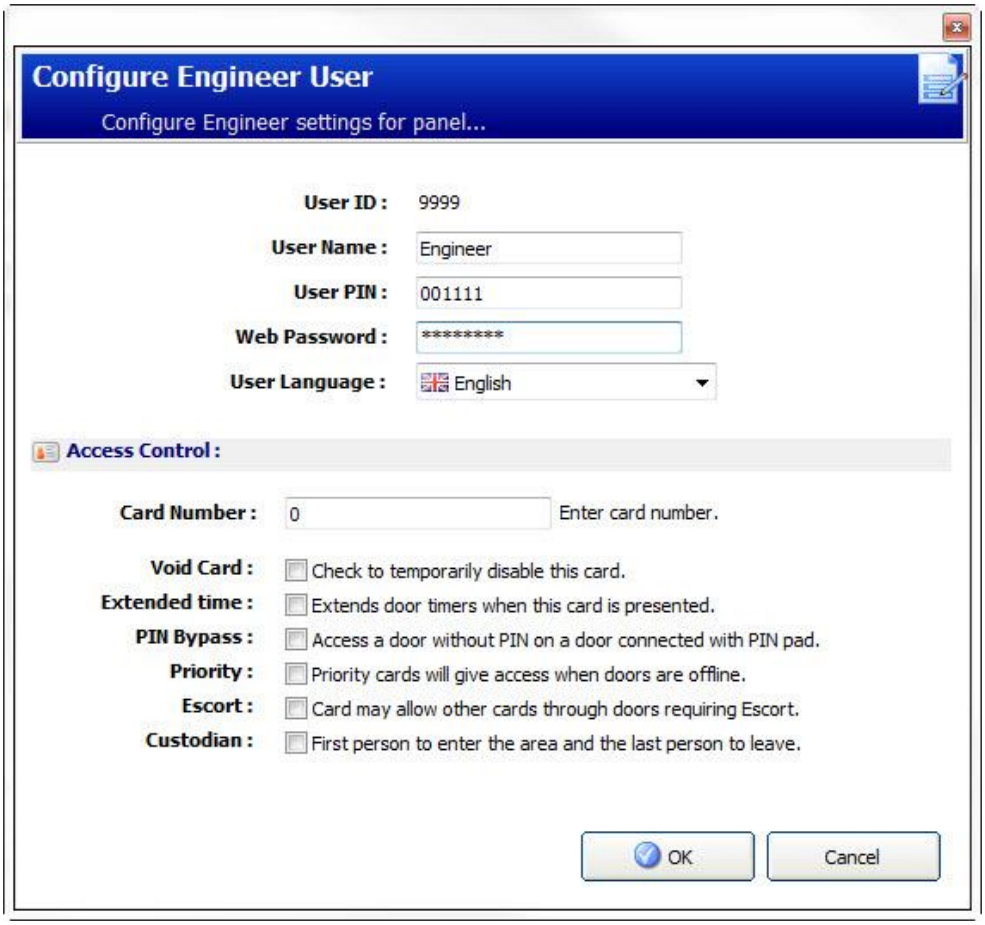


3. Click on the **Delete Web Password** button beside the Engineer or user to delete the password.

8.6 Configuring Engineer Settings

General	 Setup Users

1. Select the **All Users** tab.
2. Click the **Engineer Configure** button.



3. Edit the 'Engineer' **User Name** if required.
4. Edit the **User PIN** for the Engineer user.

The minimum number of digits required for this code depends on the security setting of the system or on the selected length of the **PIN Digits** in the menu **Panel Settings > System Settings > Options**.

5. Change the **Web Password** for accessing the Web browser (alphabetic characters A-Z, numeric digits 0-9). This password is case sensitive – ensure that you enter the correct upper or lower case alphabetic characters in your new password

The new PIN and password will only operate when the configuration file has been sent to the panel.

6. Click **OK**.

Access Control

Attribute	Description
Card Number	Enter card number. Enter 0 to unassign this card.
Void Card	Check to temporarily disable this card.
Extended Time	Extend door timers when this card is present.

Attribute	Description
PIN bypass	Access a door without PIN on a door with PIN reader.
Priority	Priority cards are stored locally in the door controllers and will grant access in case of a technical fault where the door controller cannot communicate with the control panel. The maximum number of priority users is: ● SPC4xxx – all users ● SPC5xxx – 512 ● SPC6xxx - 512
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is enabled on a door, a card with the “escort” right has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Custodian	The custodian feature enforces a card holder with custodian privilege to always be inside a room (door group) when other card holders are inside. The custodian must be the first to enter the room. Only if a custodian is in the room other cardholders are allowed to enter. The cardholder with the custodian right will not be allowed to exit until all non-custodian cards left the room. Identifies this card holder as a custodian. The user with the custodian attribute has to be the first who enters a door group which requires a custodian card holder and has to be the last that is leaving this door group.

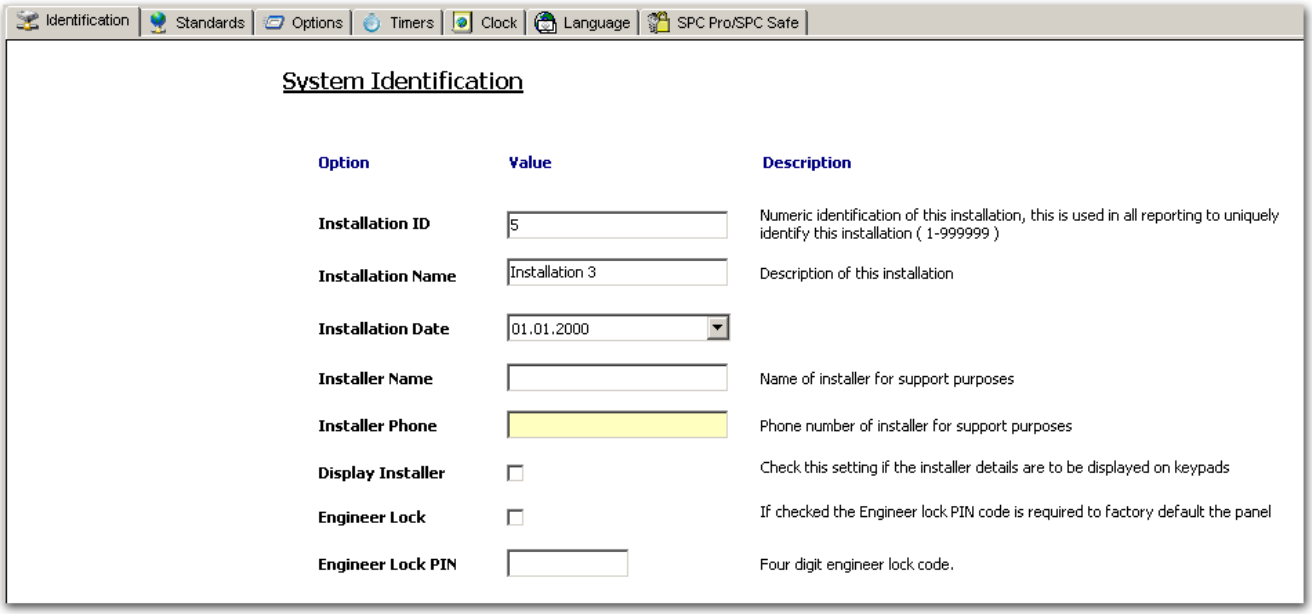
9 Changing system settings

9.1 Identification

Panel Settings

System Settings

1. Select the tab **Identification**.
   ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.



Installation ID	Enter a unique number for each installation This number identifies the installation (1 – 999999).
Installation Name	Enter the name of the installation. An installation name must be entered before the installation is saved on the system. The installation can be viewed from the keypad.
Installation Date	Select the date from the dropdown menu that the installation was completed.
Installer Name	Enter the name of the person who installed the system (for support purposes).
Installer Phone	Enter the contact phone number of the person who installed the system (for support purposes).
Display Installer	Tick this box to display the installation details on the keypad connected to the panel when in the idle condition.
Engineer Lock	Tick this box to require use of the engineer lock PIN to factory default the panel.
Engineer Lock PIN	Enter value for lock PIN (4 digits).

9.2 Standards

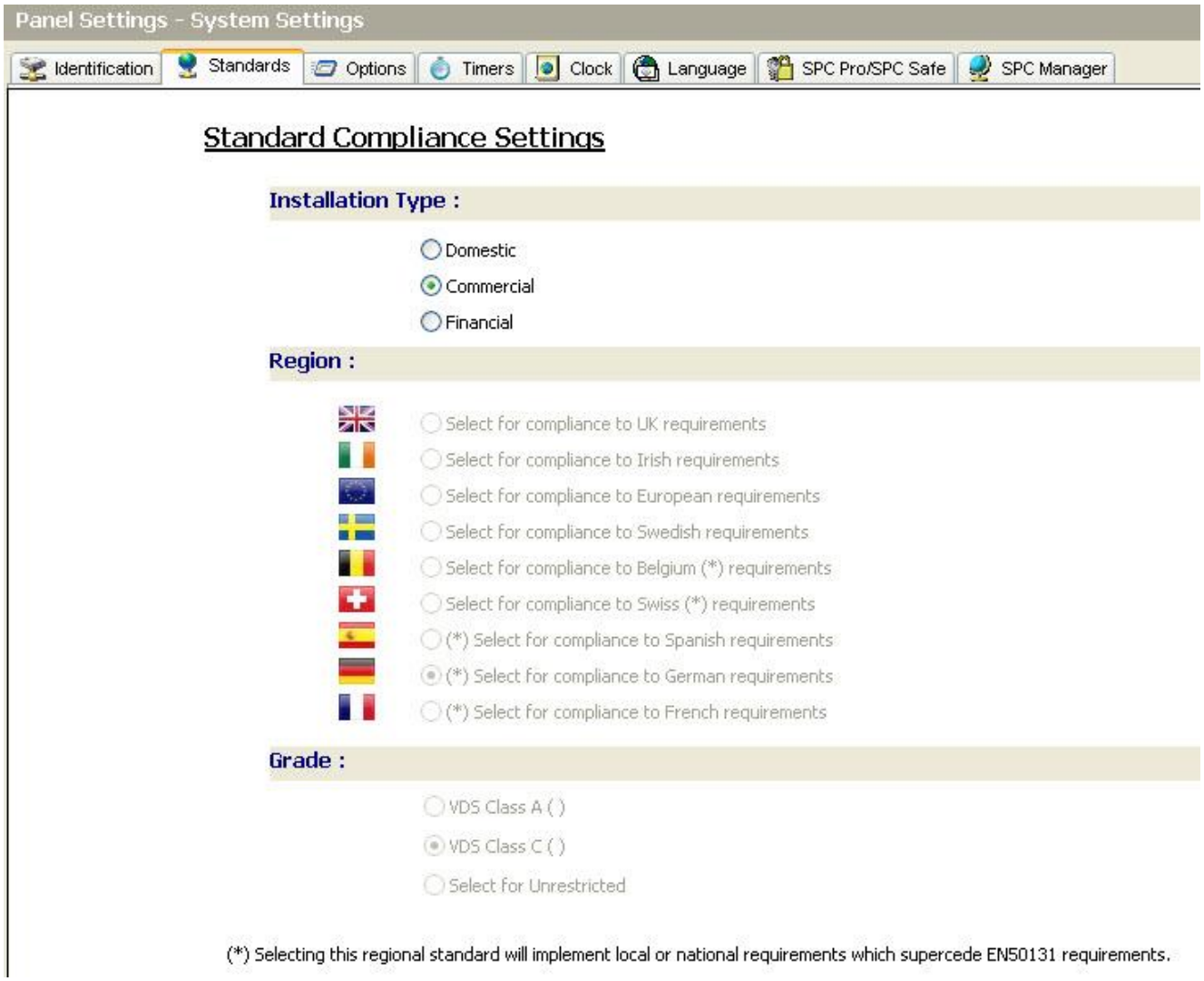
All alarm systems must comply with defined security standards. Each standard has specific security requirements that apply to the market/country in which the alarm system is installed.

Panel Settings

System Settings

- Select the tab **Standards**.
  ⇨ The following window will be displayed.

It is not possible to edit the Region or Grade in SPC Pro.



Installation Type	Select the type of installation. Options are Domestic, Commercial or Financial.
Region	To change the region on your panel, it is strongly recommended that you default your panel and select a new region as part of the start up wizard. Select the region in which the installation is installed and the regional requirements it complies with. Options are UK, Ireland, Sweden, Europe, Switzerland, Belgium (INCERT), Spain, and Germany (VDS).
Grade	Select the Security Grade that applies to the installation. ● Irish and European Regions: – EN50131 Grade 2 – EN50131 Grade 3 – Unrestricted ● UK Region: – PD6662 (EN50131 Grade 2 based) – PD6662 (EN50131 Grade 3 based) – Unrestricted ● Swedish Region: – SSF1014:3 Larmclass 1 – SSF1014:3 Larmclass 2 – Unrestricted ● Belgium Region: – TO-14 (EN50131 Grade 2 based) – TO-14 (EN50131 Grade 3 based) – Unrestricted ● Switzerland Region: – SES EN-CH-Grad 2 – SES EN-CH-Grad 3 – Unrestricted ● Spanish Region – EN50131 Grade 2 – EN50131 Grade 3 ● German Region – VdS Class A – VdS Class C – Unrestricted ● France – NF&A2P - Grade 2 – NF&A2P - Grade 3 – Unrestricted

Unrestricted Grade

A Security Grade setting of **Unrestricted** does not apply to any regionally approved security restrictions of the installation. Instead, the Unrestricted setting enables an engineer to customize the installation by changing security policy options and configuring additional options which do not comply with the selected regional security compliance.

Unrestricted configuration options are denoted in this document by the following symbol: ⏻

See System Options [→ 208] for details of configuring system policies.

9.2.1 Installation type

The installation type determines the type of zones that can be programmed on the panel and the features that will be presented.

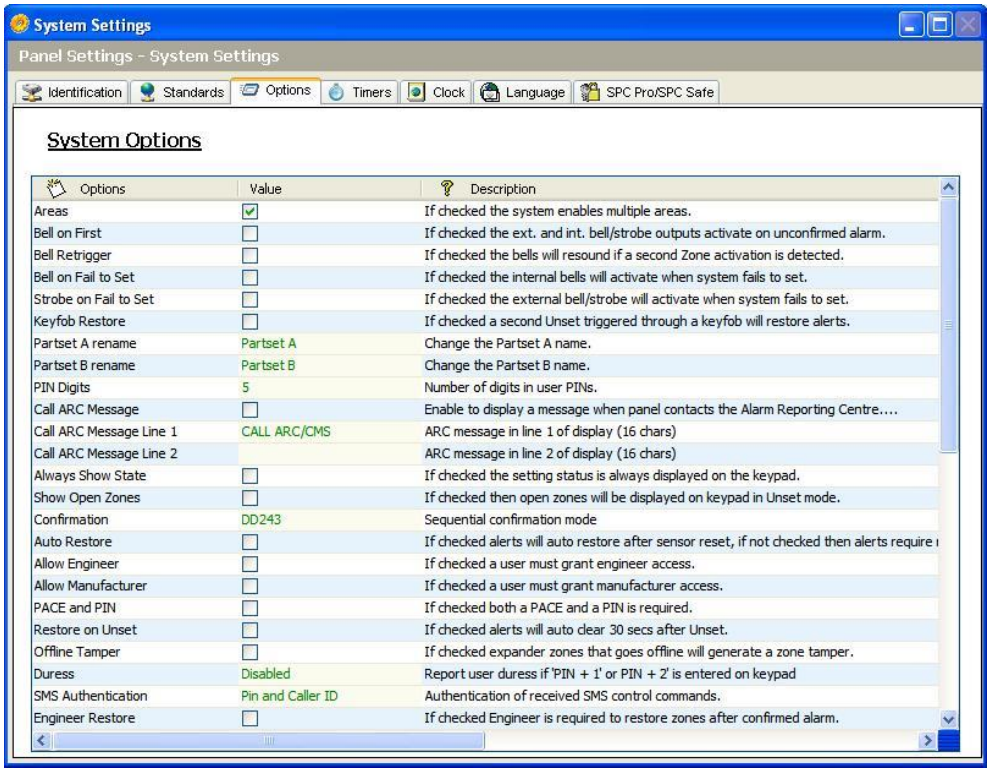
You can choose between the following installation types:

- **Domestic**: Suitable for residential installations with one or more areas and a small-to-moderate number of alarm zones. Appropriate Input and Output functions are available for the system configuration.
- **Commercial**: Suitable for business installations with multiple areas and a large number of alarm zones. Extended Input and Output functions such as calendar and autosetting are available.
- **Financial**: Suitable for banks and other financial institutions with vault and ATM environments.

9.3 Options

System Settings

1. Select the tab **Options**.
2. Configure the fields as described in the table below.



System Options

The options displayed vary depending on the Security Grade of the system.

Restriction	System Option	Description
General Settings		

Restriction	System Option	Description
	Areas	Select to enable multiple areas on the system. **Note:** This option is displayed for the Domestic and Commercial installation types, only.
	Code Restore	Grade 3 only: A user, who does not have the right to restore an alarm, is able to restore the alarm with this feature. On resetting an alarm, a 6 digit code is required. The user must call the installer to generate a restore code, with which the user is able to restore the alarm.
	Offline Tamper	Enable this for offline expander zones to generate a zone tamper.
	Keyfob Restore	If enabled, key fob is enabled to restore alerts by pressing the Unset key.
Web and SPC Pro Only	Audio Expander LED	If enabled, audio expander will not turn on LED when microphone active.
	Report in Eng mode	If enabled, the panel will always report alarm activations and panic alarms.
	Outputs in Eng Mode	If selected, the following are not deactivated in Full Engineer mode: • Controller outputs • Expander outputs • Indicator LEDs • Keyswitch LEDs
	Alarm on Reporting Fail	If a 'Fail to Communicate' alert is raised, external bells will activate.
	Retrigger Duress	If enabled, duress alarm will retrigger.
	Retrigger Panic	If enabled, panic alarm will retrigger.
	Override Reader Profile	If enabled, the LED behavior of readers will be controlled by the panel.
	Silence Audio Verification	If enabled, then the internal and external bells (system and area), the keypad buzzers and annunciation messages on the Comfort Keypad will be silenced during audio verification.
	Watchdog Output Mode	Enables output 6 on the SPC controller board to be used for monitoring purposes. The following modes of operation of the watchdog output can be selected: • Disable — Output 6 is available as a general purpose output. • Enabled — Output 6 is normally OFF but is turned ON when a watchdog fault occurs. • Pulsed — Output 6 is PULSED at 100ms intervals. • Enabled Inverted — Output 6 is normally ON but is turned OFF when a watchdog fault occurs. The following options combine the Enabled option with hardware-fault reporting in the event of a main microprocessor failure. If such a failure occurs, a SIA event is sent to ARC1. **Note:** The ARC must be configured to use SIA and SIA Extended 1 or 2. CID and FF are not supported by this reporting method. • Enabled + Reporting (10s) — The failure event is sent to ARC1 10 seconds after the fault is detected. This option must be used to comply with VdS 2252. • Enabled +Reporting (60s) — The failure event is sent to ARC1 60 seconds after the fault is detected.

Restriction	System Option	Description
		The SIA event reported is **HF** and Extended SIA reports **Hardware Fault**. **Note:** Hardware faults are not reported if the Engineer is logged in to the system. For more information on ARCs, see Alarm Reporting Centres (ARCs) [→ 155].
	SPCP355	Enable VDS power supply. For VdS installations, this option is automatically selected.
	Bell on Fail to Set (FTS)	Enable to activate the internal bell if the system fails to set.
	Strobe on Fail to Set (FTS)	Enable to activate the strobe if the system fails to set.
⏻	Hide bypass	If enabled, the bypass messages will no longer be displayed on keypad.
	Battery capacity	Total batteries capacity in AH, for panel only (3 - 100 Ah). You must enter this value and **Max current** value to view the remaining battery time on the keypad in the event of mains failure. This is indicated under the STATUS - BATTERY - BATT TIME menu.
	Max current	The total current draw from batteries when mains fail occurs (30 - 20000 mA). You must enter this value and the **Battery capacity** value to view the remaining battery time on the keypad in the event of mains failure. This is indicated under the STATUS - BATTERY - BATT TIME menu.
Partset		
	Partset A Rename	Enter a new name for your PARTSET A mode (e.g. Night Mode).
	Partset B Rename	Enter a new name for your PARTSET B mode (e.g. Floor 1 only).
Alarm		
	Bell on First	Enable to activate relevant bells/sirens on an unconfirmed alarm. When this option is disabled, the relevant bells/sirens will only activate on a confirmed alarm or if the detector that caused the unconfirmed alarm is reactivated.
	Bell Retrigger	Enable to resound bells/sirens if a second zone activation is detected (after the bell time has elapsed). If not checked then the external bells will only trigger once.
⏻ Web Only	Alert Forbid Set	If enabled, a user cannot set an area if there is an area or system alert present on the system. **Note:** This option is only available when the **Standards -> Region** selected is Switzerland or **Security Grade** selected is 'Unrestricted'.
	Restore on Unset	Enable for alerts to auto clear after 30 seconds in Unset mode. **Note:** To comply with PD6662, you must disable this option.
⏻	Antimask Set	Select the type of event reported resulting from antimask detection when panel is Set. Options are Disabled, Tamper, Trouble or Alarm. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the

Restriction	System Option	Description
		selected region: ● Ireland - Alarm ● All other regions - Alarm
⏻	Antimask Unset	Select the type of event reported resulting from antimask detection when panel is Unset. Options are Disabled, Tamper, Trouble or Alarm. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: ● Ireland - Disabled ● All other regions - Tamper
⏻	Out of bounds EOL unset	Select the type of event reported resulting from Out of Bounds EOL detection when the panel is unset. Options are: Disabled, Tamper and Trouble. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: ● Germany VDS – Tamper ● All other regions - Trouble
⏻	Out of bounds EOL set	Select the type of event reported resulting from Out of Bounds EOL detection when the panel is set. Options are: Disabled, Tamper and Trouble. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: ● Germany VDS – Tamper ● All other regions – Trouble
⏻	Zone Unstable unset	Select the type of event reported resulting from Zone Unstable detection when the panel is unset. Options are: Disabled, Tamper and Trouble. A zone is unstable if a valid sample cannot be obtained within 10 seconds. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: ● Germany VDS – Tamper ● All other regions – Trouble
⏻	Zone Unstable set	Select the type of event reported resulting from Zone Unstable detection when the panel is set. Options are: Disabled, Tamper and Trouble. A zone is unstable if a valid sample cannot be obtained within 10 seconds. The option can only be configured when the panel is in 'Unrestricted' mode. In Grade 2 or 3 mode, the type of event reported is in accordance with the standards for the selected region: ● Germany VDS – Tamper ● All other regions – Trouble
⏻	EOL Wide	If enabled, EOL wide bands are used.
	Suspicion Audible	If enabled then WPA Suspicion alerts have audible and visible indicators on the keypad. (Financial mode only).
Pro	End Of Line	Select the End Of Line termination resistors that will apply

Restriction	System Option	Description
	(EOL RESISTANCE)	to either all zones on the system or new zones added to the system. Select a value to enable the appropriate feature. To apply a new EOL setting to all existing zones, select the Update all zones checkbox. If you change the End of Line value but do not select this checkbox, the new setting applies only to zones added after changing the value.
	Seismic Test on Set	If enabled, all seismic sensors in any area that is being set will be tested before area or system set. (Financial mode only).
ⓘ	Auto Restore	Enable this feature to automatically restore alerts on the system i.e. when the open zone that triggered an alarm is closed, a manual restore operation on the keypad/browser is not required. If disabled it prevents the user from restoring alerts by resetting the input that triggered the alert.
ⓘ	Alarm on Exit	**Enabled:** If a non-entry/exit zone is activated during the exit timer countdown, a local alarm is raised by sounding the bells. **Disabled:** If a non-entry/exit zone is activated during the exit timer countdown, an alarm is not raised. **Note:** This option only displays when the **Unrestricted** grade is selected as enabling it is not in accordance with EN50131. When you choose the Swiss or Belgium **Region** under **Standard Compliance Settings**, this option is automatically enabled but it is not visible under **Options**.
ⓘ	Alarm on Entry	**Enabled:** If a non-entry/exit zone is activated during the entry timer countdown, a local alarm is raised by sounding the bells. **Disabled:** If a non-entry/exit zone is activated during the entry timer countdown, an alarm is not raised. **Note:** This option only displays when the **Unrestricted** grade is selected as enabling it is not in accordance with EN50131. When you choose the Swiss **Region** under **Standard Compliance Settings**, this option is automatically enabled but it is not visible under **Options**.
Confirmation		
ⓘ	Confirmation	The Confirmation variable determines when an alarm is deemed to be a confirmed alarm. ● BS8243: This will enforce compliance with the UK Police requirements, and is a specific requirement for UK Commercial installations. The requirement stipulates that an alarm will only be deemed to be a confirmed alarm if it meets the following condition: After an initial zone alarm has been activated and before the alarm confirmation time has expired, a second zone alarm is activated. The alarm confirmation time must be between 30 and 60 minutes. (See Timers [→ 74]) If a second zone alarm is not activated within the Alarm confirmation time, then the first zone alarm will be inhibited. The BS8243 confirmation option is automatically set whenever the **Standards -> Region** option is set to UK. ● Garda: This will enforce the policies for confirmed alarms required by the Irish Garda. The requirement

Restriction	System Option	Description
		stipulates that an alarm will be deemed to be a confirmed alarm as soon as a second zone alarm is activated on the system within the one alarm set period. The Garda confirmation option is automatically set whenever the **Standards -> Region** option is set to Ireland. ● EN-50131-9 This will enforce compliance with the EN-50131-9 standard and the Spanish “INT/316/2011 Order of 1 February on the operation of alarm systems in the field of private security”. This requirement stipulates that an alarm will only be deemed to be a confirmed alarm if it meets the following conditions: - 3 zone activations in 30 minutes (default), whereby two activations may come from the same device if the activations differ in type, i.e. alarm / tamper. - 1 Alarm activation followed by an ATS[1] Fault within 30 minutes (default). - ATS fault followed by a tamper or alarm condition within 30 minutes (default). If the 30 minutes expires and the zone is restored to its normal physical state, then the zone’s alerts will be restored if a level 2 user can restore this alert. In this case, the zone will accept a new alert condition which will cause a new activation. Alternatively, if the zone has not been restored to its normal physical state then that zone will be inhibited if that zone is allowed to be inhibited. If an alert (ATS) reoccurs after the 30 minute window (default), then the 30 minute timer will restart. The EN50131-9 confirmation option is automatically set whenever the **Standards -> Region** option is set to Spain. ● VDS This will enforce compliance with the VDS standard.
Keypad		
ⓘ	Always Show State (SHOW STATE)	If enabled, the setting status of the system (Fullset / Partset / Unset) is permanently displayed in the bottom line of the keypad display. If unchecked the setting status will disappear from the keypad display after 7 seconds.
	Show Open Zones	If enabled, open zones will display on keypad in Unset mode.
	Call ARC Message	If enabled, the ARC message will be displayed for 30 seconds after Unset, if confirmed alarm has been reported..
	Call ARC Line 1	ARC message in line 1 of display (16 chars).
	Call ARC Line 2	ARC message in line 2 of display (16 chars).
	Show Cameras	If enabled, offline cameras will be displayed on the keypad in Unset mode.
	Idle State Language	Select the language displayed in idle state. ● System Language: Language in which menus and texts on the keypads, the web interface and the event log will be displayed. ● Last Used: Last used language is displayed in idle

Restriction	System Option	Description
		state.
PIN		
	PIN Digits	Enter the number of digits for user PINs (max. 8 digits). Increasing the number of digits will add the relevant number of zeros to the front of an existing PIN, e.g. an existing user PIN of 2134 (4 digits) will change to 00002134 if the PIN digits is set to 8. If you decrease the number of PIN digits, existing PINs will have their leading digits removed, e.g. an existing user PIN of 00002134 (8 digits) will change to 02134 if the PIN digits is set to 5. **Note:** This option cannot be changed if an SPC Manager PIN digit mode is set. Refer to page [→ 80] **Note:** To comply with INCERT approvals, the user's PIN code must contain more than 4 digits.
	PACE and PIN	If enabled, both PACE and PIN are required.
	User Duress	Select one of the following Duress options to activate this function on the system. ● PIN +1(system reserves the PIN before and after the user PIN for duress. ● PIN + 2 (system reserves two PINs before and after the user PIN for duress. Duress must be enabled for individual users. See section on Adding/Editing a User. [→ 48]
	PIN Policy	Click on the **Edit** button to select options for PIN usage. ● Periodic changes required – enforces scheduled changes to the user's PIN. The period is defined in the **PIN Valid** field of **Timers**. See Timers [→ 74]. ● Warn if changes required – generates a user alert if the user's PIN is about to expire, or has expired. The warning period is defined in the **PIN Warning** field of **Timers**. See Timers [→ 74]. ● User selects the last digit – enables the user to select the last digit of their pin. The preceding digits are automatically generated by the system. ● User selects the 2 digits - enables the user to select the last two digits of their PIN. The preceding digits are automatically generated by the system. ● Limit Changes – limits the number of changes possible within a valid PIN period. This value is defined in the **PIN Changes Limit** field of **Timers**. See Timers [→ 74] ● Secure PIN - If enabled the PIN will be automatically generated by the panel.
Door		
	Reset Cards	If enabled, access cards passback state will be reset every day at midnight.
	Ignore site code	If enabled, the access system will ignore site codes. By ignoring the site code, you only add the card number and increase the card users on the system from 100 to 2,500.
	Card Formats	Click on the **Edit** button to select the card formats that will be allowed on this panel. Refer to the Appendix in the SPC Installation & Configuration Guide for details of currently supported card readers and card formats. **Note:** Selecting **Wiegand** enables all Wiegand card formats.
Web and	Door Mode Set	Select the required user identification to unlock door

Restriction	System Option	Description
SPC Pro Only		when area is set. Options are **Default**, **Card and PIN**, **Card Or PIN**.
Web and SPC Pro Only	Door Mode Unset	Select the required user identification to unlock door when area is unset. Options are **Default**, **Card and PIN**, **Card Or PIN**.
Engineer		
⏻	Engineer Restore	(Impact only if Region "UK" is chosen): If this option is enabled, then the engineer has to restore the confirmed alarms. This option works together with the function "Confirmation".
	Engineer Exit	If enabled, the engineer is allowed to leave Full Engineer mode with alerts active.
⏻	Allow Engineer	Enable this feature to ensure that the engineer can only access the system if the user allows it. If disabled, ENABLE ENGINEER menu option on keypad is not available. **Note**: Only available if Security Grade is 'Unrestricted'. For Grade 2 / 3, user control of engineer access to system is always available.
⏻	Allow Manufacturer	Enable this feature to ensure that the engineer can only access the system if the user allows it. If disabled, ENABLE MANUFACTURER menu option on keypad is not available. **Note**: Only available if **Security Grade** is 'Unrestricted'. For Grade 2 / 3, user control of engineer access to system is always available if user type is 'Manager'.
SMS		
	SMS Authentication	Select one of the following options: ● PIN Code Only: This is a valid user code. See page [→ 48]. ● Caller ID Only: This is the phone number (including three-digit country prefix code) as configured for user SMS control. SMS control will only be available for configuration by the user when this option is selected. ● PIN and Caller ID ● SMS PIN Code Only This is a valid PIN code configured for the user which is different from the user's login code. SMS controls will only be available for configuration by the user when this option is selected. ● SMS PIN Code & Caller ID.
Policy		
Web Only	System Policy	Configure engineer login and tamper reporting behavior for system.
Web Only	Timing Policy	Display system timing policy.
Web and SPC Pro Only	Output Configuration	Click on the **Edit** button to configure latch and autoset output settings [→ 204].
Web Only ⏻	System Alert Policy	This programming option allows you to restrict the user and engineer's ability to restore, Isolate and inhibit alerts. The manner in which the system reacts to alerts can also be programmed.
Web Only	Zone Alarm	Select whether particular zone alarms can be restored,

Restriction	System Option	Description
	Policy	inhibited or isolated by the user and engineer.
Web Only	Zone Tamper Policy	Select whether particular zone tampers can be restored, inhibited or isolated by the user and engineer.
Web Only	Keypad Display Policy	Select events to be displayed on keypads in both Set and Unset modes.
Web Only	Keypad LED Policy	Select which LEDs will be displayed on keypads in both Set and Unset modes.
Web Only	System General Policy	Select options to manage remote control of the system and alarm and bell settings from the following: - No confirmed alarms if internally set - Block remote restore - Block remote isolates - Block remote inhibits - No external bell if internal set - Delay reporting if entry active - Confirmed alarm cancels delay
Web Only	Confirmed Alarms System Alerts	Select which system alerts cause a confirmed alarms when at least one alarm is active, and which system alerts cause the panel to enter the tentative state.

See also

- Adding / Editing a User [→ 48]
- Adding / Editing an area [→ 122]

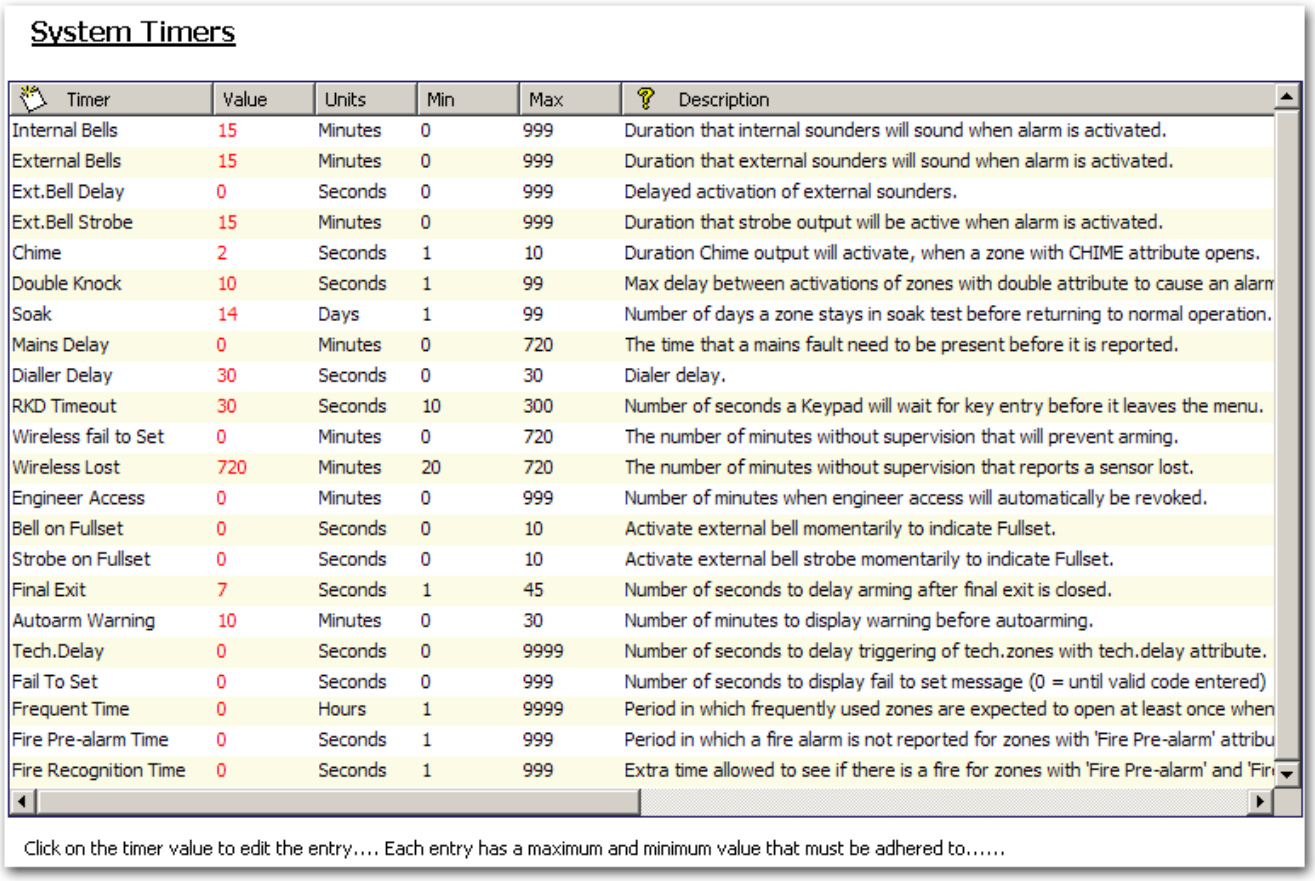
9.4 Timers

This window gives an overview about identified timer defaults and their description.

These settings, which vary depending on the defined Security Grade of the system, should only be programmed by an authorised installation engineer. Changing settings could render the SPC system noncompliant with security standards. Setting the Security Grade back to EN 50131 Grade 2 or EN 50131 Grade 3 overwrites any changes made on this page.

System Settings

1. Select the tab **Timers**.
   ⇨ The following window will be displayed.
2. See the table below for further action.
3. Click on the timer value in the column **Value**.
4. Enter the new value.



System Timers

Timer	Value	Units	Min	Max	Description
Internal Bells	15	Minutes	0	999	Duration that internal sounders will sound when alarm is activated.
External Bells	15	Minutes	0	999	Duration that external sounders will sound when alarm is activated.
Ext.Bell Delay	0	Seconds	0	999	Delayed activation of external sounders.
Ext.Bell Strobe	15	Minutes	0	999	Duration that strobe output will be active when alarm is activated.
Chime	2	Seconds	1	10	Duration Chime output will activate, when a zone with CHIME attribute opens.
Double Knock	10	Seconds	1	99	Max delay between activations of zones with double attribute to cause an alarm
Soak	14	Days	1	99	Number of days a zone stays in soak test before returning to normal operation.
Mains Delay	0	Minutes	0	720	The time that a mains fault need to be present before it is reported.
Dialler Delay	30	Seconds	0	30	Dialer delay.
RKD Timeout	30	Seconds	10	300	Number of seconds a Keypad will wait for key entry before it leaves the menu.
Wireless fail to Set	0	Minutes	0	720	The number of minutes without supervision that will prevent arming.
Wireless Lost	720	Minutes	20	720	The number of minutes without supervision that reports a sensor lost.
Engineer Access	0	Minutes	0	999	Number of minutes when engineer access will automatically be revoked.
Bell on Fullset	0	Seconds	0	10	Activate external bell momentarily to indicate Fullset.
Strobe on Fullset	0	Seconds	0	10	Activate external bell strobe momentarily to indicate Fullset.
Final Exit	7	Seconds	1	45	Number of seconds to delay arming after final exit is closed.
Autoarm Warning	10	Minutes	0	30	Number of minutes to display warning before autoarming.
Tech.Delay	0	Seconds	0	9999	Number of seconds to delay triggering of tech.zones with tech.delay attribute.
Fail To Set	0	Seconds	0	999	Number of seconds to display fail to set message (0 = until valid code entered)
Frequent Time	0	Hours	1	9999	Period in which frequently used zones are expected to open at least once when
Fire Pre-alarm Time	0	Seconds	1	999	Period in which a fire alarm is not reported for zones with 'Fire Pre-alarm' attribu
Fire Recognition Time	0	Seconds	1	999	Extra time allowed to see if there is a fire for zones with 'Fire Pre-alarm' and 'Fir

Click on the timer value to edit the entry.... Each entry has a maximum and minimum value that must be adhered to.....

Timers

Designation of the functions in the following order:

- 1st row: Web/SPC Pro
- 2nd row: Keypad

Timer	Description	Default
Audible		
Internal Bells INT BELL TIME	Duration that internal sounders will sound when alarm is activated. (1 – 15 minutes: 0 = never))	15 min.
External Bells EXT BELL TIME	Duration that external sounders will sound when alarm is activated. (1 – 15 minutes; 0 = never)	15 min.
External Bell Delay EXT BELL DELAY	This will cause a delayed activation of the external bell. (0 – 600 seconds)	0 sec.
Chime CHIME TIME	Number of seconds that a chime output will activate, when a zone with chime attribute opens. (1 – 10 seconds)	2 sec.
Confirmation		
Confirm CONFIRM TIME	• **Note:** Only available when Security Grade is 'Unrestricted' and 'DD243' is selected for 'Confirmation' variable. (See System Options [→ 66]) This timer applies to the alarm confirmation feature and is defined as the maximum time between alarms from two different non overlapping zones that will cause a confirmed alarm. (30 – 60 minutes)	30 min.
Confirmed holdup	This timer applies to the confirmed holdup feature and is defined as the maximum time between alarms from two different non-overlapping zones that will cause a confirmed alarm. (480 - 1200 minutes)	480 min.

Timer	Description	Default
Dialer Delay DIALER DELAY	When programmed, the dialler delay initiates a predefined delay period (0 -30 seconds) before the system dials out to an Alarm Receiving Centre (ARC). This is specifically designed to reduce unwarranted responses from Alarm Receiving Centres and the constabulary. In the event of a subsequent zone being tripped the dialler delay period is ignored and the dialler dials out immediately. (0 – 30 seconds)	30 sec.
Alarm abort ALARM ABORT	Time after a reported alarm in which an alarm abort message can be reported. (0 – 999 seconds))	30 sec.
Setting		
Setting Authorisation SETTING AUTH	Period for which Setting Authorisation is valid. Enter a value between 10 and 250 seconds.	20 secs
Final Exit FINAL EXIT	The Final Exit time is the number of seconds that arming is delayed after a zone programmed with the final exit attribute is closed. (1 – 45 seconds)	7 sec.
Bell on Fullset FULLSET BELL	Activates the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Strobe on Fullset FULLSET STROBE	Activates the strobe on the external bell momentarily to indicate a full set condition. (0 – 10 seconds)	0 sec.
Fail To Set FAIL TO SET	Number of seconds to display fail to set message on keypads (0 until valid PIN is entered). (0 – 999 seconds)	10 sec.
Alarm		
Double Knock DKNOCK DELAY	The maximum delay between activation's of zones with the double attribute, which will cause an alarm. (1 – 99 seconds)	10 sec.
Soak SOAK DAYS	The number of days a zone remains under soak test before it automatically returns to normal operation. (1 – 99 days)	14 days
Seismic Test Interval SEISMIC AUTOTEST	The average period between seismic sensor automatic tests (12 – 240 hours) **Note:** To enable automatic testing, the **Automatic Sensor Test** attribute must be enabled for a seismic zone.	168 hours.
Seismic Test Duration SEISMIC TEST DUR	Maximum time (in seconds) that a seismic sensor takes to trigger an alarm in response to the 'Seismic Test' output. (3 - 120 seconds)	30 sec.
Lockout Post Alarm LOCKOUT POST ALARM	Duration after alarm that access will be denied.	0 mins
External Bell Strobe STROBE TIME	Duration that the strobe output will be active when an alarm is activated. (1 – 15 minutes; 0 = indefinitely)	15 min.
Alerts		
Mains Delay MAINS SIG DELAY	The time after a mains fault has been detected before an alert is activated by the system. (0 – 60 minutes)	0 min.
Engineer		
Engineer Access ENGINEER ACCESS	The timer for the Engineer access starts as soon as the user enables the Engineer Access. (0 – 999 minutes. '0' indicates no time limitation for system access)	0 min.
Engineer auto log out ENG AUTO LOG OUT	Duration of inactivity after which the engineer will be automatically locked out	0 mins.
Keypad		
Keypad Timeout KEYPAD TIMEOUT	The number of seconds that an RKD will wait for key entry before it leaves the current menu. (10 – 300 seconds)	30 sec.
Keypad Language KEYPAD LANGUAGE	The duration a keypad will wait in idle before switching language to default (0 - 9999 seconds; 0 = never).	10 secs
Fire		

Timer	Description	Default
Fire Pre-alarm FIRE PRE-ALARM	Number of seconds to wait before reporting fire alarm for zones with 'Fire pre-alarm' attribute set. (1 – 999 seconds) See Editing a Zone [→ 120].	30 sec.
Fire recognition FIRE RECOGNITION	Extra time to wait before reporting file alarm for zones with 'Fire pre-alarm' and 'Fire Recognition' attributes set. (1 – 999 seconds). See Editing a Zone [→ 120].	120 sec.
PIN		
PIN Valid PIN VALID	Period for which pin is valid in days (1 - 330)	30 days
PIN Changes Limit PIN CHANGES LIMIT	Number of changes within a valid period (1 - 50)	5
PIN Warning PIN WARN	Time before PIN expiry after which a warning will be displayed (1 - 14)	5 days
General Settings		
RF Output Time RF OUTPUT	The time that the RF output will remain active on the system. (0 – 999 seconds)	0 sec.
Time Sync Limit TIME SYNC LIMIT	Time limit within which no event will be reported. (0 – 999 secs) Time synchronization only takes place if system time and update time are outside this limit.	0 sec.
Link Timeout LINK TIMEOUT	Timeout for Ethernet link fault (0 = Disabled) (0 - 250)	0 secs
Camera Offline CAMERA OFFLINE	Time for camera to go offline (10 - 9999)	10 secs
Tech. delay TECH. DELAY	Number of seconds to delay triggering of tech. zones with tech. delay attribute. (0 – 9999 seconds)	0 sec.
Frequent FREQUENT ⓘ	This attribute only applies to Remote Maintenance. The number of hours a zone must open within if the zone is programmed with the **Frequent use** attribute. (1 – 9999 hours)	336 hours (2 weeks)
Duress silent	Time when duress will remain silent and not restorable from keypad (0 - 999).	0 Minutes
Holdup/panic silent	Number of minutes that a holdup/panic will remain silent and cannot be restored from the keypad (0 - 999).	0 Minutes

Default times are dependent upon the Engineer configuration. The default times denoted may or may not be allowable and is dependent on the configuration by the engineer

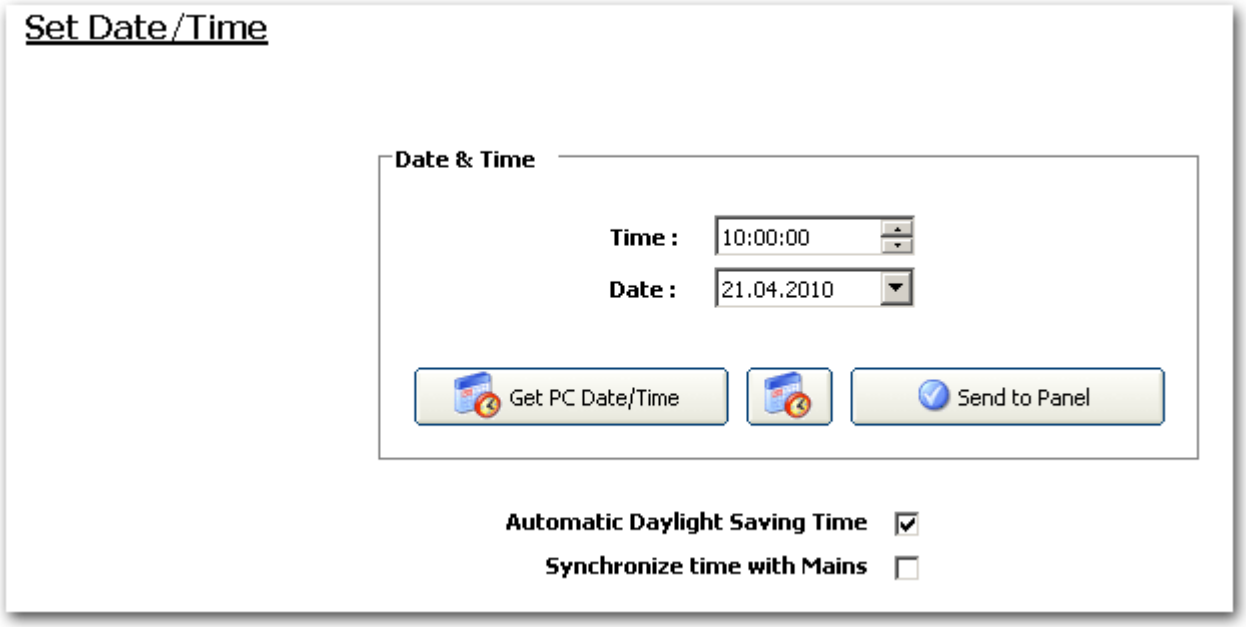
9.5 Clock

This window allows you to program the date and time on the panel. The controller contains a **R**eal-**T**ime **C**lock (RTC) that is battery backed to preserve the time and date information in the event of power failure.

System Settings

1. Click the tab **Clock**.

⇨ The following window will be displayed:



2. Select the **Time** and **Date** from the drop down menus.
   - OR -
   Click the button **Get PC Date/Time** to get the PC date and time.
3. Click the button **Send to Panel** to send the date and time information to the panel
4. Configure the following fields:

Automatic Daylight Saving Time	If selected, the system will automatically switch to summer time
Synchronize time with Mains	If selected, the RTC synchronizes itself with the sine wave in the power line

The selected time and date will be displayed on the keypad, the web interface and the event log.

9.6 Language

System Settings

1. Click the tab **Language**.
   ⇨ The following window is displayed:

2. Select a language from the dropdown menu.

⇨ The texts on the keypads, the web interface and the event log will be displayed in the selected language

The languages available in the **Language** drop-down list depend on the languages defined on the system. If you have not connected to your panel and downloaded the configuration file, all languages are displayed. If you have downloaded the configuration from the panel, only those languages available on the system are displayed in the **Language** drop-down list.

The language used in the keypads and browser depends on the language selection made for each user. For example, if the system language is set to French, but the individual user's language is set to English, English is the language used in both keypads and browser for that user, regardless of the specified system language.

9.7 SPC Pro / SPC Safe

SPC Pro / SPC Safe

SPC Pro

1. Click the **SPC Pro / SPC Safe** button.
2. Configure the fields as described in the table below.

Enable	Tick this box to enable SPC Pro to connect to the panel.
Engineer Access	Tick this box if engineer access must be granted to allow SPC Pro to connect to the panel.
Password	Enter the password for SPC Pro connection. The password is checked by the panel every time SPC Pro attempts to connect to it. If the password programmed in this field matches the password programmed on the panel, then the connection will be allowed (default:).
Enable IP	Tick this box to enable a connection to the panel using Internet Protocol (IP).

IP Port	Select the IP port that SPC Pro will use to connect to the panel.

SPC Safe

For further information about configuration of the SPC Safe please refer to the *SPCS410 Installation & Configuration Manual.*

1. Click the **Enable SPC Safe** button.
2. Configure the fields as described in the table below.

Enable	Tick this box to enable Pro to connect to the panel.
Engineer Access	Tick this box if engineer access must be granted to allow Pro to connect to the panel.
Password	Enter the password for the Pro connection. The password is checked by the panel every time the Pro attempts to connect to it. If the password programmed in this field matches the password programmed on the panel, then the connection will be allowed (default:).
Installation ID	Enter the numeric identification of this installation (can also be set in System Identification page).
Enable Reporting	Check to allow the panel to contact the server after its configuration has been changed.
Reporting Timer	Enter the minutes how long after the last configuration change the panel should contact the server to report its configuration (min: 1, max.: 120).
Enable IP	Tick this box to enable a connection to the panel using Internet Protocol (IP).
TCP/IP Port	Enter the IP port that SPC Safe will use to connect to the panel (the IP port of the panel).
Server address	Enter the Hostname, URL or IP address of the SPC Safe server (e.g the IP address of your PC).
Server TCP/IP Port	Enter theTCP port of the SPC server (e.g .the IP port of your PC).

9.8 SPC Manager

The SPC manager mode setting determines the number of digits for user PINs and therefore the number of available PINs on a global system controlled by SPC Manager.

Mode41: 4-digit PIN enables 1,000 global users

Mode51: 5-digit PIN enables 10,000 global users

Mode61: 6-digit PIN enables 100,000 global users

Mode71: 7-digit PIN enables 1000,000 global users

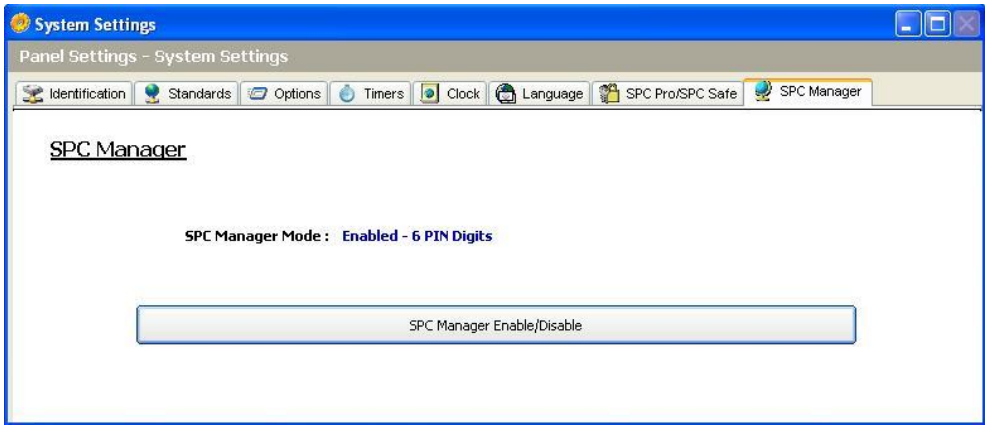
Mode81: 8-digit PIN enables 10,000,000 global users

When you set an SPC Manager mode, additional zeros are added to the front of existing 4 or 5 digits user PINs which modify the PIN for global use. For example, if **Mode71: 7-PIN Digit** is selected, 3 zeros are added to existing 4 digit PINs - 2222 will become 0002222.

To set the SPC Manager Mode:

System Settings

1. Select the tab **SPC Manager**.
   ⇨ The following window is displayed.



2. Click on the **SPC Manager Enable/Disable** button.
3. Select the SPC Manager global user mode from the drop down list in the displayed dialog.
4. Click on **OK**.

	NOTICE
	SPC Manager modes cannot be changed if global users exist on the system.

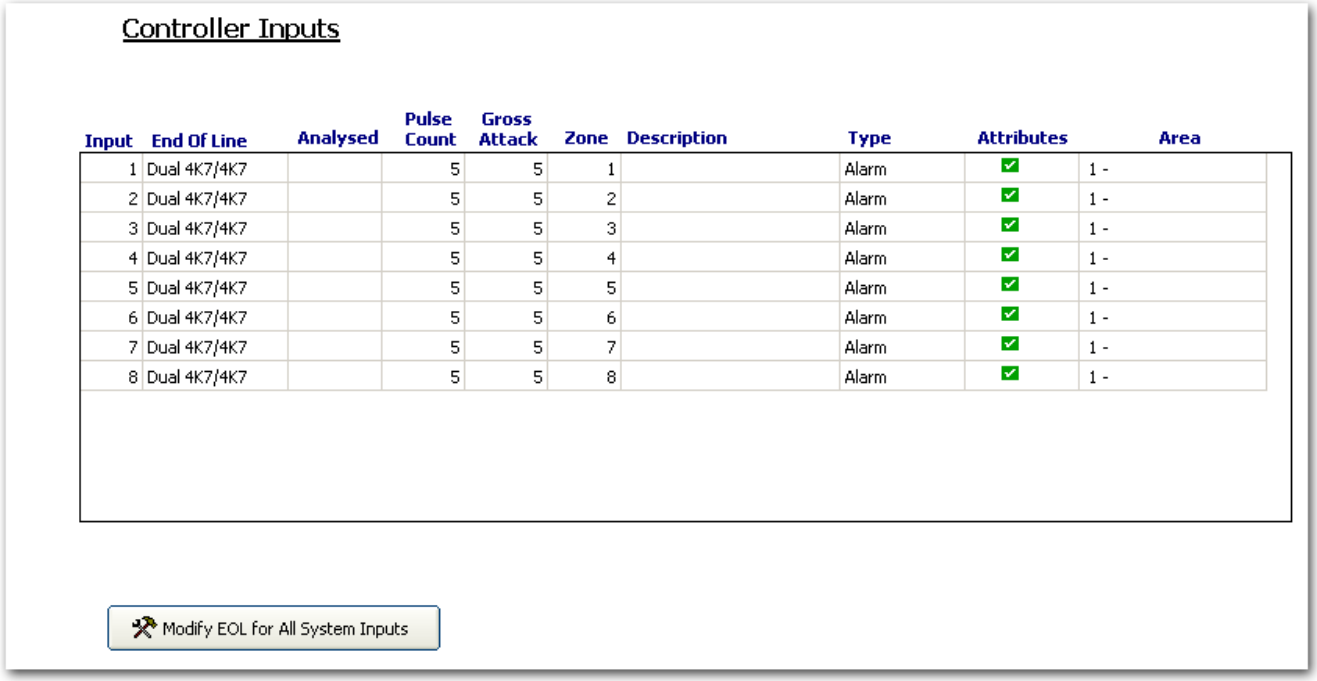
10 Configuring controller inputs & outputs

10.1 Editing an input

Panel Settings

Controller Inputs & Outputs

1. Click the tab **Inputs**.
   ⇨ The following window will be displayed:



2. Click the button to modify the End Of Line (EOL) resistance configuration for all inputs (controller and expanders).

Please ensure that the programmed EOL configuration matches the actual EOL configuration. Failure to do so may result in zones operating incorrectly.

3. Click an input from the list.
   ⇨ The following window will be displayed.
4. Configure the fields as described in the table below.
5. Click **OK**.

Input	The number is presented for reference and can not be programmed.
End of Line	Select the End of Line (EOL) for the zone input (default: 4K7).
Analyzed	Displays if the sensor is an inertia/shock type sensor
Pulse count	Pulse count programmed on the panel that will trigger an alarm from an inertia / shock sensor.
Gross Attack	The Gross attack programmed on the panel that will trigger an alarm from an inertia/shock sensor
Zone	Number of the zone on the panel
Description	Enter a text describing the input (max. 16 characters). This text will also appear on the browser and keypad.
Type	The type of zone (see page [➙ 260]).
Area	Only if (multiple) Areas is activated in menu Panel Settings > System Settings > Options. Select the areas to which this zone has been assigned.
Attributes	An icon in this field indicates that attributes have been programmed for this zone (see page [➙ 84]).

10.1.1 Input zones: attributes

Each zone on the SPC can be assigned an attribute that determines the properties of that zone.

To assign an attribute to a zone:

1. Click the tab **Inputs**.
2. Click an input from the list.
   ⇨ The following window will be displayed:

1. Check the box beside the preferred attribute.
2. Click **OK**.

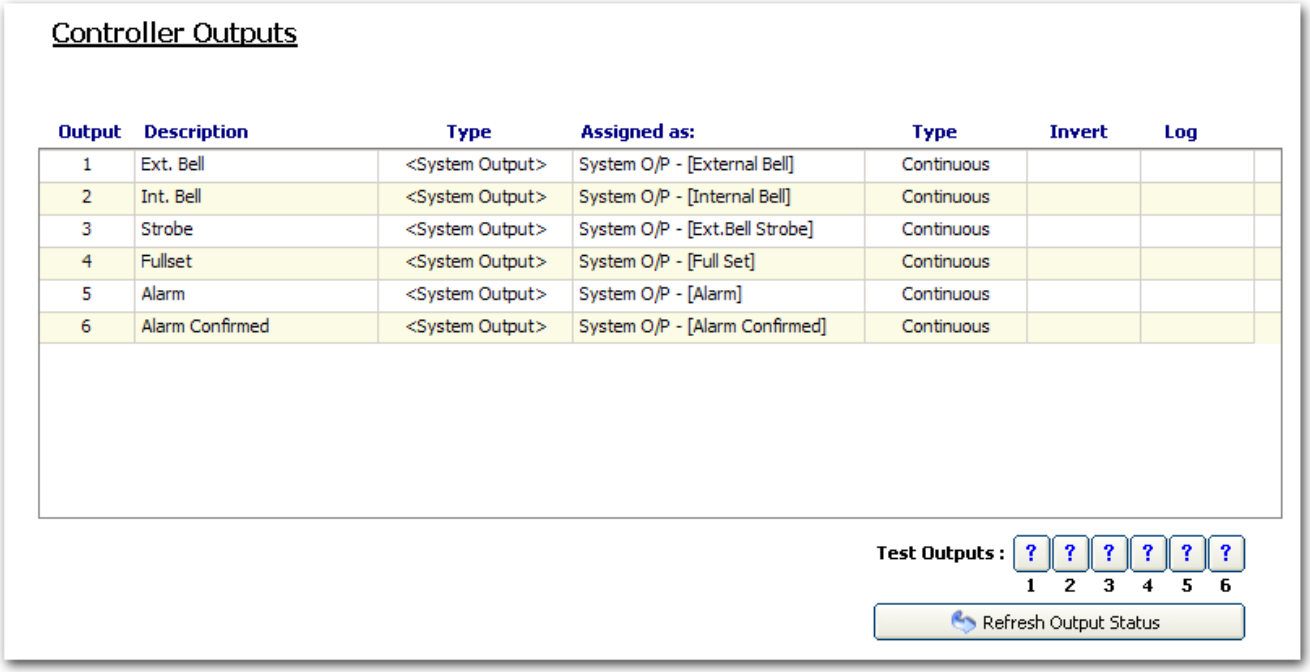
The attributes presented on this page will depend on the type of zone selected. For a list of assignable attributes see page [→ 265].

10.2 Editing an output

Panel Settings

Controller Inputs & Outputs

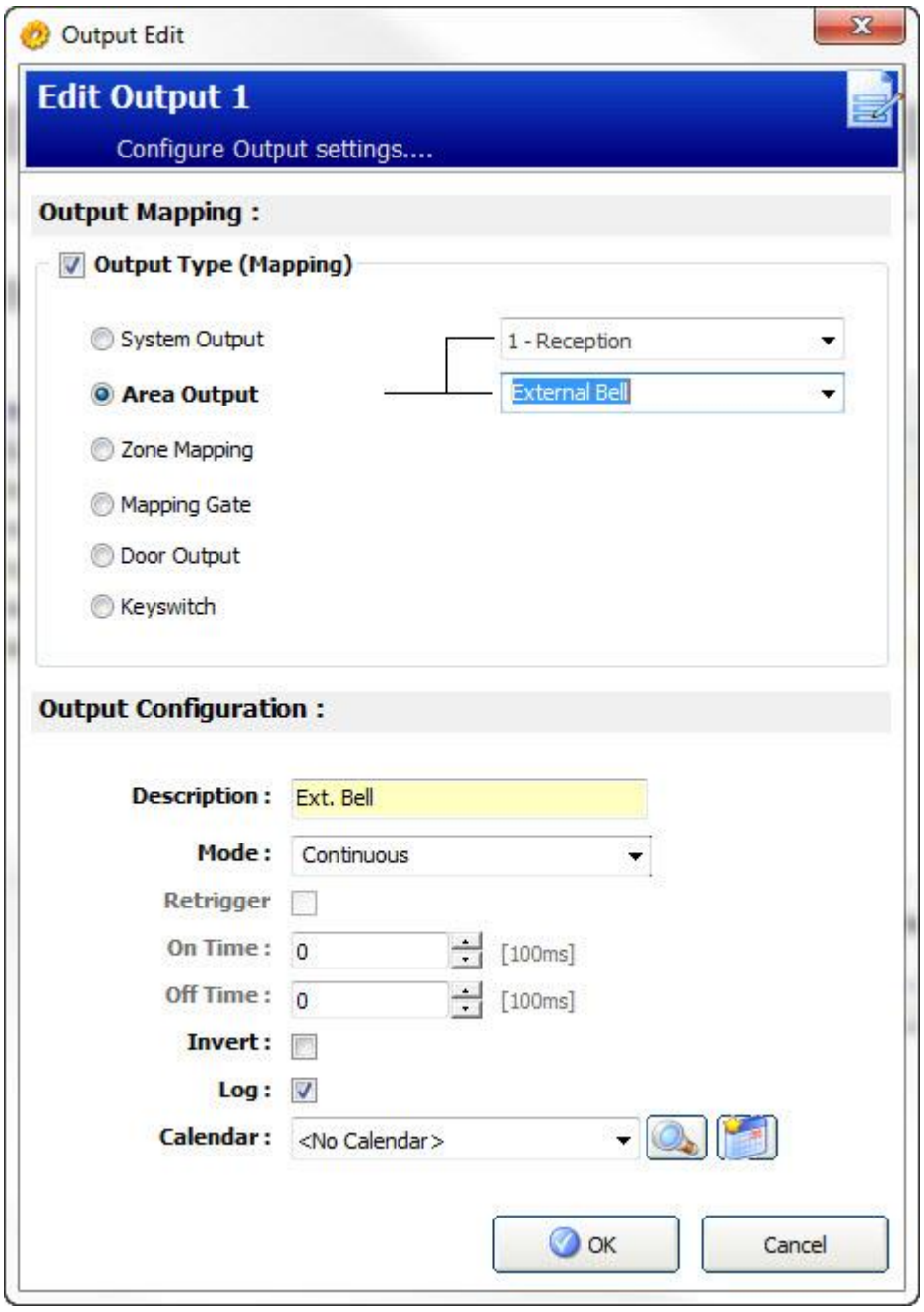
1. Click the tab **Outputs**.
   ⇨ The following window will be displayed:



2. Click on the button **Refresh Output Status**.
3. Click on one of the **Test Outputs** buttons to test if the output is connected correctly (light will go on).

The functionality **Test Outputs** is only available in Full Engineer mode.

4. Click an output from the list.
   ⇨ The following window will be displayed.
5. Configure the fields as described in the table below.
6. Click **OK**.



Output Type	• **System Output**: Select the type from the dropdown menu. (See Output Types and Output Ports [→ 87]) • **Area Output**: Only if **(multiple) Areas** is activated in menu **Panel Settings > System Settings > Options**. Select an area and the type of system output for this area. (See Output Types and Output Ports [→ 87]) • **Zone Mapping**: Select which zone should be mapped. • **Mapping Gate**: Select which mapping gate should be mapped. • **Door Output**: Select the door number and the type of system output for the door. (See Output Types and Output Ports [→ 87]) • **Keyswitch**: Select the node ID for the required keyswitch and the required key position to map to this output.
Description	Enter a text describing the output (max. 16 characters). This text will also appear on the browser and keypad.
Output Configuration	• **Mode**: Select the operational mode. Continuous follows output type; Pulsed toggles on and off when output type is active; Momentary generates a pulse when output type activates.

	• **Retrigger**: Tick the box to retrigger momentary outputs. • **On Time**: Enter the On time that applies to momentary and pulsed outputs. • **Off Time**: Enter the Off time that applies to pulsed outputs. • **Invert**: Tick this box to invert the physical output. • **Log**: Tick this box to log the output state changes to the event log. • **Calendar**: Select if necessary the desired calendar. See page [→ 194].

See also

Calendars [→ 194]

10.2.1 Outputs types and output ports

Each output type can be assigned to one of the 6 physical output ports on the SPC controller or to an output on one of the connected expanders. Output types that are not assigned to physical outputs act as indicators of events on the system and may be logged and/or reported to remote central stations if required.

The output ports on the expanders are all single pole relay type outputs (NO, COM, NC); therefore, output devices may need external power sources to activate if they are wired to expander outputs.

The activation of a particular output type depends on the zone type (see page [→ 260]) or alert condition that triggered the activation. If multiple areas are defined on the system then the outputs on the SPC are grouped into system outputs and area outputs; the system outputs are activated to indicate a system wide event (e.g. mains fault) whereas the area outputs indicate events detected in one or more of the defined areas on the system. Each area has its own set of area outputs; if the area is a common area for other areas, then its outputs will indicate the state of all the areas it is common for, including its own state. For example, if Area 1 is common for Area 2 and 3, and Area 2 Ext. Bell is active, then the Area 1 Ext Bell output is also active.

Some output types can only indicate system wide events (no specific area events). Please refer to the table below for further information.

Output Type	Description
External Bell	This output type is used to activate the system external bell and is active when any Area External Bell is active. By default, this output is assigned to the first output on the controller board (EXT+, EXT-). **Note**: An external bell output is automatically activated whenever a zone programmed as an Alarm zone triggers an alarm in Fullset or Partset modes.
External Bell Strobe	This output type is used to activate the strobe on the system external bell and is active when any area strobe is active. By default, this output is assigned to the strobe relay output (Output 3) on the Controller board (NO, COM, NC). **Note**: An external bell strobe output is automatically activated whenever a zone programmed as an alarm zone triggers an alarm in Fullset or Partset modes. The external bell strobe activates on a 'Fail to Set' condition if the strobe on the 'Fail to Set' option is checked in system options.
Internal Bell	This output type is used to activate the internal bell and is active when any area Internal Bell is active. By default, this output is assigned to the second output on the controller board (INT+, INT-). **Note**: An internal bell output is automatically activated whenever a zone programmed as an Alarm zone type triggers an alarm in Fullset or Partset modes. The internal Bell activates on a 'Fail to Set' condition if the Bell on the 'Fail to Set' option is checked in system options.
Alarm	This output turns on following alarm zone activation on the system or from any area

	defined on the system.
Alarm Confirmed	This output turns on when an alarm has been confirmed. An alarm is confirmed when 2 independent zones on the system (or within the same Area) activate within a set time period).
Panic*	This output turns on following activation of panic alarm zone types from any area. A panic alarm output is also generated if a user duress event is generated or if the panic option for the keypad is enabled.
Hold-up	This output turns on whenever a zone programmed as a Hold-up type zone triggers an alarm from any area
Fire	This output turns on following a fire zone activation on the system (or from any area)
Tamper	This output turns on when a tamper condition is detected from any part of the system. For a grade 3 system, if communication is lost to an XBUS device for greater than 100s, a tamper is generated and SIA and CIR reported events will send a tamper.
Medical	This output turns on when a medic zone is activated
Fault	This output turns on when a technical fault is detected
Technical	This output follows tech zone activity
Mains Fault*	This output activates when Mains power is removed
Battery Fault*	This output activates when there is a problem with the backup battery. If the battery voltage drops below 11 V this output activates. The 'Restore' option for this fault is only presented when the voltage level rises to above 11.8 V.
Partset A	This output is activated if the system or any area defined on the system is in Partset A mode
Partset B	This output is activated if the system or any area defined on the system is in Partset B mode
Fullset	This output is activated if the system is in Fullset mode
Fail to set	This output activates if the system or any area defined on the system failed to set; it clears when the alert is restored
Entry/Exit	This output activates if an Entry/Exit type zone has been activated; i.e. a system or area Entry or Exit timer is running
Latch	This output turns on as defined in the system latch output configuration (see Configuring system latch and auto set outputs [→ 204]). This output can be used to reset latching sensors as smoke or inertia sensors.
Fire Exit	This output turns ON if any Fire-X zones on the system are activated
Chime	This output turns on momentarily when any zone on the system with chime attribute opens
Smoke	This output turns on momentarily(3 seconds) when a user unsets the system; it can be used to reset smoke detectors The output will also activate when the zone is restored When using the zone to reset latched smoke detectors the first code entry will not activate the smoke output but will silence bells, on the next code entry if the fire zone is in the open state the smoke output will activate momentarily. This process is repeatable until the fire zone is closed.
Walk Test*	This output turns on momentarily when a walk test is operational and a zone becomes active. This output can be used, for example, to activate functional tests of connected detectors (if available).
Auto Set	This output turns on if the Auto Set feature has been activated on the system.
User Duress	This output turns on if a user duress state has been activated (PIN code + 1 has been entered on the keypad)
PIR Masked	This output turns on if there are any masked PIR zones on the system. It generates a fault output on the keypad led. This output is latched so it will remain active until restored by a level 2 user. PIR Masking is logged by default. The number of log entries do not exceed 8 between

	arming periods.
Zone Omitted	This output turns on if there are any inhibited, isolated, or walk test zones on the system
Fail to Communicate	This output turns on if there is a failure to communicate to the central station
Man Down Test	This output turns on a 'Man Down' wireless device which is activated during a 'Man Down' test.
Unset	This output is activated if the system is in Unset mode.
Alarm Abort	This output activates if an alarm abort event occurs i.e. when a valid user code is entered via the keypad after a confirmed or unconfirmed alarm. It is used, for example, with external dialers (SIA, CID, FF)
Seismic Test	This output is used to activate a manual or automatic test on a seismic zone. Seismic sensors have a small vibrator that will be attached to the same wall as the sensor and is wired to an output on the panel or one of its expanders. During the test, the panel waits up to 30 seconds for the seismic zone to open. If it does not open, the test fails. If it opens within 30 seconds the panel then waits for the zone to close within 10 seconds. If that doesn't happen, the test fails. The panel then waits a further 2 seconds before reporting the test result. The result of the test, either manual or automatic, is stored in the system event log
Local Alarm	This output activates on a local intrusion alarm.
RF Output	This output activates when a Fob or WPA button is pressed.
Modem 1 Line Fault	This output activates when there is a line fault on the primary modem..
Modem 1 Failure	This output activates when the primary modem fails.
Modem 2 Line Fault	This output activates when there is a line fault on the secondary modem.
Modem 2 Failure	This output activates when the secondary modem fails.
Battery Low	This output activates when the battery is low,
Entry Status	This output activates if an 'All Okay' entry procedure is implemented and there is no alarm generated i.e. the 'All Okay' button is pressed within the configured time after the user code is entered.
Warning Status	This output activates if an 'All Okay' entry procedure is implemented and a silent alarm generated i.e. the 'All Okay' button is not pressed within the configured time after the user code is entered.
Ready to Set	This output activates when an area is ready to set.
Setting ACK (SPC Pro — Setting Complete)	This output signals the setting status. The output toggles for 3 seconds to signal that the setting has failed. The output remains on for 3 seconds if setting is successful.
Fullset Done (SPC Pro — Setting Success)	This output activates for 3 seconds to signal that the system has been fullest.
Blockschloss 1	Used for normal Blockschloss devices. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 1' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 1' is not deactivated. If the Blockschloss is unlocked, the Blockschloss device deactivates the Keyarm input to the unset state (closed) and the area is unset. 'Blockschloss 1' is then deactivated.
Blockschloss 2	Used for Blockschloss device type - Bosch Blockschloss, Sigmalock Plus, E4.03. When all zones in an area are closed, and there are no pending faults, the 'Blockschloss 2' output is activated. If the lock on the Blockschloss is closed, a 'Keyarm' input is activated, the relevant area is set and the 'Setting Ack' output is activated for 3 seconds to signal that the setting was successful. 'Blockschloss 2' is then deactivated. If the Blockschloss is unlocked, the Keyarm zone is switched to unset (closed) and the area is unset. 'Blockschloss 2' is activated (if area is ready to set).
Lock Element	Activates if the Lock Element is in the 'locked' position.

Unlock Element	Activates if the Lock Element is in the ‘unlocked‘ position.
Code Tamper	Activates if there is a code tamper in the area. Clears when state is reset.
Trouble	Activates if any zone is in trouble state.
Ethernet Link	Activates if there is a fault on the Ethernet link.
Network Fault	Activates if there is an EDP communications fault.
Glass Reset	Used to switch on the power for the glassbreak interface module and to remove power in order to reset the device. The output is reset if a user enters their code, the zone is not in the closed state, and the bells deactivated.
Confirmed holdup	Activates in the following scenarios for PD6662 compliance: ● two hold-up zone activations more than two minutes apart ● a hold-up zone and a panic zone activation more than two minutes apart ● If a hold-up zone and a tamper zone or a panic zone and a tamper zone activation occurs within the two minute period
Full Engineer	Activates if an engineer is on site and the system is in full engineer mode.

** This output type can only indicate system wide events (no area specific events).*

See also

Configuring system latch and auto set outputs [→ 204]

11 Configuring expanders, keypads and door controllers

11.1 Configuring Expanders on an SPC panel

!	*NOTICE*
	We recommend that you connect to the panel and upload the current expander configuration before attempting to configure expanders on the panel. Only If you have an up to date and complete knowledge of the actual expander configuration on the panel, should you proceed to send your configuration settings to the panel without uploading the existing configuration from site.

When adding or editing expanders the following rules apply:

- SPC Pro will NOT allow you to send a configuration file to the panel if the number of expanders configured does not match the actual number of expanders detected on the panel. The number of expanders detected on the panel is displayed on the configuration window (see page [→ 18]) when you connect to the panel.
- SPC Pro will NOT allow you to send a configuration file to the panel if the type of expanders configured does not match the actual type of expanders detected on the system - e.g. if you configure 3 keypads and 2 I/O expanders on SPC Pro, you will be restricted from sending this configuration to a panel with 3 I/O expanders and 2 keypads.

You may configure expanders on the panel using 2 methods:

Get configuration file from panel before configuring (recommended)

This is the recommended method for adding expanders to the panel. On connecting and uploading the current configuration. See page [→ 19].

SPC Pro will present you with a copy of the existing configuration on the panel. You will then know the number, type and order of expanders connected to the X-BUS on the panel. See page [→ 92].

You may proceed to edit the expanders in the list as required and then send your changes to the panel.

Send configuration file to panel without uploading

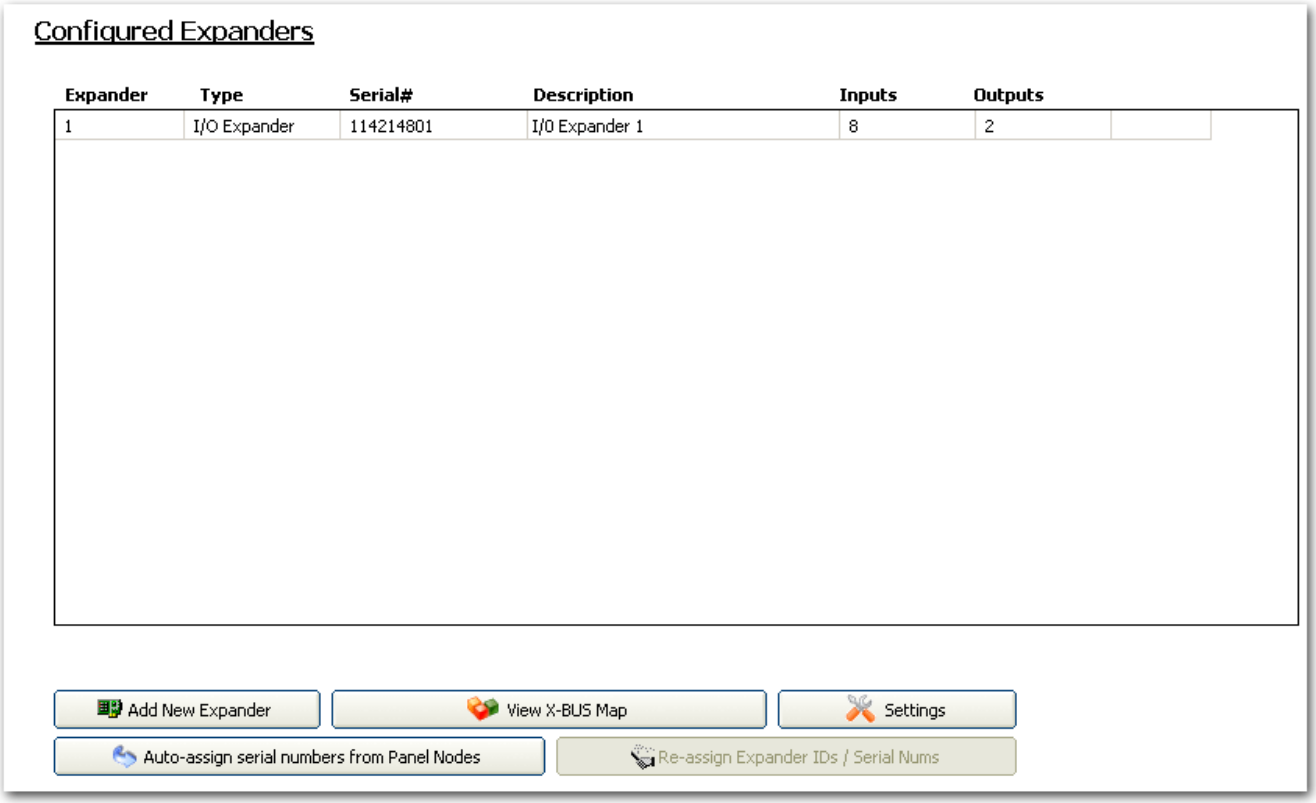
1. Before using this method it is essential that you have a complete knowledge of the number and type of expanders connected to the panel. To send your expander configuration to the panel follow these steps:
2. On first connecting to the panel, the number and type of expanders detected is displayed on the **Panel Status** – X-BUS summary window. See page [→ 34].
3. Make a note of this list detailing the number, type and order of the expanders on the X-BUS .
4. Go to **Panel settings > Expanders & Keypads > Expanders**
5. Add the appropriate number and type of expanders to match the list presented in the panel window **Status** – X-BUS.
6. You may then configure these expanders as required. See page [→ 94].
7. Send your configuration changes to the panel.

11.2 Expanders

11.2.1 Adding and Configuring Expanders

Expanders & Keypads

1. Click the **Expander** tab.
   ⇨ The following window will be displayed.



2. The following information is displayed for each expander.

Expander	The expander number on the panel.
Type	The type of the expander (Keyswitch, I/O, PSU, Wireless, etc.).
Serial Number	The serial number of the expander.
Description	The text description of the expander.
Status	The current status of the expander (online/offline).
Inputs	The number of inputs on the expander.
Outputs	The number of outputs on the expander.

Performable actions

Add New Expander	Click this button to add a new expander to the panel.
View X-BUS Map	
Settings	Click this button to configure the X-BUS on the panel.

Auto-assign serial numbers from Panel Nodes	Click this button to enable the system to automatically assign serial numbers to existing expanders on the panel.
Re-assign Expander IDs Serial Nums	Click this button to re-assign existing expanders on the panel.

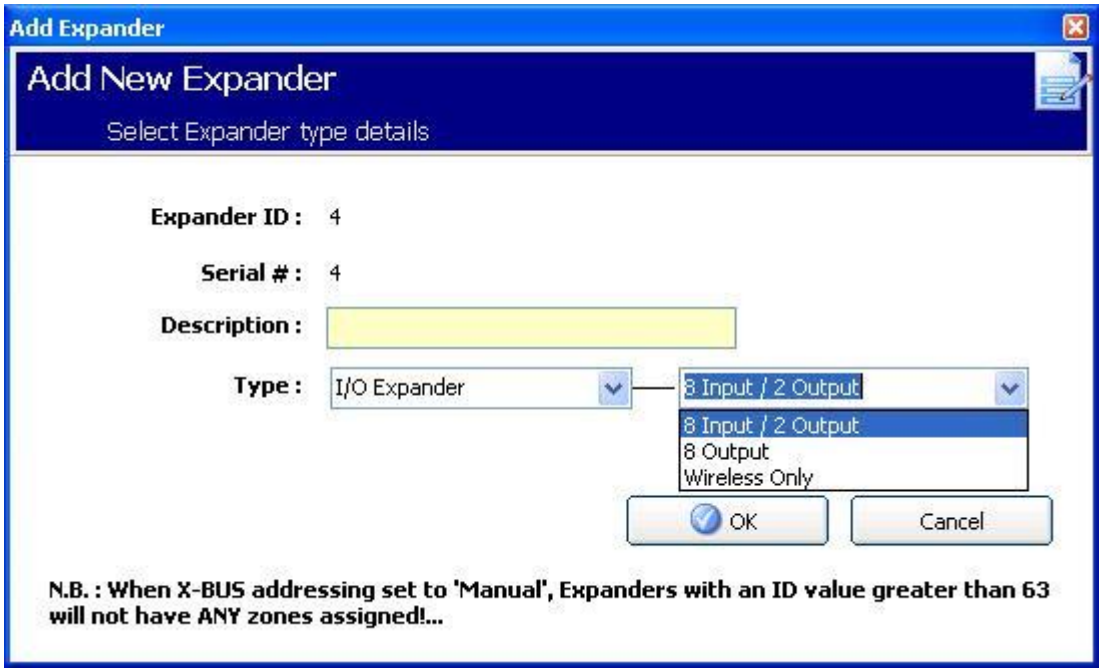
See also

- X-BUS [→ 34]
- Activate keypad emulation [→ 217]

11.2.1.1 Adding a New Expander

Add new Expander

1. Click the button **Add New Expander**.
   ⇨ The following window will be displayed.



2. Configure the fields as described in the table below.
3. Click **OK**.

Expander ID	The number is presented for reference and can not be programmed.
Serial Number	The serial number of an expander is located in the expander firmware and can not be programmed. The number listed in this field is used simply as a reference when adding the expander. The serial number field will be listed as <unassigned> in the expander list if this information has not yet been uploaded from the panel.
Description	Enter a text describing the expander (max. 16 characters). This text will also appear on the browser and keypad.
Type	Select the type of expander. If I/O Expander is selected, also select the type of I/O Expander

New expanders can only be added to the panel if they have been physically wired to the X-BUS and added to the configuration file. If expanders have been physically wired to the panel X-BUS on site but not yet added to the configuration database, then you can add them to the system using SPC Pro by following these steps:

11.2.1.2 Adding an Expander to the Configuration Database

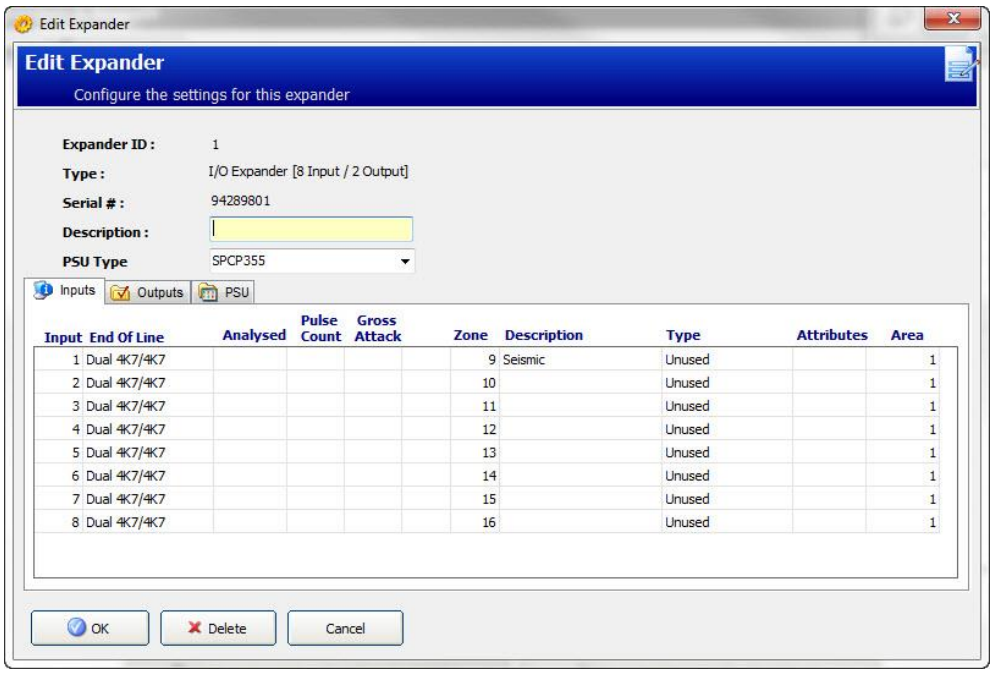
1. Connect to the panel.
2. Check the X-BUS summary status. See page [→ 34].
3. Any newly wired expanders will be displayed with a status of pending.
4. Click on the virtual keypad. See page [→ 217].
5. Enter Engineer programming mode.
6. Select FULL ENGINEER > EXPANDERS > ADD.
   ⇨ The expanders will be listed in this menu.
7. Select **Add** to add these expanders to the database.
8. Exit the virtual keypad.
9. Click **Get config file from panel**.
10. Open the Expander list.

⇨ The newly added expanders will be listed and can be configured as required.

11.2.2 Configuring an Input/Output Expander

Expanders & Keypads

1. Click an expander from the list.
   ⇨ The following window will be displayed.



2. Enter the following information for the expander:

Description	Enter a new description or edit the existing description for the expander.
Volume Limit	**Audio Expander Only:** Speaker volume for the Audio Expander and satellites (WAC 11. Range is 0 min - 7 max or disabled.
Auxillary Channnel	**Audio Expander Only:** This option should be enabled if satellites are connected to this expander to power the satellite microphones.

- Enter **Input** and **Output** information as detailed in the following sections.

Inputs

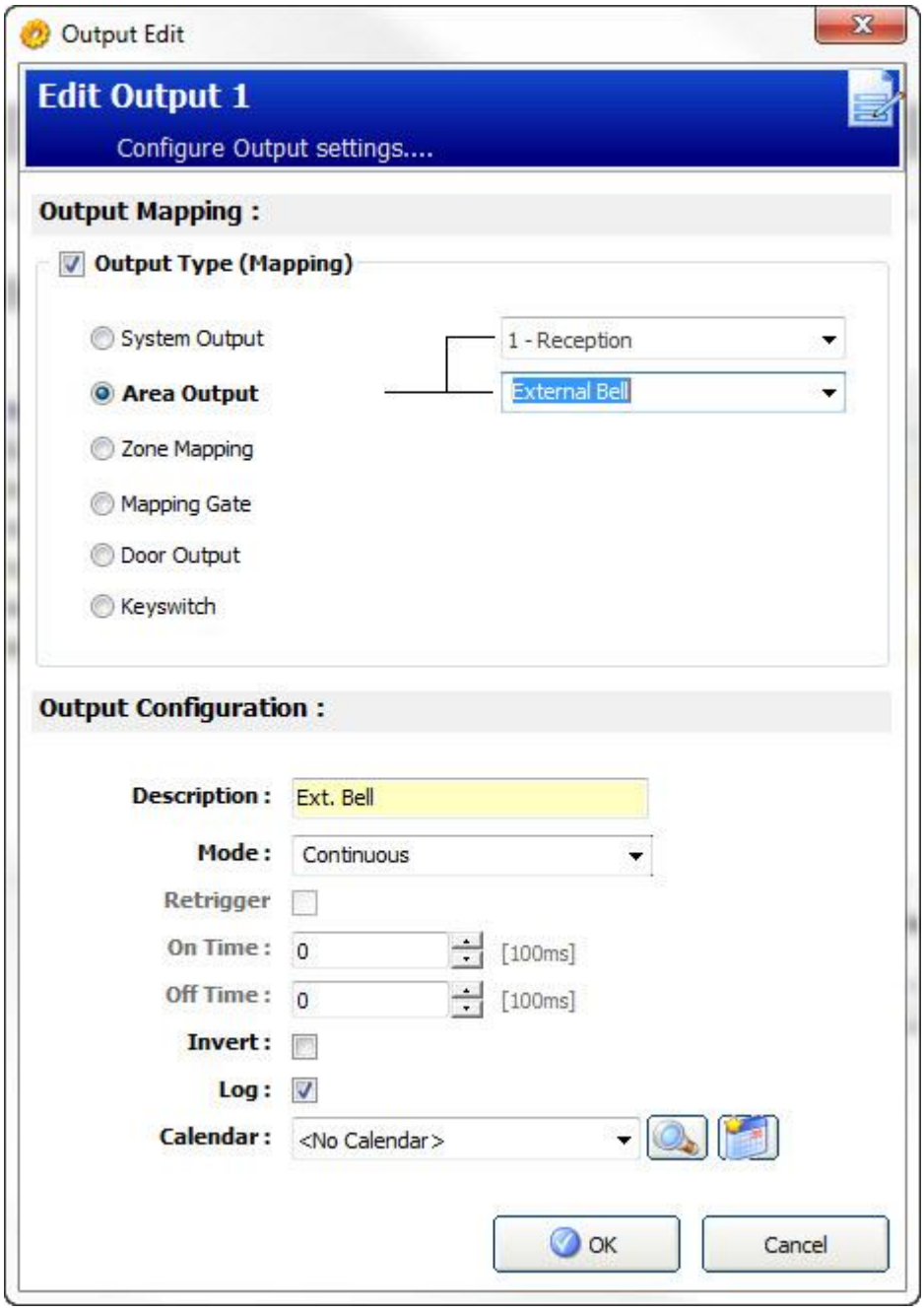
1. Click an input from the list.
   ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.
3. Click **OK**.

Input	The number is presented for reference and can not be programmed.
End of Line	Select the **E**nd **O**f **L**ine (EOL) for the zone input (default: 4K7).
Analyzed	Displays if the sensor is an inertia/shock type sensor.
Pulse count	Pulse count programmed on the panel that will trigger an alarm from an inertia / shock sensor.
Gross Attack	The Gross attack programmed on the panel that will trigger an alarm from an inertia/shock sensor.
Zone	Number of the zone on the panel.
Description	Enter a text describing the input (max. 16 characters). This text will also appear on the browser and keypad.
Type	The type of zone. See page [→ 260].
Area	Only if (multiple) **Areas** is activated in menu **Panel Settings > System Settings > Options**. The areas to which this zone has been assigned.

An icon in this field indicates that attributes have been programmed for this zone. See page [→ 262].

Outputs

1. Click the tab **Outputs** in the window **Edit Expander**.
2. Click an output from the list.
   ⇨ The following window will be displayed.
3. See tables below for further information.



Output Type	• **System Output**: Select the type from the dropdown menu. (See Output Types and Output Ports [→ 87]) • **Area Output**: Only if **(multiple) Areas** is activated in menu **Panel Settings > System Settings > Options**. Select an area and the type of system output for this area. (See Output Types and Output Ports [→ 87]) • **Zone Mapping**: Select which zone should be mapped. • **Mapping Gate**: Select which mapping gate should be mapped. • **Door Output**: Select the door number and the type of system output for the door.

	(See Output Types and Output Ports [→ 87]) ● **Keyswitch**: Select the node ID for the required keyswitch and the required key position to map to this output.
Description	Enter a text describing the output (max. 16 characters). This text will also appear on the browser and keypad.
Output Configuration	● **Mode**: Select the operational mode. Continuous follows output type; Pulsed toggles on and off when output type is active; Momentary generates a pulse when output type activates. ● **Retrigger**: Tick the box to retrigger momentary outputs. ● **On Time**: Enter the On time that applies to momentary and pulsed outputs. ● **Off Time**: Enter the Off time that applies to pulsed outputs. ● **Invert**: Tick this box to invert the physical output. ● **Log**: Tick this box to log the output state changes to the event log. ● **Calendar**: Select if necessary the desired calendar. See page [→ 194].

Performable actions

Refresh Output Status	Click on this button to refresh the status of the outputs.
Test Outputs	Click on one of these buttons to test if the output is connected correctly (light will go on).

The functionality **Test Outputs** is only available in Full Engineer mode.

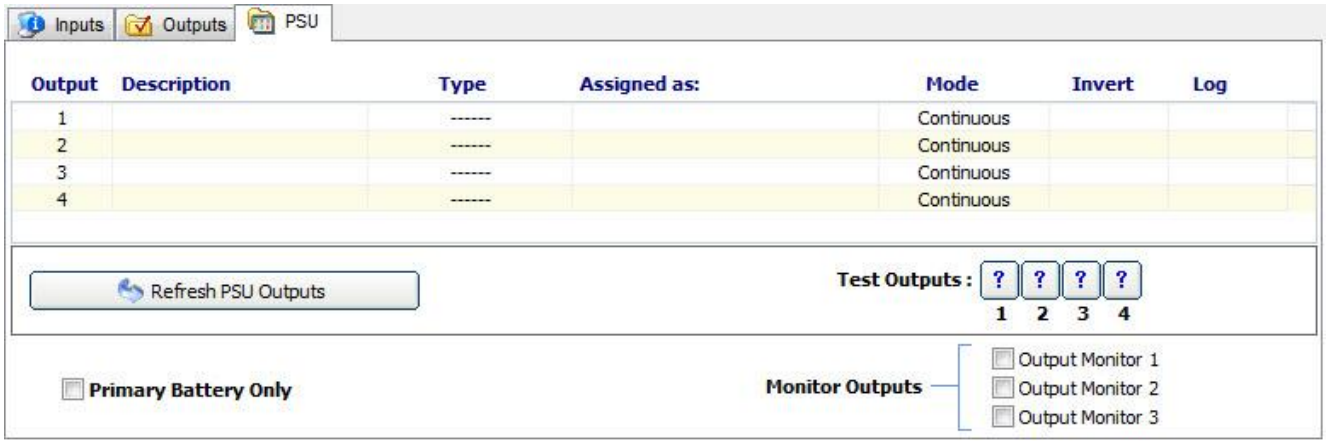
See also

Calendars [→ 194]

11.2.2.1 PSU Tab

The PSU tab enables you to configure and test the outputs for the SPCP355 Smart PSU.

Note: This tab is displayed only if SPCP355 Smart PSU is selected from the PSU Type drop-down list.



The following table lists the fields of the PSU tab:

Name	Description
Output	The numbered output. Click a line to open the Edit PSU Output window for the selected output. This enables you to assign specific behaviour to each output. For more information, see Editing an output [➔ 85].
Description	Provide description for output.
Change type	Change the type of output as necessary.
Attributes	Assign attributes to the output.
Test Outputs	Test the output.
Monitor Outputs	Select which outputs are to be monitored.
Primary battery only	Tick this box if there is no secondary battery connected to the PSU

11.2.3 Configuring an Indicator Expander

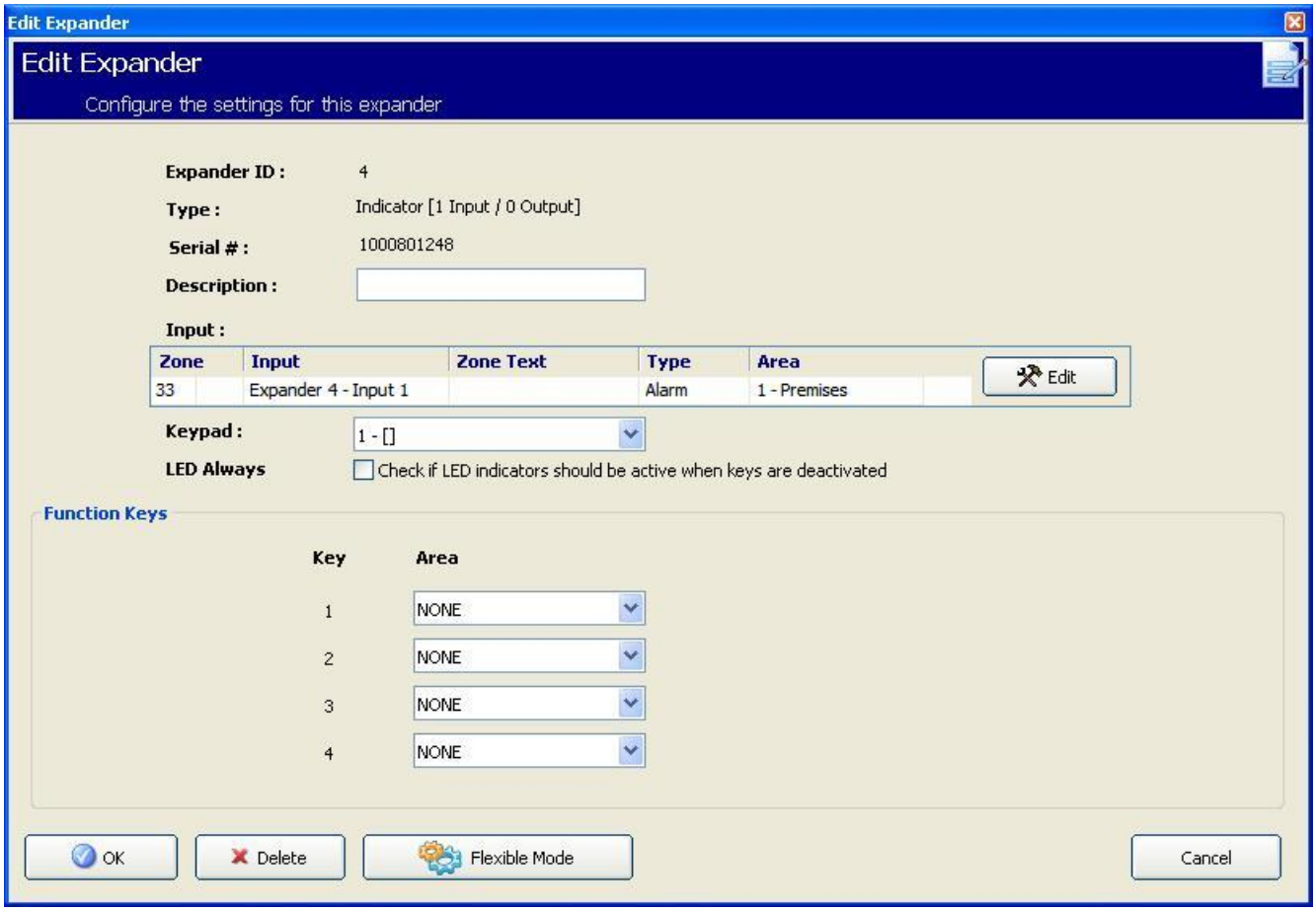
There are 2 possible configuration modes for the indication expander:

- Linked Mode
- Flexible Mode

Expanders & Keypads

- Add a new indicator expander or click on an existing indicator.

⇨ The following dialog box is displayed for **Linked Mode** configuration.



Linked Mode

1. Enter a description.
2. Select if indicator module should be limited to a valid code entered on a keypad.
3. Select the areas that are to be controlled by the 4 functions keys.
4. Configure the input.

Flexible Mode

1. Click the **Flexible Mode** button.
2. Configure the fields described in the tables below.
3. Configure the input.

WARNING

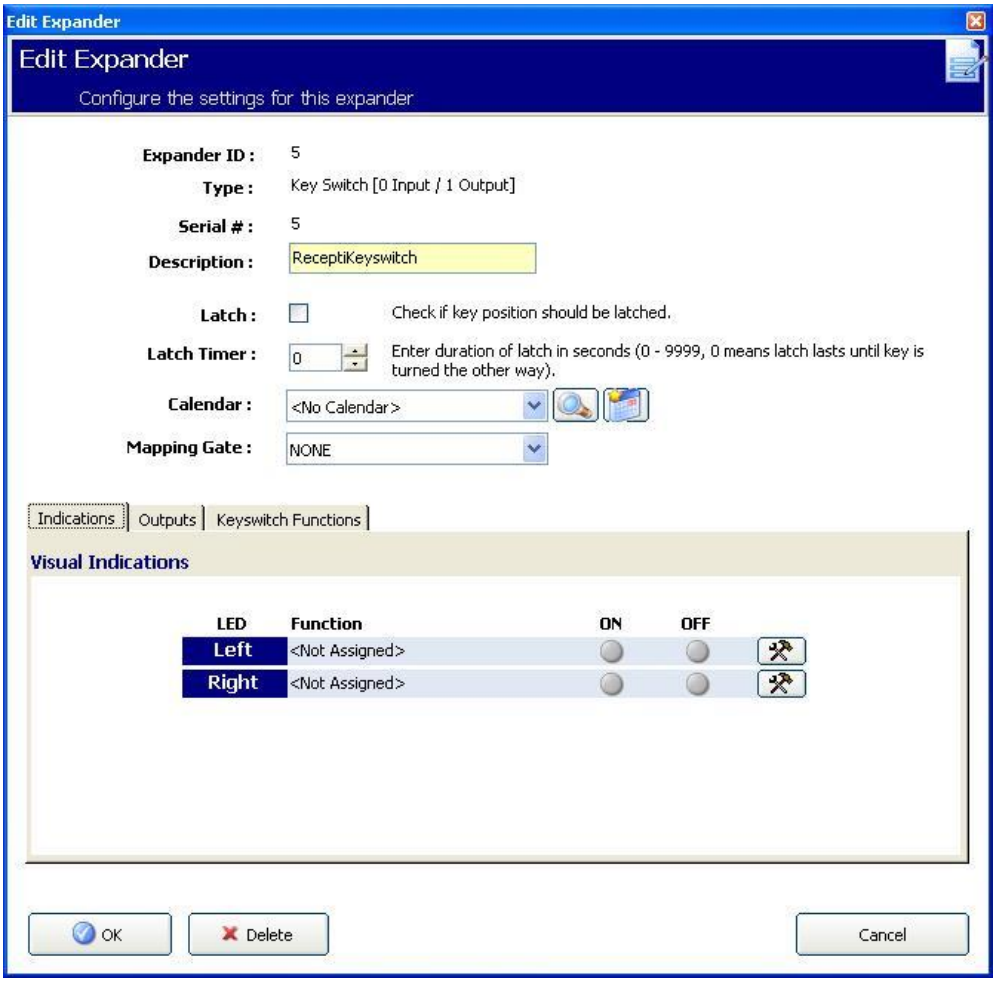
Your system will not comply with EN standards if you enable a function key to set the system without a valid PIN being required.

Function Keys	
Area	Select the area is to be controlled by the function key.
Function	Select the function to be performed by this key in this area..
Area	Select an area if the indicator module is located in a secure area.

Visual Indication	
Indicator	There are 8 indicators / LEDs on the right and 8 indicators / LEDs on the left side.
Function	The function that is indicated by this LED.
Function On	Select the colour and the state for every indicator if the selected function is ON.
Function Off	Select the colour and the state for every indicator if the selected function is OFF.
Change function	Press this button to change the function for this indicator. The function can be enabled or used for a system, area, zone or keyswitch.
Audible Indications	
Alarms	Select if the alarms should be audible.
Entry / Exit	Select if entry / exit should be audible.
Key press	Select if keypress should be audible.
Deactivation	
Calendar	Select if indicator expander should be limited by calendar.
Mapping gate	Select if indicator module should be limited by a mapping gate.
Keyswitch	Select if indication module should be limited by a keyswitch.
Keypad	Select if indicator module should be limited to a valid PIN entered on a keypad. (see warning above)
Card reader	Select if indicator module should not be activated until a valid card/fob is presented to the built-in card reader.

11.2.4 Configuring a Keyswitch Expander

- Click on the keyswitch in the list of configured expanders.
  ⇨ The following dialog is displayed:



- Configure the fields described in the tables below.

Description	Enter a description for the keyswitch expander.
Key Options	
Latch	Select if key position should be latched.
Latch timer	Enter duration of latch in seconds (0 - 9999, 0 means latch lasts until key is turned the other way).
Areas	
Location	Select the area where the keyswitch is located.
Visual Indications	
Indicator/LED	There is 1 indicator / LED on the right and 1 indicator / LED on the left side.
Function	The function for this indicator / LED.
Function On	Select the colour and the state for every indicator if the selected function is ON.
Function Off	Select the colour and the state for every indicator if the selected function is OFF.
Change function	Press this button to change the function for this indicator. The function can be enabled or used for a system, area, zone or keyswitch.
Deactivation	
Calendar	Select if the keyswitch module should be limited by calendar.
Mapping gate	Select if the keyswitch module should be limited by a mapping gate.
Output	
Output *x*	Configure and text the outputs for the keyswitch. See Outputs [→ 97] for more details
Keyswitch Functions	

Centre, Right and Left Positions	Select the **Function** that that this keyswitch position will perform and the relevant **Area**.

⚠ WARNING

Your system will not comply with EN standards if you enable a keyswitch function to set the system without a valid PIN being required.

11.2.5 Re-assigning expanders

Panel Settings 

Expanders & Keypads

The order in which expanders are listed and identified on the X-BUS is performed during the initial installation of the panel or whenever a cold start of the panel is performed.

To re-assign an expander to a different location on the X-BUS:

1. Click the button **Re-Assign Expanders** in the window **Configured Expanders**.
2. Select the expander you wish to re-assign by using the up and down arrows on the right of the window.
3. Click the button **Re-assign Now**.
   ⇨ A pop up message will be displayed informing you that the expander will be re-assigned.
4. Click **YES**.

⇨ The configured expander list window is displayed showing the new order of the expanders.

Re-assigning expanders allows you to mix and match the expander IDs to match the physical addition or replacement of an expander - i.e. an installer may have physically connected an I/O expander between existing expanders with IDs 1 & 2. The new expander might be the 6th expander on the X-BUS giving an ID pattern of 1, 2, 6, 3, 4, 5. By re-assigning expander IDs to match the physical order of expanders on the panel you can keep track of the actual configuration. The advantage of this is as follows:

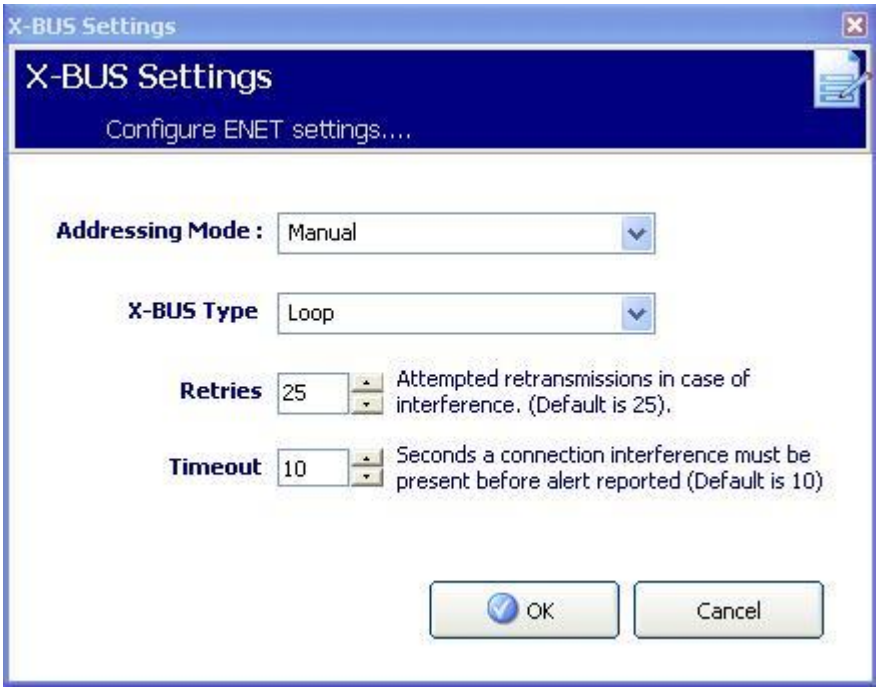
- You may wish to re-order expanders of the same type to match the programming correctly on the panel – i.e. the configuration of the third I/O expander in your configuration file may need to sent to the second I/O expander on the panel.
- If you do a cold start of your system, the configuration data of all other expanders won't be lost or overwritten as the expander numbering matches the physical order of the expanders.

11.2.6 Editing X-BUS settings

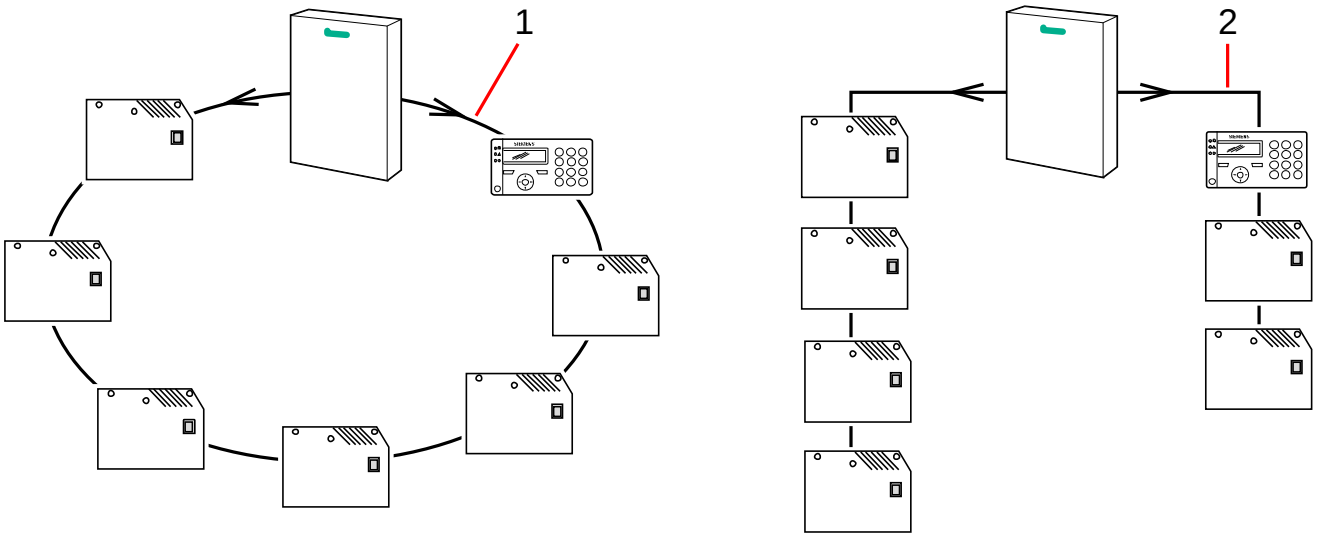
Panel Settings 

Expanders & Keypads

1. Click the button **Settings** in the window **Configured Expanders**.
2. Configure the fields as described in the table below.
3. Click **OK**.



Addressing Mode	Select if the Expander is either manually or automatically addressed on the X-BUS .
X-BUS Type	Select the type of X-BUS configuration (Loop or Spur) from the drop down list. If this data is read from the panel, changed and then send back to the panel – the actual configuration will remain unchanged unless an installer on site has physically re-wired the X-BUS to match the programmed configuration.
Retries	Select the number of communication retries on the X-BUS in the event that there is electrical interference on the installation site (1 – 99: default is 25).
Timeout	Select the number of seconds for which connection interference is present before an X-BUS communications fault is reported.



1	RS485 Closed Loop (Ring) configuration. Communication is bi-directional for all expanders (SPC5000 / SPC6000 only).
2	RS485 Open Loop (multi-drop) configuration. Expanders at the end of the open loop.

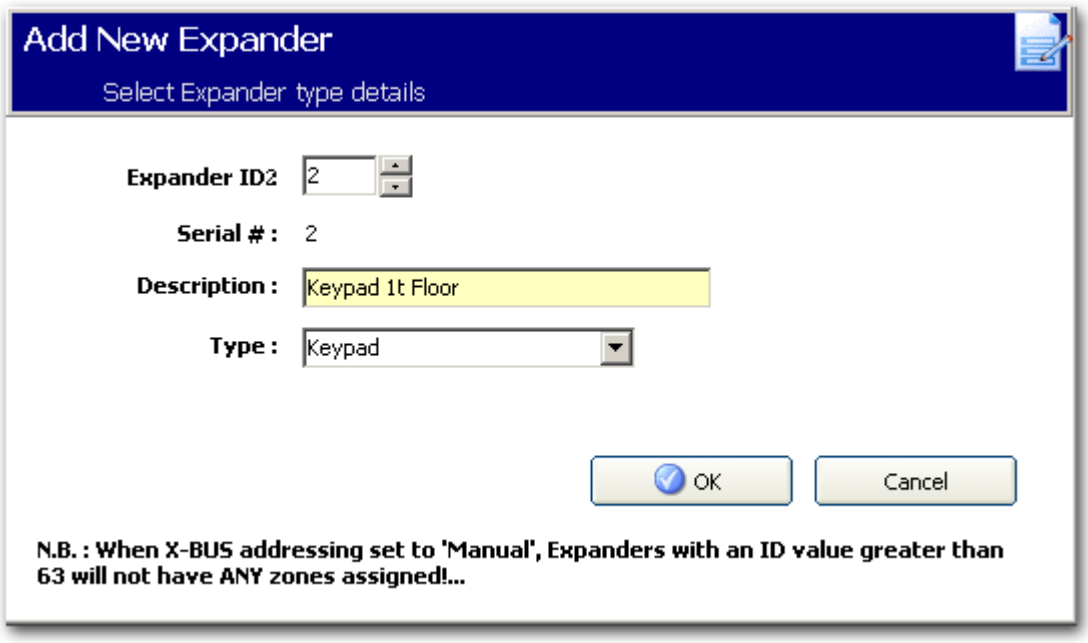
It is advisable to be aware of the physical configuration of the installation before programming these settings and sending them to the panel. The electrical characteristics of an installation may require some adjustment of the X-BUS retries and timeout parameters to deliver optimum performance.

11.3 Keypads

11.3.1 Adding a keypad

Expanders & Keypads

1. Click the tab **Keypad**.
2. Click the button **Add New Keypad**.
   ⇨ The following window will be displayed:



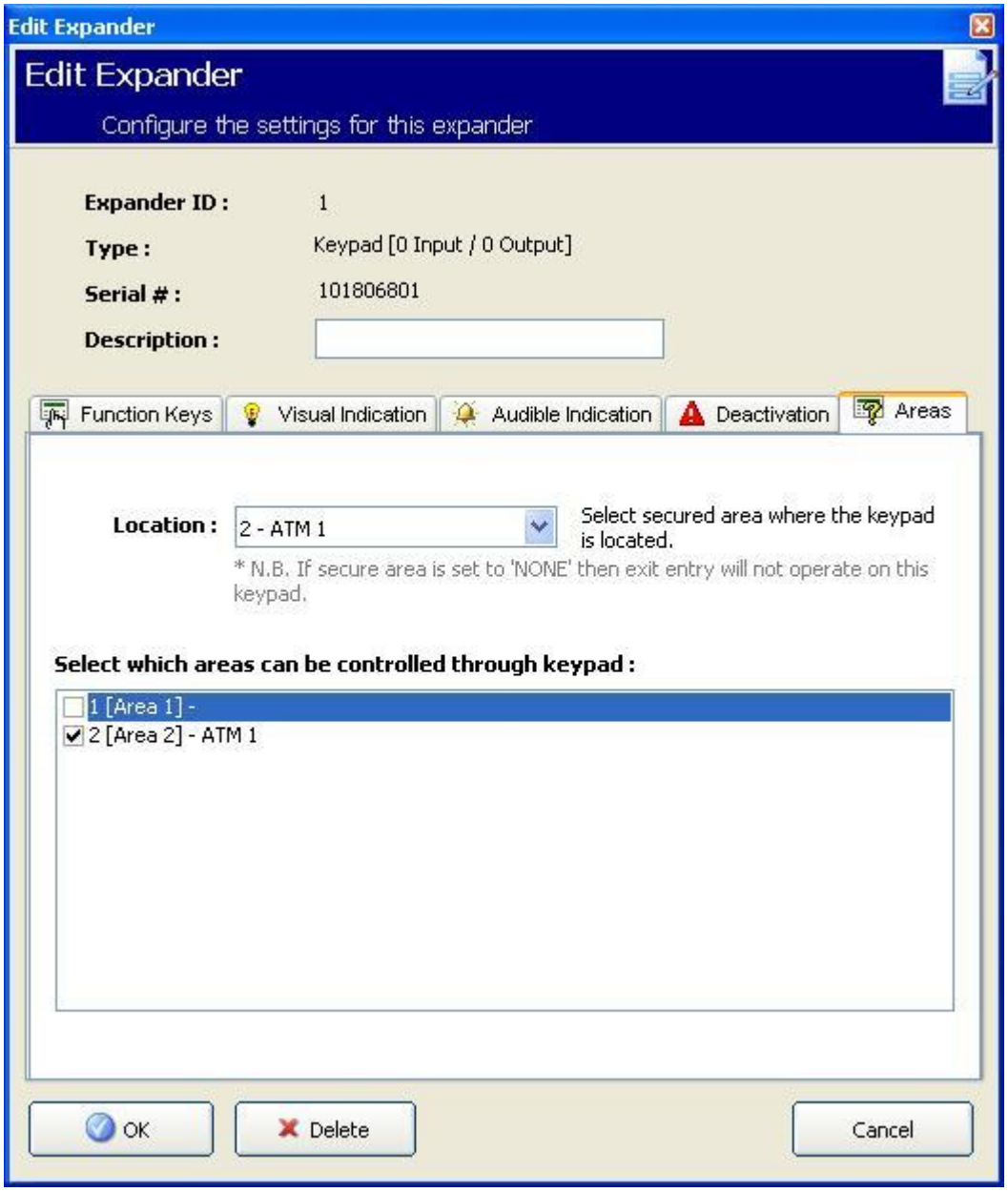
3. Configure the following fields and click **OK**.

Expander ID	The number is presented for reference and can not be programmed.
Serial #	The serial number of an expander is located in the expander firmware and can not be programmed. The number listed in this field is used simply as a reference when adding the expander. The serial number field will be listed as <unassigned> in the expander list, if this information has not yet been uploaded from the panel.
Description	Enter a text describing the keypad (max. 16 characters). This text will also appear on the browser and keypad.
Type	Select keypad.

11.3.2 Editing a Standard Keypad

Expanders & Keypads

1. Click one of the standard keypad identifying parameters.
2. Configure the fields as described in the table below.



Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing the 2 soft keys together.
Verification	If you assign a verification zone to the keypad, when a panic alarm is triggered by pressing 2 soft keys together or by entering a duress code, audio and video events are activated.
Visual Indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off..
Indicators	Enable or disable the LED's on the keypad.
Setting state	Select if setting state should be indicated in idle mode.
Audible Indications	
Buzzer	Enable or disable the buzzer on the keypad.
Partset Buzzer	Enable or disable buzzer during exit time on Partset.

Keypress	Select if the speaker volume for the key presses should be activated.
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See Calendar [→ 194].
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.
Options	
Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.

	NOTICE
	An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available

See also

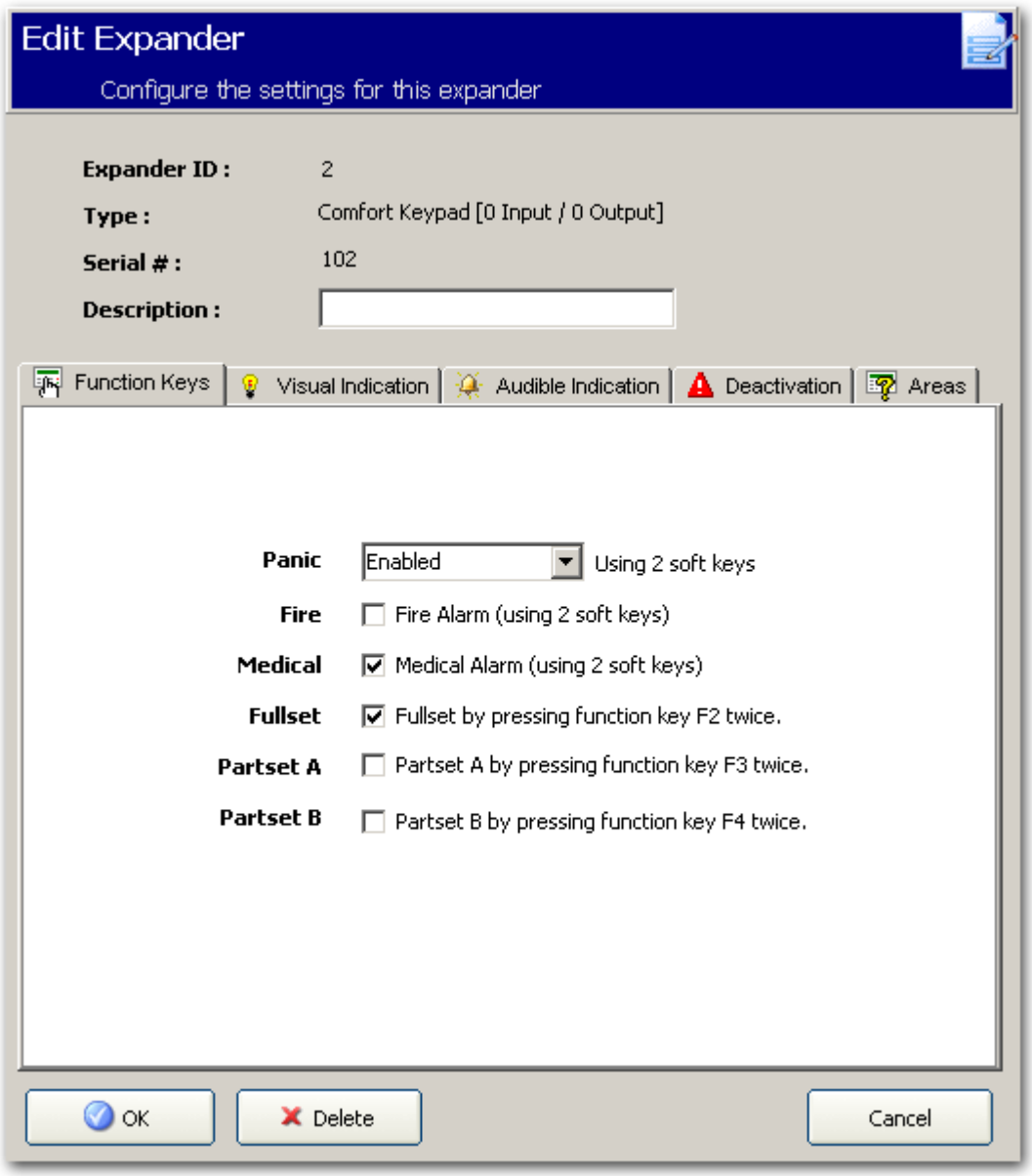
- Calendars [→ 194]

11.3.3 Editing a Comfort Keypad

Panel Settings

Expanders & Keypads

1. Click one of the comfort keypad identifying parameters.
2. Configure the fields as described in the table below.



Description	Enter a unique description to identify the keypad.
Function Keys (in idle state)	
Panic	Select Enable, Disable or Enabled Silent. If enabled, panic alarm is activated by pressing F1 and F2 soft keys together.
Fire	Enable to allow fire alarm to be activated by pressing F2 and F3 soft keys together.
Medical	Enable to allow medical alarm to be activated by pressing F3 and F4 soft keys together.
Fullset	Enable to allow Fullset to be activated by pressing F2 key twice.
Partset A	Enable to allow Partset A to be activated by pressing F3 key twice.
Partset B	Enable to allow Partset B to be activated by pressing F4 key twice.
Verification	If you assign a verification zone to the comfort keypad, when a Medical, Panic or Fire event is triggered, or if a user enters a duress code, then audio and video events are activated.

Visual indications	
Backlight	Select when keypad backlight is on. Options are: - On after key is pressed; Always on; Always off.
Backlight Level	Select the intensity of illumination of the backlight. Range 1 - 8 (High).
Indicators	Enable or disable the LED's on the keypad.
Setting state	Enable if setting state should be indicated in idle mode. (LED)
Logo	Enable if logo should be visible in idle mode.
Analog Clock	Select position of clock if visible in idle mode. Options are Left Aligned, Center Aligned, Right Aligned or Disabled.
Emergency	Enable if Panic, Fire and Medical function keys should be indicated in the LCD display.
Direct Set	Enable if Fullset/Partset function keys should be indicated in the LCD display.
Audible indications	
Alarms	Select speaker volume for alarm indications or disable sound.
Entry/Exit	Range is 0 – 7 (Max volume)
Chime	Select speaker volume for entry & exit indications or disable sound.
Keypress	Range is 0 – 7 (Max volume)
Voice Annunciation	Select speaker volume for chime or disable sound.
Partset Buzzer	Range is 0 – 7 (Max volume)
Deactivation	
Calendar	Select if the keypad should be limited by calendar. See Calendar.
Mapping gate	Select if keypad should be limited by a mapping gate.
Keyswitch	Select if keypad should be limited by a keyswitch.
PACE Entry	Tick this box to disable the keys on the keypad during the entry time when a PACE is configured on the keypad.
Areas	
Location	Select the secured area where the keypad is located.
Areas	Select which areas can be controlled through keypad.
Options	
Delay Fullset	Select to configure a delayed set across all keypads. The location of the keypad is ignored and all areas will perform a full exit time count down.

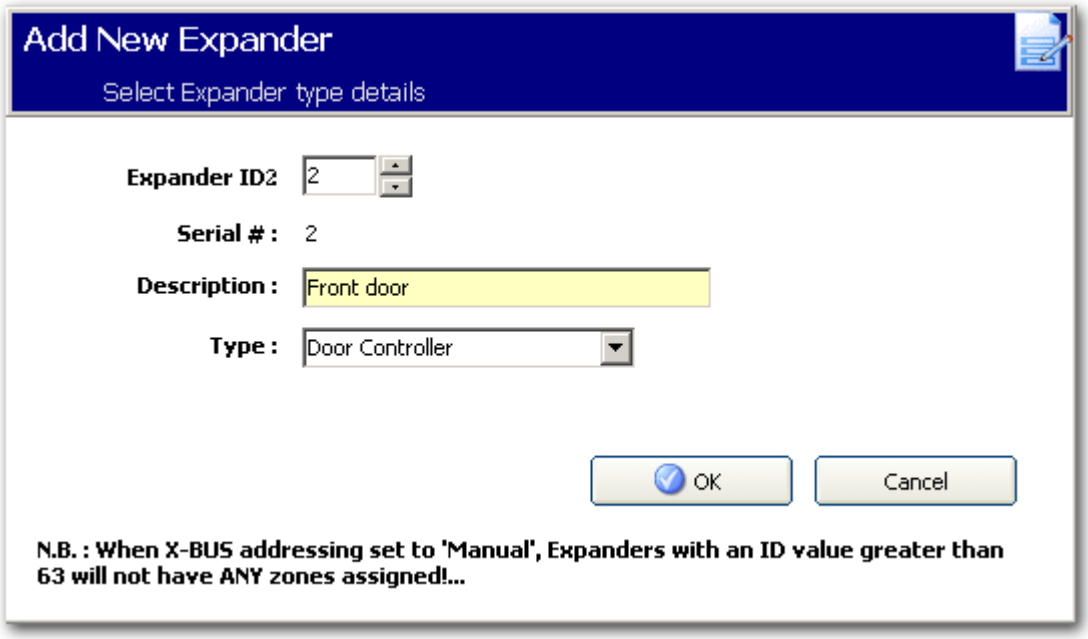
	*NOTICE*
	An area should be assigned to a keypad only if the keypad is inside the assigned area, and if an entry/exit route is defined. If an area is assigned, when the particular area is set or unset then entry and exit timers are used (if configured). Other features related to entry/exit routes also become available. If no area is assigned, the area is set or unset immediately and other entry/exit features are not available.

11.4 Door Controllers

For general information on door controllers please refer to the SPC42xx/43xx/52xx/53xx/62xx/63xx Installation&Configuration Manual.

11.4.1 Adding a door controller

1. Click the **Door controllers** tab.
2. Click the button **Add New Door Controller**.
3. See table below for further information.

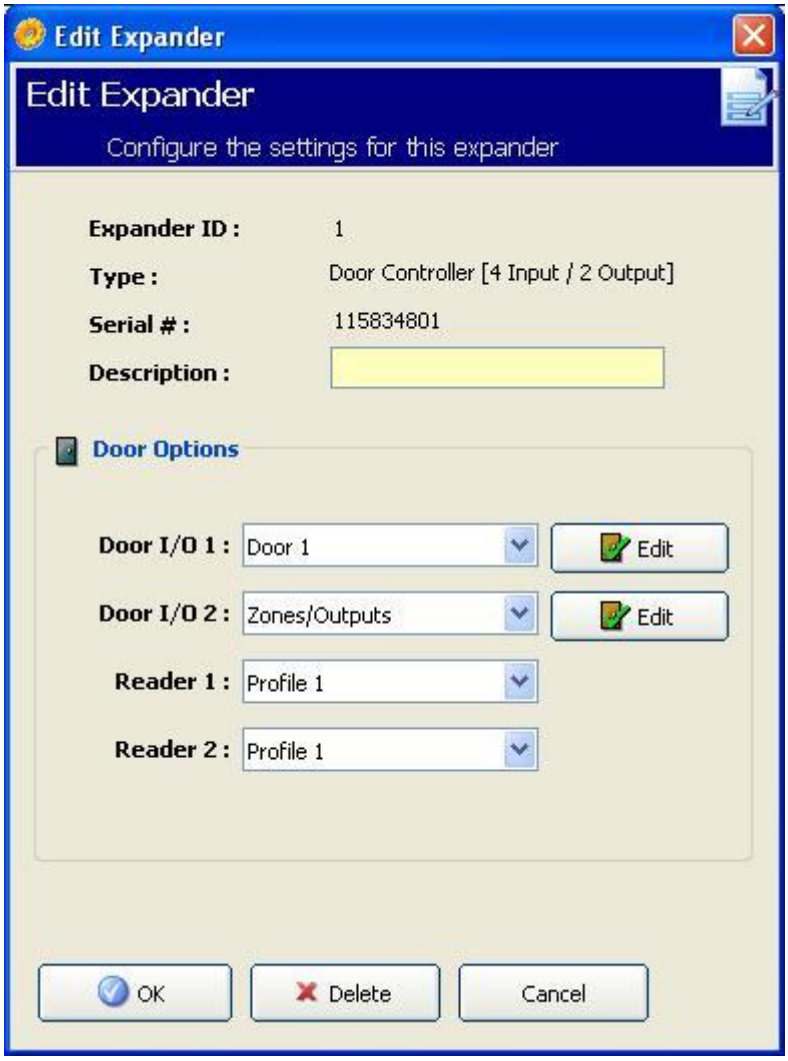


Expander ID	The number is presented for reference and can not be programmed.
Serial #	The serial number of an expander is located in the expander firmware and can not be programmed. The number listed in this field is used simply as a reference when adding the expander. The serial number field will be listed as <unassigned> in the expander list, if this information has not yet been uploaded from the panel.
Description	Enter a text describing the door controller (max. 16 characters). This text will also appear on the browser and keypad.
Type	Select Door Controller.

11.4.2 Editing a door controller

1. Click a door controller from the list.

2. Configure the fields as described in the table below.
3. Click **OK**.



For naming and identifying:

In loop configuration, each expander is numbered consecutively from the first (expander connected to the 1A 1B on the controller) to the last (expander connected to the 2A 2B on the controller).

Example for SPC63xx: Expanders, when numbered 1 through 63, are allocated zones (in groupings of 8) in subsequent identities of 1 to 512 (the greatest number in zone identification is 512). Therefore, any expander named or identified by a number greater than 63 has no allocated zones.

Expander ID	ID of the door controller set with the rotary switches.
Type	Type of the door controller.
S/N	Serial number of the door controller.
Description	Description of the door controller..
Door I/O 1 Door I/O 2	● If a door is assigned to the door I/O, select the corresponding door number. If the two inputs and outputs are configurable, select **Zones / Outputs**. ● If a door number is selected for the door I/O, the door settings can be changed by clicking on the edit button. This is equal to **Settings > Doors**.

	● If **Zones / Options** is selected, the two zones and the one output can be configured by clicking the edit button.
Profile 1	For readers with a green and a red LED.
Profile 2	For VANDERBILT readers with a yellow LED (AR618X).
Profile 3	Profile 3 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (0)
Profile 4	Profile 4 is used with HID readers that send a PIN to the panel as a card reading with a predefined site code (255).
Profile 5	Select to enable Sesam readers. It is also recommended that you select the Override Reader Profile option to provide feedback on the setting process.

Editing Zones/Outputs for a Door I/O

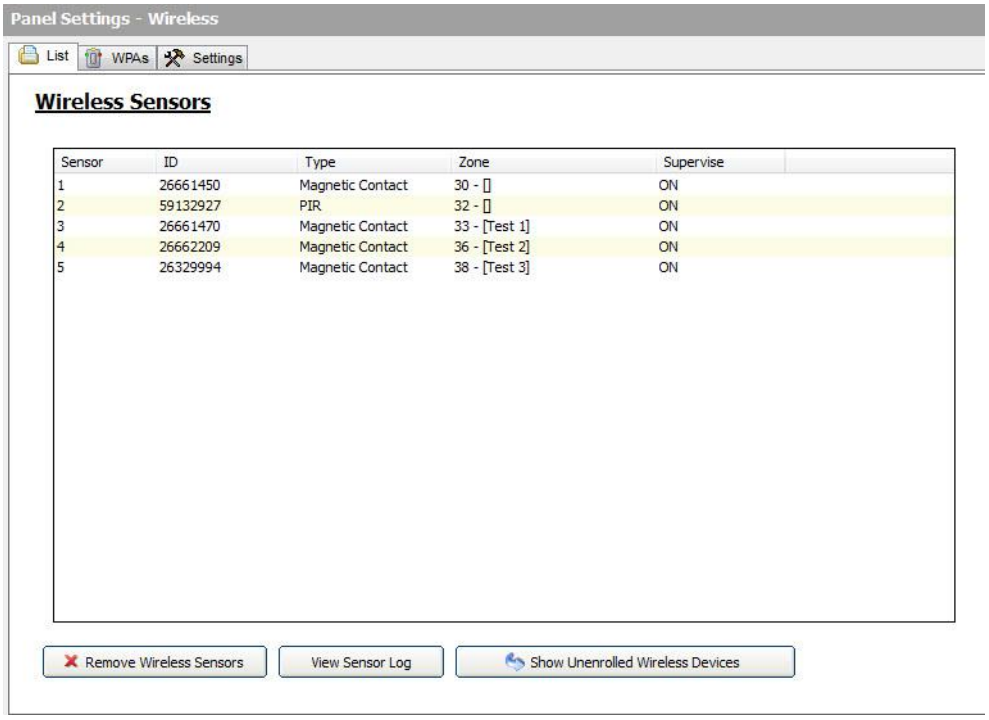
1. Select a Zone/Output for the door I/O.
2. Click the **Edit** button.
3. The 2 inputs and the output belonging to this door I/O can be configured as normal door inputs and outputs. See page [→ 139].
4. In order to use the inputs, they have to be assigned to a zone number.

12 Wireless

Wireless sensor detection (868 MHz) on the SPC panel is provided by wireless receiver modules which may be factory fitted on the keypad or on the controller, or by installing a wireless expander.

Wireless

1. Click the **List** tab.
2. See table below for further information.



Sensor	The number of the sensor enrolled on the system (1 = first, 2 = second, etc.)
ID	A unique identity number for that sensor.
Type	The type of wireless sensor detected (magnetic contact, inertia/shock, etc.)
Zone	The zone to which the sensor has been enrolled.
Battery	The status of the battery in the sensor (if fitted).
Supervise	The status of the supervisory operation (OK = supervisory signal received, Not Supervised = no supervisory operation).
Signal	The signal strength received from the sensor (01=low, 09=high). **Note:** Although it is not possible to enroll a device with a signal strength less than 3, devices whose signal drops below 3 after enrollment are not dropped.

Performable actions

Remove wireless sensor	Click this button to remove the highlighted wireless sensor from the panel. Confirm the action.
View Sensor Log	Click to view the wireless sensor Log. See page [→ 115].
Show Unenrolled Wireless Devices	Click to view the list of unenrolled wireless sensors detected by the panel. See page [→ 115].

12.1 Log - Wireless sensor X

To view a quick log of events for a wireless sensor:

1. Highlight a wireless sensor.
2. Click the **View Sensor Log** button.
3. See table below for further information.

Date/Time	The date and time of the logged event.
Receiver	The wireless receiver location, i.e. wireless module mounted on the keypad, controller or wireless expander.
Signal	The signal strength received from the sensor (01=low, 09=high).
Status	The physical status of the sensor.
Battery	The status of the battery connected to the sensor (OK, Fault).

12.2 Unenrolled devices

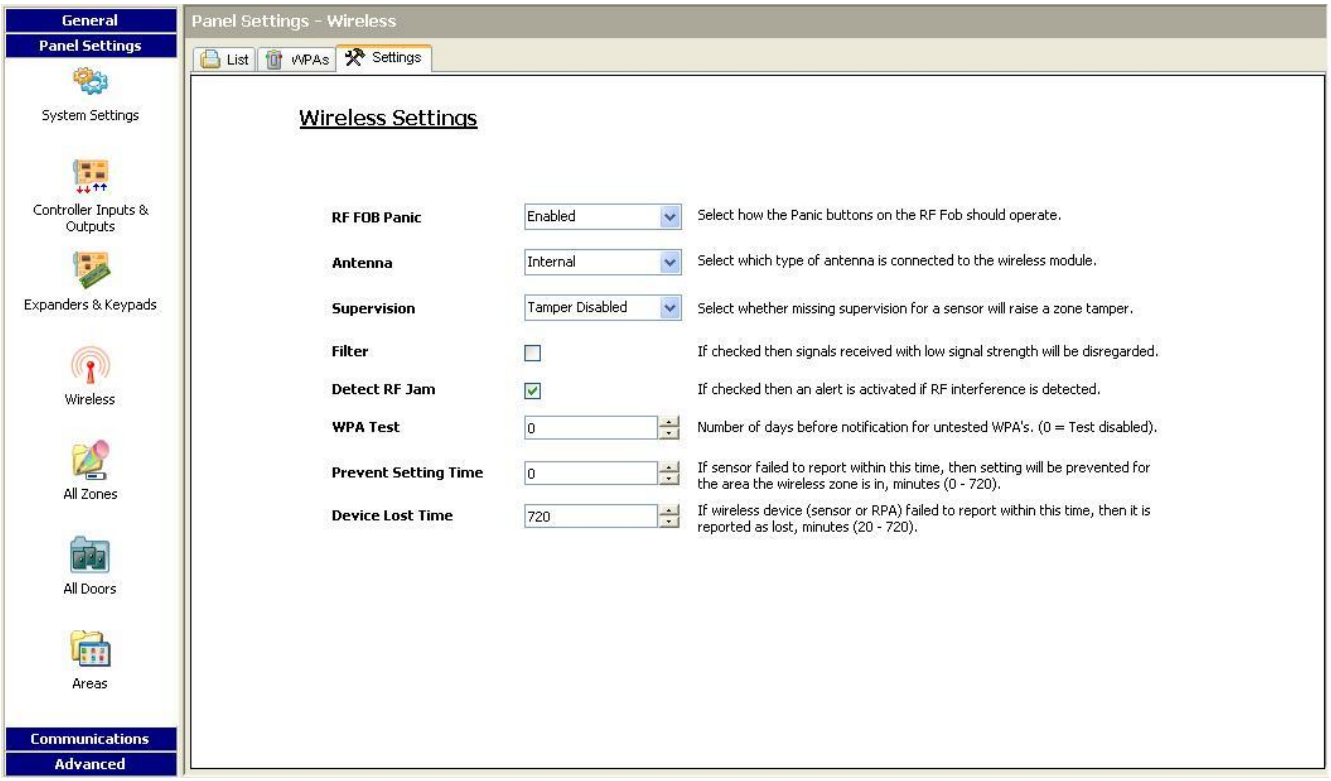
To view a list of all wireless devices that have been detected on the panel but have not yet been enrolled:

1. Click the **Show Unenrolled Wireless Devices** button.
2. See table below for further information.

Sensor ID	The ID number that uniquely identifies that sensor. This number will not be accessible until such time as a signal form the wireless device has been received by the SPC panel
Type	The type of wireless sensor detected (magnetic contact, inertia/shock, etc.).
Received	The date and time stamp of the last received signal from that sensor.
Status	The physical status of the sensor.
Receiver	The location of the wireless receiver that detected the signal from that wireless sensor.
Signal	The signal strength received from the sensor (01=low, 09=high). **Note:** If the signal strength is less than 3, the wireless sensor will not be displayed in the **Unenrolled Wireless Devices** list.

12.3 Changing wireless settings

1. Click the **Settings** tab to display Wireless Settings page.



2. See table below for further information.

Antenna	Select the type of antenna connected to the wireless module (internal or external) from the drop down menu. The type of antenna required for the wireless module depends on the type of wireless module fitted.
Supervision	Select whether a wireless sensor that is reported as missing registers a tamper condition on the signet panel. A wireless sensor is reported as missing when no supervision signal has been received from the sensor for a period greater than the programmed **Wireless Lost** timer. See page [→ 74].
Filter	Tick to filter low strength RF signals.
Detect RF Jam	Tick to activate an alert if RF interference is detected.
RF FOB SOS	Select how the SOS buttons on the RF Fob should operate.: ● Disable ● Enable ● Enabled Silent ● User Medic ● User Holdup ● RF Output
WPA Test Schedule	Enter a maximum period (in days) between WPA tests.
Prevent Setting Time	Enter a time in minutes after which, if the sensor fails to report, a setting is prevented for an area where the wireless zone is. This setting applies to the following intrusion zones only: ● Alarm ● Entry/Exit ● Exit Term ● Panic ● Hold up ● Tamper ● Lock Supervision ● Seismic

	• All OK • Setting Authorisation • Lock Element
Device Lost Time	Enter a number of minutes after which the wireless device (sensor or WPA) device is reported as lost.

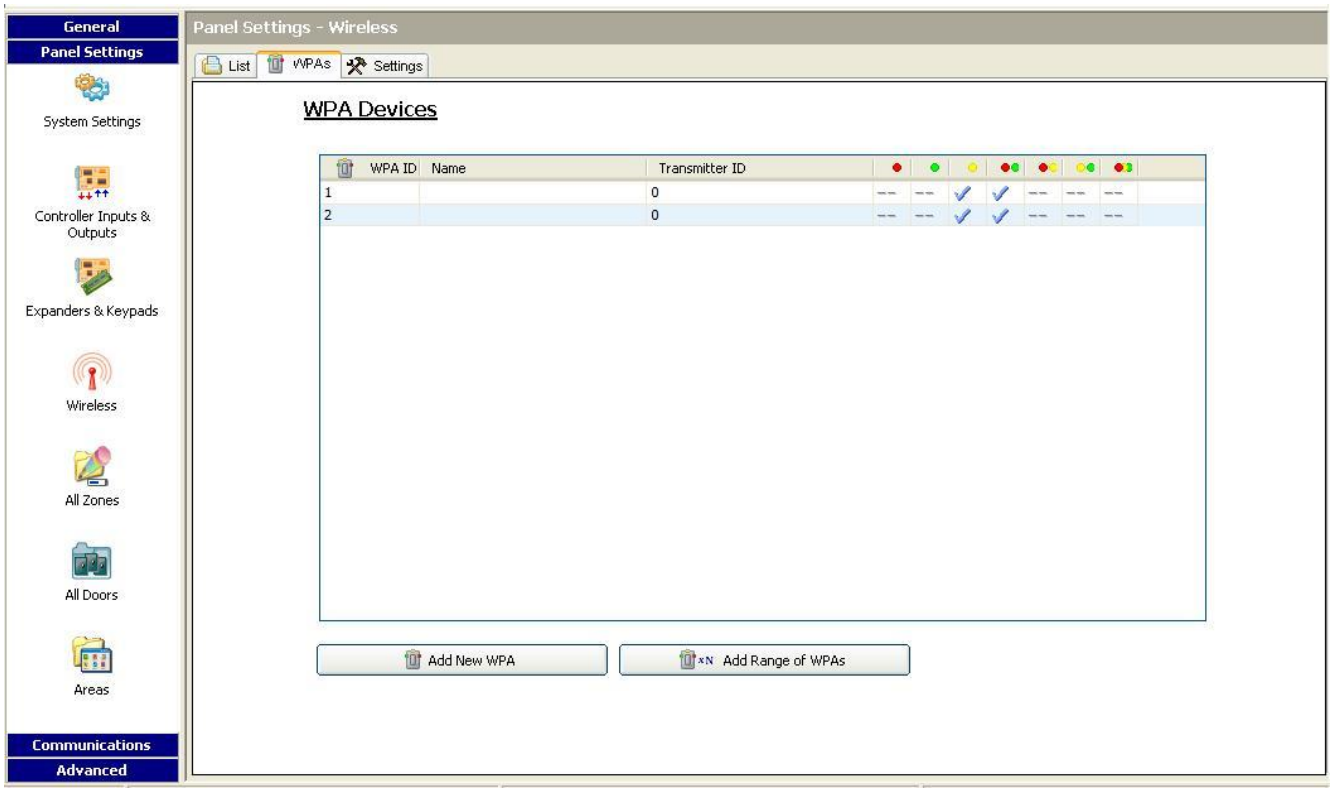
12.4 Configuring a WPA

	NOTICE
	The WPA configuration and status page is displayed only if there is a wireless module fitted on the panel or any of its expanders, and the panel is licensed for the type of module(s) fitted.

A WPA is not assigned to a user. Usually, a WPA is shared by several people, for example, security guards working in shifts or, alternatively, WPAs may be permanently attached to a surface such as under a desk or behind a till.

A maximum of 128 WPAs is allowed per panel.

To configure a WPA with SPC Pro, select **Settings/Wireless** and then the **WPA** tab.



All configured WPAs are listed with a corresponding ID. Any key combinations for the WPA are also indicated on this page.

Click on the **Add New WPA** to add and configure a WPA.

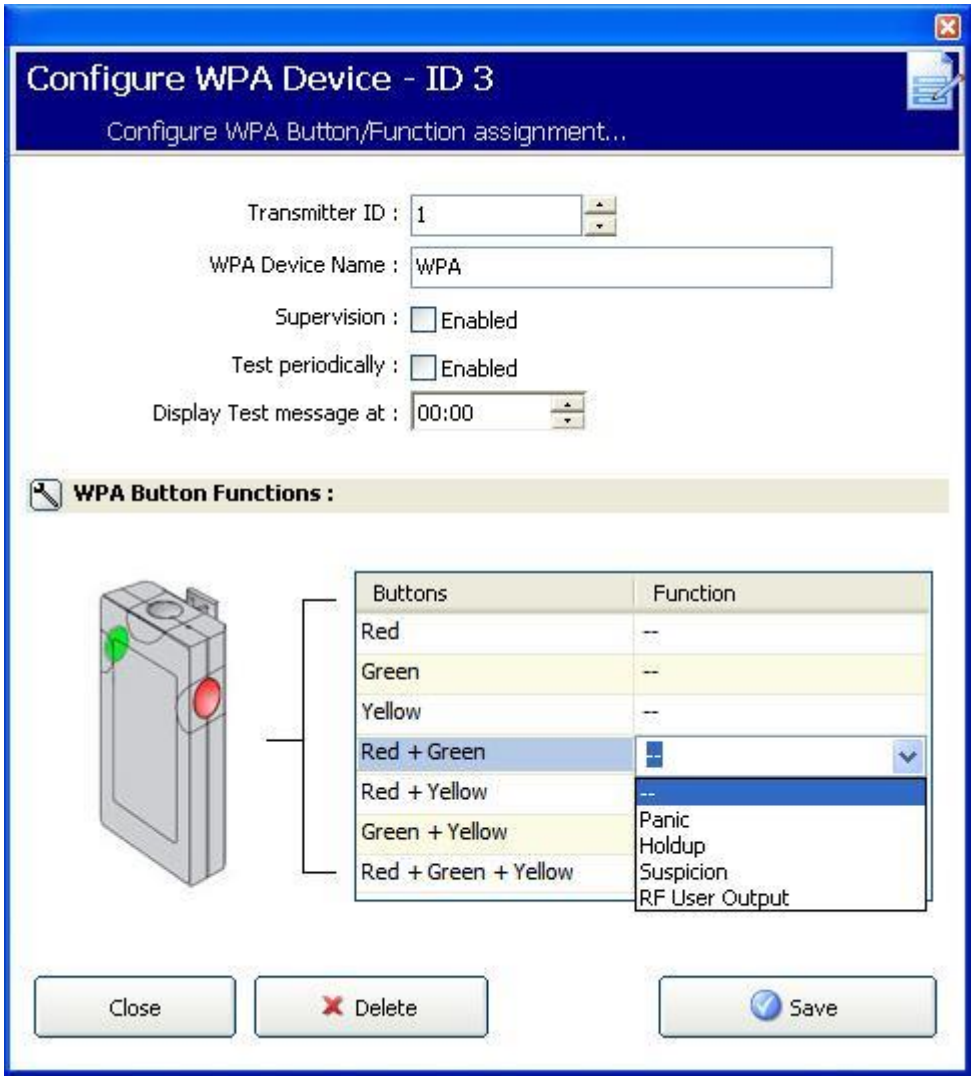
Click on the **Add Range of WPA** to add and configure a range of WPAs.

12.4.1 Adding a WPA

To add a WPA to the system:

- Click the **Add New WPA** button in the main WPA Devices page.

⇨ The Configure WPA Device page is displayed for the new WPA.



- Configure the WPA using the following details:

Description/Name	Enter a Description or Name to uniquely identity a WPA.
Transmitter ID	The transmitter ID is printed on the WPA casing and can be entered manually here. You can also identify the ID remotely by pressing any button on the WPA and then clicking the **Learn** button. The panel automatically enters this ID in this field providing no other WPA is currently defined with it
Supervise	The WPA may be configured to send periodic supervision signals. Supervision is enabled on the WPA with a jumper. The supervision function also needs to be enabled on the panel for the particular WPA for correct supervision operation. If the panel does not get a supervision signal, it raises an alarm that is shown in the keypad and logged. If supervision is not enabled, the WPA sends out a supervision message about every 24 hours to transmit the WPA battery status to the panel. This message is also randomized to decrease the chances of collision with other WPAs. Tick the **Supervise** box if supervision has been enabled for that particular

	WPA.
Test	Tick the **Test** box if a periodic WPA test is required. The timeframe for periodic testing is configured on the Changing wireless settings page.
Button Assignment	Use this section to assign functions to button combinations. Available functions are Panic, Panic silent, Holdup, Suspicion, RF User Output and Medical. More than one combination can be selected for the same function. The screen above shows the defaults for the panel for a Financial installation: ● Yellow - Suspicion ● Red + Green - Holdup For Commercial or Domestic installations, the default is: ● Red + Green - Panic **Note:** If no function is assigned to a button combination, it is still possible to use that combination by using a trigger. See Triggers

- Click on the **Save** button to save the settings.

See also

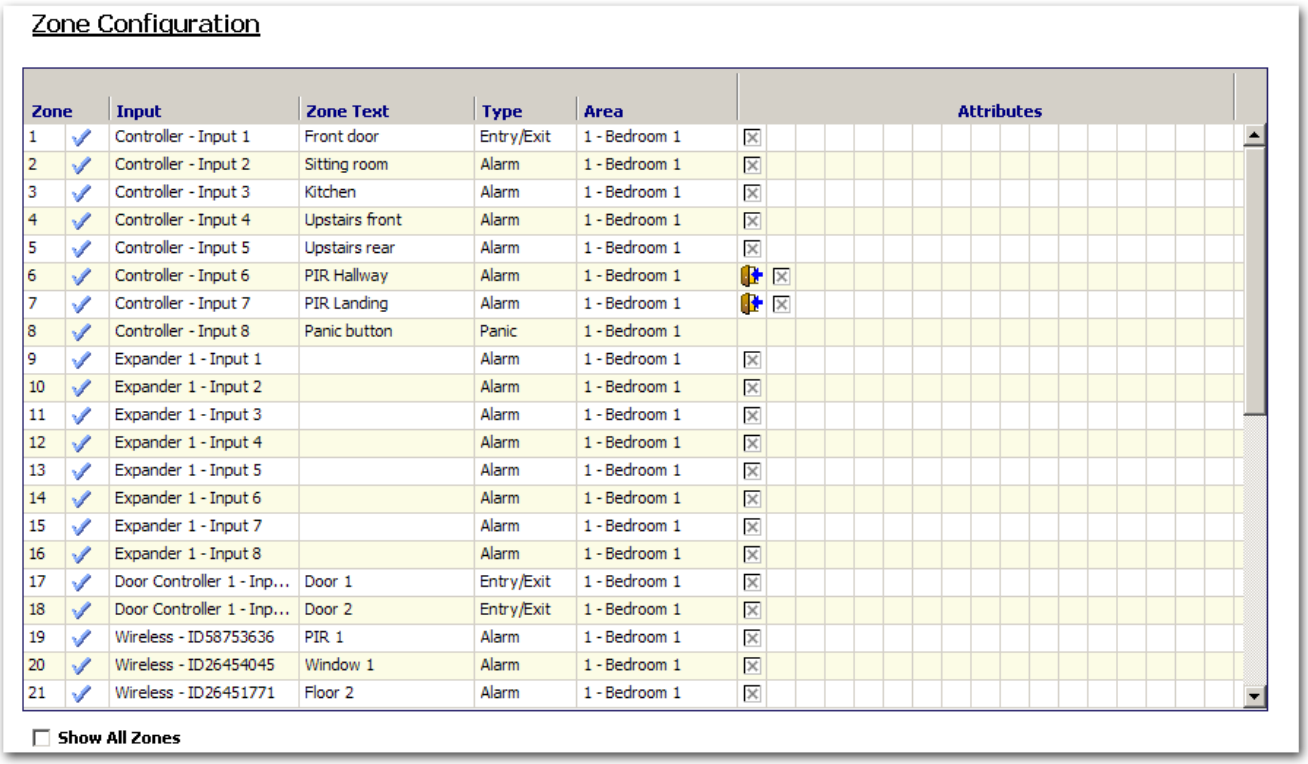
Changing wireless settings [→ 115]

13 Configuring zones, doors and areas

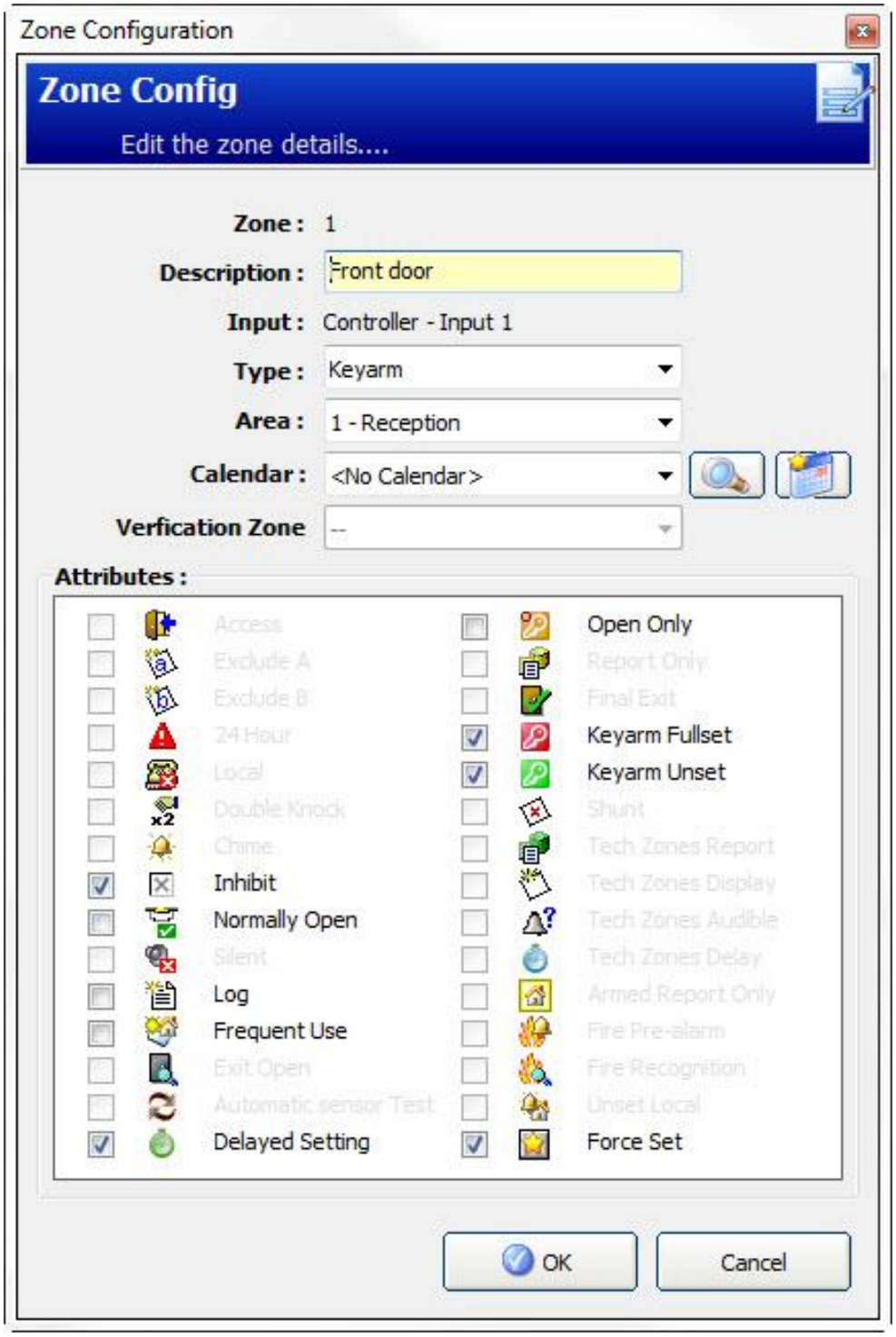
13.1 Editing a zone

Engineer and User actions include Log, Isolate/Deisolate and Soak/Desoak for each zone as allowable by the Security Grade EN 50131 Grade 2 and EN 50131 Grade 3.

1. Click the tab **List**.
   ⇨ The following window will be displayed:



2. Click a zone from the list.
   ⇨ The following window will be displayed.
3. Configure the fields as described in the table below.
4. Click **OK**.



Zone	The number is presented for reference and can not be programmed.
Zone Text	Enter a text (max. 16 characters) that serves to uniquely identify the zone.
Input	The physical input is displayed for reference and is not programmable.
Type	Select a type of zone from the drop down menu (see page [→ 260]).
Area	Only if (multiple) **Areas** is activated. Select an area to which the zone is assigned from the drop down menu.
Calendar ⓘ	Select if necessary the desired calendar (see page [→ 194]). For Security Grade 2 / 3 a calendar can be assigned only to zones of type Exit Terminator, Technical, Key Arm, Shunt and X-Shunt. For Security Grade Unrestricted a zone of any type can be associated with a calendar.

Attributes	Tick the relevant checkbox for the zone. Only attributes that apply that type of zone will be presented (see Zone Attributes [→ 262])

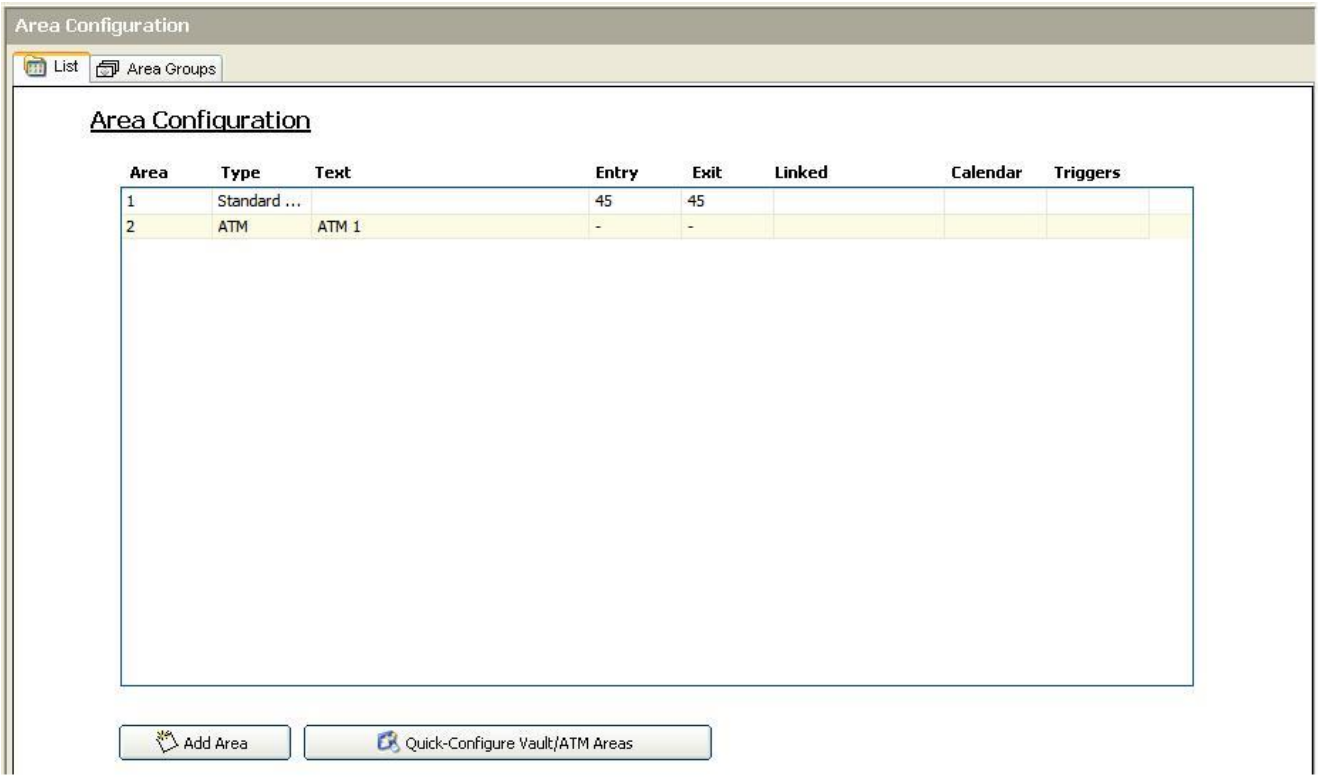
13.2 Adding / Editing an area

Panel Settings

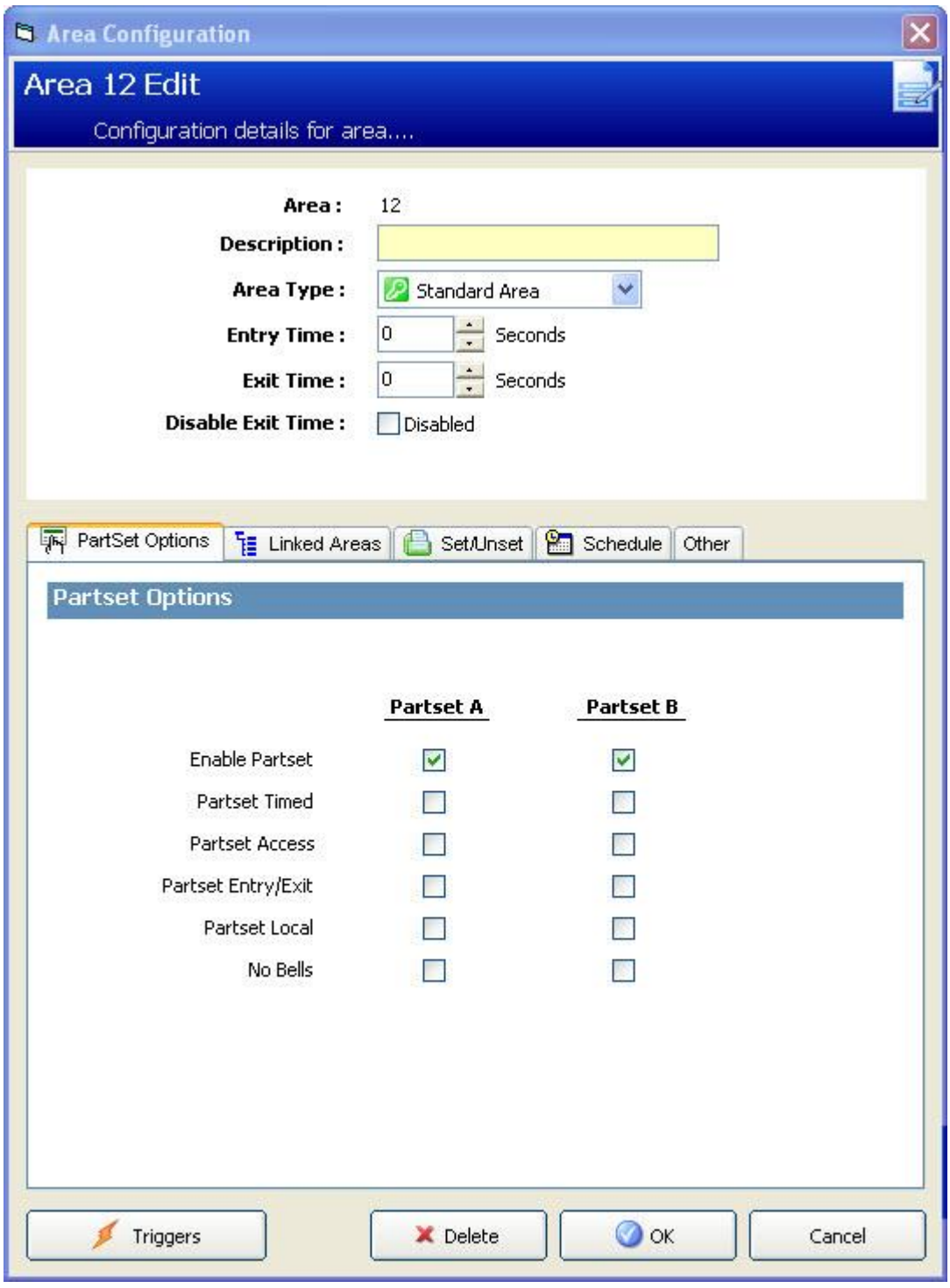
Areas

▷ Only if (multiple) **Areas** is activated.

1. Click the **List** tab.
   ⇨ The following window will be displayed:



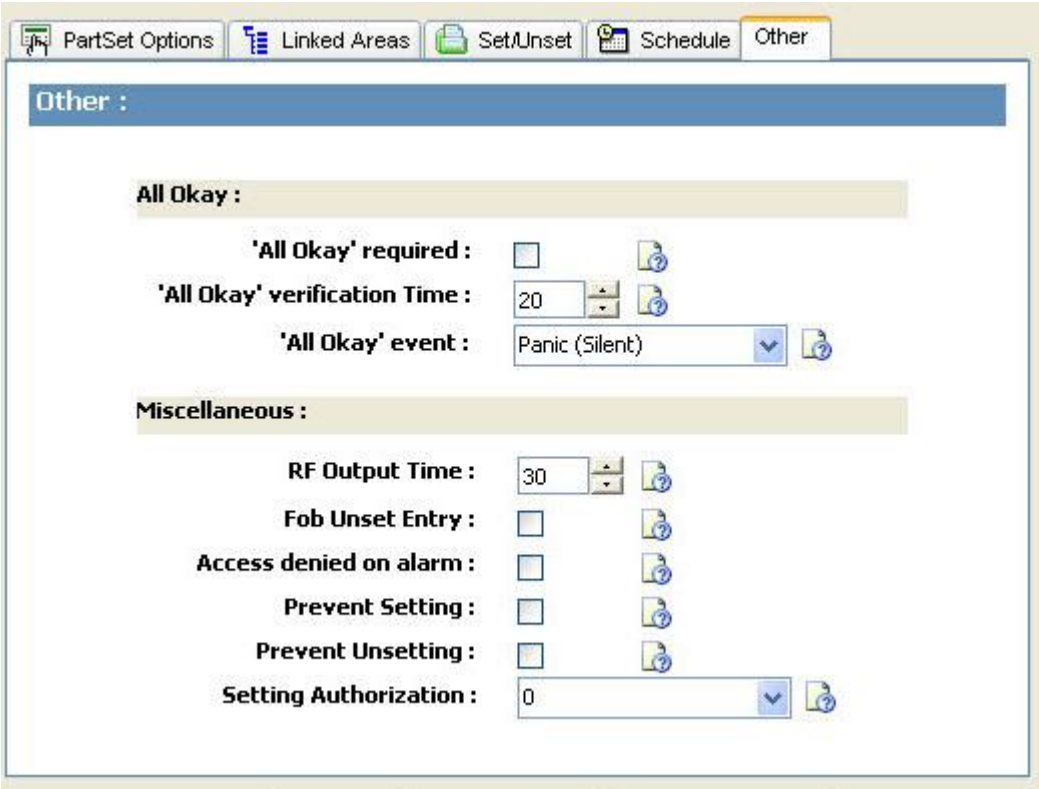
2. The Quick configure ATM/Vault areas [→ 137] button provides a shortcut to adding multiple ATM and Vault areas with default configuration settings.
3. Click on the **Add Area** button to add a single area or click an area from the list to edit.
   ⇨ The following window will be displayed.



4. Enter a unique description to identify the area.
5. Select the area type from one of the following:
   - Standard - Suitable for most areas.
   - ATM - Provides settings and defaults relevant to ATMs.
   - Vault - Provides settings and defaults relevant to vaults.
   - Advanced – Provides all area settings (Standard, ATM and Vault).

- Configure the settings for each installation type as per the following sections:

13.2.1 Entry/Exit

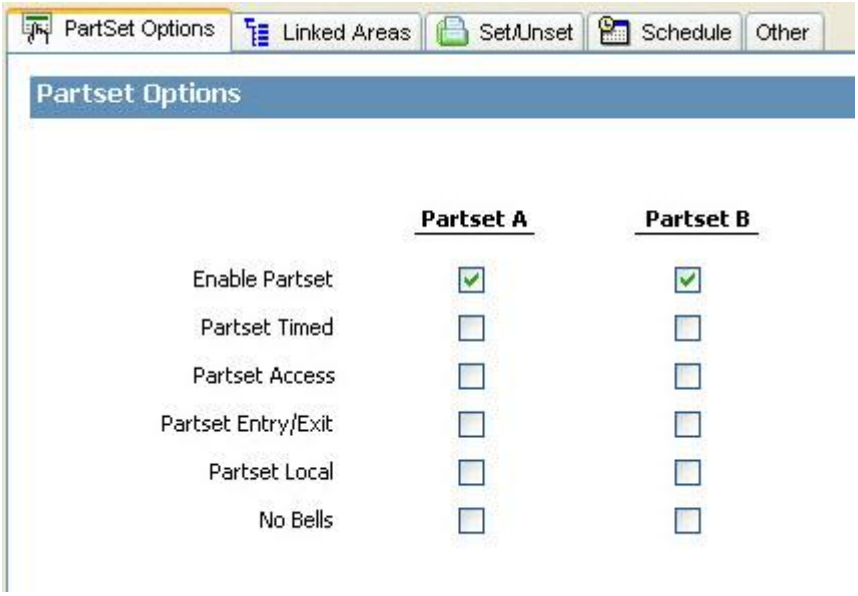


Configure the following Entry/Exit settings:

Entry time	The time period (in seconds) allowed for the user to UNSET the alarm after opening an entry/exit zone of an armed system. The entry time applies to all entry/exit zones in that area (default: 45 seconds).
Exit time	The time (in seconds) allowed for a user to leave a protected area before setting is complete. The exit time will be counted down at the keypad as the buzzer beeps to indicate to the user that the system will arm when the exit timer reaches zero. The exit time applies to all entry/exit zones in that area (default: 45 seconds).
Disable Exit Time	Select if no exit timer is required and setting is activated by 'Exit term' zone or 'Entry exit' zone with 'Final exit' attribute. See Timers [→ 74].
Fob Unset Entry	FOB will only unset when entry timer is running. Default is enabled.
Access Denied on Alarm	Access is temporarily denied to the area for the amount of time specified in the Lockout Post Alarm timer.
Prevent Setting	If enabled, setting prevented from keypad
Prevent Unsetting	If enabled, unsetting prevented from the keypad.
Setting Authorisation	Used for configuring Blocking Lock operation. Options are: ● Disabled ● Set ● Unset ● Set and Unset If the Disabled option is selected (default) then the system will set and unset normally with no change of operation. If the Set option is selected, a "Setting Authorisation" signal is required to set this area which can be received from keypads or a zone input (see Authorised Setting of the Blocking Lock) The user cannot set the system from the keypad. Any area that requires setting authorisation will appear as locked on the comfort keypad and will not appear on the

	standard keypad when setting. If the Unset option is selected, the user cannot unset the area from keypads but can use the keypad to generate the setting authorization signal. For the set and unset options, the user will be unable to change the state of the area at any stage from the keypad. A timer for setting authorisation can be configured. See Timers [→ 74].

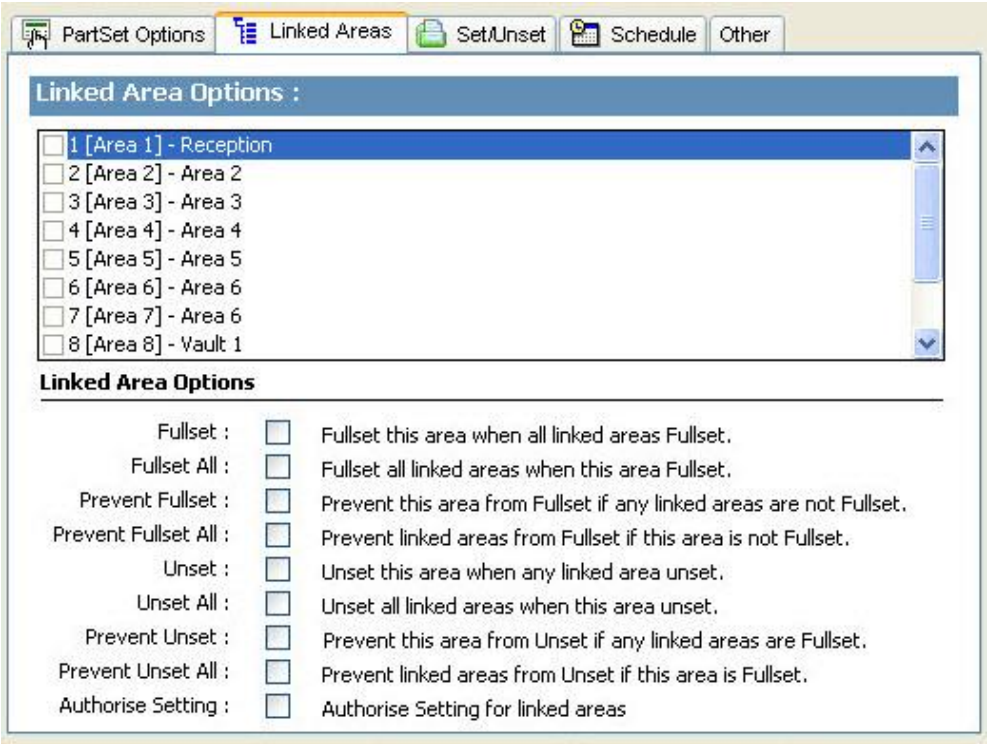
13.2.2 Partset Options



Configure the operation of particular zones for both Partset A and Partset B modes as detailed below:

Partset Enable	Enable PartSet for A and B operation as required.
Partset Timed:	Tick the relevant checkbox (Partset A or B) to apply the exit timer to the Partset A or B mode.
Partset Access:	Tick the relevant checkbox to change access zones into entry/exit type zones for either Partset A or B operation. This feature is useful for a domestic installation where a Passive Infrared (PIR) sensor is located in the hallway. If the user partsets the system at night and returns downstairs during the night, he/she may unintentionally activate the PIR sensor in the hallway and trigger the alarm. By setting the partset access option, the buzzer will sound for the entry time period when the PIR sensor is activated thereby warning the user that the alarm will activate if no action is taken.
Partset Exit/Entry:	Tick the relevant checkbox to change the behaviour of entry/exit zones to alarm zones when in Partset A or B mode. This feature is useful for a domestic installation when the system has been set in partset mode. If the user partsets the system at night he/she may wish the alarm to activate immediately if the front or back door is opened during the night.
Partset Local:	Tick the relevant checkbox to restrict the reporting of alarms in Partset Mode to local reporting only (No remote reporting).
No Bells	If ticked, no bells will be activated for partset A or B.

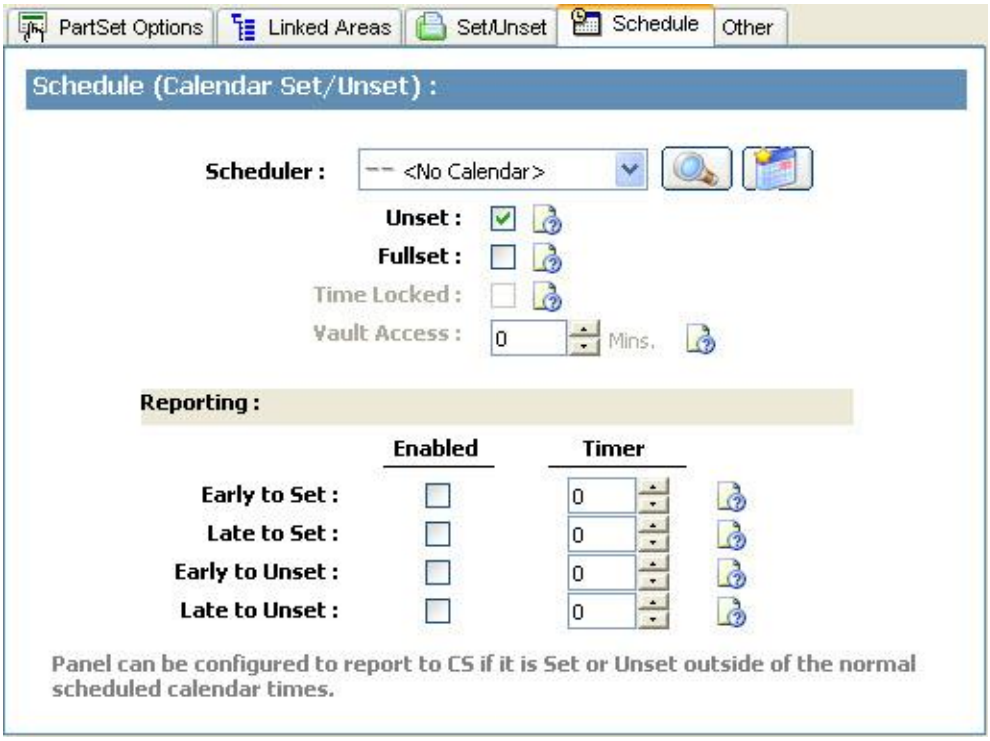
13.2.3 Linked Areas



This section enables you to link areas for setting and unsetting purposes:

Fullset	Fullset this area when all linked areas are Fullset.
Fullset All	Fullset all areas when this area is Fullset.
Prevent Fullset	Prevent this area from Fullset if all linked areas are Fullset.
Prevent Fullset All	Prevent linked areas from Fullset if this area is not Fullset.
Unset	Unset this area when all linked areas are Unset.
Unset All	Unset all areas when this area is Unset.
Prevent Unset	Prevent this area from Unset if any linked areas are Fullset.
Prevent Unset All	Prevent linked areas from Unset if this area is Fullset.
Authorise Setting	Enable authorised setting for linked areas. Refer Authorised Setting of the Blocking Lock.
Linked Areas	Click on the areas that you wish to link to this area.

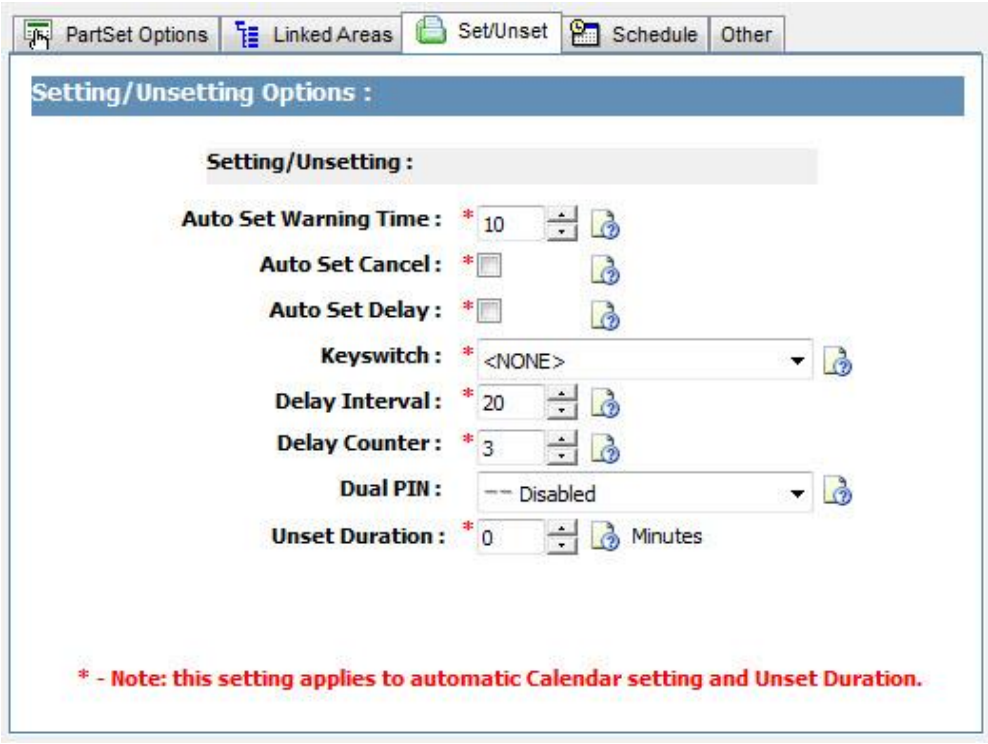
13.2.4 Schedule



Configure scheduling with the following settings:

Calendar	Select a calendar to control scheduling.
Unset	Select if area should automatically Unset as per the time specified in the selected calendar.
Fullset	Select this option to Fullset the area as per the time specified in the selected Calendar. The area will also set when the Unset Duration or Delay Interval has elapsed (See Setting and Unsetting [→ 128] section). If the Unset Duration overlaps the scheduled time, the area will use the calendar settings.
Time Locked	Select this option to time lock the area as per the selected Calendar. (Vault type area in Financial mode only)
Vault Access	Enter the number of minutes (0 – 120) to activate this timer at the end of a Time Locked Unset period. If the area is not unset after this timer expires, the area cannot be unset until the start of the next Time Locked Unset period. (Vault type area in Financial mode only)

13.2.5 Setting/Unsetting



The following parameters (with the exception of the Interlock parameter) are only relevant in the following cases:

- A Calendar is selected (see Schedule [→ 127]), or
- **Unset Duration** is enabled (has a value greater than zero), or
- Both of the above conditions are met.

Auto Set Warning	Enter the number of minutes to display a warning before Auto Setting. (0 - 30) Note that the panel sets either at the scheduled time or at the time defined by the Delay Unset parameter. The first warning is displayed at the configured time before the scheduled time. There are further warnings starting at one minute before setting time.
Auto Set Cancel	Enables the user to cancel Auto Setting by entering a code in the keypad.
Auto Set Delay	Enables a user to delay Auto Setting by entering a code in the keypad.
Keyswitch	Enables Auto Setting to be delayed using Keyswitch Expander.
Delay Interval	Enter the number of minutes by which to delay Auto Set. (1 - 300)
Delay Counter	Enter the number of times that Auto Setting can be delayed. (0 – 99: 0 = unlimited)
Delay Unset	Enter the number of minutes by which to delay an Unset. (0 = no delay)
Interlock Group	Select an Interlock Group to assign to this area. Interlocking only allows one area within the group to be Unset at any time. Typically used in ATM areas.

Unset Duration	If area is Unset for longer than this it will Set automatically. (Range 0 – 120 mins: 0 = not active).
Dual PIN	If this option is enabled, two PINs are required to Set or Unset the area with the keypad. Both PINs must belong to users who have the required user right for the operation (Setting or Unsetting). If the second PIN is not entered within 30 seconds, or it is wrong, then the area cannot be Set or Unset.

Late Working Support

An example of using the setting and unsetting parameters is for late working situations where a calendar has been configured for automatic setting of a premises at a particular time but staff may need to work late on occasion and the automatic setting needs to be delayed.

Each delay is determined by the amount configured in the **Delay Interval** parameter, and the **Delay Counter** parameter determines the number of times that setting can be delayed. A user needs the correct value in the **Auto Set Delay** in order to use this feature.

There are three ways to delay setting:

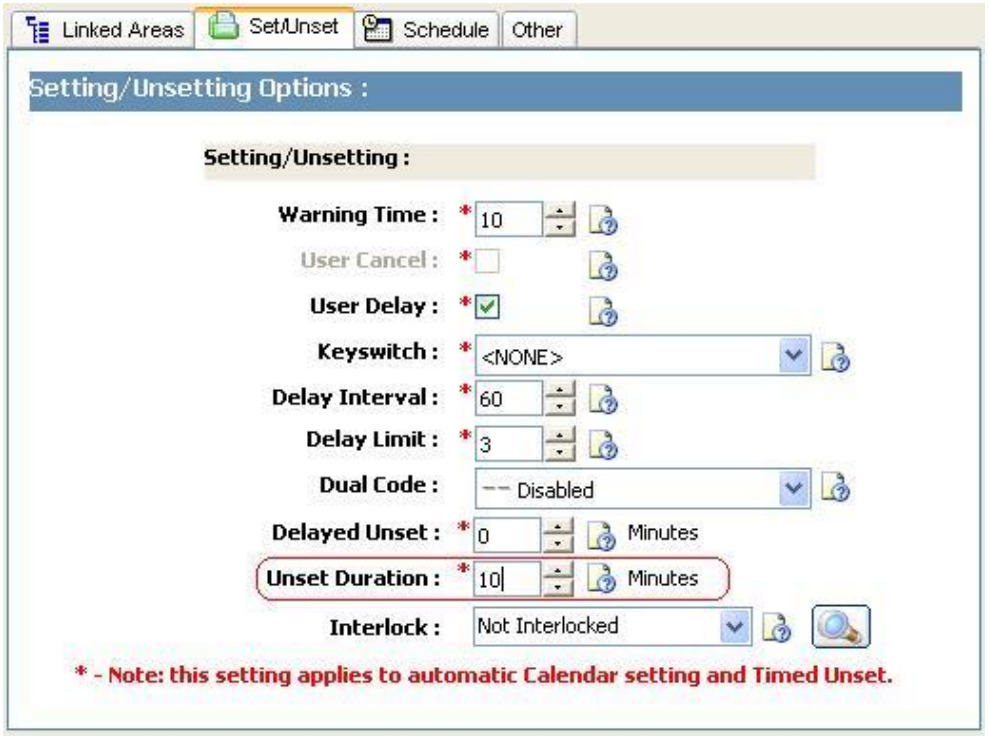
1. Entering the PIN on the keypad.
   DELAY is a menu option on the standard keypad. The buttons at the top of the comfort keypad are used to operate the delay feature
2. Using the keyswitch.
   Turning the key to the right delays setting the system by the configured delay if the maximum number of times that setting can be delayed (**Delay Counter**) has not been exceeded. Turning the key to the left sets the delay to three minutes (non-configurable). This can be done regardless of how many times setting was delayed.
3. Using a FOB, WPA or button which activates a **Delay Autoset** trigger action. (See page 172)

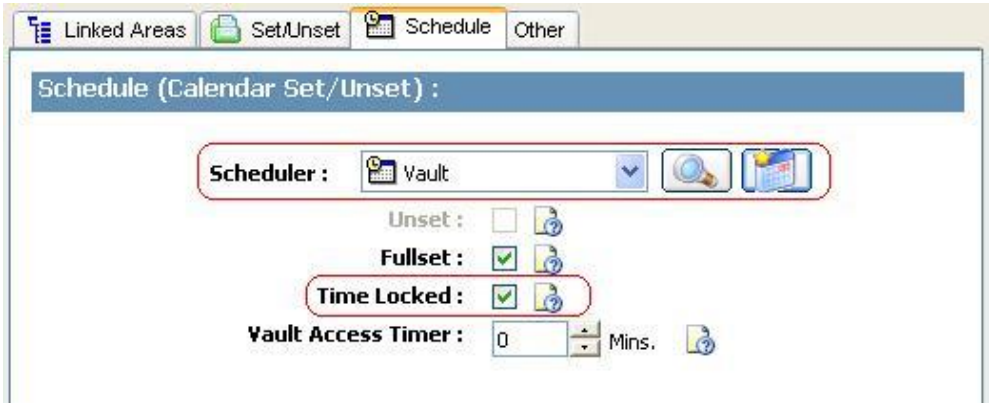
Temporary Unset

To allow a system to be temporarily unset in a time period specified by a calendar, the following three parameters need to be configured:

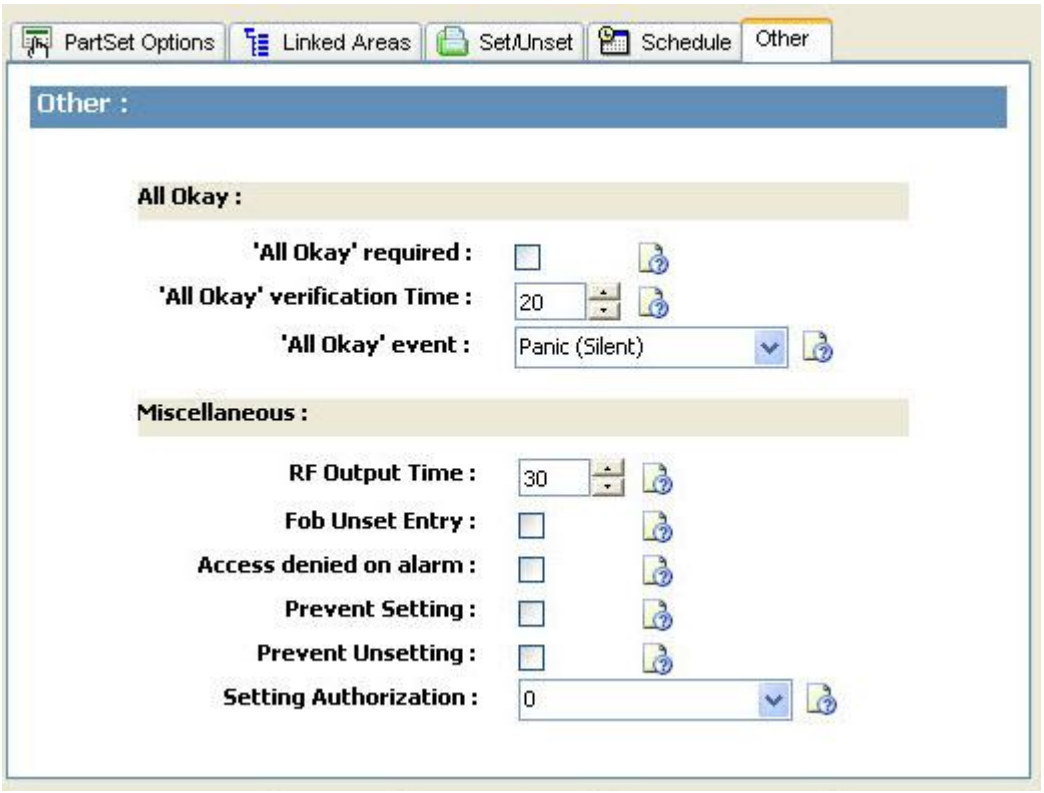
1. **Calendar**
   A calendar needs to be configured and selected for this area.
2. **Time Locked**
   This box needs to be ticked so that the area can be unset only when allowed as per the configured calendar.
3. **Unset Duration**
   This parameter needs to be set to a value greater than zero to set an upper limit on the time the area will be unset.

The following screen shows these parameters configured with appropriate settings:


Linked Areas
Set/Unset
Schedule
Other
Setting/Unsetting Options :
Setting/Unsetting :
Warning Time : * 10
User Cancel : *
User Delay : *
Keyswitch : * <NONE>
Delay Interval : * 60
Delay Limit : * 3
Dual Code : -- Disabled
Delayed Unset : * 0 Minutes
Unset Duration : * 10 Minutes
Interlock : Not Interlocked
* - Note: this setting applies to automatic Calendar setting and Timed Unset.

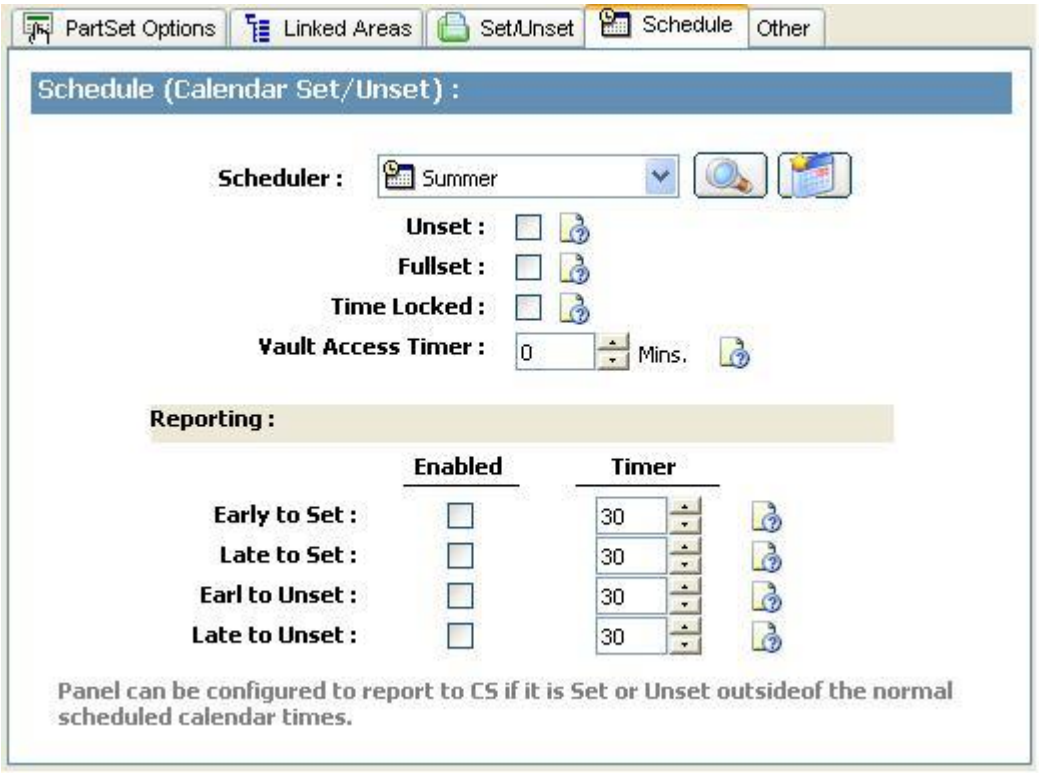

Linked Areas
Set/Unset
Schedule
Other
Schedule (Calendar Set/Unset) :
Scheduler : Vault
Unset :
Fullset :
Time Locked :
Vault Access Timer : 0 Mins.

13.2.6 All Okay



All Okay Required	If selected, user must confirm 'All okay' input or silent alarm is generated. See Editing a Zone [→ 120] for details on configuring an 'All Okay' zone input.
All Okay Time	Time (in seconds) in which 'All okay' must be confirmed before alarm is raised. (Range 1 – 999 seconds)
All Okay Event	Select the event type to be sent when the 'All okay' timer expires. Options are Panic (Silent), Panic and Duress.

13.2.7 Reporting



The Reporting configuration settings are applicable for Standard Areas in Commercial and Financial installations only and are only relevant if a calendar has been selected. (See Schedule [→ 127] section)

These settings enable a report to be sent to the Control Centre or nominated personnel if the panel is Set or Unset outside scheduled calendar times.

Early to Set	Enables a report to be sent if the panel is manually Fullset before a scheduled Set and before the number of minutes entered in the Timer field.
Late to Set	Enables a report to be sent if the panel is manually Fullset after a scheduled Set and after the number of minutes entered in the Timer field.
Early to Unset	Enables a report to be sent if the panel is manually Unset before a scheduled Unset and before the number of minutes entered in the Timer field.
Late to Unset	Enables a report to be sent if the panel is manually Unset before a scheduled Unset and before the number of minutes entered in the Timer field.

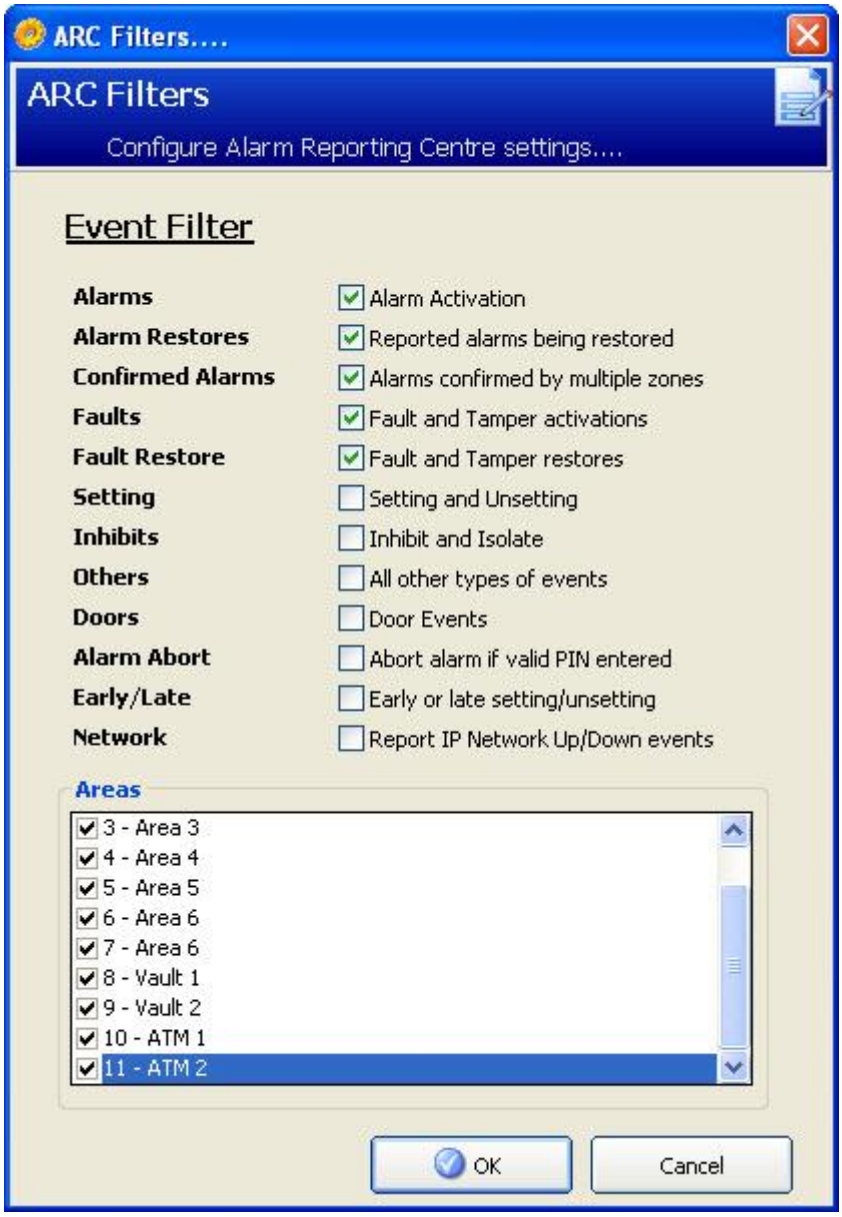
Reporting is done via SMS or to the ARC via SIA and Contact ID. An event is also stored in the system log.

Only events configured for late or early reporting for the area will be reported.

Event reporting must also be enabled for an ARC or SMS, as described in the following sections.

Enabling Reporting of Unusual Setting/Unsetting for an ARC

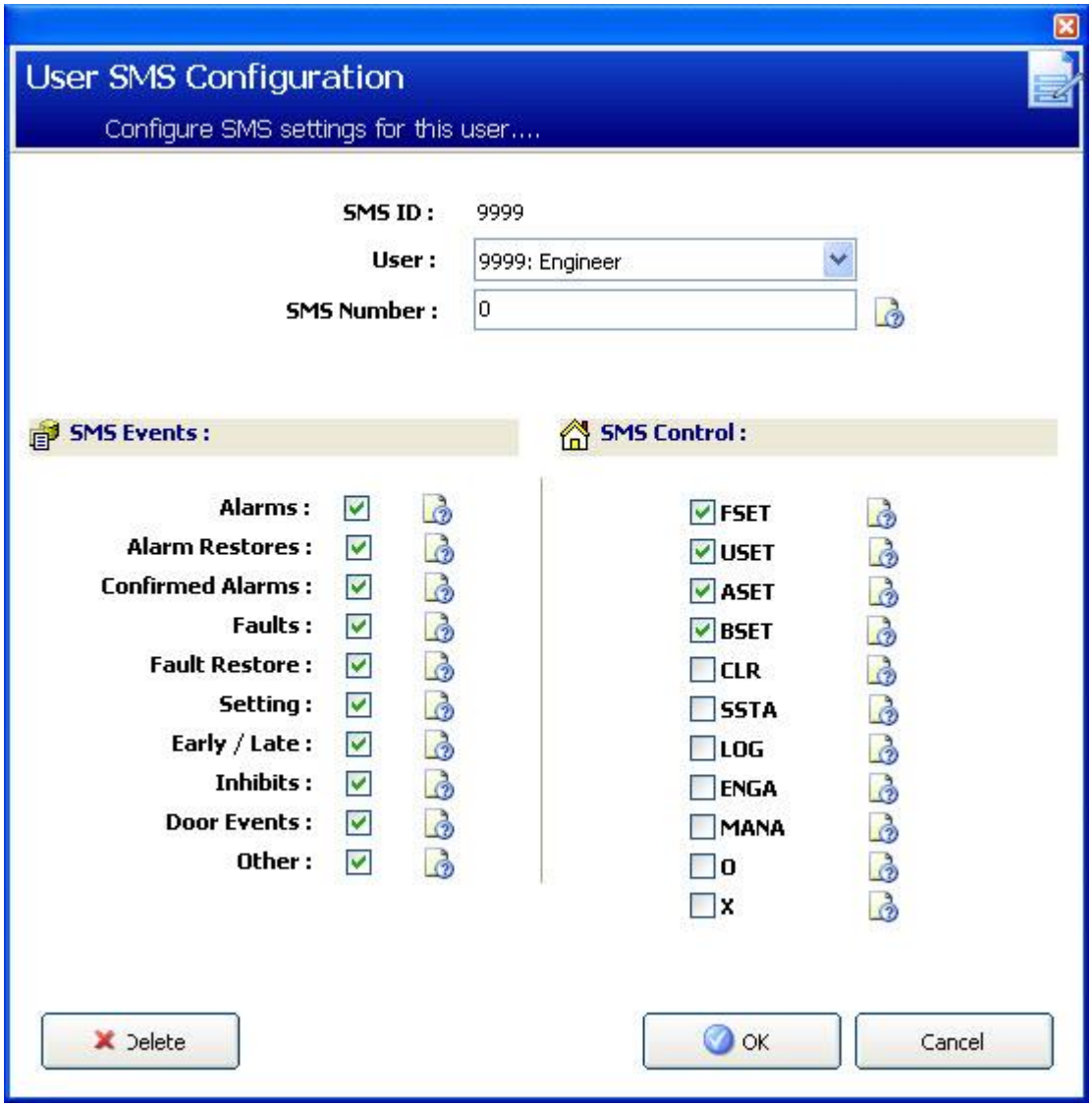
To configure event reporting for an ARC, select **Communications>ARC** to display the ARC Filters page.



The **Early or late setting/unsetting parameter** is enabled to report any setting or unsetting which differs from the schedule.

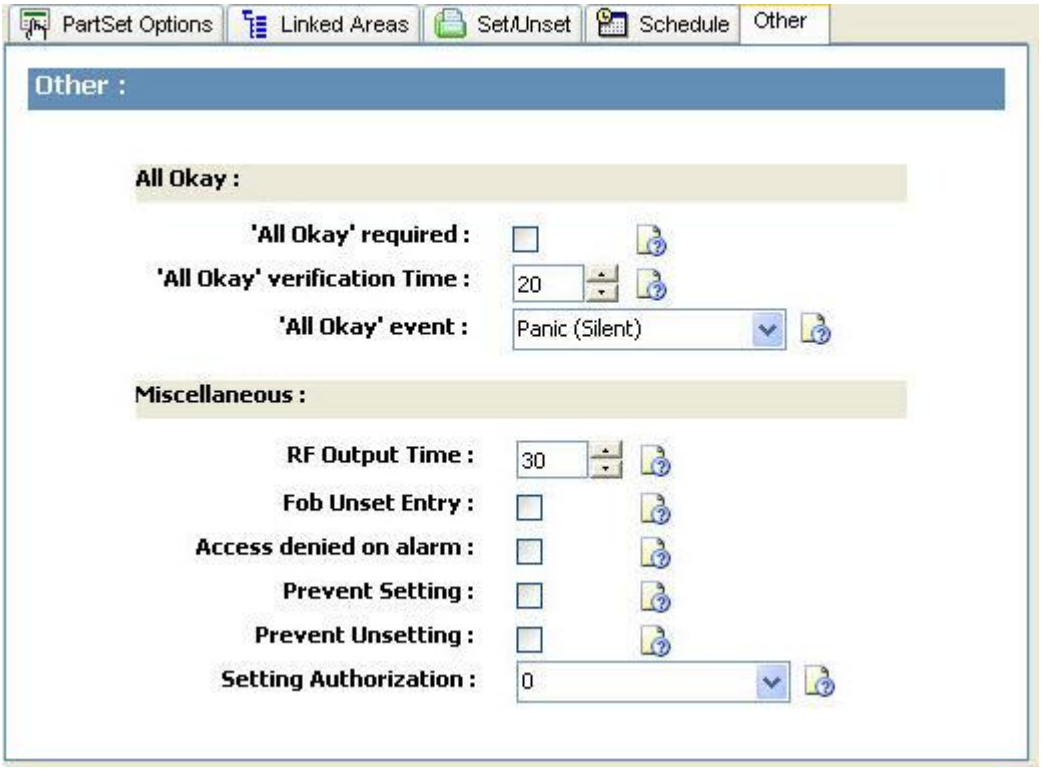
Enable Reporting of Unusual Setting/Unsetting for SMS

For Engineer configuration, select **General>Setup Users:**



Enable Early/Late to report any setting and unsetting which is not according to schedule.

13.2.8 RF Output



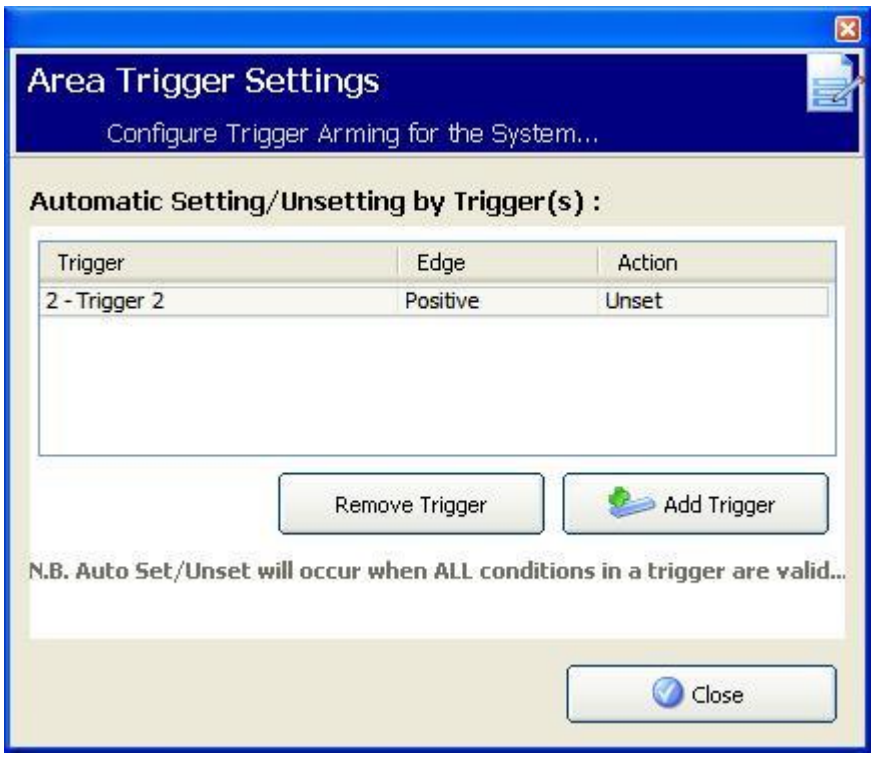
RF Output Time	Enter the number of seconds that the RF Output will remain on for. 0 seconds will toggle the output on and off.

The other Miscellaneous options are described in Entry/Exit [→ 124] for SPC Pro

13.2.9 Area Triggers

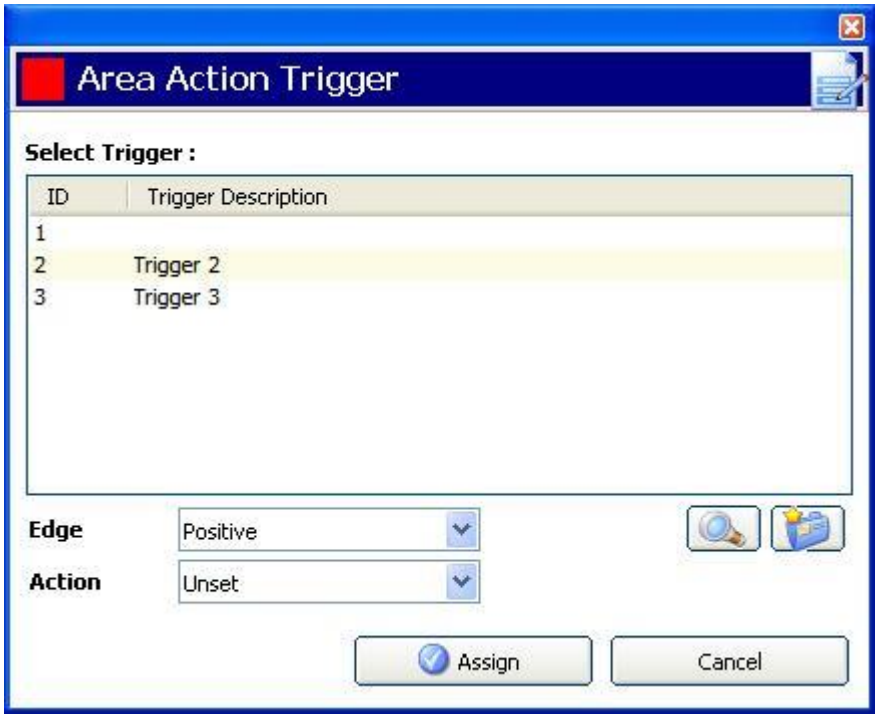
- Click on the **Triggers** button in the Area Configuration page to configure triggers for this area.

⇨ The Area Trigger Settings page is displayed.



1. Click on a trigger to edit conditions for that trigger.
2. Click on the **Add** button to add a new trigger for the area.

⇨ The Area Action Trigger page is displayed.



Select a trigger and click on the **Assign** button to assign the trigger to the area.

New triggers can be added to the system or existing triggers can be viewed or edited using the following buttons:

	Add a new trigger to the list.

	View or edit a trigger on the list.

Configure the trigger for the area using the following parameters:

Trigger	Select a trigger from the drop down list.
Edge	The trigger can activate from either the positive or negative edge of the activation signal.
Action	This is the action that is performed when the trigger is activated. Options are: ● Unset ● Partset A ● Partset B ● Fullset ● Delay autoset This action will delay alarm setting when the autoset timer is running. The trigger will only add time if the Delay Limit has not been exceeded and each trigger activation will delay setting by the time defined in Delay Interval (see section Setting/Unsetting [→ 128]. ● Restore alarms This action will clear all alarms in the configured zone.

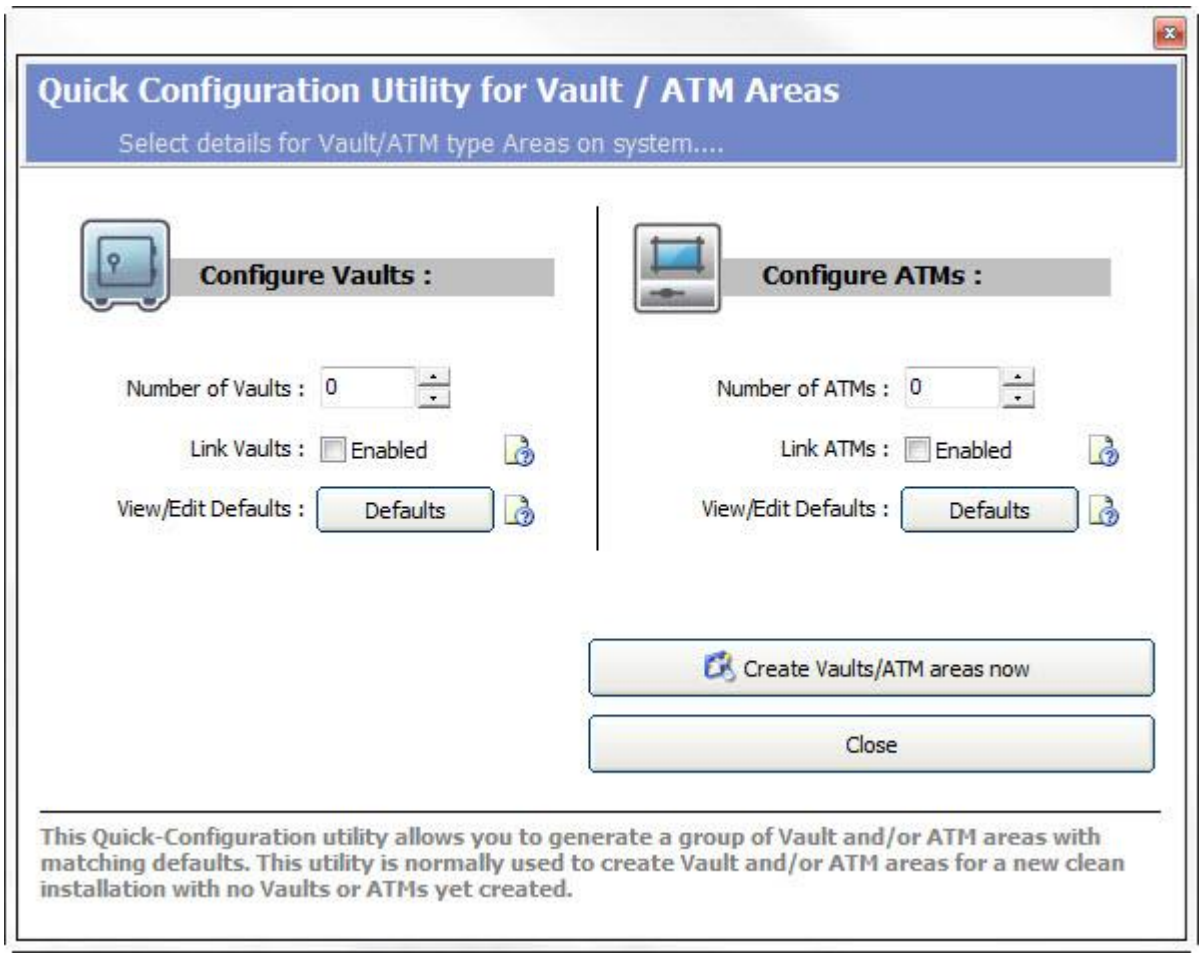
Note: Triggers cannot be configured from a keypad.

See also

Triggers [→ 197]

13.2.10 Quick configure ATM/Vault areas

When you click on the **Quick Configure ATM/vault Areas** button, the following page is displayed:



For both Vault and ATM areas:

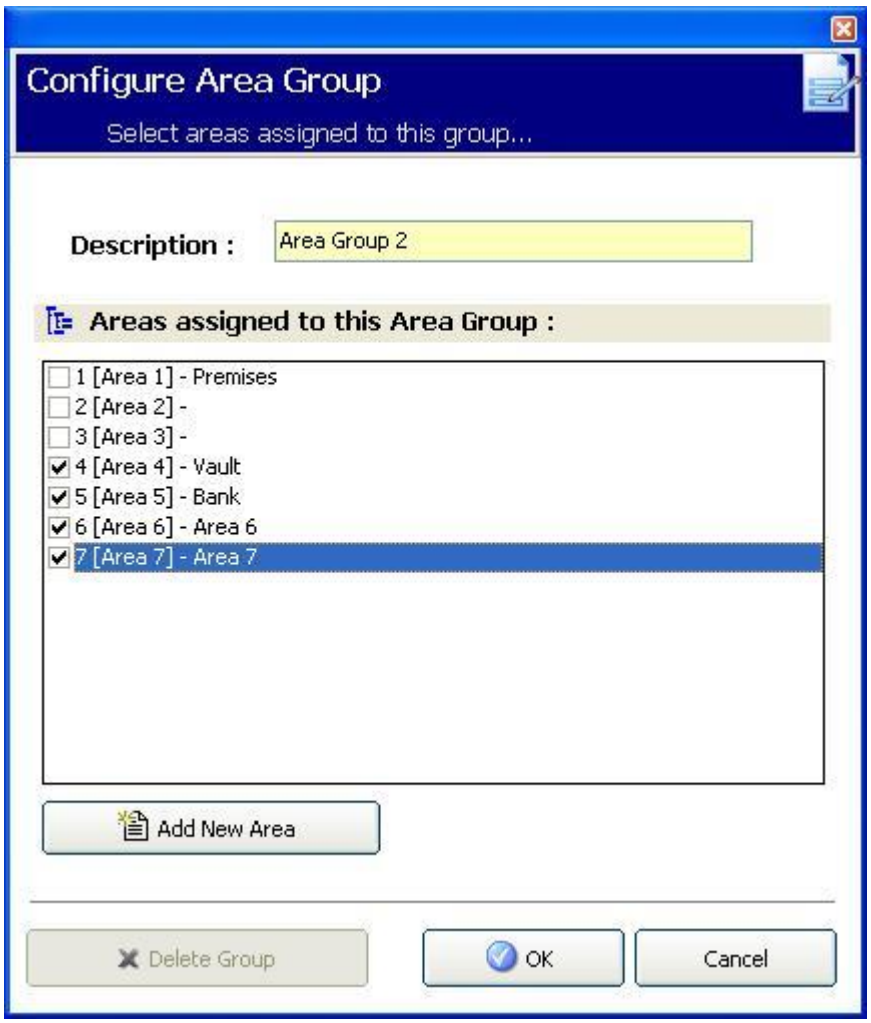
1. Enter the number of Vaults/ATM areas to be configured.
2. Tick the **Link Vaults/ATMs** check box if you want all the Vault or ATM areas to be linked.
3. Click on the **Defaults** button if you want to edit the existing defaults configured for Vault/ATM areas. (See Adding/Editing an area [→ 122] for details of area configuration)
4. Click on the **Create Vault/ATM areas now** button to create the specified number of Vault/ATM areas.

13.3 Adding an area group

You can use area groups for configuring multiple areas. So the configuration must not be done for every single area.

▷ Only if the option (multiple) **Areas** is activated.

1. Select the **Area Groups** tab.
2. Click the **Add Area Group** button.



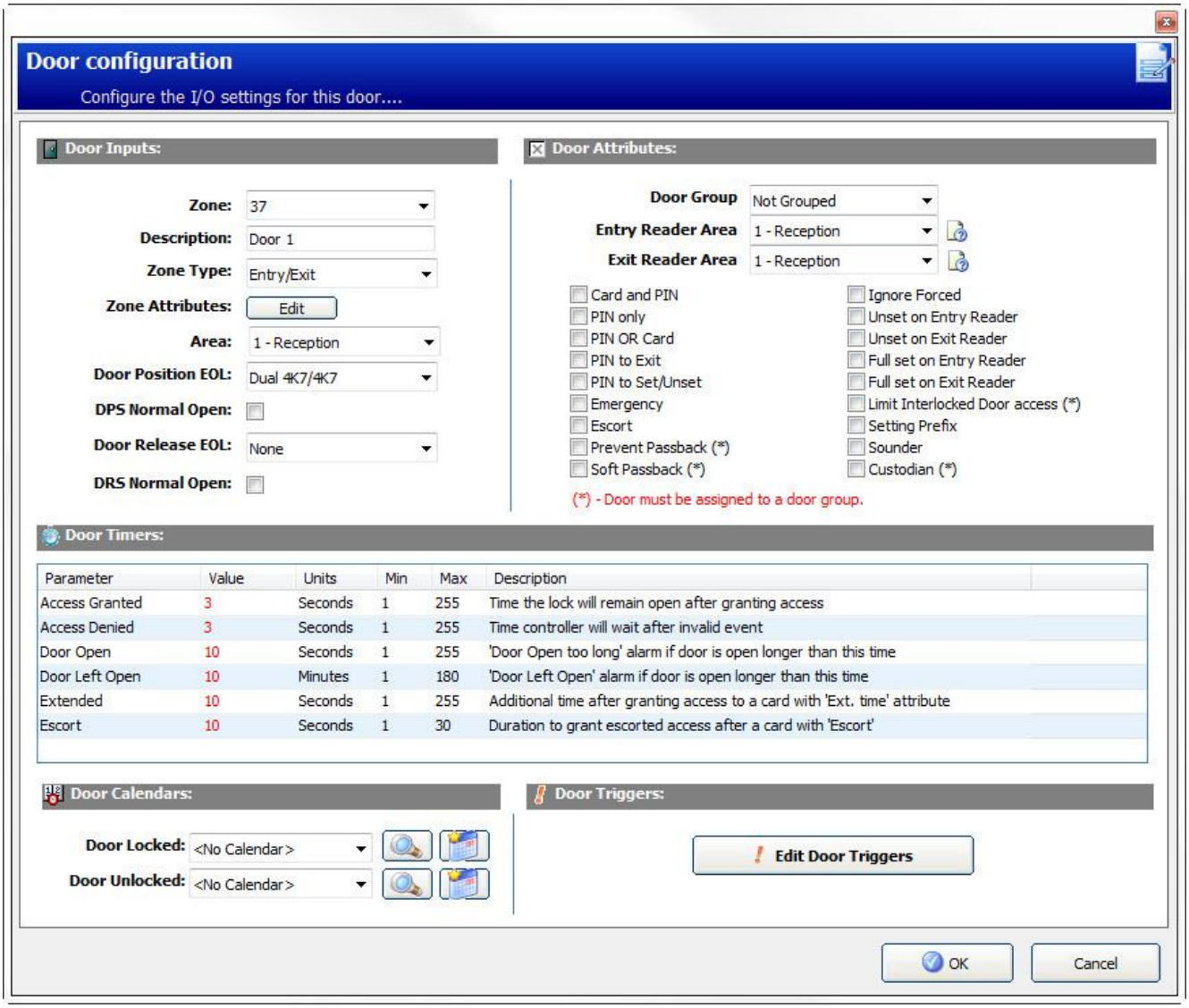
1. Enter a description for the group.
2. Select the areas that are to be assigned to this group.
3. Click **OK**.
4. Click **Add New Area** to configure a new area to add to the group.

	NOTICE
	To use the area groups for the Comfort Keypad, activate all Areas in the **Areas** tab under **Panel Settings > Expanders & Keypads > Keypads > Type: Comfort Keypad**.

13.4 Editing a door

All Doors

1. Click the tab **List**.
2. Click a door from the list.



3. Configure the fields as described in the tables below.
4. Click **OK**.

Door inputs

Each door has 2 inputs with predefined functionality. These two inputs, the door position sensor and the door release switch can be configured.

Name	Description
Zone	The door position sensor input can be used for the intrusion part as well. If the door position sensor input is used also for the intrusion part, the zone number it is assigned to has to be selected. If the door position sensor is used only for the access part, the option “UNASSIGNED” has to be selected. If the door position sensor is assigned to an intrusion zone, it can be configured like a normal zone but only with limited functionality (e.g. not all zone types are selectable). If an area or the system is set with the card reader, the

Name	Description
	door position sensor input has to be assigned to a zone number and to the area or the system which have to be set.
Description (Web and SPC Pro only)	Description of the zone the door position sensor is assigned to.
Zone Type (Web and SPC Pro only)	Zone type of the zone the door position sensor is assigned to (not all zones types are available).
Zone attributes (Web and SPC Pro only)	The attributes for the zone the door position sensor is assigned to can be modified.
Area (Web and SPC Pro only)	The area the zone and the card reader are assigned to. (If the card reader is used for setting & unsetting, this area will be set / unset).
Door Position (Web) DPS End Of Line (keypads) Door Position EOL (SPC Pro)	The resistor used with the door position sensor. Choose the used resistor value / combination.
DPS Normal Open	Select if the door release switch is to be a normally open or normally closed input.
Door Release (Web) DRS END OF LINE (Keypads) Door Position EOL (SPC Pro)	The resistor used with the door release switch. Choose the used resistor value / combination.
DRS Normal Open	Select if the door release switch is a normally open input or not.
No DRS (Web and SPC Pro only)	Select to ignore DRS. If a DC2 is used on the door, this option MUST be selected. If not selected, the door will open.
Reader Location (Entry/Exit) (Web and SPC Pro only)	Select the location of the entry and exit readers.
Reader formats (Web) READER INFO (Keypads)	Displays format of last card used with each configured reader. (not available in SPC Pro)

Each free zone number can be assigned to the zones but the assignment is not fixed. If the number ‘9’ is assigned to a zone, the zone and an input expander with the address ‘1’ is connected to the X-Bus (which is using the zone numbers 9-16). The assigned zone from the two door controller will be moved to the next free zone number. Configuration will be adapted accordingly.

Door attributes

If no attribute is activated, a valid card can be used.

Attribute	Description
Void	The card is temporarily blocked.
Door Group	Used when multiple doors are assigned to the same area and/or anti passback, custodian, or interlock functionality is required.
Card and PIN	Card and PIN are required to gain entry.

Attribute	Description
PIN Only	PIN is required. No card will be accepted.
PIN Code or Card	PIN or card are required to gain entry
PIN to Exit	PIN is required on exit reader. Door with entry and exit reader is required.
PIN to Set/Unset	PIN is required to set and unset the linked area. The card has to be presented before the PIN is entered.
Unset outside (Browser) Unset on Entry Reader (SPCPro)	Panel/area will unset, when card is presented at entry reader.
Unset inside (Browser) Unset on Exit Reader (SPCPro)	Panel/area will unset, when card is presented at exit reader.
Bypass alarm	Access is granted if an area is set and the door is an alarm or an entry zone type.
Fullset outside (Browser) Fullset on Entry Reader (SPCPro)	Panel/area will fullest, when card is presented twice at entry reader.
Fullset inside Full set on Exit Reader (SPCPro)	Panel/area will fullest, when card is presented twice at exit reader.
Force Fullset	If the user has rights, they can force set from entry reader.
Emergency	Door lock opens if a fire alarm is detected within the assigned area.
Emergency any	Fire in any area will unlock the door.
Escort	The escort feature enforces privileged card holders to escort other card holders through specific doors. If this feature is assigned to a door, a card with the “escort right” has to be presented first, to allow other cardholders without this right to open the door. The time period in which cardholders are able to present their cards after a card with escort right was presented, can be configured per door.
Prevent Passback*	Anti-passback should be enforced on the door. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry into and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a hard Anti-Passback alarm will be raised and the cardholder will not be permitted entry to the door group.
Soft Passback*	Anti-passback violations are only logged. All doors must have entry and exit readers and must be assigned to a door group. In this mode, cardholders must use their access card to gain entry to and exit from a defined door group. If a valid cardholder has presented his access card to enter a door group and not presented the card to exit it, the cardholder is in breach of the Anti-Passback rules. Next time the cardholder attempts to enter the same door group, a Soft Anti-Passback alarm will be raised. However, the cardholder will still be permitted entry to the door group.
Custodian*	The custodian feature allows a card holder with custodian right (the custodian) to give other

Attribute	Description
	cardholders (non-custodians) access to the room. The custodian must be the first to enter the room. The non-custodians are only allowed to enter if the custodian is in the room. The custodian will not be allowed to exit until all non-custodians have left the room.
Door Sounder	Door controller PCB mounted sounder sounds on door alarms.
Ignore Forced	Door forced open is not processed.
Interlock* (Browser) Limit Interlocked Door Access (SPCPro)	Only one door in an area will be allowed open at a time. Requires Door Group.
Setting Prefix	Authorisation with prefix (A,B,* or #) key to set system
* Require door group	

Door timers

Timer	Min.	Max.	Description
Access granted	1 s	255 s	The time the lock will remain open after granting access.
Access deny	1 s	255 s	The duration after which the controller will be ready to read the next event after a invalid event.
Door open	1 s	255 s	Duration within which the door must be closed to prevent a “door open too long” alarm.
Door left open	1 min	180 min	Duration within which the door must be closed to prevent a “door left open” alarm.
Extended	1 s	255 s	Additional time after granting access to a card with extended time attribute.
Escort	1 s	30 s	Time period after presenting a card with escort attribute within a user without escort right can access the door.

Door calendar

Door locked	Select a calendar which should lock the door during the configured time. No card / pin will be accepted during this time.
Door locked	Select a calendar which should unlock the door. The door will be unlocked during the configured time.

Door triggers

Trigger	Description
Triggers that will Momentarily Unlock door	If the assigned trigger is activated, the door will unlock for a defined period, then lock again.
Trigger that will lock the door	If the assigned trigger is activated, the door will get locked. No card / PIN will be accepted.
Trigger that will unlock the door	If the assigned trigger is activated, the door will

Trigger	Description
	get unlocked. No card / PIN will be needed to open the door.
Trigger that will set the door to normal	If the assigned trigger is activated, the door will get back to normal operation. This is to undo locking / unlocking of the door. A card / will be is needed to open the door.

13.4.1 Door Interlock

Door interlock is feature that prevents the remaining doors in an interlock group from opening if any one door in the group is open.

The following are example of how this feature is used:

- In two-doors entry systems used in some banks and other buildings. Usually push buttons or card readers are used to gain entrance, and red and green LEDs show if the door can be opened or not.
- In ATM technical areas connecting ATM doors. Typically all the ATM doors in addition to the door that gives access to the area would be interlocked.

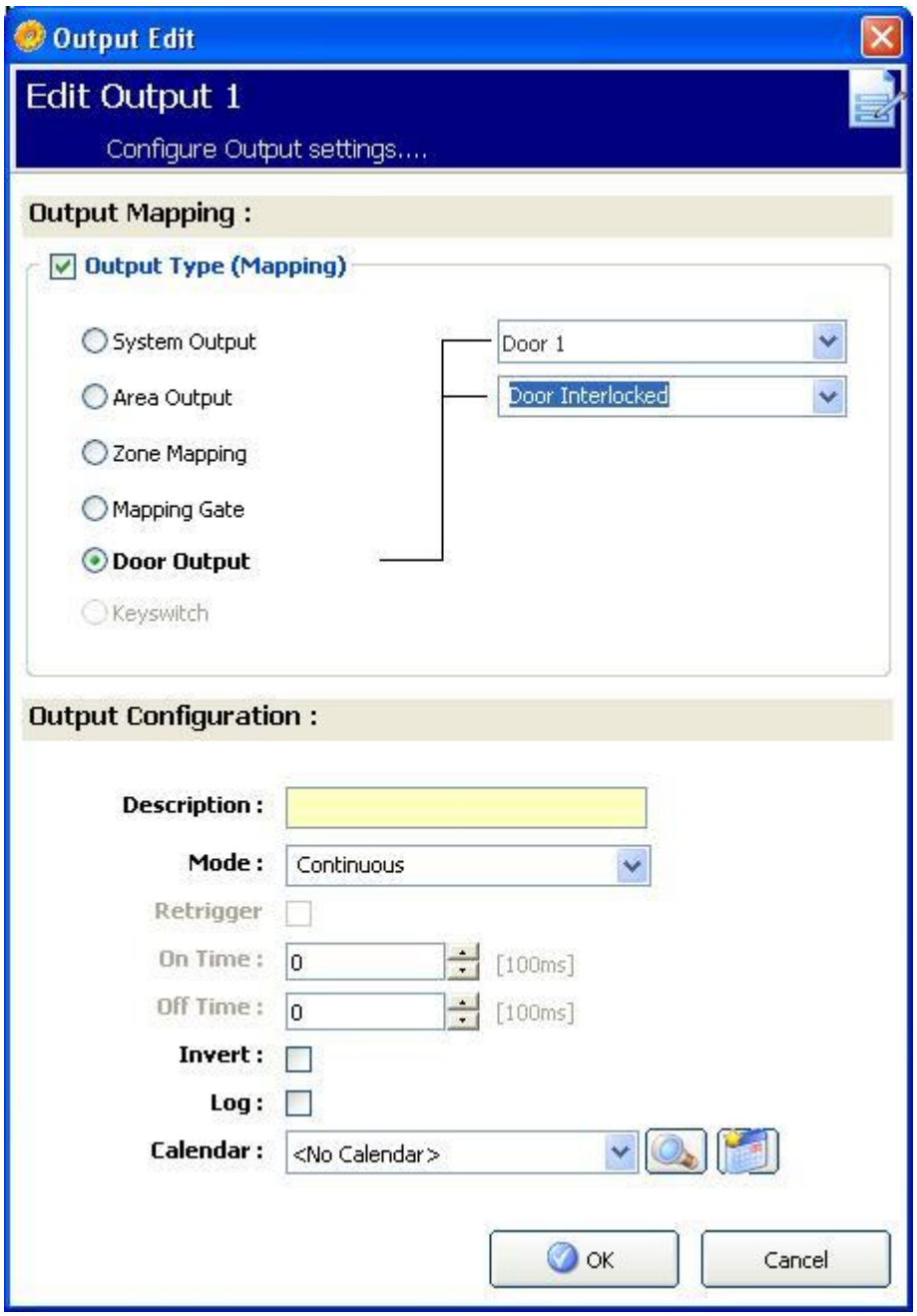
To create a door lock:

1. Create a Door Group. See Editing a door [→ 139].
2. Set the **Interlock** attribute for the required doors in the group. See Editing a door [→ 139].
3. Configure a door output for door interlock operation. This output becomes active for all the doors of the interlock group whenever a door belonging to the group is open, including the open door itself.
   This output could be connected, for example, to a red LED or light to indicate that the door could not be opened, and if inverted could be connected to a green LED or light.

To configure an output for door interlock.

Expanders & Keypads

1. Select an expander from the list.
2. Click on the **Output** tab to configure the output for this expander.
3. Select **Door Output** and select the required door and **Interlocked** as the output type.

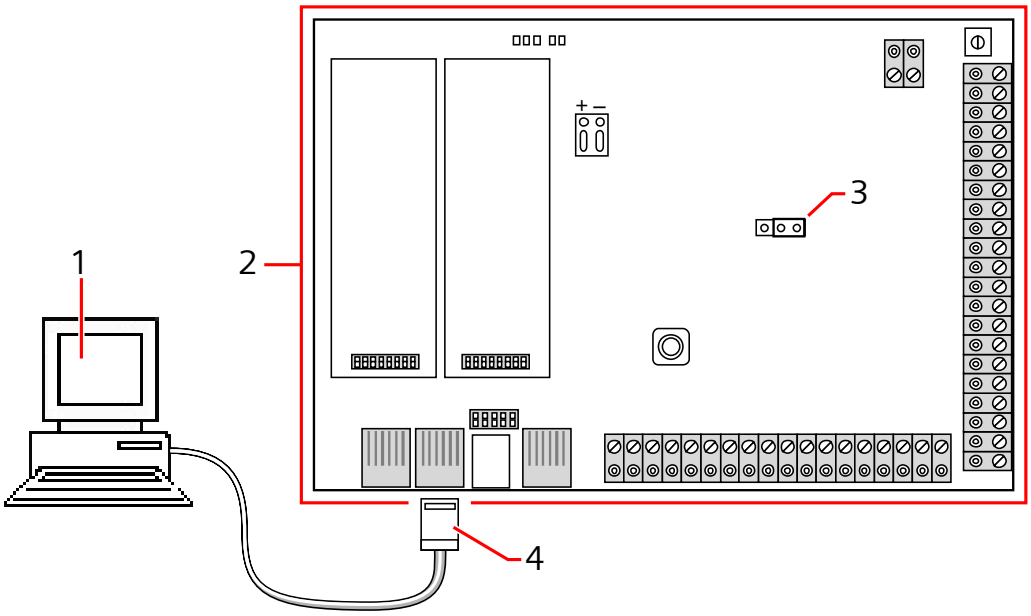

Output Edit
Edit Output 1
Configure Output settings....
Output Mapping :
Output Type (Mapping)
System Output
Area Output
Zone Mapping
Mapping Gate
Door Output
Keyswitch
Door 1
Door Interlocked
Output Configuration :
Description :
Mode :
Continuous
Retrigger
On Time :
0
[100ms]
Off Time :
0
[100ms]
Invert :
Log :
Calendar :
<No Calendar>
OK
Cancel

14 Configuring Communications

14.1 Serial ports

The SPC controller provides 2 serial ports (RS232) that offer the following functionality:

- **X10:** Serial port 1 is a dedicated interface that supports the X10 protocol. This protocol allows for use of the existing power cables of a building to transport control information to X10 devices providing the ability to trigger and monitor these devices via the SPC Controller programming interface.
- **Logging of Events:** The Serial port 2 interface provides the ability to connect to a serial port on a PC or a printer. With this connection, a terminal program can be configured to receive a log of System Events or Access Events from the SPC controller.
- **System Information:** Serial port 2 also provides an interface via a terminal program that allows for the execution of a set of commands to interrogate the controller for specific system information. This facility is available only as a tool for debug and information purposes and should only be used by experienced installers.



1	PC with serial port running hyperterminal
2	SPC controller
3	JP9
4	RS232

To configure the serial ports:

Serial Ports

- Click the tab **Settings**.
  - ⇨ The following window will be displayed:

The settings displayed will depend on the type of connection that the ports are used for. The settings are described in the following sections:

14.2 Modems

The SPC panel provides two on-board modem interface connectors (primary and backup) that allow you to install PSTN or GSM onto the system.

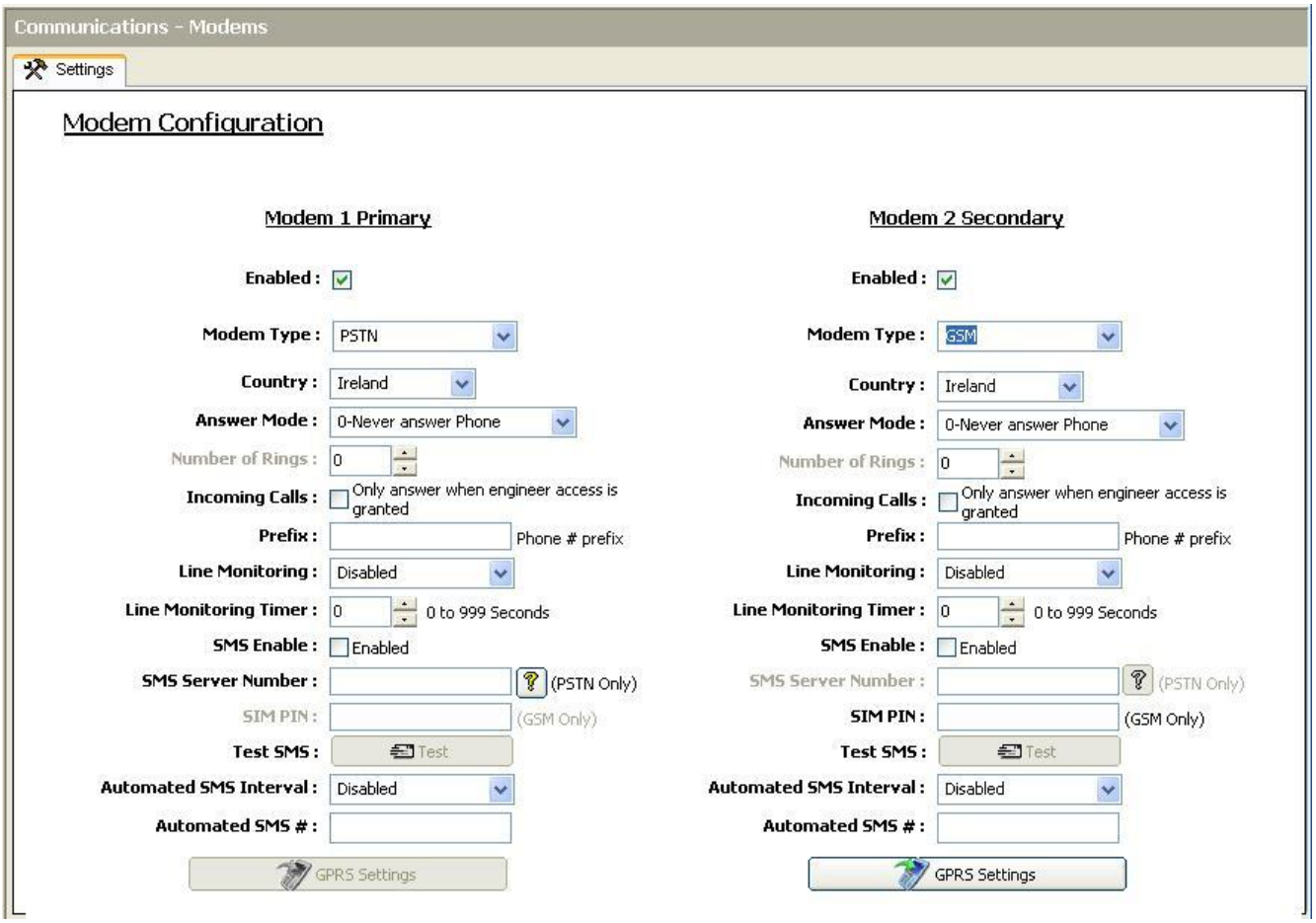
After a factory default, during the process of initial setup of the system with the keypad, the panel detects if it has a primary or backup modem fitted, and if so, it displays the modem type and automatically enables it (or them) with the default configuration. No other modem configuration is allowed at this stage.

To program the modem(s):

Note: A modem must be installed and identified. (See section Installing plug-in modules)

Communications

- Click **Enabled** and configure the modems.



SMS detection and configuration is not available unless modems that are configured and enabled.

14.2.1 SMS test

Once the SIM feature is enabled for a modem, a test may be preformed to desired recipient number with a composed message.

1. Enter the mobile phone number (including 3-digit country prefix) in the number field and a short text message in the message box.
2. Click **Send SMS** and verify the message is received on the mobile phone.

The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required:

- Caller ID needs to be enabled on the telephone line.
- Direct telephone line – not through PABX or other comms equipment.
- Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues).

14.2.2 SMS feature

The SPC controller allows remote (SMS) messaging on systems with installed modems. Once a modem is installed, the following configurations are necessary for SMS:

- SMS-enabled modem. See page.
- SMS Authentication. See page.
- Engineer SMS Control. See page.
- User SMS Control. See page.

Depending on configurations, features include these SMS abilities:

- Event notification. See page.
- Remote Commands (users may be assigned select remote commands. See page.

14.2.3 SMS system options

Once a modem is installed and the SMS feature enabled, for SMS operations the SPC system must apply the SMS Authentication.

1. Select **Configuration > System > System Options**.
2. Select the desired option from the drop-down menu **SMS Authentication**:

- **PIN Only**: This is a valid user code. See page.
- **Caller ID Only**: This is the phone number (including 3-digit country prefix code) as configured for User SMS Control. Only when this option is selected will the SMS Control be available for configuration by the user.
- **PIN and Caller ID**

- **SMS PIN Code Only**: This is a valid PIN code configured for the user which different from the user's login code. See page. Only when this option is selected will the SMS Controls be available for configuration by the user.
- **SMS PIN Code & Caller ID**

14.2.4 SMS commands

Once the SMS setup and configuration is complete, SMS features may be activated. Commands, depending on SMS configuration are sent using a code or caller ID. The type of code depends on what is set for SMS Authentication. For more information on SMS Authentication, see page [· 136]).

The table below provides all available SMS commands. Subsequent action and response are also provided.

SMS Commands are sent as texts to the phone number of the SIM card on the controller.

For commands using code, the format of the text is the code followed by either a space or a full stop. Where **** is the code and "command" is the command: ****.command or **** command.

For example, the command "HELP" is this text: **** HELP or ****.HELP.

COMMANDS (** = code)**			
Using Code	Using Caller ID	Action	Response
**** HELP ****.HELP	HELP	All available commands displayed	All available commands
**** FSET (FULLSET) ****.FSET	FSET	Fullset Alarm	Time/date of system set. If applicable, responds with open zones/forceset zones
****ASET (PARTSET A) ****.ASET		Allows Partset A of alarm by SMS	
**** BSET (PARTSET B) ****.BSET			
**** USET ****.USET	USET	Unset Alarm	System Unset
**** SSTA (STATUS) ****.SSTA	SSTA	Status displayed	Status of system and applicable areas
**** XA1.ON ****.XA1.ON		Where X10 device is identified as "A1", it is triggered on.	Status of "A1"
**** XA1.OFF ****.XA1.OFF		Where X10 device is identified as "A1", it is triggered off.	Status of "A1"
**** LOG ****.LOG		Up to 10 recent events displayed	Recent events
**** ENG.ON ****.ENG.ON	ENG.ON	Enable Engineer access	Engineer status
**** ENG.OFF ****.ENG.OFF	ENG.OFF	Disable Engineer access	Engineer status
**** MANA.ON ****.MANA.ON		Enable Manufacturer access	Manufacturer status

**** MAN.OFF ****.MAN.OFF		Disable Manufacturer access	Manufacturer status
**** O5.ON ****.05.ON		Where output is identified as “O5”, it is triggered on	Status of “O5”
**** O5.OFF ****.05.OFF		Where output is identified as “O5”, it is triggered off	Status of “O5”

For SMS recognition, output identification uses the format ONNN, where O stands for output, and NNN are the numeric placeholders, of which not all are necessary. Example: O5 for Output 5.

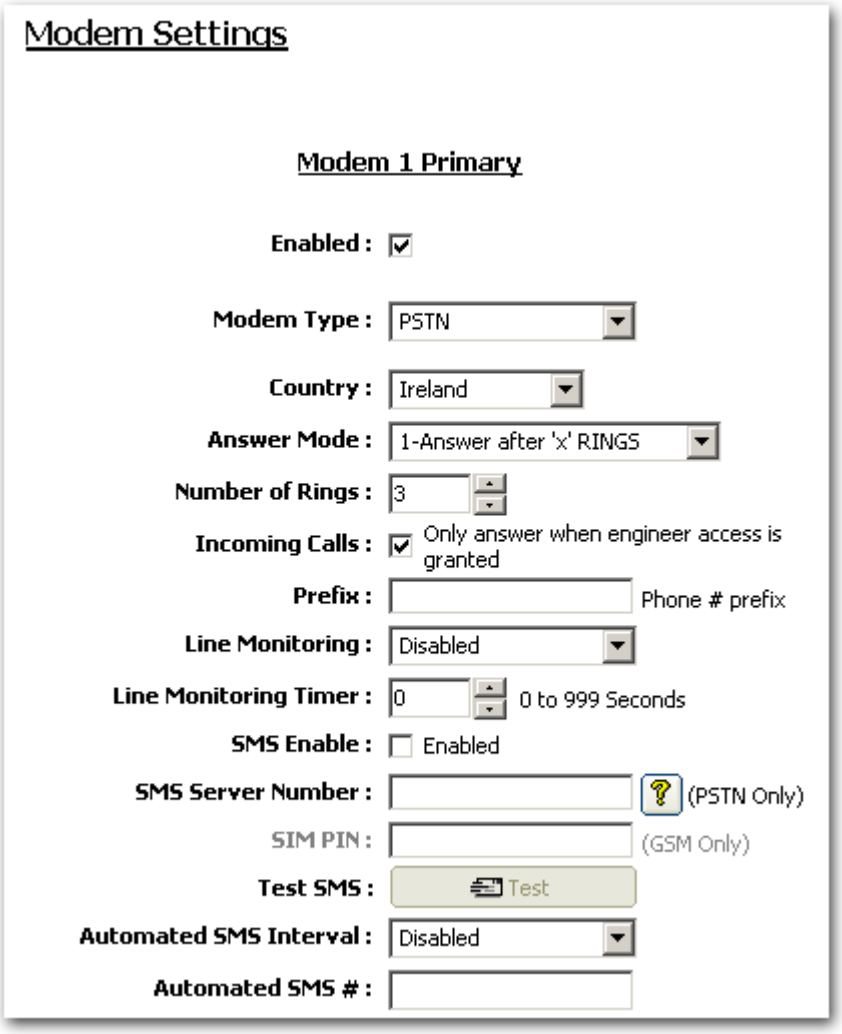
For SMS recognition, X-10 device uses the format: XYNN, where X stands for X-10; Y stands for the alphabetic identity and NN are the available numeric placeholders. Example: XA1.

14.2.5 PSTN modem

Communications

Modem Configuration

1. Click the tab **Settings**.
2. Configure the fields as described in the table below.



Modem settings

Country	Select the country that the SPC is installed in.
SIM PIN	Only for GSM. Enter the PIN for the SIM card installed in the GSM module.
Allow Roaming	Select to enable GSM roaming. **Note:** Changing this setting resets the modem. **Note:** Supported on GSM modems v3.08 or higher.
Incoming Calls	The modem can be programmed to answer calls based on the following conditions: ● Don't answer calls: Modem never answers calls. ● Answer after 'x' rings: Select the number of rings after which the modem answers the incoming call. ● Answers after the calling party calls the modem, hangs up after 1 ring burst only and then immediately re-calls the modem. The SPC system knows to automatically answer the call in this condition. ● Only answer when 'Engineer Access' is granted.
Prefix	Enter the number required to access a line. (e.g. if connected to a PBX)
Line Monitoring	**PSTN Modem:** Enable this feature to monitor the voltage of the line connected to the modem. **GSM Modem:** Enable this feature to monitor the signal level from the GSM mast connected to the modem. The **Fullset** option only enables this feature while the system is Fullset. **Note :** EN 50131-9 Confirmation configuration

	In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (refer to System Options [→ 66])
Monitor Timer	Select the period (in seconds) for which the line voltage must be seen as being incorrect before the line is deemed by the SPC to be faulty.
Modem Fault Time	Time delay for a system alert (0 - 9999 seconds). Default 60 seconds.
SMS Enable	Tick this checkbox to enable the SMS feature on the system. **Note:** The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required: Caller ID needs to be enabled on the telephone line. Direct telephone line – not through PABX or other comms equipment. Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues). **Note:** SMS over PSTN is no longer supported. The functionality remains in the product for backward compatibility.
SMS Server Number	Only for PSTN. This number automatically displays the default number for SMS for the country selected. Enter an appropriate phone number of the SMS service provider that is accessible in your location.
Automated SMS	Select the timing for automated SMS messages.
Automated SMS Number	Enter SMS number to receive automated SMS messages.
Test Call Time	Displays time of last SMS test call.
GSM Chip Version	Displays the GSM WISMO version number. If no version number is available, "---" is displayed.
GPRS Access Point (APN)	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point User Name	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point Password	Only for GSM. Access Point Details must be provided by service provider.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

Note: The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

When using the SMS message feature over a PSTN line, it is necessary to program the phone number of the SMS service provider that services the area in which the SPC is installed. The SPC system automatically dials this number to contact the SMS server whenever the SMS feature is activated. Calling line identity MUST be enabled on the PSTN line for this feature to operate. Each country will have its own SMS service provider with a unique phone number.

This feature is not released in all countries. Please contact your local supplier for more information (support of feature, recommended service provider).

Check with country specific service providers for availability of service and SMS server number.
Some SMS servers may have additional technical requirements for the correct operation of the service. Check with the local SMS service provider for details on these requirements.

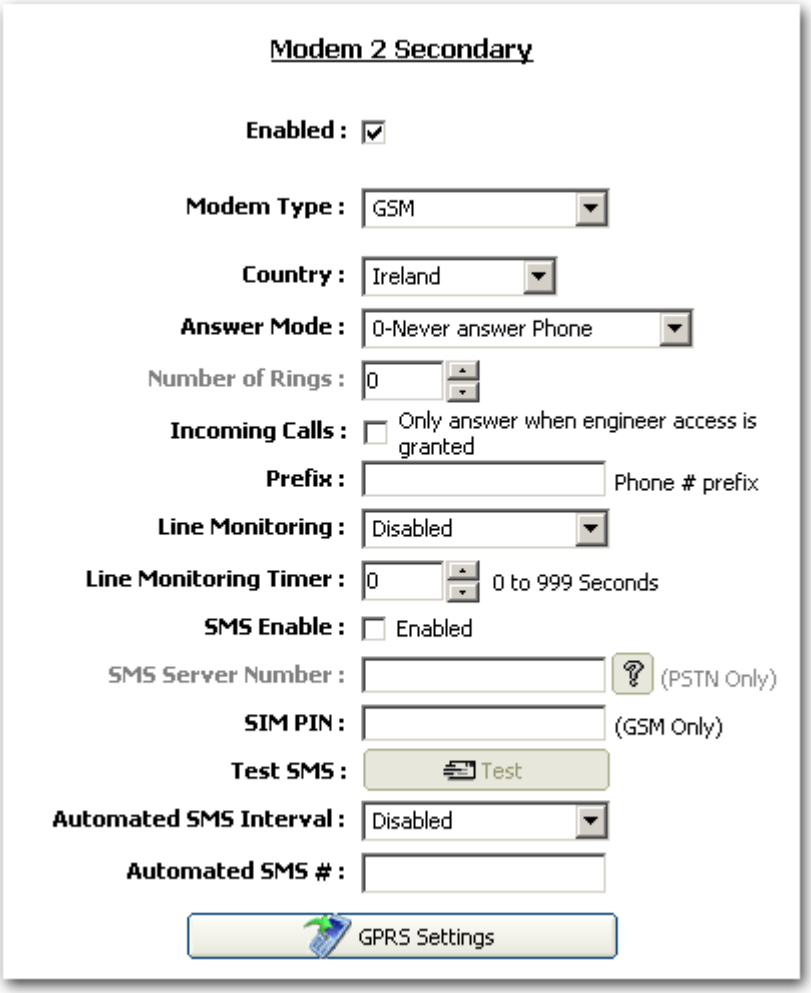
14.2.6 GSM modem

Communications

Modem Configuration

▷ A GSM modem must be properly installed and functioning correctly.

1. Click the tab **Settings**.
2. Configure the fields as described in the table below.



Modem settings

Country	Select the country that the SPC is installed in.
SIM PIN	Only for GSM. Enter the PIN for the SIM card installed in the GSM module.

Allow Roaming	Select to enable GSM roaming. **Note:** Changing this setting resets the modem. **Note:** Supported on GSM modems v3.08 or higher.
Incoming Calls	The modem can be programmed to answer calls based on the following conditions: ● Don't answer calls: Modem never answers calls. ● Answer after 'x' rings: Select the number of rings after which the modem answers the incoming call. ● Answers after the calling party calls the modem, hangs up after 1 ring burst only and then immediately re-calls the modem. The SPC system knows to automatically answer the call in this condition. ● Only answer when 'Engineer Access' is granted.
Prefix	Enter the number required to access a line. (e.g. if connected to a PBX)
Line Monitoring	**PSTN Modem:** Enable this feature to monitor the voltage of the line connected to the modem. **GSM Modem:** Enable this feature to monitor the signal level from the GSM mast connected to the modem. The **Fullset** option only enables this feature while the system is Fullset. **Note :** EN 50131-9 Confirmation configuration In order for EN50131-9 Confirmation to operate correctly, line monitoring must be enabled. (refer to System Options [→ 66])
Monitor Timer	Select the period (in seconds) for which the line voltage must be seen as being incorrect before the line is deemed by the SPC to be faulty.
Modem Fault Time	Time delay for a system alert (0 - 9999 seconds). Default 60 seconds.
SMS Enable	Tick this checkbox to enable the SMS feature on the system. **Note:** The SMS operates using a standard protocol that is used in SMS telephones. Please note that some PSTN operators do not provide the service of SMS over PSTN. For SMS to operate over PSTN the following criteria is required: Caller ID needs to be enabled on the telephone line. Direct telephone line – not through PABX or other comms equipment. Please also note that most Service Providers only allow SMS to a telephone registered in the same country (this is due to billing issues). **Note:** SMS over PSTN is no longer supported. The functionality remains in the product for backward compatibility.
SMS Server Number	Only for PSTN. This number automatically displays the default number for SMS for the country selected. Enter an appropriate phone number of the SMS service provider that is accessible in your location.
Automated SMS	Select the timing for automated SMS messages.
Automated SMS Number	Enter SMS number to receive automated SMS messages.
Test Call Time	Displays time of last SMS test call.
GSM Chip Version	Displays the GSM WISMO version number. If no version number is available, "---" is displayed.
GPRS Access Point (APN)	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point User Name	Only for GSM. Access Point Details must be provided by service provider.
GPRS Access Point Password	Only for GSM. Access Point Details must be provided by service provider.

Click the **Test SMS** button to send a short text message for the purposes of testing the system.

Note: The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

The SMS test is provided only for the purpose of ensuring the SMS feature is operating correctly. A short text message using alphabetic characters (A-Z) should be used to test this feature.

14.3 Alarm Reporting Centres (ARCs)

The SPC panel has the facility to communicate information to a remote receiving station when a specific alarm event on the panel has occurred.

These Alarm Reporting Centres must be configured on the panel to allow this remote communication to operate.

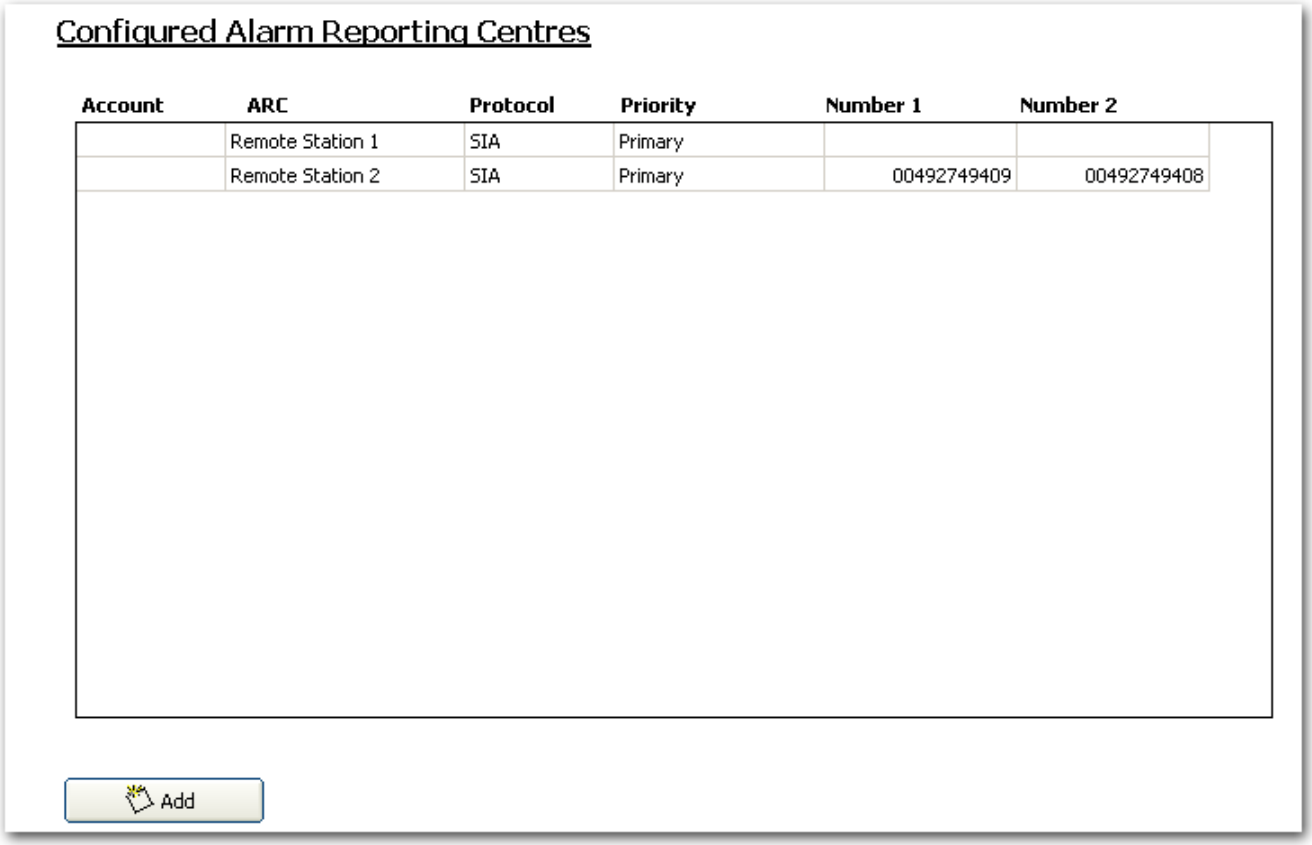
14.3.1 Adding / Editing an ARC using SIA or CID

Communications

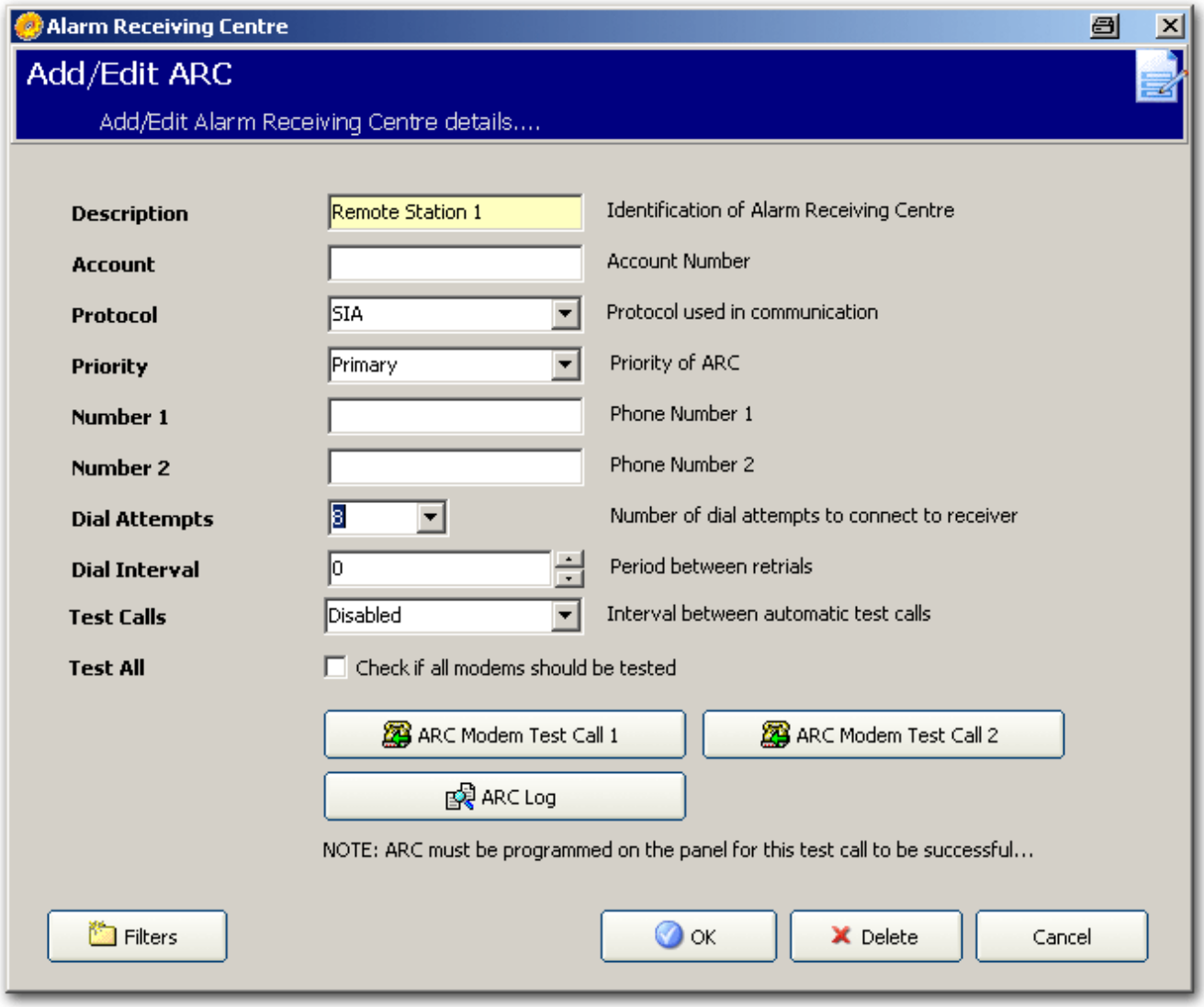
Alarm Reporting Centres

▷ A PSTN or GSM modem is installed and functioning correctly.

1. Click the tab **List**.
   ⇨ The following window will be displayed:



2. Click the button **Add** – OR –
   Click an ARC in the list.
   ⇨ The following window will be displayed.
3. Configure the fields as described in the table below.



Description	Enter a description of the remote Alarm Receiving Centre.
Account	Enter your account number. This information should be available from the receiving station and is used to identify you each time you make a call to the ARC. For a Contact ID account, a maximum of 6 characters is allowed.
Protocol	Enter the communication protocol that you intend to use (SIA, SIA Extended, Contact ID, Fast Format). **Note**: SPC supports the extended SIA protocol. Select this protocol to support additional textual descriptions of the SIA events being sent to the Alarm Receiving Station.
Priority	Select the priority for the ARC in terms of primary or back-up reporting.
Number 1	Enter the first number to be dialled to contact the ARC. This system will always attempt to contact the ARC on this number before attempting another number.
Number 2	Enter the second number to be dialled to contact the ARC. The system will only attempt to contact the ARC on this number if the first contact number did not successfully establish a call.
Dial Attempts	Enter the number of times that the system will attempt to make a call to the receiver. (Default is 8)
Dial Delay	Number of seconds to delay between failed dial attempts (0 - 999).
Dial Interval	Enter the number of seconds to delay between failed dial attempts. (0 - 999)
Test Calls	Enable the test call by choosing a time interval. This will send out an automatic test call from modem 1 to the primary ARC.
Test All	Check this box if you want to initiate also an automatic test call from modem 2 to

	the backup ARC.

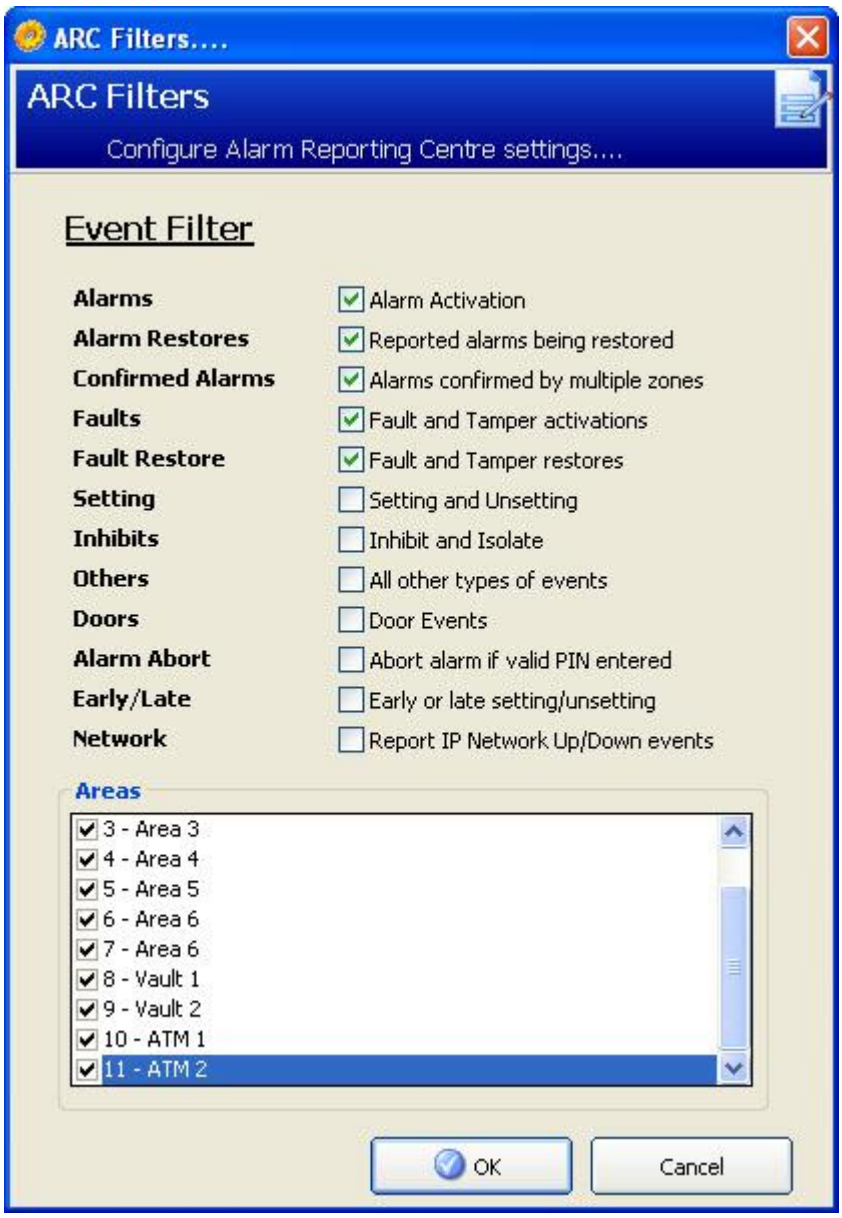
1. Click on the **ARC Modem Test Call 1** or **2** button to manually send a test call from modem 1 or modem 2 to the primary ARC.
2. Click on the **ARC Log** button to receive a log file. A log of all automatic and manual test calls is be displayed.
3. Click on the **OK** button to enter those details on the system.
   ⇨ A list of the configured ARC accounts will be displayed on the **Configured Alarm Reporting Centres** list.

14.3.2 Editing an ARC filter using SIA or CID

To configure the events on the SPC that will trigger the call to the ARC:

Alarm Reporting Centres

- Click the button **Filters** in the window **Add/Edit ARC**.
  ⇨ The following window will be displayed:



- Configure the following fields and click **OK**:

Check any of the following boxes if you want to initiate a remote call to the ARC to notify it of the particular event.

Alarms	Alarms are activated.
Alarm Restores	System alarms are restored.
Confirmed Alarms	Alarms confirmed by multiple zones
Alarm Abort	Alarm Abort events. Alarms are aborted after a valid user code is entered via the keypad after a confirmed or unconfirmed alarm,
Faults	Faults and tampers are activated.
Fault Restores	Fault or tamper alarms are restored.
Settings	System is Set and Unset.
Early/Late	Unscheduled setting and unsetting of the system.
Inhibits	Inhibit and isolate operations are performed on the system.
Door Events	Door events are activated. Only works with SIA protocol.
Other	All other types of events are detected on the system.

Network	Report IP Network Polling Up/Down events.
Areas	Select specific areas to which above events apply.

By adding a separate Alarm Receiving Centre (ARC) for each area defined on the system and programming each area to report it's own separate ARC receiver, the system can approximate a multi-tenanted system in that a high degree of autonomy is assigned to each area.

14.4 EDP Setup

IP

The system has the facility to communicate information to the SPC Com server remotely using Vanderbilt 's own protocol, the EDP (**E**nhanced **D**atagram **P**rotocol). By correctly configuring an EDP receiver on the system, it can be programmed to automatically make data calls to the SPC Com server in a remote location whenever events such as alarm activations, tampers, or arming/disarming occur. The engineer can configure the system to make calls to the remote server via the following routes:

- **PSTN** (PSTN modem required)
- **GSM** (GSM modem required)
- **Internet** (Ethernet interface)

If using the PSTN network, ensure the PSTN modem is properly installed and functioning correctly and that a functioning PSTN line is connected to the A, B terminals on the PSTN modem.

If using the GSM network, ensure the GSM module is properly installed and functioning correctly. An IP connection can be made across the internet to a server with a fixed public IP address.

If an IP connection is required, ensure the Ethernet interface is correctly configured (see page [➞ 219]) and that internet access is enabled at the router.

14.4.1 Adding an EDP Receiver

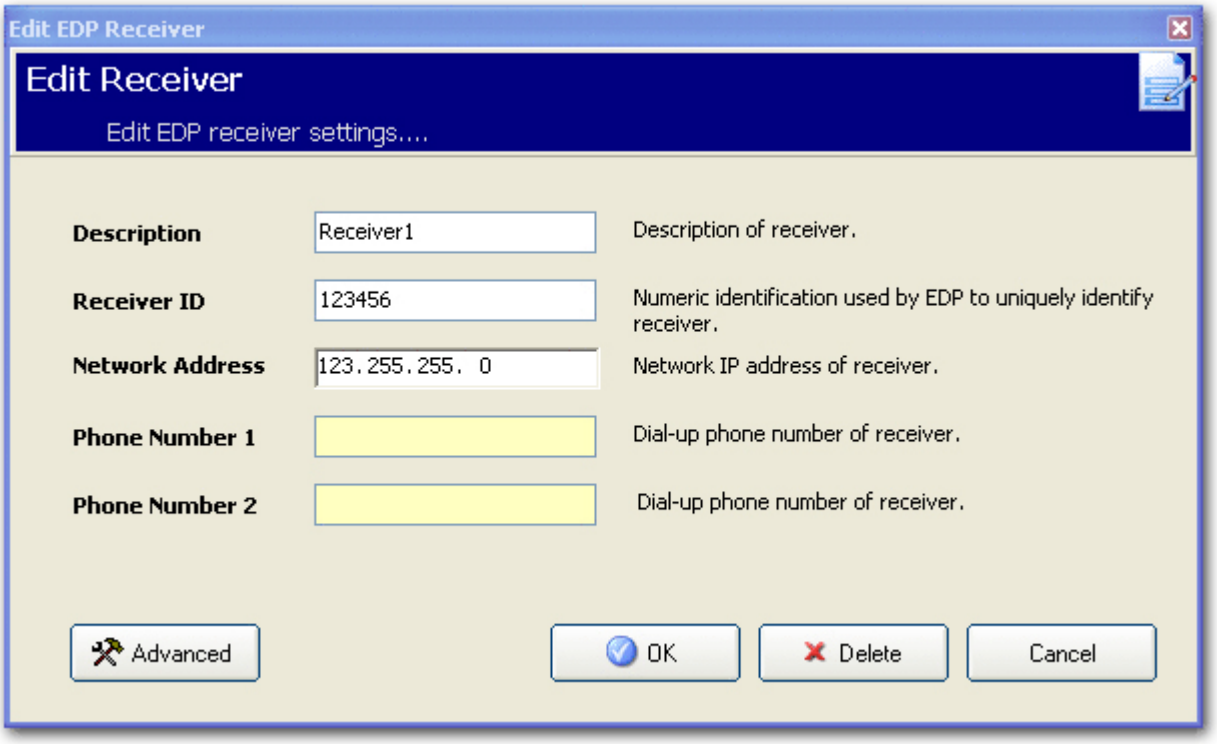
Communications

EDP Setup

1. Click the tab **List**.

Max. 8 receivers can be added to the SPC system.

2. Click the **Add New Receiver** button.
   ⇨ The following window will be displayed.
3. See table below for further information.



Description	Enter a text description of the receiver.
Receiver ID	Enter a unique number which will be used by the EDP to identify the receiver.
Network Address	Enter the IP address of the receiver. This is only required if the connection to the EDP receiver is being made over the Ethernet interface. If using one of the on-board modems then leave this field blank.
Phone Number	Enter the first phone number that the modem(s) will dial to contact the receiver.
Phone Number 2	Enter a second phone number that the modem(s) will dial in the event that the first number dialled did not result in a call being successfully established.

See also

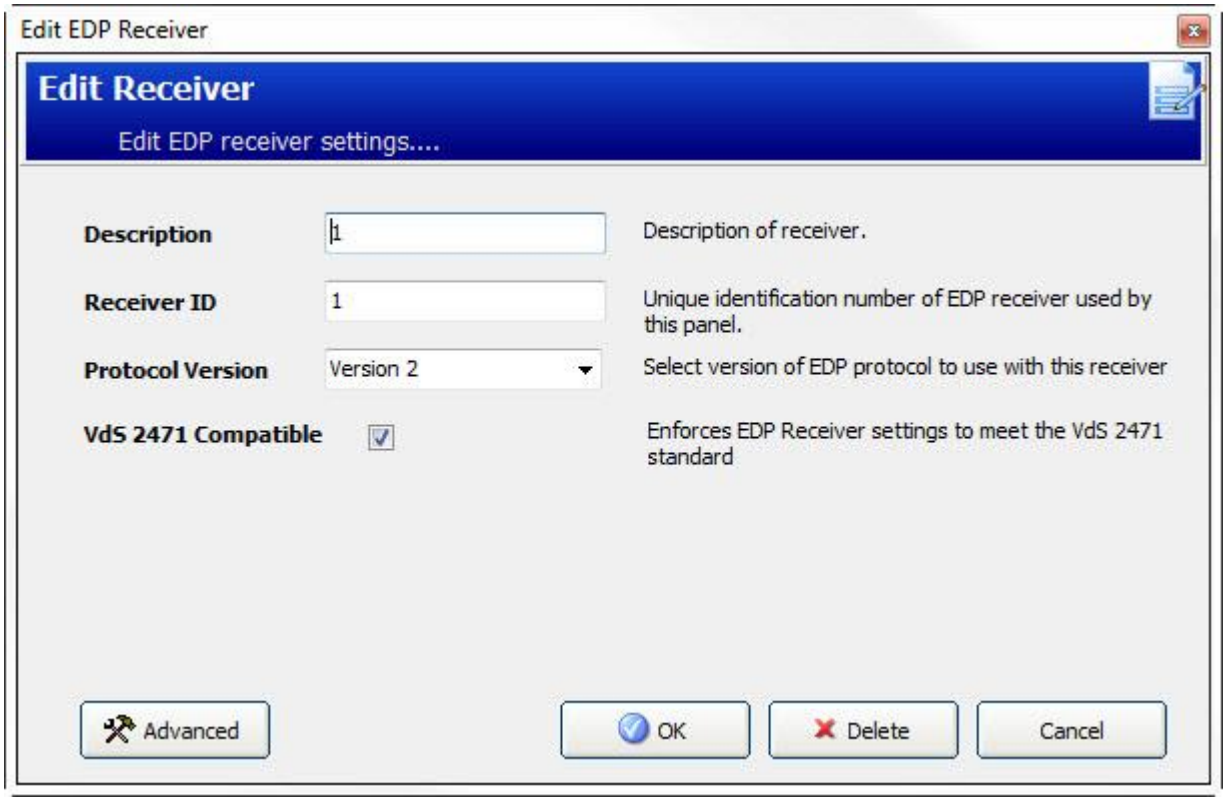
Editing EDP Receiver Settings [→ 160]

14.4.2 Editing EDP Receiver Settings

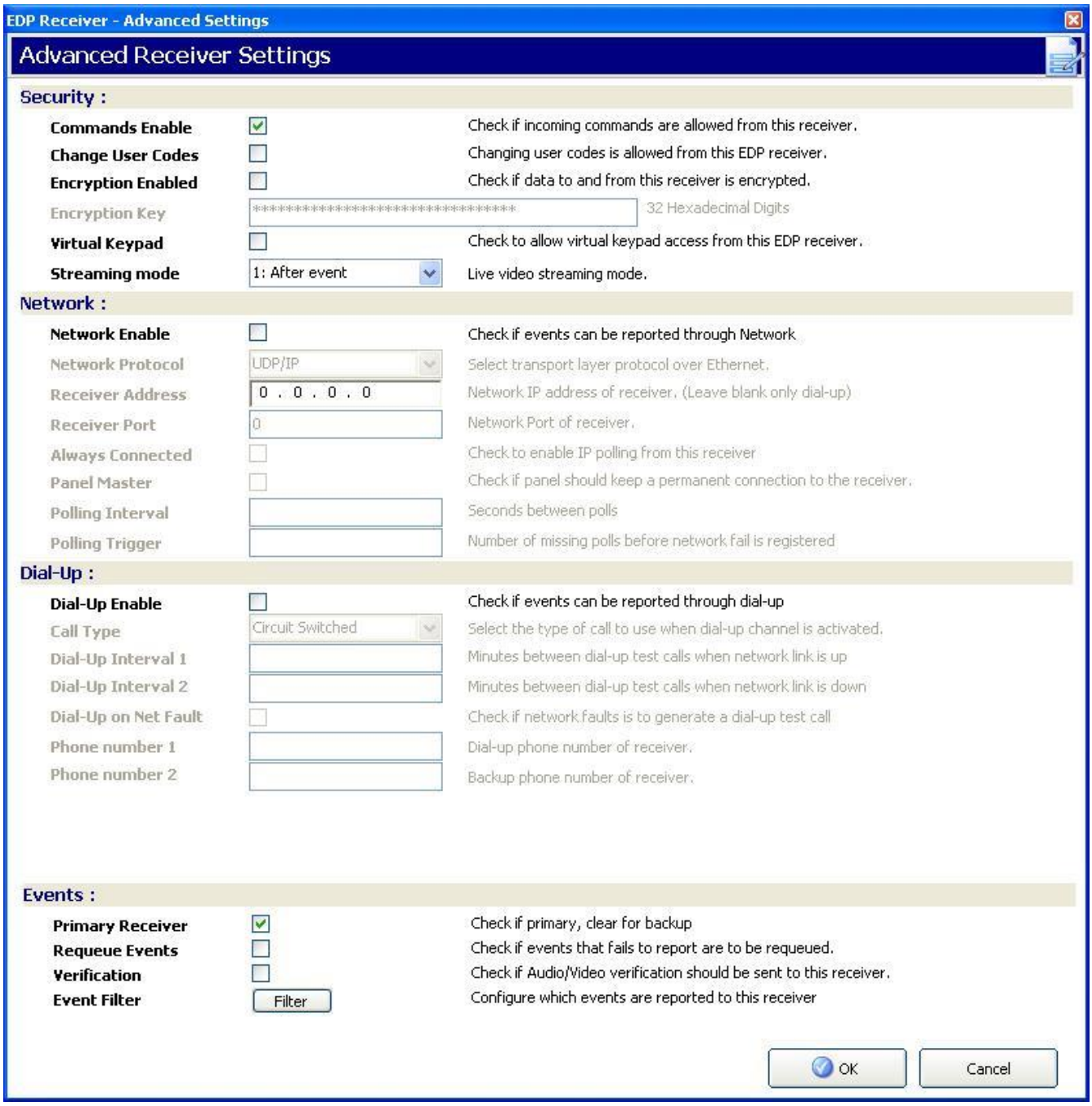
Communications

EDP Setup

1. Click on a receiver from the list of **Configured EDP Receivers**.
   ⇨ The following window is displayed.



2. Configure the fields as described in the table below.
3. Click the **Advanced** button to configure more advanced settings
   ⇨ The following window is displayed.



4. Configure the fields as described in the table below.

Description	Edit the name of the EDP receiver. Maximum 16 characters.
Receiver ID	Edit the EDP receiver ID. Range is 1 to 999997 (999998 and 999999 are reserved for special purposes)
Protocol Version	Select the EDP protocol version to use with this EDP receiver. Options are Version 1 or Version 2. Version 2 is recommended if supported by the receiver, as it is a more secure protocol.
VdS 2471 Compatible	(Vds standard only) If this option is selected then the EDP receiver will enforce the following settings for that receiver: ● 8s polling interval ● TCP protocol enforced ● TCP retries will fail before 10s (9s approx)

	• EDP event retries are set to 1 independent of the global “Retry Count” setting in “EDP Settings” • FTC will be generated within 20s of network failure.

Security	
Commands Enable	Check this box to allow commands to be accepted from the receiver.
Change User PINs	Check this box to allow user PINs to be changed from a remote location. This feature is applicable only if commands are enabled from the receiver.
Encryption Enable	Check this box to enable encryption on data to and from the receiver.
Encryption Key	Enter a hexadecimal key (max. 32 digits) that will be used to encrypt the data. **Note**: The same key will need to be used at the receiver.
Virtual Keypad	Enables access to the panel with a virtual keypad i.e. a PC software module that looks and behaves like an SPC keypad. It is available with the SPC Com client.
Live Streaming/Streaming Mode	Specifies when live streaming of audio and video is available. Options are Never, Always or Only after an alarm event. Default is ‘Only after an alarm event’. **Note:** This setting has obvious privacy implications and therefore should be enabled only where appropriate and subject to local laws and regulations.
Network (Applies to the Ethernet connection only)	
Network Enable	Check this box to allow events to be reported through the network.
Network Protocol	Select the type of network protocol for the receiver. Options are UDP and TCP. TCP is recommended if supported by the receiver.
Receiver ID Address	Enter the IP address of the receiver.
Receiver IP Port	Enter the IP port that the EDP receiver is listening on.
Always Connected	If enabled the panel will keep a permanent connection to the receiver. If disabled, the panel will only connect to the receiver after an alarm event.
Panel Master	If enabled the panel is master of polling messages. Only applicable to UDP connections.
Polling Interval	Enter the number of seconds between polls.
Polling Trigger	Enter the number of missing polls before a network connection fail is registered. Only applicable to UDP connections.
Generate a Network Fault	If polling fails, a network fault alert is generated.
Dial-up (Applies to the GPRS modem connection only)	
Dial-up Enable	Check this box to report events through a dial-up connection.
Call type	Select type of call to use when dial up is enabled. Select GPRS.
GPRS protocol	Select the transport layer protocol used over the GPRS connection. Options are UDP or TCP. Only applicable if Call Type is GPRS.
GPRS address	Enter the IP address of EDP receiver for GPRS connections. Only applicable if Call Type is GPRS.
GPRS port	Enter the port that the EDP receiver is listening on for GPRS connections Options are UDP or TCP. Only applicable if Call Type is GPRS. Default is 50000.
GPRS Hangup Timeout	Enter the time in seconds after which the GPRS call will hang up. (0 = stay connected until IP connection is up)

GPRS Autoconnect	Check this box to automatically trigger a GPRS call to the server if an IP network fault occurs.
Dial-up on Net Fault	Check this box to report network faults on a dial-up test call.
Dial-up Interval 1*	Enter the number of minutes between dial-up test calls when network link is up.
Dial-up Interval 2*	Enter number of minutes between dial-up test calls when network link is down.
Network Address*	Enter the IP address of the receiver. This is only required if the connection to the EDP receiver is being made over the Ethernet interface. If using one of the on-board modems then leave this field blank.
Phone Number*	Enter the first phone number that the modem(s) will dial to contact the receiver.
Phone Number 2*	Enter a second phone number that the modem(s) will dial in the event that the first number dialled did not result in a call being successfully established.
Events	
Primary Receiver	Check this box to indicate that this is the primary receiver. If unchecked, this is a backup receiver.
Re-queue Events	Check this box if events that failed to report are to be re-queued for transmission
Verification	Check this box if Audio/Video verification is to be sent to this receiver.
Event Filter	Click this button to edit the filter events that will trigger an EDP call. Refer to Editing Events Filter Settings [→ 164].

* EDP dial-up over PSTN is not supported in this release.

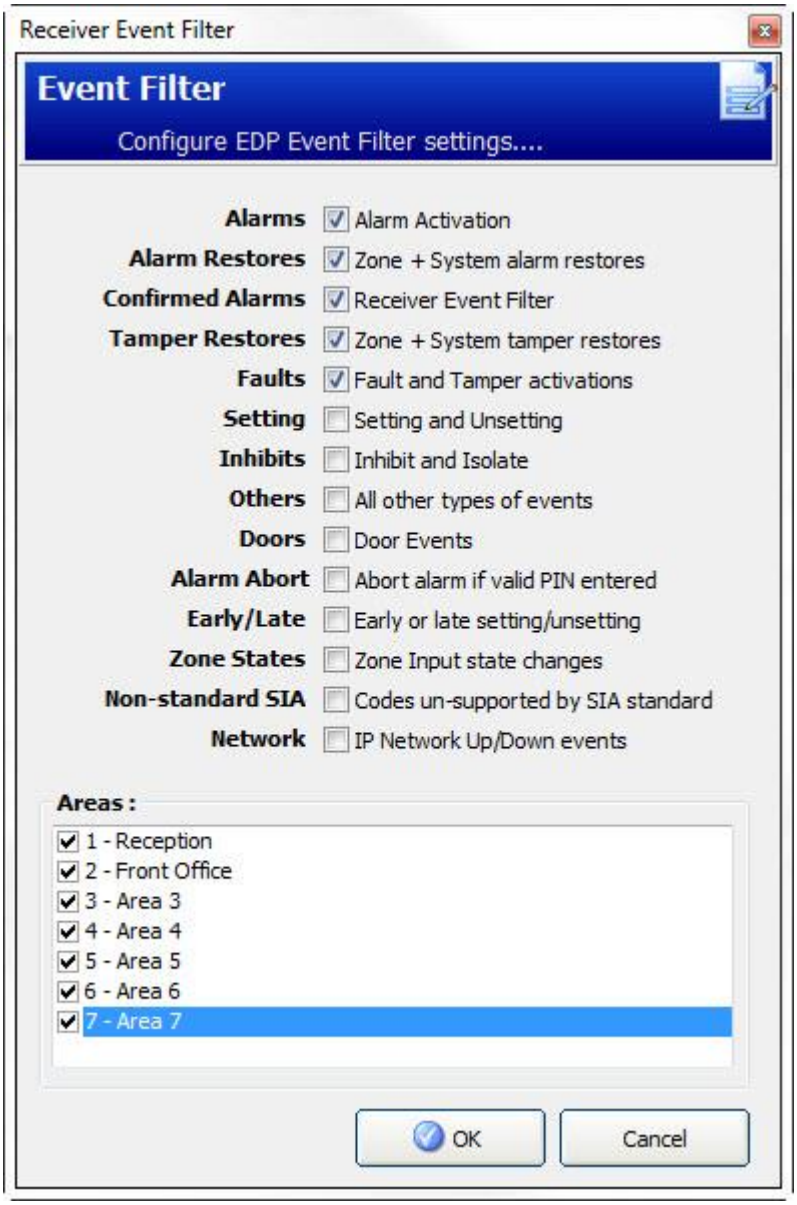
See also

- Configuring SMS [→ 56]

14.4.3 Editing Event Filter Settings

EDP Setup

1. Click the button **Advanced**.
2. Click the button **Filter**.
   ⇨ The following window will be displayed.
3. Configure the fields as described in the table below.



Check any of the following boxes if you want to initiate a remote call to an EDP Receiver to notify it of the particular event.

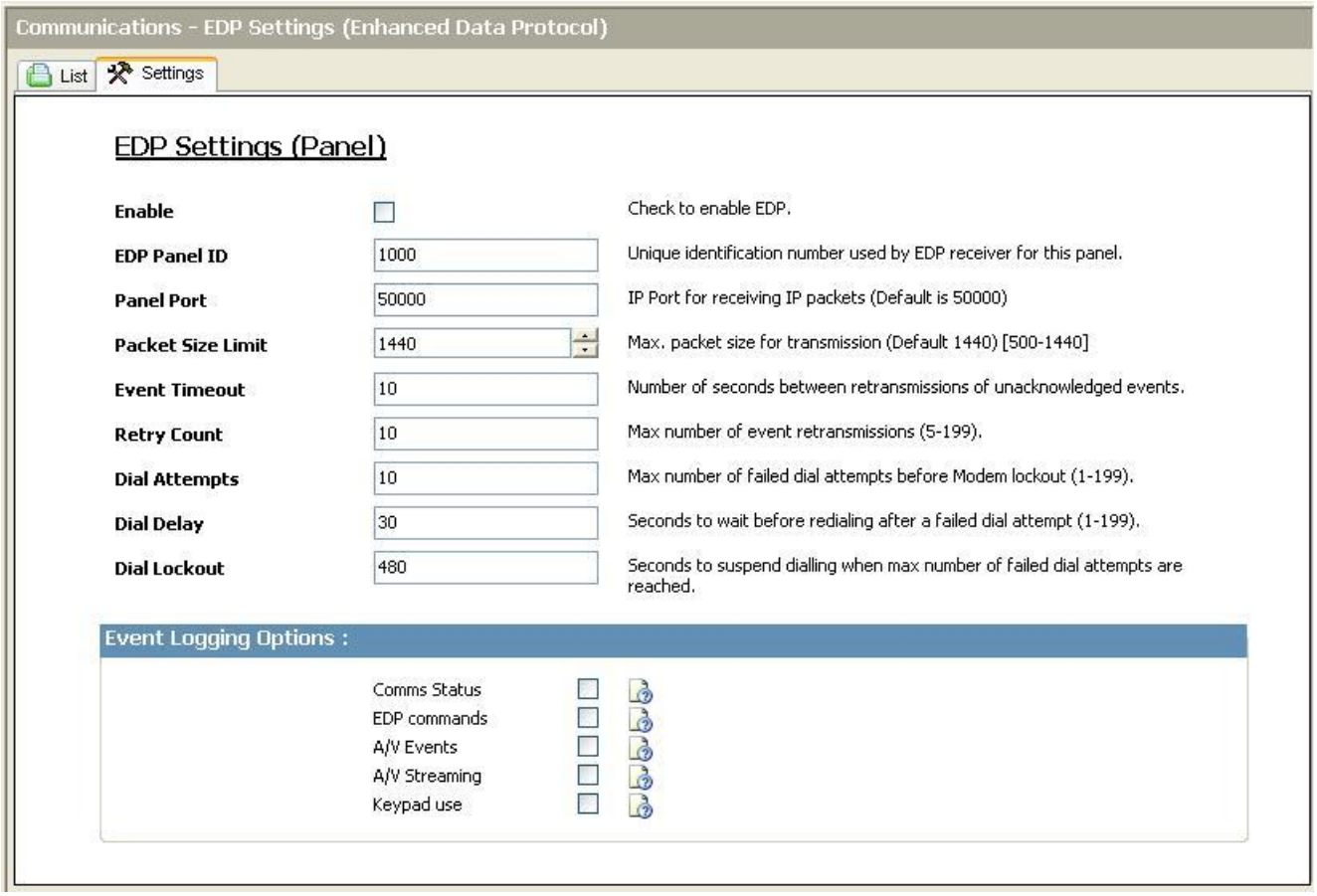
Alarms	Alarms are activated.
Alarm Restores	System alarms are restored.
Confirmed Alarms	Alarms confirmed by multiple zones
Alarm Abort	Alarm Abort events. Alarms are aborted after a valid user code is entered via the keypad after a confirmed or unconfirmed alarm,
Faults	Faults and tampers are activated.
Fault Restores	Fault or tamper alarms are restored.
Zone state	Report all zone input state changes.
Settings	System is Set and Unset.
Early/Late	Unscheduled setting and unsetting of the system.
Inhibits	Inhibit and isolate operations are performed on the system.
Door Events	Door events are activated. Only works with SIA protocol.
Other	All other types of events are detected on the system.

Other (Non standard)	Non supported SIA codes used with SPC COM XT including Camera Online/Offline events.
Network	Report IP Network Polling Up/Down events.
Areas	Select specific areas to which above events apply.

14.4.4 Editing EDP settings

EDP Setup

1. Click the tab **Settings**.
   ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.



Enable	Tick this checkbox to enable EDP operation on the system.
EDP Panel ID	Enter a numeric identifier that is used by the EDP Receiver to identify the panel uniquely.
Panel Port	Select the IP port for receiving IP packets. Default is 50000.
Packet Size Limit	Enter the maximum number of bytes in an EDP packet for transmission.
Event timeout	Enter the timeout period (in seconds) between retransmissions of unacknowledged events.

Retry Count	Enter the maximum number or event retransmissions allowed by the system.
Dial Attempts	Enter the maximum number of failed dial attempts accepted by the system before the modem is locked out (prevented from making further attempts to dial). The lockout period is defined in the option Dial Lockout.
Dial Delay	Enter the time period (in seconds) that the system will wait before redialling after a dial attempt has failed.
Dial Lockout	Enter the time period (in seconds) that the system will suspend dialling when the maximum number of failed dial attempts is reached. Enter a value of '0' to continually attempt dialling.

Event Logging Options

Comms Status	Log all communication availability.
EDP Commands	Log all commands executed through EDP.
A/V Events	Log when Audio/Video verification events are sent to Receiver.
A/V Streaming	Log when Audio/Video live streaming begins.
Keypad Use	Log when remote keypad is activated.

14.5 Remote Maintenance

For further information please refer to the Remote Maintenance Configuration Manual.

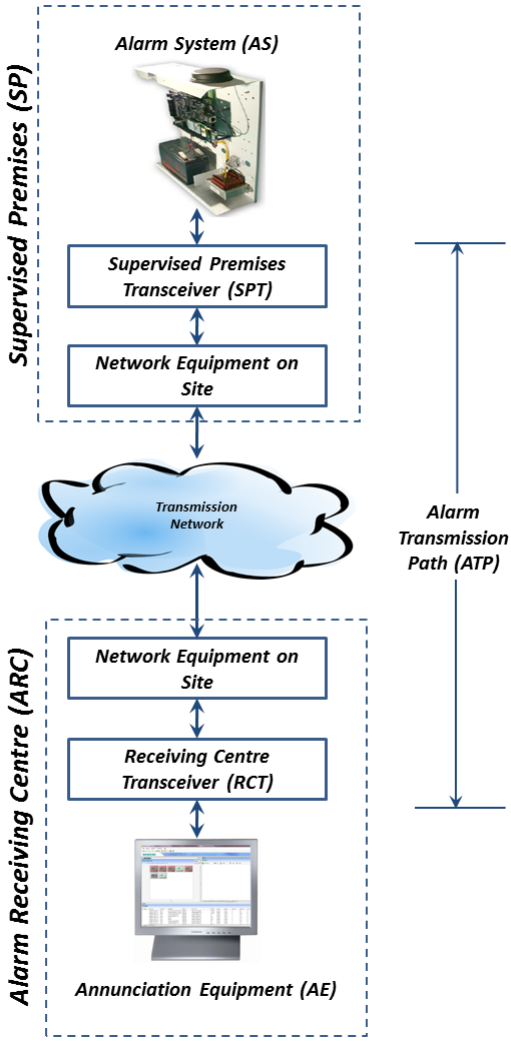
14.6 FlexC®

The SPC Flexible Secure Communications Protocol (FlexC) enables communications for an Internet Protocol (IP) based single or multiple path Alarm Transmission System (ATS). An ATS is a reliable communications link between a Supervised Premises Transceiver (SPT e.g. Ethernet integrated onto the SPC panel) and a Receiving Centre Transceiver (RCT e.g. SPC Com XT or the SPC Connect server, www.spcconnect.com). A FlexC ATS consists of a primary Alarm Transmission Path (ATP) and up to nine backup Alarm Transmission Paths (ATPs). It enables:

- Two-way transfer of data between the SPT, for example the SPC panel over Ethernet, and the RCT, for example, the SPC Com XT server or the SPC Connect server, www.spcconnect.com.
- Communication monitoring of a complete ATS and individual ATPs.

SPC intrusion panels support FlexC over IP with any of the following interfaces:

- Ethernet
- GSM modem with GPRS enabled
- PSTN modem



See also

- Quick Start ATP Configuration for EN50136 ATS [→ 168]
- Configuring Event Profiles [→ 180]
- Event Exception Definition [→ 182]
- Configuring Command Profiles [→ 184]
- Configuring an EN50136-1 ATS or Custom ATS [→ 171]

14.6.1 Quick Start ATP Configuration for EN50136 ATS

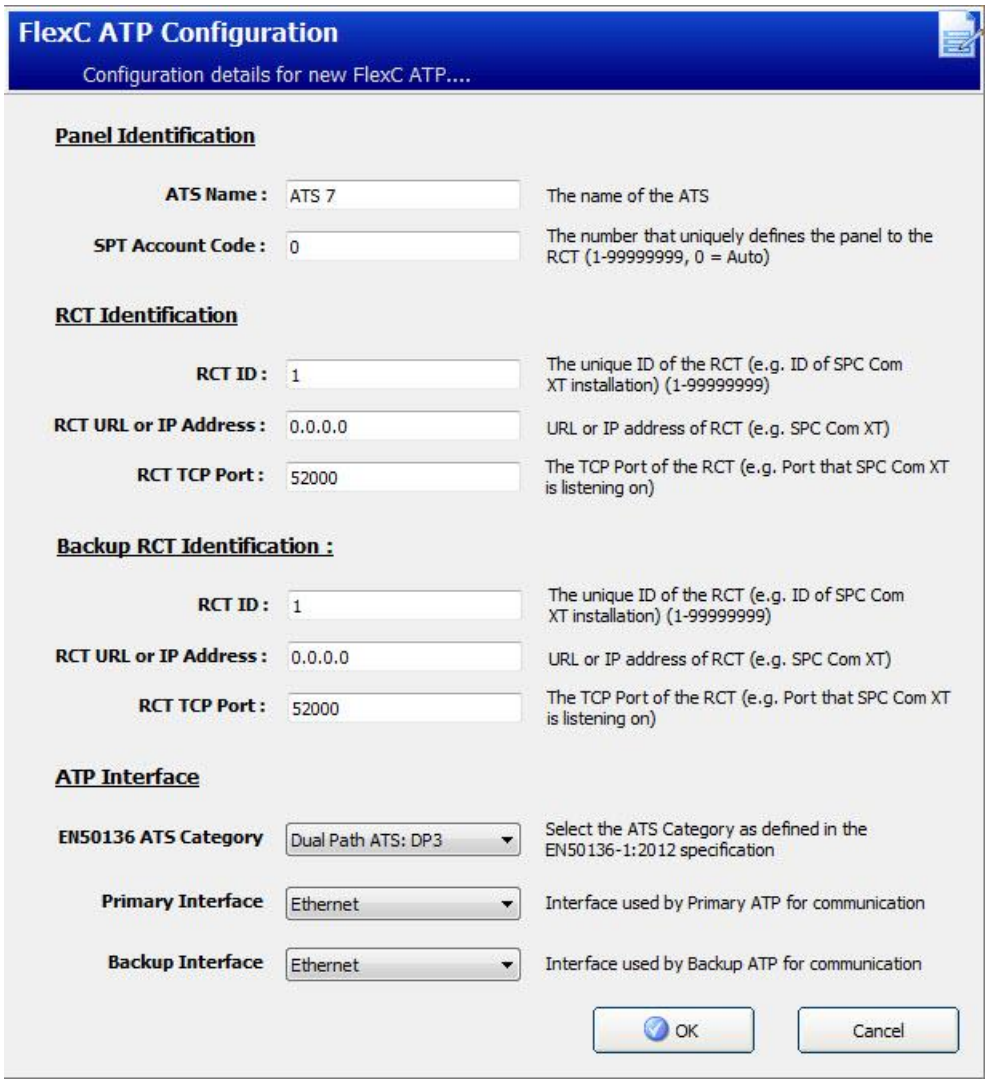
FlexC provides the following out of the box features that enable you to get FlexC up and running quickly:

- Quick start configuration screen for an EN50136 **Single Path ATS**, **Dual Path ATS** and **Dual Path Dual Server ATS**
- Default Event Profile
- Default Command Profile (this does not support audio video verification)
- Default **FlexC Command User Name** (FlexC) and **Command Password** (FlexC) for controlling the panel from the RCT (e.g. SPC Com XT)
- Auto Encryption with no password

1. To quickly configure a FlexC connection between a panel and an RCT (e.g. SPC Com XT), go to **Communications - FlexC - FlexC ATS**.

2. Under **Add EN50136-1 ATS**, choose one of the following to display the **ATP Configuration** screen:

- **Add Single Path ATS** - primary ATP only
- **Add Dual Path ATS** - primary and backup ATPs
- **Add Dual Path Dual Server ATS** - primary and backup ATPs, primary and backup servers



1. Complete the fields on the **ATP Configuration - EN50136 ATS** screen shown in the table below. At a minimum, you must complete the field **RCT URL or IP Address** to save. If you do not enter an **SPT Account Code**, you can commission the panel using the **ATS Registration ID** which is automatically generated when you save. The RCT operator must enter this **ATS Registration ID**, for example, in SPC Com XT.
2. Click **Save**. The **ATS Configuration** screen displays showing the **ATS Registration ID** and the configured primary ATP or primary and backup ATPs in the **Event Sequence Table**.
3. On the **ATS Configuration** screen, click **Save** to accept the default settings, for example, the **Default Event Profile**, the **Default Command Profile** (including the FlexC **Command User Name** and FlexC **Command Password**), and **Auto Encryption** with no password. To change the settings, see Configuring an EN50136-1 ATS or Custom ATS [➙ 171].

4. Click **Back**. The ATS displays in the **Configured ATS** table.
5. Click the **Refresh Registration ID** button to display the **Registration ID** in the ATS table.

Panel Identification	
ATS Name	Enter the name of the ATS. If you do not enter a value, the ATS name defaults to ATS 1, ATS 2 etc.
SPT Account Code	The number that uniquely identifies the panel to the RCT. Enter 0 if you do not have the SPT Account Code. In this case, you can commission the panel using the **ATS Registration ID**. For an EN50136 ATS, the **ATS Registration ID** is automatically generated when you click **Save**. The RCT can send the **SPT Account Code** to the panel when it is available.
RCT Identification & Backup RCT Identification (Dual Path Dual Server Only)	
RCT ID	Enter the **RCT ID** that uniquely identifies the RCT (e.g. SPC Com XT) to the panel. This must match the value entered in the SPC Com XT Server Configuration Manager tool in the **Server RCT ID** field in the **Server Details** tab. See the *SPC Com XT Installation & Configuration Manual*.
RCT URL or IP Address	Enter the **RCT URL or IP Address** for the RCT server location (e.g. SPC Com XT server).
RCT TCP Port	Enter the TCP port for the RCT (e.g. SPC Com XT). This must be the same value entered for the field **Server FlexC Port** in the SPC Com XT Server Configuration Manager tool.
ATP Interface	
EN50136 ATS Category	Select the EN50136 ATS Category. For a description of categories, see ATS Category Timings [→ 269].
Primary Interface	Select the **Primary Interface** to apply to the primary communications path from the following: • Ethernet • GPRS: Modem 1 • GPRS: Modem 2 • Dial Up Internet: Modem 1 • Dial Up Internet: Modem 2
Backup Interface	For a **Dual Path ATS**, select the **Backup Interface** to use for the backup communications path from the following: • Ethernet • GPRS: Modem 1 • GPRS: Modem 2 • Dial Up Internet: Modem 1 • Dial Up Internet: Modem 2

14.6.2 Configuring an EN50136-1 ATS or Custom ATS

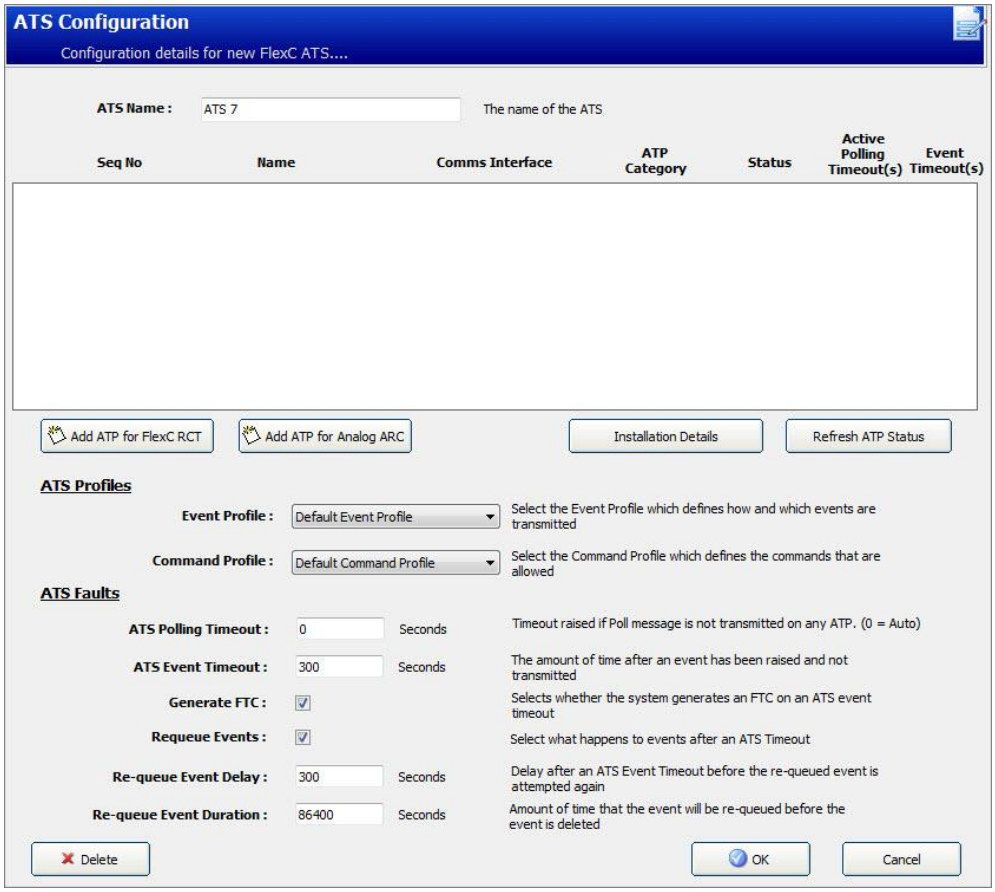
An ATS comprises an alarm panel, network paths and an RCT (e.g. SPC Com XT). It combines one or multiple paths between an SPC panel and an RCT. You can add up to 10 ATPs to an ATS.

!	*NOTICE*
	For an EN50136-1 ATS, the ATS set up sequence starts with configuring an ATP for an ATS. This provides you with a quick set up feature. See Quick Start ATP Configuration for EN50136 ATS [→ 168].

1. To configure an ATS, go to **Communications - FlexC - FlexC ATS**.
2. Choose from one of the following options:

- **Add Single Path ATS**
- **Add Dual Path ATS**
- **Add Dual Path Dual Server ATS**
- **Add Custom ATS**.

1. For an EN50136 ATS, you must configure the settings on the **ATP Configuration - EN50136** screen first. See Quick Start ATP Configuration for EN50136 ATS [→ 168].
2. The **ATS Configuration** screen displays. An EN50136-1 ATS will display a primary or primary and backup ATP in the **Event Sequence Table**.



1. Enter an **ATS Name** to identify the ATS. If you do not enter a value, the ATS name defaults to ATS 1, ATS 2 etc.
2. To add 1 primary and up to 9 backup ATPs to an ATS, click **Add ATP to FlexC RCT**, see Add ATP to FlexC RCT [→ 172] or click **Add ATP to Analog ARC**, see Add ATP to Analog ARC [→ 177].

3. Select an **Event Profile** from the dropdown menu. To customise how events are transmitted on an ATS, see Configuring Event Profiles [→ 180].
4. Select a **Command Profile** from the dropdown menu. To customise the commands enabled for an RCT to control a panel, see Configuring Command Profiles [→ 184].
5. Complete the **ATS Faults** fields as shown in the table below.
6. Click the **Edit Installation Details** button to complete the settings to identify the panel to the RCT operator. See Edit Installation Details [→ 179].
7. Click **Save** and **Back** to return to the **ATS Configuration** page. The new ATS displays in the **Configured ATS** table.
8. For multiple ATPs, you can use the up and down arrows in the **Event Sequence Table** to reorder the ATP sequence.

ATS Polling Timeout	This field is automatically calculated by adding the values of the **Active Polling Timeout** column in the Event Sequence Table, that is, for all ATPs in an ATS. You can manually overwrite this field. For example, CAT 2 [Modem] has an **Active Polling Timeout** of 24 hours 10 minutes (87000 seconds). To allow a shorter reaction time, enter a lower value.
ATS Event Timeout	The amount of time after an event has been raised and not successfully transmitted before the ATS gives up. Default: 300 seconds.
Generate FTC	Select whether the system generates a FTC on an ATS event timeout.
Re-queue Events	Select this to re-queue events after an ATS Timeout.
Re-queue Event Delay	Delay after an ATS Event Timeout before the re-queued event is attempted again. Default: 300 seconds.
Re-queue Event Duration	Amount of time that the event will be re-queued before the event is deleted. Default: 86400 seconds.

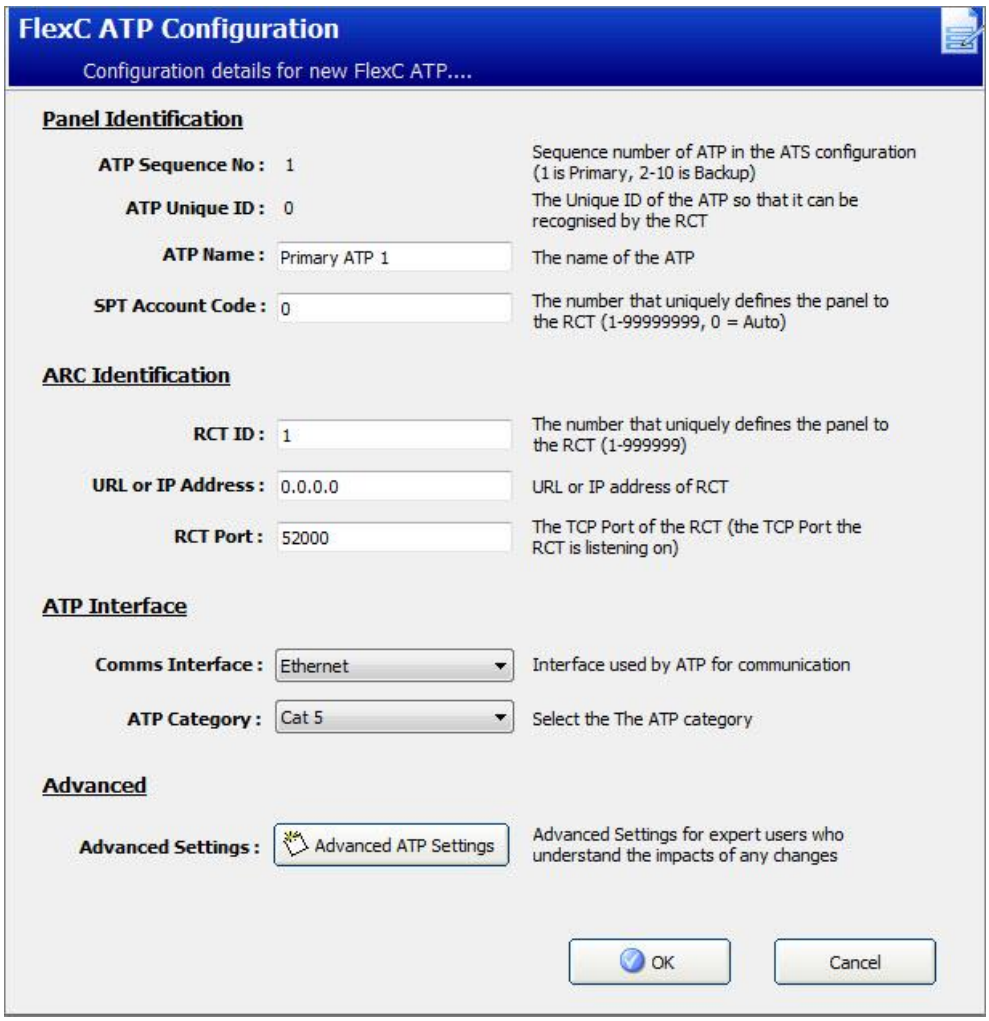
See also

ATS Category Timings [→ 269]

14.6.2.1 Add ATP to FlexC RCT

Add ATP to FlexC RCT allows you to configure an ATP between the SPC panel and the RCT (e.g. SPC Com XT). You can configure up to 10 ATPs for each ATS.

1. Click the button **Add ATP to FlexC RCT**.



1. Complete the ATP fields described in the table below.
2. If required, click **Advanced ATP Settings**, for example, if you are using auto encryption you can optionally enter a password in the **Encryption Password** field. See Configure Advanced ATP Settings [→ 174].
3. Click **Save**.

WARNING

It is not recommended to change **Advanced ATP Settings**. Changes must only be made by expert users.

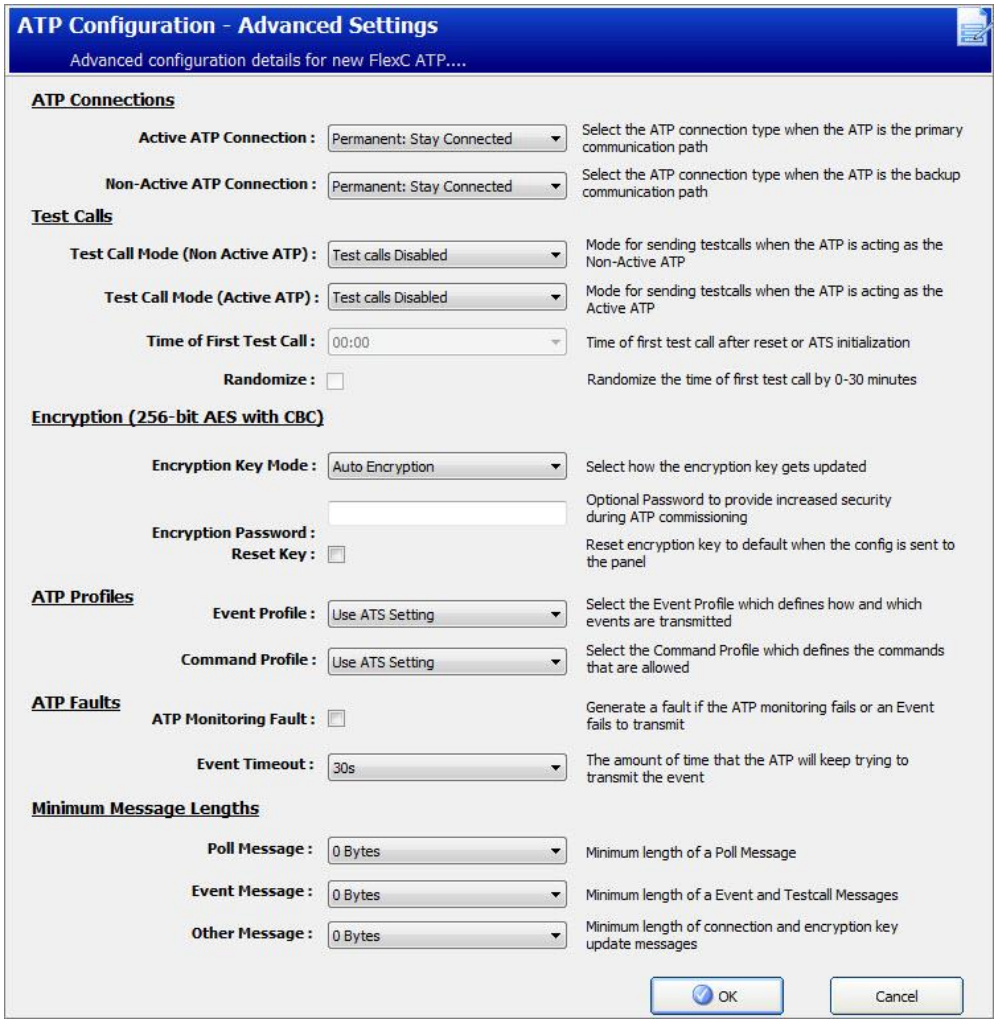
Panel Identification	
ATP Sequence No.	This field displays the sequence number of the ATP in the ATS configuration. Number 1 is primary, numbers 2 - 10 are backup.
ATP Unique ID	When you save an ATP, the system assigns a unique ID to an ATP. This is the unique ID of the ATP so it can be recognised by the RCT.
ATP Name	Enter a name for the ATP.
SPT Account Code	Enter a number to uniquely identify the panel to the RCT.
RCT Identification	
RCT ID	Enter the number that uniquely identifies the RCT (for example, SPC Com XT) to the panel. This

	must match the number entered in the field **Server RCT ID** in the SPC Com XT Server Configuration Manager tool.
RCT URL or IP Address	Enter the URL or IP address of the RCT (for example, SPC Com XT).
RCT TCP Port	Enter the TCP Port that the RCT (for example, SPC Com XT) listens on. The default is 52000. This must match the value in the field **Server FlexC Port** in the Server Configuration Manager tool. See the *SPC Com XT Installation & Configuration Manual*.
ATP Interface	
Communications Interface	From the dropdown list, select the interface this ATP uses for communication. ● Ethernet ● GPRS: Modem 1 ● GPRS: Modem 2 ● Dial Up Internet: Modem 1 ● Dial Up Internet: Modem 2
ATP Category	Select the category to apply to this ATP. For information on ATP Categories, see ATP Category Timings [→ 270].
Advanced	
Advanced ATP Settings	It is not recommended to change advanced settings. Changes must only be made by expert users.

14.6.2.1.1 Configure Advanced ATP Settings

	**⚠ WARNING**
	It is not recommended to change Advanced ATP Settings. Changes must only be made by expert users.

1. Click the **Advanced ATP Settings** button.



1. Configure the fields described in the table below.
2. Click **Save**.

ATP Connections	
Active ATP Connection	Select the ATP connection type when the ATP is operating as the primary communication path. ● Permanent: Stay Connected ● Temporary: Hangup 1second ● Temporary: Hangup 20 second ● Temporary: Hangup 80 second ● Temporary: Hangup 3 minutes ● Temporary: Hangup 10 minutes ● Temporary: Hangup 30 minutes
Non-active ATP Connection	Select the ATP connection type when the ATP is operating as a backup communication path. ● Permanent: Stay Connected ● Temporary: Hangup 1second ● Temporary: Hangup 20 seconds ● Temporary: Hangup 80 seconds ● Temporary: Hangup 3 minutes ● Temporary: Hangup 10 minutes ● Temporary: Hangup 30 minutes

Test Calls	
Test Call Mode (Non Active ATP)	Select the mode for sending test calls when the ATP is the non-active ATP. ● Test calls Disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 4 hours ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days
Test Call Mode (Active ATP)	Select the mode for sending test calls when the ATP is the active ATP. ● Test calls Disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 4 hours ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days Test call every 30 days
Encryption (256-bit AES with CBC)	
Encryption Key Mode	Select how the encryption gets updated. ● Auto Encryption ● Auto Encryption with Updates ● Fixed Encryption Note: Auto Encryption uses the default key and updates it once. Auto Encryption with Updates changes the encryption key every 50,000 messages or once per week, whichever comes first.
Encryption Password	Optional password used to provide increased security during initial ATP commissioning. The password must be entered at the SPT or RCT independently.
Reset Encryption	Reset the Encryption Key and password to the default values.
ATP Profiles	
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. ● Use ATS Setting ● Default Event Profile ● All events
Command Profile	Select the Command Profile which defines the commands that are allowed on this ATS. ● Use ATS Setting ● Default Command Profile ● Custom Command Profile
ATP Faults	
ATP Monitoring Fault	Select to generate an ATP fault if the ATP monitoring fails or an event fails to transmit on the ATP.

Event Timeout	The amount of time that the ATP will keep trying to transmit the event until the event fails on the ATP and is passed to the next ATP. ● 30 seconds ● 60 seconds ● 90 seconds ● 2 minutes ● 3 minutes ● 5 minutes ● 10 minutes
Minimum Message Lengths	
Poll Message	Minimum length of a poll message. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes
Event Message	Minimum length of an event and test call message. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes
Other Message	Minimum length of connection and encryption key and update messages. ● 0 Bytes ● 64 Bytes ● 128 Bytes ● 256 Bytes ● 512 Bytes

14.6.2.2 Add ATP to Analog ARC

If a connection between the SPC panel and RCT (e.g. SPC Com XT) goes down, FlexC has the ability to switch to a backup ATP connection between the SPC panel and an Analog ARC. You can configure up to 10 ATPs for each ATS.

1. To configure an ATP between an SPC panel and an Analog ARC, click the button **Add ATP to Analog ARC**.
2. Complete the ATP fields described in the table below.
3. Click **Save**.

Panel Identification	
ATP Sequence No.	This field displays the sequence number of the ATP in the ATS configuration. Number 1 is primary, numbers 2 - 10 are backup
ATP Unique ID	This ID uniquely identifies the ATP to the RCT
ATP Name	Enter a name for the ATP
SPT Account Code	Enter a number to uniquely identify the panel to the RCT (1 - 999999)
ARC Connection	

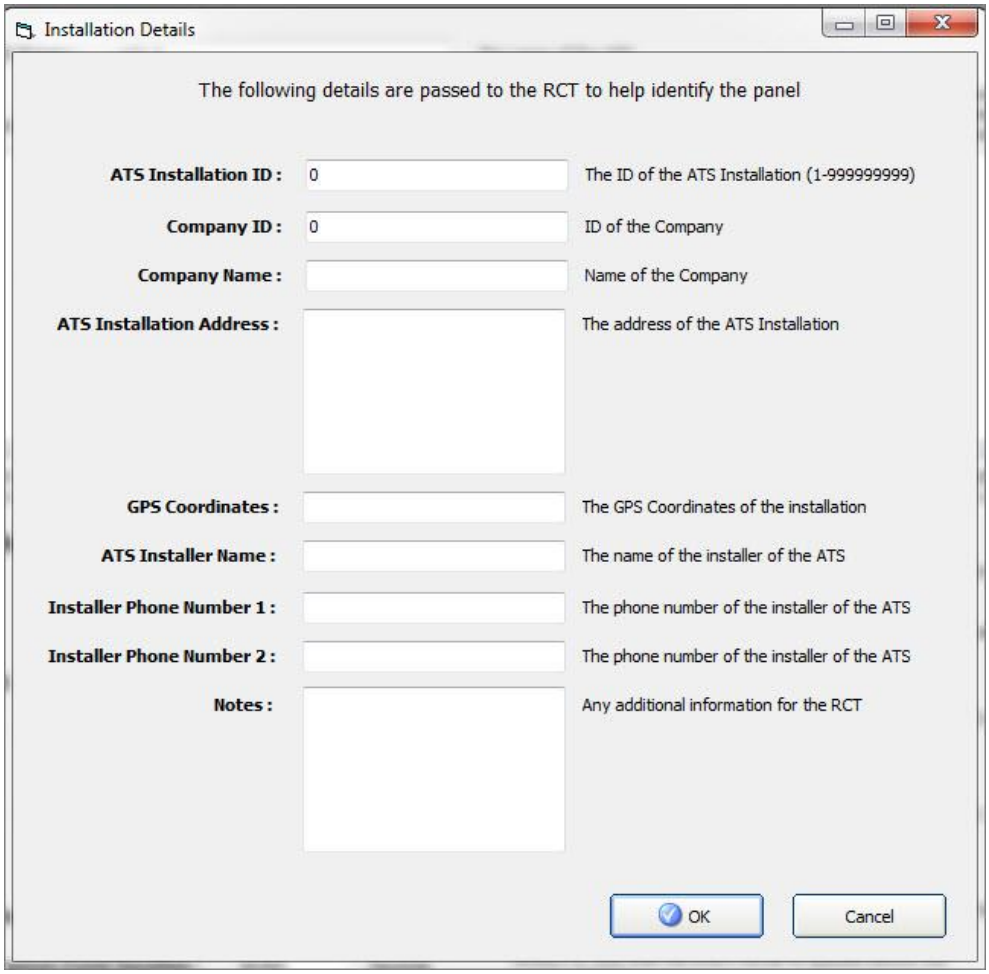
Number 1	Phone number 1
Number 2	Phone number 2
Modem Select	Select the modem to be used. ● Modem 1 ● Modem 2
Test Calls	
Test Call Mode (Non-active ATP)	Select the mode for sending test calls when the ATP is in non-active mode. Default: 24 hours. ● Test calls disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days.
Test Call Mode (Active ATP)	Select the mode for sending test calls when the ATP is an active ATP. Default: 24 hours. ● Test calls disabled ● Test call every 10 minutes ● Test call every 1 hour ● Test call every 24 hours ● Test call every 48 hours ● Test call every 7 days ● Test call every 30 days.
Time of first test call	Time of first test call after reset or ATS initialization. ● Send Immediately (default) ● or ● Select a half hour interval between 00:00 and 23:30
Event Protocol	
Protocol	Protocol used in communication. ● SIA ● SIA Extended 1 ● SIA Extended 2 ● Contact ID
Event Profile	Select the Event Profile which defines how and which events are transmitted on this ATS. ● Use ATS Setting ● Default Event Profile ● Default Portal Event Profile ● All events ● Custom Event Profile
ATP Faults	
ATP Monitoring Fault	Select to generate an ATP fault if the ATP monitoring fails or an event fails to transmit on the ATP.
Event Timeout	The amount of time that the ATP will keep trying to transmit the event until the event fails on the ATP and is passed to the next ATP. Default: 2 minutes. ● 30 seconds ● 60 seconds

	• 90 seconds • 2 minutes • 3 minutes • 5 minutes • 10 minutes

14.6.2.3 Edit Installation Details

The installation details are passed to the RCT to help the operator to identify the panel.

1. Click the **Edit Installation Button**.



1. Complete the fields in the table below.
2. Click **Save**.

ATS Installation ID	The ID of the ATS Installation (1 - 999999999).
Company ID	For future use.
Company Name	Name of the company.
ATS Installation Address	The address of the ATS installation.
GPS Coordinates	The GPS coordinates of the installation.
ATS Installer Name	The name of the installer of the ATS.
Installer Phone Number 1	The phone number of the installer of the ATS.
Installer Phone Number 2	The phone number of the installer of the ATS.
Notes	Any additional information for the RCT.

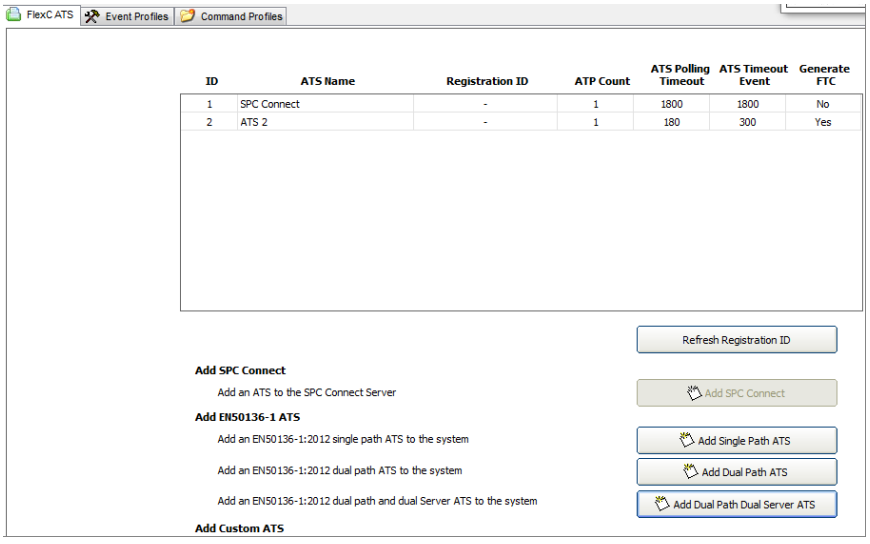
14.6.3 Configuring an SPC Connect ATS

The **Add SPC Connect** ATS functionality opens a communication between the panel (SPT) and the **SPC Connect** server (RCT), www.spcconnect.com. Using the generated SPC Connect ATS Registration ID, a panel user can register a user account and panel with the SPC Connect website to access their panel remotely.

1. To configure an SPC Connect ATS, go to **Communications - FlexC - FlexC ATS**.
2. In the ATS Configuration screen, click **Add SPC Connect** to open a communication path with the SPC Connect server.

⇨ An SPC Connect ATS is added to the **Event Sequence Table** with the following attributes:

- SPC Connect ATS Registration ID
- Default ATP over Ethernet. For information on ATP fields, see Add ATP to FlexC RCT [→ 172]
- Default Events Profile for SPC Connect
- Default Commands Profile for SPC Connect
- Default RCT URL is www.spcconnect.com
- The SPT Account Code for the ATP is populated.
- Make a note of the SPC Connect **ATS Registration ID** and provide this to the customer along with the *SPC Connect User Guide*.

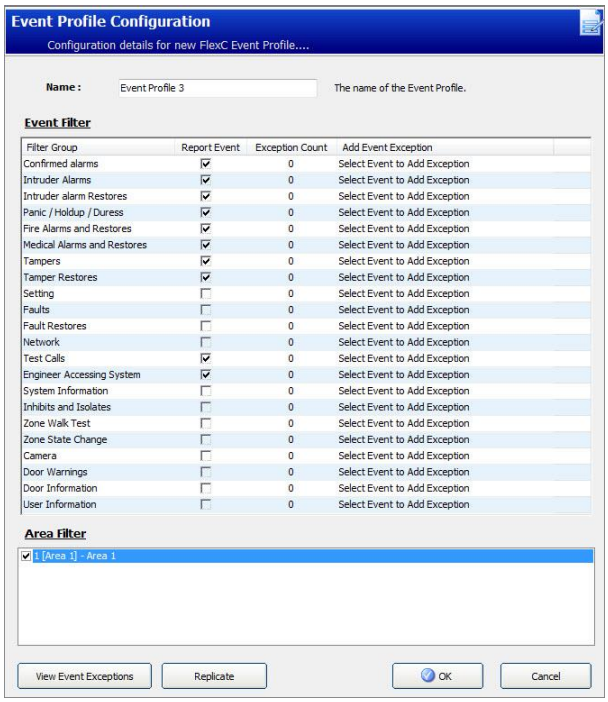


14.6.4 Configuring Event Profiles

The event profile defines which events are transmitted on an ATS, the reporting status for an event and event exceptions. Event exceptions allow you to remap default values for events to customised values. For more information, see Event Exception Definition [→ 182].

!	*NOTICE*
	To quickly create a new event profile, go to **Communications - FlexC - Event Profiles**. In the **Event Profiles** table, select an event profile and click the edit button (blue pencil). Scroll to the bottom of the screen and click **Replicate.** You can now make the changes you require.

1. To configure FlexC event profiles step by step, go to **Communications - FlexC - Event Profiles**.
2. Click **Add**. The **Event Profiles** window displays.



1. Enter a **Name** to identify the event profile.
2. Select the event filter groups to report for this profile by ticking the **Report Event** checkboxes.
3. To prevent reporting of certain events or addresses within an event, select the event from the corresponding **Add Event Exception** dropdown list.
4. Click **Add** to view the **Event Exception Definition** screen. See Event Exception Definition [→ 182].
5. To apply an event profile to an area, select the area under **Area Filter**.
6. Click **Save** and **Back**. The new profile displays in the **Event Profiles** table.

i	You can view a list of all event exceptions for an event profile under **Event Exceptions** on the **Event Profiles** screen.

	NOTICE
	You cannot delete the **Default Event Profile, the Default Portal Event Profile** or an event profile that is assigned to an ATS. If you try to delete an event profile that is in use, you will get an error.

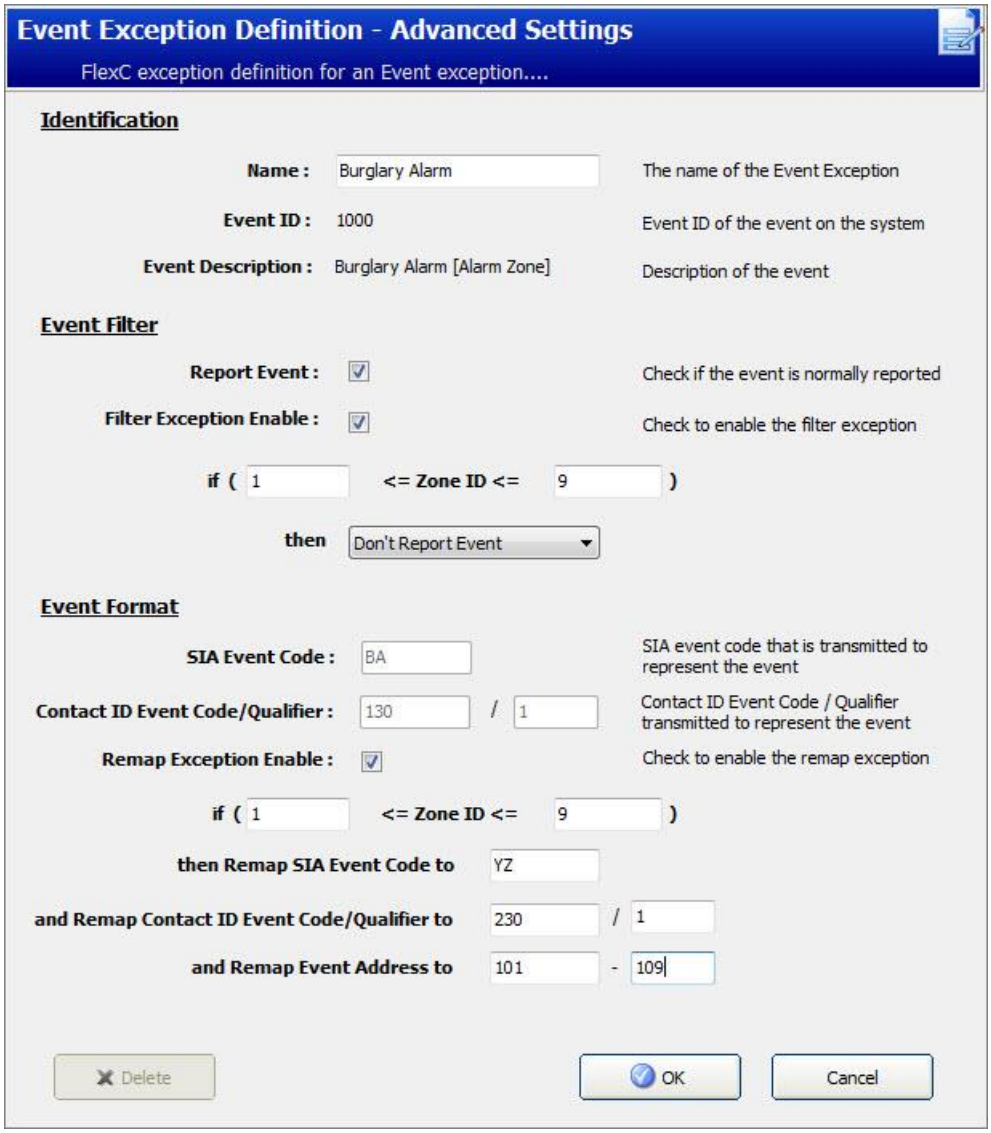
14.6.4.1 Event Exception Definition

Event exceptions allow you to change the following settings for a range of addresses within an event:

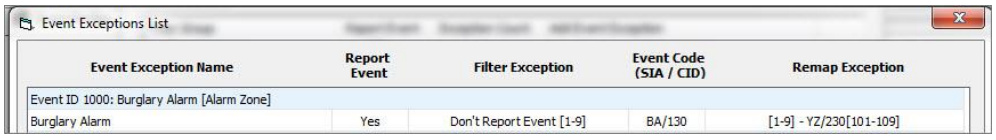
- Report Event
- SIA Code
- CID Code
- Event Address (e.g. Zone IDs, Area IDs, User IDs)

For example, in the Filter Group **Intruder Alarms** you could define an event exception for a range of Zone IDs in the Burglary Alarm (BA) event as follows:

- Do not report BA events for Zone ID 1 - 9
- Remap the SIA Code from BA to YZ
- Remap the CID from 130 / 1 to 230 / 1
- Remap the Zone ID 1 - 9 to Zone ID 101 - 109



1. To configure an **Event Exception Definition**, complete the fields described in the table below.
2. Click **Save**.
3. Click **Back** to return to the **Event Profiles** screen.
   ⇨ The name of each exception displays in the **Event Exceptions** table at the bottom of the screen. The table shows the settings for the fields **Report Event**, **Filter Exception**, **Event Code (SIA/CID)** and **Remap Exception** for the event.



1. Click the **Edit** icon to make changes or the **Delete** icon to remove an **Event Exception**.
2. To apply the event profile to an area, select the area checkbox.
3. Click **Save** to save the event profile.

4. Click **Back** to view the profile in the **Event Profiles** table.

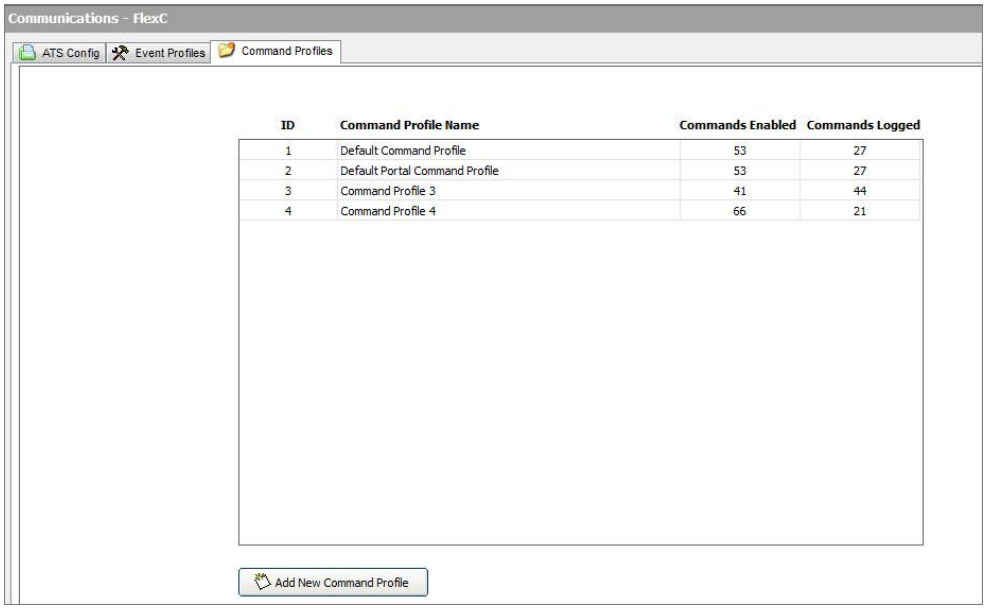
Identification	
Name	Enter the name of the Event Exception.
Event ID	Event ID of the event on the system. This is display only.
Event Description	Description of the event. This is display only.
Event Filter	
Report Event	Check to report the event. This overrides the reporting value set for the event Filter Group. For example, if the Filter Group **Intruder Alarms** is set to report, you can exclude the BA event or by disabling this setting.
Filter Exception Enable	Check to exclude a range of addresses, for example Zone IDs, from the **Report Event** field setting.
if (0 ≤ *Zone ID* ≤ 9999) then Report Event/Don't Report Event	Enter a range of addresses to exclude from the **Report Event** setting. For example, if you choose to report the event type BA, you may choose not to report *Zone ID 1 - 9* for that event. Alternatively, if you choose not to report the event type BA, you may choose to report *Zone ID 1- 9* for that event.
Event Format	
SIA Event Code	Default SIA event code that is transmitted to represent the event. This field is display only.
Contact ID Event Code / Qualifier	Default Contact ID Event Code / Qualifier transmitted to represent the event. This field is display only.
Remap Exception Enable	Check to remap the default SIA, CID code / Qualifier and Event Address to customised values, for example, to remap *Zone ID 1 - 9* to *Zone ID 101 - 109*. When enabled, the fields below display.
if (0 ≤ *Zone ID* ≤ 9999)	Enter the range of addresses to remap for an event, for example, if you want to remap *Zone ID 1 - 9* to *Zone ID 101 - 109*, enter *1* and *9*. The quantity of addresses in the range must be equal to the quantity of addresses defined in the field **Remap Event Address** below.
then Remap SIA Event Code to BA	Remap the default SIA code to a customised SIA code.
and Remap Contact ID Event Code / Qualifier to	Remap the default CID Event Code / Qualifier to a customised CID Event Code / Qualifier.
and Remap Event Address to	Enter the new range of addresses, for example, if you are remapping *Zone ID 1 - 9* to *Zone ID 101 - 109*, enter *101 and 109*.

14.6.5 Configuring Command Profiles

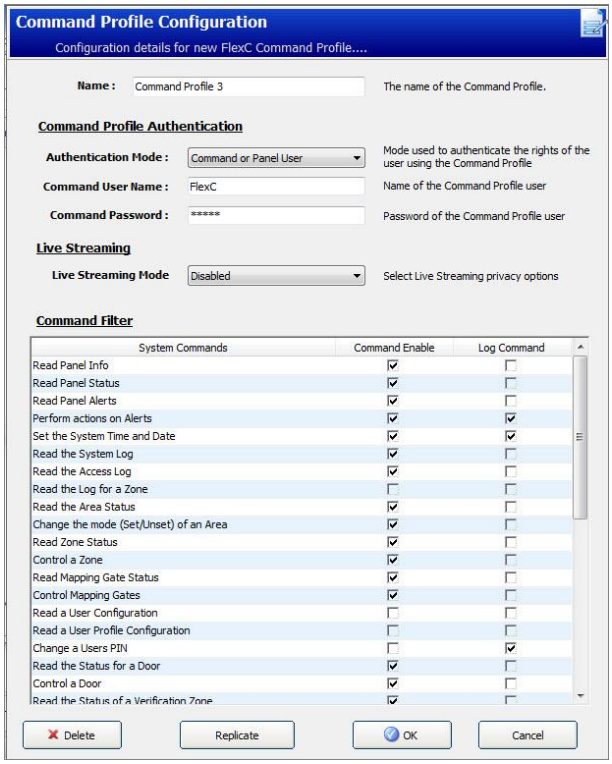
The command profile defines the commands that are allowed on an ATS. This profile determines how a CMS can control a panel. The default command profile does not support video verification.

!	*NOTICE*
	To quickly create a new command profile, go to **Communications - FlexC - Command Profiles**. In the **Command Profiles** table, select a command profile and click the edit button (blue pencil), Scroll to the bottom of the screen and click **Replicate**. You can now make the changes you require.

- To add a command profile step by step, go to **Communications - FlexC - Command Profiles**.



- Click **Add**.



1. Enter a **Name** to identify the command profile.

2. Select an **Authentication Mode** (Command User or Panel User, Command User Only, or Any Panel User) from the dropdown menu.

!	*NOTICE*
	The default **Command User Name** provides an out of the box user that quickly and easily enables control of the panel from SPC Com XT. It enables a broad range of commands. For example, the default command user can set all areas or control all zones. For tighter control, for example to only allow setting of certain areas, you can set up a customised command profile with a defined set of rights. You cannot delete the **Default Command Profile**, the **Default Portal Command Profile** or a command profile that is assigned to an ATS.

3. Enter the name of the command profile user in the **Command User Name** field. This must match the **Authentication User Name** field in SPC Com XT.
4. Enter the password of the command profile user in the **Command Password** field. This must match the authentication **User PIN or Password** field in SPC Com XT.
5. Select the **Live Streaming Mode** (Disabled, Only after alarm event, Always available, System is fullset) to determine the streaming privacy options. **Always Available** generates the highest volume of data.
6. Under **Command Filter**, select the commands to enable. For a full list of commands, see FlexC Commands [→ 268].
7. Select the commands to log.
8. Click **Save**.
9. Click **Back** to view the command profile in the **Command Profiles** table.
10. To change a command profile, click the **Edit** button (pencil icon) next to a command profile.

15 Communications Settings

15.1 Ethernet

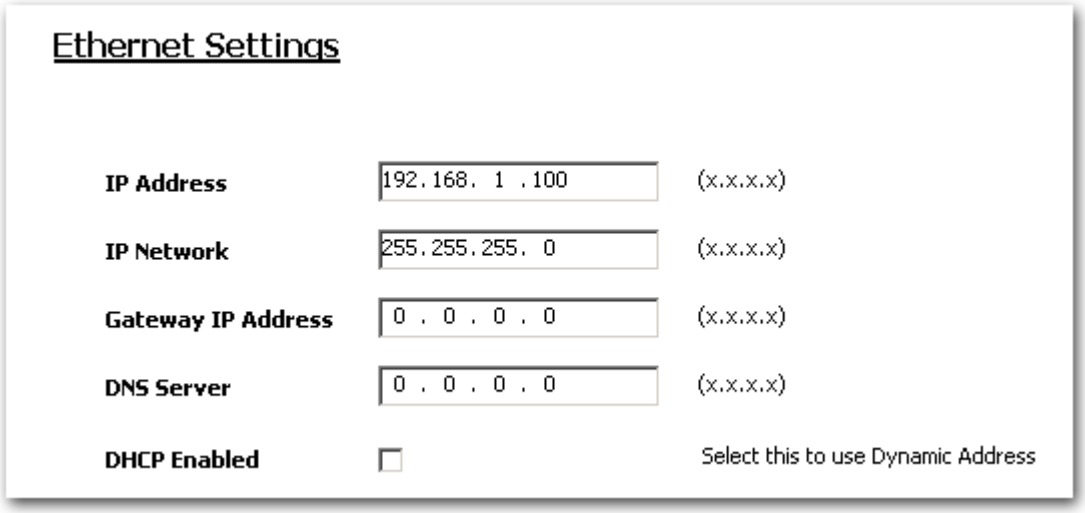
IP

If you intend to program settings for the SPC controller Ethernet interface while it is connected to an existing **L**ocal **A**rea **N**etwork (LAN), please consult the network administrator for that LAN.

Communications

Network Settings

1. Select the tab **Ethernet**.
   - ⇨ An Ethernet connection with the controller can be established using a direct connection or a LAN connection. See page [➙ 253].
   - ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.



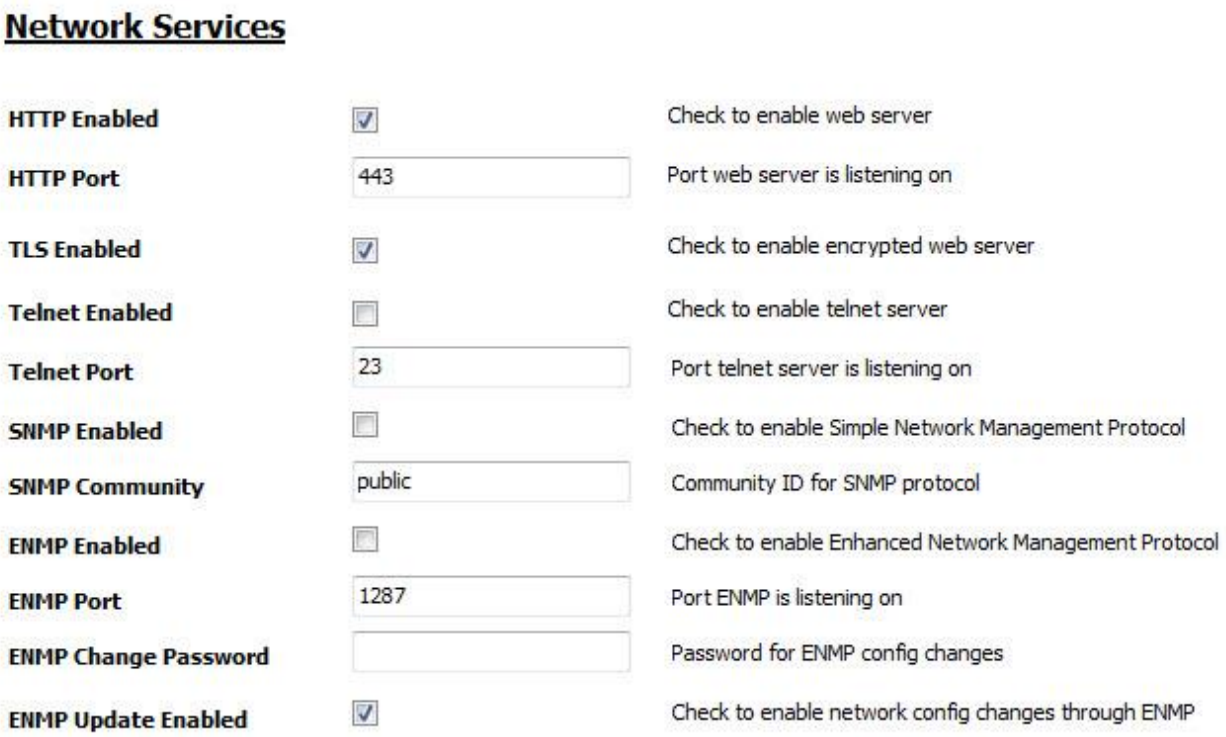
IP address	Enter the IP address of the panel.
IP Network	Enter the subnet mask that defines the type of network address structure implemented on the Local Area Network (LAN).
Gateway IP Address	Enter the IP address of the IP gateway if one exists. This is the address that IP packets will be routed through when accessing external IP addresses on the internet.
Enable DHCP	Click this Button to enable dynamic address assignment on the panel.
DNS Server	Enter the IP address of the DNS server.

15.2 Configuring the networking services of the panel

Communications

Network Settings

1. Select the tab **Services**.
   ⇨ The following window will be displayed.
2. Configure the fields as described in the table below.



HTTP Enabled	Tick this box to enable the embedded web server on the panel.
HTTP Port	Enter the Port number that the web server is 'listening' on. By default this is set to 443.
TLS Enabled	Tick this box to enable encryption operation on embedded web server. By default this is enabled. With TLS enabled, web pages can only be accessed by using 'https://' prefix before typing the IP address.
Telnet Enabled	Tick this box to enable the Telnet server. (Default: Enabled) **Note**: Using Telnet without a comprehensive knowledge can damage the controller configuration; this should only be used if the user has sufficient knowledge or is being instructed by someone with such knowledge.
Telnet Port	Enter the number of the Telnet port.
SNMP Enabled	Tick this box to enable Simple Network Management Protocol (SNMP). (Default: Disabled)
SNMP Community	Enter the Community ID for the SNMP protocol. (Default : Public)
ENMP Enabled	Tick this box to enable Enhanced Network Management Protocol (ENMP). (Default : Disabled)
ENMP Port	Enter the ENMP port number (default: **1287**).
ENMP Change	Enter the password for the ENMP protocol

Password	
ENMP Update Enabled	Check this box to enable network changes to be made with ENMP protocol.

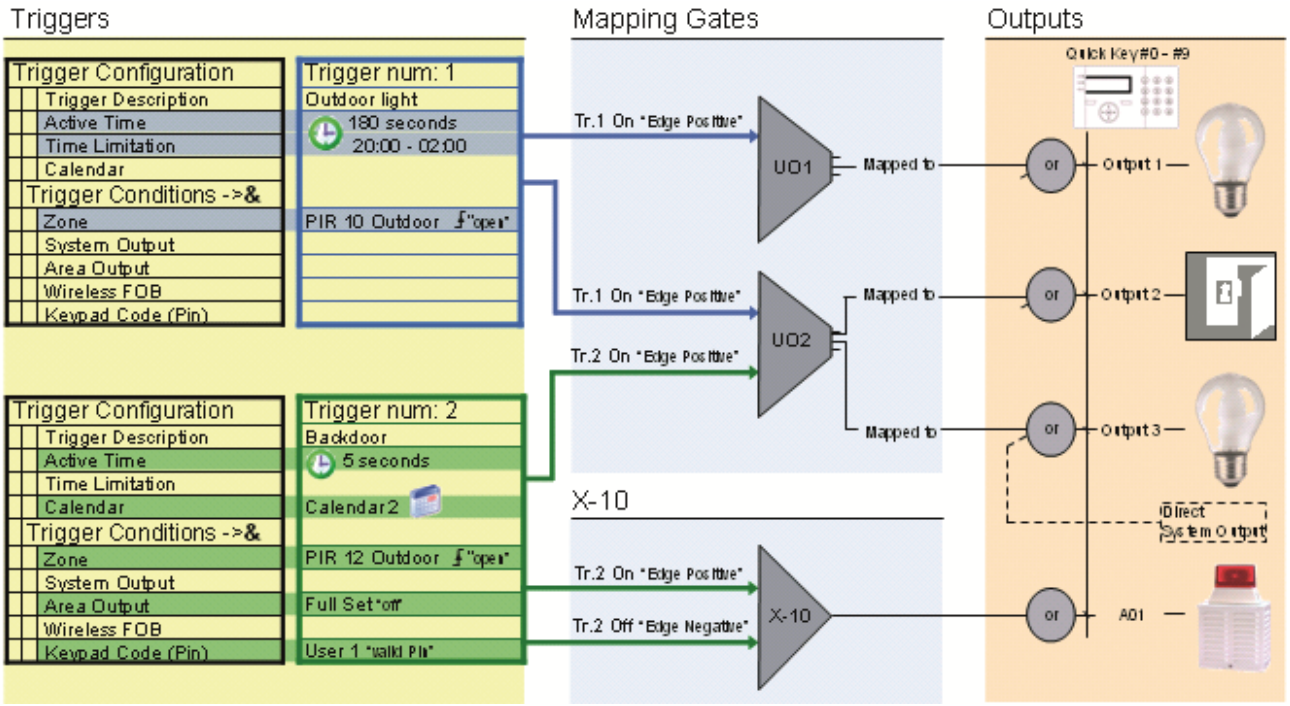
16 Configuring advanced settings

16.1 Cause & Effect

Cause & Effect refers to a set of interrelated features and functionality that have in common the evaluation of a logical (or virtual) output as a function of inputs or conditions, which may in some cases result in an effect.

The SPC Cause & Effect functionality encompasses scheduling with calendars, triggers, user outputs, physical outputs, zones, areas, keypads, X10 and user access. Specifically calendars and triggers carry most of the Cause & Effect functionality.

Function	Description
Calendars	Scheduling. This area controls user access to the panel and keypad operation and enables zones and physical outputs. Instrumental in auto-setting of areas and time-control of triggers.
Triggers	Intermediate outputs used to group logical and time conditions. Can in turn be used by X10 and user-defined outputs.
Mapping Gates	Virtual outputs defined by the user for logical control. Can be mapped to physical outputs to control actual devices.
X10 outputs	Virtual outputs used to control X10 devices. An X10 transmitter must be connected to the first serial port of the SPC panel.
Physical outputs	Ability to control external devices.
Keypad shortcuts	Ability to control user-defined outputs and X10 outputs.
SPC Pro	PC application used to configure, monitor and control a SPC panel, both remotely or locally. Ability to change X10 states and user-defined outputs.

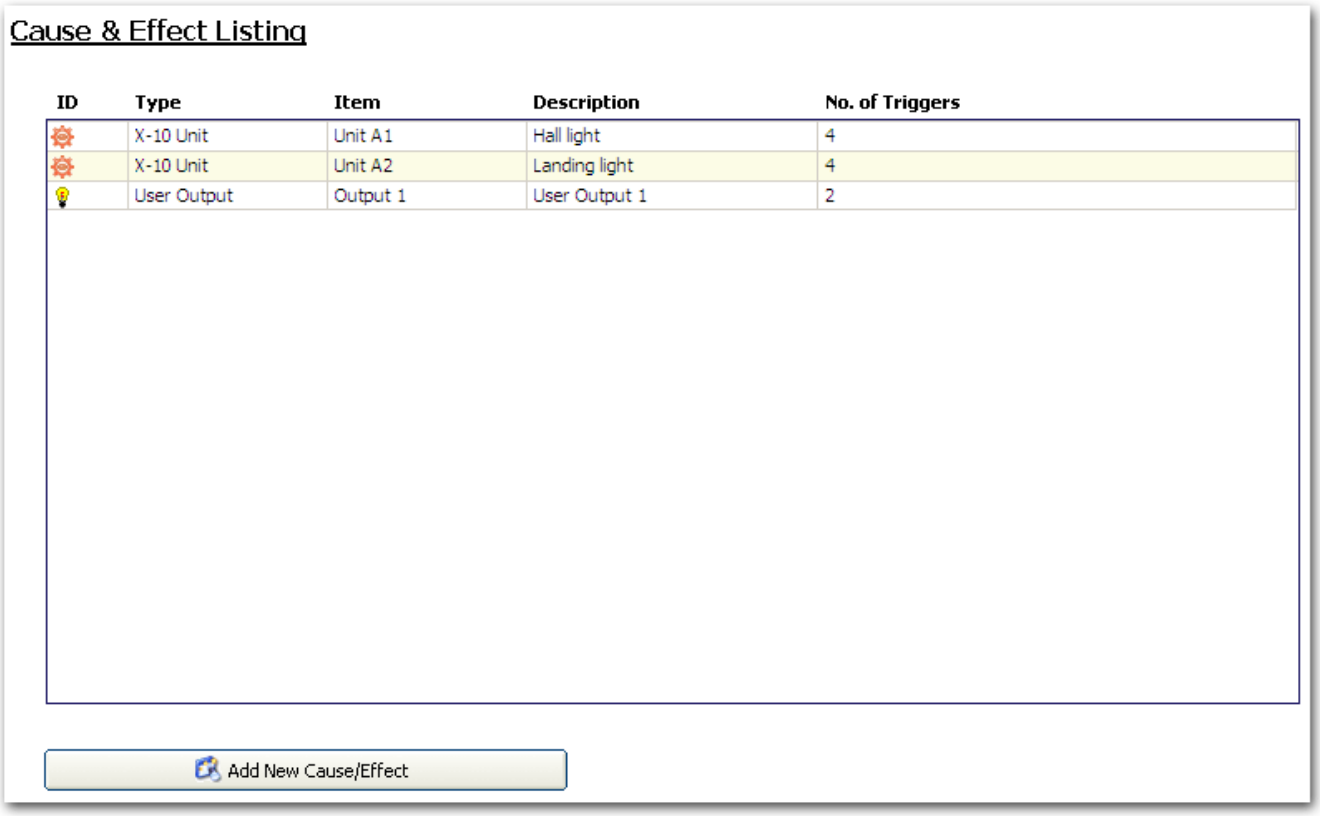


16.1.1 Adding a Cause & Effect

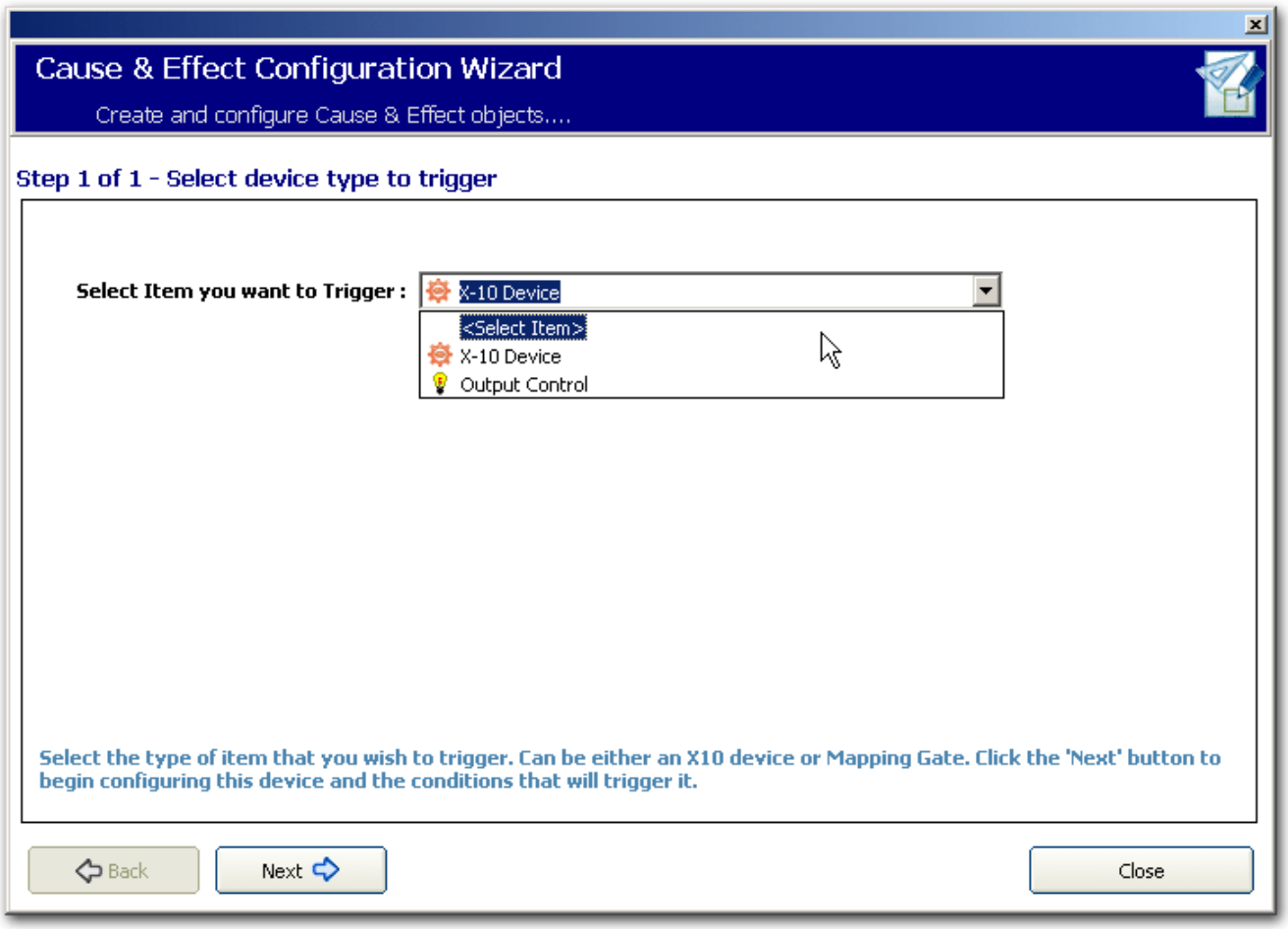
Advanced

Cause & Effect

1. Click the tab **Cause/Effect List**.
   ⇨ The following window will be displayed:



2. Click the button **Add New Cause/Effect**.
   ⇨ The following window will be displayed.
3. Configure the fields as shown in the table below.



4. Select the device type.

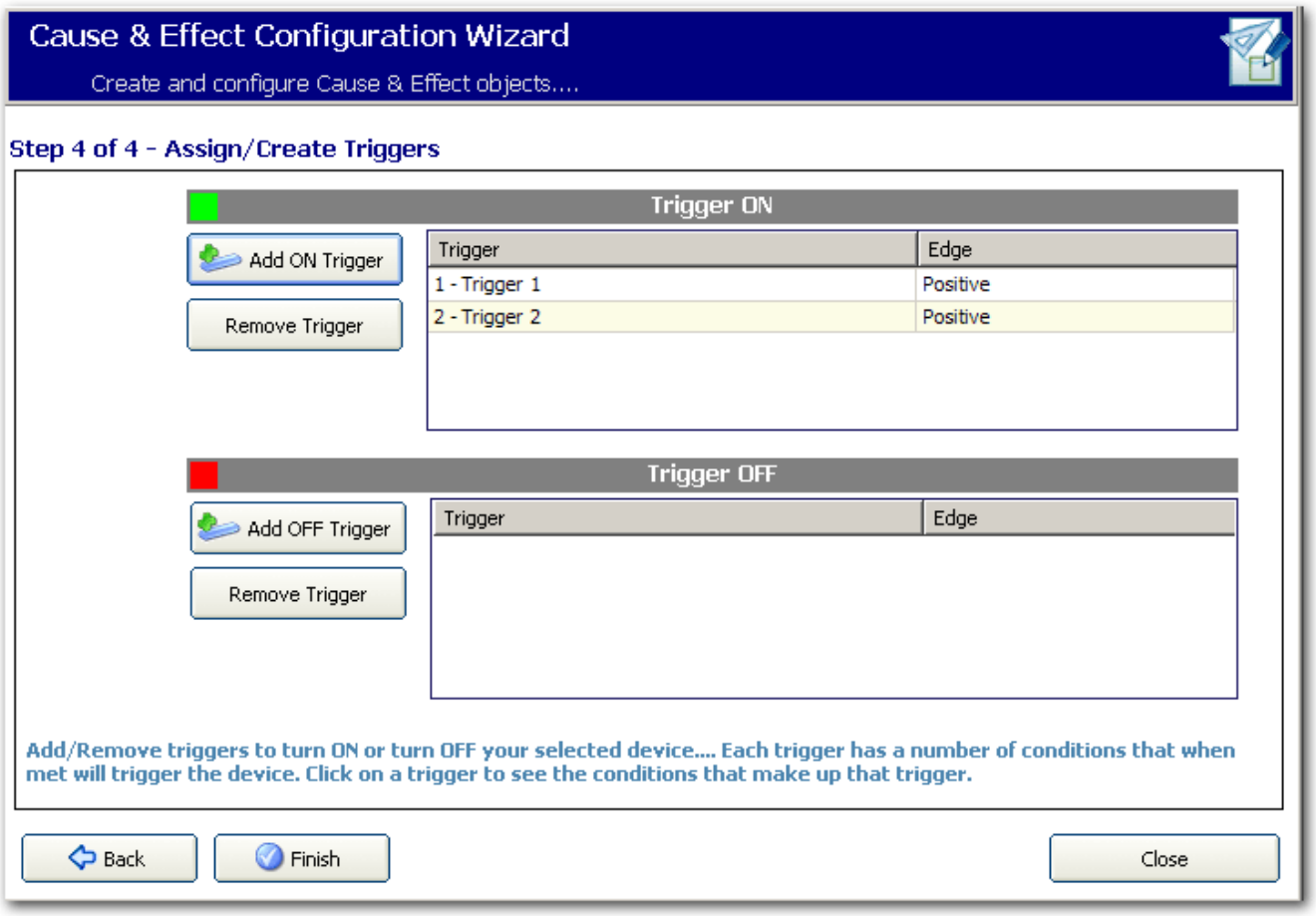
Cause & Effect Configuration Wizard		
Step 1	Select the device type X10 or Output Control.	
	X10 Device	**Output Control**
Step 2	Select a X10 device.	Select a user output from the list.
Step 3	Enter a description for the X10 device. Assign a keypad key number (optional).	Enter a description for the user output. Assign a keypad key number (optional).
Step 4	Assign/Create a trigger [→ 192].	Map user output to expander output.
Step 5		Assign/Create triggers [→ 192].

16.1.2 Assigning / Creating a trigger

Advanced

Cause & Effect

▷ You are in Cause & Effect Configuration Wizard Step 4 (X10) or Step 5 (Output Control) Assign/Create Triggers.



1. Click the button **Add ON Trigger** or the button **Add OFF Trigger**.
   ⇨ The following window will be displayed:

2. Click the button  to create a new trigger

–OR-

Mark a trigger from the list and click the button  to edit the selected trigger.

3. For further programming refer to page [➙ 197].

16.2 Calendars

Calendars are used for scheduling time-based control for multiple panel operations as follows:

- Automatic setting and/or unsetting of areas
- Automatic setting and/or unsetting of other panel operations including triggers, enabling of users, zones, physical outputs, etc.

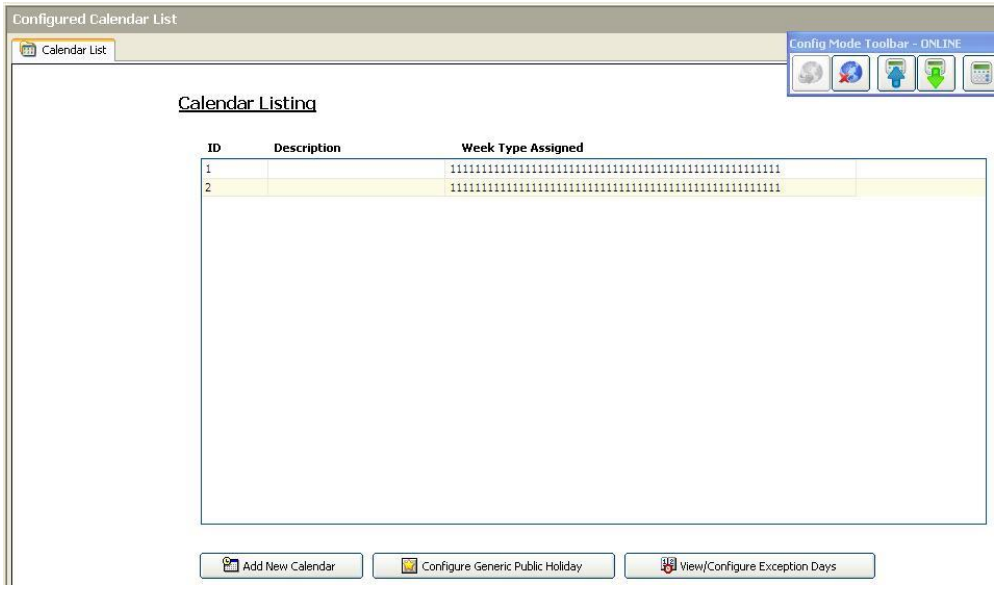
At any particular time, any schedule within the calendar can be ‘active’ if its time conditions are satisfied.

Each week of the year is assigned an ordinal number. Depending on the fall of days within a month, there may be 52 or 53 weeks in one year. The SPC calendar implementation conforms to the ISO8601international standard.

Configuring calendars

Advanced  Calendars

A list of configured calendars is displayed:



Performable actions

Add New Calendar	Create a new calendar.
Configure Generic Public Holiday	Configure setting schedules for a public holiday that is generic to all calendars.
View/Configure Exception Days	Configure setting schedules for exceptional circumstances outside of the normal weekly schedules

16.2.1 Automatic setting/unsetting of areas

A calendar can be configured for area auto-sets or auto-unsets.

For any day of the week, a configuration can have a maximum of 4 set times and 4 unset times. Configured times use the 24 hour clock (hh:mm). If the hour is 24, then minutes must be 00, such as midnight is 24:00. It is possible to define a set time without an unset and vice-versa. Configured times trigger the area to either set or unset (provided all conditions are satisfied). Times entered are not considered as a duration of time, rather they are a point in time that said action (set/unset) will occur. If the controller is powered up or reset, the set/unset status is kept and subsequent set or unset times occur according to configuration.

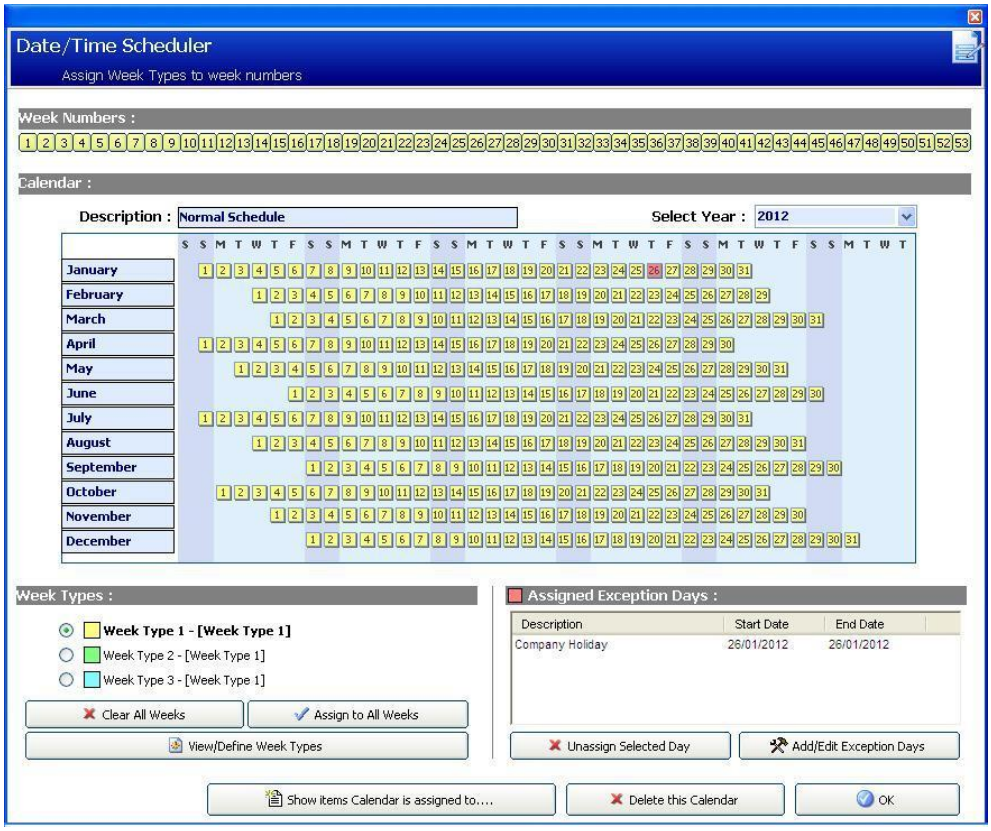
16.2.2 Automatic setting/unsetting of other panel operations

Panel operations including triggers, enabling of users, zones, physical outputs can be automatically set or unset using On/Off, True/False or Active/Inactive state configurations.

On/Off, True/False or Active/Inactive states can be assigned to an output that effectively turns on or off and can be configured for any day of the week. State configurations have a maximum of 4 set times and 4 unset times. Configured times use the 24 hour clock (hh:mm). If the hour is 24, then minutes must be 00, such as midnight is 24:00. Each configuration consists of a pairing of settings for On/Off, True/False, Active/Inactive states. Any one setting without a respective corresponding setting is disregarded.

16.2.3 Adding / Editing a calendar

1. Click the button **Add New Calendar**.
   ⇨ The following window will be displayed:



2. Provide a **Description** of the calendar (max. 16 characters)
3. Select a **Year**.

Week Types

Calendars are configured by assigning an optional Week Type for each calendar week. Up to three Week Types may be defined for each calendar. Not all weeks must have a Week Type (i.e. a Week Type may be 'None'). There is a system maximum number of 64 calendar configurations.

To configure a week type

1. Click the button **View/Define Week Types**.
   ⇨ Up to three week types may be configured.
2. Click on a week day to open the Week Type configuration dialog.
3. Enter the desired times for setting / unsetting or for triggers. Use time guidelines for Automatic Setting/Unsetting of Areas (see page [➞ 195]), or for Automatic Setting/Unsetting of other Panel Operations (see page [➞ 195]).
4. Click **Save.**

1. **To assign a week type to a calendar**
2. Click on the required **Week Number** at the top of the calendar or click on the required week(s) on the calendar.
3. Click on the desired week type in the **Week Types** section for the scheduled week. For example, a Week Type that is configured for Christmas scheduling would normally be assigned to Week 51/52.

4. If you wish to assign the Week Type to the whole calendar, click on the **Assign to all Weeks** button.

Click on the **Show items calendars is assigned to** button to display the panel items that are using this calendar.

To delete the displayed calendar, click on the **Delete** button.

Global calendars created using SPC Manager cannot be deleted.

See also

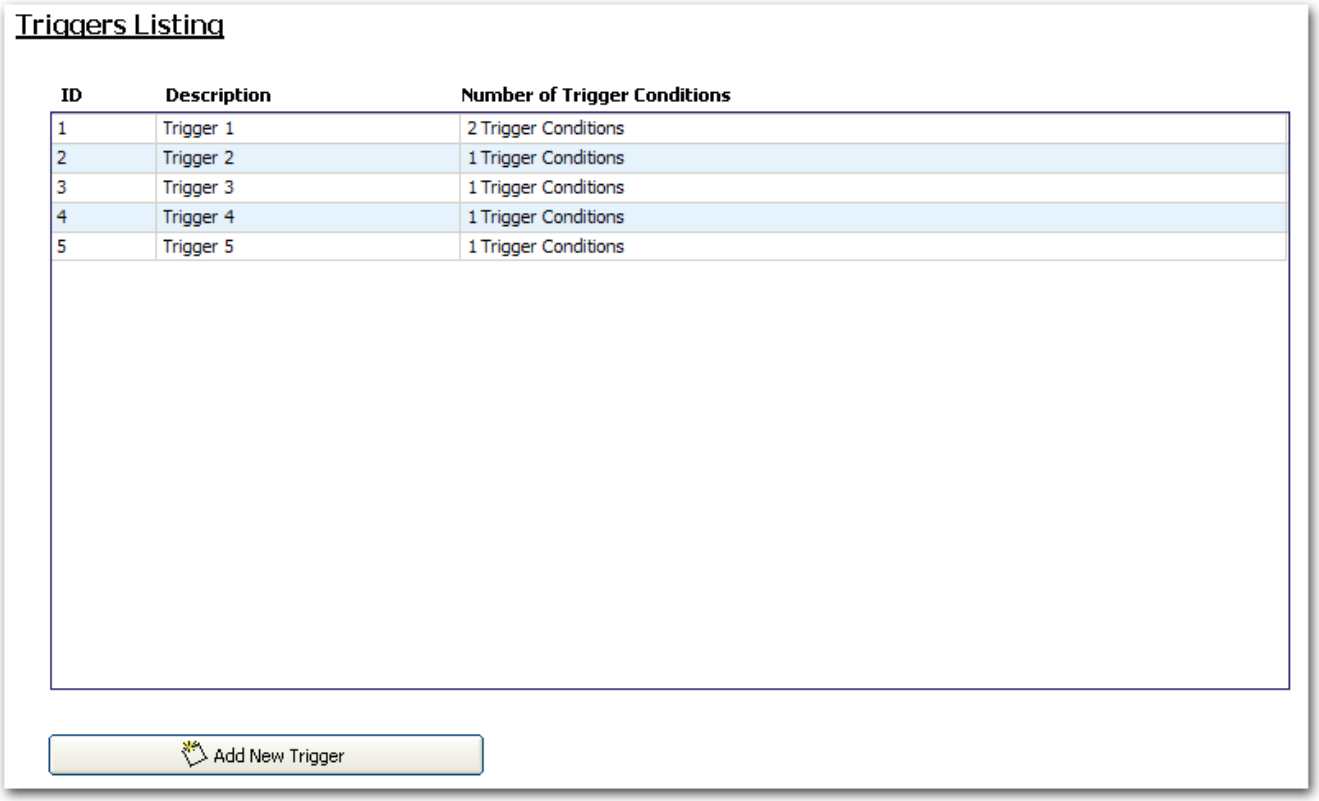
- Automatic setting/unsetting of areas [→ 195]
- Automatic setting/unsetting of other panel operations [→ 195]

16.3 Triggers

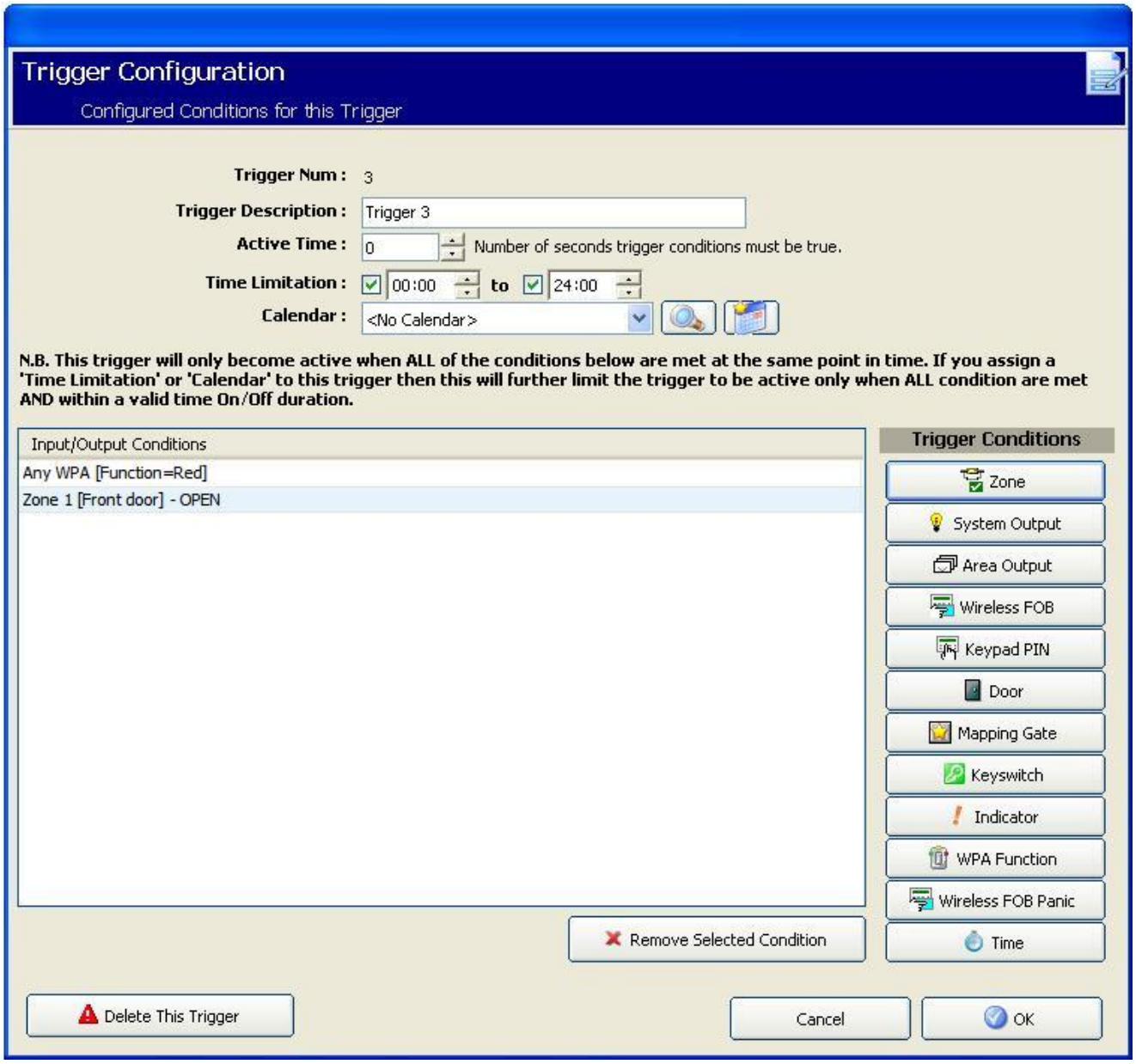
A trigger is a system state (e.g. zone closing / time / system event (alarm) etc.) that can be used as inputs to the Cause & Effects. The triggers can be logically assigned together using the logical operators and / or to create user outputs. The system supports up to a maximum of 1024 triggers across all its Cause & Effects system.

Triggers

1. Click the button **Add New Trigger**.
   ⇨ The following window will be displayed.



2. Click on **the Add New Trigger** button to add new triggers and configure trigger conditions.



3. Configure the fields as described in the table below.

Trigger Num	System generated number for new trigger. Trigger will only become active if one of the 2 optional steps (calendar/time limitation) is configured
Trigger Description	Enter a text description for the trigger
Calendar	Select a calendar, if required. If selected, the trigger will only be in effect during this calendar period. See page [→ 194].
Active Time/Timer	Enter the number of seconds that the trigger conditions must be true before the trigger will activate
Time Limitation	Select a time period between 00:00 and 24:00 during which the trigger will only be in effect. The Start time is inclusive, the end time is exclusive. **Note**: This parameter delays a trigger transition from ON to OFF only; from OFF to ON is immediate.
Trigger conditions	The trigger is ON if the following conditions are satisfied (i.e. a logical AND operation is performed):

	Zone – the trigger is ON if the configured zone is in one of the following states - open, closed, short or disconnected. **Door** – the trigger is ON if the any of the following door options are configured; Entry granted, Entry denied, Exit granted, Exit denied, Door open too long, Door left open, Door forced open, Door normal, Door Locked, Door unlocked **System** - the trigger is on if the system output is in the configured state, which can be on or off. Possible system outputs are “External Bell”, “Alarm”, etc. **Area** - the trigger is ON if the area output is in an ON or OFF state. Possible area outputs are “External Bell”, “Alarm”, etc. **Wireless FOB** – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) presses the ‘*’ key on the FOB, it will cause an instantaneous pulse OFF/ON/OFF. This only applies for FOBs that have been registered with the system. **Wireless FOB Panic** - – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) presses the ‘*’ key on the FOB Panic, it will cause an instantaneous pulse OFF/ON/OFF. This only applies for FOB Panics that have been registered with the system. **WPA** – the trigger is activated if a button or combination of buttons is pressed. It is possible to assign a trigger condition to all WPAs or just to one specific WPA. When a trigger with a WPA trigger condition is defined, it can be assigned to a mapping gate for many purposes including arming a system, turning on lights or opening a door. **Keypad valid PIN** – this condition can be configured for a particular user or for any user. With this configuration, if the configured user (or any user) enters a valid PIN, or presents a configured PACE, it will cause an instantaneous pulse OFF/ON/OFF. **Keyswitch** – the trigger can be configured for a specific key position on the keyswitch. **Time Trigger** –the trigger is on at the specific time entered in the box provided, in the format hh:mm.

⚠ WARNING

Your system will not comply with EN standards if you enable a trigger to set the system without a valid PIN being required.

16.4 Mapping Gates

Triggers are used with Mapping Gates, which are virtual outputs defined by the user that can be mapped to a physical output. There can be a maximum of 512 Mapping Gates.

For continuous output, when the trigger is a valid user code, both states must be the same, either both negative or both positive.

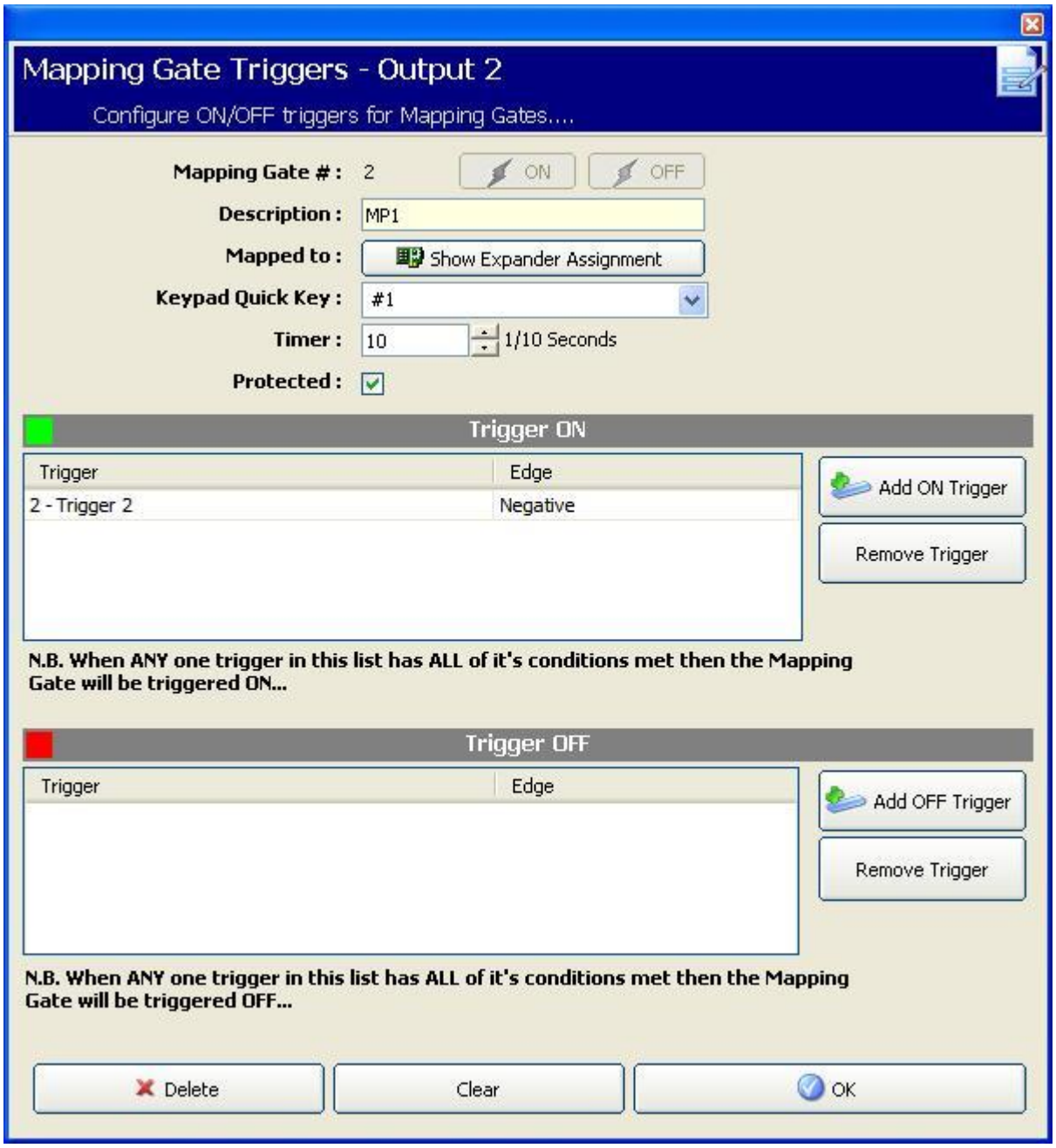
Mapping Gates

The following fields will be presented for each listed device.

- **Output**
- **Keypad**
- **Description**
- **Timers**

- **Triggers**

1. Click an output from the list.
   ⇨ The following window will be displayed:



2. Configure the fields described in the table below and click **OK**.

User Output #	The number is presented for reference and can not be programmed.
Description	Enter a description for the gate. This is important as no mapping gate number, only the description, is displayed on the **Outputs** user page for turning on and off gates
Mapped to	Click the button **Assign now** to get an overview to which controller / expander output the user output is assigned. To create a new controller/expander assignment:, click an output from the list and click the button **Assign selected output as mapping gate #.**
Keypad Quick Key	A quick key is a '#' followed by a single digit pressed at the keypad. If a shortcut is configured and is pressed at the keypad, the user is prompted to turn the

	output on or off

- Click on the **Add ON Trigger** button to configure triggers for turning the output on and turning it off. In both cases, a positive or negative edge of the trigger needs to be defined. See Triggers [→ 197] for details of configuring triggers.

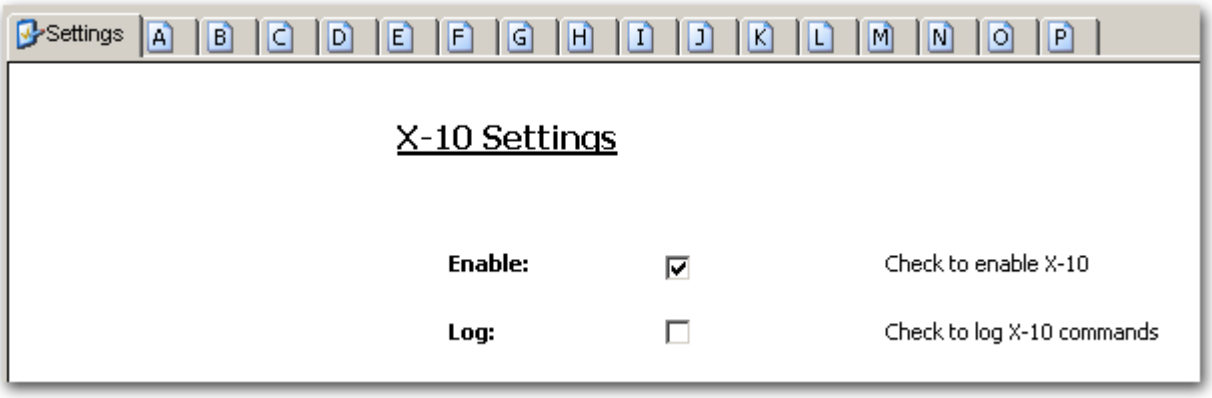
See also

Triggers [→ 197]

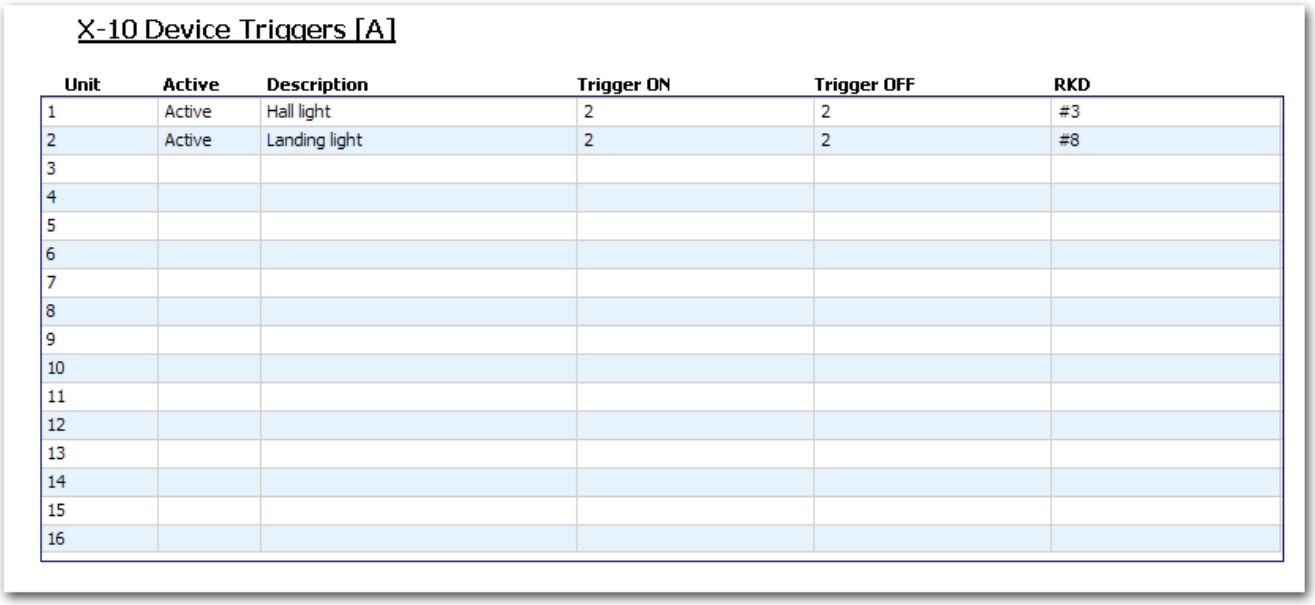
16.5 X10 Config – Settings

The X10 settings window allows you to configure the operation of X10 on the panel.

X-10



1. Activate the checkbox **Enable** to enable X10 operation on the panel.
2. Activate the checkbox **Log** to enable logging of all X10 events on the panel.
3. Click an alphabetic tab (A-P) to program X10 device triggers.
   ⇨ A list of programmable device triggers (1-16) will be presented for that alphabetic character:



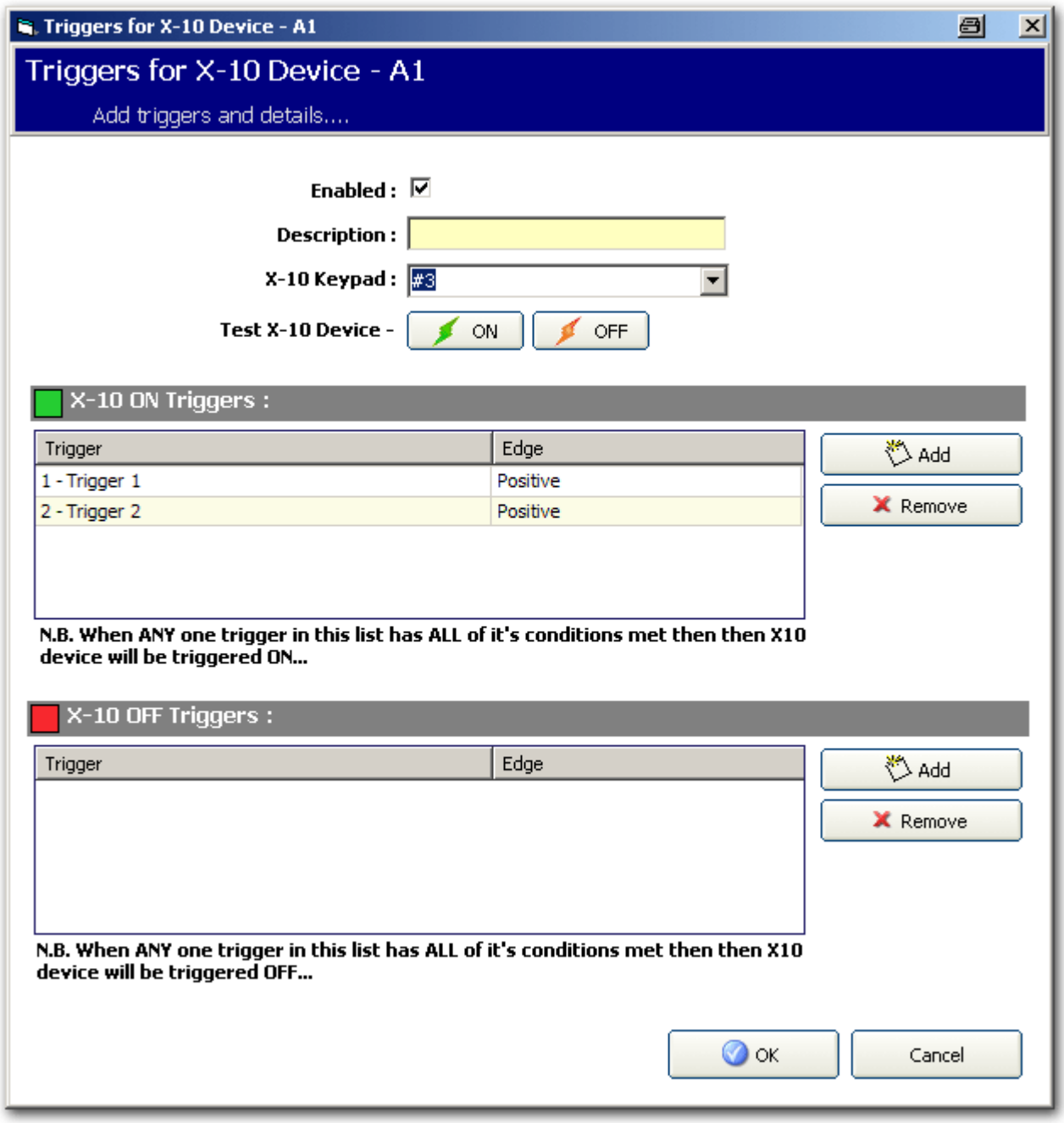
X-10 Device Triggers [A]

Unit	Active	Description	Trigger ON	Trigger OFF	RKD
1	Active	Hall light	2	2	#3
2	Active	Landing light	2	2	#8
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

Unit number	This is the number (1-16) that is assigned to the device.
Active	This field indicates if the device is active or not.
Description	This field displays a description that is used to help identify the device – e.g. downstairs light (16 characters max).
Trigger ON	This field indicates if a trigger has been programmed to activate the X10 device (1 - if a trigger is programmed, 0 - if not programmed).
Trigger OFF	This field indicates if a trigger has been programmed to deactivate the X10 device (1 - if a trigger is programmed, 0 - if not programmed).
RKD	This field indicates if the X10 device activation can be toggled by entering a code from the keypad.

To edit a X-10 device:

1. Click a trigger from the list.
   ⇨ The following window will be displayed:



2. Configure the fields described in the table below.
3. Click **Add**.
4. In the following window click the button  to create a new trigger – OR – Mark a trigger from the list and click the button  to edit the selected trigger.

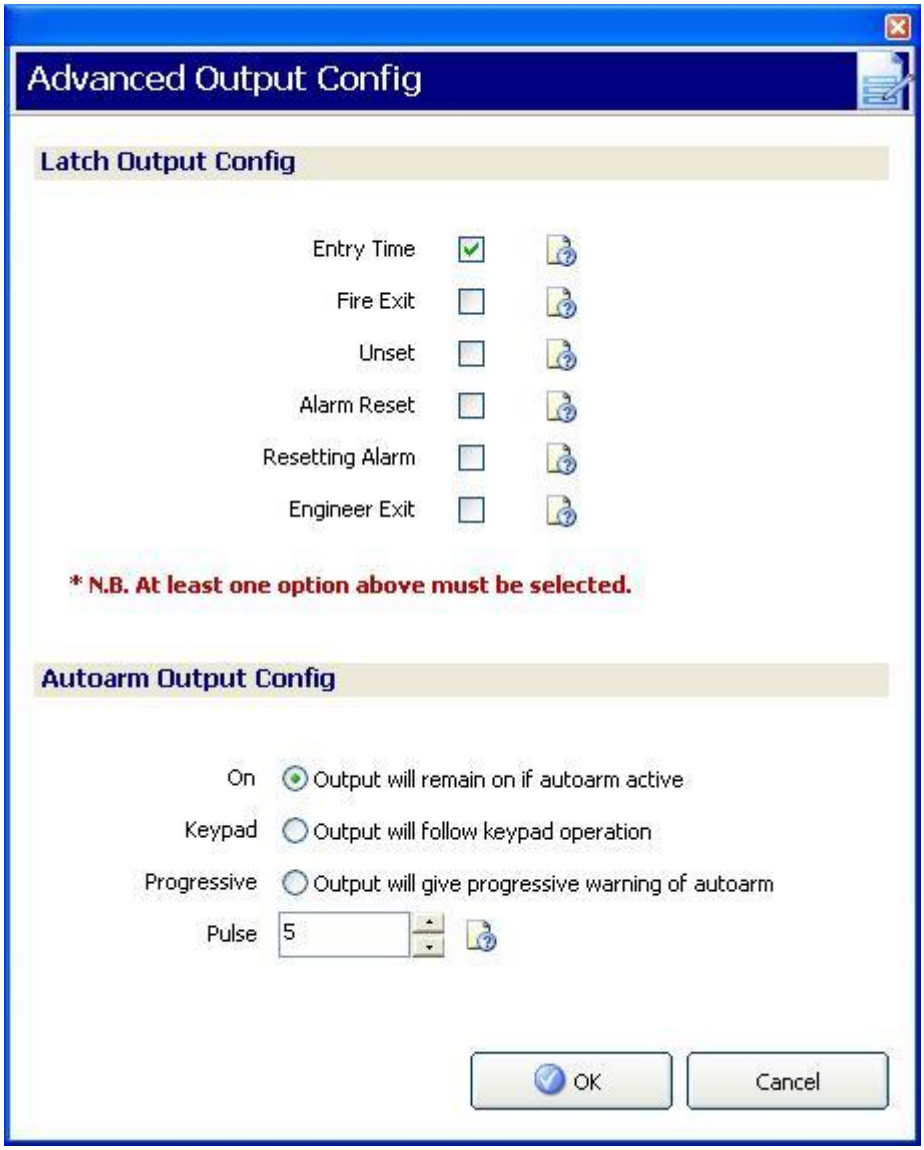
⇨ The window **Trigger Configuration** opens.

Enabled	Activate this checkbox to enable X10.
Description	Enter a text to identify the X10 device (16 characters max).
X10 Keypad	Select a code. To activate the X10 device enter this code at the keypad.
Test X10 Device	

For further programming refer to page [➙ 197].

16.6 Configuring system latch and auto set outputs

Advanced	 Advanced Output



- Select the condition under which the latch output is activated:

Entry Time	Output turns on at the end of Exit time and off at the beginning of Entry time.
Fire Exit	Output turns on if any fire exit zones are active.
Unset	Output turns on if any user unsets system momentary
Alarm Reset	Output turns on if an alarm is reset momentary.

Resetting Alarm	Output turns on during a setting procedure if glass break/smoke open and not in alarm.
Engineer Exit	Output turns on when an engineer exits from Engineer mode momentary.
Keypad Valid PIN	Output turns on when valid user PIN entered on keypad and fire zone is active

- Select the behavior of the output.

On	Output will remain on if auto set is active.
Keypad	Output will follow keypad operation.
Progressive	Output will give progressive warning of auto set.
Pulse Time	Select the duration that the auto set output will remain active when pulsed.

16.7 Logo Configuration

Logo Configuration

It is possible to load individual logos onto the SPCK620/623 keypads.

- Select **Advanced > Logo Configuration**.

⇨ The **Logo Manager** opens.

1. Click the **Load** button.
2. Select a file in one of the following formats (max. dimensions: 18 x 45 pixels)

- Raw binary 1 bit per pixel Files (*.bin)
- Monochrome Bitmap Image (*.bmp)
- Perform one of the following actions.

	NOTICE
	Click the **Save** button after each change you make. Otherwise your settings will not be applied.

Magnify	Magnifies the logo from x1 to x4.
Save	Click the **Save** button after each change you make.
Close	Closes the Logo manger.
Clear	Clears the Logo.
Preview	Shows a preview of the Logo on the keypad.

16.8 Audio Configuration

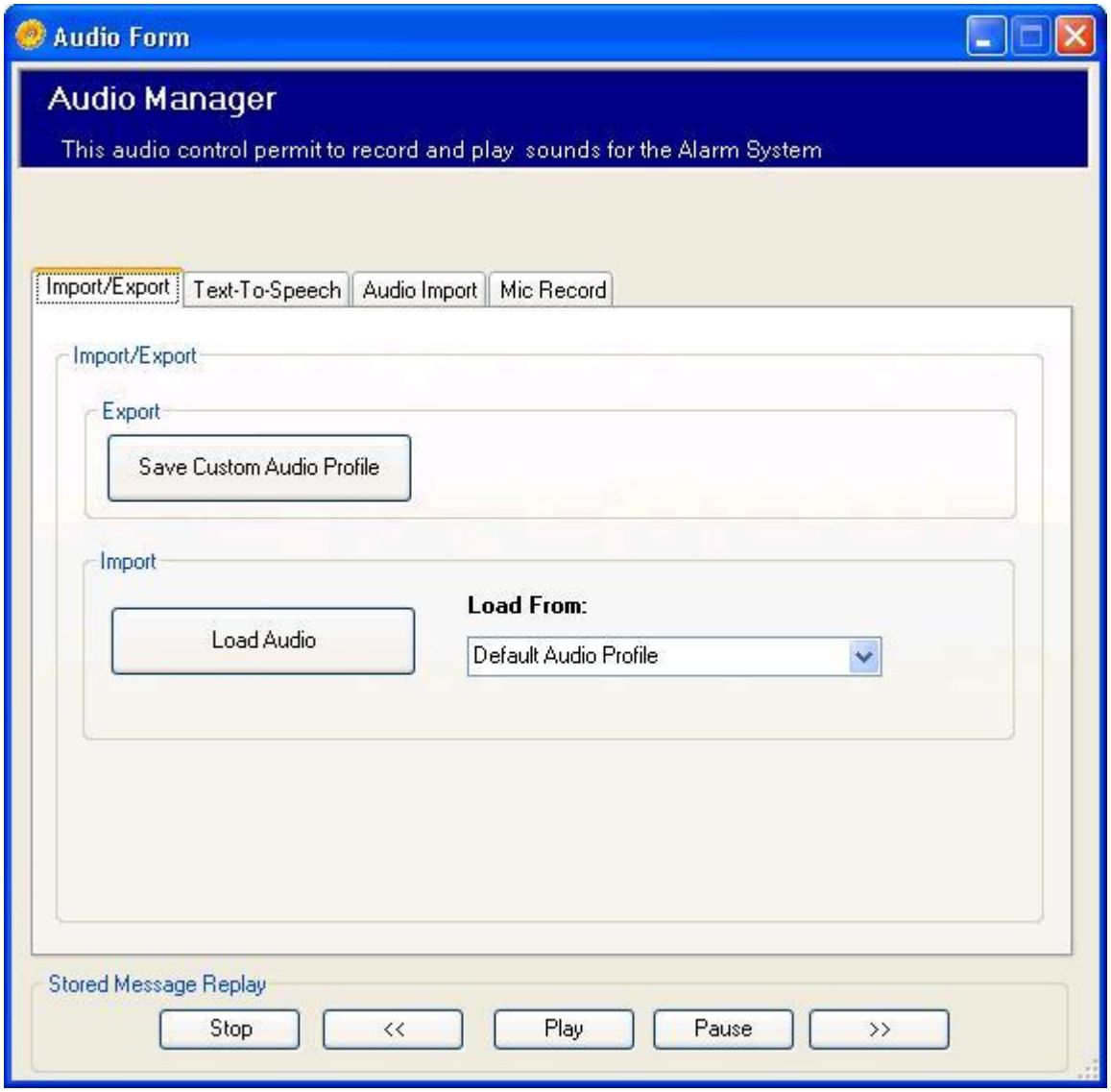
Advanced

Audio Configuration

With the Audio Manager you can record and play voice annunciations for the alarm system.

- Select **Advanced > Audio Configuration**.

⇨ The **Audio Manager** opens.



General functions

The following functions are available for all tabs within the Audio Manager.

Stop	The replay of the stored messages (audio bundle) messages (audio bundle) will be stopped.
<<	The stored messages (audio bundle) will be rewound.

Play	The stored messages (audio bundle) will be played back.
Pause	The stored messages (audio bundle) will be paused.
>>	The stored messages (audio bundle) will be fast-forwarded.
Generate AudioBundle	All single voice annunciation messages will be compressed and bundled in a downloadable file compatible with the SPC controller. The audio bundle is saved to the file spc audio.bak in the folder „C:\SPC Products\SPC Pro 2.0.0\Audio\Installations“.

Import/Export

Save Custom Audio Profile	If you change the Default Audio Profile you can save it as a Custom Audio Profile. The Custom Audio Profile will be saved by default in the folder „C:\SPC Products\SPC Pro 2.0.0\Audio\My Audio Profiles“. The file can be used as often as required.
Import Audio	You can import the Default Audio Profile or the Custom Audio Profile that you have saved.

17 System options

1. Click the menu **Options > System Options**.
2. Configure the following fields:

General	
Check Config file datestamp on panel connect	Check this box to enable time and date stamp checking of the configuration file on connecting to the panel. See page [→ 22]. This feature is enabled by default and acts as a safeguard informing you if there is a mismatch of information in the configuration file of the PC and the configuration file of the panel. **Note**: By disabling this feature you will not be aware if any differences exist between your PC configuration file and the panel configuration file when you connect to the panel
Allow custom language selection on supported panels	Check this box to enable the panel to use uploaded customer languages. See Uploading Custom Languages.
Modem Options If you intend to connect to the panel via a modem then you may need to program some initialization parameters:	
Predial String	1. Enter the modem initialization string.
Wait Time	1. Enter the time period (in seconds) that the modem will wait before making a call to the panel (max. 1 – 60 seconds).

18 Upgrading the Panel

	NOTICE
	Manufacturer Access is required for firmware upgrade operations and when enabled, is available for the completion of both controller and peripheral firmware upgrades. See System Options [→ 66].

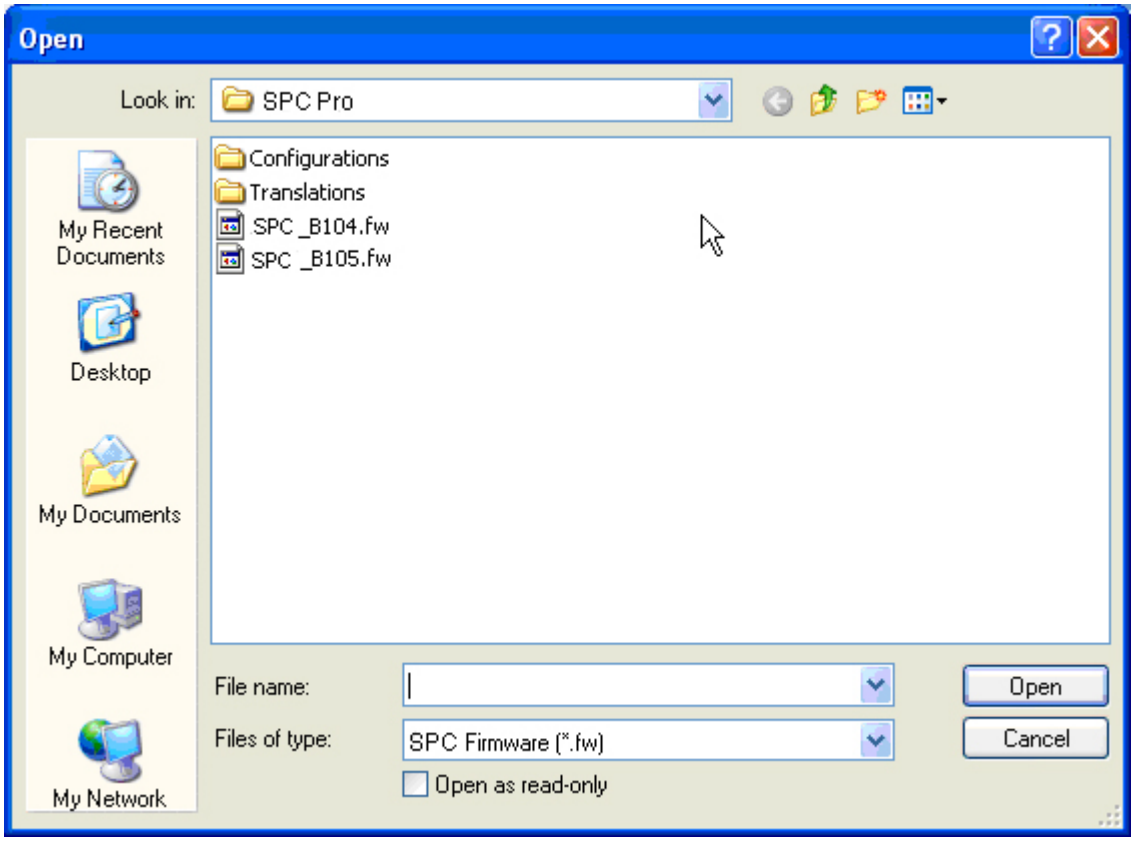
18.1 Upgrading Controller Firmware

Prerequisite:

- SPC Pro is in Full Engineer mode.
- The correct controller firmware file (.fw) located on a directory on your hard disk.

To upgrade firmware on the SPC panel:

1. Click the menu **Advanced**.
2. Select **Firmware Upgrade (Engineer Mode Only)**.
   ⇨ The following window will be displayed:



3. Select the required firmware file.
4. Click **Open**.
5. Check the values of the fields.

!	*NOTICE*
	Once the firmware upgrade procedure has been started it cannot be cancelled. It is recommended that you double check the firmware version before upgrading.

6. Click **Upgrade Now**.

After the firmware is sent the panel will restart. The connection to the panel will be lost. You will need to re-connect once the panel has rebooted again.

The following window will be displayed when the upgrade procedure is completed:

1. Click **Continue** to disconnect form the panel.
2. Re-connect to panel when the panel firmware has re-booted (re-booting takes approximately 40 seconds).

⇨ The Firmware upgrade is finished.

⚠	⚠ WARNING
	If you downgrade the controller firmware (i.e. install and older version of the firmware), the system defaults all current configuration settings.

WARNING!

18.2 Upgrading Peripheral Firmware

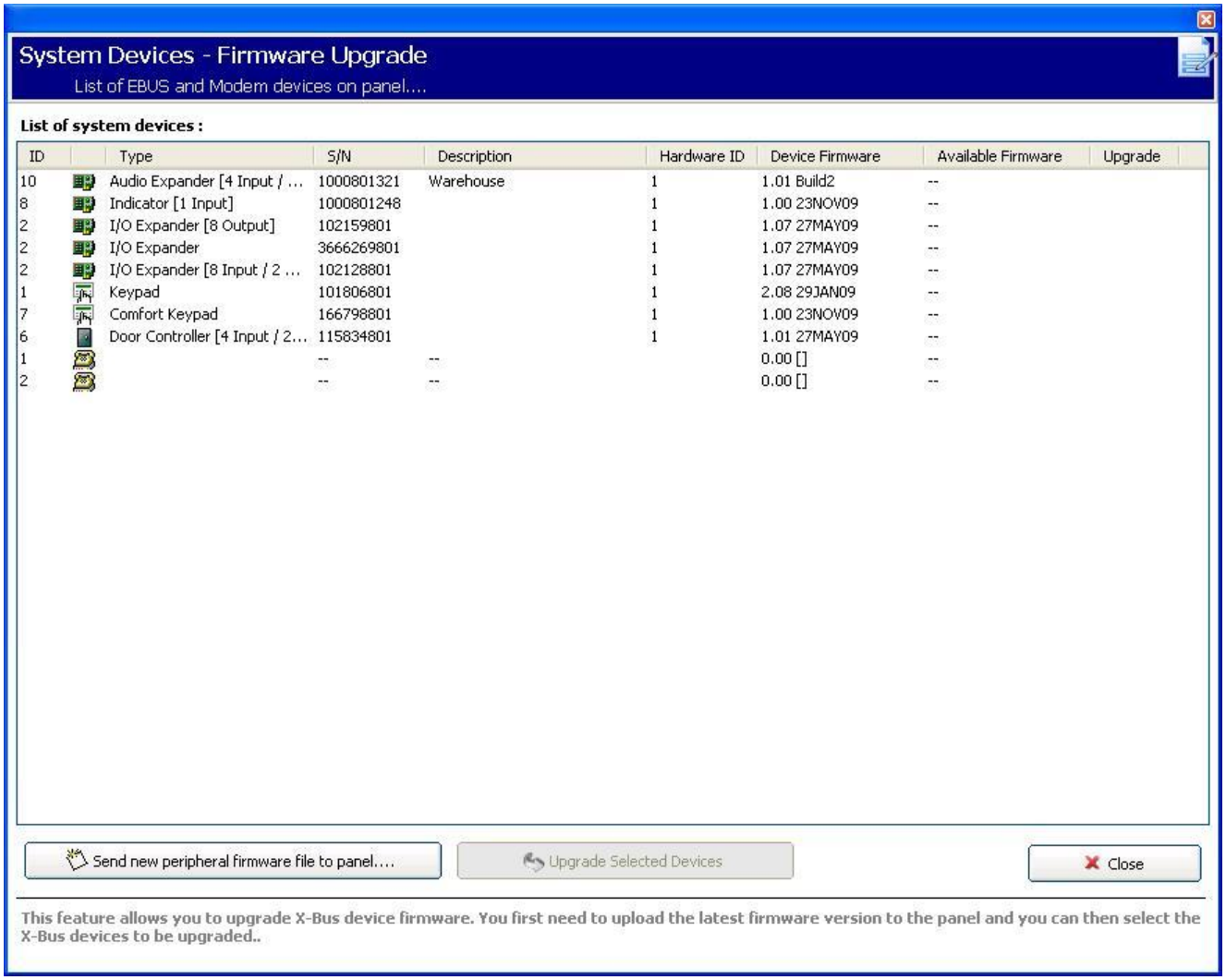
Prerequisite:

- Product Pro is in Full Engineer mode.
- The correct peripheral firmware file (.pfw) is located on a directory on your hard disk.

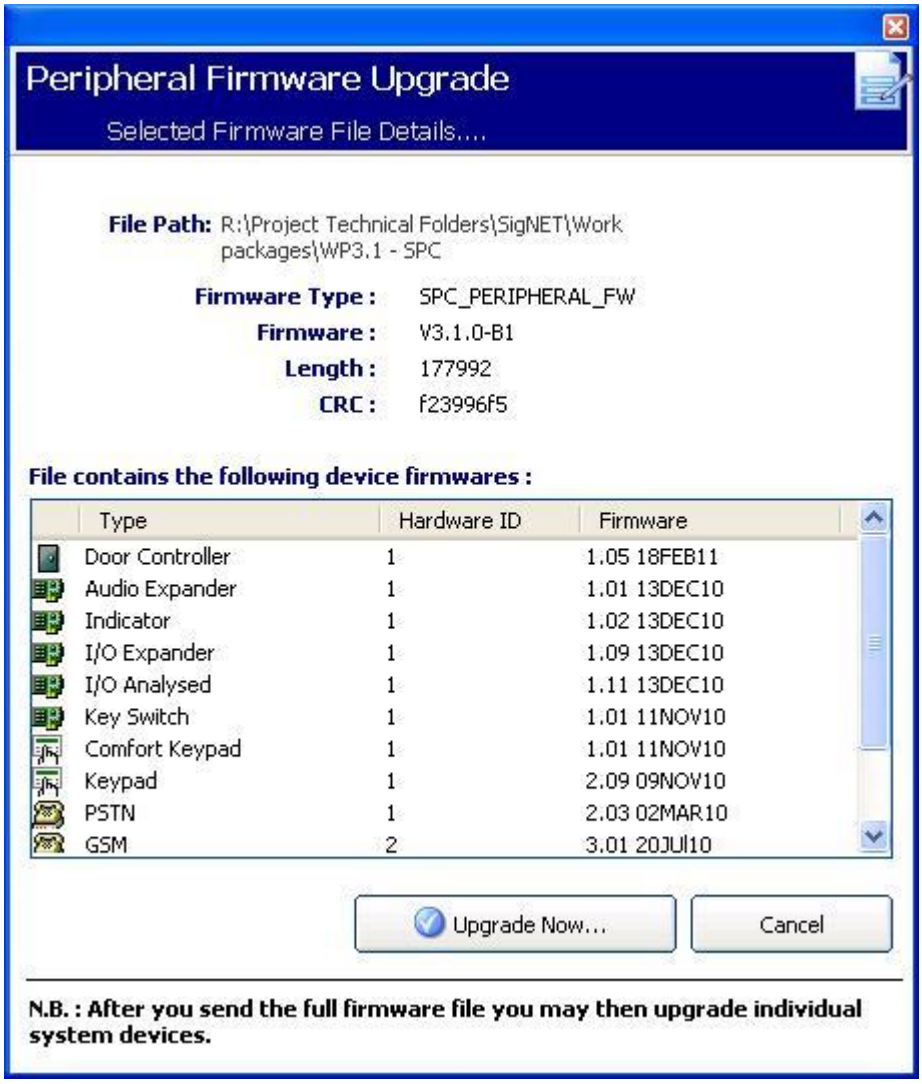
To upgrade firmware on peripherals:

1. Click the **Advanced** menu.
2. Select **Peripheral Firmware Upgrade**.

   ⇨ The following window will be displayed:



- Select the **Send new peripheral firmware file to panel** button.
  ⇨ The following window will be displayed:



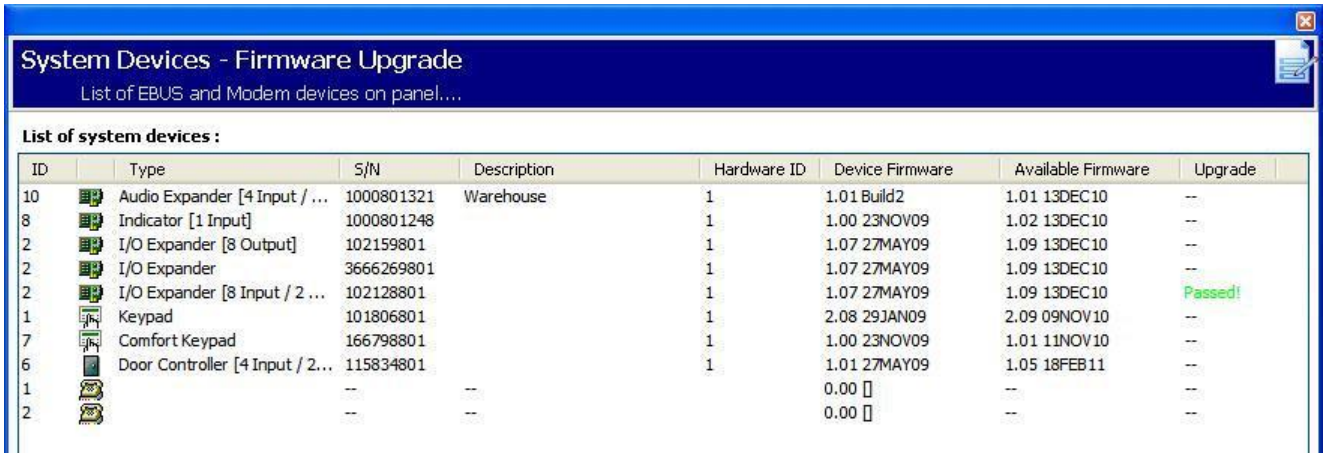
1. Click on the **Upgrade Now** button to send the peripheral firmware file to the panel.

   ⇨ If the pfw file version differs from the controller version, a warning message is displayed.

   The panel also checks if the firmware in the peripheral file supports the particular hardware versions of the installed peripherals and does not allow an upgrade for those peripherals which are not supported.

2. The peripheral firmware file is only stored temporarily in the file system. When a new peripheral firmware file is uploaded, the current and new versions of the firmware for each peripheral and modem is displayed as shown below.

   ⇨ If the major version number of the firmware available for a device differs from the existing major number of a device, a warning message is also displayed.



1. When the file is uploaded, select the devices that you wish to upgrade and click on the **Upgrade Selected Devices** button.

   If the firmware for a peripheral device in the pfw file is older than the existing firmware of that device a **Downgrade Selected Device** button is available.

2. If the upgrade is successful for a device, its Upgrade status will change to 'Passed'.

The peripheral firmware can also be upgraded with the web browser or Fast Programmer.

18.3 Updating SPC Licenses

The **License Options** feature provides a mechanism for the user to update or add functionality to the SPC system, for example, for migrations, where installed peripherals, which are not licensed for SPC, need to be supported by an SPC controller.

1. Connect online to the panel.
2. Click on the **Advanced** menu.
3. Select the **License Panel (Engineer Mode Only)** option.
   ⇨ The following dialog box is displayed:

4. Contact technical support with the requested functionality and quote current license key as displayed.
   ⇨ If request is approved, a new license key is issued.
5. Enter the new key in the field provided and click the **Send Key to Panel** button.

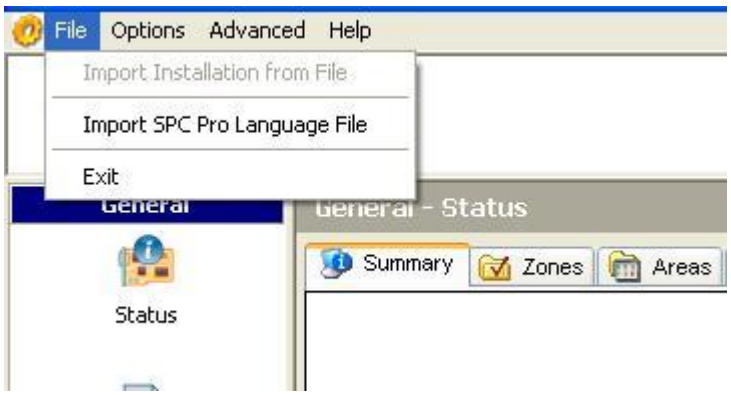
⇨ If the license key is changed successfully, the following dialog box is displayed:

18.4 Importing Custom Languages for the SPC Pro User Interface

You can import a custom language for the SPC Pro user interface which is completely independent from the custom language installed or at the panel for the browser and keypads. You can use a specific language for configuration in SPC Pro and a different language for the panel.

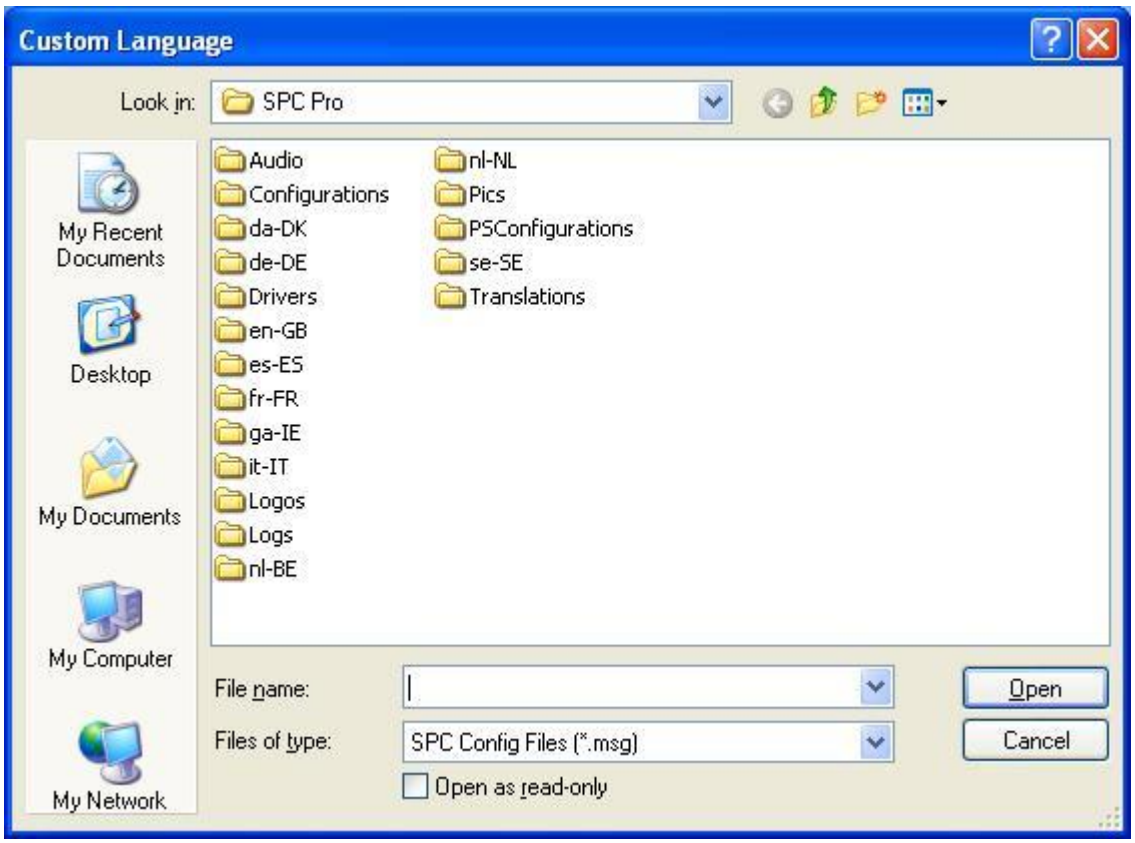
To import the SPC Pro language:

1. Click on the **File** menu in SPC Pro.
2. Select the **Import SPC Pro Language File** from the **File** menu.



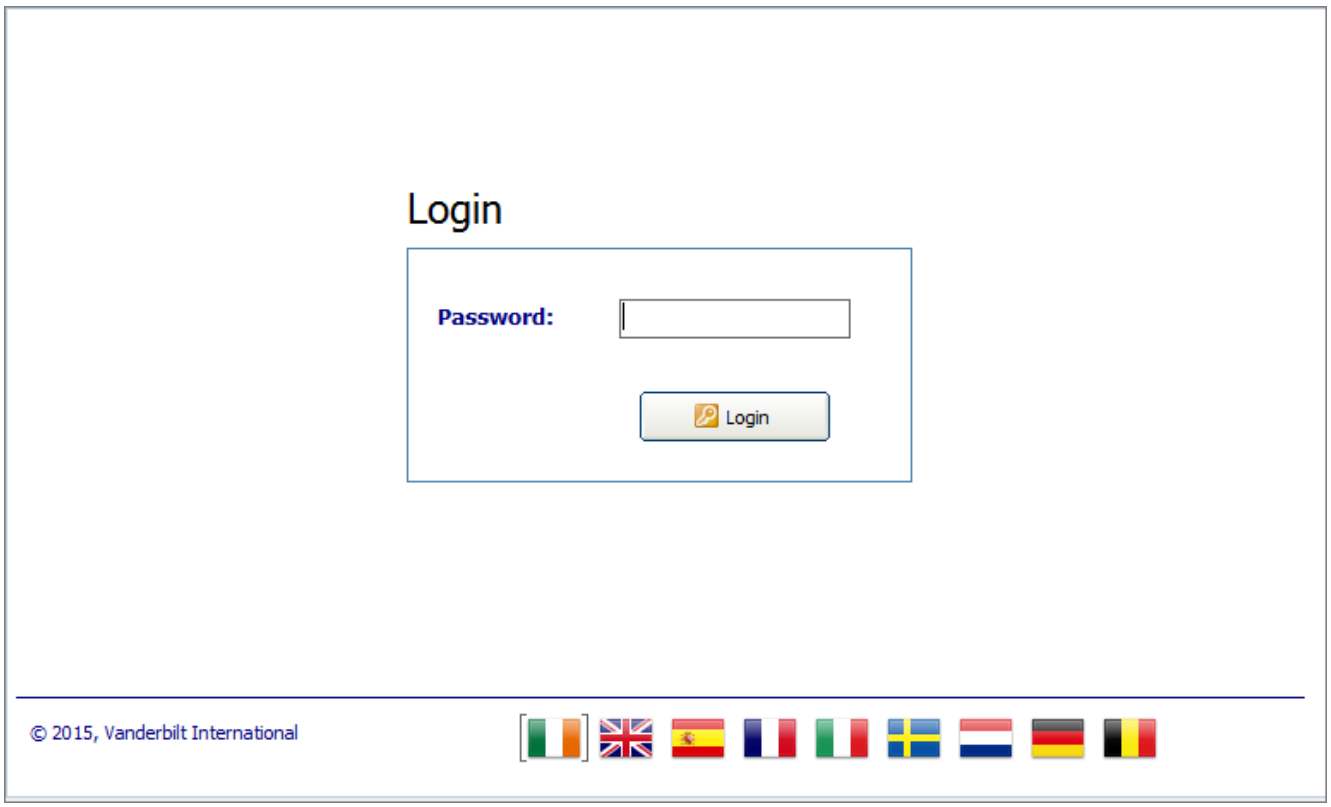
- Select a language file from the file location dialog box and click **Open**.

!	*NOTICE*
	SPC Pro language files have a *.msg extension.



To use the new custom language:

1. Exit from SPC Pro.
2. Start the SPC Pro application again.
3. At the login screen, click on the globe icon which indicates the custom language.



This language will always be used for SPC Pro configuration until it is specifically changed again.

19 Activate keypad emulation

SPC Pro provides you with the ability to emulate a keypad when you are connected to the panel.

The keypad emulation is a virtual keypad providing access to programming and status information on the panel via the standard keypad interface. It is not directly linked to any physical keypad on the system and as such will not retain the attributes of any physical keypad.

- Click the icon  in the config mode toolbar.
  - ⇨ The keypad will be displayed on the screen providing you with the following functionality.

System information

The keypad display will update in real time to match information that is displayed on an actual keypad connected to the panel (i.e. time, date information alerts detected on the panel, etc.).

Access to programming

- Enter the engineer PIN by clicking on the numbered buttons. (see Installation & Configuration Manual for details of default Engineer PINs.)

⇨ The display will update accordingly as digits are entered.

⇨ All of the keypad programming options will be presented as detailed in the panel specific SPC Installation&Configuration Manual.

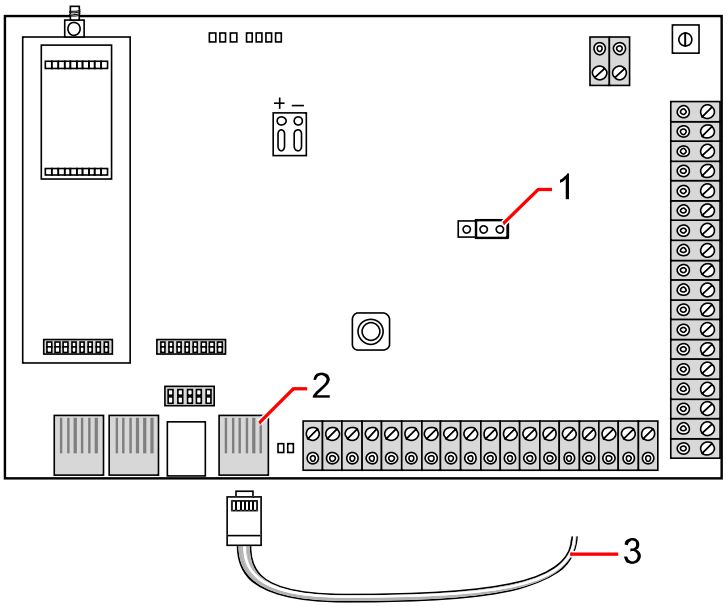
1	Live panel status information
2	Click on the buttons to enter programming codes
3	Click to exit the keypad emulation

4	Click on the navigation buttons to move through programming menus

20 Connecting to the panel

20.1 Ethernet interface

IP



Connect

1	JP9 ~~SPC4xxx~~
2	Ethernet port
3	To Ethernet port on PC

If the SPC Ethernet interface is connected to an existing **L**ocal **A**rea **N**etwork (LAN), please consult the network administrator for that LAN before connecting to the panel. Default IP Address: 192.168.1.100

Connect the cable

- Connect an Ethernet cable from the Ethernet interface on the PC to the Ethernet port on the controller board
  – OR –
  If connecting directly from a PC then a cross over-cable must be used. See page [➙ 253].

  ⇨ The LEDs to the right of the Ethernet interface indicate a successful data connection (Right LED on) and Ethernet data traffic (Left LED flashing).

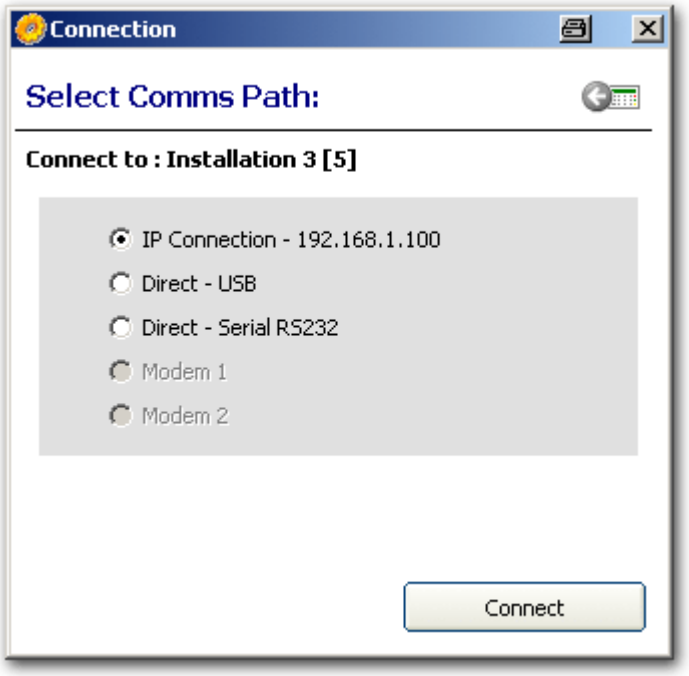
Determine the IP address of the SPC controller

1. Entering the Engineer mode (See Engineering PINs).

2. Using the up/down arrow keys, scroll down COMMUNICATION option and press SELECT.
3. Scroll to ETHERNET PORT and press SELECT.
4. Scroll to IP ADDRESS and press SELECT.

SPC Pro

1. Start the program SPC Pro.
2. Select an installation.
3. Click the button **Configure**.
4. Click the button **Connect to Panel** in the Config Mode Toolbar.
   ⇨ The following window will be displayed:



5. Select the option **IP Connection**.
   ⇨ The IP address will be displayed.
6. If the IP address needs to be changed, edit the installation details and enter the correct IP address in the field IP address. See page.
7. Click **Connect**.

⇨ The connection is finished.

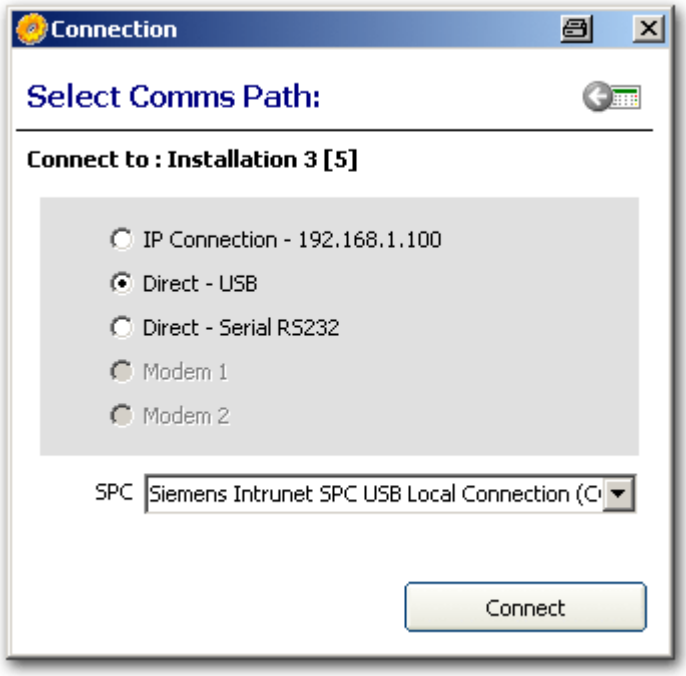
20.2 USB interface

The USB port on the SPC controller connects to a PC via a standard USB type A to type B cable.

To make a USB connection from the SPC controller to your PC:

1. Copy the batch file SPC_USB.bat to your PC.
2. Run the file.
3. Connect the USB cable from the SPC controller to a USB interface on your PC.
4. Start the program SPC Pro.

5. Select an installation.
6. Click the button **Configure**.
7. Click the button **Connect to Panel** in the Config Mode Toolbar.
   ⇨ The following window will be displayed:

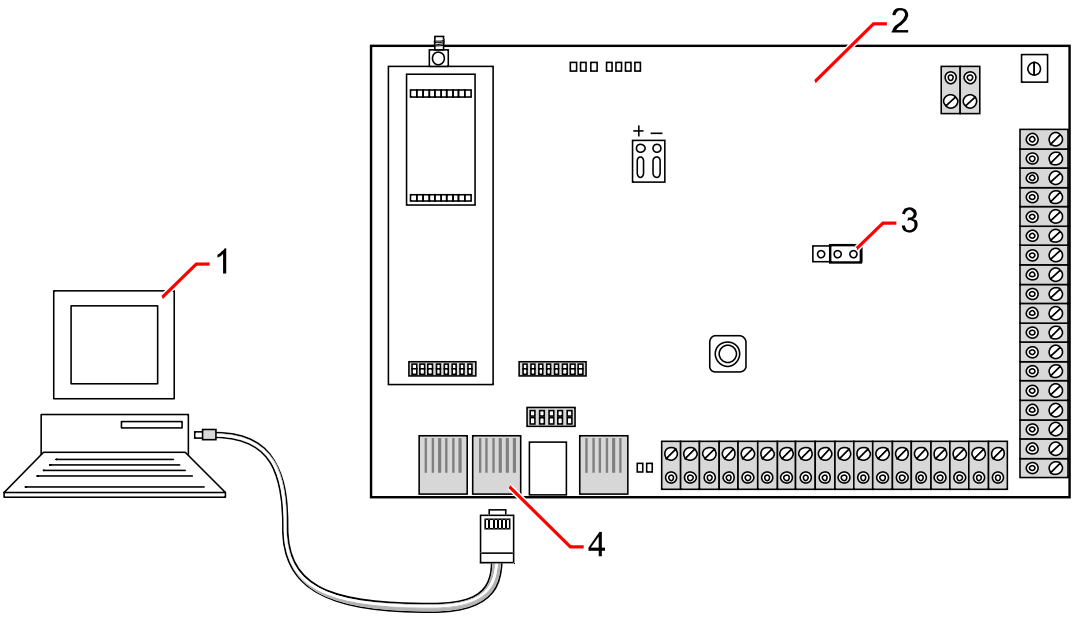


8. Select the option **Direct – USB**.
9. Ensure that the correct serial port networking connection is selected in the drop down window.
10. Click **Connect**.

⇨ The connection is finished.

20.3 Serial port

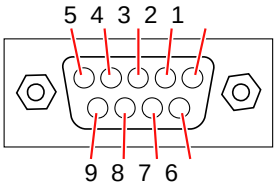
The SPC controller serial port (RS232) can be used to provide access to the SPC Pro. The serial cable detailed below must be used and the system must be configured accordingly. Once the serial cable has been connected and the serial port on the panel configured accordingly, you can connect directly to the panel from SPC Pro.

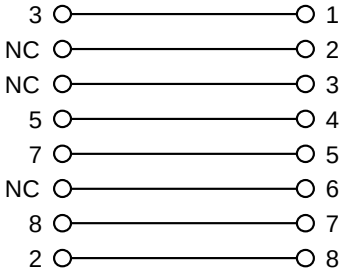


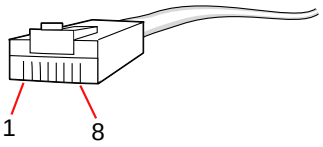
1	PC with Serial Port running Hyperterminal
2	SPC Controller
3	JP9 ~~SPC4xxx~~
4	RS232

To make a serial connection from a PC to the SPC controller:

1. Connect the DB9 serial port on the PC to the RJ45 interface on the SPC labelled RS232.
2. Using the following cable configuration:







Serial port 2 shares a communications channel with the back-up modem. If a back-up modem is installed, then it must be removed to enable serial communications on this serial port. The Serial Port 2 interface is also available as a terminal block connection (TX, RX, GND).

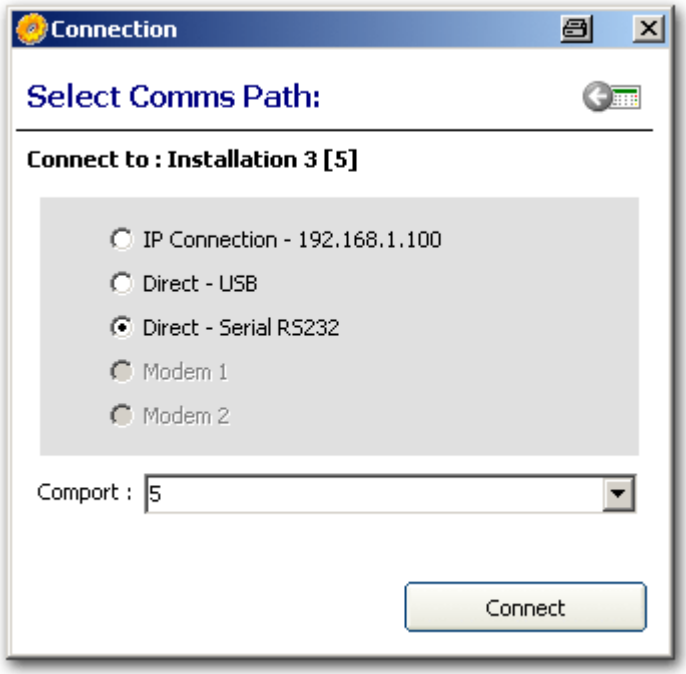
To configure the serial port via keypad:

1. Enter Engineer programming (Default code 1111) from a keypad connected to the SPC controller.
2. Enter the Full Engineer mode.
3. Select COMMUNICATION.
4. Scroll down to SERIAL PORTS and press SELECT.
5. Select the serial port you wish to connect to (Port 1 or 2).

6. In the TYPE Menu select the PRINTER option to access the SPC event log or TERMINAL to access system information.
7. In the BAUD RATE menu select 115200.
8. In the DATA BITS menu select 8 DATA BITS.
9. In the STOP BITS menu select 1 STOP BIT.
10. In the PARITY menu select NO PARITY.
11. In the FLOW CONTROL menu select RTS/CTS CONTROL.

To configure the serial port via SPC Pro:

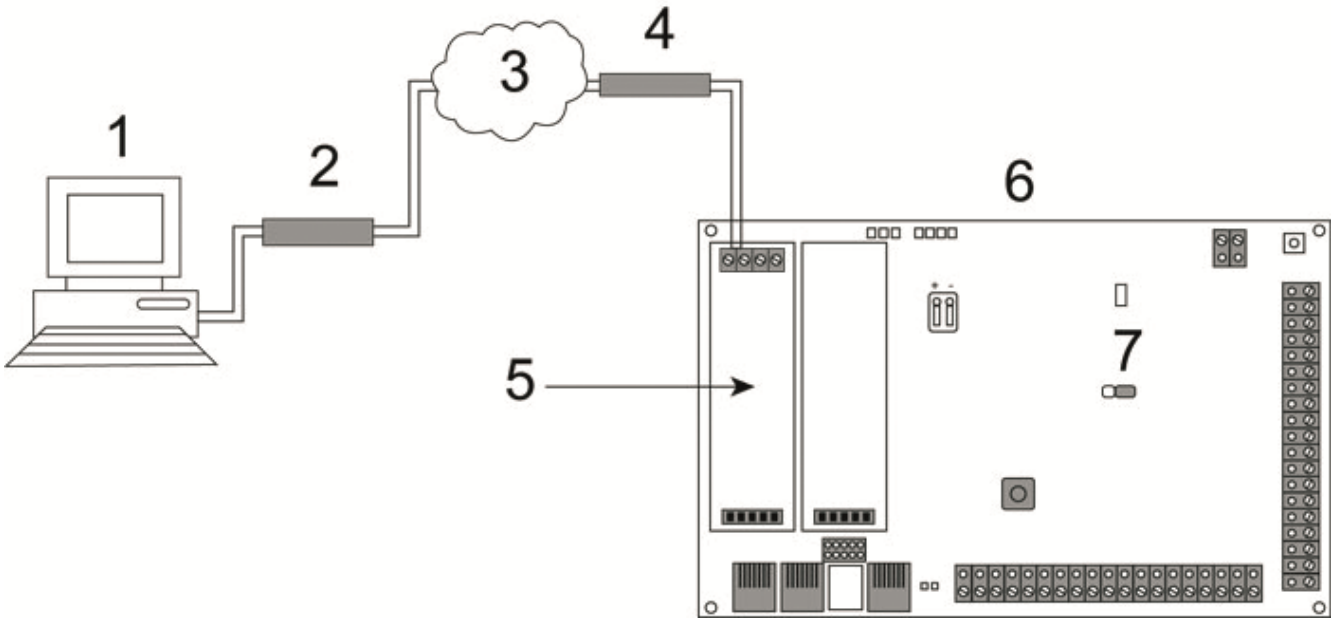
1. Start SPC Pro.
2. Select an installation.
3. Click the button **Configure**.
4. Click the button **Connect to Panel** in the Config Mode Toolbar.
   ⇨ The following window will be displayed:



5. Select the option **Direct – Serial (RS232)**.
   ⇨ The Comport drop down menu will display the number of COM ports configured on your PC.
6. Select the COM port that the serial cable is connected to.
7. Click **Connect**.

⇨ The connection is finished.

20.4 PSTN modem



PSTN Connection

1	Remote PC with browser
2	PSTN modem
3	PSTN network
4	Telephone line
5	PSTN modem
6	SPC controller
7	JP9 SPC4xxx

The SPC controller can be accessed via a remote connection over a PSTN telephone line.

Prerequisites:

- A PSTN line must be connected to the controller.
- On the remote side of the connection the user must have a PSTN modem installed on a PC with access to a PSTN line.

Configure the modem on the SPC controller via the keypad:

▷ A PSTN modem is installed on the controller. Please refer to the panel specific SPC Installation&Configuration Manual.

1. Connect the phone line to the A, B screw terminals on the connector at the top of the modem.
2. Enter Engineer programming.
3. Scroll to COMMUNICATION and press SELECT.
4. Scroll to MODEMS and press SELECT.
5. Select PRIMARY or BACKUP and press SELECT.

   ⇨ Parameters and details, if applicable, are displayed for editing as shown in the table below.

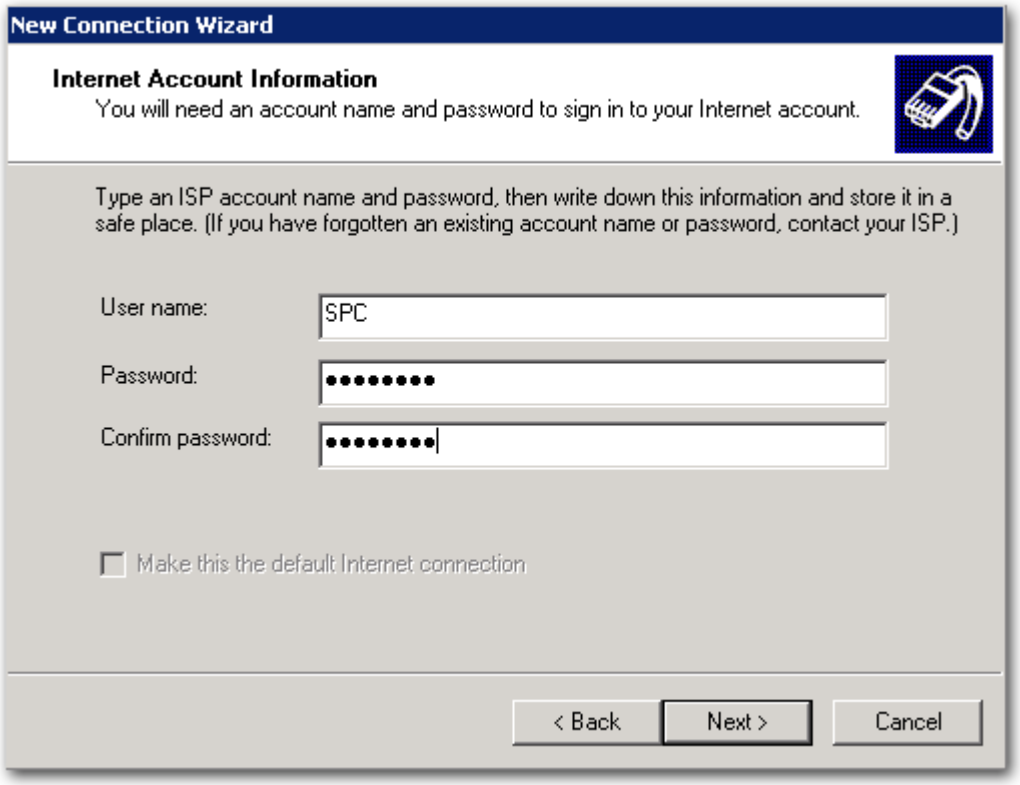
6. Create a dial-up connection on the remote PC using the phone number of the telephone line connected to the PSTN module on the SPC.

Enable Modem	Set to **Modem Enabled**.
Type	Displays the type of modem (PSTN).
Country Code	Select the relevant country code (Ireland, UK, Spain, etc…).
Answer mode	Select numbered rings. This tells the modem to wait for a number of rings before answering the incoming call.
Modem Rings	the number of rings to allow before answering the call (8 rings max).

On Windows XP

1. Open the menu **Control panel > Network Connections > Create New Connection**.
   ⇨ The following window will be displayed:

2. In the **Network Connection Type** window, select “Connect to the Internet”.
3. In the **Getting ready** window choose “Setup my connection manually”.
4. In the **Internet connection** window choose “Connect using Dialup modem”.
5. In the **connection name** window enter the connection name e.g. “SPC Remote connection”.
6. In the **Phone number to dial** window, enter the phone number of the PSTN line connected to the PSTN modem.
7. In the connection availability window choose whether you want this connection to be available to all users.

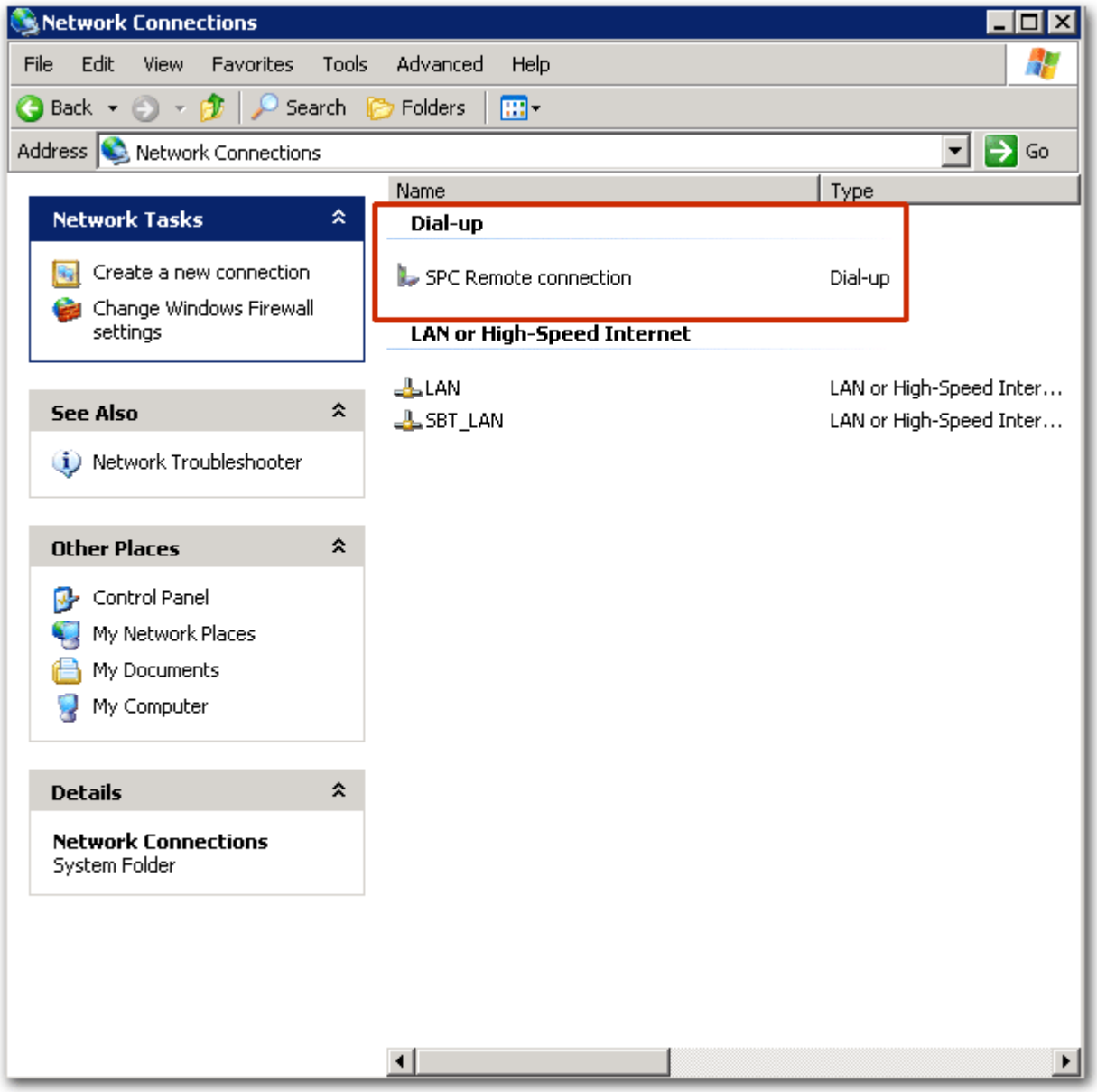


In the internet account information window enter the following details:

1. Username: SPC
2. Password: password
3. Confirm Password: password
   ⇨ A window with the title “Completing the new connection wizard” will be displayed.
4. Click the **Finish** button to save the Dial-up connection to your PC.

Activate the dial-up connection

- Click the icon located in the control panel.
  ⇨ The following window will be displayed:



The PC will make a data call to the PSTN line connected to the PSTN module.

The PSTN module will answer the incoming data call after the designated number of rings and establish an IP link with the remote computer.

An IP address will be automatically assigned to the remote PC by the SPC system.

1. To obtain this IP address right click the icon **Dial-up**.
2. Click the tab **Details**.

⇨ The IP address will be displayed as the Server IP address. This is the IP address to specify in the SPC Pro connection type window. See page [➞ 26].

For details on connecting remotely to the panel with a GSM modems see Appendix.

21 Using the Fast Programmer

21.1 Installing the Fast Programmer on a PC

For Windows XP

▷ SPCPro must be installed on the Windows XP PC.

1. Connect the Fast Programmer to a USB interface on the PC.
   ⇨ The **Found New Hardware** wizard is displayed.
2. Press **Next.**
3. Click **Continue Anyway**.
   ⇨ At the end of the installation process, a window indicates that the installation process is complete.
4. Click **Finish**.

For Windows 7

▷ You have administration privileges.

▷ SPCPro must be installed on the Windows 7 PC.

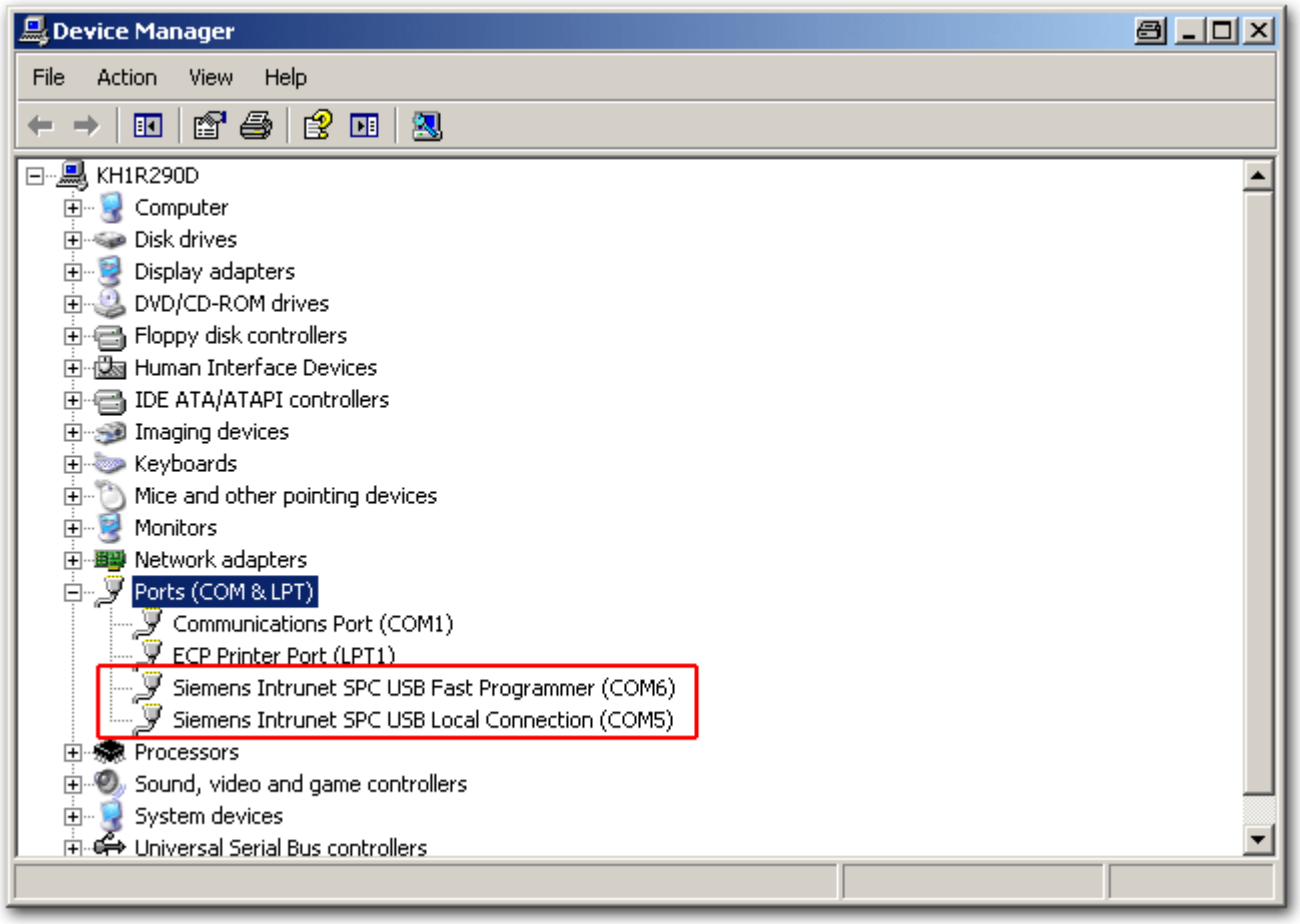
- Connect the Fast Programmer to a USB interface on the PC.

⇨ The drivers are installed automatically

View SPC Fast Programmer

- Open the Windows menu **Start > Control panel > System > Device Manager**.

⇨ The Fast Programmer driver will be listed under the Ports (COM & LPT) directory as SPC **USB Fast Programmer (COM X)** (X = com port number).

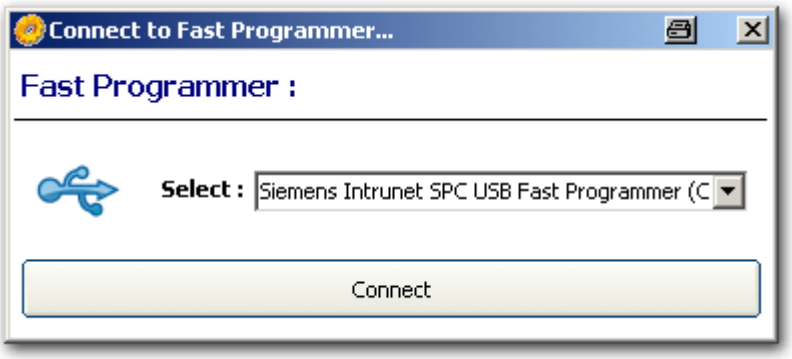


21.2 Connecting to the Fast Programmer

You cannot connect to the Fast Programmer if you are in Config mode.

When the Fast Programmer has been successfully installed on your PC, start SPC Pro.

- Click the button **Fast Programmer** on the main installation page.
  - ⇨ The following window will be displayed.

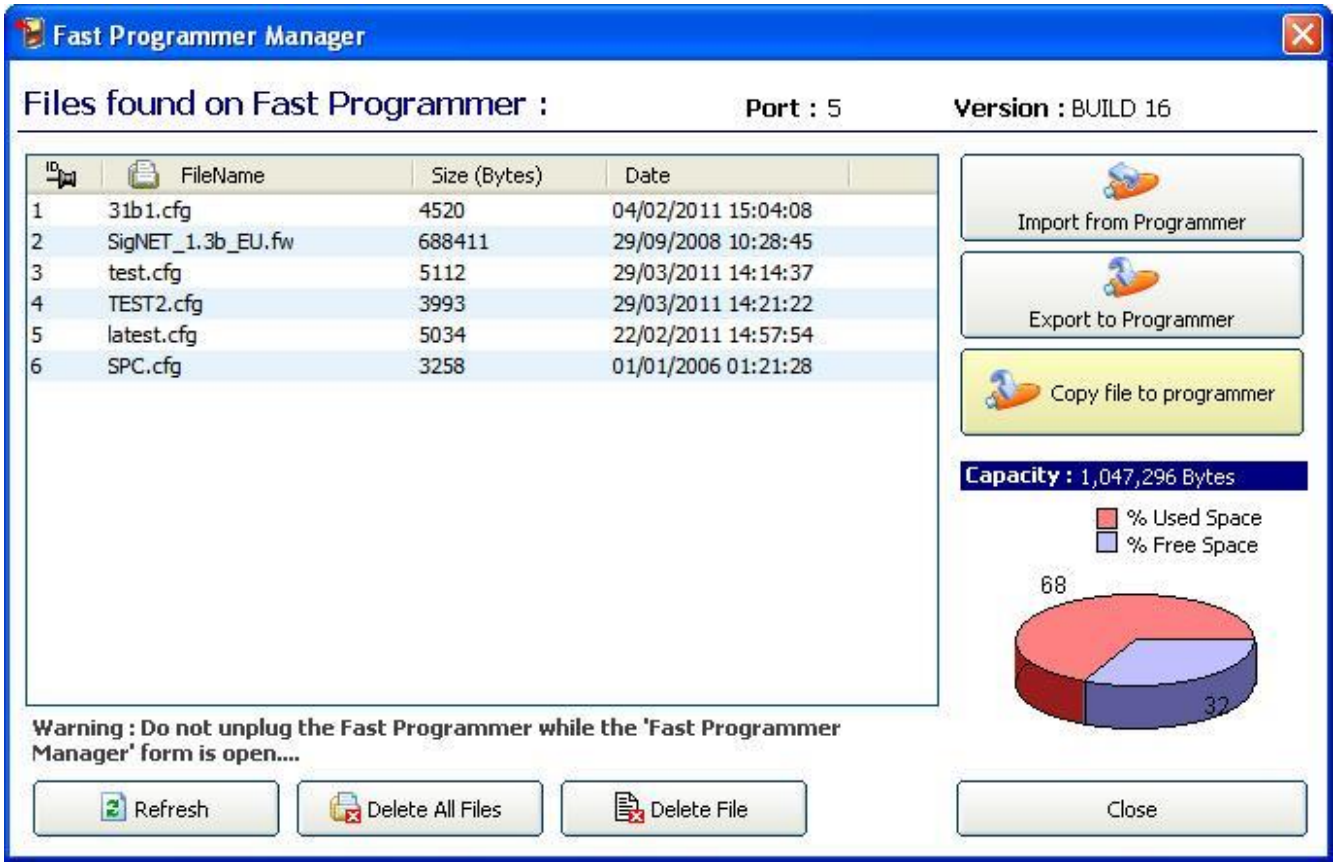


The window displays the serial port that the Fast Programmer has been detected on.

If the SPC Pro does not detect the fast programmer a pop-up message will be displayed.

Please re-install the fast programmer and ensure that it is displayed in the COM ports section of the device manager.

- Click **Connect**.
  - ⇨ The following window will be displayed.



This window will display a list of the files found on the device along with the available free memory remaining for storing further configurations.

!	*NOTICE*
	Do **NOT** unplug the Fast Programmer while the window **Fast Programmer Manager** is open. Doing so will corrupt the data stored in the fast programmer device.

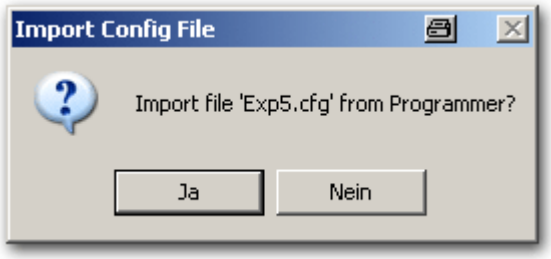
The following operations can be performed:

- Importing Configuration Files from the Programmer [→ 231]
- Exporting Configuration File to the Programmer [→ 232]
- Copying Firmware and Language Files to the Programmer [→ 233]

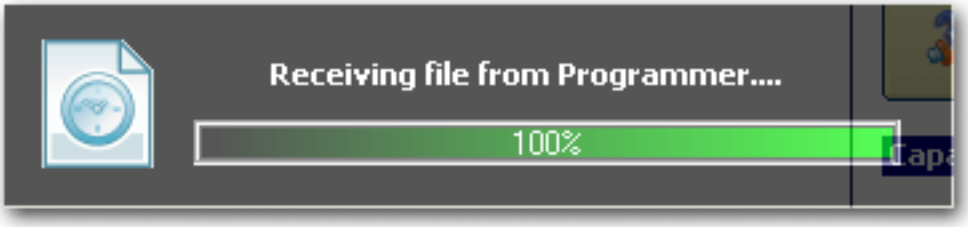
21.3 Importing Configuration Files from the Fast Programmer

To import a configuration file from the SPC Fast programmer:

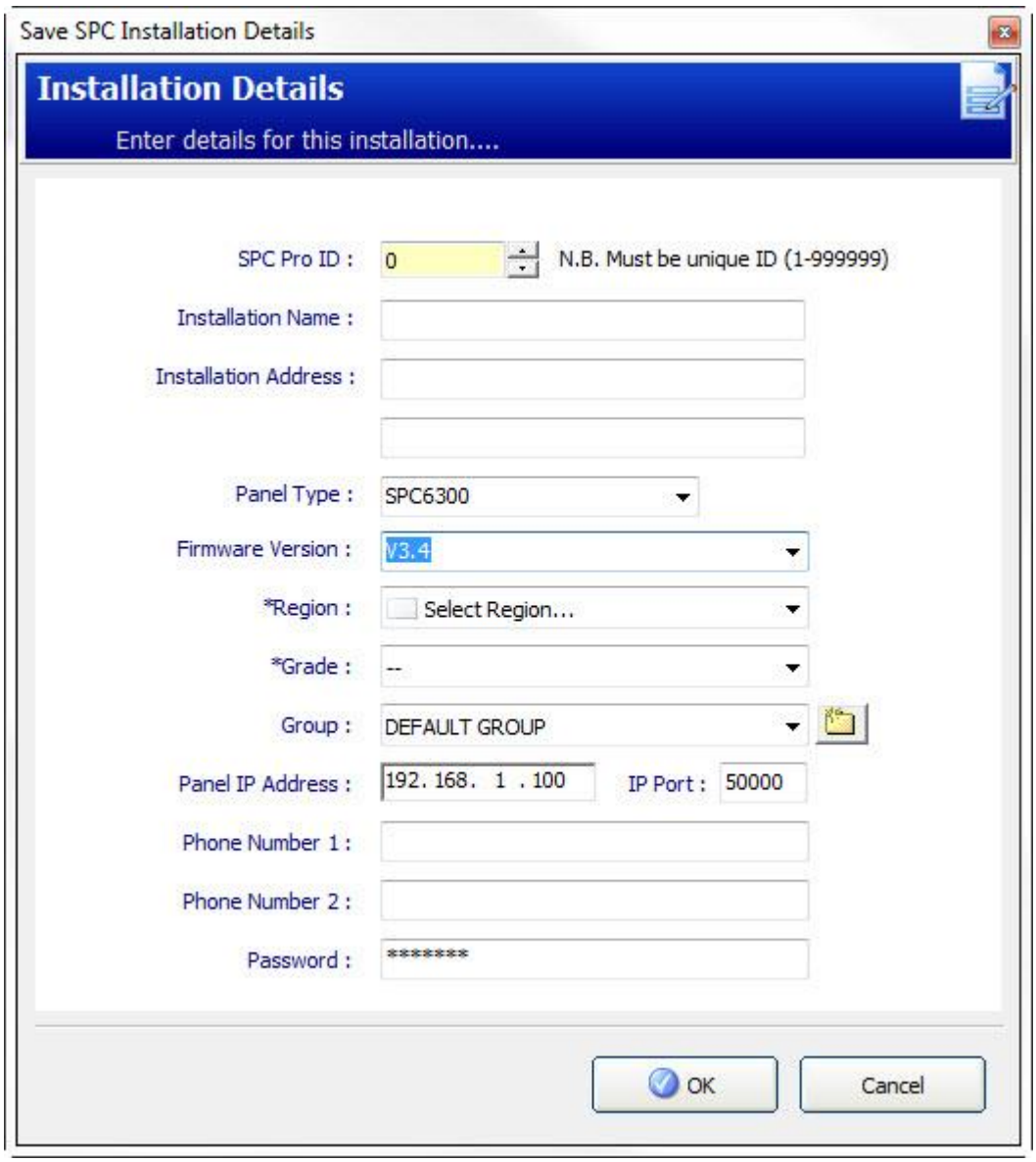
1. Click on the file you require.
2. Click on the button **Import from Programmer**.
   ⇨ The following window will be displayed.



3. Click **Yes**.
   ⇨ The following window will be displayed:



On loading the configuration file the following window will be displayed:



The window Installation Details displays the basic installation configuration data of the loaded file. If you already have an installation on SPC Pro with the same Installation ID you will be required to change the ID before proceeding.

- Click **OK** to import the file.

It is strongly recommended that you review the configuration details of a file imported from a fast programmer BEFORE sending that configuration to a panel.

21.4 Exporting Configuration Files to the Fast Programmer

To save your configuration settings to the fast programmer:

1. Click the button **Export to Programmer**.
   ⇨ The following window will be displayed:

2. Select the installation you wish to export from the drop down menu **Select Installation to Export**.
   ⇨ A list of all of the installation configurations currently available on SPC Pro will be displayed.
3. Enter the name of the configuration file in the field **Filename on Programmer** (characters 'a-z' and digits '0-9' are permissible).

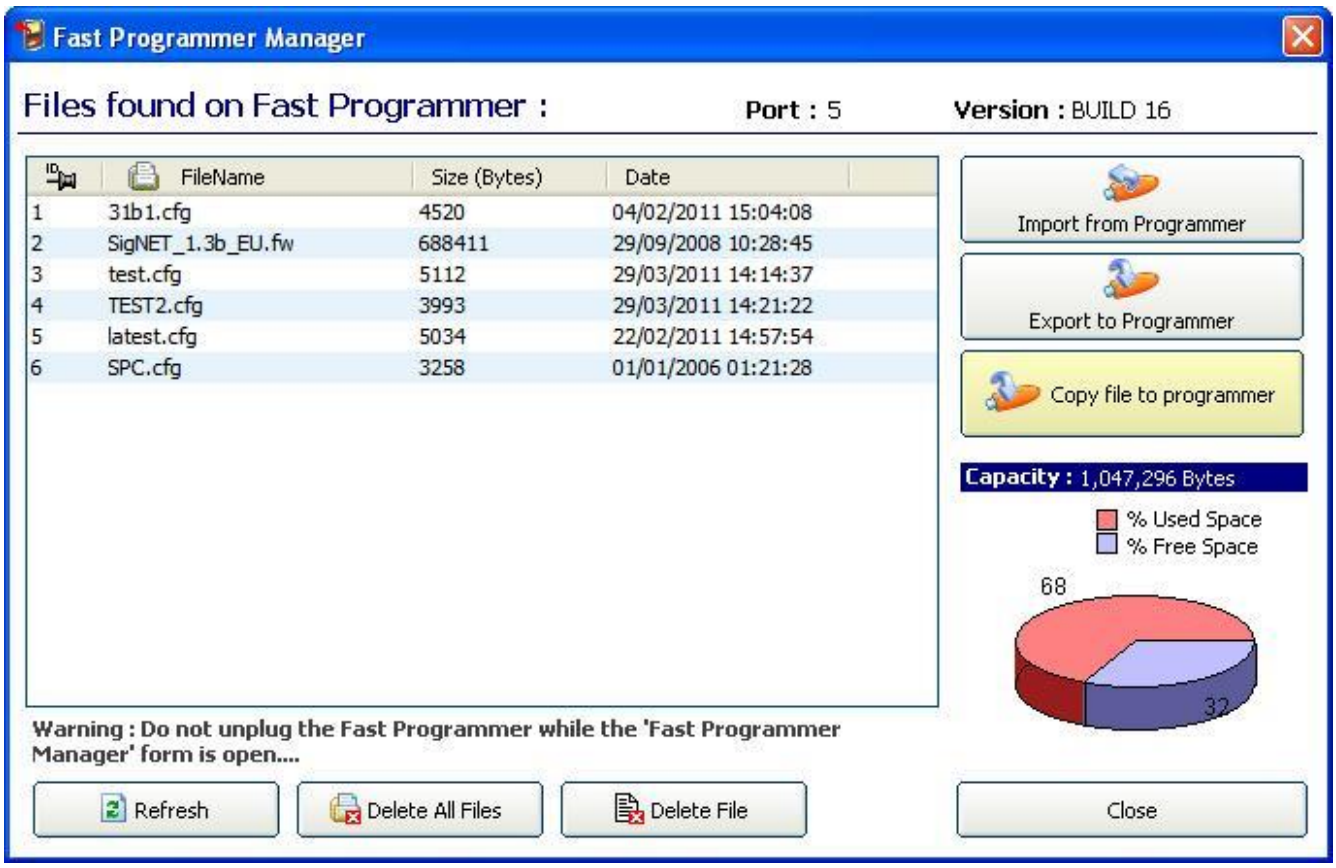
⇨ This name will appear on the file when you attempt to import it from the programmer.

Enter a unique name for the installation. If a configuration file with the same name exists on the Fast programmer the warning message shown will be displayed and you will be prompted to re-name the configuration.

21.5 Copying Firmware & Language Files to the Fast Programmer

Controller and peripheral firmware files and custom language files can be copied to the Fast Programmer for upgrading on a panel using a keypad for SPC browser.

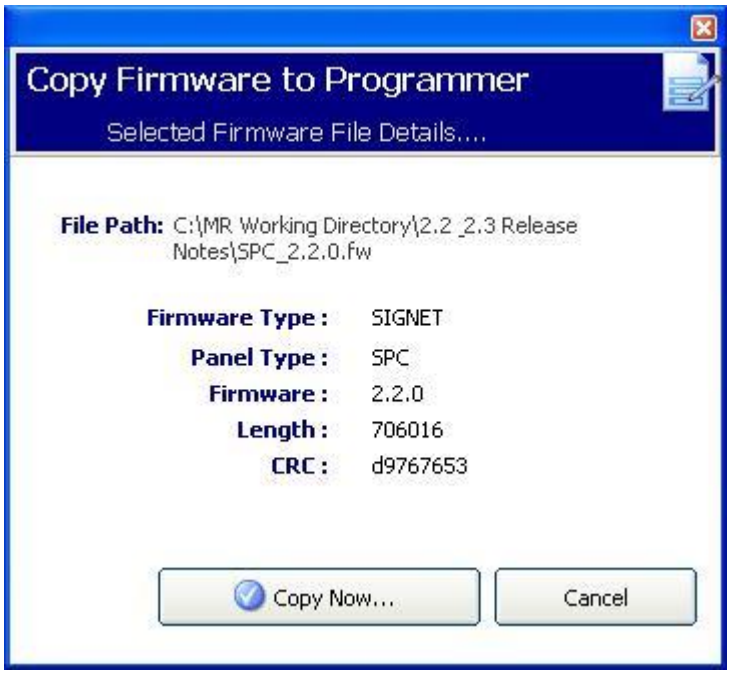
!	*NOTICE*
	The last version of firmware may not fit on older Fast Programmer models. You may need to upgrade your Fast Programmer to copy new firmware versions.



To copy a file to the Programmer.

1. Click on the **Copy file to programmer** button in the File Programmer Manager dialog box.
2. Select the required firmware or language file from the file location dialog box.

⇨ The file details are displayed as shown.



- Click on the **Copy Now** button.

⇨ The file is displayed in the Fast Programmer Manager dialog box.

Firmware and custom languages are upgraded on a panel using the keypad or SPC browser. Refer to the *SPC Installation and Configuration Manual* for details.

22 Audio/Video Verification

To set up Audio/Video Verification on an SPC system:

1. Install and configure Audio Expander (s)
2. Install and configure Video Camera(s).
3. Install and configure Audio Equipment.
4. Configure Verification Zone(s).
5. Test audio playback from verification zones.
6. Assign Verification Zone(s) to physical zone(s).
7. Configure Verification Settings.
8. View images from verification zones in web browser or SPC Pro.

!	*NOTICE*
	Keypads and access control may be disabled for several minutes while sending an audio file to the panel, depending on the size of the file.

22.1 Configuring Video

Overview

Cameras are used for video verification. The SPC panel supports a maximum of four cameras. Only IP cameras are supported and the panel must have an Ethernet port.

i	*NOTICE*
	Cameras must not be shared with other CCTV applications.

Cameras can only be configured with the web browser or SPC Pro. Configuration with the keypad is not supported. SPC Pro provides an easier method of configuration and is recommended.

The panel supports two camera resolutions:

- 320X240
  This setting is recommended if you want to view images on the browser)
- 640X480 (with some restrictions).

The following cameras are supported in addition to other generic cameras:

- Vanderbilt CCIC1410 (1/4” VGA IP Colour Camera)
- Vanderbilt CFMC1315 (1/3” 1.3 MP Indoor Dome Colour Camera)

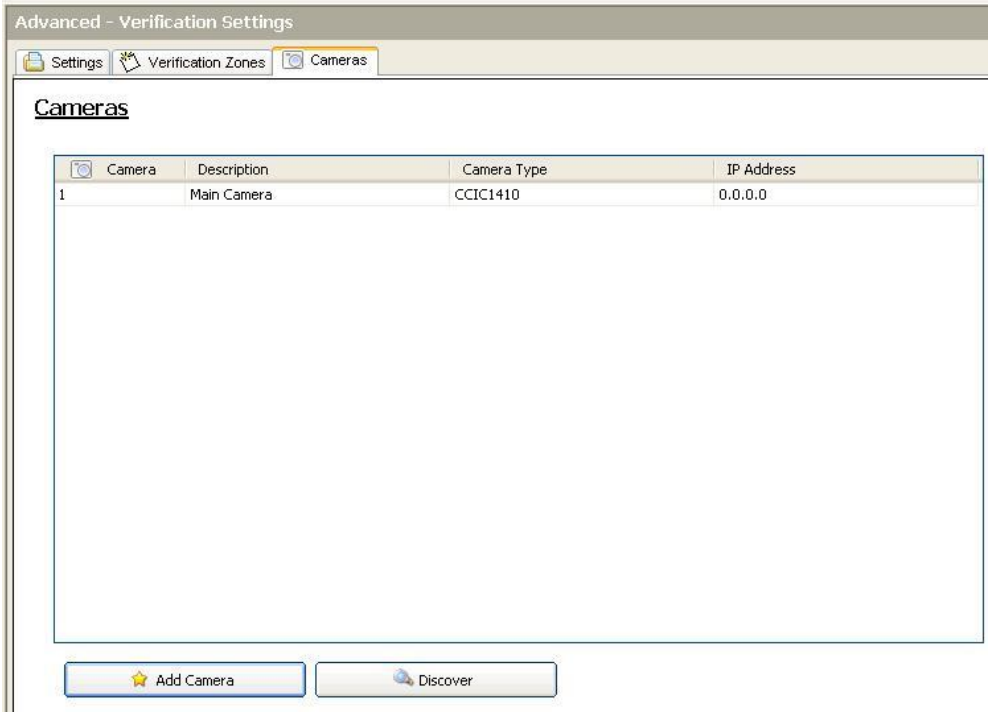
A command string is available as a default to access configuration details for the above cameras directly. Other generic IP cameras require a command string to be entered manually.

Adding Cameras

Verification

1. Click on the **Cameras** tab.

⇨ A list of any previously configured cameras is displayed.



2. Click on the **Add** button to add a new camera.
3. Click on an existing camera to edit the configuration for that camera.
4. Configure the camera. (See Configuring a Camera [→ 237])

22.1.1 Read Camera Settings

When the **Read Camera Settings** button is clicked, SPC Pro will connect to the camera to read its settings.

SPC pro uses the IP address and TCP port shown in the configuration dialog box. If authentication is enabled, it will also use the configured user name and password.

This operation will timeout and fail in any of the following cases:

- The camera is off.
- The camera is not connected.
- The IP address or port is wrong.
- The user name or password is wrong.

22.1.2 Configuring Cameras

The **Add IP Camera** dialog box is displayed when:

- the **Add Camera** button is pressed on the main **Cameras** screen to manually add a new camera.
- a camera is clicked for editing on the main **Cameras** screen.

Configure the following settings:

General Settings	
Camera ID	System generated Camera ID.
Description	Enter a description to identify this camera.
Type	Select from one of the following camera types: ● Generic ● Vanderbilt CCIC1410 ● Vanderbilt CFMC1315
Camera IP	Enter the IP address of the camera.
Camera Port	Enter the TCP port the camera listens on. Default is 80.
Command String	Enter the command string to be sent to the HTTP server on the camera in order to obtain images. This string should include the user name and password for the camera. Consult the camera documentation for the specific string required for the camera type selected. SPC Pro can configure this automatically if connected to the camera over a LAN. The default command string for a Vanderbilt CCIC1410 or CFMC1315 camera with no password is "/cgi-bin/stilljpeg". Disabled for non-generic cameras.
Pre-event images	Enter the number of pre-event images to record (0 - 16). Default is 8.
Pre-event interval	Enter the time interval, in seconds, between pre-event images (1 - 10). Default is 1 second.
Post-event images	Enter the number of post-event images to record (0 – 16). Default is 8.
Post-event interval	Enter the time interval, in seconds, between post-event images, in seconds (1 - 10). Default is 1 second.
Camera Settings (Vanderbilt CCIC1410 and CFMC1315 cameras only)	
Authentication	Check this box if authentication is required for the camera.
Username	Enter a login username for the camera for authentication.
Password	Enter a login password for the camera for authentication.
Resolution	Select the jpg picture resolution for the camera. (320 x 240 or 640 x 680) **Note:** The 320 x 240 setting is recommended if you want to view images on the browser.

Camera Settings can be modified by an engineer and updated on the remotely on the camera.

The following functions are available in this dialog box.

Button	When disabled	Function
Read Camera Settings	Always disabled for generic cameras.	Enables SPC Pro to communicate with the camera to read its settings.
Advanced Camera Settings	Always disabled for generic cameras. Enabled for other types of cameras only after the button **Read Camera Settings is** pressed and settings are successfully read.	Opens a direct browser connection to the camera for configuration purposes.
Camera Snapshot	Never.	Attempts to obtain a snapshot from the camera to test functionality.
Send Settings to Camera	Always disabled for generic	Sends configuration settings to the

	cameras.	camera.

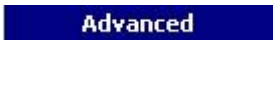
Click on the **Save** button to save the settings to the configuration file.

Click on the **Remove** button to remove the current camera configuration from the configuration file.

Click on the **Cancel** button to cancel any configuration and to return to the previous settings.

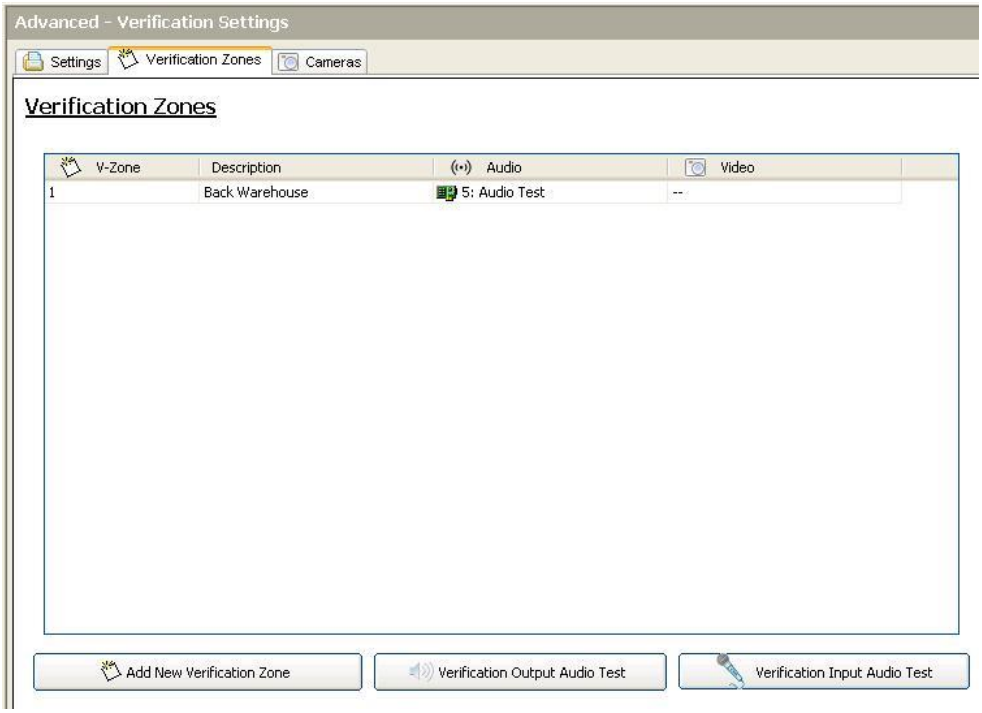
22.2 Configuring Verification Zones

To create a verification zone:



Verification

1. Click on the **Verification** tab.
   ⇨ A list of any existing verification zones is displayed.



2. Click on the **Add New verification Zone** button.
   ⇨ The following dialog box is displayed.

3. Enter a **Description** for the zone.
4. Select an **Audio** expander from the drop down list.
5. Select a **Video** from the drop down list.
6. Click on the **Save** button.
7. Assign this verification zone to a physical zone on the SPC system. (See Editing a Zone [→ 120])

The audio input and output for the verification zone can be tested by the engineer only in SPC Pro.

See also

- Editing a zone [→ 120]

22.2.1 Testing Audio

The audio input and output for the verification zones can be tested by the engineer only in SPC Pro.

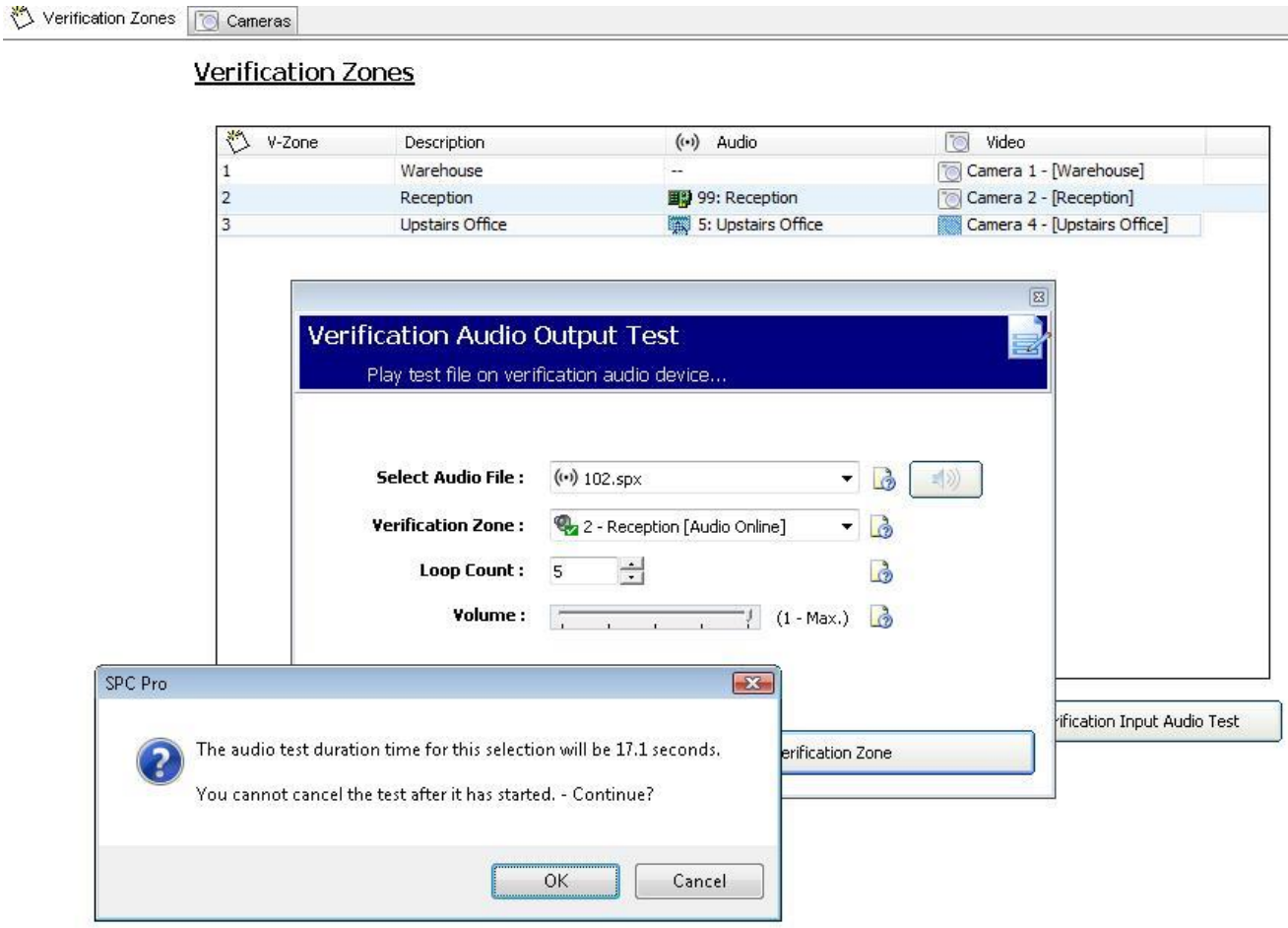
In order to carry out these tests, the PC running SPC Pro must be fitted with a headset or speakers and microphone. Ensure that the speaker volume is not muted.

22.2.1.1 Testing Audio Playback

1. Click on the **Verification Output Audio Test** button in the Verification Zones tab.
   ⇨ The following dialog box is displayed.

2. Select an **Audio File** to send to the panel. The audio files listed contain annunciation messages that are installed with SPC Pro. The files are Speex encoded.
3. Select a **Verification Zone** to test. Only zones that are online and have an audio device configured and online can be tested.
4. Set the **Loop Count** to the number of times that the audio file will be played repeatedly to enable longer tests. The maximum count is 100.
5. Set the **Playback Volume** for the audio device. Default is 7. This setting sets a maximum limit for the volume on the device in order to protect it.
6. Click on the **Play Audio via Verification Zone** button to play the file.
   - ⇨ The following message is displayed.
   - ⇨ SPC Pro calculates how long it will take to playback the audio sample (17.1 seconds in the following example) by multiplying the time per sample by the loop count, including an interval of one second between replays. This time does not include the time needed to upload the audio file to the panel.

	**⚠ WARNING**
	Keypads and access control may be disabled for several minutes while sending an audio file to the panel, depending on the size of the audio file.



The following dialog is displayed during playback.

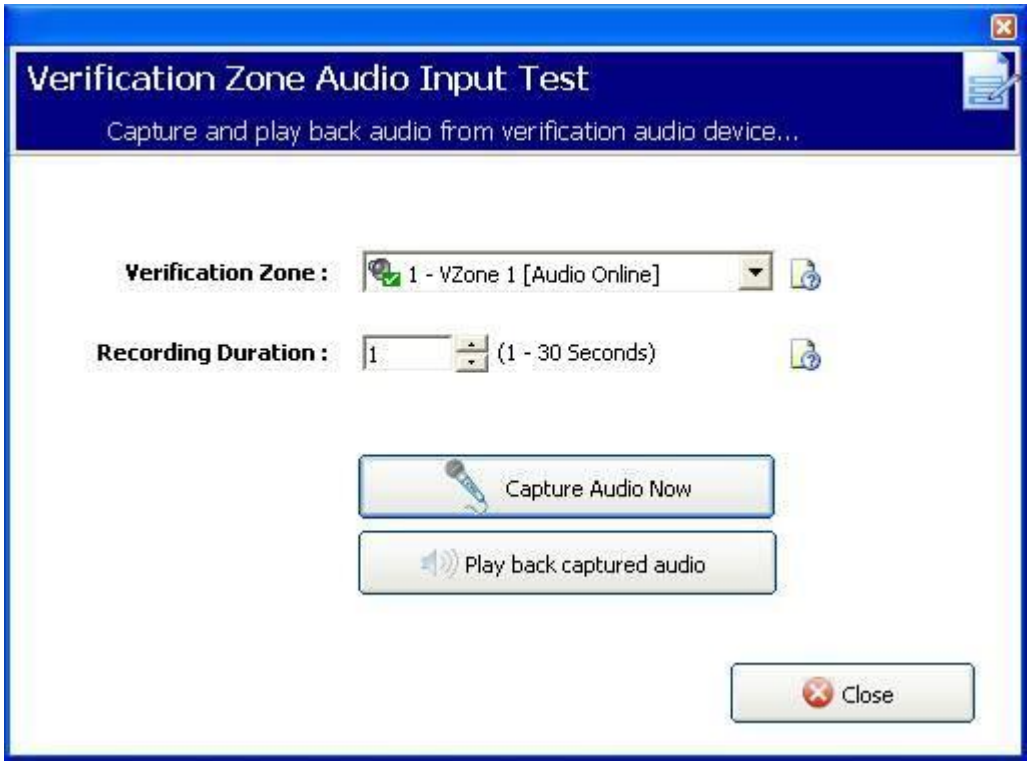
Playing the audio file on the PC

- Click on the speaker button beside the **Select Audio File** field.

The audio file will be played on the PC. This is useful to compare playback with that on the panel.

22.2.1.2 Testing Audio Recording

1. Click on the **Verification Input Audio Test** button.
   ⇨ The following dialog box is displayed



2. Select a **Verification Zone** to test. Only zones with an audio device configured and online can be tested.
3. Select the amount of time for the **Recording Duration.** Range is 1- 30 seconds.
   ⇨ A progress bar is displayed showing the elapsed recording time.
   ⇨ The captured audio is then downloaded to the PC which is indicated by another progress bar.

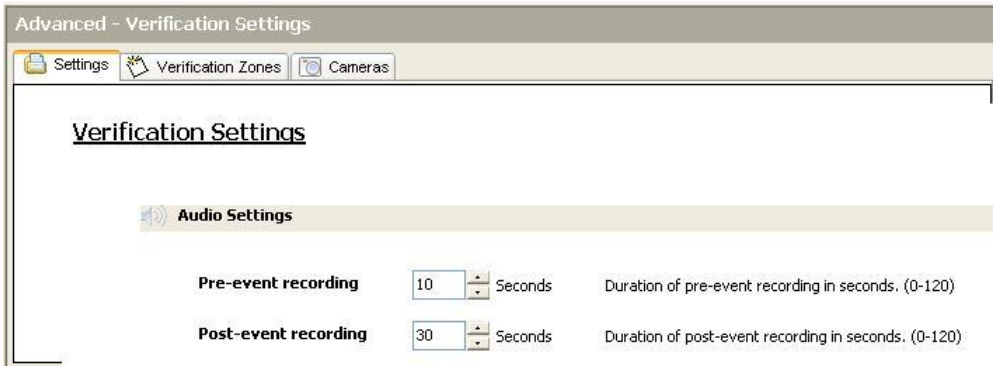
4. Click on the **Play Back Captured Audio** button which is now enabled.
   ⇨ The recorded audio is played on the PC.

22.3 Configuring Verification Settings

Note: The following settings apply to all verification zones [→ 239].

Advanced

1. Click on the **Settings** tab.
   ⇨ The following screen is displayed.



2. Configure the following settings.

Pre-event recording	Enter a required duration of pre-event audio recording, in seconds (0 - 120). Default is 10.
Post-event recording	Enter a required duration of post-event audio recording, in seconds (0 - 120). Default is 30.

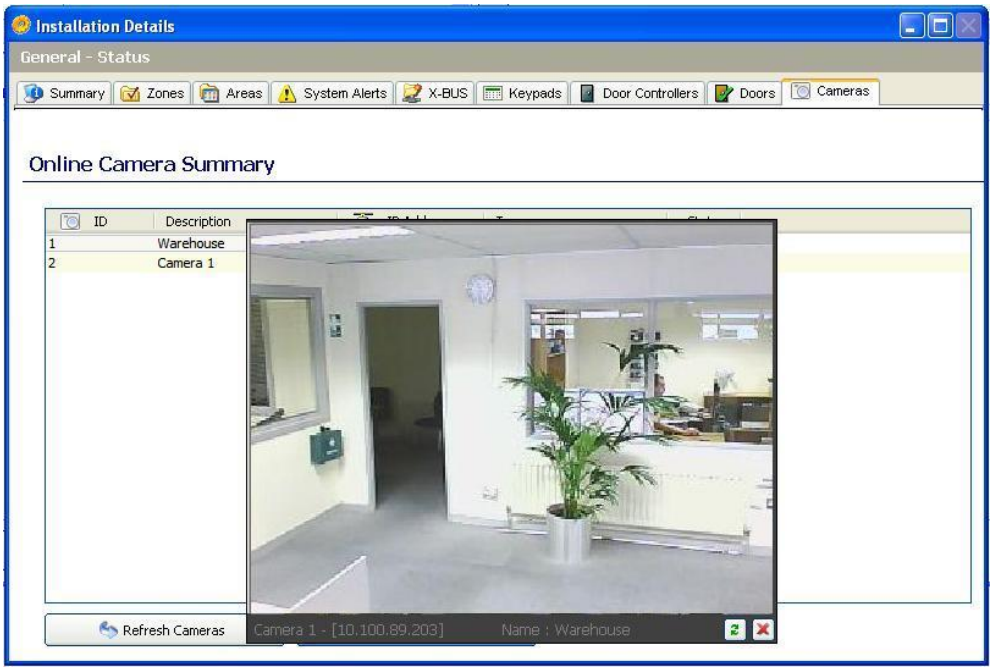
22.4 Viewing Video Images

Video images from the configured cameras can be viewed in the SPC Pro. Unlike the web browser that can display all configured cameras images simultaneously, SPC Pro can only display one camera image at a time.

To view a camera image:

General	Status

1. Click on the **Cameras** tab.
   ⇨ The **Online Camera Summary** dialog box is displayed.
2. Select a camera from the list of configured cameras.
   ⇨ An image from this camera is displayed.



3. Click on the **Refresh** icon to manually refresh the image.

To view images from other cameras, cancel the current image and select a new camera from the list in the **Online Camera Summary** dialog box.

Note: SPC Pro can display images at resolutions of 320 x 240 and 640 x 480.

23 Seismic Sensors

Vibration sensors, also called seismic sensors, are used to detect intrusion attempts by mechanical means, such as drilling or making holes through walls or safes.

Support for seismic sensors is available only if the installation type for the panel is ‘Financial’.

There are several ways to test seismic sensors. The simplest way to test seismic sensors is by hitting a wall or safe and seeing if the zone opens during a walk test. This means of testing is available with all types of seismic sensors.

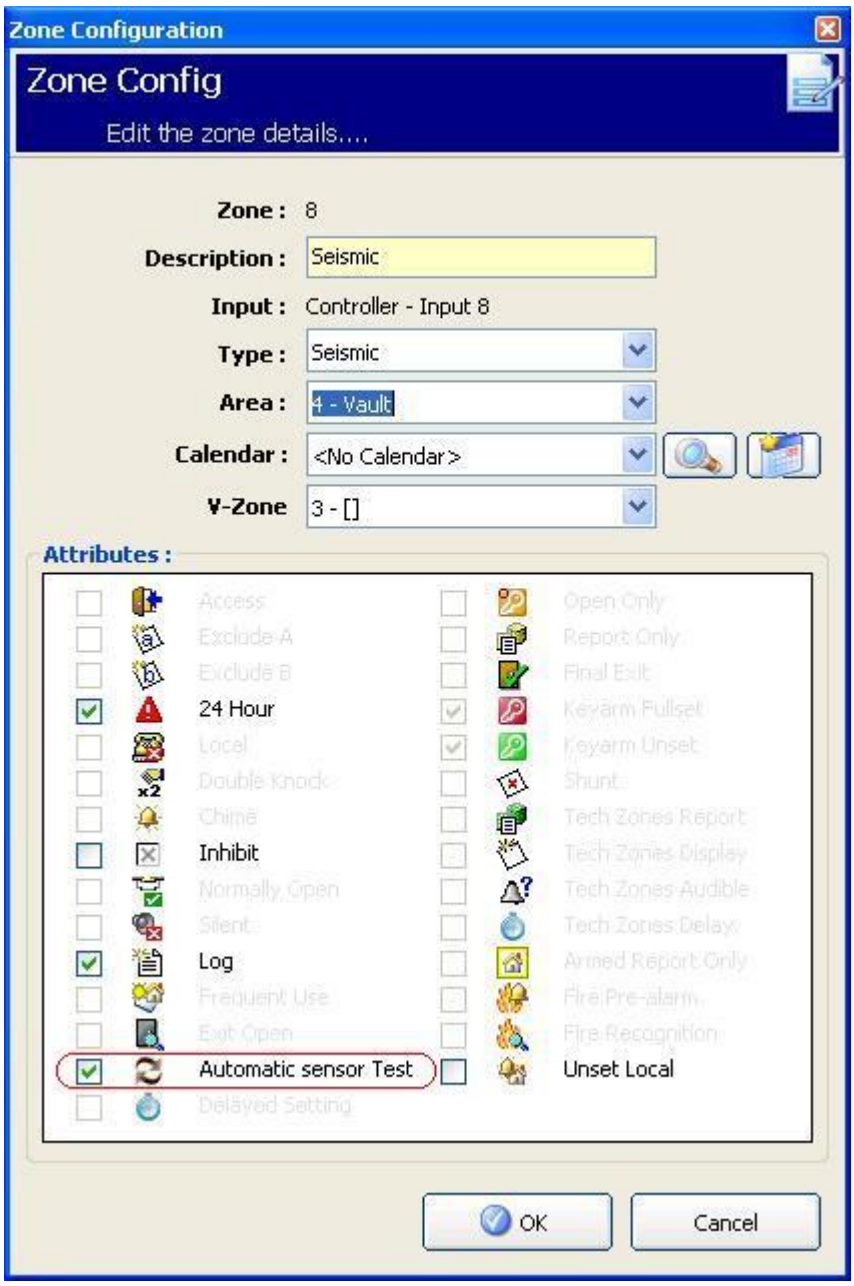
If the seismic sensor is installed with a test transmitter, the following test options are available:

- Manual testing initiated at the keypad or with SPC Pro (not supported by the browser);
- Automatic testing on a periodic basis or when the panel is set using the keypad.

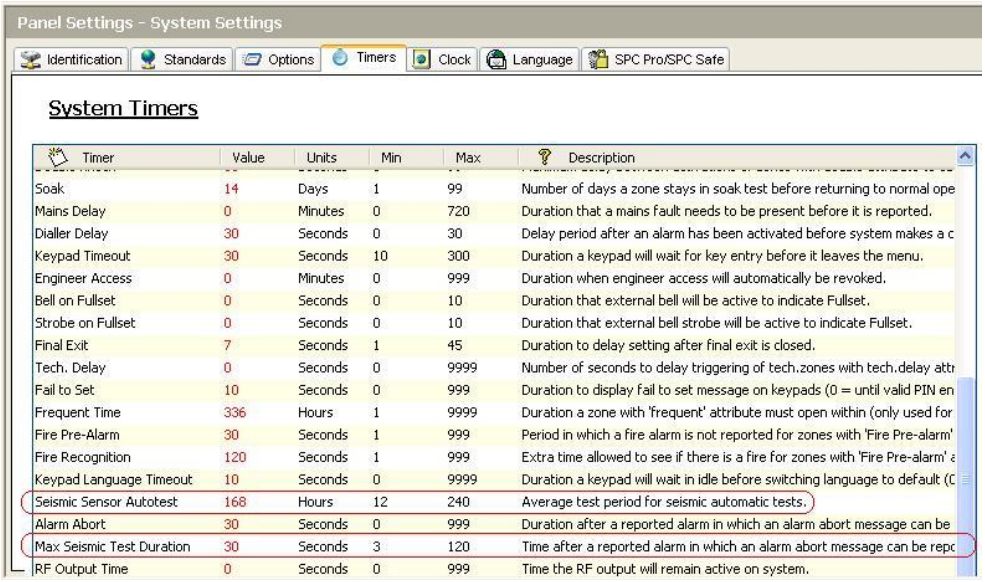
The test transmitter is a small high frequency vibrator that is attached a short distance from the sensor on the same wall. The test transmitter is wired to an output on the panel or an expander.

Configuring Seismic Sensors in the Panel

1. Configure a seismic zone. Seismic sensors must be assigned to a zone. (See Editing a Zone [→ 120])
2. Set the attributes for the zone as shown.

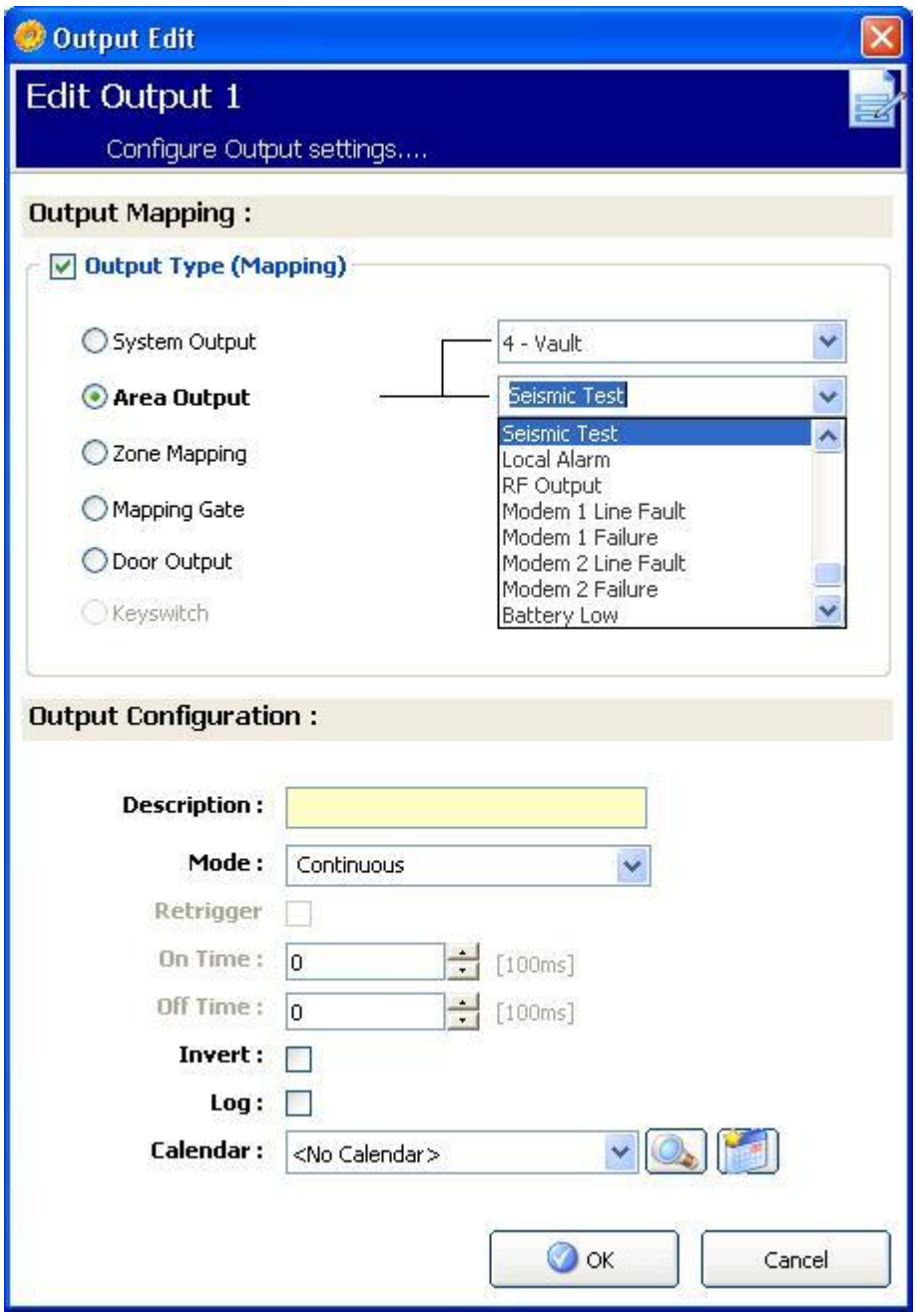


3. Enable automatic testing of the sensor with the **Automatic Sensor Test** attribute.
4. Select a calendar to control the seismic zone, if required.
5. Assign this zone to a verification zone if audio/video verification is required..
6. Configure timers to specify how often to test seismic zones (default is 7 days) and the duration of the tests. (Automatic Seismic Test zone attribute must be set). (See Timers [→ 74])



Timer	Value	Units	Min	Max	Description
Soak	14	Days	1	99	Number of days a zone stays in soak test before returning to normal ope
Mains Delay	0	Minutes	0	720	Duration that a mains fault needs to be present before it is reported.
Dialler Delay	30	Seconds	0	30	Delay period after an alarm has been activated before system makes a c
Keypad Timeout	30	Seconds	10	300	Duration a keypad will wait for key entry before it leaves the menu.
Engineer Access	0	Minutes	0	999	Duration when engineer access will automatically be revoked.
Bell on Fullset	0	Seconds	0	10	Duration that external bell will be active to indicate Fullset.
Strobe on Fullset	0	Seconds	0	10	Duration that external bell strobe will be active to indicate Fullset.
Final Exit	7	Seconds	1	45	Duration to delay setting after final exit is closed.
Tech. Delay	0	Seconds	0	9999	Number of seconds to delay triggering of tech.zones with tech.delay attr
Fail to Set	10	Seconds	0	999	Duration to display fail to set message on keypads (0 = until valid PIN en
Frequent Time	336	Hours	1	9999	Duration a zone with 'frequent' attribute must open within (only used for
Fire Pre-Alarm	30	Seconds	1	999	Period in which a fire alarm is not reported for zones with 'Fire Pre-alarm'
Fire Recognition	120	Seconds	1	999	Extra time allowed to see if there is a fire for zones with 'Fire Pre-alarm' a
Keypad Language Timeout	10	Seconds	0	9999	Duration a keypad will wait in idle before switching language to default (0
Seismic Sensor Autotest	168	Hours	12	240	Average test period for seismic automatic tests.
Alarm Abort	30	Seconds	0	999	Duration after a reported alarm in which an alarm abort message can be
Max Seismic Test Duration	30	Seconds	3	120	Time after a reported alarm in which an alarm abort message can be repo
RF Output Time	0	Seconds	0	999	Time the RF output will remain active on system.

7. Configure an output for testing a seismic zone. (See Output Types and Output Ports [→ 87])
   The output can be assigned to either the system or an area, if the panel is configured to use areas as is usually the case in financial environments. The output should only be assigned to the system if the panel does not use areas.



See also

- Timers [➙ 74]
- Configuring an Input/Output Expander [➙ 94]
- Outputs types and output ports [➙ 87]
- Editing a zone [➙ 120]

23.1 Seismic Sensor Testing

Seismic zones must be configured in order for both manual and automatic tests to be available. The results of either manual or automatic testing are stored in the system event log.

During a seismic test, one or more seismic zones are tested. When a zone is tested, all other zones in the same area are temporarily disabled as there is a single seismic test output per area

23.1.1 Manual and Automatic Test Process

A manual or automatic test operates as follows:

1. The panel activates the Seismic Test Output for the appropriate area(s) in which the seismic zone(s) are to be tested.
2. The panel then waits for all seismic zones under test to open and then verifies that all seismic sensors in the area enter the alarm state within the time configured for the '**Seismic Test Duration'**. Any zone(s) that have not opened within the maximum period are deemed to have failed the test.
3. When all seismic zones in the area are open or the maximum Seismic Test Duration has been reached (whichever comes first), the panel will clear the Seismic Test Output for that area.
4. The panel then waits a fixed time for all seismic detectors in the area to close. Any zone(s) that have not closed are deemed to have failed the test.
5. The panel then waits another fixed period before reporting the test result. The result of the test, either manual or automatic, is stored in the system event log.

The seismic output is normally high, and goes low during tests (i.e. when it is active). If this signal is not suitable for a particular sensor then the physical output can be configured to be inverted.

23.1.2 Automatically Testing Sensors

Seismic sensors are tested either periodically or after the system is set using the keypad.

Periodic Automatic Testing

Periodic automatic tests are performed on all seismic zones for which automatic tests are enabled.

Automatic tests are randomized within the configured test period and are done independently for each area.

All seismic zones in the same area (for which automatic tests are enabled) are tested simultaneously.

The **Seismic Test Interval** configuration option in the Timers [→ 74] menu determines the average test period for seismic sensors automatic tests. The default value is 168 hours (7 days) and the allowed values are in the range 12 – 240 hours.

The test time is random within the specified range +/- 15%. For example, if a test is scheduled every 24 hours, a test may be performed between 20.4 and 27.6 hours after the last test.

A seismic test is performed after a reboot if automatic tests are enabled. If the panel was in Full Engineer mode before reboot, then the test is performed only after the panel is out of Full Engineer mode after a reboot.

If a seismic test fails, a Trouble event is reported (SIA code "BT"). There is also a corresponding Restoration event (SIA code "BJ").

Automatic Test on Setting

The option **Seismic Test on Set** is configurable in the System Options [→ 66] menu. If enabled, all seismic zones in all areas that are to be set are tested before the usual setting sequence. This applies to keypad operation only.

While the test is being performed, 'SEISMIC AUTOTEST' is displayed on the keypad. If the seismic test succeeds, the setting proceeds as normal.

If all areas or an area group or a single area are selected to be set, and a seismic test fails, then 'SEISMIC FAIL' will be displayed. Pressing **Return** displays a list of the failed zones which can be scrolled through using the up and down arrow keys.

Depending on the **Inhibit** settings for the failed seismic zones and your user profile, the following can occur:

- If all of the seismic zones that failed the test have the **Inhibit** attribute set, and your user profile user is configured with the **Inhibit** right:

1. Press **Return** on any of the failed zones.

   ⇨ The message “FORCE SET ALL?” is displayed.

2. Press **Return** again to inhibit all seismic zones that failed the test. (Alternatively, go back to the previous menu.)

   ⇨ Setting proceeds as normal.

- If some of the seismic zones that failed the test do not have the **Inhibit** attribute set or your user profile user does not have the **Inhibit** right:

- Press **Return**.

  ⇨ The message ‘FAIL TO SET’ will be displayed and no areas will be set.

There is no automatic seismic test for areas that are auto-set for any reason (for example, areas activated by a calendar or trigger). Likewise there is no automatic seismic test when the system is set with SPC Com, with SPC Pro or the browser. However, there is an automatic seismic test when a virtual keypad is used with SPC Com or SPC Pro.

No event is reported if seismic testing on set fails.

The periodic automatic system test timer restarts after a test is performed after setting.

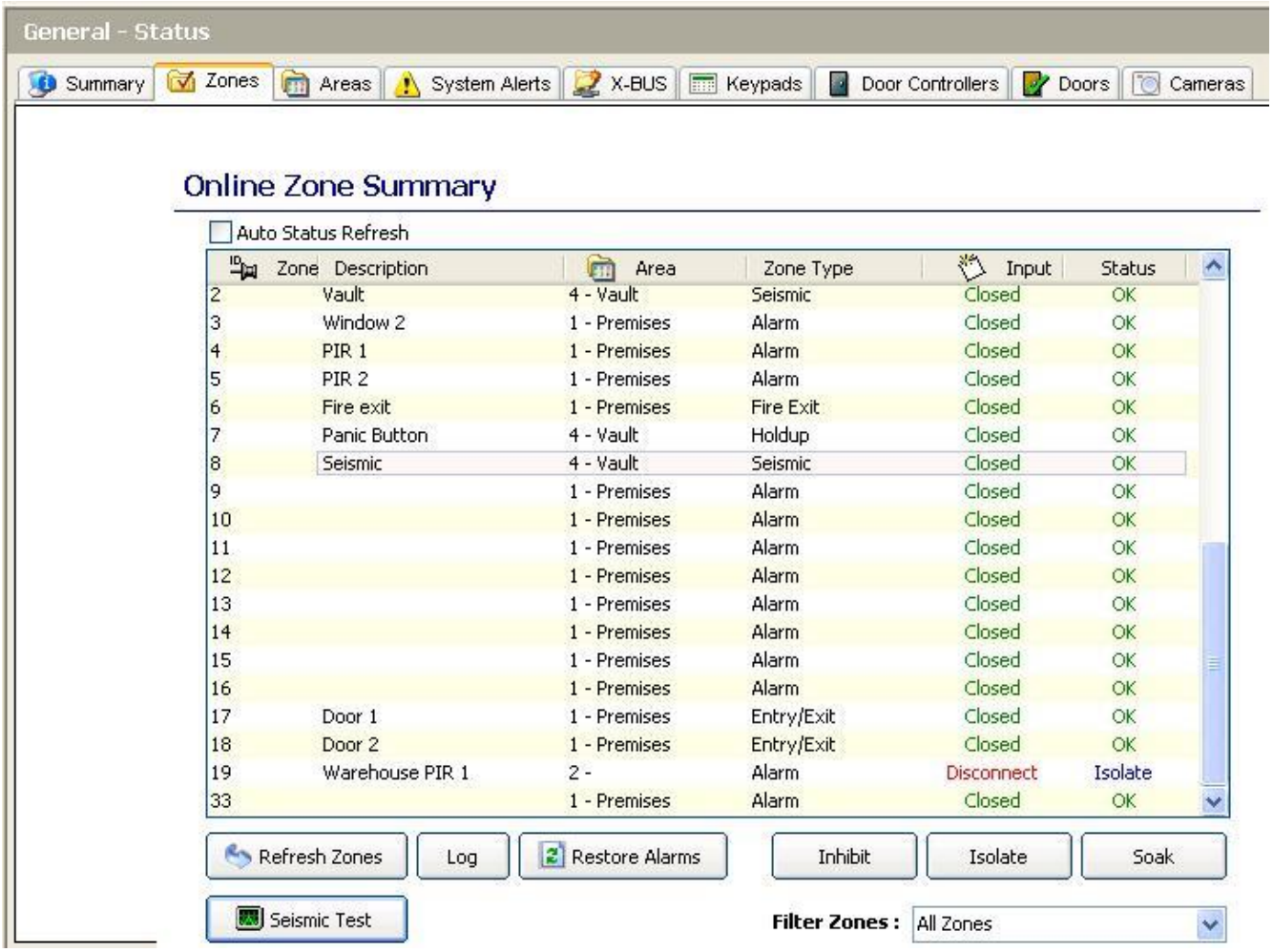
23.1.3 Manually Testing Sensors

General

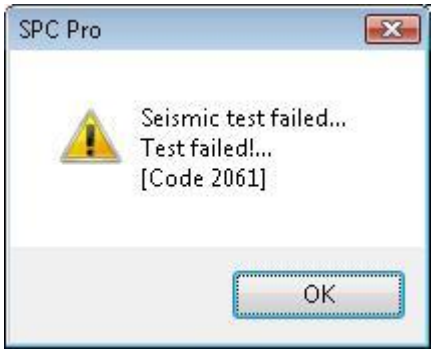
Status

To manually test sensors:

1. Select the **Zones** tab of the **General Status** dialog box.
2. Select a specific seismic zone from the list.
3. Click on the **Seismic Test** button. (Only available when a seismic zone is selected)



If the test is successful or if it fails, a message similar to the following is displayed:



The test is recorded in the event log with the following details:

- result (OK or FAIL)
- user ID (for example, 513)
- zone number and name

No event is reported as a result of the test.

24 Appendix

24.1 Network cable connections

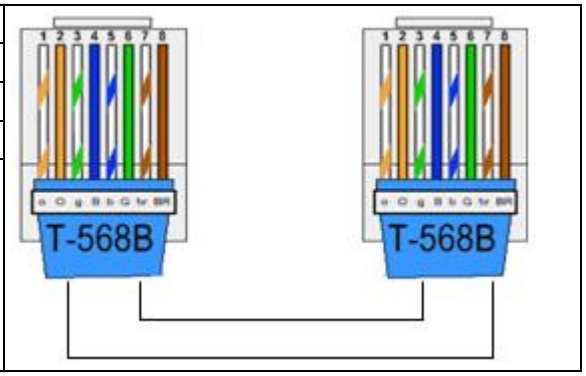
IP

A PC can be connected directly to the Ethernet interface of the SPC controller or via a LAN connection. The tables below show the 2 possible connection configurations.

- If the SPC is connected to an existing network via a hub, then connect a straight through cable from the hub to the SPC and another from the hub to the PC.
- If the controller is not connected to a network (i.e. a hub or switch is not used), then a crossover cable should be connected between the SPC controller and the PC.

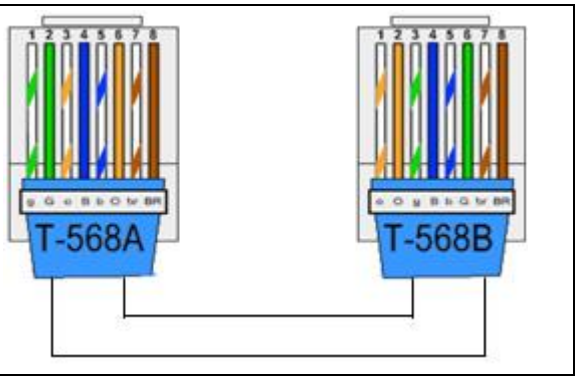
Use the straight through cable for connecting the SPC controller to a PC via a hub.

RJ45 PIN	RJ45 PIN
1 (RX +)	1 (TX +)
2 (RX -)	2 (TX -)
3 (TX+)	3 (RX+)
6 (TX-)	6 (RX-)



Use the crossover cable for connecting the SPC controller directly to a PC.

RJ45 PIN	RJ45 PIN
1 (RX +)	3 (TX+)
2 (RX -)	6 (TX-)
3 (TX+)	1 (RX +)
6 (TX-)	2 (RX -)



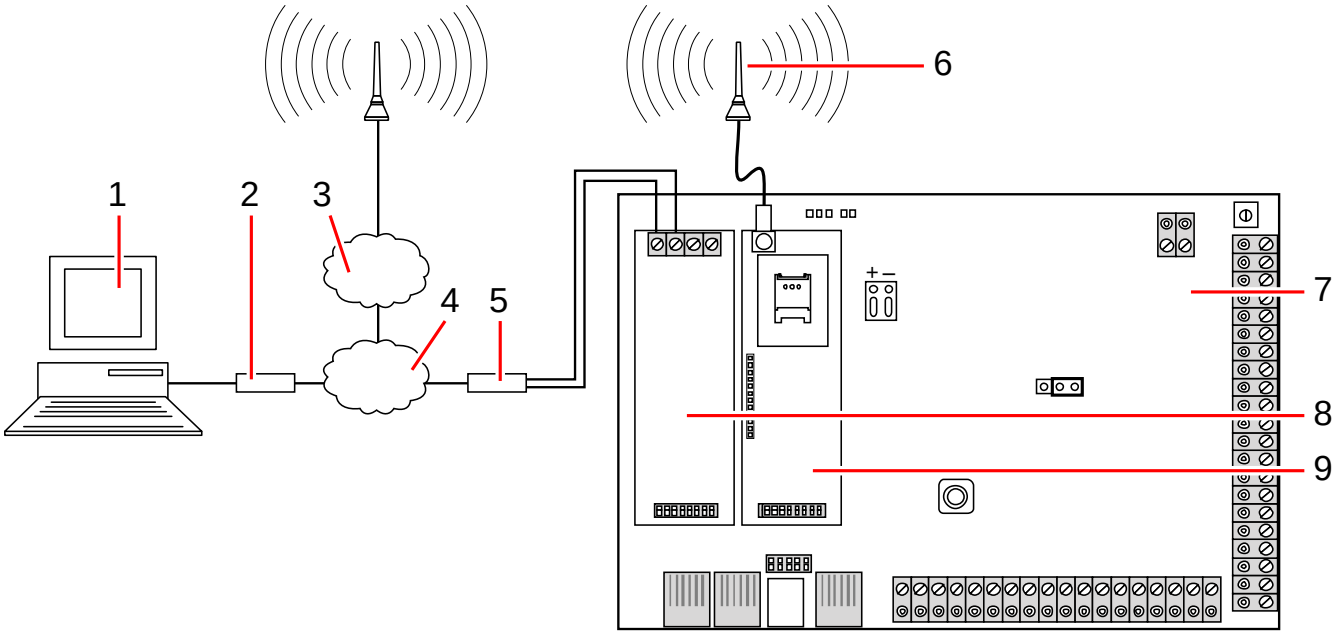
24.2 Alarm Receiving Station (ARC)

The SPC panel has the facility to communicate information to a remote receiving station when a specific alarm event on the panel has occurred. See page [➙ 253] for an overview of the Alarm Receiving Station. The engineer can configure the system to make calls to an Alarm Receiving Centre (ARC) via the PSTN or GSM network. Ensure that the PSTN or GSM modem is properly installed and functioning correctly) before configuring an ARC on the system.

When replacing or installing modules on the SPC system always ensure that the mains supply and the battery are disconnected. Ensure that all anti-static precautions are adhered to when handling connectors, wires, terminals and PCB's.

When replacing or installing modules on the SPC system always ensure that the mains supply and the battery are disconnected. Ensure that all anti-static precautions are adhered to when handling connectors, wires, terminals and PCB's

Installing the plug-in modules



1	Alarm Receiving Station (ARC)
2	PSTN Modem
3	GSM Network
4	PSTN Network
5	Telephone Line
6	External Antenna
7	SPC Controller
8	PSTN Modem
9	GSM Modem

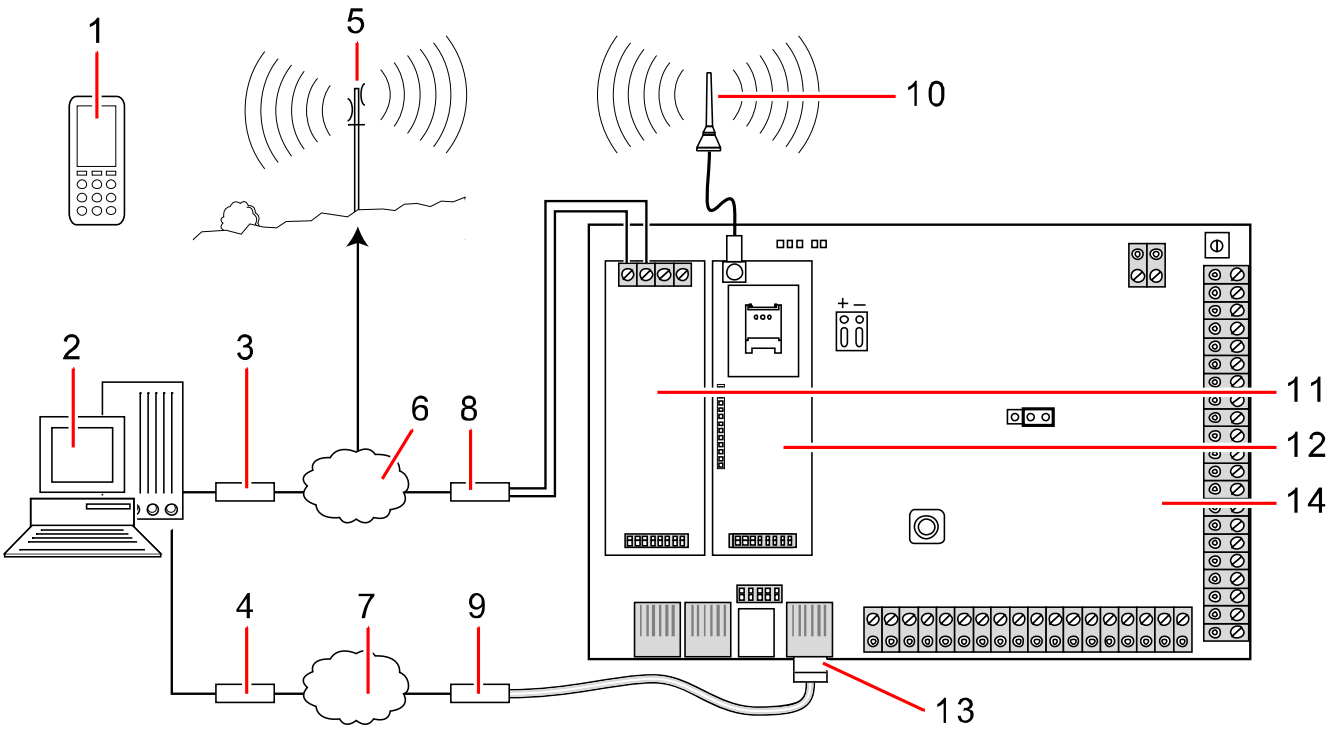
24.3 Enhanced Datagram Protocol (EDP)

IP

The system has the facility to communicate information to the SPC Com server remotely using Vanderbilt 's own protocol, the EDP (**E**nhanced **D**atagram **P**rotocol). By correctly configuring an EDP receiver on the system, it can be programmed to automatically make data calls to the SPC Com server in a remote location whenever events such as alarm activations, tampers, or arming/disarming occur. The engineer can configure the system to make calls to the remote server via the following routes:

- **PSTN** (PSTN mode required)

- **GSM** (GSM modem required)
- **Internet** (Ethernet interface)



Network

1	Control/Event reporting	**8**	Telephone line
2	SPC Com server	**9**	Router
3	PSTN modem	**10**	External antenna
4	IP network	**11**	PSTN network
5	GSM network	**12**	GSM modem
6	PSTN network	**13**	Ethernet interface
7	IP network	**14**	SPC controller

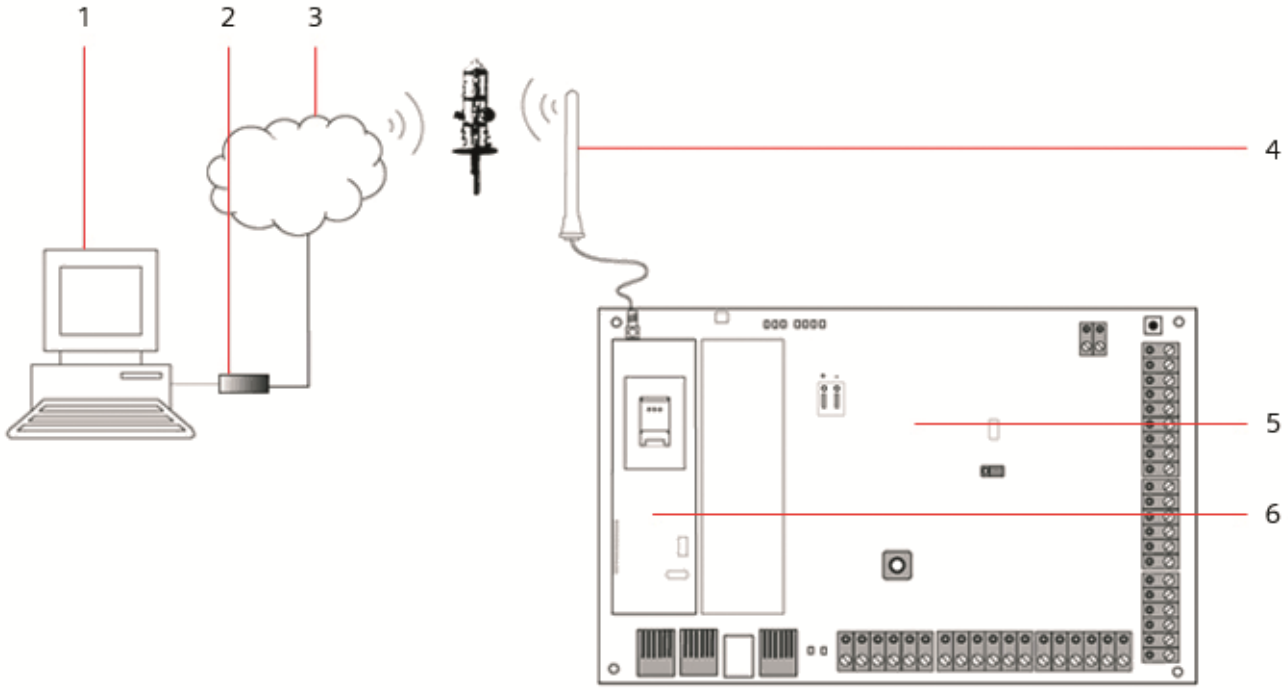
If using the PSTN network, ensure the PSTN modem is properly installed and functioning correctly and that a functioning PSTN line is connected to the A, B terminals on the PSTN modem.

If using the GSM network, ensure the GSM module is properly installed and functioning correctly (see page). An IP connection can be made across the internet to a server with a fixed public IP address.

If an IP connection is required, ensure the Ethernet interface is correctly configured (see page) and that internet access is enabled at the router.

When the SPC system has been setup to connect to the SPC Com server, an EDP receiver must be configured on the SPC.

24.4 Establishing a remote connection to the panel via GSM



1	PC with SPC Pro
2	PSTN / GSM modem
3	PSTN / GSM network
4	External antenna
5	SPC Controller
6	GSM modem

The SPC controller can be accessed via a remote connection over the GSM network. A GSM module (with SIM card) must be installed on the controller as shown above to provide remote access to the SPC. On the remote side of the connection the user must have a PSTN or GSM modem installed on a PC with SPC Pro installed. If a PSTN modem is installed then it must be connected to a working PSTN line.

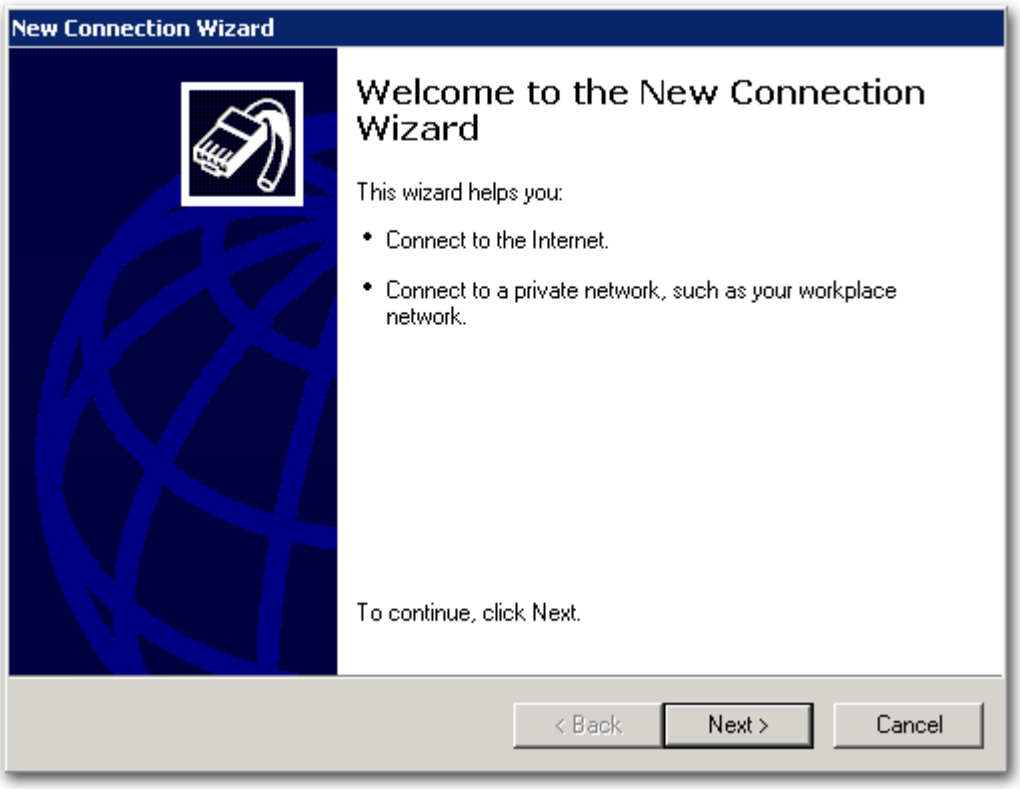
Configure the modem on the SPC controller:

Install a GSM modem on the SPC controller and check that it is functioning correctly. (Please consult the SPC Technical guide for precise details). Enter Full Engineer programming from a keypad connected to the SPC and configure the modem (Primary or Backup) to answer an incoming call.

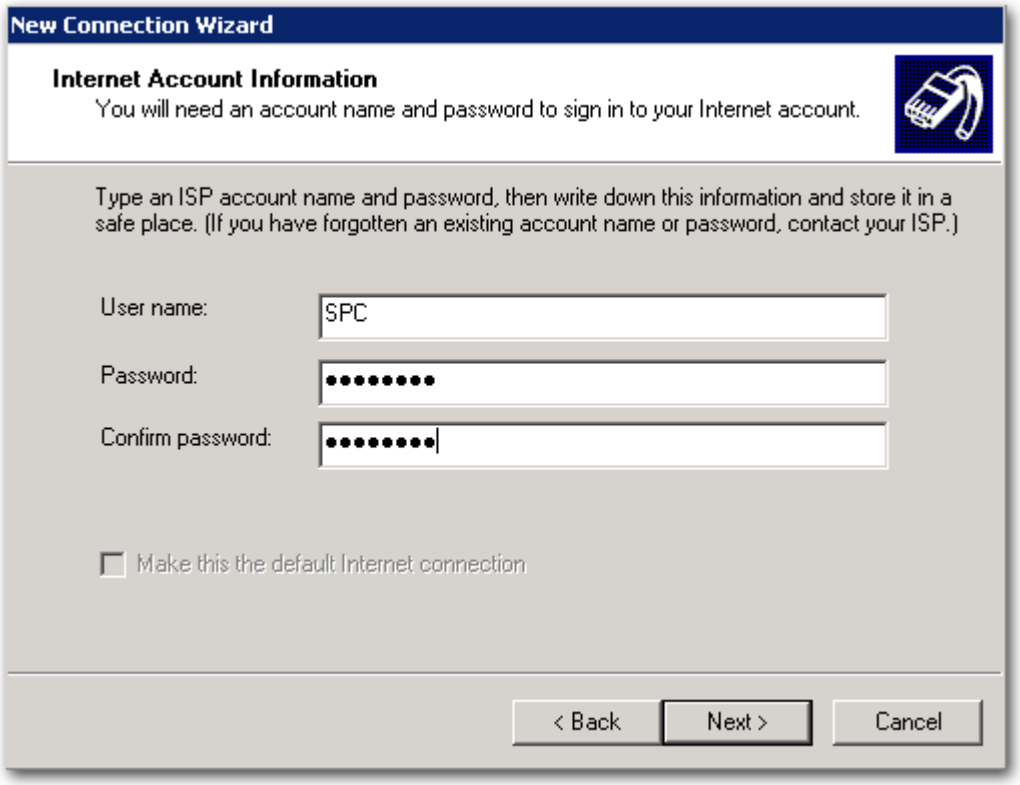
- Enable modem – Set to Modem Enabled.
- Type – Displays the type of modem (GSM).
- Country code – Select the relevant country code (Ireland, UK, Spain, etc…).
- Answer mode – Select numbered rings. This tells the modem to wait for a number of rings before answering the incoming call.
- Modem rings – Select the number of rings to allow before answering the call (8 rings max).

On Windows XP

1. Open the New Connection Wizard by clicking on **Control panel > Network Connections > Create New Connection** (in the Network Tasks window).



2. In the Network Connection Type window, select **Connect to the Internet**.
3. In the Getting ready window choose **Setup my connection manually**.
4. In the Internet connection window choose **Connect using Dialup modem**.
5. In the connection name window enter the connection name e.g. “SPC Remote connection”.
6. In the Phone number to dial window, enter the phone number of the PSTN line connected to the SPC PSTN modem.
7. In the connection availability window choose whether you want this connection to be available to all users.



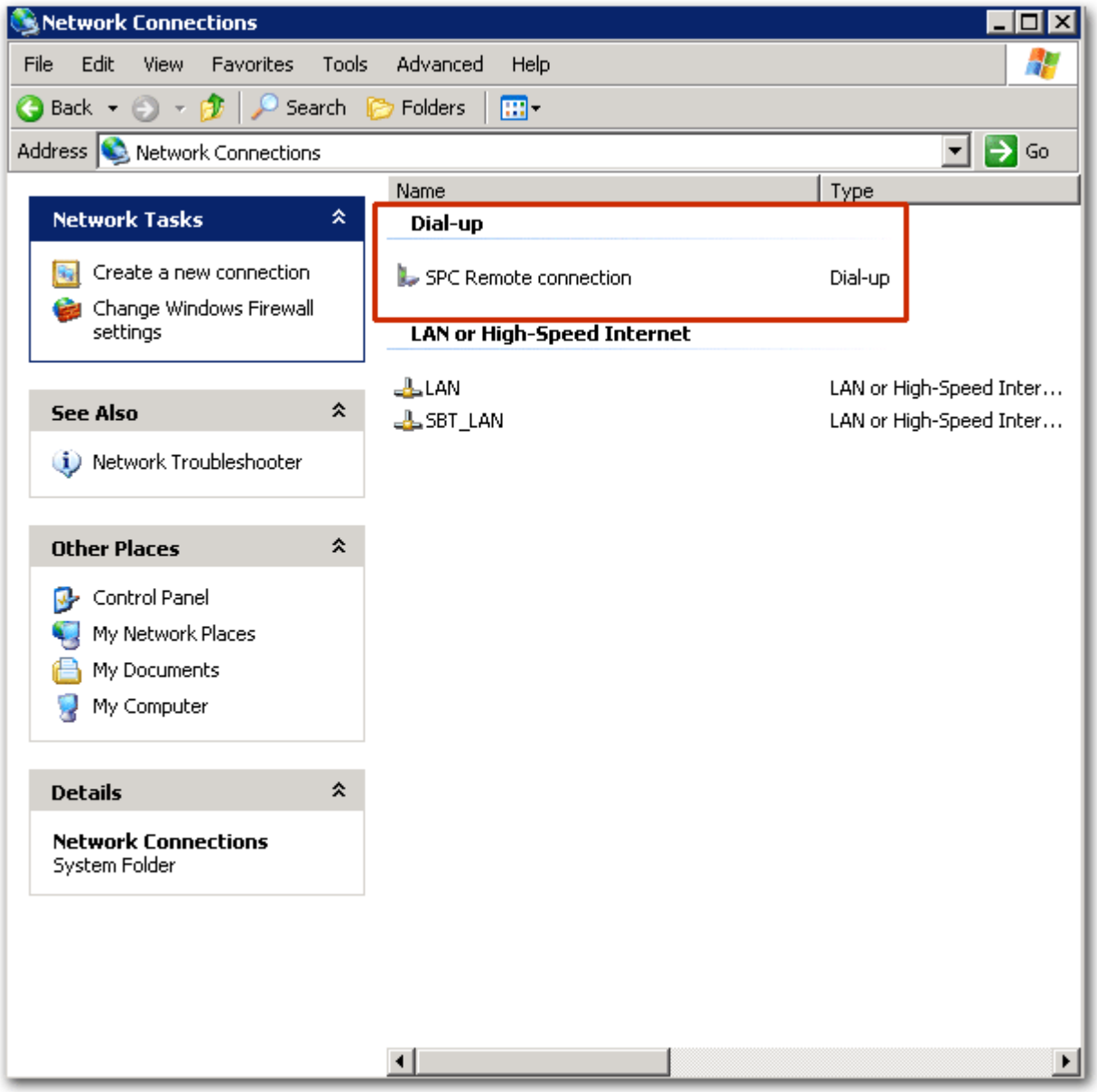
8. In the internet account information window enter the following details:
   - Username : SPC
   - Password: password
   - Confirm Password: password

   ⇨ The window **Completing the new connection wizard** will be displayed.
9. Click the button **Finish** to save the Dial-up connection to your PC.

To activate this dial-up connection:

- Click the icon located in the menu **Control panel > Network Connections**.

  ⇨ The PC will make a data call to the PSTN line connected to the SPC PSTN module.



⇨ The SPC PSTN module will answer the incoming data call after the designated number of rings and establish an IP link with the remote computer.

⇨ An IP address will be automatically assigned to the remote PC by the SPC system.

To obtain this IP address:

1. Right click the icon Dial-up.
2. Click the tab **Details**.

⇨ The IP address will be displayed as the Server IP address. This is the IP address to specify in the SPC Pro connection type window. See page [→ 26].

It is recommended that the BAUD rate of the modem on the PC is set at 9600 bps.

24.5 Zone types

The zone types on the SPC system are programmable from both the browser and keypad. The table below gives a brief description of each zone type available on the SPC system. Each zone type activates its own unique output type (an internal flag or indicator) that can then be logged or assigned to a physical output for activation of a specific device if required.

Zone Type	Processing Category	Description
ALARM	Intruder	This zone type is the default zone type setting and is also the most frequently used zone type for standard installations. An Open, Disconnected, or Tamper activation in any mode (except unset) causes an immediate full alarm. In the Unset mode, Tamper conditions are logged, causing the alert message ZONE TAMPER and triggering a local alarm. In Partset A, Partset B and Full Set modes, all activity is logged.
ENTRY/EXIT	Intruder	This zone type should be assigned to all zones on an entry/exit route (i.e. a front door or other access area to the building or premises). This zone type provides an entry and exit time delay. The entry timer controls this delay. When the system is being full set, this zone type provides an exit delay allowing time to vacate an area. The exit timer controls this delay. In Part set A mode, this zone type is inactive.
EXIT TERMINATOR	Intruder	This zone type is used in conjunction with a push button on an exit route and acts as an exit terminator – that is, it provides an infinite exit delay period and will not allow the system to set until the button is pressed.
FIRE	Hold-up	Fire zones are 24-hour zones for fire monitoring and their response is independent of panel operating mode. When any fire zone opens, a full alarm is generated and the FIRE output type is activated. If the 'Report only' attribute is set then activation will only be reported to the central station and a Full Alarm will not be generated.
FIRE EXIT	Hold-up	This is a special type of 24-hour zone for use with fire exit doors that should never be opened. In Unset mode, an activation of this zone will trip the Fire-X output, causing alert messages.
LINE	Fault	Telemetry line monitoring input. This is usually used in conjunction with a telephone line health output from an external digital dialer or direct line communication system. When activated, it produces a local alarm in Unset mode and a full alarm in all other modes.
PANIC ALARM	Hold-up	This zone type is active on a 24-hour basis and activated via a panic button. When a Panic zone is activated it will report a Panic event, independent of panel arming mode. All activation's are logged and reported if log attribute is active. If the SILENT attribute is set then the alarm will be silent (Activation is reported to ARC), otherwise it will generate a Full alarm.
HOLD-UP ALARM	Hold-up	This zone type is active on a 24-hour basis and activated via a button. When a Hold-up zone is activated it will report a Hold-up event, independent of panel arming mode. The SILENT attribute is set by default therefore the alarm will be silent. If unset, it will generate a full alarm. All activations are logged and reported if log attribute is active.
TAMPER	Tamper	When open in the Unset mode, a Local Alarm is generated but no external bell will activate. If the system is Full Set, a Full alarm is generated. If the Security Grade of the system is set to Grade 3 then an engineer code is required to restore the alarm.
TECHNICAL	Intruder	The tech zone controls a dedicated tech zone output. When a tech zone changes state, the tech zone output will follow. That is: • When the tech zone opens, tech zone o/p triggers on • When the tech zone closes, tech zone o/p goes off If more than one tech zone has been assigned, the tech zone output will remain on until all tech zones are closed.

MEDICAL	Hold-up	This zone type is used in conjunction with radio or hardwired medical switches. Activation in any mode will: ● Trigger the medical digital communicator output (unless Local attribute is set) ● Cause the panel buzzer to sound (unless Silent attribute is set) ● Display the message Medic Alarm
KEYARM	Intruder	This zone type is normally used in conjunction with a key lock mechanism. A Keyarm zone will SET the System / Area / Common Areas when it is OPENED and will UNSET the System/Area/Common Areas when it is CLOSED. ● If the zone with the keyarm zone type is assigned in an non area system then the keyarm operation will SET/UNSET the system. ● If the zone with the keyarm zone type is assigned to an area then the keyarm operation will SET/UNSET the area. ● If the zone with the keyarm zone type is assigned to a common area then the keyarm operation will SET/UNSET all the areas in the common area. ● If the 'Open only' attribute is set then the armed status of the System / Area / Common Areas will toggle on each opening of the key lock. (i.e. Open once to SET the system, Close and Open again to UNSET) ● If the 'Fullset Enable' attribute is set then zone activation will only Fullset the system. ● If the 'Unset Enable' attribute is set then zone activation will only unset the system. Keyarming will force set the system/area and auto-inhibit any open zones or fault conditions. **Note: Your system will not comply with EN standards if you enable this zone type to set the system without first entering a valid PIN on an external device.**
SHUNT	Intruder	This zone type is only available in Commercial Mode of operation. Though the Shunt Alarm Zone type can be set in Domestic Mode of operation, it has no effect. This zone type when opened inhibits all zones that have the shunt attribute set. This operation applies for both SET and UNSET modes. As soon as the shunt zone is closed, the zones with the shunt attribute set will become un-inhibited again.
X-SHUNT	Intruder	This zone type is only available in Commercial Mode of operation. A zone programmed with the x-shunt zone type inhibits the next consecutive zone on the system whenever it is opened. This operation applies for both SET and UNSET modes. As soon as the x-shunt zone type is closed the next zone becomes de-inhibited again.
DETECTOR FAULT	Fault	Detector Fault zones are 24 hour zones that are applicable to a detector device, for example, a PIR. The fault zone type triggers the Fault output. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed.
LOCK SUPERVISION	Intruder	Only available in Commercial mode. Used to monitor a door lock. System can be programmed not to set unless door is locked.
SEISMIC	Intruder	Only available if the panel is in Financial mode of operation. Vibration sensors, also called seismic sensors, are used to detect intrusion attempts by mechanical means, such as drilling or making holes through walls or safes.
ALL OKAY	Intruder	This zone type enables a special entry procedure to be implemented using a user code and 'All Okay' input. A silent alarm is generated if an All Okay button is not pressed within a configurable time after a user code is entered. (See Areas [→ 122] for details of 'All Okay' configuration)

		All Okay uses two outputs, Entry Status (Green LED) and Warning Status (Red LED), to indicate entry status using LEDs on the keypad.
UNUSED	Intruder	Allows a zone to be disabled without the need for each zone to have EOL resistors fitted. Any activation on the zone will be ignored.
HOLDUP FAULT	Fault	Holdup Fault zones are 24 hour zones that are applicable to a holdup signaling device, for example, a WPA. The fault zone type triggers the Fault output. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed. This zone type will report the SIA messages, HT (Holdup Trouble) and HJ (Holdup Trouble Restore) and for CID, a sensor trouble event (380) is produced.
WARNING FAULT	Fault	Warning Fault zones are 24 hour zones that are applicable to a warning signaling device, for example, an internal or external bell. The fault zone type triggers the Fault output. When the system is armed, a fault output is triggered. Both the keypad LED and the buzzer are activated when Unarmed. This zone type will report the SIA messages, YA (Bell Fault) and YH (Bell Restore) and for CID, a sensor trouble event (380) is produced. Note: On a grade 2 system, a cable fault will cause a fault and not an alarm.
SETTING AUTHORISATION.	Intruder	Applicable to Blockschloss operation. This zone type is used to send a setting authorisation signal to the panel that the Blockschloss is ready to set. The Set option must be selected for the 'Setting Authorisation' attribute for the area
LOCK ELEMENT	Intruder	If using a Lock Element (bolt) with a Blockschloss, this zone type signals the position of the lock element to the panel (locked or unlocked). This bolt locks the door in the set state. This signal is checked during setting process. If the 'locked' information is not received, the setting will fail.
GLASSBREAK	Intruder	Zone is connected to an RI S 10 D-RS-LED glassbreak interface in combination with GB2001 glassbreak detectors. • This zone type is available on controllers and expanders. It is not available as wireless or as a door zone type if the DC2 is configured as a door. • The zone type reports in the same way as an alarm zone over SIA and contact ID. • The rights to restore/inhibit/isolate glassbreak are the same as the alarm zone type • Power up condition — As the power is supplied by the panel any state changes within the first 10 seconds are ignored in order to allow the device to settle. • Reset condition — Signals are ignored from the glassbreak interface for 3 seconds after the device has been reset. • Exiting engineer mode — The glassbreak output may be toggled when exiting engineer mode, in which case the signals from this sensor will be temporarily ignored for 3 seconds.

24.6 Zone attributes

The zone attributes on the SPC system determine the manner in which the programmed zone types function.

Zone attribute	Description
Access	When the 'Access' attribute on a zone is set, then on opening that zone, an alarm will not be generated if either the entry or exit timer is running. When the system is full set the Access attribute is not active and opening the zone will initiate a full alarm. The 'Access' attribute is most often used for PIR

	sensors located close to an entry/exit zone. It allows the user free movement within the access area while the entry or exit timer is counting down. The 'Access' attribute is only valid for Alarm zone types. All connected devices (Bells - Internal & External, Buzzers, Strobe) are activated. **NOTE**: An alarm zone with Access attribute can automatically be changed to an entry/exit zone in Partset mode if the Partset Access Option is set.
Exclude A	If the 'Exclude A' attribute on a zone is set, then an alarm will not be generated by that zone opening while the panel is in the Partset A mode. The 'Exclude A' attribute is valid for Alarm zone type and Entry/Exit zones only. A FULL alarm is generated if a zone with the EXCLUDE A attribute is opened while the system is in FULLSET or PARTSET B Mode (Bells - Internal & External, Strobe).
Exclude B	When the 'Exclude B' attribute is set, the zone opening will not generate an alarm while the panel is in the Partset B mode. The 'Exclude B' attribute is valid for Alarm zone type and E/Exit zones only. A FULL alarm is generated if a zone with the EXCLUDE B attribute is opened while the system is in FULLSET or PARTSET A Mode (Bells - Internal & External, Strobe).
24 Hour	If a Zone is assigned the '24 Hour' attribute, then it is active at all times and will cause a full alarm if opened in any mode. This attribute can only be assigned to the ALARM zone type. Generates a FULL Alarm in UNSET, SET and PARTSET modes. **NOTE**: The 24 Hour attribute overrides the settings of any of the other attributes for a particular alarm zone.
Local	When the 'Local' attribute is set, an alarm generated by a zone opening will not result in the external reporting of the event. The 'Local' attribute is valid for Alarm, E/Exit, Fire, Fire Exit and Medic zone types.
Unset Local	When this attribute is set, an alarm generated by the zone opening when the area is fullset or partset will be reported in the usual way. However, if the area is unset there will be only a local alarm i.e keypad buzzer, LED flash and zone display. This attribute is only applicable to Alarm, Fire and Seismic zones.
Double Knock	Use this attribute to deal with troublesome detectors. (i.e. some detectors may generate activation signals spuriously, thereby inadvertently trigger alarms on the system). If the same double knock zone activates twice during the double knock period, then an alarm is generated. Double knock time is set in seconds (see page [→ 74]). Two open actions within that time period will generate an alarm. All open double knock zones are logged when the system is armed.
Chime	When the 'Chime' attribute is set for a zone, any opening of the zone during the Unset mode will cause the internal buzzers to activate for a short period (2 seconds approx.). The Chime attribute is valid for Alarm, Entry/Exit, and Tech. zones types.
Inhibit	When the 'Inhibit' attribute is set, a user may inhibit this zone. The inhibit operation will disable that fault or zone for one setting period only.
Normal Open	When the 'Normal Open' attribute is set, the system expects that a connected detector/sensor is a Normally Open device. (i.e. a sensor is deemed to be activated whenever the contacts are closed on the device).
Silent	If the 'Silent' attribute is set then there will be no audio or visual indications of the Alarm. The alarm activation will be sent to the Receiver station. If the system is unset then a warning message is shown on the display.
Log	If this attribute is set then all zone state changes are logged.
Exit Open	If set then zone will be indicated if open during setting.
Frequent	This attribute only applies to Remote Maintenance*. If this attribute is set for a zone, the zone must open for remote service purposes within the defined frequent time period.
End of Line	The End Of Line (EOL) attribute provides a number of input zone wiring

	configurations on the system.
Analysed	The Analysed Attribute must be set for a zone if that zone is wired with an inertia sensor. The Pulse count and Gross attack values should be programmed for each inertia sensor on the system in accordance with the results of a simple calibration of the device.
Pulse Count	Pulse count trigger level for analysed inertia sensors.
Gross Attack	Gross attack trigger level for analysed inertia sensors
Final Exit	The Final Exit attribute can only be assigned to an Entry/Exit Zone type. Use this attribute to override the standard process of counting down the exit timer whenever the system is full set. When all other entry/exit routes in the premises are closed, fullset the system and close the final exit/entry zone. As soon as the door is closed the Final Exit time will count down to setting the system.
Shunt	A zone with the shunt attribute set will be inhibited whenever a shunt type zone is opened. This provides a mechanism to group the inhibition of zones with the opening of the shunt zone type.
Report Only	This attribute only applies to the FIRE zone type. If this attribute is set, then activation of the fire zone will only report the activation to the central station. No alarms will be generated on site.
Open Only	This attribute only applies to the KEYARM zone type. If set then the setting state of the building will toggle on openings only.
Fullset Enable	This attribute only applies to the KEYARM zone type. If this attribute is set then zone activation will Fullset the system/area. Apply this attribute if it is intended that the user should only have the ability to FULLSET the system from a keyarm zone.
Unset Enable	This attribute only applies to the KEYARM zone type. If set then zone activation will Unset the system/area. Apply this attribute if it is intended that the user should only have the ability to UNSET the system from a keyarm zone.
Tech Zone Report	Allows a zone when opened, regardless of the mode to send an alarm to the ARC in FF, CID, SIA and SIA extended. When areas are selected, the alarm will only be sent to the ARC to which the area has been assigned to. This would be a “UA” Unknown Alarm followed by the zone number and text if SIA extended is selected. It will also send an SMS to the end user and engineer if select to do so when the unconfirmed alarm filter is selected.
Tech Zone Display	Allows an opening zone to be displayed on the system keypad. The alert led should also activate. When areas are selected it will only be displayed on the keypad which is assigned to the area in which the zone has been selected. The alert may only be displayed on the keypad when the area is in the unset mode and not in the Part A, Part B and set mode.
Tech Zone Audible	Allows an activated zone to operate the buzzer. This will operate the same as the Tech Zone Display in the different setting modes and on systems with areas.
Tech Zone Delay	Allows the zone to have a programmable delay. The delay is variable from 0 to 9999 seconds and will apply to all Tech Zones. The operation is the same as the Mains Delay timer, if the zone is closed within the delay time, then no alarm is sent to the ARC, no SMS is sent to the user and the Technical Output will not trip. NOTE: The Technical Output will not trip until the delay timer has expired.
Armed report only	Openings are reported only in armed mode.
Fire pre-alarm	If enabled and a fire alarm occurs, a Fire Pre-alarm timer is started and internal bells and buzzers are activated. (See Timers [→ 74].) If the alarm is not cancelled within the timer duration, a fire alarm is confirmed, internal and external bells are triggered and an event is sent to ARC.
Fire Recognition	If enabled, a Fire Recognition timer is activated which adds extra time to the Fire Pre-alarm timer duration until a file alarm is reported for the zone. See Timers [→ 74].
Seismic Test/Automatic Sensor	A Seismic zone type may be tested manually or automatically. This attribute

Test	allows automatic testing to be enabled. Refer to the section on timers [→ 74] for details of how to configure the timer that determines how often the panel tests any seismic zones that have this attribute set. The default value for the timer is 7 days.
Timed	The 'Timed' attribute is used for Key Arm zones to delay the setting of an area. The delay follows the exit timer for the area to which the key arm is associated.
Verification	Select the configured verification zone to assign to this zone to trigger audio/video verification.
Force Set	If enabled, the keyarm device can set the system, automatically inhibiting all open zones.

24.7 Applicable attributes to zone types

The following table shows which attributes are applicable to each zone type:

			⊛		⊛	⊛		⊛				⊛		⊛	⊛	⊛	⊛		⊛					
Zone Type / **Attribute**	Alarm	Entry/Exit	Exit Term	Fire	Fire Exit	Line	Panic	Holdup	Tamper	Tech	Medical	Keyarm	Unused	Shunt	X-Shunt	Detector Fault	Lock Supervision	Seismic **	All Okay	Hold-up Fault	Warning Fault	Setting Authorisation	Lock Element	Glass Break
Access	√																							√
Exclude A	√	√																					√	√
Exclude B	√	√																					√	√
24 Hour	√																	√						√
Local	√	√		√	√						√					√				√	√		√	√
Unset Local	√			√														√						√
Double Knock	√																							√
Chime	√	√								√												√		√
Inhibit	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√		√	√
Normal Open	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√		√	√	√	√	√	√
Silent	√						√	√																√
Log	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Shunt	√	√			√																			√
Frequent *	√	√	√							√		√		√	√									√
Analyzed	√	√			√																			
Pulse Count	√	√			√																			
Gross attack	√	√			√																			
Calendar	√	√	√	√	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√
Verification	√	√		√	√		√	√		√	√							√						√
Exit Open		√																						
Seismic Test																		√						
Timed												√												
Report Only				√																				
Open Only												√										√		
Final Exit		√																					√	
Fullset enable												√												
Unset enable												√												
Shunt	√	√			√																			√
Report (Tech)										√														
Display(Tech)										√														
Audible (Tech)										√														
Delay (Tech)										√														
Report When Set										√														
Fire Pre-alarm				√	√																			
Fire Recognition				√	√																			
Force set												√												

⊛ *Only available in Commercial Mode.*

** Only in conjunction with Remote Maintenance.*

*** Only available in Financial Mode*

24.8 FlexC Glossary

Acronym	EN50136-1 Description	FlexC Example

AE	**Annunciation Equipment** Equipment located at an ARC which secures and displays the alarm status, or the changed alarm status of ASs in response to the receipt of incoming alarms before sending a confirmation. The AE is not part of the ATS.	SPC Com XT Client
ARC	**Alarm Receiving Centre** Continuously manned centre to which information concerning the status of one or more AS is reported.	SPC Com XT would be installed in an ARC.
AS	**Alarm System** Electrical installation, which responds to the manual or automatic detection of the presence of a hazard. The AS is not part of the ATS.	SPC Panel
ATE	**Alarm Transmission Equipment** Collective term to describe SPT, MCT (Monitoring Centre Transceiver) and RCT.	-
ATP	**Alarm Transmission Path** Route an alarm message travels between an individual AS and its associated AE. The ATP starts at the interface between AS and SPT and ends at the interface between RCT and AE. For notification and surveillance purposes the reverse direction may also be used.	A defined path between the SPC panel and SPC Com XT. e.g. A system with ethernet as the primary path and GPRS as a backup path would be two separate ATPs of an ATS.
ATS	**Alarm Transmission System** ATE and networks used to transfer information concerned with the state of one or more ASs at a supervised premises to one or more AEs of one or more ARCs. An ATS may consist of more than one ATP.	A system combining one or multiple paths between SPC panel and SPC Com XT.
RCT	**Receiving Centre Transceiver** ATE at the ARC including the interface to one or more AE(s) and the interface to one or more transmission networks and being part of one or more ATPs. In some systems this transceiver may be able to indicate changes of the status of an AS and to store log-files. This may be needed to increase the ATS availability in case of AE failure.	SPC Com XT Server
SPT	**Supervised Premises Transceiver** ATE at the supervised premises including the interface to the AS and the interface to one or more transmission networks and being part of one or more ATPs.	Integrated onto SPC Panel using Ethernet, GPRS, PPP over PSTN.

FlexC also uses the following acronyms.

Acronym	Description
ASP	**Analogue Security Protocols** The analogue security protocols traditionally used for alarm transmission over the telephone network e.g. SIA, Contact ID.

24.9 FlexC Commands

The following table lists the commands that you can enable for a command profile. The command profile you assign to an ATS defines how you can control a panel from SPC Com XT.

Command Filter	Commands
System Commands	Get Panel Summary
	Set the System Time and Date
	Grant Engineer Access
	Grant Manufacturing Access
Intruder Commands	Get the Area Status
	Get the Change Mode Status of an Area
	Change the mode (Set/Unset) of an Area
	Get Status of Panel Alerts
	Perform actions on Alerts
	Silence Bells
	Get Zone Status
	Control a Zone
	Get the System Log
	Get the Log for a Zone
	Get the Wireless Log
Output Commands	Get Mapping Gate Status
	Control Mapping Gates
User Commands	Verify a User on the Panel
	Get a User Configuration
	Add a User
	Edit a User
	Delete a User
	Get a User Profile Configuration
	Add a User Profile
	Edit a User Profile
	Delete a User Profile
	Change a User's own PIN
Calendar Commands	Read Calendar Configuration
	Add a Calendar
	Edit a Calendar
	Edit a Calendar Week
	Delete a Calendar
	Add a Calendar Exception Day
	Edit a Calendar Exception Day

	Delete a Calendar Exception Day
Communication Commands	Get the status of the Ethernet
	Get the status of a modem
	Get the log for a modem
	Get the log for a ARC receiver
FlexC Commands	Get the status of a FlexC ATS
	Get the Network Log for a FlexC ATS
	Get the Event Log for a FlexC ATS
	Get the log for a FlexC ATP
	Get the Network log for a FlexC ATP
	Export a FlexC ATS configuration file
	Import a FlexC ATS configuration file
	Delete a FlexC ATS
	Delete a FlexC ATP
	Delete a FlexC Event Profile
	Delete a FlexC Command Profile
	Request a testcall for a FlexC ATP
Access Control Commands	Get the Configuration for a Door
	Read the Status for a Door
	Control a Door
	Get the Access Log
Verification Commands	Read a Camera Image
	Get the Status of a Verification Zone
	Get the data for a Verification Zone
	Send data to a Verification Zone
Virtual Keypad Commands	Control keypad
File Commands	Upgrade the Panel Firmware
	Upgrade Peripheral Firmware
	Upload a File
	Download a File
	Saves the Panel Configuration
	Reset the Panel
Legacy Commands	Get Panel Info
	Get Panel Status
	Get Headers of Configuration Files
	Get Language Configuration
	Get Intruder Configuration
	Get Status of X-BUS Devices
	Get the Area Configuration

24.10 ATS Category Timings

This table describes the EN50136-1 ATS Category Timings laid down in the standard and how the FlexC implementation meets these standards.

		EN50136-1 ATS Category Timing Requirements				FlexC Implementation of ATS Category Timing Requirements			
ATS	Default	Event	Primar	Backup	Backup	Event	Primar	Backup	Backup

Category	Interfaces	Timeout	y Polling Timeout	ATP Polling Timeout (Primary OK)	ATP Polling Timeout (Primary Down)	Timeout	y Polling Timeout	ATP Polling Timeout (Primary OK)	ATP Polling Timeout (Primary Down)
SP1	Cat 1 [Ethernet]	8 min	32 days	-	-	2 min	30 days	-	-
SP2	Cat 2 [Ethernet]	2 min	25 hr	-	-	2 min	24 hr	-	-
SP3	Cat 3 [Ethernet]	60 s	30 min	-	-	60 s	30 min	-	-
SP4	Cat 4 [Ethernet]	60 s	3 min	-	-	60 s	3 min	-	-
SP5	Cat 5 [Ethernet]	30 s	90 s	-	-	30 s	90 s	-	-
SP6	Cat 6 [Ethernet]	30 s	20 s	-	-	30 s	20 s	-	-
DP1	Cat 2 [Ethernet] Cat 2 [Modem]	2 min	25 hr	50 hr	25 hr	2 min	24 hr	24 hr 30 min	24 hr 10 min
DP2	Cat 3 [Ethernet] Cat 3 [Modem]	60 s	30 min	25 hr	30 min	60 s	30 min	24 hr 30 min	30 min
DP3	Cat 4 [Ethernet] Cat 4 [Modem]	60 s	3 min	25 hr	3 min	60 s	3 min	24 hr 30 min	3 min
DP4	Cat 5 [Ethernet] Cat 5 [Modem]	30 s	90 s	5 hr	90 s	30 s	90 s	4 hr 10 min	90 s

24.11 ATP Category Timings

The following table shows the settings applied for event timeouts, polling intervals (active and non-active) and polling timeouts (active and non-active) for each ATP category. For the purpose of ethernet, polling interval and retry interval are identical. To reduce costs related to GPRS calls, the interval and retry interval for GPRS paths differ, for example, Cat 3 [Modem] polls once every 25 minutes and thereafter it polls every 60s for 5 minutes until it times out after 30 minutes. For a visual overview of the configured polling interval, go to **Status - FlexC - Network Log**.

!

If an ATP is up and active and then goes down, it will remain on active polling rates for two more polling cycles before converting to the **ATP Down** polling intervals.

Ethernet ATP Categories		Polling when ATP Active			Polling when ATP Non-active			Polling when ATP Down	
ATP Category	**Event Timeout**	**Polling Interval**	**Retry Interval**	**Polling Timeout**	**Polling Interval**	**Retry Interval**	**Polling Timeout**	**Polling Interval**	**Timeout**
Cat 6 [Ethernet]	30 s	8 s	30 s	20s	8 s	30 s	20 s	30 s	30 s
Cat 5 [Ethernet]	30 s	10s	30 s	90s	10s	30 s	90 s	30 s	30 s
Cat 4 [Ethernet]	60 s	30 s	30 s	3 min	30 s	30 s	3 min	30 s	30 s
Cat 3 [Ethernet]	60 s	60 s	60 s	30 min	60 s	60 s	30 min	60 s	30 s
Cat 2A [Ethernet]	2 min	2 min	2 min	4 hr	2 min	2 min	4 hr	2 min	30 s
Cat 2 [Ethernet]	2 min	2 min	2 min	24 hr	2 min	2 min	24 hr	2 min	30 s
Cat 1 [Ethernet]	2 min	2 min	2 min	30 days	2 min	2 min	30 days	2 min	30 s
Modem ATP Categories									
Cat 5 [Modem]	30 s	10 s	30 s	90 s	4 hr	2 min	4hr 10 min	10 min	90 s
Cat 4A [Modem]	60 s	60 s	60 s	3 min	4 hr	2 min	4hr 10min	30 min	90 s
Cat 4 [Modem]	60 s	60 s	60 s	3 min	24 hr	2 min	24 hr 30 min	1 hr	90 s
Cat 3 [Modem]	60 s	25 min	60 s	30 min	24 hr	2 min	24 hr 30 min	4 hr	90 s
Cat 2A [Modem]	2 min	4 hr	2 min	4hr 10min	24 hr	2 min	24 hr 30 min	4 hr	90 s
Cat 2 [Modem]	2 min	24 hr	2 min	24hr 10min	24 hr	2 min	24 hr 30 min	24 hr	90 s
Cat 1 [Modem]	2 min	24 hr	10 min	25 hr	30 days	10 min	30 days 1 hr	7 days	90 s

Issued by
Vanderbilt

Clonshaugh Business and Technology Park
Clonshaugh
Dublin
D17 KV84
www.service.vanderbiltindustries.com

Document ID A6V10216077
Edition 01.10.2015