PRT-TS50

Protege LCD Touchscreen Keypad

Installation Manual

Last Published: 08-Oct-21 2:04 PM

Contents

Introduction

The Protege LCD Touchscreen Keypad provides a sleek, user friendly human interface to the Protege System, an advanced technology security product providing seamless and powerful integration of access control, security and building automation.

The current features of the keypad include:

- Securely login with user codes from 1 to 8 digits.
- Intuitive menu function allowing scrollable options according to user security level, with quick access short cut keys for the power user.
- Dual code and master code features for secure ATM and banking vault area access with automatic timeout and delayed opening functions.
- Individual reportable duress code trouble for each Protege keypad.
- Activation of 3 reportable panic events (Panic, Medical and Fire).
- Smoke detector reset provided on Clear and Enter keys, selectable for an output or output group.
- 4 inputs (duplex mode) that can be used to perform any system alarm and automation functions, along with a dedicated enclosure tamper switch.
- 1 low current output for driving any signaling device.
- 5" capacitive touchscreen.
- 480 x 800 color LCD display.
- Configurable for portrait or landscape orientation.
- Available in white or black.

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- AS/NZS 2201.1 Intruder Alarm Systems
- The Local Authority Having Jurisdiction (AHJ)

Mounting

The keypad should be mounted on a wall with adequate air flow around and through it.

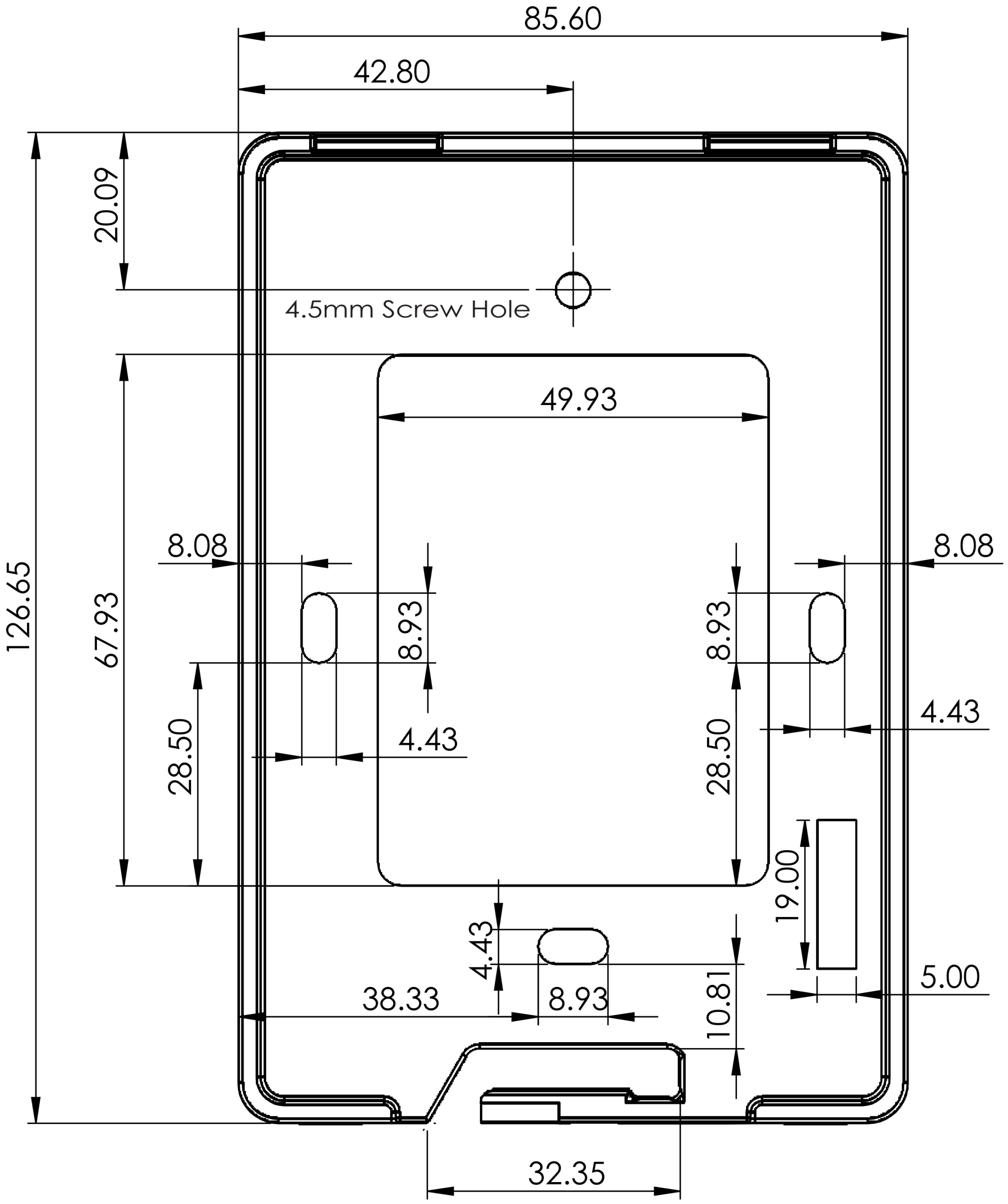
The LCD Touchscreen Keypad can operate in either portrait or landscape orientation and can be changed by loading the appropriate firmware version. For more information, see Orientation (page 16).

Mounting Instructions

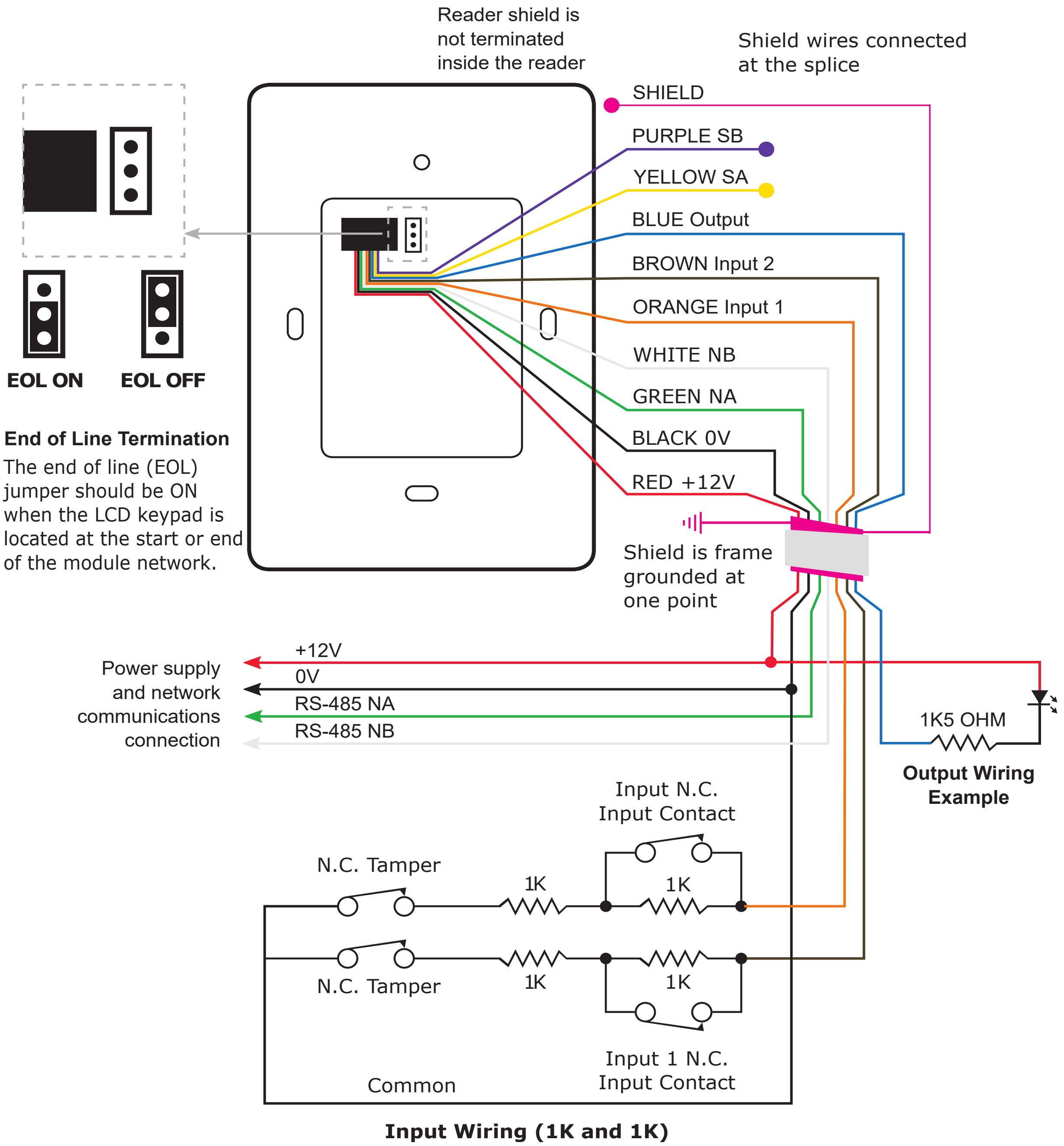
1. Select where to mount the LCD Touchscreen Keypad, ensuring it is mounted a minimum of 1.1m (3.5ft) away from other wiring such as ACM power, computer data wiring, telephone wiring and wiring to electric lock devices. Use the Technical Diagram provided below as a guide to correctly position the unit.
2. Hold the rear case half against the wall and mark the mounting holes and cable entry area. The cable entry area should align with a hole cut through the plaster wall-board. Cables are intended to be run inside the wall. Use appropriate screws (not supplied) to affix the case to the wall.
3. Run the wiring. Refer to the Communication section of this manual (see page 9) for the electrical connections. Leave about 20cm (8") of wire protruding through the center of the mounted half of the case and connect the wiring to the reader electronics.
4. Align the top of the front body of the reader onto the recessed hinge points at the top of the rear case, then press gently on the front body until the bottom portion snaps in to place onto the rear case.

Technical Diagram

The dimensions shown below outline the essential details needed to help ensure the correct installation of the LCD Touchscreen Keypad.



Wiring Diagram



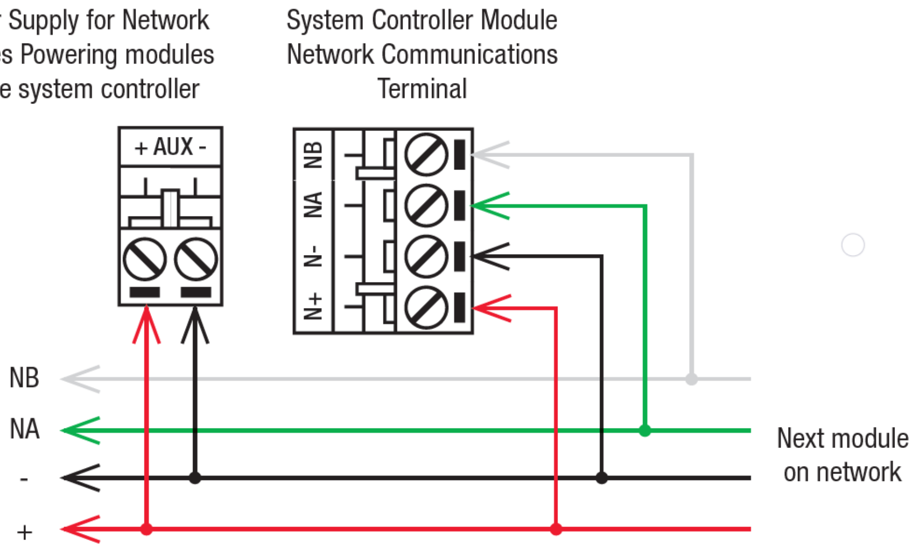
End of Line Termination

The end of line (EOL) jumper should be ON when the LCD keypad is located at the start or end of the module network.

Input Wiring (1K and 1K)

Communication

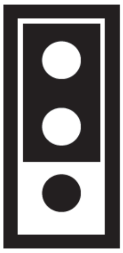
The Protege system incorporates encrypted RS-485 communications technology for its module network. Each system controller supports up to 250 keypads.


Power Supply for Network Devices Powering modules on the system controller
System Controller Module Network Communications Terminal
+ AUX -
NB
NA
N-
N+
NB
NA
-
+
Next module on network

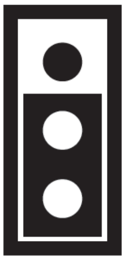
Connections

End of Line Termination (EOL)

The EOL (End of Line) jumper should be placed in the ON position when the keypad is inserted as the **first or last** module on the RS-485 network.



EOL Jumper OFF



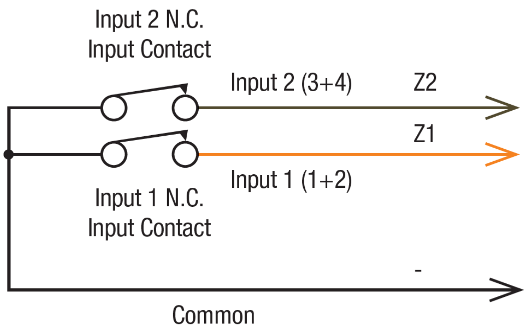
EOL Jumper ON

Inputs

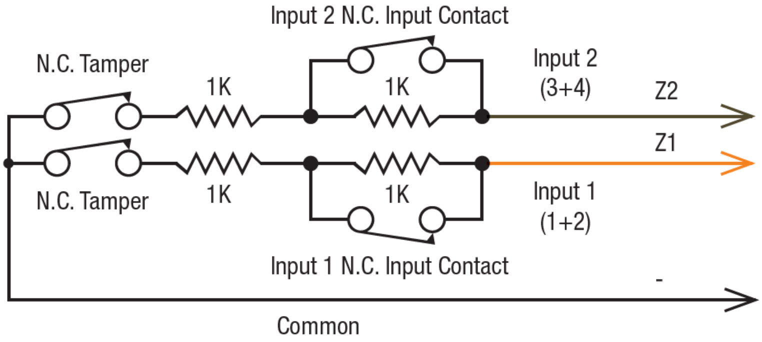
The keypad is capable of connecting to 4 inputs, each of which can be programmed to perform the required function in the Protege system.

The following diagrams show examples of the input wiring configuration settings that can be programmed under the input options within the Protege software.

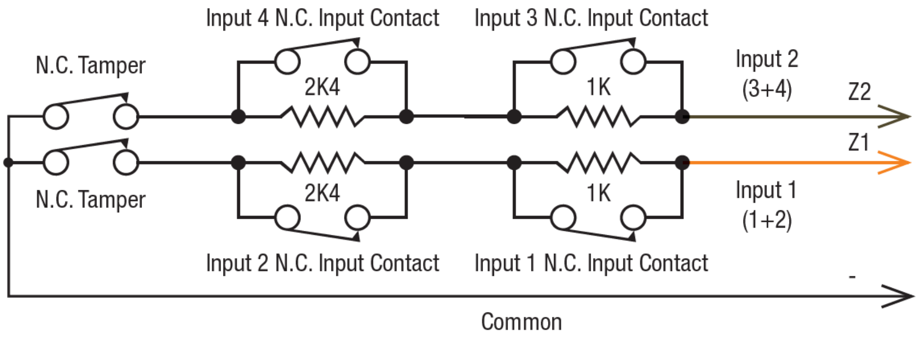
Input (No Resistors):



Input (1K and 1K):



Input Duplex Mode (1K and 2K4):


Input 4 N.C. Input Contact
Input 3 N.C. Input Contact
N.C. Tamper
2K4
1K
Input 2
(3+4)
Z2
Z1
N.C. Tamper
2K4
1K
Input 1
(1+2)
Input 2 N.C. Input Contact
Input 1 N.C. Input Contact
-
Common

To utilize the input duplex mode configuration shown above, the **Duplex Inputs** setting must be enabled in the keypad programming (**Keypads | Options 2**).

Trouble Inputs

Each keypad can monitor up to 8 trouble inputs.

Trouble inputs are used to monitor the module status and in most cases are not physically connected to an external input.

The following table details the trouble inputs that are configured in the system and the trouble type and group that they activate.

Trouble Input	Function	Type	Group
KPXXX:01	**Module Tamper** Opens when the keypad is removed from the wall.	Module Tamper	System
KPXXX:02	Reserved	-	-
KPXXX:03	**Keypad Panic** Keys 1 and 3 are pressed together generating a panic message.	-	-
KPXXX:04	**Keypad Duress** A user code with the duress option enabled has entered a code on the keypad.	-	-
KPXXX:05	Reserved	-	-
KPXXX:06	Reserved	-	-
KPXXX:07	**Too Many Codes** Too many incorrect codes have been entered at the keypad and it has been locked out for the programmed lockout time.	Number of Attempts	Access
KPXXX:08	**Module Offline** The keypad has either been removed from the system or lost communications.	Module Lost	System

Replace 'xxx' with the appropriate address of the module that you are programming.

The panic and duress features have not been evaluated for UL/ULC installations.

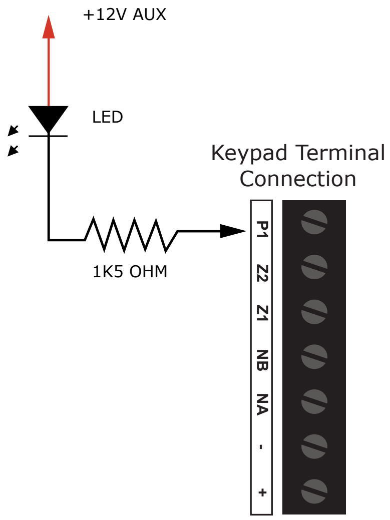
Outputs

The keypad has 5 programmable outputs. These outputs are used to control the system status indicators, system beeper and the open collector output. The outputs can be activated and deactivated based on specific events or functions within the Protege System.

Output	Function
KPXXX:01	Open collector output on the keypad connector (P1)
KPXXX:02	Armed status indicator (Red)
KPXXX:03	Disarmed status indicator (Green)
KPXXX:04	Beeper output
KPXXX:05	Confidentiality mode

Replace 'xxx' with the appropriate address of the module that you are programming.

Example Open Collector Output Connection (P1):



Warning: The open collector output can switch to a maximum capacity of 50mA. Exceeding this amount will damage the output.

Configuration

Before the keypad will communicate with the Protege system it must be assigned an address.

To program an address using the system configuration menu, apply power to the keypad, and while the screen displays **Initializing** press the [**CLEAR**] key, then the [**ENTER**] key. The configuration screen is displayed. Set the available options as required.

The configuration menu can only be accessed when the keypad powers up and is initializing. It cannot be accessed when the keypad is operational.

Language

The operating language can be selected by scrolling through the list of available language options.

Keypad Address

The address selection sets the address of the keypad. This address must be a unique address in the Protege system that is below an address of 250.

Select the **Address** menu to access the setting. Use the keypad keys to set the new address and press **Save** to save the setting. To exit without making changes press **Cancel**.

Theme

Toggle the **Theme** slider to select the dark or light keypad display configuration.

Backlight Brightness Setting

The backlight brightness setting adjusts the brightness of the screen when the keypad is in use.

Move the **Backlight** slider or use the touchscreen keypad to set the brightness level and press **Save** to save the setting. To exit without making changes press **Cancel**.

Screen Timeout Setting

The screen timeout setting controls how long the backlight will stay on with no user interaction before dimming. Setting the timeout to 0 will cause the backlight to never dim.

Select the **Screen Timeout** menu to access the setting. Use the keypad keys to set the backlight timeout (in seconds) and press **Save** to save the setting. To exit without making changes press **Cancel**.

Default Configuration

The default option resets the keypad to the factory default settings.

Press **Default** to default the keypad. You will be prompted to **Press [Enter] to default keypad**. To exit without defaulting the keypad press **Cancel**.

Keypad Information

The information screen displays configuration details about the keypad. Press **Info** to access the information screen. Press **Cancel** to exit.

Keypad Functions

Key	Function
0-9	The primary function of the numeric keys is to enter user codes. When controlling devices the **[1]** key turns the device on, the **[2]** turns the device off, and in the on state the **[3]** key latches the device.
🔒	The **[ARM]** key is used to start the arming process for an area.
🔓	The **[DISARM]** key is used to silence alarms, disarm the area, and cancel an arming sequence.
⧉	The **[MENU]** key is used to access the menu and can be followed by menu shortcut selection key(s) that represent a menu item. When the **[MENU]** key is held for 2 seconds, the keypad will recognize it as the **[FUNCTION]** key, which can be programmed to unlock a door.
⌂ Stay	The **[STAY]** key is used to initiate the stay arming process for an area.
⤓ Force	The **[FORCE]** key is used to force arm an area.
Memory	The **[MEMORY]** key will take a user directly to the memory view menu.
Bypass	The **[BYPASS]** key can be pressed when an area is breached during an arming process to bypass the displayed area.
X	The **[CLEAR]** key will log off the user currently logged in to the keypad. When pressed while not logged in the display will be refreshed.
↵	The **[ENTER]** key is used to confirm an action on the keypad, acknowledge memory and alarm information, and move to the next programming screen.
ARROW KEYS	The arrow keys are used to scroll the menu, move the focus of a program window to the next screen, and move the cursor when programming or editing values.

Orientation

LCD Touchscreen Keypad orientation is determined by its operating firmware. The keypad can operate in either portrait or landscape orientation and can be changed by loading the appropriate firmware version.

The required portrait or landscape version will need to be specified when downloading the keypad firmware or requesting firmware from ICT Technical Support.

Update Keypad Firmware

Protege GX

To update firmware on the LCD Touchscreen Keypad, Protege GX controllers must be running firmware version 2.08.1140 or higher.

1. Log in to the web interface of the Protege GX controller that the keypad is associated with.
2. Navigate to the **Application Software** menu.
3. In the Update Module Firmware section, select the required keypad from the **Module** dropdown.
4. Click **Upload Firmware** and browse to the firmware Bin File (.bin format) supplied by ICT.
5. Open the file to install the new firmware on the selected keypad.

When the update is complete the keypad will restart in the new orientation.

Protege WX

To update firmware on the LCD Touchscreen Keypad, Protege WX controllers must be running firmware version 4.00.607 or higher.

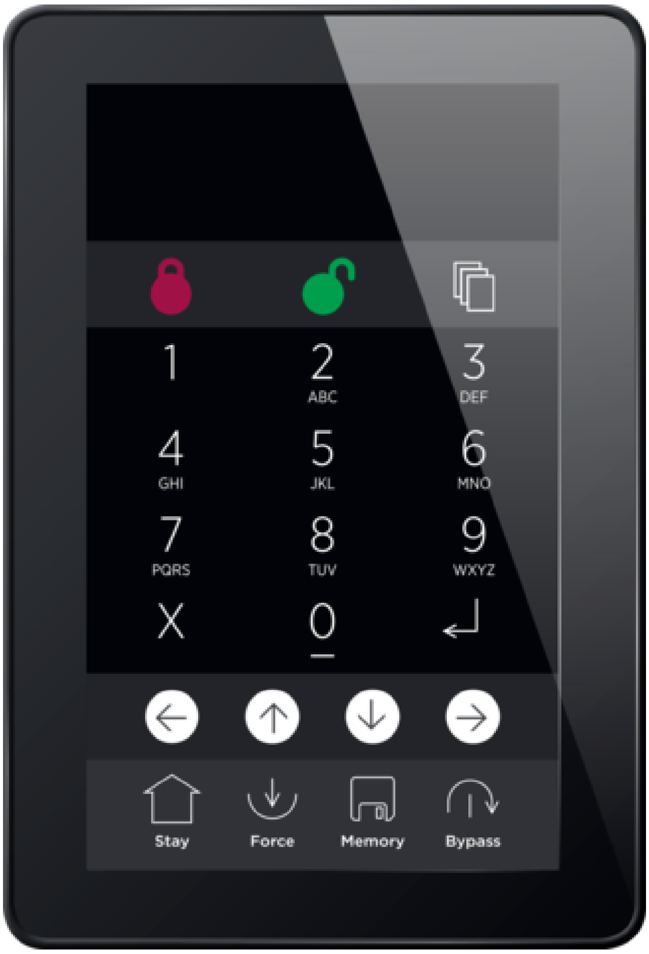
1. Log in to the Protege WX web interface.
2. Navigate to **System | Application Software**.
3. In the Update Module Firmware section, select the required keypad from the **Module** dropdown.
4. Click **Upload Firmware** and browse to the firmware Bin File (.bin format) supplied by ICT.
5. Open the file to install the new firmware on the selected keypad.

When the update is complete the keypad will restart in the new orientation.

Warning: Updating module firmware will put the entire network into maintenance mode, preventing normal activity for the duration of the update process. Module firmware **must not** be updated remotely.

Status Indicators

The keypad features two status indicators showing the condition of the Protege system.



Armed / Alarm Indicator

When the armed/alarm indicator is **flashing** the system is in alarm and you need to enter your user code to silence the alarm. When **on**, the system is armed.

This indicator is programmable and may not function as described here. Verify the operation with your installation company or security professional.

Disarmed Indicator

When the disarmed indicator is **on** the system is disarmed. Alternatively, when the disarmed indicator is **on** the system may be ready to arm (all inputs are secure). Enter your user code to arm.

This indicator is programmable and may not function as described here. Verify the operation with your installation company or security professional.

Confidentiality Mode

Keypads include a confidentiality mode where activation of the onboard output will cause all lights (Power, Disarm, Arm and LCD backlight) to turn off when the keypad is not in use. This feature is enabled by default. When the onboard output is not activated, these lights serve their normal functions.

Error Messages

When the keypad attempts to register or communicate with the system controller after powering up, errors can be generated indicating access to the Protege system has been denied or was unsuccessful. This is a normal part of the Protege system.

Keypad Version Error

The version of the keypad is incorrect for the system controller. This error cannot be corrected without updating the keypad firmware. The event log in the system controller will display the version of the keypad and the version that is required if this error has occurred.

Please contact your distributor for information on how to update the firmware.

Keypad Address Too High

The address of the keypad that is programmed is beyond the maximum number of keypads that are allowed to connect to the controller. Press the **[EXIT]** key to restart the keypad. Set the keypad address to a lower value.

Duplicate Keypad Address

The address of the keypad is already programmed into the system controller. Press the **[EXIT]** key to restart the keypad then set the keypad address to a free address.

Security Violation

The system controller has security enabled and devices cannot be added to the Protege system. Remove the security setting for the system controller then press the **[EXIT]** key to restart the keypad.

Invalid Serial Number

The keypad has an invalid serial number programmed and cannot be registered on the Protege system. Return the keypad to your distributor. This error cannot be corrected without updating the keypad firmware.

Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
PRT-TS50-STD-B	Protege LCD Touchscreen Keypad - Black
PRT-TS50-STD-W	Protege LCD Touchscreen Keypad - White
Power Supply	
Operating Voltage	11-14VDC
Operating Current	260mA (340mA Max)
User Interface	
User Interface Display	480 x 800 Color LCD display
User Input	5" capacitive touchscreen
Inputs	
Inputs	2 standard or 4 using Input Duplex mode
Outputs	
Outputs	1 open collector (50mA Max) output. Programmable for all output functions 2 system status indicators 1 system beeper
Dimensions	
Dimensions (L x W x H)	131 x 90 x 20mm (5.15 x 3.54 x 0.77")
Weight	192g (6.77oz)
Operating Conditions	
Operating Temperature	-10° to 55°C (14° to 131°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)

It is important that the unit is installed in a dry cool location that is not affected by humidity. Do not locate the unit in air conditioning or a boiler room that can exceed the temperature or humidity specifications.

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.ict.co) for the latest documentation and product information.

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

European Standards

CE Statement

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol),
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency magnetic field immunity tests (EN 61000-4-8)

EN50131

In order to comply with EN 50131-1 the following points should be noted:

- Ensure for Grade 3 or 4 compliant systems, the minimum PIN length is set for 6 digits.
- To comply with EN 50131-1 Engineer access must first be authorized by a user, therefore Installer codes will only be accepted when the system is unset. If additional restriction is required then Engineer access may be time limited to the first 30 seconds after the system is unset.
- Reporting delay –Violation off the entry path during the entry delay countdown will trigger a warning alarm. The warning alarm should not cause a main alarm signal and is not reported at this time. It can be signaled locally, visually and or by internal siren type. If the area is not disarmed within 30 seconds, the entry delay has expired or another instant input is violated, the main alarm will be triggered and reported.
- To comply with EN 50131-1 neither Internals Only on Part Set Input Alarm nor Internals Only on Part Set Tamper Alarm should be selected.
- To comply with EN 50131-1 Single Button Setting should not be selected.
- To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.

Anti Masking

To comply with EN 50131-1 Grade 3 or 4 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input.

I.e. Use 2 inputs per detector. One input for alarm/tamper and one input for masking.

To comply with EN 50131-1:

- Do not fit more than 10 unpowered detectors per input,
- Do not fit more than one non-latching powered detector per input,
- Do not mix unpowered detectors and non-latching powered detectors on an input.

To comply with EN 50131-1 the Entry Timer should not be programmed to more than 45 seconds.

To comply with EN 50131-1 the Bell Cut-Off Time should be programmed between 02 and 15 minutes.

EN 50131-1 requires that detector activation LEDs shall only be enabled during Walk Test. This is most conveniently achieved by using detectors with a Remote LED Disable input.

FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Subpart A

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

ICES-003

This is a Class A digital device that meets all requirements of the Canadian Interference Causing Equipment Regulations.

CAN ICES-3 (A)/NMB-3 (A)

Disclaimer and Warranty

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.

For warranty information, see our Standard Product Warranty.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.