PRT-ENTR-17

Protege Vandal Resistant Touchscreen Entry Station

Installation Manual

Last Published: 09-May-24 8:56 AM

Contents

Introduction

Tough, durable and extremely robust, the Protege Vandal Resistant Touchscreen Entry Station is the ideal solution for creating an outstanding user experience. The 17” touchscreen entry station is designed to be the first thing people notice as they approach the building, and their gateway for gaining access.

The entry station provides an intuitive interface for visitors to communicate with tenants, building management or a concierge, and connects guest to off-site locations such as corporate housing owners. VoIP and video capability enable users to view live video from multiple sources and utilize two-way voice communication to SIP compliant phones and intercoms, providing the ability to grant entry from virtually anywhere.

Features of the entry station include:

- Vandal resistant and waterproof (IP65 rated) enclosure.
- 17″ touchscreen display.
- Built-in high resolution camera with wide viewing angle.
- Speaker and microphone for full duplex audio communication.
- Fully SIP compliant to allow communication with other Protege intercoms and third-party SIP devices including external and mobile phones.
- 12V DC power supply input or PoE.
- One programmable open collector output.
- Onboard postal lock input.
- A surface mount model designed for mounting directly onto a wall or flat surface.
- A flush mount model designed for mounting into a wall cavity so the front plate is flush with the wall surface.
- Optional flush mount rough-in box allows a cavity to be built in place for the entry station during construction.
- Protege GX and Protege WX integration for directory list population and extension listings.
- Interact with Protege integrated system controllers to allow control of doors and programmed outputs.
- A customizable graphics page displays a background image such as a floor plan or company branding.

Supported Protocols

The entry station supports the following protocols:

- SIP
- DHCP Client
- RTP
- Audio Encodings:
  - PCMU (G.711 mu-law)
  - PCMA (G.711 A-law)

SIP Servers

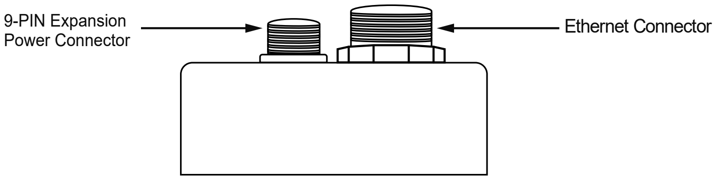
The entry station supports SIP servers that comply with SIP protocol standards including Asterisk and 3CX.

Connections

Connection Terminals

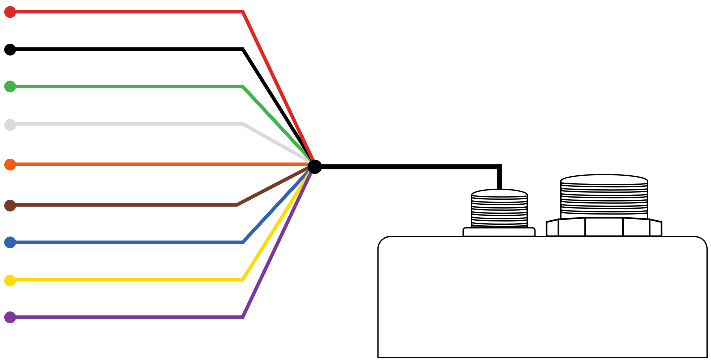
The entry station has two connection terminals.

- The ethernet connector provides network connectivity.
- The 9-Pin expansion connector provides a 12V DC power connection, postal lock input, and a programmable output connection.



Installation Wiring

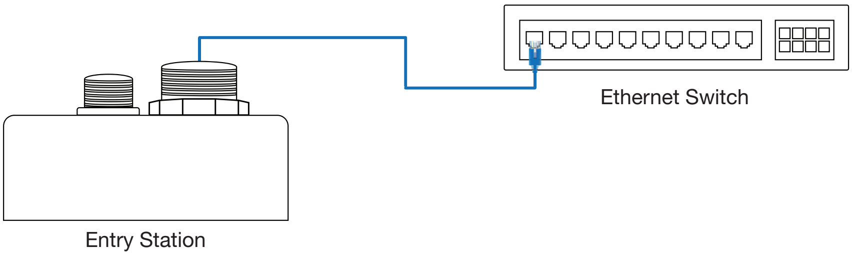
The entry station is supplied with a 9-Pin expansion cable.



Color	Wire	Function
🔴	Red	+12VDC
⚫	Black	0V GND
🟢	Green	Wiegand D0
⚪	White	Wiegand D1
🟠	Orange	Input 1 (Postal Lock)
🟤	Brown	Reserved
🔵	Blue	Output 1
🟡	Yellow	Reserved
🟣	Violet	Reserved

Ethernet Connection

Ethernet connection allows installations to either use a dedicated Protege network (recommended for installations with multiple entry stations), or simply connect the entry station to the building's existing network.



Ethernet Wiring: CAT5e / CAT6. Maximum length 100m (330 ft).

Power Requirements

Specific power requirements must be met for the entry station to function correctly. If these are not met there is a risk of damaging the unit or encountering performance issues.

Power requirements are listed in the Technical Specifications (see page 52).

The entry station requires a **minimum** supply of 10V to operate correctly. Voltage drop between the power supply and the entry station may cause the entry station to receive insufficient voltage. If this occurs the display may be faint or flickering and the unit may reboot unexpectedly.

When designing the supply of power to the entry station, ensure that you account for the following factors which may contribute to voltage drop:

- The run length (length of cable from power supply to entry station) - ensure that the entry station is as close to the splitter or source as possible
- The composition of the wire
- The CSA (cross-sectional area) / AWG of the cable
- The temperature of the cable and how mechanical protection applied to the cable relates to the temperature

After installation, we recommend that you measure the input voltage at the entry station to ensure that it is sufficient for correct operation.

Cable Length and Gauge

The length and gauge of the cable connecting the entry station to the power supply will affect the voltage being supplied to the entry station. By identifying the allowable voltage drop (the power supply voltage minus the 10V minimum operating requirement) and dividing this by the voltage drop per meter (the wire resistance multiplied by the entry station's maximum operating current) you can calculate the maximum cable length that can be used.

The following formula can be used as a guide to calculate the maximum cable length.

- Cable length = 0.5 * (V_{PSU} - 10.0/0.132)/(R_{Wire} * 4.0)
  where R_{Wire} = wire resistance per meter

Using the 20AWG example in the table below, this would be calculated as 0.5 * (13.8 - 10.0)/(0.033 * 4.0) = 14.4m

Note: This assumes that no other devices are drawing current from the power supply. Any additional devices will reduce the power supply's capacity and affect the maximum cable length.

Common Examples

The table below demonstrates maximum cable length calculations for 20AWG and 24AWG cable, assuming a power supply of 13.8V.

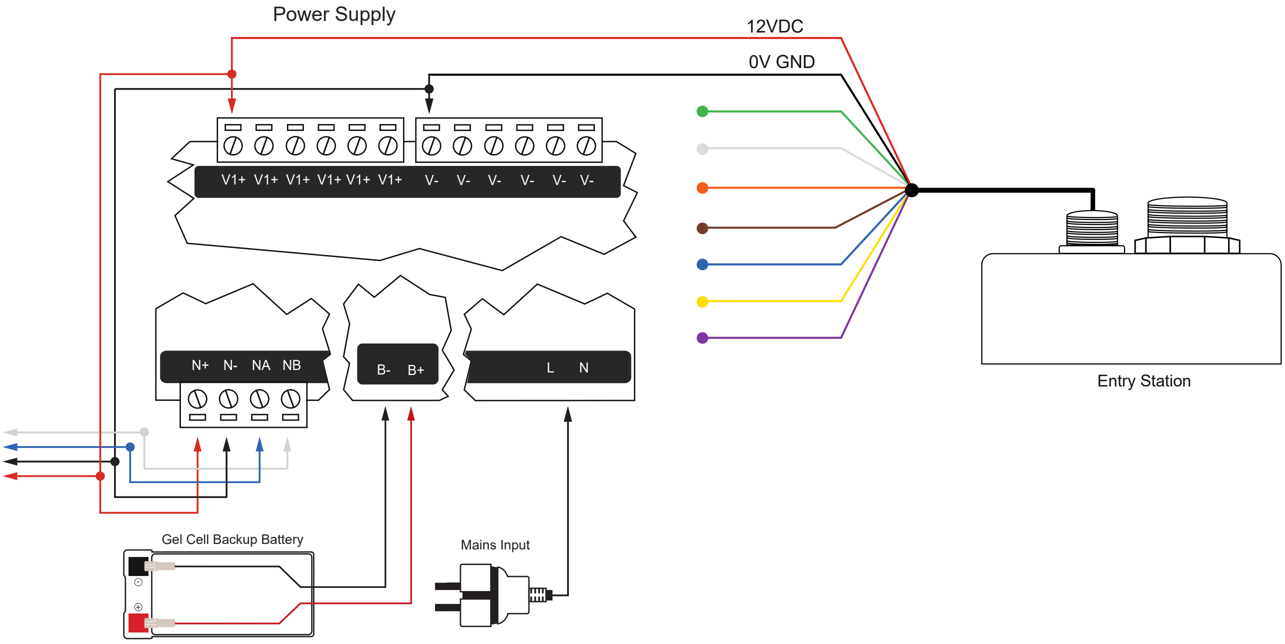
	20AWG	24AWG
V_{PSU}	13.8V	13.8V
Minimum operating voltage	10.0V	10.0V
Maximum allowable voltage drop	3.8V	3.8V
R_{Wire} (wire resistance per meter)	0.033	0.084
Operating current	4.0A	4.0A
Total length of wire (two wires - positive and negative)	28.8m	11.3m
Maximum cable length	**14.4m**	**5.65m**

This is intended as a guide only. After installation, we recommend that you measure the input voltage at the entry station to ensure that it meets the 10V minimum required for correct operation.

12V DC 4A Power Supply

Power is supplied to the entry station via a 12V DC power supply capable of supplying a minimum of 4A.

A Protege power supply module is recommended for this purpose, although any clean 12VDC 4A power supply is suitable. When using a Protege power supply, connect V+ to the red wire and V- to the black wire of the 9-PIN expansion cable, as illustrated below.



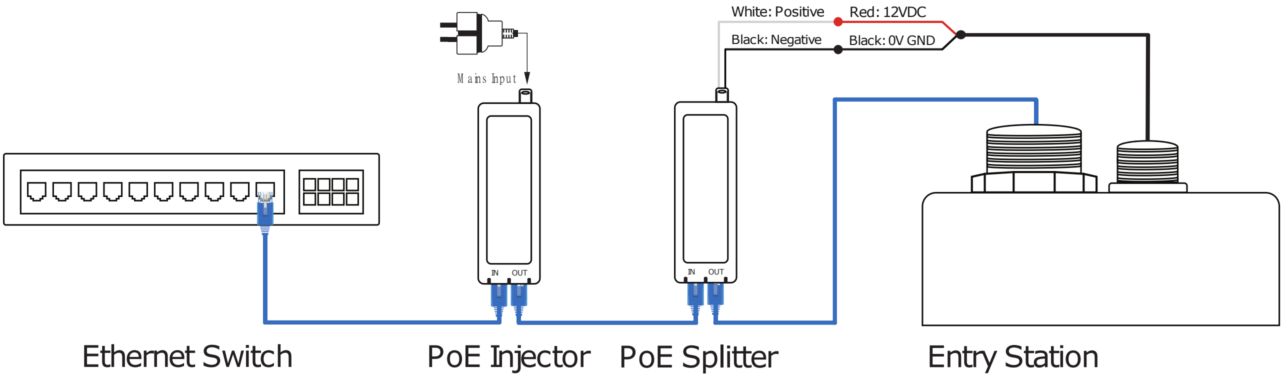
After installation, measure the input voltage at the entry station to ensure that it has a minimum supply of 10V.

If using a Protege power supply module, a battery backup must be connected to the module network to provide a monitored supply. The battery plays an important role in power conditioning and provides a continuous source of power in the event of a power outage.

Power over Ethernet (PoE)

The PoE injector supplies a higher voltage (56V) and transmits PoE to the splitter which regulates the voltage down to 12V for supply to the entry station.

This must **ONLY** be installed with the supplied PoE injector (POE61W-560DG) and PoE splitter (POE45-120-R).



Ethernet Connection

- Connect the **Ethernet Switch** to the **IN** port of the **PoE injector**.
- Connect the **OUT** port of the **PoE injector** to the **IN** port of the **PoE splitter**.
- Connect the **OUT** port of the **PoE splitter** to the RJ45 Ethernet connector on the back of the **entry station**.

Total ethernet wiring length must be a maximum of 100m (330 ft). This includes all connections from the ethernet switch to the injector, from the injector to the splitter, and from the splitter to the entry station.

9-PIN Expansion Power Connection

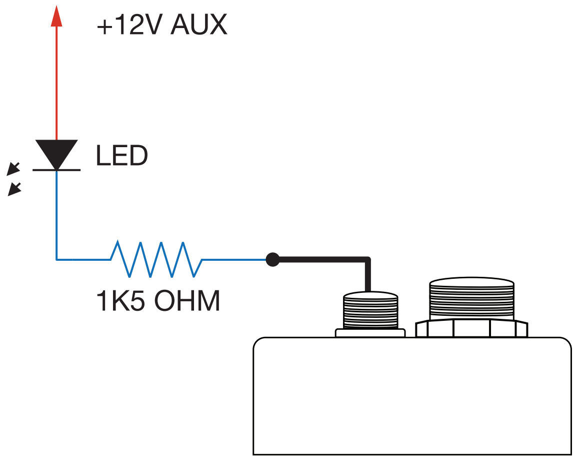
- Connect the **white** (positive) wire from the PoE splitter to the **red** (12V DC) wire of the expansion cable.
- Connect the **black** (negative) wire from the PoE splitter to the **black** (0V GND) wire of the expansion cable.
- Connect the expansion cable to the 9-Pin expansion connector on the back of the **entry station**.

Do not insert any additional wiring between the PoE splitter wires and the entry station expansion cable wires.

After installation, measure the input voltage at the entry station to ensure that it has a minimum supply of 10V.

Output Connection

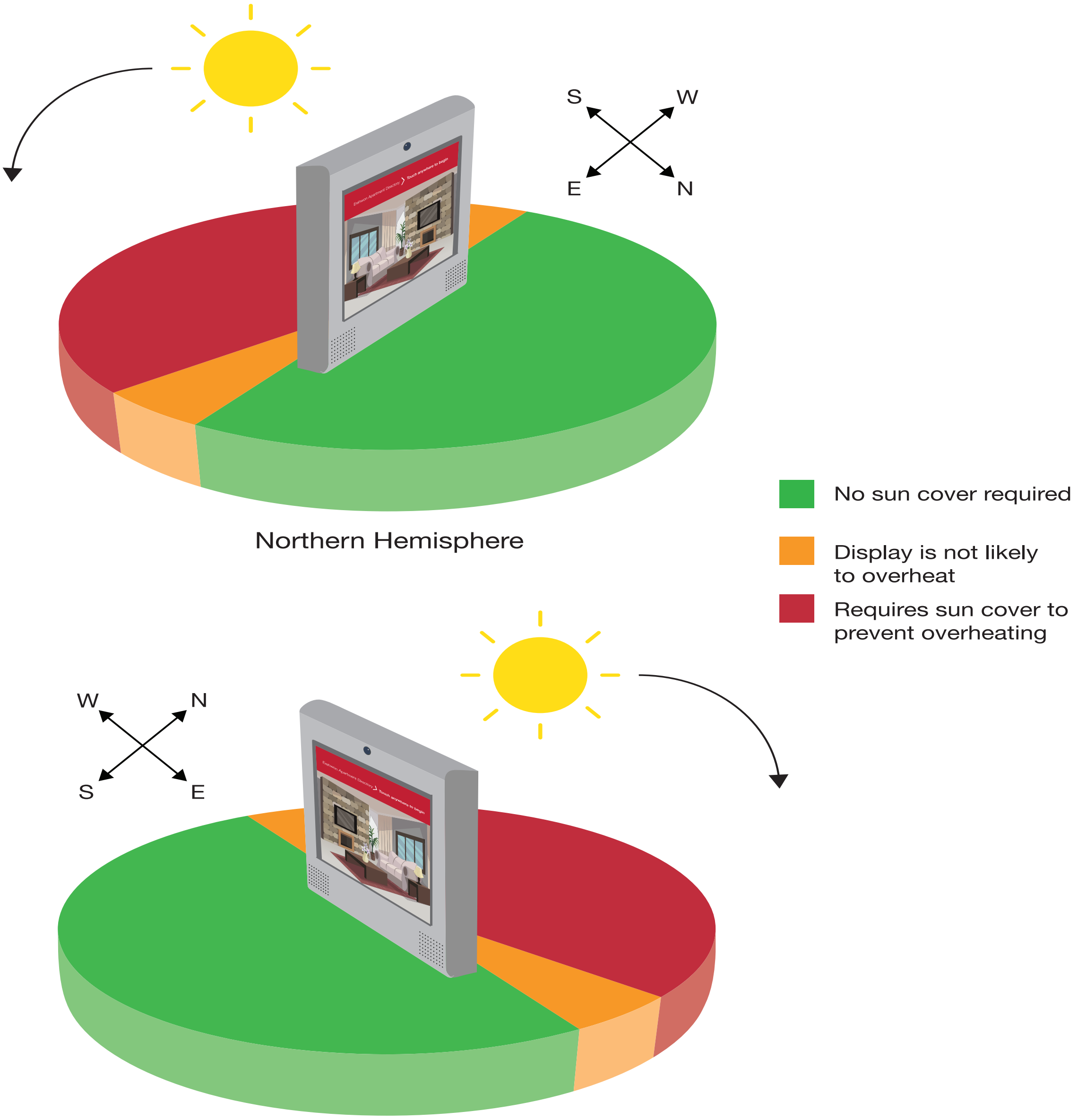
The entry station has one onboard programmable open collector output suitable for digital relay control. It should be connected as indicated in the diagram below:



Mounting and Installation

Before mounting, ensure that the screen of the entry station is in a position where it is not exposed to direct sunlight. Correct positioning is essential to prevent the display from overheating. If it is not possible to install the entry station facing the required direction, a sun cover must be used to reduce potential operating issues.

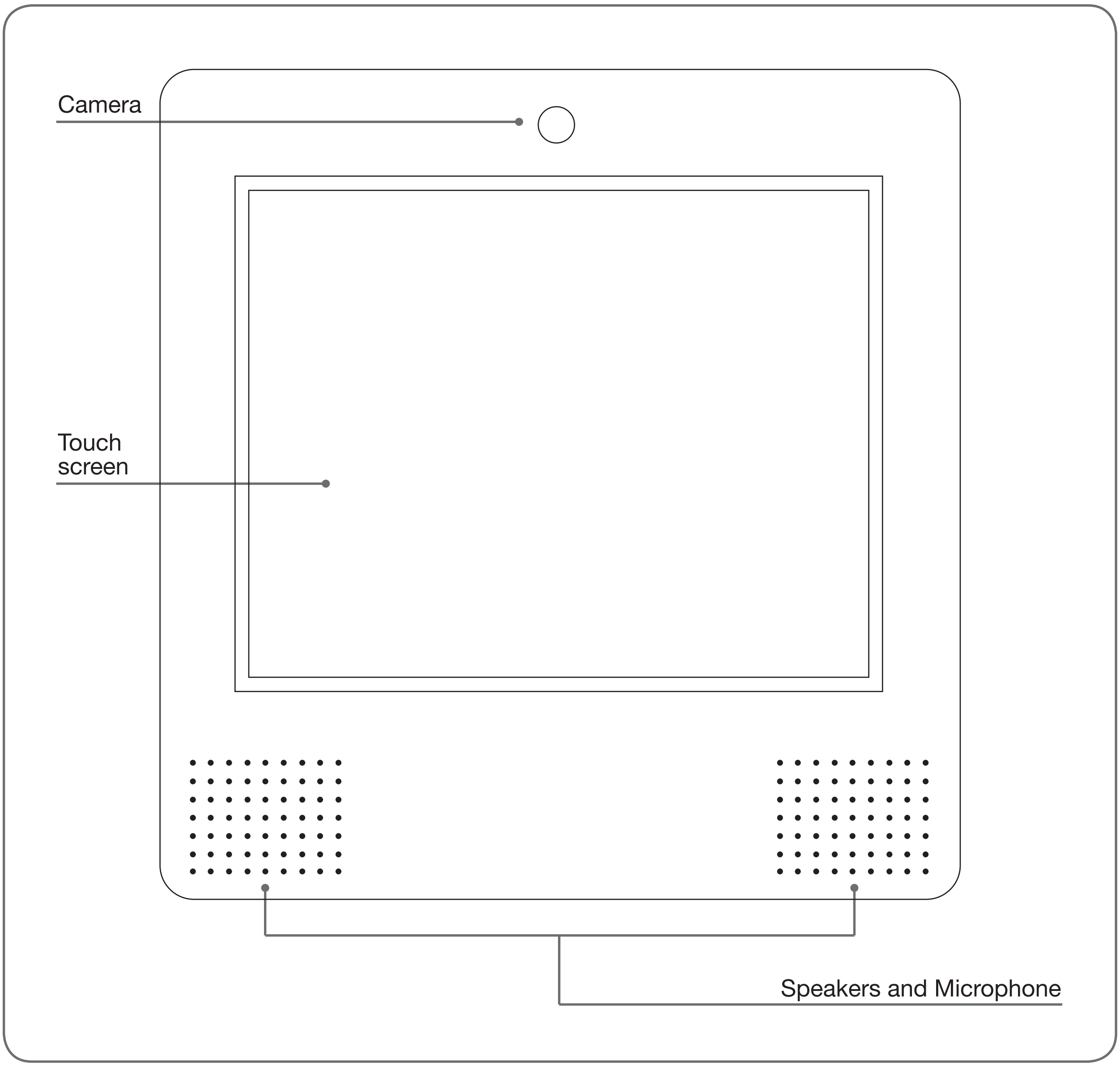
The below diagrams illustrate the ideal orientations for both the northern and southern hemispheres, and identify the mounting positions that will require a sun cover.


S
W
E
N
🟩 No sun cover required
🟧 Display is not likely to overheat
🟥 Requires sun cover to prevent overheating
W
N
S
E

Northern Hemisphere

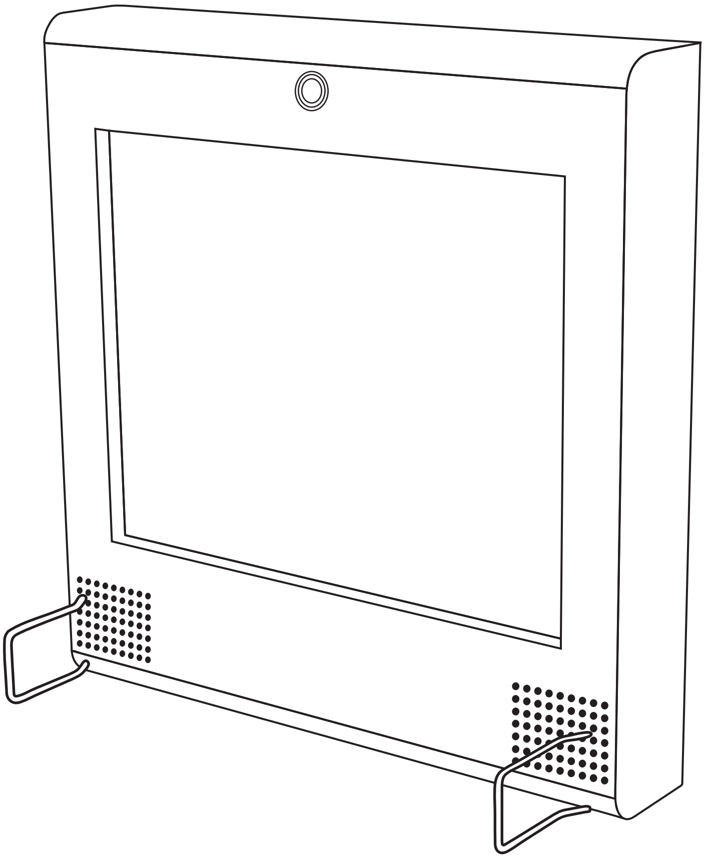
Southern Hemisphere

Mechanical Diagram



Face Plate Removal

You must first remove the front face plate from the entry station to access the back plate for mounting.

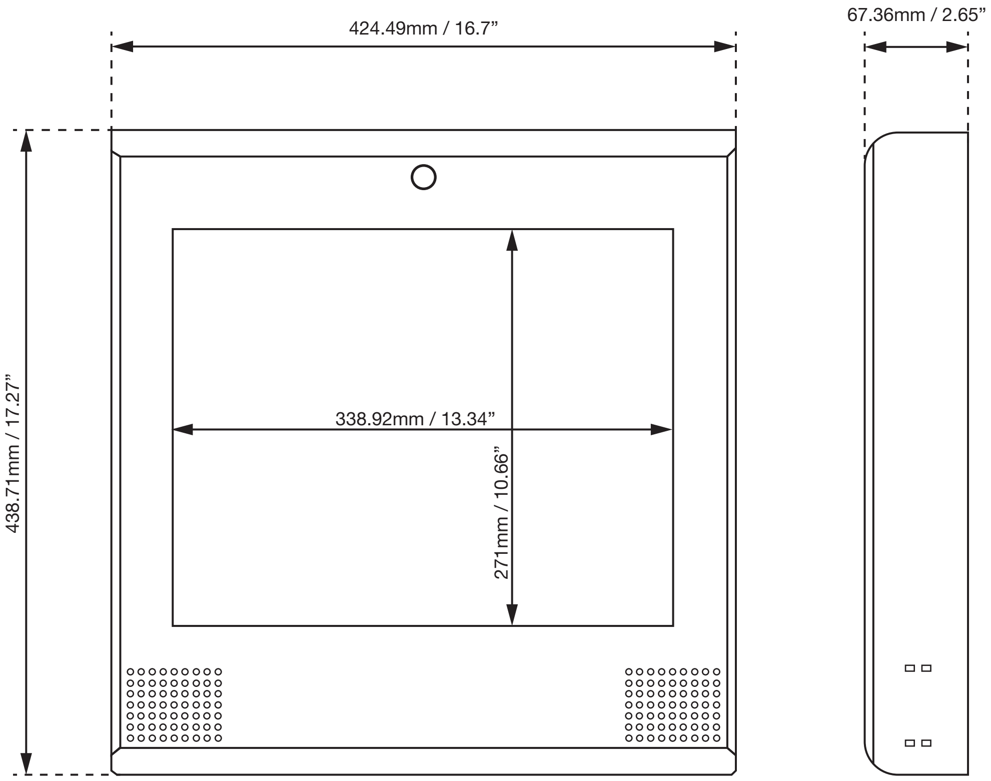


To remove the front face plate, carefully insert both of the provided tools through the outer speaker holes and push them all the way in to release the front section, then lift the cover out from the bottom.

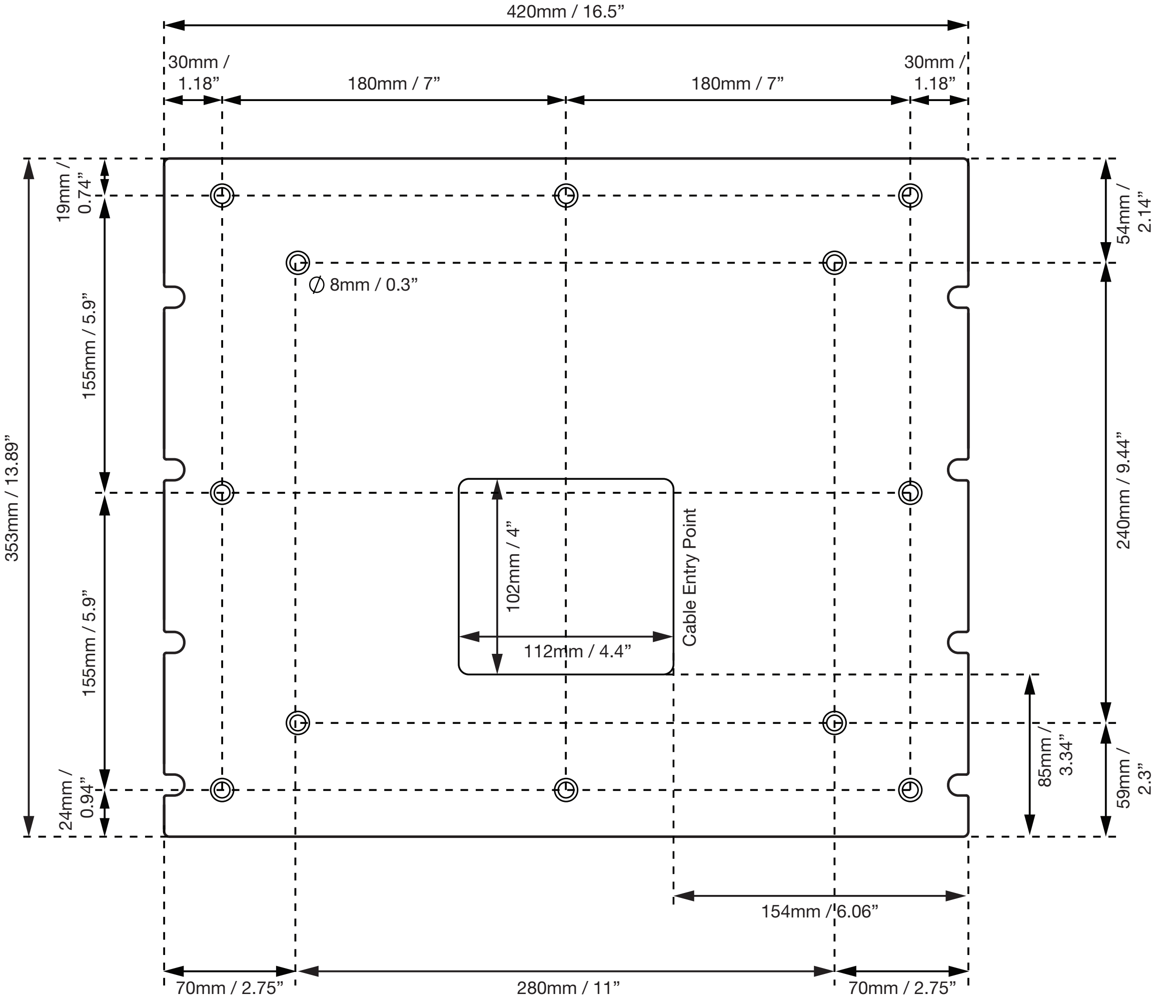
Surface Mounting

The below diagrams indicate the dimensions of the surface mount enclosure and back plate, for use when mounting the entry station directly onto a wall or flat surface.

Surface Mount Enclosure



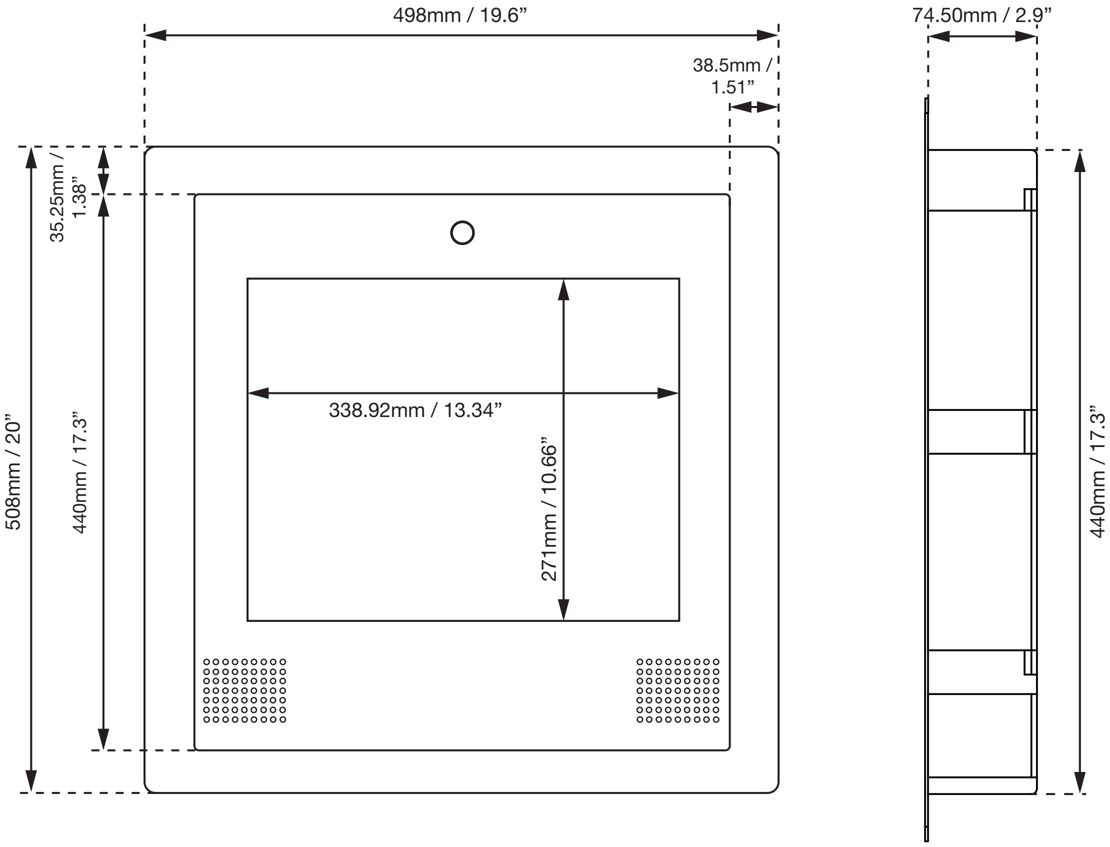
Surface Mount Back Plate



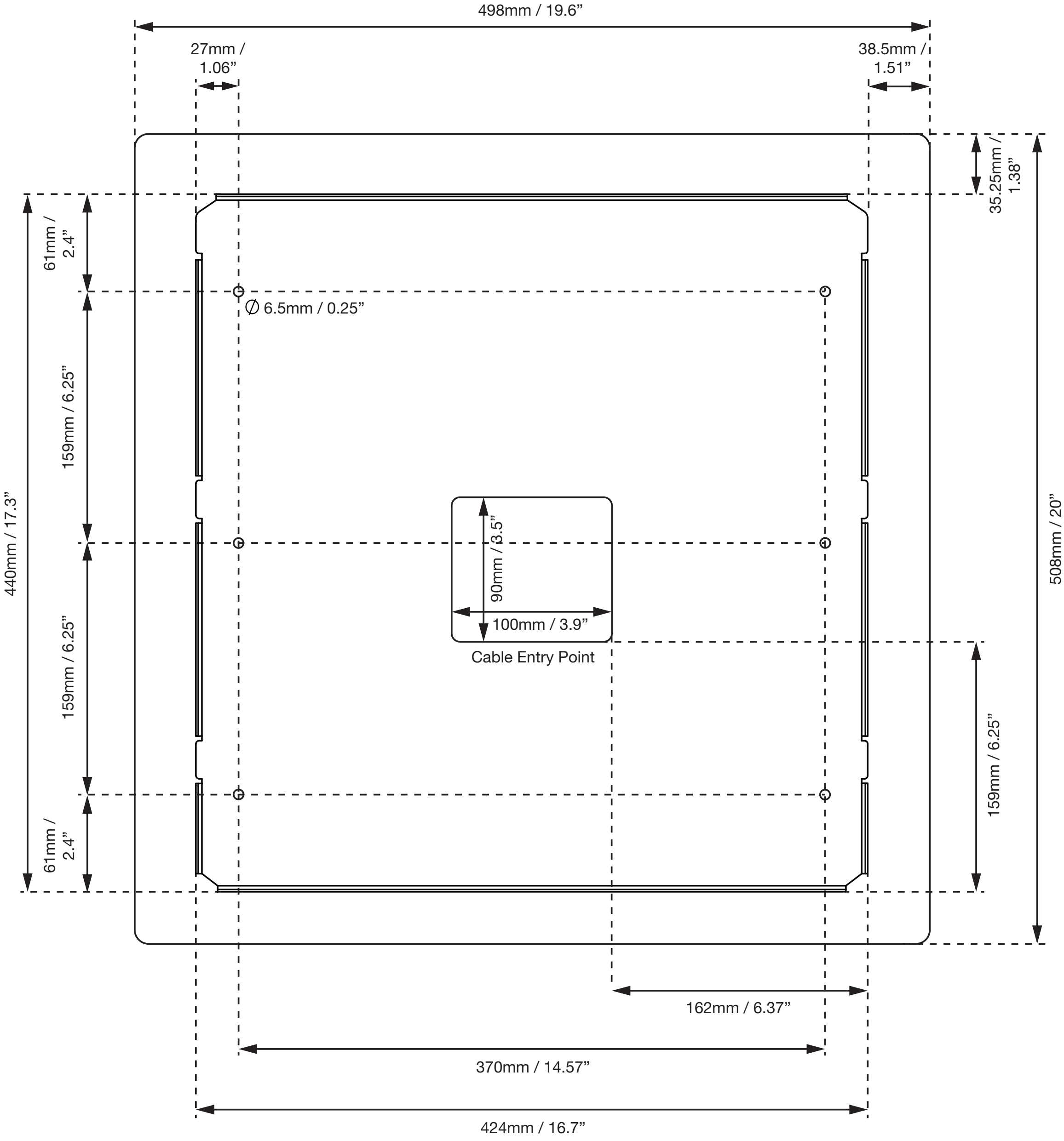
Flush Mounting

The below diagrams indicate the dimensions of the flush mount enclosure and back box, for use when mounting the entry station into a wall cavity so that the front plate is flush with the wall.

Flush Mount Enclosure

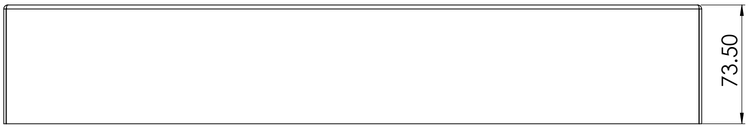


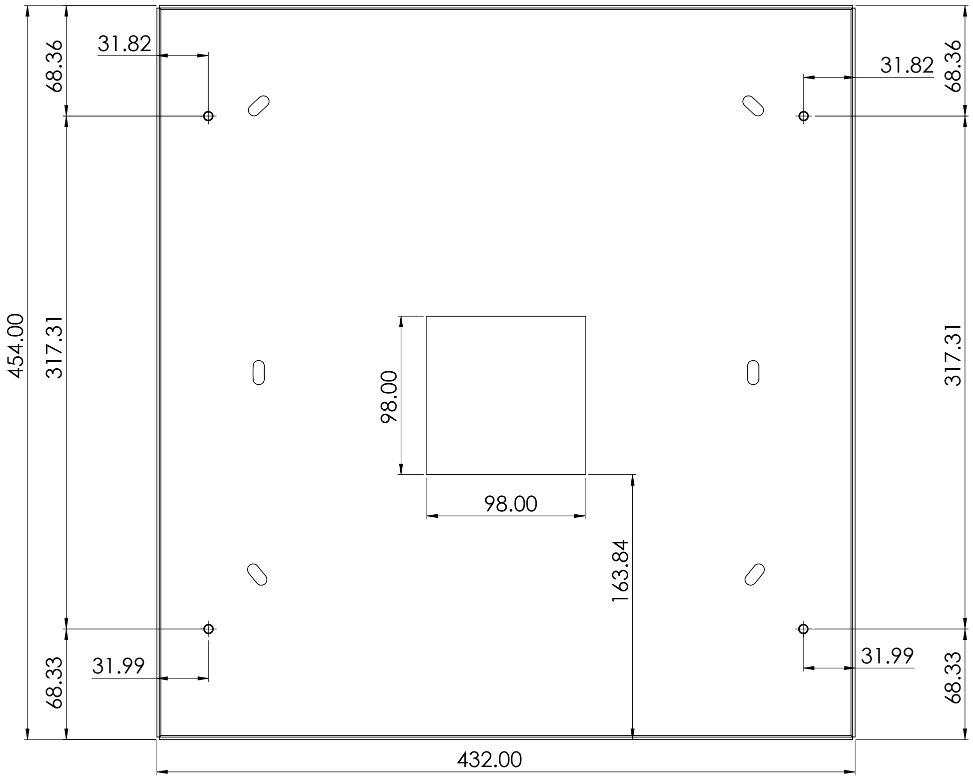
Flush Mount Back Box



Flush Mount Rough-In Box

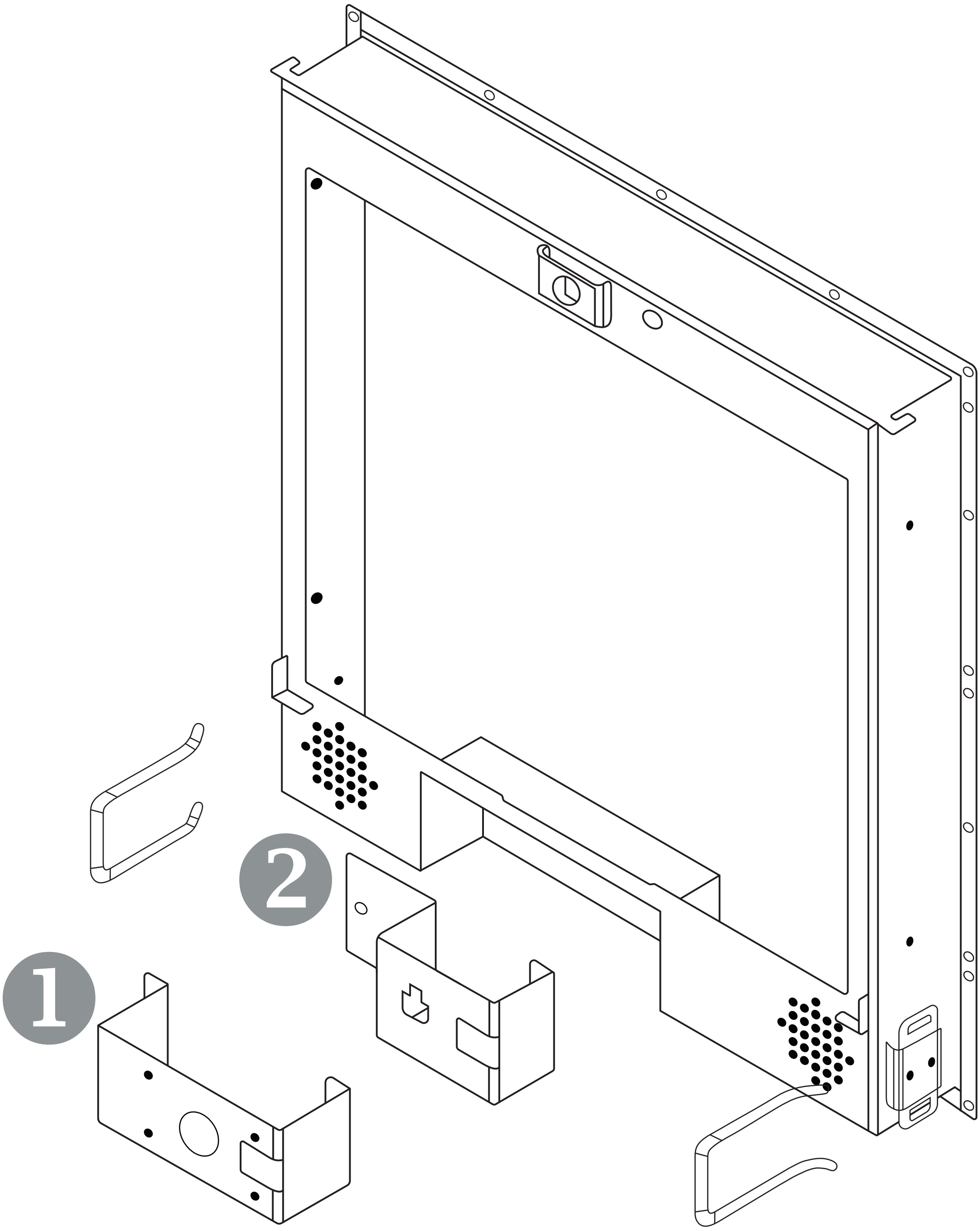
The below diagrams indicate the dimensions of the optional flush mount rough-in box, available for use when building a cavity in place for the entry station during construction.





Postal Lock Installation

The supplied postal lock brackets enable you to fit compatible postal locks, as indicated by the diagram below.



1. USPS Master Locks
2. USPS Mailbox Locks

Postal Lock Connection

1. A postal lock and contact switch must be obtained from a suitable supplier, as these are not supplied.

   The supplied postal lock brackets are compatible with standard USPS Master locks and USPS Mailbox locks only. Postal lock connection is possible using the supplied postal lock brackets only.

2. The locking mechanism needs to be mounted onto the appropriate mounting bracket.
3. The bracket is then mounted on the posts in the bottom of the entry station, in the postal lock cavity.
4. A hole must be drilled in the front panel of the entry station to accommodate the lock. A pilot hole is marked in the center of the front panel to help align the hole correctly with the mounted bracket and lock position.

   Drilling stainless steel is a specialized process and it is recommended to have this done by a professional.

5. The postal lock engages the contact switch. The contacts of the switch must be connected to the **orange** Input 1 (postal lock input) and **black** (ground) wires on the 9-PIN expansion cable.

   Refer to the Connections section (see page 8) for further details on wiring connections.

Hardware Configuration

Power On Sequence

The entry station takes approximately 60 seconds to boot after power has been supplied. Once booted, the screen displays the customizable graphics page.

Defaulting the Entry Station

The entry station can be set back to its factory default settings using the following procedure:

1. Reboot the entry station by removing and reapplying power.
2. During the startup sequence, wait for the screen to go completely black, after the world logo disappears.
3. Repeatedly tap the bottom quarter of the touchscreen until it displays Default Settings.
4. Wait for the entry station to timeout. It will reset to the default configuration.

Defaulting the entry station does not reset the IP address. For instructions on how to reset the address, refer to Temporarily Defaulting the IP Address below.

Temporarily Defaulting the IP Address

The entry station IP address can be temporarily set to 192.168.111.222. If the currently configured IP address is unknown, this allows you to connect to the web interface to view and/or change it.

The temporary IP address is used until the entry station is power cycled. After power cycling, the programmed IP address is used.

Temporarily default the IP address using the following procedure:

1. Reboot the entry station by removing and reapplying power.
2. During the startup sequence, wait for the screen to go completely black, after the world logo disappears.
3. Repeatedly tap the bottom quarter of the touchscreen until it displays Temporary IP (192.168.111.222).
4. Wait for the entry station to complete the boot sequence. When it starts it will use the following settings:
   - **IP Address**: 192.168.111.222
   - **Gateway**: 192.168.111.254
   - **Net Mask**: 255.255.255.0
   - **DHCP**: Disabled
5. Connect to the web interface by entering 192.168.111.222 into the address bar of your web browser, and view or change the IP address as required.

Temporarily defaulting the IP Address does not remove any programming. For instructions on how to reset the entry station's programming, refer to Defaulting the Entry Station above.

Programming the Entry Station

This section describes the available settings, functions and features of the entry station and how to configure them through the web interface.

Entry Station Web Interface

The web interface provides access to the functions required for configuration and deployment of the entry station, either for integration with a Protege system or for standalone operation.

Accessing the Web Interface

1. Open a web browser and enter the default IP address of the entry station: 192.168.1.34
2. Enter the default operator login of admin with the password admin.

   > For security reasons, this password should be changed before deployment (see page 28).

3. Click **Login**. The Home Page is displayed.

Initial Setup of the Entry Station

To prepare the entry station for standard operation some basic settings must be configured via the web interface.

- Add the entry station's unique SIP account (see below)
- Configure the call settings (see next page)
- Configure the network connection (see page 26)
- Change the admin password (see page 28)

Add the SIP Account

> SIP hacks are quite common, cause a considerable amount of disruption when they occur, and require a lot of time and effort to identify. If the entry station will be connecting to the SIP server over the internet, you should ensure that the network is configured to only permit SIP messages from the legitimate SIP server to the entry station(s) (i.e. whitelisting the SIP server and blocking anything else on the port used for communications with the SIP server), to prevent attacks from malicious SIP servers. Specific configuration is beyond the scope of this document and should be performed by the network administrator.

The SIP account will need to be configured to enable phone calls, using the information from your SIP provider.

1. Navigate to **Device Settings**.
2. Select the **SIP Server** tab and enter the required account and configuration settings.
   - The **SIP Server IP Address** is the IP address of the SIP service connection.
   - The **Account** is the SIP account login ID that has been allocated by the SIP system.

     > Where a site has multiple entry stations, each must have its own unique SIP account and login ID.

   - The **Password** is the SIP registration password for the SIP account.
   - When enabled, the **Auto Answer** function forces the intercom to automatically answer any calls it receives.
   - The **Realm** is the security domain where this account is valid. Entering * will allow your authentication password to be sent to the server without the realm being verified.
   - Enter the Authentication **Scheme** used by the SIP server. The default is digest.
   - Enter the **Port** used for communications with the SIP server.

- The **RTP Timeout** defines (in seconds) how long the entry station will wait before ending a call if it does not detect any incoming audio.
- When **Hangup on DTMF** is enabled, the entry station automatically hangs up when * is pressed during a call.

3. Click **Save**.

The SIP settings can take some time to authenticate, and the entry station web interface will be unresponsive until this has finished. The process is complete when the **Save** button is once again visible.

Home Page

The **Home Page** displays the entry station serial number, firmware version and status information.

To load the latest firmware, click **Update Firmware** and select the firmware image file in the file selection.

Call Settings

The **Call Settings** menu allows you to configure the call, volume and sound options.

1. Navigate to **Call Settings | General**.
2. The **Call Timeout** setting defines how long a call will ring before timing out. The timeout can be set from 10-30 seconds.
3. The **Max Call Duration** can be set from 1-60 minutes. Once this time has elapsed, the intercom hangs up the call. Enable the **Unlimited** option to allow an unlimited call connection time.
4. Click **Save**.

Volume Settings

1. Select the **Volume** tab.
2. The **Call Volume** defines the volume level used when a call connects. Set a volume level from 1-5.
3. The **Microphone Volume** defines the sound level transmitted through the microphone during a call. Set a volume level from 1-5 or enable the **Mute Microphone** option to prevent any sound being transmitted.
4. The **Ringer Volume** defines how loud the entry station rings when it is called. Set a volume level from 1-5.
5. Click **Save**.

Sounds

1. Select the **Sounds** tab. This tab allows you to upload customized audio files to play for:
   - Incoming Call
   - Call in Progress
   - Call Connected
   - Call Disconnected
   - Lock Switch Activation

   Sound files must be in MP3 format.
2. To upload a new sound, click **Change**.
3. Click **Choose File** to browse to and select the audio file.
4. Click **OK**.

Device Settings

From the **Device Settings** menu, you can configure the entry station's network settings.

Network Configuration

The **General** tab allows you to edit the IP address and other connection settings of the entry station.

Programming the IP address, subnet mask, and default gateway requires knowledge of the network and subnet that the system is connected to. You should always consult the network or system administrator before programming these values.

1. Navigate to the **Device Settings** menu and select the **General** tab.
2. If you require the entry station to request its network configuration settings from a local DHCP server, select the **DHCP client enabled** option. The remaining network settings will then become unavailable.
3. Enter the **IP Address** of the entry station. The default is 192.168.1.34
4. Leave the DNS IP field blank. This is reserved for future use.
5. Enter the **Network Mask** used by the entry station. The network mask is used in conjunction with the above IP addresses. A network mask must be configured to allow access to the appropriate node on the subnet. By default this is set to a value of 255.255.255.0
6. Enter the **Default Gateway** used by the entry station. Use the gateway to allow access to a router for external communications beyond the subnet where the entry station is located. By default this is set to a value of 192.168.1.1.

   Changes to the default gateway field will require you to power cycle your entry station.

   The **Controller** settings below are only required when integrating the entry station with a Protege GX or Protege WX system. These options do not apply when the entry station is used in standalone mode. Refer to the relevant integration section for Protege GX (see page 32) or Protege WX (see page 46) for full programming details.

7. The **Con IP Address** is the IP address of the controller that the entry station communicates with.
8. The **Mod TX Port** is the port that the entry station communicates with the controller.
9. The **Address** is the keypad address assigned to the entry station for door control.

   The **Wiegand Output Configuration** settings below are only relevant when using the Wiegand output.

10. For the **Wiegand Keypad Format**, select which Wiegand format the entry station should use when PIN codes are entered via phone calls or the onscreen keypad.
11. For the **Site Code** option, set which site code to use for Wiegand keypad formats that require a fixed site code (26 Bit, 36 Bit IEI)

    The **External Network** setting below is only relevant when using the entry station with the Protege Mobile App.

12. The **External JPEG Video Port** is used to configure which external port the Protege Mobile App uses to reach the entry stations camera feed.
    - If the entry station is directly accessible via the internet, this should be set to 8080.
    - If the entry station has been port forwarded through a NAT, this should be set to the port number where http://{ENTRIPADDRESS}:8080/video is internet accessible.
13. Click **Save**.
14. If you have changed the **Default Gateway**, power cycle the entry station to implement the new setting.

Display Settings

From the **Display Settings** tab you can customize how the entry station home page and directory are displayed.

1. By default, tenants can log in to the entry station with a PIN or lock code using the **Login** button on the home screen. To remove this button for higher security, disable the **Login Keypad** option.
2. To change the **Background Image**, click **Change** and click **Choose File** to browse to the image, then click **OK**. To use the default background image, click **Reset to Default**.

   The image must be a JPEG (sRGB color space) file. The optimal resolution is 1280x1024.
3. The **Name Display Format** setting determines the way the names are displayed when users browse through entry station's directory. Click the dropdown and select from:
   - First Name Last Name
   - Last Name First Name
   - First Initial Last Name
   - Last Name First Initial
4. To configure how long the screen display remains on after being touched, use the slider to set the **Sleep Timeout** (in seconds). If the **Unlimited** option is enabled, the screen will always remain on.
5. Click **Save.**

Directory Sync

The Directory Sync settings allow automated synchronization of entry station directory records. These settings are not needed for standalone functionality.

Note: Only one of tenancy portal integration or SOAP directory integration may be used.

Tenancy Portal Directory Integration

Tenancy portal integration synchronizes a Protege Tenancy Portal phonebook with the entry station's directory. When a tenancy portal phonebook is designated for directory integration, the entry station will automatically sync the phonebook with its directory every 60 minutes. The entry station replaces the existing directory with the new phonebook sync, so no manual deleting, importing or maintenance of the entry station directory is required.

- The **Phonebook ID** is the tenancy portal ID of the phonebook you want to sync.

  When a Phonebook ID is entered, any SOAP Directory Integration (see below) is disabled.

When a Phonebook ID is saved in the entry station configuration the existing directory is immediately deleted.

To obtain the ID of the tenancy portal phonebook to sync:

1. Log in to the tenancy portal at https://wirelesscredentials.com/Tenancies.
2. Browse to the phonebook you wish to sync.
3. The phonebook ID is displayed in a read-only field. Click **Copy to Clipboard**.
4. In the entry station web interface, paste the ID into the **Phonebook ID** field, then **Save** the new settings.
5. Within 30 seconds the phonebook details with be synched to the entry station directory. The entry station will re-sync the phonebook every 60 minutes.

For information on tenancy portal integration, see the Protege Tenancy Portal User Guide, available from the ICT website.

SOAP Directory Integration

SOAP directory integration synchronizes Protege GX or Protege WX user records with the entry station's directory. The SOAP settings are required only when integrating with Protege GX or Protege WX. Refer to the relevant integration section for full programming details.

- The **SOAP Server Address** is the IP address configuration used for connection to Protege GX / Protege WX.

  > The remaining settings are required only when integrating the entry station with Protege GX. Only configuration of the **SOAP Server Address** is required for Protege WX integration.

- The **SOAP Server Port** is the communication port of the Protege GX SOAP service.
- The **Site ID** is the database ID assigned to the Protege GX site.
- The **Username** is the operator used to log in to the Protege GX SOAP service.
- The **Password** is the password used to log in to the Protege GX SOAP service.

Time and Date

If the entry station loses power, you must reset the time and date.

1. Select the **Time and Date** tab.
2. To manually set the time and date:
   - Click to select the current **Date** for the entry station.
   - Enter the current **Time** for the entry station.
   - From the dropdown list, select the **Time Zone** where the entry station is operating.
   - Click **Save**.
3. To automatically set the time and date:
   - Click **Apply PC Time and Date Now** to set the current time and date using your PC time and date.

   > This option should only be used when your PC is operating in the same time zone as the entry station.

Operators

Operators are accounts used to log in to the entry station's web interface.

Changing the Admin Password

For security reasons, it is important that you change the default admin password before the entry station is deployed.

1. Navigate to the **Operators** menu and select the **Administrator** operator.
2. Click **Change Password**.
3. Enter and confirm your new password, then press **OK**.
4. Click **Save**.

Creating New Operators

The Operators menu also enables you to create additional operators.

1. From the **Operators** menu, click **Add**.
2. Enter a **Name** for the operator. This is for identification only.
3. Enter the **Username** of the operator. This is the name used when logging in to the web interface.
4. Enter the **Password** for the operator. This is the password used when logging in.
5. Select the **Default Language** that the operator will use in the web interface.

6. Enable or disable the **Operator Timeout**. When enabled, the operator will be automatically logged out after the time specified below.
7. If the timeout option is enabled, set a value for the **Operator Timeout** (in minutes).
8. Click **Save**.

Standalone Functionality

Integration with Protege GX or Protege WX overrides any standalone programming.

Directory

In standalone mode, VoIP users can be created and edited in the directory via the web interface to allow visitors to search for a unit number or call an extension from the entry station.

- **First Name**: The first name of the user displayed in the onscreen directory.
- **Last Name**: The last name of the user displayed in the onscreen directory.
- **Unit Number**: The user's apartment number displayed in the onscreen directory.
- **Extension 1**: The SIP extension number or direct IP of the call receiving device.
- **Email**: If you are calling a device using the Protege Mobile App, set this to the email address of the user's app account.

If the entry station directory has been integrated with Protege GX or Protege WX, the **Directory** page displays a non-editable list of the users included in the directory. Refer to the relevant Directory Integration section for instructions on configuring the directory within Protege GX (see page 34) or Protege WX (see page 47).

Directory CSV Import / Export

The CSV Import feature transfers user data from an external source to the entry station's web interface, automatically mapping the user information to the corresponding fields.

Prerequisites

- The CSV file must be in the following format: `FirstName,LastName,Room,URI,Email`
- The file must contain a header row to define which columns relate to each of the fields.

To Import Users From a CSV File:

1. From the **Directory** page, click **Import**.
2. Click **Choose File** and browse to and select the CSV file you wish to import the users from, then click **OK**.

To Export Users from the Directory:

1. From the **Directory** page, click **Export**.
2. A CSV file is automatically downloaded and opened.

Output Control

In the web interface, the **Lock** menu is used to configure the behavior of the entry station's onboard output when the entry station is offline (operating in standalone mode).

Configuring Output Operation

1. Navigate to the **Lock** menu.
2. If you are controlling a lock from the entry station, enable the **DTMF Lock Enabled** option.
3. The **Schedule** field must be set to **Always**. This field is reserved for future use.
4. From the **Lock Mode** dropdown, select either **Bistable** or **Monostable** mode.

- In **Bistable** mode, the lock toggles between activated and deactivated each time a user enters a valid lock code.
- In **Monostable** mode, the lock activates for a set period each time a user enters a valid lock code, defined by the **Switch-On Duration**.

5. The **Switch-On Duration** option defines the lock activation time (from 1-120 seconds).

   This option is only available when Monostable mode is selected.

6. Select the **Sound** to play during lock activation / deactivation.
   - **None**: When selected, no sound is played during lock activation / deactivation.
   - **Short Beep**: When selected, the entry station plays a short beep during lock activation / deactivation.
   - **Lock Switch Activation Sound**: When selected, the Lock Activation Sound (see page 25) plays during lock activation / deactivation.
7. The **Activate By Call** option is reserved for future use.
8. Click **Save**.

Programming Lock Codes

Lock Codes enable you to remotely activate / deactivate the lock output. During a VoIP call from an IP phone to the entry station, a lock code can be entered, followed by the * key, to remotely trigger the lock.

If you have mistyped the lock code and want to start over, press # to clear the PIN field.

1. From the **Lock** menu, select the **DTMF Lock Codes** tab.
2. **Add** up to 10 unique codes. Each code is a numerical value up to fifteen digits long.
3. The **Schedule** applied to all lock codes must be set to **Always**. This field is reserved for future use.
4. Click **Save**.

Viewing the Camera Feed

To view the entry station's camera feed, navigate to the **Camera** menu. The live feed is displayed on the screen.

Camera Integration

- To view the entry station's camera feed within Protege GX, follow the configuration instructions outlined in the Protege GX Camera Integration section (see page 43).
- To view the entry station's camera feed within Protege WX, follow the configuration instructions outlined in the Protege WX Camera Integration section (see page 51).
- If accessing the feed from other software the direct URL http://<IP_ADDRESS>:8080/video provides a live mpeg camera feed.

RTSP is **not** supported.

Protege GX Integration

Protege GX integration with the entry station provides the option of directory access with user synchronization, or system module integration including monitoring, access control and building management functionality.

Directory Integration

Directory integration synchronizes Protege GX user records with the entry station's directory. Directory listings automatically synchronize and display on the entry station, and can be accessed from the touchscreen to call tenants listed in the directory. Tenants can unlock a door or allow elevator access using valid Protege GX credentials.

Module Integration

Protege GX module integration with the entry station allows it to communicate with any Protege GX controller to control physical devices connected to the Protege GX network. When the entry station is integrated with Protege GX, you can program functions that enable users to use the touchscreen to unlock the doors leading to their apartment, trigger lighting along the way, and authorize elevator access to the appropriate floor.

User PIN encryption: Integration with Protege GX requires the entry station to access and validate user PIN codes, via the Protege GX SOAP service. If the **Encrypt User PINs** feature is enabled the SOAP service is not able to view user PINs, therefore the entry station is not able to integrate with Protege GX.

Tenancy Portal Integration

The Protege Tenancy Portal offers improved user synchronization between Protege GX and the entry station.

- User records are programmed in Protege GX and automatically synchronized to the tenancy portal.
- The tenancy portal automatically creates a SIP account and Protege Mobile App account for each user. The directory is synchronized to the entry station, enabling visitors to video call tenants on the Protege Mobile App.
- If module integration with Protege GX is also enabled, the tenant can unlock the front door and elevator from the mobile app call screen.

For more information and programming instructions, see the Protege Tenancy Portal User Guide.

Protege GX Integration Prerequisites

The following sections outline how to populate the entry station's directory with Protege GX users, and program integrated functionality including opening a door and providing elevator access using the entry station, and viewing the camera feed and answering calls at a Protege GX workstation.

Controllable devices can also be configured to be activated as part of the trigger sequence when a PIN is entered. Additional configuration for these devices is beyond the scope of this document.

Entry station integration with Protege GX requires the following to be installed and operational:

Component	Prerequisites
Protege GX	Version 4.2 or higher is required to integrate elevator/floor access control.
Protege GX SOAP Service	Version 1.5.0.17 or higher is required to integrate elevator/floor access control.
Protege Vandal Resistant Touchscreen Entry Station	Firmware version 1.12.157 or higher is required to integrate elevator/floor access control.

Tenancy portal integration has different requirements. See the Protege Tenancy Portal User Guide.

Licensing

License	Order Code	Notes
Protege GX Client License	PRT-GX-CLNT	One license must be available for use by the SOAP service. This can support multiple entry stations.

Protege GX Directory Integration

The entry station's directory is populated from Protege GX user records using the Protege GX SOAP Service. Custom fields must be created in Protege GX to store additional user information specific to the entry station directory.

Configuring the Entry Station's Directory Sync Settings

The entry station must first be configured to communicate with the Protege GX SOAP Service.

1. Log in to the entry station's web interface.
2. Navigate to **Device Settings | Directory Sync**.
3. Enter the IP address of the SOAP server in the **SOAP Server Address** field.
4. Enter the **SOAP Server Port**. This is configurable but must match your Protege GX SOAP Service installation. The default is 8030.

   The SOAP server's port must be open on the server.

5. Enter the **Site ID** (the database ID assigned to the site, found in Protege GX under **Global | Sites**).
6. Enter the **Username** of the Protege GX operator that will be used to access the SOAP service.

   This operator will need sufficient access rights, typically using the **Administrator** role.

7. Enter the operator's **Password**.
8. Click **Save**.

Show PIN Numbers for Users

1. In Protege GX, navigate to **Global | Operators** and select the operator configured to access the SOAP service in the entry station's **Directory Sync** settings above.
2. In the **Configuration** section, check the **Show PIN numbers for Users** checkbox, and click **OK** on the warning.
3. Click **Save**.

This configuration option is necessary in order for the SOAP service to access user PIN codes for use by the entry station, and must be enabled for any operator configured in the Directory Sync settings of any entry station that is integrated with Protege GX.

Protege GX Custom Field Programming

Follow the steps below to configure the Protege GX custom fields required to implement user integration.

The settings and naming (spelling and spacing) of these fields must be entered **exactly** as listed below in order to correctly link to the entry station, otherwise the synchronization will fail.

Directory Tab

This creates the **Directory** tab that will be used to add users to the directory and record their details.

1. In Protege GX, navigate to **Users | Custom Field Tabs**.
2. Click **Add**.
3. Enter Directory in the **Name** field.
4. Click **Save**.

Room Custom Field

This creates the field that will be used to record the user's room details.

1. Navigate to **Users | Custom Fields**.
2. Click **Add**.
3. Enter Room in the **Name** field.
4. Set the **Tab** to Directory.
5. Set the **Field Type** to Text.
6. Click **Save**.

Extension Custom Field

This creates the field that will be used to record the user's contact extension.

1. Click **Add**.
2. Enter Extension 1 in the **Name** field.
3. Set the **Tab** to Directory.
4. Set the **Field Type** to Text.
5. Click **Save**.

Note that although this field will be used to record extension numbers, the text field type is required to accommodate longer numbers, leading zeros and international prefixes, which the numerical field type does not support.

Add User to Directory Option

This creates the checkbox that will be used to add the user to the Protege GX directory listing. Once added to the Protege GX directory, the user will also be listed on the entry station.

1. Click **Add**.
2. Enter Add User To Directory in the **Name** field.
3. Set the **Tab** to Directory.
4. Set the **Field Type** to Option.
5. Click **Save**.

Additional custom fields can be created to record further information in Protege GX, such as parking allocation or emergency contact. However, these fields will not be synchronized with the entry station directory.

Adding Protege GX Users to the Directory

Before Protege GX users will appear on the entry station's directory list, their room and extension details must first be added to the Protege GX directory, using the custom fields created above.

1. To add a Protege GX user to the directory, navigate to **Users | Users** and select the user record.
2. Go to the **Directory** tab.

   This tab will only be available after it has been configured in Protege GX Custom Field Programming above.
3. In the **Room** field, enter the user's room number or name. This is equivalent to the **Unit Number** in the entry station.
4. In the **Extension 1** field, enter the phone number to dial to contact the user.

   The phone number cannot contain spaces or hyphens.
5. Check the **Add User To Directory** checkbox to include this user in the directory listing.
6. Click **Save**.

Custom Entry Station Directories

Each entry station can be configured to display a specific directory. This can be helpful where a site has multiple buildings or areas that each require their own unique directory.

Record groups and security levels are used to specify which users appear on each directory list, and operator roles determine which directory is displayed on each entry station.

To implement multiple directories, you will need:

- A record group for the directory custom fields and custom field tab
- A record group for each entry station directory
- A security level for each entry station directory
- An operator role for each entry station directory
- An operator for each entry station directory
- Configuration of the Directory Sync settings for each entry station to use the appropriate operator logon

Note: If users are to appear in multiple directories, you will need to create a record group that is shared between those directory lists. Then, in the operator role configuration, add the shared record group to the security level to enable those users on the entry station(s) where that role applies.

Custom Fields Record Group

First, you need to create a record group that will be assigned to the directory custom fields and tab.

This record group only needs to be created and applied once, as it will be used by all entry stations. It grants the entry station access to the required custom fields.

1. Navigate to **Sites | Record Groups** and click **Add**.
2. Enter a **Name** to describe the record group, such as Entry Station Directory Fields.
3. Click **Save**.
4. Navigate to **Users | Custom Field Tabs** and select the Directory custom field tab.
5. Set the **Record Group** to the Entry Station Directory Fields record group created above.
6. Click **Save**.
7. Navigate to **Users | Custom Fields** and assign the Entry Station Directory Fields record group to the following custom fields:
   - Room
   - Extension 1
   - Add User to Directory
8. Click **Save**.

Directory Record Groups

A record group must be created for each unique directory listing. This may mean a record group for each entry station, for each building or area, or a combination of shared directory lists based on roles or access privileges.

1. Navigate to **Sites | Record Groups** and click **Add**.
2. Enter a **Name** to describe the record group, such as Entry Station 1 Directory Group.
3. Click **Save**.
4. Navigate to **Users | Users** and select the users that will appear in this directory list.

   Hold **Control** and click to select multiple users.
5. Set the **Record Group** to the Entry Station 1 Directory Group record group created above.

6. Click **Save**.
7. Assign this record group to all users that are to be displayed in this directory list.

Directory Security Levels

As with record groups, a security level must be created for each unique directory listing.

While this may vary depending on your site configuration, a corresponding security level should typically be added for each directory record group that was created.

1. Navigate to **Sites | Security Levels** and click **Add**.
2. Enter a **Name** to describe the security level, such as Entry Station 1 Security Level.
3. Click **Save**.

Operator Roles

Operator roles are used to set the access level and record groups that determine which directory will be displayed on each entry station. You will need a separate operator role for each unique directory configuration.

1. Navigate to **Global | Roles** and click **Add**.
2. Enter a **Name** to describe the role, such as Entry Station 1 Role.
3. Ensure that the **Preset** selection is set to Administrator.

   Entry station operators require Administrator rights to access directory lists via the SOAP service.

4. Click the **Security Levels** tab, and in the **Security Levels** section click **Add**.
5. In the popup window select the **Security Level** created for this entry station/directory.
6. In the **Name** section select both the record group used for the custom fields and the record group used for this specific entry station directory.

   The Entry Station Directory Fields custom fields record group created earlier **must** also be included in this selection (hold the **Control** key and click to select multiple record groups).

7. Click **OK** to add the security level configuration.
8. Click **Save**.

Operators

To apply the above configuration, an operator must be created for each unique directory listing, with the appropriate role assigned, and then configured in the Directory Sync settings for each entry station.

1. Navigate to **Global | Operators** and click **Add**.
2. Enter a **Name**, such as Entry Station 1 Operator.
3. Set a unique **User Name** and **Password**.
4. Select the appropriate operator **Role**, as configured above. This will determine which directory is displayed on any entry stations that use this operator logon.
5. Click **Save**.

Operators must then be assigned as the SOAP operator for each entry station. Once this is complete, each entry station will display the directory listing that is configured under the role assigned to its logon operator.

Refer to the Configuring the Entry Station's Directory Sync Settings section (see page 34) for directions on configuring the operator that entry stations will use to connect to the SOAP Service to retrieve the directory listing.

Protege GX Module Integration

When the entry station is connected to your Protege GX system network, you can program the entry station to activate controllable devices, such as doors, elevator floors, lighting and climate control.

Users can then enter the PIN assigned to them in Protege GX, either into the numeric keypad of the touchscreen or into their phone during a call with the entry station, to activate the programmed functions.

Protege GX module integration requires configuration of Directory Integration (see page 34).

User PIN Operation

To unlock a door and activate any other functionality programmed for the entry station output, the user simply needs to enter their PIN, either into the numeric keypad of the entry station touchscreen or into their phone during a call with the entry station.

Depending on your system configuration, PIN entry can trigger multiple functions. Entering a PIN will always trigger all programmed functions.

Via Phone Call

To activate programmed functions while on a phone call with the entry station, simply enter your **PIN** into your phone's keypad, then press * to send.

If you have mistyped your PIN and want to start over, press **#** to clear the PIN field.

On the Touchscreen

1. Navigate to the **Directory** page on the entry station.
2. Press **Login**.
3. Enter your **PIN** and press enter.

Providing Protege GX User Access

Only users who have been assigned the necessary credentials will be able to unlock a door or elevator floor via the entry station. The user must be assigned a valid PIN, along with the necessary access level to be granted the requested access.

1. To provide a Protege GX user with the credential access to activate the entry station output control, navigate to **Users | Users** and select a user that requires this access.
2. In the **PIN** section, ensure that the user has a **PIN** code assigned.

   If providing access for an elevator service, PINs used to unlock floor access **must** be **5** digits in length.
3. Select the **Access Levels** tab and click **Add**.
4. Select the appropriate access level(s) for the user's required access, then click **OK**.
5. Click **Save**.

Door Control

Door control is achieved by adding the entry station as a keypad and configuring the desired functionality, including assigning the necessary door and access level requirements.

Configuring the Entry Station in Protege GX

The following instructions describe how to add the entry station to Protege GX as a keypad. This enables door control using keypad programming.

Configure the Entry Station Settings

1. Open the entry station's web interface by entering the IP address into your web browser address bar.
2. Log in using your operator login details.
3. Navigate to **Device Settings | General**.
4. In the **Controller** section, set the **Con IP Address** to the IP address of the controller you want to connect the entry station to.
5. Set the **Mod TX Port** to 9450 (the controller's module TCP port).
6. Set the **Address** to a currently unassigned keypad physical address number.
7. Click **Save**.

Configure the Controller

Controller module TCP communications are disabled by default and must be enabled by a command.

1. In Protege GX, navigate to **Sites | Controllers**.
2. Expand the **Commands** section and enter the following command:

   ```
   EnableModuleTCP = true
   ```
3. Click **Save**.

Confirm Connection

1. In Protege GX, navigate to **Sites | Controllers**.
2. Right click on the controller you are linking the entry station to and click **Module addressing**.
3. The entry station should display within the module addressing window as a keypad.

   > If you have multiple keypads connected, use the entry station's serial number to locate the correct record.

Add Keypad

1. If the entry station is displayed in the module addressing window, navigate to **Expanders | Keypads** and click **Add**.
2. Enter a **Name** for the entry station.
3. For the **Physical address**, select the keypad address configured in the entry station's web interface.
4. Click **Save**.
5. In the **Configure Module** popup window:
   - Set the **Inputs** to 0
   - Set the **Outputs** to 1
   - Disable the **Add trouble inputs** option.
6. Click **Add now** to complete the process.

Linking a Door to the Entry Station

Once the entry station has been configured as a keypad in Protege GX, it can be configured for door control. The following instructions outline how to link a Protege GX controlled door to the entry station.

Create a Keypad Group

1. Navigate to **Groups | Keypad groups**.
2. Click **Add** and enter a **Name** for the keypad group.
3. In the **Keypads** section, click **Add**.

4. Select the entry station's **Keypad** record and click **OK**.
5. Click **Save**.

Create a Menu Group

1. Navigate to **Groups | Menu groups** and click **Add**.
2. Enter a **Name** for the menu group.
3. In the **Settings** section, ensure that the **User (2)** option is enabled.
4. In the **Keypad groups** section, add the keypad group containing the entry station's keypad record.
5. Click **Save**.

Configure the Keypad Door Control

1. Navigate to **Expanders | Keypads** and select the entry station's keypad record.
2. Select the **Configuration** tab.
3. In the **Door connected to keypad** field, select the door you want to control with the entry station.
4. In the **Options 1** tab, enable the **Function key unlocks door when logged in (REX)** option.

   This configures the keypad to grant access with entry of a valid PIN, using either onscreen login or phone.
5. Click **Save**.

PIN-free Access

The entry station can be configured to unlock the door via phone call without the need for a PIN. To activate this feature, go to the **Options 1** tab and enable the **Function key unlocks door when logged out (REX)** option. The door can then be unlocked by simply entering * into a phone keypad during a call with the entry station.

PIN-free access is via phone call only. Doors cannot be unlocked via the onscreen login without a valid PIN.

Configure the Access Level

1. Navigate to **Users | Access levels** and create or select an existing access level.
2. In the **Doors** tab, ensure that the door linked to the entry station is added.
3. In the **Menu groups** tab, click **Add**.
4. Select the menu group created for the entry station and click **OK**.
5. Click **Save**.

Protege GX Postal Lock Configuration

Protege GX integration enables the entry station's onboard postal lock to be configured to open a Protege GX controlled door.

When the entry station is configured for door control, the postal lock will automatically be configured to open the **Door connected to keypad** assigned in the entry station's keypad record. For more information, see Door Control (page 38).

Note: The **Function key unlocks door when logged in (REX)** option must be enabled for the postal lock to open the door.

Elevator Control

The Protege GX integration makes it possible to use the entry station to unlock elevator access to designated floors. Users and associated access levels are configured within Protege GX and used to validate which floors they can travel to and when.

Users can then unlock the designated floor by entering the PIN assigned to them in Protege GX, either into the numeric keypad of the entry station touchscreen or into their phone during a call with the entry station. Once the floor is unlocked the elevator will authorize travel to the unlocked floor when it is selected.

Prerequisites

The following instructions outline how to integrate floor access control in Protege GX with the entry station. Ensure that all prerequisites (see page 32) have been met before proceeding, including all required elevator programming as appropriate for your elevator integration.

Linking an Elevator Car to the Entry Station

The entry station can be linked to an elevator car by using the elevator control configured in Protege GX and assigning the appropriate access levels to the users listed in the directory.

The following instructions outline how to link a Protege GX controlled elevator to the entry station.

Create Floor Groups

Floor groups are created to specify the floors that are physically accessible by each user access level, to define the floors that any given user is permitted to access. Depending on your site configuration and access permissions, you may require only one floor group to allow access to all floors, or you could require a number of floor groups to limit which floors are accessible by each elevator car, user group or permission level.

1. Navigate to **Groups | Floor groups** and click **Add**.
2. Enter a **Name** to identify the floor group.
3. In the **Floors** section, click **Add** and select the required **Floors**.
4. Click **Save**.

If you need to grant a user access to only one floor (e.g. the floor that a resident lives on), you must create a floor group containing only that floor. Assigning individual floors to an access level does not function correctly with this integration. This is a known issue.

Create Elevator Groups

Elevator groups are created to specify the elevator cars that each user is permitted to access. Depending on your site configuration and access permissions, you may require only one elevator group to allow access to all elevators, or you could require a number of elevator groups to limit which elevator cars are accessible to each access level.

1. Navigate to **Groups | Elevator groups** and click **Add**.
2. Enter a **Name** for the elevator group.
3. In the **Elevators** section, click **Add** and select the required **Elevator cars**.
4. Click **Save**.

Configure Access Levels

1. Navigate to **Users | Access levels** and create or select an existing access level.
2. In the **Floor groups** tab, click **Add** to add the floor group this user access level will have access to.
3. In the **Elevator groups** tab, click **Add** to add the elevator group this user access level will have access to.

   If required, individual elevators can be added in the **Elevators** tab.

4. In the **Menu groups** tab, click **Add** and select the menu group that was created for the entry station during the Linking a Door to the Entry Station process (see page 39), then click **OK**.
5. Click **Save**.

The above will need to be completed for each access level required. This could be a single access level, an access level for every floor, or any combination depending on your site configuration and access permissions.

Create the Intercom Service

An intercom service is required to manage requests for floor control access between the entry station and the Protege GX controller.

1. Navigate to **Programming | Services**.
2. In the toolbar, select the **Controller** that the entry station is communicating with.

   > The service must be programmed on the same controller as the entry station, even if the elevators are on a different controller.

3. Click **Add**.
4. Enter Entry Station Intercom Service as the **Name** to identify the intercom service.
5. In the **Type** section, set the **Service type** to Intercom.
6. Set the **Service mode** to 1 - Start with controller OS.
7. Go to the **General** tab and enter the following **Configuration** settings:

Port number	TCP/IP
TCP/IP Port	8082
Intercom type	MESH
Identify user type	User PIN
Elevator group	Select an elevator group containing all elevators that can be accessed by the entry station.
Floor group	Select a floor group containing all floors that can be unlocked by the entry station.

8. Click **Save**.
9. Start the service by right clicking the record in Protege GX and selecting **Start service**. The service can also be stopped via this option if required. Once configured the service starts automatically with the controller.

Single Keypress Unlock

By default, when a user receives a call to a phone number or third-party app, they have to enter their Protege PIN code to unlock the door and elevator. When the entry station has both directory and module integration with Protege, it is possible for users to instead enter a single digit, then press the asterisk key to unlock the door and elevator. The entry station will retrieve the user's PIN code from the directory and send it to the controller to unlock the door.

To enable this feature:

1. Navigate to **Device Settings | General**.
2. Check **Single Keypress enabled**.
3. Enter the required **Single Keypress value**.
4. Click **Save**.

> This feature is not required for Protege Mobile App users, as they can use the **Unlock** button.

Protege GX Camera Integration

Protege GX supports the monitoring of the entry station camera as a streaming MJPEG video feed.

1. Navigate to **Monitoring | Setup | Cameras** and click **Add**.
2. Set the **Type** to H.264 & motion JPEG stream camera.
3. Enter the **URL** for the camera's image stream: http://<IP_ADDRESS>:8080/video.

   If authentication is required to view the camera feed, include the login username and password in the URL. For example: http://username:password@192.168.1.2:8080/video

4. When the **Show sidebar controls in status page** option is enabled, playback controls are displayed when the camera feed is embedded into a status page.
5. When the **Stretch camera** option is enabled, the aspect ratio adjusts with the tile size. This may cause the image to be distorted.
6. The **Floor plan** selection defines the floor plan that the camera is associated with.
7. Click **Save**.

Once correctly configured, the camera can be monitored on floor plans and status pages and associated with particular devices, allowing you to view archived camera footage from selected events.

Calling a Protege GX Workstation

Protege GX workstations can be configured to act as a SIP client so that operators are able to answer calls from the entry station.

Each workstation must be registered with an extension in the SIP server.

1. Navigate to **Events | Workstations** and click **Add** to create a SIP client workstation.
2. Enter the **Name** to identify the workstation in the entry station directory.
3. The **Computer name** must be the network name of the computer to correctly identify it.
4. The **Server address** is the domain name or IP address of the SIP service connection.
5. The **Account name** is the name of the SIP extension allocated on the SIP PBX system for this workstation.
6. The **Account password** is the password of the SIP extension allocated on the SIP PBX system.
7. The **Realm** is the security domain where this account is valid. Entering * will allow your authentication password to be sent to the server without the realm being verified.
8. Enter the **SIP port** used for communications with the SIP PBX server.
9. The **Network interface** defines the network interface card used for communications.
10. Select the **Microphone** connected to the workstation.

    A microphone must be connected for the workstation to register as a SIP client.

11. The **Default microphone setting** defines the microphone level to be used when the call window is launched.
12. Select the **Speakers** connected to the workstation.
13. The **Default speaker setting** defines the speaker level to be used when the call window is launched.
14. Click **Save**.

Once configured, the workstation will appear in the entry station directory list and can be called just the same as any other extension.

Door Access

If you would like to also be able to open a door from the SIP client workstation, you can create an intercom record and associate it with the required door.

One Intercom Station license (Ordering code: PRT-GX-VOIP-10) is required for each intercom configured.

1. Navigate to **Monitoring | Setup | Intercoms** and click **Add**.
2. Enter a **Name** for the intercom record that reflects the workstation that will utilize it.
3. Enter the **URI** (Uniform Resource Identifier) for connecting to the intercom.
4. Assign the entry station's **Camera** for the video feed to come through to the operator during the call.
5. You may also want to associate the intercom with a **Floor plan**.
6. Click **Save**.
7. Navigate to **Programming | Doors** and select the door to be opened by the intercom.
8. Scroll down to the **Graphics** section and select the **Intercom (Entry)**.
9. Click **Save**.

Troubleshooting

The most common issues experienced with entry station integration are related to user and directory synchronization with Protege GX. The following are the key troubleshooting recommendations.

- Confirm that the entry station's Directory Sync settings (see page 34) are correct, particularly the SOAP Server Address and operator Username.
- Confirm that the SOAP service port is open on the server.
- Confirm that the SOAP service is functional. The best method is to install the Protege GX Web Client and confirm that you can log in using the same operator information as in the Directory Sync settings.
- Confirm that the user custom fields are named and configured correctly (see page 34).
- Confirm that there is a concurrent client license available for use by the SOAP service (see page 32). If this is not available, SOAP cannot connect to the data service to synchronize the directory from Protege GX.

Protege WX Integration

Protege WX integration with the entry station provides basic user integration with directory access, or system module integration including extended monitoring, access control and building management functionality.

Directory Integration

Directory integration enables the use of Protege WX directory user records. Directory listings automatically synchronize and display on the entry station, and can be accessed from the touchscreen to call tenants listed in the directory. Tenants can unlock a door using validated credentials.

Module Integration

Protege WX module integration with the entry station allows it to communicate with the Protege WX controller to control any physical devices connected on the Protege WX network. When integrated with Protege WX, you can program functions that enable you to use the touchscreen to unlock the doors leading to your apartment and trigger lighting along the way.

Tenancy Portal Integration

The Protege Tenancy Portal offers limited integration between Protege WX and the entry station.

- There is no synchronization between the tenancy portal and Protege WX. User information (names, email addresses and PIN codes) must be entered into the tenancy portal manually.
- The tenancy portal automatically creates a SIP account and Protege Mobile App account for each user. The directory is synchronized to the entry station, enabling visitors to video call tenants on the Protege Mobile App.
- If module integration with Protege WX is also enabled, the tenant can unlock the front door from the mobile app call screen.

For more information and programming instructions, see the Protege Tenancy Portal User Guide.

Protege WX Integration Prerequisites

The following instructions outline how to populate the entry station's directory with Protege WX users, configure the entry station in Protege WX as a keypad, and program integrated functionality including opening a door using the entry station.

Entry station integration with Protege WX requires:

- An operational Protege WX system.
  - The user directory integration does not currently work on controllers which are using HTTPS communications. To enable this integration you will need to disable HTTPS in **System | Settings | General**.
  - Module integration requires the Protege WX controller to be licensed with Advanced mode enabled.
- An operational Protege Vandal Resistant Touchscreen Entry Station.

Tenancy portal integration has different requirements. See the Protege Tenancy Portal User Guide.

Protege WX Directory Integration

The touch screen's directory is populated with Protege WX users by using the controller's IP address to connect to the Protege WX system and retrieve user records.

This feature is not available when HTTPS is enabled on the controller.

Configuring the Entry Station's Directory Sync Settings

The entry station must first be configured to communicate with the Protege WX controller.

1. Log in to the entry station's web interface.
2. Navigate to **Device Settings | Directory Sync**.
3. In the **SOAP Server Address** field, enter the IP address of the Protege WX controller as follows:

   <IPADDRESS>/voipphonebook.xml

   The remaining Directory Sync settings are not required when integrating with Protege WX. Only the controller's IP address is needed, and must be entered in exactly the format displayed above.
4. Click **Save**.

Adding Protege WX Users to the Directory

Before Protege WX users will appear on the entry station's directory list, the integration must first be enabled and users must be added to the Protege WX directory by entering their extension details.

Enable Integration

1. In the Protege WX web interface, navigate to **System | Settings**.
2. In the **General** tab, check whether **Use HTTPS** is enabled. If so, disable this checkbox, save and click **Restart** in the toolbar to restart the controller.
3. Go to the **Options** tab and check the **Enable VOIP Integration** checkbox to enable this feature.

Add User to Directory

1. To add a Protege WX user to the directory, navigate to **Users | Users** and select the user record.
2. Enter the user's **Phone Extension**.

   If no phone extension is present, the user will **not** appear in the directory. The phone number cannot contain spaces or hyphens.
3. Click **Save**.

Protege WX Module Integration

When the entry station is connected to your Protege WX system network, you can program the entry station to activate controllable devices, such as doors, lighting and climate control.

Users can then enter their PIN, either into the numeric keypad of the touchscreen or into their phone during a call with the entry station, to activate the programmed functions.

Protege WX module integration requires configuration of Directory Integration (see previous page).

User PIN Operation

To unlock a door and activate any other functionality programmed for the entry station output, the user simply needs to enter their PIN, either into the numeric keypad of the entry station touchscreen or into their phone during a call with the entry station.

Depending on your system configuration, PIN entry can trigger multiple functions. Entering a PIN will always trigger all programmed functions.

Via Phone Call

To activate programmed functions while on a phone call with the entry station, simply enter your **PIN** into your phone's keypad, then press ***** to send.

If you have mistyped your PIN and want to start over, press **#** to clear the PIN field.

On the Touchscreen

1. Navigate to the **Directory** page on the entry station.
2. Press **Login**.
3. Enter your **PIN** and press enter.

Providing Protege WX User Access

Only users who have been assigned the necessary credentials will be able to unlock a door via the entry station. The user must be assigned a valid PIN, along with the necessary access level to be granted the requested access.

1. To provide a Protege WX user with the credential access to activate the entry station output control, navigate to **Users | Users** and select a user that requires this access.
2. In the **Access Cards** section, ensure that the user has a **PIN Code** assigned.
3. Select the **Access** tab and click **Add**.
4. Select the appropriate access level(s) for the user's required door access, then click **OK**.
5. Click **Save**.

Configuring the Entry Station in Protege WX

The following instructions describe how to add the entry station to Protege WX as a keypad. This enables door control using keypad programming.

Configure the Entry Station Settings

1. Log in to the entry station's web interface.
2. Navigate to **Device Settings | General**.
3. In the **Controller** section, set the **Con IP Address** to the IP address of the controller you want to connect the entry station to.
4. Set the **Mod TX Port** to 9450 (the controller's module TCP port).

5. Set the **Address** to a currently unassigned keypad physical address number.
6. Click **Save**.

Configure the Controller

Controller module TCP communications are disabled by default and must be enabled by a command.

1. In Protege WX, navigate to **System | Settings**.
2. Enter the following command in the **Commands** section:
   ```
   EnableModuleTCP = true
   ```
3. Click **Save**.

Add Keypad

1. In the Protege WX web interface, navigate to **Wizards | Expanders Wizard**.
2. Click **Step 2 - Auto Detection**.
3. The entry station should display in the auto-detection section as a keypad.

   If you have multiple keypads connected, use the entry station's serial number to locate the correct record.

4. Enter a **Name** for the entry station.
5. Click **Step 3 - Additional Modules**.
6. Click **Save and Return to Menu**.

   When the entry station is added to Protege WX as a keypad, some extra inputs and outputs are automatically programmed. As these are not required for the entry station, you can delete them from the web interface.

7. To delete the inputs, navigate to **Programming | Inputs** and select the two inputs created.
8. Click **Delete** and when prompted to confirm, click **Yes**.
9. To remove the extra outputs, navigate to **Programming | Outputs**.
10. Select the **Red LED**, **Green LED** and **Beeper** outputs, and click **Delete**. When prompted to confirm, click **Yes**.

    Leave **Output 1** remaining as this can be used for programming the entry station's programmable output.

Linking a Door to the Entry Station

Once the entry station has been configured as a keypad in Protege WX, it can be configured for door control. The following instructions outline how to link a Protege WX controlled door to the entry station.

Create a Keypad Group

1. Navigate to **Programming | Keypad Groups**.
2. Click **Add** and enter a **Name** for the keypad group.
3. In the **Keypads** section, click **Add**.
4. Select the entry station's **Keypad** record and click **OK**.
5. Click **Save**.

Create a Menu Group

1. Navigate to **Programming | Menu Groups** and click **Add**.
2. Enter a **Name** for the menu group.
3. In the **Settings** section, ensure that the **User (2)** option is enabled.

4. In the **Keypad Groups** section, add the keypad group containing the entry station's keypad record.
5. Click **Save**.

Configure the Keypad Door Control

1. Navigate to **Expanders | Keypads** and select the entry station's keypad record.
2. Select the **Configuration** tab.
3. In the **Door connected to keypad** field, select the door you want to control with the entry station.
4. In the **Options 1** tab, enable the **Function Key Unlocks Door When Logged In (REX)** option.

   This configures the keypad to grant access with entry of a valid PIN, using either onscreen login or phone.

5. Click **Save**.

PIN-free Access

The entry station can be configured to unlock the door via phone call without the need for a PIN. To activate this feature, go to the **Options 1** tab and enable the **Function Key Unlocks Door When Logged Out (REX)** option. The door can then be unlocked by simply entering * into a phone keypad during a call with the entry station.

PIN-free access is via phone call only. Doors cannot be unlocked via the onscreen login without a valid PIN.

Configure the Access Level

1. Navigate to **Users | Access Levels** and create or select an existing access level.
2. In the **Doors** tab, ensure that the door linked to the entry station is added.
3. In the **Menu Groups** tab, click **Add**.
4. Select the menu group created for the entry station and click **OK**.
5. Click **Save**.

Protege WX Postal Lock Configuration

Protege WX integration enables the entry station's onboard postal lock to be configured to open a Protege WX controlled door.

When the entry station is configured for door control, the postal lock will automatically be configured to open the **Door connected to keypad** assigned in the entry station's keypad record. For more information, see Linking a Door to the Entry Station (previous page).

Note: The **Function Key Unlocks Door When Logged In (REX)** option must be enabled for the postal lock to open the door.

Single Keypress Unlock

By default, when a user receives a call to a phone number or third-party app, they have to enter their Protege PIN code to unlock the door and elevator. When the entry station has both directory and module integration with Protege, it is possible for users to instead enter a single digit, then press the asterisk key to unlock the door and elevator. The entry station will retrieve the user's PIN code from the directory and send it to the controller to unlock the door.

To enable this feature:

1. Navigate to **Device Settings | General**.
2. Check **Single Keypress enabled**.
3. Enter the required **Single Keypress value**.
4. Click **Save**.

This feature is not required for Protege Mobile App users, as they can use the **Unlock** button.

Protege WX Camera Integration

Protege WX supports the monitoring of the entry station camera as a streaming MJPEG video feed.

1. Navigate to **Programming | Cameras** and click **Add**.
2. Enter the **Name** of the entry station camera.
3. Select the **Door** that the entry station camera is associated with.
4. In the **Manual Configuration** section enter the **Streaming MJPG URL** for the MJPEG video stream: http://<IP_ADDRESS>:8080/video.

   If authentication is required to view the camera feed, include the login username and password in the URL. For example: http://username:password@192.168.1.2:8080/video

   The **Static Image URL** and **Refresh Rate** settings have been superseded and are no longer functional.

5. Click **Save**.

Once correctly configured, the **Camera Preview** will be displayed in the Protege WX interface.

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		Surface Mount Model	Flush Mount Model
Entry Station Models		PRT-ENTR-17-SFC	PRT-ENTR-17-FMT
Optional Rough-In Box		N/A	PRT-ENTR-17-FMT-RIB
Power Supply			
Operating Voltage		12VDC (10 -16VDC)	
Operating Current		4A (Typical)	
Power over Ethernet		PoE 802.3at Class 4 (25.5W max) For use **ONLY** with the supplied PoE injector (POE60U-560E-R) and PoE splitter (POE45-120-R)	
Communication			
Ethernet Speed		10/100	
Ethernet Port		HTTP:80 Web Interface, UDP:5060 SIP, TCP:9450 Module Comms	
Camera			
Resolution		720p (1280x720 pixels)	
Viewing Angle		140° horizontal / 70° vertical	
Frame Rate		15 fps	
Audio			
Out	Speakers	2 x 8Ω, 1W RMS	
	Amplifier	1.5W, 0.1% THD	
	Max Volume	85dB at 1m	
In	Microphone	6mm Electret Condensing	
	Direction	Omnidirectional	
	Sensitivity	-46dB Nominal Sensitivity	
	Signal/Noise Ratio	> 60dB	
I/O			
Inputs	Postal Lock Input	1	
Outputs	Open Collector Output	1	
Environment			
Operating Temperature		0°- 55° Celsius (32° - 131° Fahrenheit)	
Working Humidity		10% to 90%	
Environmental IP Rating		IP65	
Dimensions		**Surface Mount Model**	**Flush Mount Model**

Visible	Height	438mm (17.3″)	508mm (20″)
	Width	424.5mm (16.7″)	498mm (19.6″)
	Depth	67.4mm (2.65″)	1.5mm (0.06″)
Bracket / Back Box	Height	353mm (13.89″)	440mm (17.3″)
	Width	420mm (16.5″)	424mm (16.7″)
	Depth	2mm (0.07″)	74.5mm (2.9″)
Net Weight		13.0kg (28.7lb)	13.8kg (30.4lb)
Gross Weight		17.7kg (39.0lb)	17.1kg (37.7lb)

Dimensions	Optional Flush Mount Rough-In Box
Dimensions (L x W x H)	454 x 432 x 73.5mm (17.9 x 17.0 x 2.9″)
Net Weight	3.6kg (7.9lb)
Gross Weight	5.5kg (12.1lb)

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.

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

FCC Compliance Statements

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

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 class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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.