PRT-WX-DIN

Using Protege WX

Programming Reference Manual

Last Published: 13-Sep-23 11:23 AM

Contents

Introduction

Protege WX is an all-in-one, web-based, cross-platform system that gives you a fully functional access control and intrusion detection solution in a fraction of the time of conventional software. With no software to install, setup is quick and simple. Connect the controller and system components, then open a web browser to launch the intuitive wizard-driven interface which guides you through the process of configuring your system.

This manual covers how to get started with Protege WX and program, monitor and report on the system. It also contains full reference documentation for all of the options available in Protege WX.

You can also access this documentation online using any device with an internet connection and web browser. The online version is more up-to-date and easier to search and navigate. There are two ways to access the online help:

- Log in to a Protege WX controller and click **Help**. If the controller can access the internet, it will open the online help. If the controller has no internet access, it will open the PDF manual saved on the device.
- Open a web browser and navigate to: https://doc.ict.co/wxhelp/index.htm

You don't need to log in to access the documentation - bookmark the page to get help from your PC, laptop or phone even when the controller itself doesn't have internet access.

Controller Models

The controller is the central processing unit responsible for the control of security, access control and automation in the Protege WX system, and is available in the following models.

- PRT-WX-DIN-IP: The Protege WX DIN Rail Integrated System Controller (IP only) has 2 reader ports, independently configurable for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **.

  It also has a USB port which enables offsite communication via cellular network with connection to a Protege DIN Rail Cellular Modem.
- PRT-WX-DIN: The Protege WX DIN Rail Integrated System Controller has 2 reader ports, independently configurable for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **.

  It also has a USB port which enables offsite communication via cellular network with connection to a Protege DIN Rail Cellular Modem, and features a built-in modem dialer for phone line monitoring.
- PRT-WX-DIN-1D: The Protege WX DIN Rail Single Door Controller has 1 RS-485 enabled reader port, allowing connection of up to 2 RS-485 capable readers providing entry/exit control for a single door.

All models provide onboard access control and offsite IP reporting via the ethernet connection.

	PRT-WX-DIN-IP	PRT-WX-DIN	PRT-WX-DIN-1D
Wiegand Reader Ports	2**	2**	-
RS-485 Reader Ports	2**	2**	1
Inputs	8	8	2
Bell Output	1	1	-
Outputs (Open Collector)	4	4	-
Relay Outputs	2	2	1
USB Port	1	1	-
Telephone Dialer (for PSTN monitoring)	-	1	-

** Each reader port supports either Wiegand or RS-485 reader operation, but not both at the same time. If combining reader technologies, they must be connected on separate ports.

Each port configured for RS-485 operation supports 2 readers, with the wiring identifying which is the entry reader, and which is the exit reader.

RS-485 reader port connections support configuration for OSDP protocol. The ICT implementation of OSDP conforms to a subset of the OSDP functionality. For specifications and reader configuration, refer to Application Note 254: Configuring OSDP Readers, available from the ICT website.

What This Manual Covers

This manual is divided into the following sections:

- **Getting Started**: Logging in and registering your controller.
- **Basic Programming**: Using the Protege WX configuration wizards to set up your site.
- **Monitoring Your System**: Using the Events page, Status Lists and LED indicators to show what is happening.
- **Property Reference Guide:** An explanation of the available programming options and what they do.
- **Maintaining Your System**: Basic system maintenance, including how to backup and restore controller programming and update firmware.
- **Troubleshooting**: Helpful troubleshooting information, including how to resolve health status messages.

For information on installing the controller and other system modules, see the Protege WX DIN Rail Integrated System Controller Installation Manual.

Operation Mode

Protege WX launches in basic mode with full access control and intrusion detection ready to go. This hides the more complicated features, making the system more intuitive and simple to use.

Undertake an optional training course to unlock the advanced mode features including building automation, programmable functions and elevator control.

To find out more about training and unlocking advanced mode, please contact ICT.

System Expansion and Capacities

The modular-based hardware design provides the flexibility to accommodate any installation, small or large, residential or commercial. Optional expandable modules allow you to scale your system as your requirements change. Need more PIRs? Add an input expander. Want more doors? Add a reader expander.

If you reach capacity, you can easily upgrade to the enterprise level Protege GX.

System Capacities	Protege WX System
Users	10,000
Events	50,000
Schedules	512
Doors	128
Areas	32
Inputs	512
Outputs	512
Floors	32*
Elevator Cars	8*
Programmable Functions	248*
Keypads	200
Reader Expanders	64
Input Expanders	248
Output Expanders	32
Analog Expanders	32

* Floors, Elevator Cars, and Programmable Functions are only available in Protege WX Advanced mode.

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-WX-DIN-IP	Protege WX DIN Rail Integrated System Controller (IP only)
Power Supply	
Operating Voltage	11-14V DC
Operating Current	120mA (Typical)
DC Output (Auxiliary)	10.45-13.85V DC 0.7A (Typical) Electronic shutdown at 1.1A
Bell DC Output (Continuous)	10.4-13.45V DC 8 ohm 30W Siren or 1.1A (Typical) Electronic shutdown at 1.6A
Bell DC Output (Inrush)	1500mA
Total Combined Current*	3.4A (max)
Electronic Disconnection	9.0V DC
Communication	
Ethernet	10/100Mbps ethernet communication link
RS-485	3 RS-485 communication interface ports - 1 for module communication, 2 for reader communication
USB	Type-A
Readers	
Readers	2 reader ports, independently configurable for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **
	RS-485 reader port connections support configuration for OSDP protocol
Inputs	
Inputs (System Inputs)	8 high security monitored inputs
Outputs	
Outputs	4 (50mA max) open collector outputs for reader LED and beeper or general functions
Relay Outputs	2 Form C relays - 7A N.O/N.C. at 30V AC/DC resistive/inductive
Dimensions	
Dimensions (L x W x H)	156 x 90 x 60mm (6.14 x 3.54 x 2.36")
Net Weight	348g (12.3oz)
Gross Weight	428g (15.1oz)
Operating Conditions	
Operating Temperature	UL/ULC 0° to 49°C (32° to 120°F) : EU EN -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)

Mean Time Between Failures (MTBF)	560,421 hours (calculated using RDF 2000 (UTE C 80-810) Standard)

* The total combined current refers to the current that will be drawn from the external power supply to supply the expander and any devices connected to its outputs. The auxiliary outputs are directly connected via thermal resettable fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses. The Bell output is connected in the same way.

** Each reader port supports either Wiegand or RS-485 reader operation, but not both at the same time. If combining reader technologies, they must be connected on separate ports.

The size of conductor used for the supply of power to the unit should be adequate to prevent voltage drop at the terminals of no more than 5% of the rated supply voltage.

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.

Getting Started

This section outlines the process for logging in for the first time and performing initial system configuration.

Logging In for the First Time

The web interface can be accessed by entering the controller's current IP address into the address bar of a browser, then logging in with valid credentials.

Protege controllers come equipped with a factory loaded HTTPS certificate, ensuring a secure encrypted web connection. This means HTTPS must be used when accessing the web interface (e.g. https://192.168.1.2). The factory loaded HTTPS certificate is a self-signed certificate, so when connecting to the controller's web interface a certificate warning may be displayed, but your connection is still secure.
For older controllers not equipped with a default certificate, HTTP must be used to connect to the interface.

When using Safari, ensure that private browsing mode is disabled. This applies to all versions of Safari: Mac, iPad and iPhone. If private browsing mode is enabled an error message prompts you to disable it.

To log in to the controller for the first time, open a web browser and enter the default IP address of **192.168.1.2** with the prefix https:// (e.g. https://192.168.1.2).

If you cannot access the controller with this URL, remove the https:// prefix and try again (e.g. 192.168.1.2).

If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the controller web page.

Once you connect to the controller's web interface you will be prompted to create the admin operator, which is the default login for accessing the web interface.

One-door controllers may require additional steps to access the web interface (see below).

Creating the Admin Operator

The controller's factory default settings do not contain a default operator. When a controller is first connected or has been factory defaulted you will be prompted to **Create Admin Operator**. The admin operator must be added before the controller can be accessed and configured through the web interface.

Earlier versions of the controller firmware have a preconfigured admin operator. If you are not prompted to create a new operator you can log in using the default username admin with the password admin.

1. **Add a Username** for the admin operator. This does not need to be 'admin'.
2. **Choose a Password** for the admin operator.

   The password cannot be blank or 'admin' and must comply with password policy requirements.
3. **Verify Password**.

A very secure password is recommended for the admin operator (see Creating a Secure Password).

Browsing to One-Door Controllers

One-door controllers which do not have a USB port use an older hardware type which does not support more recent security protocols and cipher suites. This means that any older one-door controller with a security certificate installed is not trusted by modern web browsers. Most web browsers will not allow users to access the web interface pages of these controllers, even if users trust the site and accept the risk.

If you have a one-door controller which does not have a USB port, you may see one of the following errors when you attempt to access the web interface:

- **Chrome**: "This site can't be reached"
- **Edge**: "Hmmm... can't reach this page"
- **Firefox**: "Secure Connection Failed" (PR_END_OF_FILE_ERROR)

In this situation the recommended solution is to allow access to the controller's web interface by creating a Firefox profile with downgraded security.

To avoid security vulnerabilities it is recommended to use this profile only for accessing one-door controllers.

1. Download and install Firefox from the Mozilla website if you do not already have it.
2. Open Firefox, type **about:profiles** into the URL bar and press **Enter**.
3. Click **Create a New Profile** to open the wizard.
4. Click **Next**.
5. Enter a descriptive profile name (e.g. Controller).
6. Click **Finish**.
7. Click **Launch profile in new browser**.

   You can return to the **about:profiles** page at any time to switch between profiles or set a default profile.
8. In the new browser, type **about:config** into the URL bar and press **Enter**.
9. Click **Accept the Risk and Continue**.
10. In the search bar, enter **security.tls.version.enable-deprecated**.
11. By default this is set to false. Click the toggle button on the right to set it to true.
12. Attempt to browse to your controller on https://192.168.1.2 (use your controller's configured address if it has been changed from the default). Firefox will report that there is a potential security risk, because the controller has a self-signed certificate.
13. Click **Advanced...**
14. Click **Accept the Risk and Continue**.
15. The browser will present the controller's login screen. In future, you should be able to browse to this controller using this Firefox user profile.

Creating a Secure Password

When creating or changing the admin operator password it is **highly recommended** that you create a very secure password.

As a guideline, a secure password should include these features:

- Minimum 8 characters in length
- Combination of upper and lower case letters
- Combination of numbers and letters
- Inclusion of special characters

Passwords must comply with password policy requirements.

Signing In

To access the system after the initial setup you need to sign in with a valid operator username and password.

1. Open a web browser and enter the controller's IP address, with the prefix https:// (e.g. https://192.168.1.2).

   If you cannot access the controller with this URL, remove the https:// prefix (e.g. 192.168.1.2).

2. If you are presented with a security warning when accessing the HTTPS web page, use the advanced options to proceed to the controller web page.
3. The **Sign In** window is displayed.
4. Enter your operator **Username** and **Password**.
5. Click **Sign In**.

Repeatedly entering incorrect passwords at the sign in window forces a login stand down. Three consecutive incorrect attempts will result in the sign in process being locked for 5 seconds. If another three attempts fail, the sign in process is locked for 60 seconds between all subsequent attempts until a valid login is made. It is not possible to configure the length of time for the login stand down.

Older one-door controllers may require additional steps to access the web interface. For more information, see Browsing to One-Door Controllers (page 15).

Registering Your Controller

Once logged in, you will be prompted to register your controller:

1. Navigate to **System | Licensing** and select the **License Update** tab.
2. Enter your **Site** and **Installer** details.

   If desired, enable the **Display Site Name** option to display the site name in the top right corner.

3. Select the **Automatic** or **Manual** option to download and activate your Protege WX license.

To Automatically Activate Your License:

4. Click **Download License**.
5. Your details are passed to the ICT web registration service, then your license is activated automatically.

Important: The automatic activation process requires an internet connection on the workstation you are using to connect to the controller. If this is not available, you will need to use the manual activation option.

To Manually Activate Your License:

4. Click **Generate File** to create a license request file. When prompted, save the .req file to a folder on your network or a portable drive.
5. Click on the link to select your licensing options. This opens a web page where you will be prompted to enter your site, installer, and serial number details.
6. Browse to the saved .req file and click **Submit**.
7. Your details are passed to the web registration service. Once registration is complete you will be prompted to download your license (*.lic) file.
8. Return to Protege WX. Click **Browse** to select the license file and activate your Protege WX license.

Set the Controller Time

1. Navigate to **Scheduling | Time**.
2. Click **Apply PC Time and Date Now** to set the current date and time to that of your PC then click **Save**.

Configuring the IP Address

The controller must be programmed with a valid IP address to allow communication. By default this is set to **192.168.1.2** but can be adapted to suit your network requirements and addressing scheme.

If the IP address has been configured previously and you are not sure what it is, you can temporarily default it to 192.168.111.222. For more information, see Temporarily Defaulting the IP Address.

1. Log in to the controller and navigate to **System | Settings**.
2. In the **Adaptor - Onboard Ethernet** tab, enter the required connection settings:
   - **Enable DHCP**: When the option is enabled, the controller will use DHCP to dynamically allocate an IP address instead of using a static IP address.

     To use this feature, there must be a DHCP server on the network you are attempting to connect to.
   - **IP Address**: This is the IP address that the controller is currently using. By default this is set to **192.168.1.2**.
   - **Subnet Mask**: Used in conjunction with the IP address, a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to **255.255.255.0**.
   - **Default Gateway**: Used in conjunction with the IP address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the controller is connected. By default this is set to **192.168.1.254**.

     Set this field to **0.0.0.0** to prevent any external communication.
3. Click **Save**.
4. Click **Restart** in the toolbar to restart the controller and implement the changes.

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.

Setting Up Integrated DDNS

DDNS (Dynamic Domain Name Server) is a method which allows you to create a static hostname even when the external IP address of the controller is not fixed. The controller contains an integrated DDNS client which automatically updates the DDNS provider whenever the IP address changes.

Controllers currently support two DDNS providers: Duck DNS (free provider) and No-IP (free accounts available, paid plans for further services).

In order to set up DDNS, the controller must be port forwarded so that it is externally accessible.

Setting Up Duck DNS

Duck DNS can be used for HTTPS certification via third-party certificates.

1. Browse to Duck DNS and create a free account by signing in with Google or another existing account. Take note of the **Token** that is generated when you create your account.
2. Create a new **subdomain**. The full hostname will have the form [subdomain].duckdns.org.
3. The **Current IP** field should automatically populate with the external IP address of your network. Ensure that this is the controller's externally accessible IP address.
4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings**.
6. In the **Adaptor - Onboard Ethernet** tab, select the **Enable DDNS** checkbox.
7. Enter the **Hostname** [subdomain].duckdns.org and **DDNS Server** duckdns.org.
8. Leave the **DDNS Username** blank. For the **DDNS Password**, enter the **Token** generated by your Duck DNS account.
9. **Save** your settings.
10. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

    If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.duckdns.org:1000).

Setting Up No-IP

The free No-IP Dynamic DNS service does not support third-party certification. This is only supported with the additional Plus Managed DNS service.

1. Browse to No-IP and create a **Dynamic DNS** account (free or paid as required).

   Free Dynamic DNS hostnames provided by No-IP require confirmation every 30 days, whereas paid accounts do not.
2. Create a new **Hostname** and select a **Domain**.
3. Ensure that the **IP Address** matches the controller's externally accessible IP address.
4. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
5. Navigate to the **System Settings**.
6. In the **Adaptor - Onboard Ethernet** tab, select the **Enable DDNS** checkbox.
7. Enter the **Hostname** and **DDNS Server**.
8. Enter the **Username** and **Password** that you used to sign up to No-IP.

9. **Save** your settings.
10. Confirm that the controller is externally accessible by browsing to the hostname on another PC.

    If the controller's external port is not the default port, you will need to append the port number to the URL (e.g. controller.ddns.org:1000).

Setting Up an HTTPS Connection

Protege controllers come preconfigured with a self-signed certificate and HTTPS enabled by default, so that communications between the controller and the web browser are always encrypted. However, an alternative certificate can be installed if preferred. Installing a third-party certificate on the controller will remove the security warning which you may see in your browser when accessing a controller with a factory certificate.

For older controllers without a default HTTPS certificate, it may be possible to install an HTTPS certificate after upgrading the controller's operating system. This is **strongly recommended** for any controller that is connected to internal or external networks via a router. Contact ICT Technical Support for more information.

Two different connection methods are available, each of which can be configured directly within the web interface:

- Validating and installing a third-party certificate obtained from a certificate authority.
- Installing a self-signed certificate (recommended for testing only).

If the controller is factory defaulted, any user-created HTTPS certificates are removed and the default certificate is reloaded. Custom certificates will need to be reinstalled.

For configuration and version requirements refer to AN-280 HTTPS Connection to the Protege WX Controller, available from the ICT website.

Connectivity Requirements for HTTPS

To acquire a third-party certificate for HTTPS connection to the controller's web interface, the controller must be accessible over the internet. This section discusses some of these requirements so that the system can be properly prepared for HTTPS implementation.

Operating on an active network requires knowledge of the configuration and structure of the network. Always consult the network or system administrator before you begin.

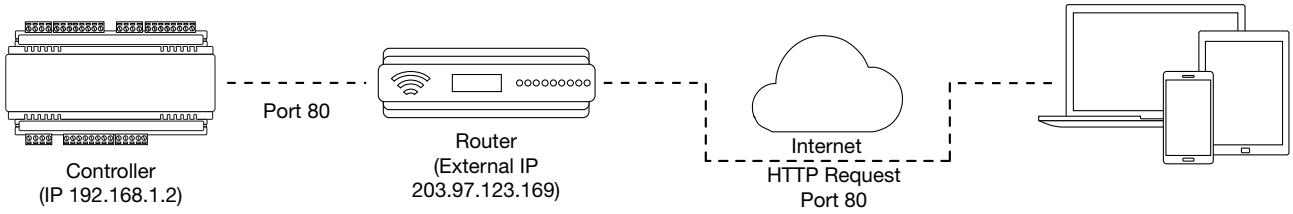
More Information

- For detailed networking information, see the Protege WX Network Administrator Guide.
- For basic information on Protege WX controller networking see AN-189: Protege WX Connectivity Guide.

Port Forwarding Requirements

In order for the controller to be accessible externally, port forwarding must be configured at the router. Port forwarding is a method of mapping an IP address and port on a local subnet to an external port, so that the networked device is accessible over the internet.

In particular, validating a third-party certificate generally requires the controller to be accessible via **external port 80**. This is the default port for HTTP requests. This external port must be set up to forward traffic to an internal port on the controller that accepts HTTP requests. By default this is **internal port 80**; however, if required this can be changed in the **System Settings**.



Once this port has been forwarded, the controller will be accessible via the external IP address of the network. In this example, typing 203.97.123.169 into an external web browser will open the controller's web interface.

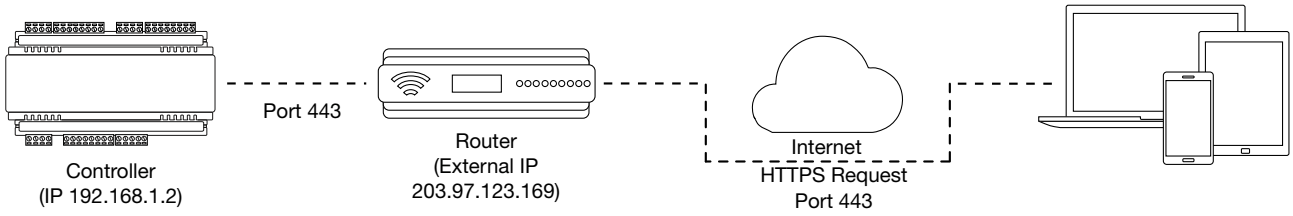
External access via HTTP is only required in order to validate and install your certificate. Once the certificate has been installed, HTTP access will be disabled because the more secure HTTPS connection is available. Therefore it will no longer be necessary to forward external port 80 to the controller.

Port forwarding is configured from the router's utility interface, which can be accessed by browsing to the router's IP address. Different routers have different interfaces, so it is recommended that you consult the documentation for your router.

Optional Port Forwarding

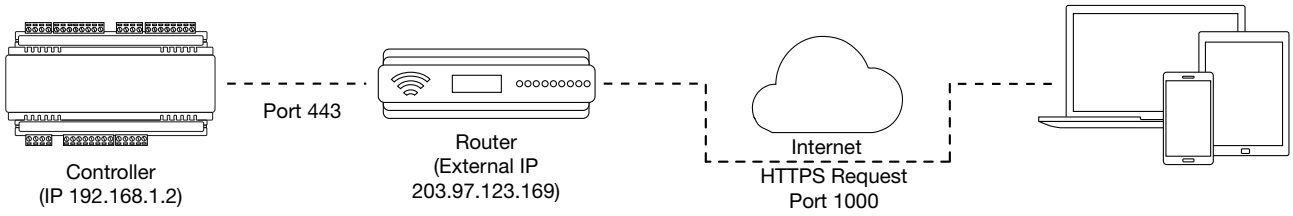
After you have installed a certificate and established an HTTPS connection to the controller, you may wish to continue accessing the controller over the internet. To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed if necessary in the **System Settings** (available once **Use HTTPS** is enabled).

The easiest method is to configure the router to forward all traffic from **external port 443** (the default HTTPS port) to the controller's internal HTTPS port, as in the image below.



In this case, all traffic directed to the external HTTPS IP address will be forwarded to the controller. The controller's web interface could be accessed by typing https://203.97.123.169 into an external web browser.

However, it is possible to grant external access by forwarding any external port to the controller's HTTPS port. This is especially useful if external port 443 is not available on your network.



In this case, any traffic directed to **external port 1000** will be forwarded to the controller's HTTPS port. The controller's web interface can be accessed simply by appending the external port number onto the end of the URL: e.g. https://203.97.123.169:1000.

Note: If the controller does not have a factory loaded certificate, it will not be accessible via HTTPS until an HTTPS certificate has been installed, regardless of whether port forwarding has been configured.

Controller Default Gateway

In order for the controller to send and receive external communications via the router, its default gateway needs to be set to the router's **internal** IP address.

1. Log in to the controller's web interface.
2. Navigate to the **System Settings | Adaptor - Onboard Ethernet** tab.
3. In the **Default Gateway** field, enter the IP address of the router.
4. **Save** the configuration and **Restart** the controller.

Note: The default gateway must be set to the router's internal IP address that identifies it on the local internal network, not the external IP address used to connect over the internet.

Mapping an IP Address to a Domain

In order to achieve third-party HTTPS certification, it is necessary to map the controller's externally accessible IP address to a domain. The domain name becomes the **hostname** for the controller: a fixed, human readable point of access to the device.

Domain names can be purchased from Domain Name Registrars and assigned to a **static IP address**, usually for an annual fee. For example, the IP address 203.97.123.169 could be assigned the domain name controller.com, and would then be accessible by typing that domain name into a browser address bar.

However, typically routers are assigned a **dynamic IP address**. This IP address is not static: internet service providers may reassign the address whenever the router is reset or even more frequently. A fixed domain name would have to be constantly monitored and updated, as the IP address it is mapped to will change unpredictably. If necessary, a **static IP address** may be purchased from your internet service provider.

Alternatively, you may use a **Dynamic Domain Name Server (DDNS)**, which allows a dynamic IP address to be mapped to a static domain name. Generally a DDNS service will provide a client application which runs on the web server PC and automatically updates the domain's IP address mapping whenever the external IP address changes. Controllers also have an **integrated DDNS client** which supports several free DDNS providers.

Third-Party Certificate

This method uses a certificate generated by a recognized third-party certificate authority (CA) to encrypt the HTTPS connection. Unlike the self-signed certificate method, third-party certificates generally require an annual fee; however, they are trusted by web browsers.

The process has five main stages:

1. The installer generates a private/public encryption key pair and certificate signing request for their domain.
2. The installer submits the certificate signing request to the certificate authority.
3. The certificate authority provides a validation file which is loaded onto the controller.
4. The certificate authority validates the domain and provides the certificate.
5. Finally, the installer converts the certificate format (if necessary) and installs the certificate onto the controller.

Requirements for Third-Party Certificates

- The controller must be exposed to the internet via external port 80.
- The controller must be externally accessible via a hostname.

  Either static IP or DDNS (see page 19) can be used to assign this hostname.

- The operator must renew the certificate whenever it expires.
- Different certificate authorities may have different requirements. For example, some CAs do not require manual validation of domain names, allowing you to skip the certificate authentication stage. It is recommended that you carefully note all requirements for your chosen CA before beginning.

If you need help when obtaining and loading a third-party certificate, consult your IT support. ICT Technical Support cannot assist with this process.

Creating a Private Key and Certificate Signing Request

To begin, it is necessary to generate the private/public encryption key pair which will be the basis for the HTTPS encryption. The public key will be integrated into a certificate signing request which will be submitted to the CA.

The following instructions will use the free OpenSSL utility. The latest version of OpenSSL for Windows can be downloaded from this page.

1. Download and install the OpenSSL utility.
2. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
3. To **generate the key pair**, enter the following command, replacing `[name]` with your desired filenames:

   ```
   req -newkey rsa:2048 -keyout [name].key -out [name].csr
   ```

   This generates a new 2048-bit private key (.key file) and certificate signing request (.csr file). The files should appear in the current OpenSSL directory.
4. Enter a **passphrase** for the private key. This is a phrase used to encrypt the private key to protect it against anyone with access to your local system. It will be required whenever the private key is used.

   Note that passphrase characters will not be displayed in the console. Only alphanumeric characters are supported for the passphrase.

5. Enter your **location and identity information** as requested. These details will be incorporated into your certificate and publicly viewable from the web browser.

   Ensure that the **Common Name** is the same as the **Domain Name** which is being used for the controller.

   Some details are optional. Confirm with your CA which fields are required.

6. **Save** both files in a safe, known location, as both are required for the following steps. It is especially important that the private key is not publicly accessible.

Purchasing a Certificate

Below are very basic instructions for purchasing a third-party certificate from a CA. Every CA will have different processes and requirements - this is only intended to be a rough guide to what is required for implementation on a controller.

1. Begin the process of generating a certificate from a recognized CA such as:
   - **GoDaddy**: https://nz.godaddy.com/web-security/ssl-certificate
   - **Network Solutions**: https://www.networksolutions.com/
   - **RapidSSL**: https://www.rapidsslonline.com/

   It is important that you select **File-Based or HTTP-based Validation** (or equivalent) when asked to choose an authentication/validation method. You will require a .txt file to upload to the controller.
2. When prompted, upload the text of your **Certificate Signing Request** (.csr).
3. Follow the CA's instructions to complete the request. You should be prompted to download a **.txt** validation file.

   DO NOT change the name or contents of this file.

Authenticating the Certificate

The .txt file that you received in the previous steps must be uploaded to a known directory on your domain (in this case, the controller) so that it can be viewed by the CA. This verifies that you are the owner of the domain in question.

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**.
3. In the **General** tab, select the **Use HTTPS** checkbox (if not already enabled).
4. Enter an appropriate **HTTPS Port**. The default is port 443, which is commonly used for this purpose. You should retain the default port unless you are required to use another port by your system administrator.
5. Click **Load Validation File** and browse to the .txt validation file to load it onto the controller.
6. Open the **Adaptor - Onboard Ethernet** tab. Enter the controller's domain name in the **Controller Hostname** field.
7. Confirm that the file is publicly accessible by using another machine to navigate to [domainname]/.wellknown/pki-validation/[filename].txt. You should be able to view the content of your validation file.

Once the CA has verified that your domain is accessible, you will be sent the signed certificate. Wait times can vary between providers, but will typically take from one hour to several hours.

Converting the Certificate Format

The controller requires a file with the .pfx extension. Your CA may have provided a different file type, potentially several files such as a certificate (e.g. .cer, .crt or .pem) and an intermediate certificate. These must be combined with the private key generated with your certificate request to create a .pfx file. The following instructions will use the OpenSSL utility installed above.

1. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
2. **Export** your certificate as a .pfx file using the following command, replacing `[name]` with your filenames:

   ```
   pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -nomac -out
   [name].pfx -inkey [name].key -in [name].[cer/crt/pem]
   ```

   Replace `[cer/crt/pem]` with the extension on your certificate file as required.

   Note: If you have been provided with an intermediate certificate you **must** include intermediate certificates by appending to the end of the command: `-certfile [intermediatename].[cer/crt/pem]` as shown below.

   ```
   pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -nomac -out
   [name].pfx -inkey [name].key -in [name].[cer/crt/pem] -certfile
   [intermediatename].[cer/crt/pem]
   ```

   Android devices will fail to connect if intermediate certificates are not included in the certificate loaded onto the device.

3. Enter the **passphrase** for the private key (set above) to continue.

   Note that passphrase characters will not be displayed in the console.

4. Enter an **export password** when requested. This will be required when installing the certificate on the controller.
5. This process will generate a [name].pfx file in the current OpenSSL directory. This is your third-party certificate. Store this file in a safe, known location.

Installing the Certificate on the Controller

1. Log in to the controller's web interface and navigate to the **System Settings**.
2. Scroll to the **Certificate File** section. Click **Install Certificate** and browse to the .pfx certificate file to install it on the controller.
3. Enter the **export password** that you created when generating the certificate file.
4. Click **Save**, then **restart the controller** using the button on the top right to implement the new settings.

   Once the restart process is complete, the controller will restart but the web page will not automatically refresh.

5. Browse to the controller web page by adding the prefix https:// to the beginning of the IP address or URL.

A lock or similar icon in the browser toolbar should indicate that the connection is secure. Click on this icon to see details about the certificate, including the information you entered in the certificate signing request.

Self-Signed Certificate

Self-signed certificates do not require the certificate to be validated by an authority, or for the controller to be accessible over the internet. They can also be created for free. However, self-signed certificates are not considered secure by web browsers, which will generate warnings whenever the web interface is accessed. This method is fine for testing and development but is **not recommended** for live sites.

Requirements for Self-Signed Certificates

- There is no requirement for the controller to be externally accessible.
- The operator must manually renew the certificate whenever it expires.

Generating a Self-Signed Certificate with OpenSSL

The following instructions will use the free OpenSSL utility. The latest version of OpenSSL for Windows can be downloaded from this page.

1. Download and install the OpenSSL utility.
2. Navigate to the installation directory, open the **bin** folder, locate the **openssl** executable and run it as an administrator. This will open the OpenSSL command prompt.
3. To **generate** your certificate, enter the following command:

   ```
   req -new -newkey rsa:2048 -x509 -sha256 -subj "/C=[Country code]/CN=
   [Common name]" -days 365 -out [name].crt -keyout [name].key
   ```

   - Replace `[name]` with your desired filenames
   - The country code is optional, but recommended best practice. You can find your country code here.
   - The common name is typically in the form [hostname].[domain name]. For a self-signed certificate this does not need to be an externally accessible hostname. For example, you could use secure.controller.com.

   This generates a new key pair (.crt certificate and .key private key) with 2048-bit encryption that will expire after 365 days. The files should appear in the current OpenSSL directory.
4. Enter a **passphrase** for the private key. This is a phrase used to encrypt the private key to protect it against anyone with access to your local system. It will be required whenever the private key is used.

   Note that passphrase characters will not be displayed in the console. Only alphanumeric characters are supported for the passphrase.
5. Enter your **location and identity information** as requested. These details will be incorporated into your certificate and publicly viewable from the web browser.

   Ensure that the **Common Name** is the same as the **Domain Name** which is being used for the controller, if any.
6. To **export** your certificate, enter the following command, replacing `[name]` with your desired filename:

   ```
   pkcs12 -export -certpbe PBE-SHA1-3DES -keypbe PBE-SHA1-3DES -nomac -out
   [name].pfx -inkey [name].key -in [name].crt
   ```
7. Enter the **passphrase** assigned above when prompted.
8. Create an **export password** when prompted. This will be required when installing the certificate on the controller.

   This process will generate a [name].pfx file in the current OpenSSL directory. This is your self-signed certificate. Store this file in a safe, known location.

Installing the Self-Signed Certificate to the Controller

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**.
3. In the **General** tab, select the **Use HTTPS** checkbox (if not already enabled).

4. Enter an appropriate **HTTPS Port**. The default is port 443, which is commonly used for this purpose. You should retain the default port unless you are required to use another port by your system administrator.
5. Click **Install Certificate** and browse to the .pfx certificate file to install it on the controller.

   No .txt validation file is required for this method, as the connection is not validated by a third party.

6. Enter the **export password** that you created when generating the certificate file.
7. Click **Save**, then **restart the controller** using the button on the top right to implement the new settings.

   Once the restart process is complete, the controller will restart but the web page will not automatically refresh.

8. Browse to the controller web page by adding the prefix https:// to the beginning of the IP address or URL.

When using a self-signed certificate, you will likely be presented with a security warning if you attempt to access the HTTPS web page. The connection is still encrypted, but the browser has flagged the certificate as untrustworthy as it lacks third-party validation.

Basic Programming

This section outlines the use of the Protege WX wizards and other basic programming steps to get you started using your system.

Understanding the Defaults

To simplify things and make programming your site as easy as possible, Protege WX includes a number of default settings. These can be used 'as is' for quick and simple deployment, or adapted to suit your needs. Either way, it helps if you understand what the defaults are and what they do. You'll find the names describe them pretty well.

Users

You'll find three users by default: Installer, Master, and User (Demo). There are also three access levels that determine what users can do in the system, and three menu groups each providing different levels of control:

User	PIN Code	Description/Purpose
Installer	000000	Assigned the Installer access level and Installer menu group, this user has full access to program the system via a keypad, but no area control or door access.
Master	123456	Assigned the Master access level and All Menus menu group, this is a power user with access to all areas and doors. They have complete control from a keypad with the exception of the Installer menus.
User (Demo)	111111	Assigned the Users access level and User menu group, this is a typical staff member/end user, with access to all areas, but with no doors or door groups configured yet. Keypad control (via the menu group), allows basic control over the system for arming/disarming.

Schedules

There are schedules for Work Hours, After Hours, and Break Hours. These can be edited as required, and used to enable a function or access level to operate only within certain scheduled periods. They can be used to control when a user can gain access to things, to unlock doors automatically, to arm or disarm areas at certain times or days, and to turn thing on and off or change the way they behave at certain times of day.

Inputs, Outputs, and Trouble Inputs

Inputs, Outputs, and Trouble Inputs for the Controller are included by default. Others are added automatically when you add an Expander module using the wizard. For example, adding a Reader Expander will add the inputs, outputs and trouble inputs for that module. These are then configured using the wizard.

Door Types and Input Types

The Door types - Card Only, Card and PIN, Card or PIN, PIN Only - are used to define how a door will operate and when the entry mode is valid. Use these as they are or create your own door types to allow different modes of control over the method a user has to access a door. For example, you can create a door type that allows card only access between standard office hours of 8am and 5pm, but requires both card and pin outside these hours for added security.

Input Types define how an input will operate in an area. For example, Delay will go into entry delay when triggered, whereas Instant will activate immediately. There are a range of predefined input types included by default. In most cases these will be enough, but you can modify them as needed or create your own to suit your requirements. The four most commonly used input types are:

- Instant: Activates an armed area immediately when input opens
- Delay: Activates entry delay when input opens

- Trouble Silent: Used for system trouble inputs. Generates an alarm without the Bell
- 24 Hour Alarm: Used for panic inputs. Generates an alarm even when area is disarmed

Using the Protege WX Wizards

Once logged in, the Home Page is displayed. Select the **Wizards** menu at the top of the page to run through each of the wizards that will guide you through the initial setup, giving you a fully functional access control and intrusion detection solution in no time.

1. Expanders Wizard
2. Access Control Wizard
3. Security Wizard
4. Users Wizard

Expanders

The Expanders Wizard is used to detect and add the connected expander modules to the system, and add their corresponding inputs, outputs and trouble inputs.

1. Ensure the modules are connected to the network and that the LED indicators show the module address is too high. The Fault light should be constantly on and Status light should be flashing three times in quick succession.
2. Click **Step 2- Auto Detection** to continue. The wizard automatically detects the modules and displays them.

   Each module is assigned a name automatically. These can be renamed as required to provide a more meaningful name for easier identification.
3. Click **Step 3- Additional Modules** to continue. If required, add additional modules for any hardware not yet connected.
4. Click **Save and Return to Menu** to finish.

Progress is shown as the Controller is programmed and the corresponding inputs, outputs and trouble inputs are created. Once complete, you are returned to the Home page.

Access Control

The Access Control Wizard detects the available reader ports and creates the doors. It also enables you to assign an unlock schedule to each door to determine when the door will unlock. For example, a typical staff entry door may need to unlock at 8am and be locked again at 5pm. Use the Schedule Operates Late to Open (see page 64) option to prevent the door unlocking on schedule until the first user accesses the door. You can use the default Work Hours schedule which you can adapt to suit your needs later, or create your own schedules (see page 35).

1. The wizard automatically detects the reader ports.
2. Use the **Rename** button to assign your own door names and adjust the **Reader Location** as required.
3. Click **Save and Continue** to proceed to step 2.
4. Select the Unlock Schedule if required then click **Save and Return to Menu**.

Progress is shown as the Doors are created. Once finished, you are returned to the Home page.

Security

The Security Wizard allows you to configure the Areas in your system, the Inputs that are used to trigger events, and set up basic offsite monitoring services.

This step disarms any areas that are currently armed, and will prompt you to confirm the action.

1. The wizard lists the placeholder area that is created by default which you can now edit to fit your needs. If you require additional areas create these first, or create and configure them later.

- Select the **Bell Output** and the **Bell Time**. This is the output that will be triggered when the area alarm is activated and the time it will be activated for. In most cases, this will be used to connect a siren
- Select the **Entry Delay Output** and the **Entry Delay Time**. This is the output that will be activated whenever the area goes into entry delay and the time users will be given to disarm the area before an alarm is triggered
- Select the **Exit Delay Output** and the **Exit Delay Time**. This is the output that will be activated whenever the area goes into exit delay and the time users will be given to exit the area before an alarm is triggered

2. Click **Save and Continue** to proceed to the next step. The wizard lists each of the Inputs in your system.
   - Rename each input to provide a more meaningful description for easier identification
   - Select the **End of Line Resistors** according to those used when wiring the EOL configuration
   - Select the **Input Type** to define how an input will operate in an area. For example, Delay will go into entry delay when triggered, whereas Instant will activate immediately
   - Select the **Area** the input is assigned to
3. Click **Save and Continue** to proceed and configure Offsite Monitoring. All modules will be restarted automatically.
4. If using PSTN Monitoring, enter the Dialer (Contact ID) information:
   - Enter the **Client Code** (or account number). This is the code used to identify the system at the monitoring station and will usually be issued by the monitoring company
   - Set the **Primary Phone Number** of the monitoring station
   - Set the **Backup Phone Number** of the monitoring station. This number will be dialed if a connection with the station cannot be made on the primary phone number
5. If using IP Reporting:
   - Enter the **Client Code** (or account number). This is the code used to identify the system at the monitoring station and will usually be issued by the monitoring company
   - Enter the **IP Address** and **IP Port Number** as supplied by your monitoring station
   - If the monitoring station has a backup path, enter the secondary **IP Address 2** and the Secondary **IP Port 2 Number** to be used if the first IP address fails
   - Select the **Reporting Protocol** to be used. This will usually be supplied by your monitoring station
   - If using an encrypted protocol, select the **Encryption Level** and the **Encryption Key** to be used
   - If required, adjust the **Poll Time**. One of the advantages of IP reporting is that essentially it is always 'on'. This is achieved by sending regular poll messages at the frequency set here. This defaults to 30 seconds, however your monitoring station may request a different setting
6. Click **Save and Return to Menu** to complete configuration and return to the setup menu.

Users

The Users Wizard enables you to quickly create new Users, and define which Areas and Doors they are able to access.

For each user, enter the name, PIN, and card details. Select the Area(s) and Door(s) you wish to grant them access to, then click **Add User**. Repeat until you have added all the users you need.

Configuring Additional Areas

Areas allow for the Protege system to be divided up into separate sections (alarm areas or partitions) that will be monitored for intrusion or other purposes.

There is one placeholder Area that is created by default which you can configure using the Security wizard to fit your needs. If you require additional areas you can either create these before running the wizard then use the wizard to configure them, or create and configure them later.

Creating an Area

1. Navigate to **Programming | Areas** and click **Add**.
2. Enter a **Name** for the area, then select the **Configuration** tab to set the timings, including entry and exit delays:
   - The **Entry Time** defines a delay period allowing any users that enter the area time to disarm it before the area generates an alarm
   - The **Exit Time** defines a delay period allowing users to exit the area once the arming of the area has begun before an alarm is triggered as a result of an input being activated.
   - The **Alarm Time** determines how long the bell/siren output for the area will remain activated before timing out.
   - If required, adjust the schedule and set the **Disarm Area When Schedule Starts** and **Arm Area When Schedule Ends** options to automatically disarm/arm the area when the schedule starts/ends.
3. Select the **Outputs** tab to define the outputs used by the area and how they behave when triggered:
   - The **Bell Output** determines the output that will be triggered when the area alarm is activated. In most cases, this will be used to connect a siren.
   - The **Exit Delay Output** and **Entry Delay Output** are activated whenever the area starts the exit or entry delay cycle. Using an audible output like a keypad beeper provides a distinctive warning to users to let them know the area has begun arming and they need to get out, or that the entry delay period has been triggered and they need to disarm the area before it generates an alarm.
   - The **Disarmed Output** and **Armed Output** are activated whenever the area completes the disarming or the arming cycle. Using an output such as a keypad LED provides a visual indication of the status of an area.
   - The **Pulse On Time** and **Pulse Off Time** allow you to configure the output to beep or flash when triggered. For example, you may set a keypad beeper to make short beeps for an exit delay, and a long continuous beep for entry delay.
4. Click **Save** to finish creating the area.

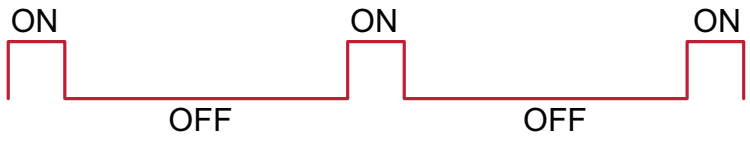
For a full list of the available properties and a description of what they do, refer to the Property Reference Guide (see page 47).

Pulse Times

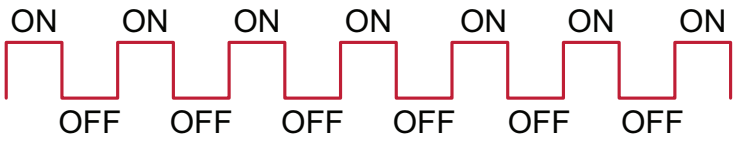
Pulse times allow an output or group of outputs to be pulsed for the duration of an area state. For example, the keypad beeper can be used to make short beeps for an exit delay, then a long continuous beep for entry delay.

Pulse times are measured in tenths of a second, or 100ms. A pulse time of 10 equates to 1 second.

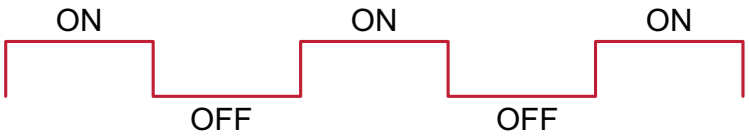
Setting the **Pulse On** to **1** and the **Pulse Off** to **9**, provides a short pulse (such as a short beep or flash) every second.



Setting both the Pulse On and Pulse Off values to **1** provides a rapid pulse on/pulse off.



Setting both values to **5** provides a slow, steady pulse on/pulse off.



- If the Pulse On and Off values are both set to zero (the default setting), the pulse is disabled and the output will remain on for the duration of the cycle time
- If Pulse On is given a value but Pulse Off is set to zero, the output will pulse (flash or beep) **once only**, then remain off

Configuring Schedules and Holidays

Schedules are defined timeframes that enable a function or access level to operate only within certain specified periods. They can be used to control when a user can gain access, unlock doors automatically, arm or disarm areas at certain times, turn devices on and off or change the way they behave at certain times of day. Schedules are central to automating access control and intrusion detection within the Protege system.

As schedules are commonly used to control access or secure areas it is a common requirement to have the schedule behave differently on a holiday. This is achieved by adding holiday groups which are then used to prevent (or allow) periods within a schedule to function during the holiday duration.

Once a schedule is programmed it will always be either valid or invalid. When it becomes valid, items that are programmed to depend on that schedule become active. For example:

- An access level will only grant access when its **operating schedule** is valid
- A door will unlock when its **unlock schedule** becomes valid
- An output will turn on when its **activation schedule** becomes valid

This section provides some useful programming tips for programming schedules effectively.

Creating Holiday Groups

Before creating a schedule, it is convenient to program one or more holiday groups that apply to it. These should include national, local and other holidays which might cause your site to operate differently - for example, a retail business might have shorter (or longer) hours on a public holiday.

There is no need to program weekends as holiday groups.

1. Navigate to **Scheduling | Holiday Groups** and click **Add**.
2. Enter a **Name** for the holiday group.
3. Select the **Holidays** tab and **Add** holidays to the group.
   - Enable the **Repeat** option for holidays that occur on the same day every year.
   - For holiday periods that span multiple days (such as Christmas Day and Boxing Day), define the start (first day) and end (last day) dates.
   - For holidays that fall on a different day each year (such as Easter), these need to be programmed for each annual occurrence as the dates do not repeat. However, by adding multiple entries you can program many years in advance.
4. Click **Save**. Once you have programmed your holiday group(s), they can be applied to your schedules.

Creating and Editing Schedules

1. Navigate to **Scheduling | Schedules**.
2. Click **Add** and enter a **Name** for the schedule, or select the schedule that you wish to edit.
3. Each schedule has multiple periods that can be programmed, which can be used for different days of the week or holidays. For each period, enter the start and end times that you wish the schedule to operate, and tick the boxes for the required days of the week.

   For more information, see Schedules and Multiple Time Spans (next page).

   Note how the **Graphics View** updates to show when the schedule will be valid.
4. For each period, select the **Holiday Mode** to define how the schedule will operate during a holiday period. Choose from:
   - **Disabled on Holiday**: When selected, the period will **not** make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule, it will not unlock on a holiday when this option is selected. This is the default mode of operation for schedules

- **Enabled on Holiday**: When selected, the period will only ever make the schedule valid **on** a holiday. For example, a user might have different access hours on a holiday compared to a normal day.
- **Ignore Holiday**: When selected, the period will make the schedule valid **regardless** of whether the day is a holiday or not. For example, the manager might be able to access the building at all times, holiday or not.

5. Select the **Holiday Groups** tab. Click **Add** and select the holiday groups you wish to apply to the schedule.

   This tells the schedule which days are holidays, but it does not tell the schedule what to do if it is a holiday. This is defined by the **Holiday Mode** above.

6. Click **Save** to finish creating your schedule.

Schedules and Multiple Time Spans

There may be times when schedules need to turn on and off more than once, or at different times on different days. Each schedule has 8 periods to allow for these scenarios.

Below are some examples of when you might use this.

Different Hours for Weekends

Premises may need to open for shorter (or longer) hours on a weekend.

To set this up, simply add a second period with shorter hours and select the relevant day(s).

Different Hours on a Holiday

In some installations, especially retail, a schedule must still operate on a holiday but may do so for shorter or longer hours.

To set this up, simply set up another period with the required days and times, and set the **Holiday mode** to Enabled on holiday.

Multiple Periods in a Single Day

Sometimes multiple periods are required in a single day. Consider a movie theater where there are multiple session times, so the doors must be unlocked during certain periods.

Set as many separate periods for the same day(s) as required.

Overnight Schedules

Where a schedule is required to operate overnight, enter a start time, but leave the end time as **12:00 AM**. This results in the period being valid from the start time until midnight.

Now program a second period to start at midnight and continue until the end of the shift. By extending the days that the period is valid, we can create an overnight Monday to Friday shift.

The graphics view is useful for providing a visual representation of when the schedule is valid.

Overlapping Periods

Where periods overlap, the schedule will take the sum of all periods.

Rules for Schedules and Holidays

If you program times and days into a schedule but don't do anything else, the schedule will **always** operate.

For a holiday to prevent the schedule from becoming valid, the following must have been programmed:

1. The holiday must be programmed in a holiday group.
2. That holiday group must be applied to the schedule in the **Holiday groups** tab.
3. The **Holiday mode** for the schedule period must be set to Disabled on holiday.

Monitoring Your System

The **All Events** page and **Status Lists** provide functions for monitoring your site.

The LED indicators on the Controller and Power Supply are useful for diagnosing faults and conditions.

Viewing Events

The All Events window provides a live and historic view of all events.

- Use the **Previous** and **Next** buttons to navigate through the pages
- Click **Live View** to return to the real time display

Status Lists

Status lists are accessed from the Monitoring menu and provide a real-time display of the devices configured within the system.

This Option:	Is Used To:
Doors	Display a list of all Doors and their current status. The Doors status list can also be used to view a list of recent events associated with the door.
Inputs	Display a list of all Inputs and their current status.
Areas	Display a list of all Areas and their current status. The Areas status list can also be used to view a list of recent events associated with the area.
Outputs	Display a list of all Outputs and their current status.
Trouble Inputs	Display a list of all Trouble Inputs and their current status.
Elevators*	Displays a list of all Elevators and their current status.
Schedules	Display a list of all Schedules and their current status.
Programmable Functions	Display a list of all Programmable Functions and their current status.
Services	Display a list of all Services and their current status.

Elevators only available in Advanced Mode (see page 11).

Each status list also enables you to manually control the items from the web interface. For example, you can use the Door Status List to lock and unlock doors, or use the Area Status List to arm and disarm areas.

Reporting

Reporting is accessed from the **Monitoring** menu and provides the option to configure, view and export reports from the Protege WX interface.

This Option:	Is Used To:
Event Reports	Configure, view and export event reports.
Central Monitoring Reports	Export report maps for the Contact ID and Report IP services.

Creating an Event Report

1. Navigate to **Monitoring | Reporting | Event Reports** and enter a **Name** for the report.

   A name is only required if you wish to save the report. If you simply wish to view events as they happen, entering a name is optional.

2. Enter a valid **Start Date** and **End Date**.
3. To include all events, simply click **Save**, **View** or **Export**.

   -or-

   To filter based on users, door and/or areas, use the additional tabs. A number of common reporting scenarios, and the filter criteria required, are outlined below.

   The limit on the number of records you can select is 1500. If you select more than this number of records and attempt to save the report you will see an error. Due to a known limitation it is not possible to remove excess records and save the report again; you will need to recreate the report from scratch.

4. Click **View** to display the relevant events.
5. Click **Export** to save the events in CSV format, enabling you to extract event data which can then be formatted and manipulated as required.

   Depending on your browser settings, you may be prompted to save the file. Otherwise, will be automatically downloaded automatically to your Downloads folder.

Common Reporting Scenarios

The following scenarios cover common reporting requirements and the options to select:

- To view the activity of a particular **user or users**, define a date/time range and select the relevant users.
- To view activity at a particular **door or doors**, define a date/time range and select the relevant doors.
- To determine whether a **specific user has gained access to a particular door**, define a date/time range and select the relevant user and door.
- To determine **which user has armed or disarmed an area**, define a date/time range and select the relevant area.
- To determine whether a **specific user has armed or disarmed a particular area**, define a date/time range and select the relevant user and area.

Exporting Central Station Reports

You'll often need to supply your offsite monitoring station with a Report Map. These maps can be easily exported from within Protege WX.

To export a Report Map

1. Navigate to **Monitoring | Reporting | Central Station Reports**.
2. Click **Export** for either of the two services to generate a CSV format report that can be forwarded to your monitoring station.

Depending on your browser settings you may be prompted to save the file, otherwise it is downloaded automatically to your Downloads folder.

LED Indicators

Protege DIN rail modules feature comprehensive diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

Controller

Power Indicator

The power indicator is lit when the correct input voltage is applied to the controller.

Note that this indicator may take several seconds to light up after power has been applied.

State	Description
On (green)	Correct input voltage applied
Off	Incorrect input voltage applied

Status Indicator

The status indicator displays the status of the controller.

State	Description
Flashing (green) at 1 second intervals	Controller is operating normally

Fault Indicator

The fault indicator is lit any time the controller is operating in a non-standard mode. During normal operation the fault indicator is off.

State	Description
Off	Controller is operating normally
On (red)	Controller is operating in a non-standard mode

Ethernet Link Indicator

The ethernet indicator shows the status of the ethernet connection.

State	Description
On (green)	Valid link with a hub, switch or direct connection to a personal computer detected
Flashing (green)	Data is being received or transmitted
Off	Ethernet cable not connected, no link detected

Modem Indicator

Modem model only.

The Modem indicator shows the status of the onboard modem.

State	Description
On (green)	Modem has control of telephone line
Off	Modem is not active

Reader Data Indicators

The R1 and R2 indicators display the status of the data being received by the onboard readers.

State	Description
Short flash (red)	A SHORT flash (<250 milliseconds) will show that data was received but was not in the correct format
Long flash (red)	A LONG flash (>1 second) indicates that the unit has read the data and the format was correct

Bell Indicator

The Bell indicator shows the status of the bell output and the over current or circuit fault conditions.

State	Description
Off	Bell is connected, output is OFF
On (green)	Bell is ON
Single flash (green)	Bell is ON, the circuit is in over current protection
Two flashes (green)	Bell is OFF, the circuit to the siren/bell is cut, damaged or tampered

Relay Indicators

The relay indicators show the status of the lock output relays.

State	Description
Constantly on (red)	Relay output is ON
Constantly off	Relay output is OFF

Input Indicators

Whenever an input on the module is programmed with an input type and area, the input status will be displayed on the front panel indicator corresponding to the physical input number. This allows for easy test verification of inputs without the need to view the inputs from the keypad or the Protege software.

State	Description
Constantly off	Input is not programmed
Constantly on (red)	Input is in an open state
Constantly on (green)	Input is in a closed state
Continuous flash (red)	Input is in a tamper state
Continuous flash (green)	Input is in a short state

Power Supply (4 Amp)

Power Indicator

The power indicator is lit whenever the correct module input voltage is applied across the mains input terminals.

State	Description
Constantly on	Correct module input voltage applied
Constantly off	Incorrect module input voltage applied

Status Indicator

The status indicator displays the module status.

State	Description
Fast flash (green)	Module attempting registration with controller
Slow flash (green)	Module successfully registered with controller
Flashing (red)	Module communications activity

When the fault and status indicators are flashing alternately, the module is in identification mode, enabling the installer to easily identify the module in question. Upon either a module update or the identification time period expiring, the module will return to normal operation.

Fault Indicator

The fault indicator is lit any time the module is operating in non-standard mode. If the fault indicator is flashing, the module requires a firmware update or is in firmware update mode. When the fault indicator is on, the status indicator will flash an error code.

State	Description
Continuous slow flash (red)	Module is in boot mode awaiting firmware update
Constantly on (red)	Module is in error state and will flash an error code with the status indicator

V1 Output/V2 Output Indicators

The V1 and V2 output indicators show the status of the 12VDC output.

State	Description
On (green)	12VDC output operating OK
Flashing (red)	12VDC output failure

Battery Indicator

The battery indicator shows the status of the backup battery.

State	Description (with mains power connected - power indicator on)
Flashing (red)	Backup battery is disconnected
On (red)	Backup battery failed its dynamic battery test
On (green)	Last backup battery dynamic test successful
State	**Description (with mains power disconnected - power indicator off)**
Flashing (red)	Mains has failed and the PSU is drawing power from the battery. State is Battery Low
Flashing (green)	Mains has failed and the PSU is drawing power from the battery. State is Battery Restore

Temp Indicator

The temp indicator shows the status of the unit's core temperature.

State	Description
On (red)	Core temperature exceeded. **Over Temp Shutdown Activated**
Flashing (red)	Core temperature within 10°C of Over Temp Shutdown
On (green)	Core temperature OK

Output Current Indicator

The output current indicator shows the status of the output current for both V1+ and V2+.

State	Description
Constantly on	Output current exceeded. **Over Current Shutdown Activated**
Continuous flash	Output current exceeded maximum, approaching Over Current Shutdown
Constantly on (all indicators)	Maximum output current level reached
Constantly on (partial)	Indicated output current level reached

Power Supply (2 Amp)

Power Indicator

The power indicator is lit whenever the correct module input voltage is applied across the low voltage AC input terminals.

State	Description
Constantly on	Correct module input voltage applied
Constantly off	Incorrect module input voltage applied

Status Indicator

The status indicator displays the module status.

State	Description
Fast flash (green)	Module attempting registration with controller
Slow flash (green)	Module successfully registered with controller
Flashing (red)	Module communications activity

When the fault and status indicators are flashing alternately, the module is in identification mode, enabling the installer to easily identify the module in question. Upon either a module update or the identification time period expiring, the module will return to normal operation.

Fault Indicator

The fault indicator is lit any time the module is operating in non-standard mode. If the fault indicator is flashing, the module requires a firmware update or is in firmware update mode. When the fault indicator is on, the status indicator will flash an error code.

State	Description
Continuous slow flash (red)	Module is in boot mode awaiting firmware update
Constantly on (red)	Module is in error state and will flash an error code with the status indicator

V1 Output/V2 Output Indicators

The V1 output and V2 output indicators shows the status of the 12VDC output.

State	Description
Constantly on	12VDC output operating OK
Constantly off	12VDC output failure

Battery Indicator

The battery indicator shows the status of the backup battery.

State	Description (with mains power connected - power indicator on)
Flashing (red)	Backup battery is disconnected
On (red)	Backup battery failed its dynamic battery test
On (green)	Last backup battery dynamic test successful
State	**Description (with mains power disconnected - power indicator off)**
Flashing (red)	Mains has failed and the PSU is drawing power from the battery. State is Battery Low
Flashing (green)	Mains has failed and the PSU is drawing power from the battery. State is Battery Restore

Temp Indicator

The temp indicator will show the status of the unit's core temperature.

State	Description
On (red)	Core temperature exceeded. **Over Temp Shutdown Activated**
Flashing (red)	Core temperature within 15˚C of over temp shutdown
On (green)	Core temperature OK

Over Current Indicator

The over current indicator will show the status of the output current for both V1+ and V2+.

State	Description
On (red)	Output current exceeded. **Over Current Shutdown Activated**
Off	Maximum output current not exceeded

Error Code Display

The following table is only valid if the **fault** indicator is constantly on and the **status** indicator is flashing red.

If the fault indicator is flashing the module requires a firmware update or is currently in firmware update mode.

The status indicator will flash red with the error code number. The error code number is shown with a 250ms on and off period (duty cycle) with a delay of 1.5 seconds between each display cycle.

Flash	Error Description
1	**Unknown Error Code** The error code returned by the system controller could not be understood by the module.
2	**Firmware Version** The firmware version on the module is not compatible with the system controller. To clear this error, update the module using the module update feature in the controller's web interface.
3	**Address Too High** The module address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the module by disconnecting the power.
4	**Address In Use** The address is already in use by another module. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.
5	**Controller Secured Registration Not Allowed** The controller is not accepting any module registrations. To allow module registrations use the network secure command to change the setting to not secured.
6	**Serial Number Fault** The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	**Locked Device** The module or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

Trouble Inputs

Trouble inputs are used to monitor the status of the controller and in most cases are not physically connected to an external input. These can then be used to report a message to a monitoring station, remote computer, keypad or siren.

The following lists the trouble inputs that are configured in the controller:

Input Number	Description
CP001:02	12V Supply Failure
CP001:04	Real Time Clock Not Set
CP001:05	Service Test Report
CP001:06	ContactID Reporting Failure
CP001:07	Phone Line Fault
CP001:08	Auxiliary Fuse / Supply Fault
CP001:09	Bell Siren Tamper / Cut
CP001:11	Bell Siren Current Overload
CP001:13	Module Communication Fault
CP001:14	Module Security Violation
CP001:20	Report IP Reporting Failure
CP001:24	Installer Logged In
CP001:29	System Restarted
CP001:30	PoE Connection Lost (legacy PoE model only)
CP001:31	Output Over-Current Failure (legacy PoE model only)

Property Reference Guide

The following sections describe the properties available when programming your system, and what they do. Each section represents a menu selection within the web interface, and the relevant options available.

Certain options are only available in Advanced Mode. These are indicated with an asterisk [*] in the following section.

Users Menu

The Users menu contains the various functions for working with and configuring users (sometimes referred to as cardholders), and defining the access they have within a site.

This Option:	Is Used To:
Users	Add and manage users into the system with access credentials
Access Levels	Configure the access levels that will be assigned to users and determine what they can do within the system

Users

A user is a person programmed into the system with access control and alarm credentials. The user is then assigned access to programmed doors and functions of the system.

General

- **First Name:** The first name of the user
- **Last Name:** The last name of the user
- **Display Name:** The display name of the user as it appears on LCD and touchscreen keypads. This field prefills automatically based on the first/last names entered, but is limited to 16 characters and can be edited as required.
- **Reporting ID**: The code by which the user is reported to a monitoring station. ContactID, SIA, and ReportIP use this code.
- **Default Language**: Defines the language that applies to the user. Choose from English, Francais, Espanol, Estonian, or Italiano.
- **Database ID**: The unique ID used to identify the user when programming items from a touchscreen
- **Phone Extension**: If an entry station is integrated with the Protege WX system, users' phone extensions can be extracted if entered in this field.
- **Company Name:** The company name associated with the user

Access Cards

- **PIN Code:** Security PIN code the user logs on with
- **Facility/Card Number:** The security card and facility number for the user. Each user can have up to 8 facility/card codes.
- **Add Card From Reader**: Opens a new dialog window that picks up any raw card data recorded by the system (once the window has opened). Apply the card information (once displayed) to the user.

Start / End Times

- **Start Date:** Optional setting enabling you to set a start date for the user. For example, for an employee who starts work on a specific date
- **Expiry Date:** Optional setting enabling you to set an expiry date for the user. For example, for a contractor who finishes work on a specific date

Areas

- **User Area:** Optional setting enabling you to set an area for the user

Users | Credentials

When a credential type is added it is automatically available to apply to every user. To assign the credential, enter the user's unique details.

From this section, you can enable/disable credential types for users and manually enter the relevant data.

Choose the credential type and enter the credential details.

Users | Search

Provides operators with a quick way to find users within the system based on fields such as Display Name, Reporting ID, Default Language or PIN.

- The Export button provides an easy way of exporting a list of all users and their programming. The exported CSV file can be opened in an Excel spreadsheet or similar

Users | Access

Define the access level(s) for the user. When the user performs an action the system checks the access level(s) to ensure the user has the relevant permissions to perform the action.

1. Click **Add** to open the Select Record window.
2. Select the relevant Access Level(s) and click **OK**. Insert relevant dates.
3. If required, you can set a schedule for the access level. By default, the schedule is set to Always, meaning the user can use the access level based on the access level's own operating schedule. Assigning another schedule restricts the usage of the access to the period set by the schedule.

Users | Options

General Options

- **Disable User**: When selected the user record is disabled, preventing access via keypad or card reader.
- **Show A Greeting Message To User:** When enabled the user is shown a greeting upon entering their code on a LCD user station (for example, Good Morning John Smith). Disabling this option takes the user to the area control menu or directly to the main menu. This setting can be overridden by the same option in the users menu group assigned to the access level of the user.
- **Go Directly To The Menu On Login:** When enabled the user is taken directly to the main menu and not shown the area control functions. Display of the area control is by default. Enable this option for users who won't normally perform area operations on the keypad.
- **User Can Acknowledge Alarm Memory:** When enabled the user is able to acknowledge alarm memory. Alarm memory is stored for each area and will record the last 4 activations. The alarm memory can be viewed from MENU 5 on the keypad and must be enabled to allow acknowledgment to occur. This setting can be overridden by the same option in the menu group.
- **Show Alarm Memory On Login:** When enabled the user is shown upon login the memory of any alarms that have occurred on the primary area that the keypad is assigned. This option can be overridden by the same option in the menu group.
- **Turn Off The Primary Area If User Has Access On Login:** When enabled the primary area for the keypad that the user logs into will be disarmed automatically.
- **Turn Off The User Area On Login If User Has Access**: When enabled the area that is programmed in the user's global area will be turned off when the user logs in to a keypad.
- **Acknowledge System Troubles:** When enabled the user is able to acknowledge system trouble conditions from the view menu (MENU 5) on the LCD keypad.
- **Treat User PIN+1 As Duress:** When enabled the user can enter a duress code, allowing access but sending a silent alarm to the offsite monitoring station. The duress code is the last digit of a user's PIN plus 1. For example, if the user's PIN is 1234 but the PIN is entered as 1235, it will be processed as a duress code. (Note that

the plus 1 counter applies to the **last** digit only. This means if the user PIN is 1239, the PIN to trigger a duress code would be entered as 1230.)

Advanced Options

- **User Has Super Rights And Can Override Antipassback:** When enabled the user is deemed to be a super user, allowing them to override dual code functions and Antipassback violations, and unlock doors in a lockdown situation.
- **User Operates Extended Door Access Function:** When enabled door access time is extended, say for entry by people with disabilities.
- **User Loiter Expiry Count Enabled*:** When enabled the user is included in the loiter area timing calculations. This means the user is allowed access for the period of loiter time set for the area they have entered. The areas used for the loiter time must be configured as loiter area and used as the inside and outside areas for the door. This is an administrative setting and should be edited only by the system administrator.
- **User Can Edit User Settings from Keypad:** When enabled the user can add new users, modify user settings and delete users, from a keypad. This should generally be enabled for system administration users only.

  When this option is enabled the user is not able to edit their own PIN code on the keypad, except when prompted due to an expired PIN.

  The user's access level menu group must have the **User (2)** menu enabled to access the keypad **User Menu**.
- **User Is A Duress User:** When enabled the user is a duress user and will activate the duress trouble input on a keypad and monitoring console. The duress trouble input must be enabled and programmed for the keypad.
- **Rearm Area In Stay Mode**: This option is used in conjunction with the User Rearm in Stay Mode option under Area programming. If both User and Area options are enabled, when the user disarms the area and once the rearm period has elapsed the area will automatically rearm in Stay mode.

Dual Custody Options

- **Dual Custody Master**: This option is used in conjunction with the Requires Dual Authentication option under the Door Types settings. If the door type requires dual authentication then two users must activate the reader for the door to unlock. The door can be set to require a Dual Custody Master first, then a Dual Custody Provider second, or it can be set to accept any combination of master and provider. This option defines the user as master.
- **Dual Custody Provider**: This option is used in conjunction with the Requires Dual Authentication option under the Door Types settings and defines the user as a provider. With this option enabled the user can access a Dual Custody door only if another user with Dual Custody Master enabled has activated the reader first.

Users | Events

Recent Events

- Shows a list of all recent events associated with the user

Access Levels

Access levels are assigned to users. When a user is assigned an access level that user is able to access the programmed options within the access level. The access level determines what they can do in the system and contains Alarm Areas, Doors, and Keypad Menus.

Configuration

- **Operating Schedule**: Determines when the access level is valid
- **Time to Activate Output (seconds)**: Defines the time the access level output is activated for. This option overrides the activation time programmed under the output.
- **Enable Multi-badge Arming:** Used in conjunction with the Reader Arming Mode (defined under Reader Expander settings) to enable a user to perform various operations when badging their card multiple times
- **Reader Access Activates Output:** When enabled the access level output will activate when a user with this access level presents a valid credential to a reader. For this option to work, the Activate Access Level Output option must be turned on for the reader used.
- **Keypad Access Activates Output:** When enabled the access level output will activate when a user with this access level enters a valid user code at a keypad. For this option to work, the Activate Access Level Output option must be turned on for the keypad used.
- **Activate Output Until Access Level Expiry**: When enabled the output will be activated for the duration of the access level expiry period as set in the user record.
- **Toggle Access Level Output**: When enabled the access level's output state will be toggled when access is granted.

  Note: Only one of **Activate Output Until Access Level Expiry** and **Toggle Access Level Output** may be selected. Checking one replaces the other.

Commands

- **Commands***: Used to send manual commands to a device.

Access Levels | Doors

Defines the Doors a user has access to, the direction a user can pass and the schedule used.

By default, the direction is set to Entry and Exit, meaning a user can pass through a door in both directions.

The schedule is set to Always by default, meaning access to the defined doors is permitted at all times. Assigning another schedule will restrict access to the door for the period set in the schedule. For example, limiting access to an office so it may only be entered during office hours.

Access Levels | Door Groups

Defines the Door Groups a user has access to, the direction a user can pass through the door, and the schedule used.

Include All Doors

- **Include All Doors**: Select this option to include ALL doors.

By default, the direction is set to Entry and Exit, allowing a user to pass through the defined doors in both directions.

The schedule is set to Always by default, meaning access to the defined doors is permitted at all times. Assigning another schedule will restrict access to doors within that group for the period set in the schedule. For example, limiting access to an office so it may only be entered during office hours.

Access Levels | Area Groups

In Advanced mode there are separate **Arming** and **Disarming Area Groups,** enabling differentiation between the areas a user is allowed to arm or disarm. In Basic Mode, there is a single option for area groups.

Defines the area groups a user is allowed to arm and disarm, and the schedule that is used.

Selecting the option **Include All Areas** means a user can arm/disarm all areas at all times. Assigning an Area Group and a schedule will restrict arming/disarming to the period set in the schedule.

Access Levels | Floors

This feature is only available in Advanced mode.

Defines the Floors a user has access to, and the schedule used.

By default, the schedule is set to Always, meaning access to the defined floors is permitted at all times. Assigning another schedule will restrict access to the floors for the period set in the schedule.

Access Levels | Floor Groups

This feature is only available in Advanced mode.

Defines the Floor Groups a user has access to, and the schedule used.

Include All Floors

- **Include All Floors**: Select this option to include ALL floors.

By default, the schedule is set to Always, meaning access to the defined floor group is permitted at all times. Assigning another schedule will restrict access to the floor group for the period set in the schedule.

Access Levels | Elevator Groups

This feature is only available in Advanced mode.

Defines the Elevator Groups a user has access to, and the schedule used.

Include All Elevators

- **Include All Elevators**: Select this option to include ALL elevators.

By default, the schedule is set to Always, meaning access to the defined elevator group is permitted at all times. Assigning another schedule will restrict access to the elevator group for the period set in the schedule.

Access Levels | Menu Groups

Defines the Menu Groups a user has access to. This determines what a user can do at a keypad.

Access Levels | Outputs

This feature is only available in Advanced mode.

Used with the Reader Access Activates Output / Keypad Access Activates Output options to define the output activated when a user with this access level presents a valid credential to a reader or enters a valid user code at a keypad.

Access Levels | Output Groups

This feature is only available in Advanced mode.

Used with the Reader Access Activates Output / Keypad Access Activates Output options to define the output group activated when a user with this access level presents a valid card to a card reader, or enters a valid user code at a keypad.

Credential Types

Credential Types is a licensed feature enabling the Protege WX system to use license plate, barcode, QR code, biometric and smart card data to identify users. Credential Types are created within Protege WX and applied to custom Door Types as the Entry or Exit Reading Mode. The third-party device or software used to collect the credential data is configured as a Smart Reader, with the data sent through to the controller via the onboard RS-485 reader ports or via Ethernet.

Configuration

- **Format**: The data sent to the Protege WX controller by the third-party device. Supported formats include:
  - **Unicode**: The credential data sent to the controller uses two bytes to represent each character as per the Unicode standard.
  - **UTF8**: The credential data sent to the controller uses a variable number of bytes to represent each character as per the UTF-8 standard.
  - **ASCII**: The credential data sent to the controller uses a single byte to represent each character as per the ASCII standard.
  - **Numeric**: The credential data sent to the controller is a binary number composed of up to 8 bytes. The bytes are ordered using little endian. The preceding, trailing and prefix character settings are ignored.
  - **Hexadecimal**: The credential data is sent to the controller as an array of binary numbers. When the specific credential is entered into the user programming for each user, the format used is hexadecimal with the numbers 0-9 and letters A-F representing each nibble of the credential.
  - **Wiegand**: The credential data sent to the controller is composed of a Wiegand bit stream.

    This bit stream can be encoded in numerous different ways and a format descriptor must be included in the **Wiegand or TLV Format** field. For the Wiegand format the preceding, trailing and prefix character settings and case sensitive setting are ignored.
- **Preceding Characters:** The maximum number of characters to be ignored at the start of the data packet being sent to the application.

  This setting is determined by the third-party device/application.
- **Trailing Characters:** The maximum number of characters to be ignored at the end of the data packet being sent to the application.

  This setting is determined by the third-party device/application.
- **Prefix:** The characters that are required at the start of the credential data packet sent to the controller.

  This setting is determined by the third-party device/application.
- **Case Sensitive**: Defines whether the data is case sensitive or not

User CSV Import

When importing users from a CSV file, there is currently no duplicate checking on the PIN and Card Numbers meaning it is possible to create users with conflicting numbers. We recommend checking the CSV file before import to ensure all numbers are unique.

The CSV Import feature enables the transferring of user data from an external source into Protege WX, automatically mapping the user information to the corresponding fields in Protege WX.

Only UTF-8 character set is supported in a CSV file.

Important:

The CSV file must be in the following format:

```
FirstName,LastName,FullName,Facility,Card,PIN,AccessLevel
```

The following rules apply:

- Each field must have a value, however the firstname/lastname can be omitted if the fullname is used and vice versa.
- The facility can be omitted **if** it is prepended to the card number and separated with a colon (e.g. 123:4567)
- If a matching Access Level is not found, a new access level is created.
- The PIN and card must be unique for each user.
- The file cannot contain a header row.

The following are valid examples:

```
Joe,Stanley,Joe Stanley,123,4587,1418,Warehouse Staff
Georgia,Smith,,123,4654,6884,Warehouse Staff
,,Billy Randall,123,4727,3492,Warehouse Staff
Frank,Powell,,,123:4639,3160,Warehouse Staff
```

To Import Users From a CSV File:

- Navigate to **Users | Users** and select the Import button.
- Browse to and select the CSV file you wish to import the users from, then click **OK.**
- The Users records are created and a message displayed to indicate the action was successful.

Monitoring Menu

Functions for monitoring a site are contained under the Monitoring menu.

This Option:	Is Used To:
Events	Display a live view of all events as they occur
Doors	Display a list of all doors and their current status
Inputs	Display a list of all inputs and their current status
Areas	Display a list of all areas and their current status
Outputs	Display a list of all outputs and their current status
Trouble Inputs	Display a list of all trouble inputs and their current status
Elevators*	Displays a list of all elevators and their current status
Schedules	Display a list of all schedules and their current status
Programmable Functions	Display a list of all programmable functions and their current status
Services	Display a list of all services and their current status
Reports	Allows the configuration, viewing and exporting of Event Reports as well as the exporting of Report Maps for the ContactID and ReportIP services

Reporting | Event Reports

Allows operators to create, view and export customized event reports based on users, doors and areas.

General

- **Name**: The report can be named if saving is required.

Start / End Times

- **Start Date**: A valid start date must be entered.
- **End Date**: A valid end date must be entered.

Reports can be viewed from within the Protege WX interface by clicking on the **View** icon, and exported in CSV format by clicking on the **Export** icon.

To generate a report showing **all** events that have occurred during the defined time period, do not enter any additional criteria under the users, doors and areas tabs.

Common Reporting Scenarios

The following scenarios cover common reporting requirements and the options to select:

- To view the activity of a particular **user or users**, define a date/time range and select the relevant users.
- To view activity at a particular **door or doors**, define a date/time range and select the relevant doors.
- To determine whether a **specific user has gained access to a particular door**, define a date/time range and select the relevant user and door.
- To determine **which user has armed or disarmed an area**, define a date/time range and select the relevant area.
- To determine whether a **specific user has armed or disarmed a particular area**, define a date/time range and select the relevant user and area.

Event Reports | Users

The limit on the number of records you can select is 1500. If you select more than this number of records and attempt to save the report, you will see an error. Due to a known issue, it is not possible to remove excess records and save the report again, so you will need to recreate the report from scratch.

Users

- Defines the users displayed in the report.

Event Reports | Doors

Doors

- Defines the door(s) displayed in the report.

Event Reports | Areas

Areas

- Defines the areas displayed in the report.

Reporting | Central Station Report

Central Station Reports (report maps) for the Contact ID and Report IP services can be exported from the Protege WX interface and supplied to the monitoring station.

Programming Menu

Functions for programming a site, such as configuring doors, areas, inputs, outputs, are all found under the Programming menu.

This Option:	Is Used To:
Doors	Configure doors to control user access or to monitor and control the flow of people into an area
Door Groups	Create and manage door groups that define which doors a user can access and/or control
Inputs	Configure inputs, such as motion detectors, door contacts and other protection devices
Door Types	Create and manage door types to define how a door operates
Input Types	Create and manage input types to define how an input operates in an area
Areas	Configure areas enabling the Protege WX system to be divided into separate sections (alarm areas or partitions)
Area Groups	Create area groups used to control the areas a user can arm and disarm
Outputs	Create and manage outputs to control devices from the Protege WX system, such as those that activate lighting or a siren, turn on an indicator, or unlock a door
Output Groups	Create output groups that group a number of outputs together and are used to control the outputs a user can activate and deactivate
Menu Groups	Create menu groups that determine which keypad functions those users have access to
Trouble Inputs	Configure the trouble inputs used to monitor the status and condition of the system
Elevators	Configure elevator cars to control user access or to monitor and control floors in a multi-storey high-rise building
Elevator Groups	Create elevator groups to control the elevators a user has access to
Floors	Define the floors on your system for use with elevator cars
Floor Groups	Create floor groups to control the floors a user has access to when accessing an elevator
Phone Numbers	Configure the phone numbers assigned to a service that communicates using a modem or telephone connection
Services	Create and manage services to provide interaction between Protege WX and external systems

Doors

To control access by users, or to monitor and control the flow of people into an area.

Setup

- **Door Type:** Door type selection allows the door to function in different modes. Each mode requires the user to present specific credentials, for example, a card, a card and PIN, a card or PIN, or PIN only. Different door types (requiring different security credentials) can be scheduled for different times of the day.
- **Slave Door**: You can assign another door record as a slave door. When a user unlocks the primary door, the slave door will be unlocked as well if the user has access to it. This might be used to control two adjacent doors with a single reader port.

  By default, slave doors will only follow the primary door when it is unlocked by access with a valid credential. To enable slave door operation for REX, REN and manual commands, add the `SlaveREX = true` in the **Commands** field for the primary door.

- **Area Inside Door:** The inside area defines which area is on the inside of the door. This is used to prevent a user from gaining access to a door when the area is armed and they cannot disarm it, as well as automatically disarming the area when the door is accessed. Using the door and area control integrates the two systems and is an ideal solution for false alarm prevention.
- **Area Outside Door:** The outside area defines which area is on the outside of the door. This is used to prevent a user from gaining access to a door when the area is armed and they cannot disarm it, as well as automatically disarming the area when the door is accessed. Using an inside and an outside area usually requires that the door is programmed with both an entry and exit reader.
- **Unlock Schedule:** The unlock schedule determines when the door unlocks. For example, if an employee entry door needs to be unlocked at 7am and locked at 5pm, assign a corresponding schedule. (Under Doors | Options tab, enable Schedule Operates Late To Open so door does not unlock on schedule until the first access has been accepted at the door.)
- **Door Pre-Alarm Delay Time:** The pre-alarm time is programmed to allow the door to be left open for a certain period before it will generate a pre-alarm condition. When the pre-alarm condition is reached this will typically activate an output on the reader expander that is controlling the door.
- **Door Left Open Alarm Time:** The maximum amount of time after a door opening event is generated before a door left open alarm is generated. This typically activates the appropriate trouble input and output on the reader expander that is controlling the door. For the trouble inputs to activate they must be set in the reader expander.

  Note: The pre-alarm delay time and door left open alarm time operate on a timeline. They do not specify the time period between state changes of the door. This means that as soon as the door is opened, a countdown starts for both the pre-alarm delay and the left open alarm time. For example, setting the Door Pre-Alarm Delay Time to 5 seconds and Door Left Open Alarm Time to 10 seconds, the door will go into pre-alarm after 5 seconds of the door being open, then a door alarm is generated after a further 5 seconds (10 seconds total). If the Door Pre-Alarm Delay Time is the same as or larger than the Door Left Open Alarm Time, the open door alarm will never be triggered.

- **Interlock Door Group***: The interlocking group is assigned to a door that cannot be opened or accessed when any of the doors assigned in the interlocking group are not secure. Access will be denied to the user based on an interlock.

Commands

- **Commands***: Used to send manual commands to a device.

Doors | Outputs

Lock Output:

- **Lock Output/Output Group:** Assign an output or output group to control the physical electric lock for the door. This is typically the lock control output on the reader expander used to control the door.
- **Lock Activation Time (seconds)**: The unlock time in seconds, i.e. the time that the lock output will be activated for when the door is unlocked. If additional lock outputs are being used this controls the activation time of the first lock output.

  Setting the activation time to 0 will cause the door state to toggle between locked and unlock latched when unlocked by a user or operator. However, the REX and REN functions are disabled.

  The maximum lock activation time is 128 seconds.

Pre-alarm Output:

- **Pre Alarm Output/Output Group:** Assign an output or output group to activate when the programmed pre-alarm time is reached. Use this to warn users that the door will generate an alarm if it is left open any longer.
- **Pre Alarm Pulse On/Off Time**: These fields are used to make the pre alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

Door Left Open Output:

- **Left Open Alarm Output/Output Group:** Assign an output or output group to activate when the programmed maximum open time is reached, indicating that the door has been left open. This tells users that the door must be closed immediately and that the system has generated an alarm.
- **Left Open Alarm Pulse On/Off Time**: These fields are used to make the left open alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

Door Forced Open Output:

- **Force Open Output/Output Group:** Assign an output or output group to activate when the door is forced open without any access. This feature activates a local output at the door indicating it has been forced. To generate an alarm on a forced door, use the forced door trouble input and assign this to an area so a report can be sent to a monitoring station or local control computer.
- **Force Open Pulse On/Off Time**: These fields are used to make the forced open output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

To configure a door forced delay, add the **`DoorForcedStateDelay = X`** command in the **Commands** field for the door, where **X** is the delay time in seconds.

Doors | Function Outputs

For more information and programming instructions, see Application Note 336: Programming Function Outputs in Protege GX and Protege WX.

- **Function 1-3 Output / Output Group**: This output or output group will be activated when the door is unlocked. Up to three function outputs can be programmed for each door, operating independently. These can be used to activate additional mechanisms or logic when the door is unlocked, such as bypass shunts or automatic door pumps.

  By default, the function outputs are activated for the set activation time when the door is unlocked by any method. The options below can modify this behavior.
- **Function 1-3 Activation Time**: The duration (in seconds) that the function output will be activated for when the door is unlocked. When the activation time is set to 0, the function output will be activated indefinitely.

  When the door is latch unlocked, the function output will be activated until the door is locked again. After the door is locked the function output will remain on for the programmed activation time, then will be deactivated.

  The maximum function output activation time is 128 seconds.

  This setting overrides the **Activation Time** set in the output programming.
- **Activate On Access**: When this option is enabled the function output will only be activated when the door is unlocked by access. It will not be activated when the door is unlocked by other methods such as schedule, area or programmable function.

  This option can be combined with **Activate On REX/REN** below.
- **Activate On REX/REN**: When this option is enabled the function output will only be activated when the door is unlocked by REX or REN. It will not be activated when the door is unlocked by other methods such as schedule, area or programmable function.

  This option can be combined with **Activate On Access** above.
- **Deactivate on Door Open**: When this option is enabled the function output will be deactivated immediately when the door is opened. If the door is not opened the output will still deactivate after the normal activation time.

  This feature does not operate while the door is latch unlocked.
- **Deactivate on Door Close**: When this option is enabled the function output will be deactivated immediately when the door is closed. If the door is not closed the output will still deactivate after the normal activation time.

  This feature does not operate while the door is latch unlocked.
- **Recycle Time on Access**: When this option is enabled, unlocking the door by access again when the function output is still on will reset the function output's activation time. This allows users to extend the time that the function output is activated.

  Activate On Access must be enabled to use this feature. In addition, you must enter the command **`RecycleDoorTimeOnAccess = true`** in the **General** tab.
- **Recycle Time on REX/REN**: When this option is enabled, unlocking the door by REX again when the function output is still on will reset the function output's activation time. This allows users to extend the time that the function output is activated.

  Activate On REX/REN must be enabled to use this feature. In addition, **Always Allow REX** and **Recycle REX Time** must be enabled in the **Inputs** tab.

Doors | Inputs

Door Input Options

- **Door Position Input**: Defines the input used for Door Position. When defined the reader sends door events when the door input is opened or closed.
- **Invert Door Input**: When enabled the door contact input is inverted. This does not affect the input functionality, if used. When disabled door contact functions normally.

REX Input Options

- **REX Input**: Defines the input used for the Request to Exit function. When set, the reader expander the door is linked to generates a request to exit event from the REX input. When disabled the reader expander does not generate any REX events.

  To enable a secondary REX input, add the command **`AltREX = #`** in the **Commands** field for the door, where **#** is the input's **Module Input** number. The secondary REX input operates using the extended REX time instead of the standard door lock time.

- **Invert REX Input**: When enabled the reader inverts the Request to Exit input. When disabled, REX input operates normally.

Bond Input Options

- **Bond Sense Input**: Defines the input used for the Bond Sense function. The magnetic bond sense is a contact indicating whether the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used, however the generation of door events should be processed using both inputs.
- **Invert Bond Input**: When enabled the reader inverts the bond sensing input. When disabled bond sensing operates normally.

REN Input Options

- **REN Input**: Defines the input used for the Request to Enter function. When set, the reader expander the door is linked to generates a request to enter from the REN input.
- **Invert REN Input**: When enabled the reader inverts the request to enter input. When disabled REN input operates normally.

Beam Input Options

- **Beam Input**: Defines the input used for beam control. Beam control allows the reader expander the door is linked to control an automatic gate, which must have its contacts held open even if the pathway is blocked.
- **Invert Beam Input**: When enabled the reader inverts the beam control input. When disabled the beam control input operates normally.

General Options

- **Always Allow REX:** When enabled the reader will always allow a Request to Exit event, even if the door is forced open. This will not restart the forced door or door alarm operation. When disabled REX input will operate only when the door is closed.
- **Recycle Door Open Time on REX:** When enabled the reader extends the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the Request to Exit once the door has been open too long requires the door to be closed. This option will not affect the ability of the Request to Exit action to unlock the door. When disabled REX input will not alter the door open time once the door has been opened.
- **Forced Door Sends Door Open:** When enabled the reader expander processes door forced open events as door open events. When disabled the reader will process forced door events as normal.

- **Recycle REX Time**: When enabled the door open time restarts, allowing the door to be held open and the REX pressed at each point the pre-alarm starts, silencing the pre-alarm and restarting the open timer. This allows a door to be held while furniture is being moved or to provide extended access for mobility users.
- **Maintain REX**: When enabled the door stays unlocked for as long as the REX button is held down.
- **Pulse Reader Beeper on REX**: When enabled the reader associated with the door produces a double beep when the REX button is pressed.
- **REX Time Different to Lock Time**: When enabled the REX Activation Time field appears, allowing for specification of duration for unlocking the door using the REX button. This overrides the time set for the Lock Activation Time (under Doors | Outputs).

Doors | Options

Door Options

- **Always Check Unlock Schedule**: Enabling this option causes the door to latch unlock when the **Unlock Schedule** is valid, and lock when the schedule is invalid. While the schedule is valid, if the door is locked by another function it will immediately unlock again. This prevents the door from being manually locked when it should be unlocked.

  You can use this option together with **Schedule Overrides Latch** to also prevent the door from being latch unlocked when the schedule is invalid.

  Using the **Prevent Unlock On Schedule If Inside Area / Outside Area Armed** options alongside this setting will prevent the door from unlocking while the schedule is valid, but does not relock the door when the area is armed. To achieve this use **Area Disarmed AND Schedule Valid Unlock Door** instead.
- **Enable Open/Close Events On Schedule:** When enabled the door will not log a door opened event when it is unlocked on schedule. This prevents the door from filling the event buffer with events that are not needed.
- **Relock On Door Close:** When enabled the door will lock when it detects a door close event and the lock output is activated.
- **Relock On Door Open:** When enabled the door lock will reactivate when the door sense detects the door is open.
- **Unlock Door On REX:** When enabled the door will activate the lock output when a request to exit occurs.
- **Unlock Door On REN:** When enabled the door will activate the lock when a request to enter occurs.
- **Schedule Operates Late To Open:** When enabled the door will not unlock on schedule until the first access has been accepted at the door.

Door Options 2

- **Door Lock Follows Inside Area:** When enabled the door will unlock if the inside area is disarmed. If no arm/disarm schedule is set the Area Disarmed OR Schedule Valid Unlock Door option MUST be enabled for this function to operate.
- **Door Lock Follows Outside Area:** When enabled the door will unlock if the outside area is disarmed. If no arm/disarm schedule is set the Area Disarmed OR Schedule Valid Unlock Door option MUST be enabled for this function to operate.
- **Prevent Slave Unlock On Inside Area**: When enabled the door will not activate the slave door if the inside area is armed.
- **Prevent Unlock On Schedule If Inside Area Armed:** When enabled the door will not unlock when the schedule is valid if the inside area is armed. Use this option with the late open option to prevent false alarms by entry of personnel before an area is disarmed. This option only operates if the Door Lock Follows Inside Area and Door Lock Follows Outside Area options are not enabled. To prevent unlocking and locking based on schedule and area status, set the Area Disarmed AND Schedule Valid Unlock Door and Area Disarmed OR Schedule Valid Unlock Door options to the required values.
- **Prevent Unlock On Schedule If Outside Area Armed:** When enabled the door will not unlock when the schedule is valid if the outside area is armed. Use this option with the late open option to prevent false alarms by entry of personnel before an area is disarmed.

- **Area Disarmed AND Schedule Valid Unlock Door:** When enabled the door will unlock if the door unlock schedule is valid AND the inside or outside area is disarmed dependent on the options set for Prevent Unlock On Schedule If Inside Area Armed and Prevent Unlock On Schedule If Outside Area Armed.
- **Area Disarmed OR Schedule Valid Unlock Door:** When enabled the door will unlock if the door unlock schedule is valid OR the inside or outside area is disarmed dependent on the options set for Prevent Unlock On Schedule If Inside Area Armed and Prevent Unlock On Schedule If Outside Area Armed.
- **Enable Access Taken On REX/REN Events:** When enabled the door will generate a Request to Exit (or Enter) event if the door opens while the door is unlocked from a request to exit. If the door remains closed, an Access Not Taken event is generated.

Doors | Advanced Options

Advanced Options

- **Update User Area When Passback Disabled:** When enabled the door will update the user's current area, even if the door is not programmed with card Antipassback. This can be used to keep track of the last area the user entered.
- **Lock Out REX When Inside Area Armed:** When enabled the door will deny a request to exit when the inside area has been armed to prevent egress from an armed area.
- **Deny Entry if Inside Area is Armed:** When enabled the door will deny entry if the inside area is armed.
- **Deny Exit if Outside Area is Armed:** When enabled the door will prevent any exit if the outside area is armed.
- **Disable Door Alarms on Schedule Unlock:** When enabled the door will not generate the door left open alarm events to any reader expander's programmed beeper and LED ports. This allows a door to be 'propped open' during normal opening times, however a pre-alarm warning will still be generated. This option DOES NOT prevent the door left open trouble input being sent to the monitoring station if reporting on the trouble input is programmed. To prevent the door open alarms from being sent, schedule the input type for the door open alarm events to operate without reporting during the day.
- **Prompt User For Access Reason Code:** When enabled the user will be prompted on the reader expander's associated keypad to enter their reason for access. The user must enter the reason before access will be granted.
- **Enable Access Taken on Door Unlock Events:** When enabled the door will generate a User Access Taken event if the door opens while the door is unlocked after entry has been granted. If the door remains closed, an Access Not Taken event is generated.

Extended Access Time Options

- **Door Extended Access Time:** The duration (in seconds) the door remains opens for users tagged as requiring extended access.
- **Antipassback Entry User Reset Time***: The duration (in minutes) before resetting the antipassback on entry. Requires the Enable Timed Users Antipassback Reset option to be activated in the Controller settings.
- **Antipassback Exit User Reset Time***: The duration (in minutes) before resetting the Antipassback on exit. Requires the Enable Timed Users Antipassback Reset option to be activated in the Controller settings.
- **Reset Antipassback Status On Schedule**: When enabled resets the antipassback status of all users, using a defined schedule.
- **Enable Timed User Antipassback Reset**: When enabled antipassback is reset according to User Reset Time.

Doors | Alarm Options

To set the outputs used by the alarms below, see the **Outputs** tab.

Pre-Alarm Options

- **Enable Pre-Alarm Alarms**: The door pre-alarm is activated when the door has been left open for the **Door Pre-Alarm Delay Time**, activating an output to warn users that the left open alarm is about to be activated. Disable

this option to disable the pre-alarm function for this door.

- **Disable During Unlock Schedule**: Enable this option to disable the door pre-alarm while the door has been latch unlocked by an unlock schedule.
- **Disable During Manual Commands**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by an operator using a manual command. The pre-alarm will still activate when the door has been unlocked (i.e. temporarily unlocked) by a manual command.
- **Disable Whilst Unlocked By Area**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by an area (e.g. using the **Area Disarmed OR Schedule Valid Unlock Door** option in the **Options** tab).
- **Disable Whilst Unlocked by Programmable Function**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by a programmable function.
- **Disable Whilst Unlocked by Fire Drop**: Enable this option to disable the door pre-alarm when the door has been latch unlocked by a programmable function with the **Door Control Mode** 2 - Fire Control Door Unlock.
- **Alarm Operating Schedule**: The door pre-alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

Left Open Options

- **Enable Left Open Alarms**: The door left open alarm is activated when the door has been left open for the **Door Left Open Alarm Time**, activating an output and opening the Door Left Open trouble input to report the alarm to the monitoring station. Disable this option to disable all left open alarm functions for this door.

  Disabling the left open alarm will not automatically disable the pre-alarm.

- **Disable During Unlock Schedule**: Enable this option to disable the left open alarm when the door has been unlocked by an unlock schedule.
- **Disable During Manual Commands**: Enable this option to disable the left open alarm when the door has been latch unlocked by an operator using a manual command. The pre-alarm will still activate when the door has been unlocked (i.e. temporarily unlocked) by a manual command.
- **Disable Whilst Unlocked By Area**: Enable this option to disable the left open alarm when the door has been latch unlocked by an area (e.g. using the **Area Disarmed OR Schedule Valid Unlock Door** option in the **Options** tab).
- **Disable Whilst Unlocked by Programmable Function**: Enable this option to disable the left open alarm when the door has been latch unlocked by a programmable function.
- **Disable Whilst Unlocked by Fire Drop**: Enable this option to disable the left open alarm when the door has been latch unlocked by a programmable function with the **Door Control Mode** 2 - Fire Control Door Unlock.
- **Alarm Operating Schedule**: The left open alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

Forced Open Options

The door forced operation can also be delayed via commands. For more information see Application Note 304: Delaying Door Forced Commands.

- **Enable Forced Open Alarms**: The door forced alarm is activated when the door is forced, activating an output and opening the Door Forced Open trouble input to report the alarm to the monitoring station. Disable this option to disable all door forced alarm functions for this door (although the door will still have the 'Forced Open' status on a floor plan or status page).

  Alternatively, see the **Forced Door Sends Door Open** option (**Inputs** tab).

- **Alarm Operating Schedule**: The door forced alarm will be enabled when this schedule is valid and disabled when this schedule is invalid.

Doors | Events

Recent Events

- Shows a list of all recent events associated with the door.

Door Groups

Door groups define which doors a user can access and/or control. A door group is assigned to an access level to restrict the ability of a user to gain entry to or exit from certain doors.

Click **Add** to add doors, then apply a schedule.

Inputs

Motion detectors, door contacts and other protection devices are connected to the system on inputs. An input belongs to an area to protect the area and the system from unauthorized entry. For example, a motion sensor input in reception may be assigned to an Administration Area.

Address

- **Module Type:** The type of module the input is attached to
- **Module Address Input:** The address of the module the input is attached to
- **Module Input:** The index of the specified input on that module

Configuration

- **Control Output/Output Group:** The output assigned to the input. This activates whenever an input type processes the input with the activate input output options enabled. The input type must have the appropriate input control output options set in the output options. An output can be assigned to the input type and to the input, allowing many to one and one to many configurations.
- **Control Automation**: This is a legacy option that has no effect.

  Automation control can be programmed in the input type configuration.
- **Reporting ID:** The Input Reporting ID allows the installer to program any reporting number to any input. This provides an extremely high level of flexibility to assign true reporting numbers to the inputs. An input assigned the same reporting ID as another input results in both inputs reporting that ID. If an input is assigned an ID number higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for the format.
- **Alarm Input Speed**: The alarm input speed determines how long an input must be open for before an alarm event is generated. This can be set from 0 seconds up to 1 hour. If the Alarm Input Speed is set at 0 seconds, the Restore Input Speed cannot be set below 100ms.
- **Restore Input Speed**: The restore input speed determines how long an input must be closed for before a restore event will be generated. This can be set from 0 seconds up to 1 hour. If the Alarm Input Speed is set at 0 seconds, the Restore Input Speed cannot be set below 100ms.
- **Enable Input Lockout**: When this option is enabled, each time this input triggers an alarm a counter is incremented. Once the counter reaches the **Input Lockout Count** the input is locked out and further activations will not cause alarms. The lockout is reset when the area is disarmed and rearmed again. This feature is useful for inputs which occasionally trigger false alarms.
- **Input Lockout Count**: If this input uses the **Enable Input Lockout** feature above, this setting defines the number of times the input can activate the alarm before it is locked out.

Commands

- **Commands***: Used to send manual commands to a device.

Inputs | Areas and Input Types

Assigned Areas

- **Area**: The input must be assigned to at least one area for it to perform any function in the system and can be assigned to up to four different areas. An input can perform a different function in each area, which is defined by the input type. For example, an input can be a delay input in one area and an instant input in another.
- **Input Type:** When an input is assigned to an area the input must be programmed with the type of input (24HR Panic, Burglary Delay, etc.) in order to function.

- **KLES Input LED**: If a Protege LED keypad is used, the area selected can be assigned to one of the keypad's LEDs. Any area assigned to LEDs 9 or higher is displayed on the keypad with a 0 representing the '10s' digit. For example, when the number 15 is displayed, the 0 and 5 will flash.

Inputs | Options

Options 1

- **Log to Event Buffer:** When enabled the input will generate an event whenever it is opened, closed, tampered with or shorted. The input will still perform all programmed functions if this is not enabled. When using inputs as automation inputs it is recommended to disable the event logging option to reduce the impact on the event log buffer.
- **Test For Trouble Condition:** When enabled the input will be monitored for a trouble condition and cause a trouble alarm to be generated. The trouble will be generated only if the input is either shorted or tampered with.
- **Bypassing Not Allowed:** When enabled the input is a high-security input and cannot be bypassed. However the input can still be force armed if the Force Arming option is turned on. In order to avoid this, and to ensure the input is not ignored when force arming, the Input Force Arming option should be turned off in the input type assigned to the input.
- **Latch Bypassing Not Allowed:** When enabled the input is a high-security input and cannot be latch bypassed. However the input can still be force armed if the Force Arming option is turned on. In order to avoid this, and to ensure the input is not ignored when force arming, the Input Force Arming option should be turned off.
- **Tamper Follows Bypass State:** When enabled the input will bypass the tamper monitoring of the input at the time the input is bypassed.
- **No Bypass If Any Area Armed:** When enabled the input will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.
- **Log Input Event When Bypassed**: By default, if the input is bypassed the system will not log events when it changes state (e.g. opens or closes). With this option enabled events will be logged even while the input is bypassed.
- **Tamper Input if Module Offline:** When enabled the input will operate as a tamper input when the module is offline.

Options 2

- **Input End of Line (EOL)**: Defines the resistors used for EOL configuration
- **Contact Type**: Defines whether the input is Normally Closed or Normally Open. Normally Closed is the default.

Door Types

Door Types defines how a door will operate, including passback mode and reading mode (card, PIN), and when valid.

General Configuration

- **Operating Schedule:** The Door Types schedule allows a door type to be scheduled for use during a certain time period. For example, setting a door type schedule for Card Only between 9am and 5pm, then a secondary door type of Card and PIN means that between the hours of 9am and 5pm any door assigned this door type requires card-only access, but outside this time period access requires a card and PIN number. Use this option to increase the security of the main entry doors after hours while maintaining a faster traffic flow during working hours.
- **Secondary Door Type:** Used in conjunction with the Operating Schedule this allows a door to have a secondary configuration for when the schedule is invalid. It allows different modes of control over the method a user has to access a door. For example, between 9am and 5pm the user may be required to access the door with only a card, but outside these hours a card and PIN are required.
- **Fallback Door Type:** This option enables you to define an alternate set of credentials that the door can accept as a fallback.

Entry

- **Entry Passback is Qualified with Door Opening*:** If enabled passback is qualified by the default door sense input for the associated door. This means if a user badges their card but does not open the door, it is not identified as a passback event.
- **Entry Passback Mode*:** The reader Antipassback operation mode determines how an entry reader controls the ability of a user to pass back their card or details to another person to gain access while they are already inside a protected area. The Protege System uses global Antipassback per controller. Selecting Soft Passback allows the user entry, but logs an error in the buffer that a passback violation has occurred. Selecting Hard Passback prevents the user from gaining entry and also logs an event.
- **Entry Reading Mode:** The reader entry operation mode determines how an entry reader associated with the door with this door type assigned operates. Choose from:
  - Card only
  - PIN only
  - Card and PIN
  - Card or PIN
  - Card or Biometric
  - Card and Biometric
  - Custom (When set to Custom, an 'Entry Credential Types' tab appears from which one or more standard credential types can be selected. For the door to unlock, all selected credential types must be presented and, if the 'Sequence' option is checked, the credential types must be presented in the specified order.)

Exit

- **Exit Passback is Qualified with Door Opening*:** If enabled passback is qualified by the default door sense input for the associated door. This means if a user badges their card but does not open the door, it is not identified as a passback event.
- **Exit Passback Mode*:** The reader Antipassback operation mode determines how an exit reader controls the ability of a user to pass back their card or details to another person to gain access while they are already inside a protected area. The Protege System uses global Antipassback per controller. Selecting Soft Passback allows the user to exit, but logs an error in the buffer that a passback violation has occurred. Selecting Hard Passback prevents the user from exiting the area and also logs an event.

- **Exit Reading Mode:** The reader exit operation mode determines how an exit reader associated with the door with this door type assigned operates. Choose from:
  - Card only
  - PIN only
  - Card and PIN
  - Card or PIN
  - Card or Biometric
  - Card and Biometric
  - Custom (When set to Custom, an Exit Credential Types' tab appears from which one or more standard credential types can be selected. For the door to unlock, all selected credential types must be presented and, if the 'Sequence' option is checked, the credential types must be presented in the specified order.)

Commands

- **Commands***: Used to send manual commands to a device.

Door Types | Options

Options

- **Door REX Not Allowed**: When enabled the door will disable the REX (request to exit) operation.
- **Door REN Not Allowed**: When enabled the door will disable the REN (request to enter).
- **Requires Dual Authentication***: When enabled the door will require two individual users to activate the reader before it unlocks. Under User programming, those users must be defined as having either Dual Custody Master or Dual Custody Provider access rights.
- **Dual Card Provider Can Initiate Access***: When enabled the door will unlock provided both users have either Dual Custody Provider or Dual Custody Master access rights. If disabled the Dual Custody Provider will only be recognized after a Dual Custody Master has activated the reader first.

Input Types

Input types define how an input operates in an area.

Configuration

- **Operating Schedule:** Determines when the input type is valid and whether it uses a secondary input type when the schedule is invalid.
- **Secondary Input Type:** Allows an input to have a secondary configuration when the Operating Schedule is invalid. This option is only enabled when the Operating Schedule is not set to Always.
- **Keypad Alarm Display Group:** Determines which keypads are presented with alarm information when the input that the input type is assigned to generates an alarm.
- **Control Automation**: The automation point activated when the input opens or closes. This can be used for various functions, such as gardening irrigation, lighting circuits, etc. Configure also the appropriate options under the Input Type in order to trigger the automation point.
- **Custom Reporting Code:** Each input type has a default reporting code already assigned which determines the code sent to the central station when an alarm is generated. This option enables changing the reporting code of the inputs to which this input type is assigned.
- **Control Output Time:** Overrides the programmed activation time for an output by setting an activation time in the input type.
- **Control Output / Output Group:** Assigns an output or output group to activate whenever an input type processes an alarm or a restore for an input. The input type must have the control output options set in Output options.
- **Control Area:** An input type can be programmed to control the arming and disarming state of an area from an input (key switch control). The area to be controlled by the input type must be programmed with the force arming option. Arming using an input type is deemed to be an unattended arming condition and therefore the system will attempt to arm the area in the force mode.

Commands

- **Commands***: Used to send manual commands to a device.

Input Types | Options 1

Alarm Options

- **Generate Alarms:** When enabled the input type will process alarms from the input assigned.
- **Generate 24HR Alarms:** When enabled the input type will process tamper alarms from the input assigned.
- **Entry Delay Input:** When enabled the input type will start the entry delay timer for the assigned area when the input generates an alarm.
- **Entry Delay Follow Input**: When this option is enabled, inputs using this input type will not generate alarms during the entry delay period, but will generate alarms if the entry delay has not started. Without this option enabled inputs will generate alarms even during entry delay.

  This option should be used for inputs which cover the route between the entry and the disarming point. For example, a PIR in the entryway should not generate an alarm when someone enters through the door (beginning the entry delay), but should generate an alarm if someone is detected in the room without opening the door.
- **Exit Delay Input**: When this option is enabled, inputs with this input type will not generate alarms during the exit delay period. When this option is disabled the input will generate alarms even during exit delay.

  This option should be enabled for any inputs that users may trigger as they exit the building during arming. It may be disabled for other inputs to prevent people from re-entering parts of the building during the arming process.

- **Short Exit On Restore:** When enabled the input type will shorten the exit delay time of an area to five seconds when the input restores. Use this feature to reduce the arming time of an area.
- **24hr Panic Input:** When enabled the input type will generate a 24-hour alarm if the input generates an alarm. The area state does not affect the generation of this alarm.
- **Fire Input:** When enabled the input type will generate a fire alarm when it is activated. This input type operates similarly to the 24hr Alarm option. Most smoke detectors use a Normally Open contact, so any input assigned this option must have the inverted state option selected and the EOL Resistors option enabled.

Reporting Options

- **Report Alarms:** When enabled the input type will generate a reportable alarm message.
- **Report Tampers:** When enabled the input type will generate a reportable tamper message.
- **Report Bypass:** When enabled the input type will generate a reportable bypass message.
- **Report Restores:** When enabled the input type will generate a reportable restore message.
- **Stay Input:** When enabled the input type will generate an alarm if the area is armed in stay mode. The input will stay armed. For inputs that will be active when an area is armed in stay mode it is recommended to disable the event log for the input.
- **Force Input:** When enabled the input type will allow the inputs it is assigned to be force armed.
- **Exit Alley Input Do Not Test It:** When enabled the input type will not verify the status of an input prior to the area starting to arm. Use this feature to assign inputs in exit locations to prevent the area from generating an input open warning when being armed.
- **Recycle Input Alarm on Exit Delay End:** When enabled the input type will recheck the inputs it is assigned when the area completes the exit delay cycle and, if an input is open, recycle the input to force it into generating an alarm. Use this feature for an input type used on an input that may be breached during the exit delay, such as a window or door contact.

Input Types | Options 2

Miscellaneous Options

- **Activate Bell Output:** When enabled the input type will activate the siren bell output programmed for the area.
- **Retrigger Bell Time:** When enabled the input type will restart the bell timer on each subsequent alarm.
- **Save To Area Memory:** When enabled the input type will save an alarm message to the area's alarm memory storage area.
- **Disarm Control Area On Input Restore:** When enabled the input type will disarm the control area when an input assigned the input type restores from an alarm condition. Use this feature and the arming control area feature as an on and off key switch arming input.
- **Arm Control Area On Input Alarm:** When enabled the input type will start arming the control area when an input assigned the input type generates an alarm condition.
- **Toggle Control Area On Input Alarm:** When enabled the input type will toggle the state of the control area when the input assigned this input type generates an alarm.
- **Allow Force Arming Of Tampered Input:** When enabled the input type will allow the input to be force armed if the input assigned the input type is tampered with.
- **Activate Entry Output on Bell Time:** When enabled the input type will activate the entry output programmed for the area for the duration of the bell siren time. Use this feature for an input generating only a beeper alarm and assign the entry output a keypad beeper output. This option will not function if the bell option is enabled.

Output Activation Options

- **Activate Bypass Output:** When enabled the input type will activate bypass output for the area if an input is bypassed.
- **Activate 24HR Tamper Output:** When enabled the input type will activate the tamper output for the area if a tamper alarm occurs.

- **Activate Memory Output:** When enabled the input type will activate the memory output for the area if an alarm occurs. This option can be used to indicate an alarm has occurred in the system. Use this feature to display an indication to the users of the system to prevent possible 'sitter' and 'hostage' situations.
- **Input Retriggers Output Time**: When enabled the input type re-initiates the activation time of an output when the input is triggered. For example, reactivating lights when a motion sensor is triggered.
- **Activate Control Output On Alarm*:** When enabled the input type will activate the control output when the input assigned generates an alarm.
- **Activate Control Output On Restore*:** When enabled the input type will activate the control output when the input assigned restores from an alarm.
- **Deactivate Control Output On Alarm*:** When enabled the input type will deactivate the control output when the input assigned generates an alarm.
- **Deactivate Control Output On Restore*:** When enabled the input type will deactivate the control output when the input assigned restores from an alarm.
- **Toggle Control Output State On Alarm*:** When enabled allows for toggling of output state.

Input Types | Options 3

Automation Options

- **Activate Automation On Alarm:** When enabled the input type will activate the automation point when the input assigned this input type generates an alarm.
- **Activate Automation On Restore:** When enabled the input type will activate the automation point when the input assigned this input type restores from an alarm.
- **Deactivate Automation On Alarm:** When enabled the input type will deactivate the automation point when the input assigned this input type generates an alarm.
- **Deactivate Automation On Restore:** When enabled the input type will deactivate the automation point when the input assigned the input type restores from an alarm.
- **Toggle Automation State:** When enabled the input type will toggle the current state of the assigned automation number.
- **24HR Generates Bell If Armed:** When enabled the input type will activate the bell output if a 24HR alarm is generated when the area is armed. Note this option will be overridden by the 24HR Always Generates Bell option and have no effect.
- **24HR Always Generates Bell:** When enabled the input type will always activate the bell output for the area if a 24HR tamper alarm occurs. This option will override the 24HR Generates Bell If Armed option when enabled.

Control Options

- **Use Input Type Output Time:** When enabled the input will activate the output timed (if a time is programmed) and use the Output Time set in the Input Type. If the input type does not have a time programmed, no time will be used.
- **Toggle Input Output State:** When enabled the input control output will be toggled when the input goes into alarm. Use this option to activate an output on alarm and deactivate on the next alarm. This is ideal for lighting control and automation applications.
- **Activate Input Control Output On Alarm:** When enabled the input type will activate the input control output when the input assigned generates an alarm.
- **Activate Input Control Output On Restore:** When enabled the input type will activate the input control output when the input assigned restores from an alarm.
- **Deactivate Input Control Output On Alarm:** When enabled the input type will deactivate the input control output when the input assigned generates an alarm.
- **Deactivate Input Control Output On Restore:** When enabled the input type will deactivate when the input control output assigned restores from an alarm.

Input Types | Options 4

General Options

- **Always Log Input Event:** When enabled the input will generate an event whenever it is opened, closed, tampered with or shorted.
- **Use Alternate Entry Time:** When enabled the input type will start the alternate entry delay timer for the assigned area when the input generates an alarm.

Areas

Areas allow for the Protege WX system to be divided into separate sections (alarm areas or partitions). This allows areas to be grouped for easy management of multiple areas at a time.

An installation may contain up to 32 areas or partitions, depending on the configuration and size of the system. Areas can contain inputs and trouble inputs that protect the area. Inputs can be assigned to as many as four areas and perform a different function in each area independent of the other area's status.

General

- **Name:** The name of the area
- **Database ID:** Unique ID used to identify the area when programming items using a touchscreen

Areas | Configuration

Timings

- **Entry Time (seconds):** Setting an entry delay time for the area allows users time to disarm the area before the area generates an alarm. Only inputs that have an input type assigned with an entry delay option set will start the entry delay timer for the area.
- **Alternate Entry Time (seconds)**: Defines the entry delay time when using an alternate entry to the area. For example, if an area can be accessed through a secondary entry point, such as a garage door, users can be allowed more (or less) time to disarm the area before an alarm is generated.
- **Exit Time (seconds):** Setting an exit delay time for the area allows users to exit once the arming of the area has begun without triggering an alarm. Inputs that are part of the exit route should be programmed with the exit option in the assigned input type.
- **Alarm Time (minutes):** The time determines how long the bell/siren output for the area will remain activated before timing out. If the option to retrigger the bell time is set in the input type assigned to an input triggered in the area, the siren bell time is reloaded on each subsequent alarm activation. Use the siren bell time and the retrigger bell option from the input type for smart automation of lighting and building control.
- **Smart Input Timer (seconds)*:** Used in conjunction with the Smart Input Count (under the Areas Configuration tab) and Enable Smart Input settings (under the Areas Options (2) tab) to prevent false alarms. Setting an intelligent false alarm prevention time allows the area to process alarms using smart alarm verification. For an alarm to occur in the area it will require that the Smart Input Count for the area is exceeded in the time programmed.
- **Rearm Area Time (minutes):** Setting the rearm delay results in the area automatically re-arming after the rearm timer has elapsed. This should be programmed for areas used to monitor and control system functions that should not be disarmed. This is also used to control vault and automatic teller machines when using the banking area functions to prevent an area from being disarmed for longer than the time programmed.
- **Vault Disarm Delay (minutes)*:** If the Vault Control Area option is enabled, this defines an additional time delay that needs to elapse before the area actually disarms.
- **Vault Dual Code Delay (seconds)*:** If the Dual Code Vault Control option is selected, this defines the time period within which the second user must log in to successfully disarm the area.
- **Recent Closing Time (seconds):** The Recent Closing Time defines how long the system considers an armed area recently closed. If after arming the area an alarm is generated within the programmed period, the Protege System Controller transmits a recent closed message. For this feature to operate correctly the input must have its report options enabled in the assigned input type.

Schedule

- **Arm/Disarm Schedule**: Defines a schedule that enables the area to be armed and disarmed automatically.
- **Disarm Area When Schedule Starts**: When enabled the area will automatically disarm when the assigned Arm/Disarm Schedule starts.

- **Arm Area When Schedule Ends**: When enabled the area will automatically arm when the assigned Arm/Disarm Schedule ends.

Setup

- **Child Area:** The child area is an area dependent on another area (the parent area). For example, if an area is armed its child area can also be automatically armed. If you select None the area will not have a child area assigned. Use this option to program a common area as there is no limit to the number of areas containing the same child area. A common area is an area which is the child area of more than one parent areas. The common area can only be armed once all its parent areas are armed.
- **Maximum Bypass Input Count:** The bypass count number sets the maximum number of inputs that can be bypassed within the programmed area.
- **Max User Count*:** The user count defines the maximum number of users who can be in the area at any one time. For example, if the user count is set to 10, the 11th user who attempts to enter the area is denied access. Typically, the user count feature is used when an area is controlled by an entry and an exit reader. When an access control card is presented to exit the area the user count goes down. The count is reset to 0 when the area is armed. You can also program the area to auto-arm when the count reaches 0 by enabling the Last User Arm option.
- **Client Code:** The client code for the area is the code used to report alarms to the monitoring station. If the client code is left at the default value of FFFF, the client code assigned to the service used to report alarms will be used.
- **Interlock Area Group*:** An interlock area group can be assigned to an area to prevent it from being armed or disarmed, depending on the status of all areas within the assigned interlock group.
- **Smart Input Count*:** Used in conjunction with the Smart Input Timer (under the Areas Configuration tab) and Enable Smart Input settings (under the Areas Options (2) tab) to prevent false alarms. If the count reaches the Smart Input Count then the alarm is triggered. If the time period elapses before the count is reached the counter and timer are reset.
- **Reporting ID**: The code by which the area will be reported to a monitoring station. Both ContactID and ReportIP use this code.
- **Lock Door Group On Arming*:** When programmed this door group will be locked before the arming process starts. This helps to ensure that any door left open inputs are closed as the associated doors are locked so the area will be able to arm successfully.

Loiter

- **Loiter Time (minutes)*:** The loiter time defines how long a user can remain in a specific loiter-enabled area. If the loiter time has elapsed and the user is still in the area, the user will be denied access when an attempt is made to exit the area. If the user has not exited the loiter area before the loiter time has elapsed, the user status must be reset manually from the operator software or local keypad. For this option to operate, the Loiter Mode options must be turned on for the user and a loiter area must be programmed. Furthermore, the area requires an entry and exit reader set with the Antipassback feature to control user traffic.
- **Loiter Reset Area*:** The loiter reset area setting is used when a user has violated the loiter configuration for the installation, and must be set to an area they cannot enter or exit from. The setting is typically an area not used in the system and defined as an invalid area.

Defer Warning

- **Defer Warning Keypad Group*:** The defer warning keypad group is used to define the keypads that will warn users when the area is about to automatically arm. The keypads will display the warning provided they do not have any higher priority messages displayed. The keypad beeper is recommended to be programmed in the defer output group. The Defer Automatic Arming option must be enabled, and for the keypads to generate a message they must also be programmed with the Display Defer Messages.

- **Defer Warning Time (minutes)*:** The defer warning time sets the duration that the area will warn users it is about to automatically arm and they need to defer the arming (log in and press the Disarm Key). When this is enabled, keypads in the assigned keypad group will beep once then display a warning message until either the Defer Warning Time elapses or an authorized user logs in and disarms the area.

  If a user disarms the area it will remain disarmed for the duration of the Defer Warming Time, and will then automatically re-enter the arming process, beginning with the defer warning.

User Selectable Defer Time

Alternatively, a user selectable defer time can be enabled. When this feature is enabled and a user disarms the area, the keypad will prompt the user to enter the number of hours to defer arming for.

Enable this feature by entering the command: `AskForDeferTime = true`

The minimum time that arming can be deferred from the keypad is 1 hour and the maximum is 9 hours. Arming can only be deferred in whole hours.

Commands

- **Commands***: Used to send manual commands to a device.

Areas | Reporting Services

Reporting Services defines the primary reporting service for the area.

Areas | Outputs

- **Bell Output/Output Group:** Assigns a bell/siren output or output group to activate whenever the area goes into alarm. The input that triggers the alarm must have the bell output option enabled for the input type. The bell/siren output and output group will be deactivated when the bell timer times out or when the area is disarmed. The bell/siren may also be disarmed when the user logs in to the keypad.
- **Bell Pulse On/Off Time**: These fields are used to make the bell output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Exit Delay Output/Output Group:** Assigns an exit delay output or output group to activate whenever the area starts an exit delay cycle. The exit delay output or output group will be deactivated when the area completes the arming cycle or if an alarm occurs during the exit delay period. Disarming the area will also result in the exit delay output or output group being deactivated.
- **Exit Delay Pulse On/Off Time**: These fields are used to make the exit delay output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Entry Delay Output/Output Group**: Assigns an entry delay output or output group to activate whenever the area starts an entry delay cycle. The entry delay output or output group will be deactivated when the area is disarmed during the entry delay period or the area activates the alarm due to the entry delay timing out.
- **Entry Delay Pulse On/Off Time**: These fields are used to make the entry delay output or output group pulse on and off when activated.

The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Disarmed Output/Output Group**: Assigns an output or output group to activate whenever the area completes the disarming cycle. The disarmed output or output group will be deactivated when the area completes the arming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling the system is disarmed and can be entered. It can also be used for interlocking non reader controlled doors to prevent entry to areas if the area is armed. Use this output in conjunction with user areas to control multiple storage lockers or storage facilities.
- **Disarmed Pulse On/Off Time**: These fields are used to make the disarmed output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Armed Output/Output Group:** Assigns an output or output group to activate whenever the area completes the arming cycle. The armed output or output group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling the system is armed.
- **Armed Pulse On/Off Time**: These fields are used to make the armed output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Bypassed Inputs Output/Output Group:** Assigns an output or output group to activate whenever the area has a bypassed input. The bypass output or output group will be deactivated when the area completes the disarming cycle.
- **Bypassed Inputs Pulse On/Off Time**: These fields are used to make the bypassed inputs output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Tamper Alarm Output/Output Group:** Assigns an output or output group to activate whenever the area has a tamper alarm. The tamper output or output group will be deactivated when the area completes the disarming cycle on the 24HR portion of the area.
- **Tamper Alarm Pulse On/Off Time**: These fields are used to make the tamper alarm output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).

- **Alarm Memory Output/Output Group:** Assigns an output or output group to activate whenever the area has an alarm and the output or output group will remain activated. The memory output or output group will be deactivated when the area completes the disarming cycle. Use this to drive local indicators on keypads, card readers and relays for signaling that the system has had an alarm activation.
- **Alarm Memory Pulse On/Off Time**: These fields are used to make the alarm memory output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **User Count Reached Output/Output Group***: Assigns an output or output group to activate whenever the user count in an area either reaches 0 or reaches the maximum count (set in the area options). The count output or output group will be deactivated depending on the programmed option for the area. Use this option to control car parking and user counting for specific building areas that require limited staff access.
- **User Count Reached Pulse On/Off Time***: These fields are used to make the user count reached output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Area Defer Arming Started Output/Output Group***: Assigns an output or output group to activate whenever the area begins the defer warning cycle and is about to arm. The defer warning time is programmed in the defer time setting. The defer output or output group will be deactivated when the area begins the arming cycle or when the defer time is canceled by a user.
- **Defer Arming Started Pulse On/Off Time**: These fields are used to make the defer arming output or output group pulse on and off when activated.

  The output or output group will turn on for the pulse on time, turn off for the pulse off time, then repeat. These times are set in 100ms increments. For example, if the pulse on time is set to 2 and the pulse off time is set to 8 the output will turn on for 200ms, turn off for 800ms, then repeat, for a total cycle of 1 second.

  If either or both of the pulse on and pulse off times are set to 0 the output will turn on continuously. Each of these fields supports a maximum value of 255 (25.5 seconds).
- **Fail to Arm Output/Output Group:** Assigns an output or output group to activate whenever the area fails to arm.
- **Ready Output/Output Group:** Assigns an output or output group to activate when all inputs or trouble inputs in an area are closed and the area is ready for arming.

Areas | Options 1

General Options

- **Input Restore on Bell Cut-Off:** When enabled the inputs assigned to this area will restore when the bell time completes. This does not prevent the input from generating multiple alarms for another area when this setting is specific to the area assigned. The inputs in the area will still log an event regardless of the bell time. To prevent an input from triggering an event remove the event log option in the input configuration. Setting this option will prevent the re-trigger bell timer from operating in the input type. Do not use this option for an area used for automation control or motion controlled lighting.
- **Re-Arm Enabled**: With this option enabled, whenever the area is disarmed it will be automatically rearmed after a certain time. The delay before rearming is set by the **Rearm Area Time** (**Configuration** tab). This function force arms the area, so **Enable Force Arming** must be selected (**Options (2)** tab).

This feature should be used for areas that are used for system monitoring and control, which should never be disarmed. It can also be used to ensure bank vaults, automatic teller machines and similar are not disarmed for longer than the programmed time.

When you enable rearming you must arm and disarm the area for the setting to take effect.

- **Arm Child Area:** When enabled the child area will be armed when the parent (this) area is armed. Can be used in conjunction with the option below.
- **Arm Child If All Other Areas Are Armed:** When enabled the child area will only be armed if ALL the areas the child area is assigned are armed. Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.
- **Disarm Child Area:** When enabled the child area will only be disarmed when the parent (this) area disarms.
- **Disarm Child If All Other Areas Are Disarmed:** When enabled the child area will only be disarmed if ALL the areas the child area is assigned are disarmed. Use this option when multiple areas are assigned the same child area that needs to be controlled with a specific disarming and arming order. This effectively allows an OR and AND operation to be done on the child area.
- **Use Unattended Brute Force Arming:** When enabled the area will not be prevented from arming if an input that is not a force enabled input is open when the area is armed in an unattended mode.

Reporting Options

- **Report Arming:** When enabled the area will generate a reportable event that can be directed to a monitoring station.
- **Report Disarming:** When enabled the area will generate a reportable event that can be sent to a monitoring station.
- **Report 24HR Area Disarming:** When enabled the area will report both an opening (Disabling) or closing (Enabling) of the 24HR section of this area.
- **Report User Bypass:** When enabled the area will report all inputs that are bypassed once it completes the arming process.
- **Report Entry Alarm Immediately:** When enabled the area will report the activation of an entry input immediately, even though the alarm may be in an entry delay operation.
- **Enable User Counting*:** When enabled the users that access this area will be counted using the area counting function.
- **Arm On User Count At 0*:** When enabled the area will arm when the count in the area reaches the terminal 0 count.
- **Clear User Count When Armed*:** When enabled the area will clear the count setting in the area to 0 when the area is armed.

Areas | Options 2

Advanced Options

- **Enable Stay Arming:** When enabled the area can be stay armed.
- **Enable Force Arming:** When enabled the area can be force armed.
- **Enable Instant Arming:** When enabled the area can be instant armed.
- **Do Not Arm if Trouble Condition:** When enabled the area will be prevented from arming if a trouble condition is present in the system.
- **Prevent Arming On Count Not Zero:** When enabled the area will be prevented from arming if the count value for the area is greater than 0.
- **Always Verify Area Schedule:** When enabled the area will verify that the programmed schedule has not changed or that the area has not been disarmed when it should have been armed. This will occur every one minute period.

- **Area can be Reset**: When enabled allows the area to arm while it is already armed. This means that an area that goes into alarm can be reset to the armed state, turning sirens etc. off, without having to be disarmed first. Use this option for areas that should never be disarmed.
- **Vault Control Area***: When enabled the area is used to control a vault area.
- **Dual Code Vault Control***: When enabled the area requires that two users control this area when enabled as a vault control area. This feature will not function unless the area has the Vault Control Area setting enabled.
- **Enable Smart Input***: Used in conjunction with the Smart Input Timer and Smart Input Count settings (under the Areas Configuration tab) to prevent false alarms. Normally when an input in the area is activated an alarm will be triggered immediately. When Smart Input is enabled, a counter is started when an input is first activated and increments each time another input within the same area is activated. An alarm is only triggered once the counter (the Smart Input Count value) is reached within the defined period (the Smart Input Timer value).

  For example, if the Smart Input Count is set to 2 and the Smart Input Counter is set to 60 seconds, two different inputs must activate within the 60 seconds before the area enters alarm. When the first input opens, the timer starts and the count increments to 1. When another input in the same area is opened within the same 60 seconds, the count increments to 2 and the area is sent into alarm. Consecutive reactivation of the same input during the timer does not increment the counter.

Arming Options

- **Always Force Arm Using Card Reader:** When enabled the area will force arm the area when the arming process is started by a card reader.
- **Disable Exit Output on Stay Arming:** When enabled the area will not activate the Exit Output when the area is stay armed.
- **Clear Alarm Memory after Arming:** When enabled the area clears all alarm memory when the area is armed.
- **Enable Late Arm Report:** When enabled the area generates Early to Arm and Late to Arm reportable events, according to the normal operating schedule (see above).
- **Enable Early Disarm Report:** When enabled the area will generate Early to Disarm and Late to Disarm reportable events, according to the normal operating schedule (see above).
- **Disable Rearm On Schedule**: When this option is enabled, automatic rearming will be disabled when the area has been disarmed by the **Arm/Disarm Schedule** (**Configuration** tab). Use this to ensure the area does not automatically rearm when it is supposed to be disarmed.

  The command `ReArmLevelTrigger = true` prevents the area from automatically rearming while the schedule is valid, regardless of how the area was disarmed.
- **User Rearm in Stay Mode:** When enabled and a user with the Rearm Area in Stay Mode option enabled disarms the area, the area will automatically rearm in Stay mode. Prior to rearming, the area will remain disarmed for the length of time specified by the Rearm Area time setting.
- **Defer Automatic Arming***: When enabled the area will begin a defer arming cycle prior to starting the area arm process when the area is set to automatically arm on schedule.

Squawk Options

Squawk operation is not supported on the controller's onboard reader expander outputs.

- **Bell Squawk on Arming Start:** When enabled the area will generate a bell squawk when the arming process starts.
- **Bell Squawk on Arming Complete**: When enabled the area will generate a bell squawk when the arming process is complete and the exit delay has ended.
- **Bell Squawk Only When Unattended:** With this option enabled the bell output will only squawk when the area is armed or disarmed by an unattended method such as schedule, automated rearming or programmable function. It will not squawk when armed or disarmed from the keypad or card reader.
- **Bell Squawk on Disarm:** When enabled the area will generate a bell squawk when the area is disarmed.
- **Bell Squawk on Successful Report:** When enabled the area will generate a bell squawk when a successful Area Armed report has been sent and acknowledged by a reporting service.

Schedule

- **Normal Disarm Schedule:** Period 1 of the schedule defines the time period when the area can be disarmed. If the area is disarmed before the start of Period 1, an Early to Disarm event will be generated. If the area is still armed when Period 1 ends, the system will generate a Late to Disarm event. No event is generated if the area is disarmed while Period 1 of the schedule is valid.
- **Normal Arm Schedule:** Period 2 defines the time period when the area can be armed. If the area is armed before the start of Period 2, an Early to Arm event will be generated. If the area is still disarmed when Period 2 ends, the system will generate a Late to Arm event. No event is generated if the area is armed while Period 2 of the schedule is valid.

Areas | Events

Recent Events

- Shows a list of all recent events associated with the area

Area Groups

Area groups are assigned to an access level and are used to control the areas that a user can arm and disarm. An area group can be assigned for arming and disarming. Areas assigned in the disarm area group can also be armed by the user.

Select the **Areas** tab to manage the areas assigned to the group.

Areas

- The areas that belong to the area group. Click **Add,** select and click **OK** to add to the list displayed.

Outputs

Outputs are used to control devices from the Protege System. An output can be used to control lighting, activate a siren, turn on an indicator or unlock a door.

Address:

- **Module Type:** The type of module the output is attached to
- **Module Address:** The address of the module the output is attached to
- **Module Output**: The index of the specified output on that module

Configuration:

- **Activation Schedule:** The activation schedule is programmed to activate the output at a certain time of the day or to activate the output between certain hours. The schedule will be checked at the start and end times and, if the start is valid, the output will be activated. If the end time of the schedule is valid, the output will be deactivated. If an output is controlled by an operator, user or other function during this activation time and is deactivated, it will remain in the deactivated state.

  Setting the recheck schedule option for the output will force the output to have the schedule verified every 60 seconds. This will prevent the output from being controlled manually as the schedule overrides the manual operation.

- **Always Verify Schedule:** When enabled the output will re-verify the programmed schedule every 60 seconds. If the output is scheduled to be activated but is in a deactivated state, the system will activate the output.
- **Activation Time (seconds):** Any device controlling the output will only activate the output for the programmed activation time. Setting the time to 0 will result in the output staying on continuously until manually turned off or controlled via automation or programmable function.
- **Activation Retrigger**: When enabled if an output receives a command to activate for a defined period, and during that time it receives a second command to activate, this option retriggers the output for the second period. If this option is disabled, the second command is ignored.

Commands

- **Commands***: Used to send manual commands to a device.

Outputs | Options

General

- **Log Output Events:** When enabled the output will generate an event whenever it is activated or deactivated. The output will still perform all functions that are programmed if this is not enabled.

  When using output's as automation control outputs it is recommended to disable the event logging option to reduce the impact on the event log buffer.

- **Invert Output:** When enabled the output will operate inverted. Deactivation will result in the output being activated and activation will result in the output being deactivated.

Preset State

- **Preset Controller Power Up:** When enabled the state of the output will be set when the controller is reset or powered up for the first time.
- **Output Turns On When Controller Powers Up:** Defines the state of the output when the Preset Controller Power Up option is enabled. If enabled the output will be activated. If disabled the output will be deactivated.
- **Preset Module Power Up:** When enabled the state of the output will be set when the module powers up, and will override the current state held in the controller.

- **Output Turns On When Module Powers Up:** Defines the state of the output when the Preset Module Power Up option is enabled. If enabled the output will be activated. If disabled the output will be deactivated.
- **Preset Module Offline**: When enabled the state of the output will be set when the module goes offline.
- **Output Turns on When Module Offline**: Defines the state of the output when the Preset Module Offline option is enabled. If enabled the output will be activated. If disabled the output will be deactivated.

Output Groups

Output groups are used to group a number of outputs together, and are assigned to an access level to determine the outputs a user can activate and deactivate.

Select the **Outputs** tab to manage the outputs assigned to the group.

Outputs

- The outputs that belong to the group. Click **Add,** select and click **OK** to add to the list displayed.

Keypad Groups

Keypad Groups are used to group a number of keypads together to restrict access. Keypad Groups are assigned to Menu Groups which, when assigned to Access Levels, determine the keypads a user can log into.

Menu Groups

Menu groups provide a way of grouping together the various keypad menus programmed in the system. Menu groups can be assigned to an access level to determine which keypad functions those users have access to.

General

- **Name:** The name of the menu group
- **Database ID:** Unique ID used to identify the Menu Group when programming items using a touchscreen
- **Operating Schedule:** Determines when the menu group is valid
- **Secondary Menu Group:** The menu group to be used when the operating schedule is invalid

Settings

- **Area (1):** When enabled the menu group will allow the user to access the Area menu
- **User (2):** When enabled the menu group will allow the user to access the User menu
- **Events (3):** When enabled the menu group will allow the user to access the Events menu
- **Installer (4):** When enabled the menu group will allow the user to access the Installer menu
- **View (5):** When enabled the menu group will allow the user to access the View menu
- **Time (6):** When enabled the menu group will allow the user to access the Time menu
- **Bypass (7):** When enabled the menu group will allow the user to access the Bypass menu
- **System (8):** When enabled the menu group will allow the user to access the System menu
- **Extended Time Menus (6, 2-4):** When enabled the menu group will allow the user to access the Extended Time menus
- **Bypass Trouble Input (7, 2):** When enabled the menu group will allow the user to access the Bypass Trouble Input menu
- **Area Group Control Allowed:** When enabled will allow the user to access the area group control screen from the area status display screen
- **Tamper Area Control Allowed:** When enabled will allow the user to access the tamper area control screen
- **Stay Arming:** When enabled will allow the user to stay arm an area. The area must also have the stay arming option enabled
- **Force Arming:** When enabled will allow the user to force arm an area. The area must also have the force arming option enabled

Menu Groups | Keypad Groups

Keypad Groups can be assigned to Menu Groups to restrict which keypads a user can log into. When a Menu Group is assigned to an Access Level, those users will only be able to log into keypads included in the Keypad Groups that are assigned to the associated Menu Group.

If no Keypad Groups are assigned to the Menu Group, users will have access to all keypads.

Menu Groups | Options

- **User Advanced Menu:** When enabled the current menu group will be acknowledged as a user advanced menu.
- **Installer Menu Group:** When enabled the current menu group will be acknowledged as an installer menu group.
- **Show User Greeting:** When enabled the menu group will display the time of day greeting to the user once they have entered their user code.
- **User Can Acknowledge Alarm Memory:** When enabled the user will be able to acknowledge alarm memory that is displayed when they first login.

- **Show User Alarm Memory On Logon:** When enabled the user will be shown any alarms that are in the memory when they log in to the keypad.

Trouble Inputs

Trouble inputs operate similarly to regular inputs, however they are used to monitor the status and condition of the system. For example, if the enclosure door on the main control device is opened, it will open the Enclosure Tamper trouble input.

Address

- **Module Type:** The type of module the input is attached to
- **Module Address Input:** The address of the module the trouble input is attached to
- **Module Input:** The index of the specified input on that module

Configuration

- **Trouble Group:** The high level of flexibility provided by the Protege System allows for the definition of the trouble type and group generated by a trouble input. Trouble events are grouped by a trouble group and then a trouble type within the group. When the trouble input generates an alarm it will also generate the appropriate trouble condition that is configured. The trouble group and type are used to generate trouble conditions on the keypad and to prevent an area from arming based on the trouble condition.
  - **1- General**: The General trouble group consists of trouble types related to main system operation. Trouble conditions such as AC Failure, Real Time Clock and Bell Output Troubles belong to this group and are assigned the General Trouble Group and the appropriate trouble type from the group by default.
  - **2- System**: The System trouble group is used for module-related system messages, hardware faults and other system conditions that do not belong in the general trouble group.
  - **3 - Access**: The Access trouble group consists of trouble conditions related to access control and door operation. These include door forced open, door left open, and number of attempts.
- **Trouble Group Options:** When a trouble input is assigned to a trouble group it can then have a trouble type assigned. The trouble input types belong to the trouble groups. Selecting a trouble group will allow the appropriate trouble type from that group to be selected. The following trouble types are shown for each of the three groups below:
  - **AC Failure:** AC Failure has occurred on one or more devices in the system
  - **Module Tamper:** A module in the system has been tampered with
  - **Forced Door:** A door in the system has been forced open or opened without being accessed correctly

    To configure an alarm delay to occur when the door forced trouble input is activated, add the `AlarmSpeed = X` command in the **Commands** field for the door forced trouble input, where **X** is the delay time in milliseconds. Valid delay times are 10, 50, 100, 250, 500, 1000, 2000, 3000, 4000, 5000, 10000, 30000, 60000, 120000, 600000, 1800000 and 3600000 milliseconds.
  - **Battery:** A Low Battery or Missing Battery on one or more devices in the system
  - **Module Loss:** A module has failed to communicate with the system controller
  - **Door Left Open:** A door has been left open past the left open time
  - **Clock Loss:** The Real Time Clock has not been set since the System Controller has powered up. To reset the associated trouble, set the time from the time menu
  - **Module Security:** A module has attempted to register with the system controller, however the system controller is secured
  - **Number Attempts:** The number of attempts to gain entry to a door or keypad device has been exceeded. The next valid access will reset this trouble condition
  - **Reporting:** The System Controller has failed to get a report through to the monitoring station in the programmed number of attempts. This will restore when the next reporting event is successful
  - **Hardware Fault:** The system controller cannot communicate with an accessory interface board, or a device connected to the system controller has a hardware failure
  - **User Denied:** A user has been denied entry to a keypad or door

  - **Phone Line:** The phone line on the system controller is either cut or damaged
  - **Unknown Card:** An unknown card has been received by the system on a card reader input
  - **Input Fault:** An input in the system has been tampered with or short circuited
  - **Fire Loop:** A fire input has a loop fault
  - **Power:** A power problem (auxiliary, fuse or analog) has occurred on the Controller or a device in the system
  - **Bell:** The Bell/Output on the system controller or a device in the system has either been disconnected or it has shut down due to excessive current consumption
- **Reporting ID:** The Trouble Input Reporting ID allows the installer to program any reporting number to any trouble input. This provides an extremely high level of flexibility to assign true reporting numbers to the trouble inputs. A trouble input assigned the same reporting ID as another trouble input will result in both trouble inputs reporting that same ID. If a trouble input is assigned an ID number that is higher than the maximum number that can be reported by a particular service, the service will use the maximum number that can be assigned for the format.

Commands

- **Commands***: Used to send manual commands to a device.

Trouble Inputs | Areas and Input Types

Assigned Areas

- **Area**: The trouble input must be assigned to an area for it to perform any function in the system. By default ALL trouble inputs are assigned to the predefined trouble area which is the last programmable area in the system. A trouble input can be assigned in up to 4 different areas. A trouble input can perform a different function in each area which is defined by the trouble input type.
- **Input Type:** When a trouble input is assigned to an area the input must be programmed with the type of trouble input (24 Hour Panic, Burglary Delay, etc.)

Trouble Inputs | Options

General Options

- **Log to Event Buffer:** When enabled the trouble input will generate an event whenever it is opened or closed.
- **Bypassing Not Allowed:** When enabled the trouble input is a high security trouble input and cannot be bypassed.
- **Latch Bypassing Not Allowed:** When enabled the trouble input is a high security trouble input and cannot be latch bypassed.

Advanced Options

- **No Bypass If Any Area Armed:** When enabled the input will be prevented from being bypassed if it is already assigned to an area that has either the 24HR processing enabled or the area is armed.

Elevators

This feature is only available in Advanced mode.

Elevators are used to control user access or to monitor and control floors in a multi-storey high-rise building.

Configuration

- **Reader Expander:** The reader expander selection programs the elevator to send the activation of floor information and floor selection to the reader expander programmed. The port number in the next screen must also be set to the appropriate port driving the elevator.
- **Reader Port:** The reader port selection programs the elevator to communicate on this port with the expander number selected above. Set the reader expander number in the previous screen.
- **Unlock Access Time (seconds):** The length of time (in seconds) that the floor outputs will be activated when a user is granted access. When destination reporting is not enabled the user will have this length of time to select a floor. When destination reporting is enabled the selected floor will be activated for this length of time.
- **Unlock Intercom Time (seconds)**: The length of time (in seconds) that a floor will be unlocked when it is triggered by an intercom service. Once access has been granted at the intercom the user will have this length of time to enter the elevator car and select a floor.

  For more information on programming the intercom and elevator integration, see the ProtegeVandal Resistant Touchscreen Entry Station Installation Manual.

- **Floor Select Time**: When destination reporting is enabled the user has this time (in seconds) to press a floor button after they are granted access. This option is not required when destination reporting is not enabled.
- **Destination Reporting Enable:** When enabled the elevator will operate in Destination Reporting mode (DRM), allowing only one button to be selected by the user when they present their card.

To configure the **Authentication Mode** for an elevator car, add `EntryMode = #` to the **Commands** field for the elevator, where **#** is the required type of authentication, as defined in the table below:

Card Only	0
PIN Only	1
Card and PIN	2
Card or PIN	3

Commands

- **Commands***: Used to send manual commands to a device.

Elevators | Schedules and Areas

Each floor in an elevator can be assigned options, an unlock schedule and an area. These options configure how the floor will function. Select the floor to modify for the elevator.

- **Schedule:** The floor operation schedule can be assigned to each floor, allowing the floor to unlock at the programmed times within the schedule. A schedule is valid when the time of day falls between any start and end time, provided the day of the week is selected and holidays are not affecting the schedule.
- **Area:** This option defines the area inside the floor. Use this option in conjunction with Follow Area or Disarm Area to integrate area control with elevator access.
- **Late To Open:** When enabled the floor only unlocks on schedule if valid access has been made to the selected floor. This option only applies when Destination Reporting is enabled.
- **Verify:** When enabled the floor state is checked against the schedule every minute and changes state accordingly.

- **Follow Area:** When a floor area is defined and this option is enabled, the floor will follow the state of the area. If the area is armed, the floor will lock. And if the area is disarmed, the floor will unlock.
- **Input**: Defines the input used to monitor button presses to the floor from the elevator car. This option only applies when Destination Reporting is enabled.
- **Output**: Defines the output linked to the floor select button inside the elevator car. For every button that can be pressed to select a floor, an output must be configured.
- **Disarm Area**: When a floor area is defined and this option is enabled, the area will automatically be disarmed when the floor is accessed by a user with the ability to disarm the area. In addition, this option will prevent a user from accessing a floor when the area is armed and they cannot disarm it. This option is only available when Destination Reporting is enabled.

Elevator Groups

This feature is only available in Advanced mode.

An elevator group contains a list of elevators that belong in a particular group from the elevators programmed in the system. An elevator group can be assigned to an access level to determine the elevators a user has access to.

Select the **Elevators** tab to manage the elevators assigned to the group.

Elevators

- The elevator cars that belong to the elevator group.

Floors

This feature is only available in Advanced mode.

Floors are used in conjunction with elevators and represent a physical level of the building (floor).

General

- **Name**: The name of the floor
- **Floor Relay**: Specifies a link to the physical hardware controlling the elevator. This is the index of a relay on an Output Expander module which, if wired correctly, will correspond directly to the Floor number in the building

Commands

- **Commands***: Used to send manual commands to a device.

Floor Groups

This feature is only available in Advanced mode.

A floor group contains a list of floors that belong in a particular group from the floors programmed in the system. A floor group can be assigned to an access level to control the floors that a user has access to when accessing an elevator (the access level must also have an elevator group).

Floors

- The floors that belong to the floor group. Click **Add** to select floors to add to the list displayed.

Phone Numbers

Phone numbers are defined so that a telephone number can be assigned to a Contact ID service that communicates using a modem or telephone connection.

Phone numbers are only used by controller models with onboard modem dialers.

Configuration

- **Operating Schedule:** The operating schedule for the telephone number determines when the telephone number is valid to be dialed, and whether it will use a secondary telephone if the schedule is not valid. A schedule is a series of times and days that can be programmed to prevent the operation of functions based on a 7 day week and 24 hour clock. For example, the schedule may allow you to report messages during a normal day (8am to 5pm) to one telephone number or monitoring station, and to report them to another location outside of these hours
- **Secondary Phone Number:** When programmed a secondary telephone number will be used when the schedule of the telephone number that is being programmed is not valid. The schedule of the secondary telephone number must be valid or set to none
- **Phone Number:** Program the telephone number that you want to assign to this telephone number entry

Services

Services are used to provide interaction between Protege and external systems.

Type

- **Service Type:** The type of service that is programmed determines the operation the service performs. It also determines the programming screens that follow in each of the sub sections as the programming of services contains features and options dependent on this selection. The following section provides an explanation of each service type. Services require the use of onboard hardware devices or expansion devices.
  - **Contact ID:** Sends alarms, tests and events using the Contact ID reporting format to a monitoring station capable of receiving the Contact ID format.

    Contact ID reporting is only available for controller models with onboard modem dialers.
  - **Report IP:** Allows the Protege system controller to send alarm and activation information over an IP connected network. The Report IP Service supports multiple formats and allows the connection to third-party reporting, if required.
  - **Automation and Control**: Provides a generic interface for integration with third-party automation products, such as Savant, Control 4, Crestron, AMX, C-Gate and Command Fusion
  - **C-Bus**: Provides integration with building control and automation products using the Clipsal C-Bus protocol.
- **Service Mode:** The service mode determines how this service operates with the system controller. By default a service is set to start with the operating system. Setting a service to Start With Controller Operating System (Start With Controller OS) allows the service to operate automatically; if the system controller is reset or restarts, the service will automatically restart with the operating system. To only start and stop the service manually, select Manual Mode.

Commands

- **Commands***: Used to send manual commands to a device.

Contact ID

The Contact ID Service is used to sends alarms, tests and events using the Contact ID reporting format to a monitoring station capable of receiving the Contact ID format.

Contact ID reporting is only available for controller models with onboard modem dialers.

Contact ID | General

- **Client Code:** The client code is used to identify the system to the remote monitoring company when a report is generated. The client code will accept hexadecimal numbers, however this will be dependent on the ability of the receiver and should be verified before configuration.
- **PABX Number:** The PABX phone number is dialed to gain an outside line if the system is connected to an internal phone extension. The PABX phone number can also be programmed with a schedule in the case that between certain times the phone line is directly connected with an outside line.
- **Phone Number 1:** The primary phone number will be dialed by the contact ID service when it is first initiated to report an event. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).
- **Phone Number 2:** The secondary phone number will be dialed by the contact ID service if a connection with the central station cannot be made on the primary phone number. This may be dialed after the total number of attempts is reached on the primary or alternate until the total number of attempts is reached for the primary and secondary numbers. The sequence of telephone number dialing is limited by the number of dialing attempts and the method of dialing that is configured (alternate or sequential).

- **Phone Backup:** The backup phone number will be dialed by the contact ID service if a connection with the central station cannot be made on either the primary or secondary phone number. This will be dialed after the total number of attempts is reached on the primary and secondary numbers. The backup number will be dialed for the configured number of dialing attempts programmed for the service.

Contact ID | Options

- **Use Alternate Dialing Method:** When enabled the service will switch attempts between phone numbers 1 and 2 if a connection cannot be made. If the first phone number fails, the service will switch to the second phone number, and alternate until the max number of attempts is reached.
- **Pause After PABX:** When enabled the dialer will insert a pause of 2.5 seconds after the PABX telephone number is dialed.
- **Report Open:** When enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Close:** When enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Alarms:** When enabled the service will report alarms for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Tampers:** When enabled the service will report tampers for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Restore:** When enabled the service will report restores for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Bypass:** When enabled the service will report bypasses for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Service Operates as Backup:** When enabled the service will NOT report messages and alarms unless it is started by another service that has failed. It will then start reporting messages immediately from the point that the service that started it failed to report and then return operation to the service that started. This cycle will continue until the service that failed operates normally.
- **Log Modem Events to Event Buffer:** When enabled the service will provide step by step event information showing the call progression and detailed logging information. This option can be turned on for diagnostic purposes but should not be enabled permanently as large volumes of events are stored.

Contact ID | Settings

- **Dial Attempts:** Determines how many times the dialer will attempt to dial a number before failure. This setting will be overridden by the modem configuration dependent on the country of installation. For UL and ULC installations this value cannot be set above 8 and will be internally restricted if a value is programmed above this value. The dialing attempts operates in conjunction with the dialing delay setting.
- **Port Attempts:** The port open attempts determines how many times the service will wait for the modem to become available if another service is already using modem communication. This operates in conjunction with the port open time settings.
- **Report Count:** If set to a value other than 000 the report count will restrict the service from sending more than the programmed number of reports to the monitoring station. When using multiple reporting paths that potentially can report the same event to 2 or more locations, the report count should be programmed with an acceptable limit (Between 8 and 16 is recommended).
- **Handshake Time:** The handshake time determines the time it takes for the remote receiving unit to answer and provide a handshake message for the contact ID format. By default this is set to 030 seconds and should only be adjusted if a longer than normal call completion is required.
- **Dial Time:** The redial time determines inter phone number dialing timeout. A value of 20 seconds is programmed by default, meaning each phone number will be dialed with 20 second intervals from the time the previous call was terminated.
- **Off Hook Output/Output Group:** The Off Hook output or output group is activated when the service takes the telephone line, and is deactivated when the service completes communication. This output setting can be used with remote exchange systems that require ground start communication connections.

- **Report OK Output/Output Group:** The Report OK output or output group is activated when the service completes the reporting and the messages have been successfully acknowledged by the service returning a reporting complete result OK message. The output is not automatically deactivated and should be programmed with a timer, which can be connected to an external audible device to signal that the report was completed. Using this feature with the shorten exit delay for an area allows an end user to verify the communication path on arming of the building.

Background Monitoring

- **Enable Background Monitoring**: When background monitoring is enabled the service will regularly send polling messages to confirm that the phone lines are operational. This ensures that issues in any of the phone lines (whether primary or backup) are detected.
- **Background Poll Time When OK**: Determines how often (in seconds) the controller will check the status of the service when there are no known issues.
- **Background Poll Time When Known Failure**: Determines how often (in seconds) the controller will check the status of the service when there is a known issue.
- **Offline Poll Report**: The Contact ID event code, group number and zone number that the controller will send to poll the backup phone numbers.
- **Phone 1 Failed**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone Number 1**.
- **Phone 2 Failed**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with **Phone Number 2**.
- **Backup Phone Failed**: The Contact ID event code, group number and zone number that the controller will use to report failed communication with the **Backup Phone**.

Report IP

This service allows the controller to send alarm and activation information over an IP connected network. The Report IP service supports multiple formats and allows the connection to third-party reporting if required.

In addition, the Report IP service can be used to send push notifications to the Protege Mobile App. The specially configured push notification service is created automatically when the option is enabled in the app, and reports on all areas in your system. For more information, see the Protege Mobile App User Guide.

Report IP | General

Configuration

- **Client Code:** The account number for the Report IP Service can be up to 8 digits. An account code with leading zeros will be truncated to send the minimum number of digits. For example the account code 004311 will be sent as 4311. Where there are more digits set in the account code than the format that is selected allows, the account number will be truncated.
- **Reporting Protocol:** The reporting protocol defines how the IP communication data will be sent to the monitoring station. Various protocols are supported to allow the most comprehensive solution.
  - **ArmorIP:** ArmorIP will communicate to the ArmorIP server software running on a remotely connected server. The ArmorIP Server provides a standard Ademco 685 output and allows routing and redirection of signals to other reception devices such as email, SMS messaging and websites. The ArmorIP software is designed to be used with a concentrator operating in the central station control room.
  - **SIA Over IP:** SIA Over IP communicates a SIA Level 2 message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification.
  - **CID Over IP:** CID Over IP communicates a Contact ID message using the SIA DC09 specification format to any receiver that supports the SIA DC09 specification. SIA DC09 Specification is currently not released as a formal specification and is subject to change.
  - **CSV-IP:** By default the CSV-IP service will use the Contact ID reporting format. Information is sent using a login and password and then event information in a ASCII comma separated data format.

  - **Patriot LS30:** Patriot LS30 Protocol is the IP Communication format used by Patriot Systems central station automation application. By default the Patriot LS30 service will use a form of Contact ID reporting. Information is sent using a proprietary format and to obtain details the user should contact Patriot Systems directly.
- **Encryption Level**: Sets the encryption type used to encrypt messages from the service. The encryption settings here must match those in the receiving device so that the messages can be decrypted.
- **Encryption Key**: If the **Encryption Level** is set, this field defines the associated encryption key. The key is any sequence of letters and numbers shared with the receiving device. For 128 bit encryption the key must be 16 characters long; for 192 bit it must be 24 characters; and for 256 bit it must be 32 characters.
- **Poll Time (seconds):** The polling time is set to schedule periodic connections with the server. The polling messages sent to the receiver will depend on the format. Some formats require that the polling time be set at both the controller and receivers. In this case ensure that this setting matches the setting provided by the central monitoring station company.
- **Back Up Service:** A backup service can be programmed to allow the IP reporting functions to be backed up by a telephone dialer or similar. Using a backup service can be beneficial to allow link failures and internet access to be reported over an alternate connection.
- **Time Before Switching to Backup (seconds)**: If a backup service has been programmed, this field defines the length of time (in seconds) before the service will switch over to backup if it cannot establish a connection through the specified IP channels. If no backup service is specified, this field is ignored.

Primary Channel Settings

- **IP Address/Host Name:** The primary IP address is the IP of the server that has the receiver attached. The receiver can be the ArmorIP server or an IP receiving device.
- **IP Port Number:** The primary port configures the reporting service with the remote port number to communicate on. Consult the documentation provided with the receiver software or hardware to find this information. This information may also be different based on how the device is connected to the internet or intranet that you are communicating on.
- **Network Adaptor:** The network adapter on the controller that the Report IP service uses for communication. This should be set to Cable to use the onboard ethernet interface, or USB Ethernet to use a cellular modem.
- **Number of Port Open Attempts:** The number of times the service should try to open the communications port.
- **Ack Wait Time**: Denotes the wait time (in seconds) for signal acknowledgement.
- **Report Fail Output:** The output to activate when the service's communications fail.
- **Report Fail Output Group**: The output group to activate when the service's communications fail.
- **Enable Offline Polling**: This option enables polling to detect whether the alternative backup service is working (see Service Operates as Backup under Services | Report ID | Options).
- **Communication Failure Report:** When offline polling is enabled, these are the three codes displayed in a Contact ID message sent to the monitoring station when the channel becomes unstable and when the channel is restored.
  - **CID Code:** Industry standard three-digit code signifying the type of event.
  - **CID Group:** A two-digit reporting ID for area.
  - **CID Zone:** Denotes the specific reporting ID for the input, e.g. of a particular PIR.
- **Offline Poll Count** and **Offline Test Report Time(minutes)** are set here.

Secondary Channel Settings

- **IP Address/Host Name:** The secondary IP address is the IP of the server that has the receiver attached and can be set so that it will be routed through a separate connection. For example an ADSL modem maybe used for primary and a wireless connection for the secondary communications. For higher security it may also be desirable to have two internet service providers.
- **IP Port Number:** The secondary port configures the reporting service with the remote port number to communicate on for the secondary IP. By using this information in association with the secondary IP, a specific route can be set for this connection.

- **Network Adaptor:** The network adapter on the controller that the secondary channel uses for communication. This should be set to Cable to use the onboard ethernet interface, or USB Ethernet to use a cellular modem.
- **Number of Port Open Attempts:** The number of times the service should try to open the communications port.
- **Ack Wait Time**: Denotes the wait time (in seconds) for signal acknowledgement.
- **Report Fail Output:** The output to activate when the service's communications fail.
- **Report Fail Output Group**: The output group to activate when the service's communications fail.
- **Enable Offline Polling**: This option enables polling to detect whether the alternative backup service is working (see Service Operates as Backup under Services | Report ID | Options).
- **Communication Failure Report:** When offline polling is enabled, these are the three codes displayed in a Contact ID message sent to the monitoring station when the channel becomes unstable and when the channel is restored.
  - CID Code: Industry standard three-digit code signifying the type of event.
  - CID Group: A two-digit reporting ID for area.
  - CID Zone: Denotes the specific reporting ID for the input, e.g. of a particular PIR.
- **Offline Poll Count** and **Offline Test Report Time(minutes)** are set here.

Report IP | Options

- **Switch Secondary IP Immediately:** When enabled the service will immediately use the secondary IP settings.
- **Report Open:** When enabled the service will report opens (Disarming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Close:** When enabled the service will report closes (Arming) for the areas that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Alarms:** When enabled the service will report alarms for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Tampers:** When enabled the service will report tampers for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Restore:** When enabled the service will report restores for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Report Bypass:** When enabled the service will report each bypass for the inputs that are part of the area group assigned. An area group of none will mean ALL areas will be sent using this service.
- **Log Acknowledge Response:** When enabled the service will log acknowledge communication events.
- **Log Polling Message:** When enabled the service will log and event when the polling has been accepted by the remote host receiver.
- **Log Message Retries:** When enabled the service will log a communications retry that occurs because of a network failure or loss of service.
- **Log Reporting Failure:** When enabled the service will log an event when communications have failed completely and the service is waiting on another attempt.
- **Service Operates as Backup**: When enabled the service will not report messages and alarms unless it is started by another service that has failed. It will then start reporting messages immediately from the time the other service failed to report, and then return operation to the service that started. This cycle will continue until the service that failed operates normally again.

Automation and Control

This service provides a generic interface for integration with third-party automation products such as that provided by Savant, Control 4, Crestron, AMX, C-Gate, and Command Fusion.

This feature is only available in Advanced mode.

Automation and Control | General

Configuration

- **IP Port**: Defines which port the controller will use for communication with the automation service.
- **Encryption Level**: Defines the type of AES (Advanced Encryption Standard) that will be used.
- **Encryption Key**: If the Encryption level is set, defines the associated Key that will be used. For 128 bit encryption the Key should be exactly 16 characters long. For 192 bit encryption the Key should be exactly 24 characters long. For 256 bit encryption the Key should be exactly 32 characters long. The Key can be comprised of any combination of letters and numbers.
- **Checksum Type**: Defines the type of check sum that will be appended to the end of each Control packet. '8 bit sum' is a simple addition of all previous bytes in the packet. 16 bit CRC is a standard CRC (Cyclic Redundancy Check) based on the CRC-16-CCITT polynomial.

Options

- **Numbers are Big Endian**: When selected will send multi byte numbers with the most significant byte first.
- **Allow Status Requests When Not Logged In**: When selected the external process connecting to the service can request and receive status updates without needing to log in as a User. This does not allow the external process to send control commands. For example, a process that can monitor the state of an area while not logged, but in order to arm or disarm that area the process must log in.
- **Use Logon Lock Out Timer if Incorrect PIN is Supplied**: When selected the service will block further log in attempts if it receives three incorrect log in codes in a row. Further attempts will be blocked for 60 seconds.
- **Ack Commands**: Specifies whether the service should send an Acknowledge (or Ack) back after it receives a control command.
- **Expect Ack for Status Monitoring**: Specifies whether the service should expect an Acknowledge to be returned to it after it sends a status update to the external process. If selected, and no Ack is returned within three seconds then the Status update will be resent.
- **Resend Status Monitoring if not Ack after 5 Attempts**: If the Expect Ack for Status Monitoring option is selected, this option tells the service whether or not to abandon the transmission of the status if it has not received a response after 5 attempts. If enabled the service will keep trying until it receives an Ack. If not enabled the service will abandon the transmission of the current status update after 5 attempts, then begin trying to send the next status change.
- **Expect Ack for Events**: Specifies whether the service should expect an Acknowledge to be returned to it after it sends system events to the external process. If selected and no Ack is returned within three seconds then the system event will be resent.
- **Resend Events if not Ack after 5 Attempts**: If the Expect Ack for Events option is selected, this option tells the service whether or not to abandon the transmission of the system events if it has not received a response after 5 attempts. If enabled the service will keep trying until it receives an Ack. If not enabled the service will abandon the transmission of the current system event after 5 attempts, then begin trying to send the next system event.

C-Bus

The C-Bus service provides integration with building control and automation products using the Clipsal C-Bus protocol.

This is a licensed feature and only available in Advanced mode.

C-Bus | General

Configuration

- **CNI IP Address**: The IP address of the CNI (C-Bus Network Interface).
- **CNI Port**: The port that the CNI is located at.

- **Communication Failure Output**: The output to activate when the service's communications fail.
- **Communication Failure Output Group**: The output group to activate when the service's communications fail.

Options

- **Enable Text Output**: Skips the initialization of the PCI and sends the commands regardless of whether a CNI is connected or not. Used for debugging.
- **Add CR to Text Output**: Adds the Carriage Return character (0x0D) onto the end of text output.
- **Add LF to Text Output**: Adds the Line Feed character (0x0A) onto the end of text output.
- **Log C-BUS PCI Failure Message**: Logs events when the CNI initialization fails.
- **Log C-BUS ACK Message**: Logs events for each packet that is successfully exchanged with the CNI.
- **Log C-BUS Data Activity**: Logs events for each message packet that is sent to or received from the CNI.

Scheduling Menu

The Scheduling menu contains the functions relating to date and time information, including schedules and holiday groups.

This Option:	Is Used To:
Time	Set the current date and time
Holiday Groups	Configure holiday periods for use in schedules to prevent (or allow) periods within a schedule to function during the holiday duration
Daylight Savings	Define the daylight savings period associated with a controller
Schedules	Configure schedules for use by system controllers that enable a function or access level to operate only within certain scheduled periods

Time

Current Time and Date

- **Date**: The current date.
- **Time**: The current time.
- **Apply PC Time and Date Now**: When selected sets the current date and time to that of the PC being used.

Network Time

- **Automatically Synchronize with an Internet Time Server**: Select this option to automatically synchronize the controller with an internet time server.
- **Primary SNTP Time Server:** IP address of the primary SNTP time server for the controller to update its time from.
- **Secondary SNTP Time Server:** IP address of the secondary SNTP time server for the controller to update its time from should it not be able to connect to the primary SNTP server.
- **Time Zone:** The current time zone that should be assigned to the controller. Offset from GMT.

When using a time server the time provided is always in UTC (Coordinated Universal Time), which has no time zone and is not subject to any daylight saving time rules. This means that you must correctly configure the time server, the time zone that the controller is operating in, and the daylight savings settings for the time to be synchronized correctly. Failure to configure any of these will result in the time being inaccurate.

Holiday Groups

Holiday Groups are used to prevent (or allow) periods within a schedule from functioning during the holiday duration.

Select the **Holidays** tab to add holidays to the group.

- **Name:** The name of the holiday.
- **Repeat:** When enabled the holiday will recur on an annual basis.
- **Start Date:** The start date of the holiday.
- **End Date:** The end date of the holiday.

A maximum of 128 holidays can be added to a holiday group.

Daylight Savings

Daylight savings periods are associated with a controller. Programming the daylight saving settings in the Protege system allows the system to accurately compensate for daylight savings adjustments for the time zone the system controller is located in.

Configuration

- **Start Day:** Determines the date that daylight savings will start on.
- **Start Month:** Determines the month that daylight savings will start on.
- **End Day:** Determines the date that daylight savings will end on.
- **End Month:** Determines the month that daylight savings will end on.

Daylight Savings and Network Time Servers

When configuring daylight savings you must also ensure the controller is using the correct date and time. The exact steps required depend on whether you are using an Internet/Network Time Server.

Systems without a Time Server

After daylight savings has been programmed you may get an event that daylight savings has started or ended depending on the configured dates. You must then manually set the time of the controller to the correct value to ensure that the time is updated automatically the next time there is a shift in daylight savings.

1. Navigate to **Scheduling | Time**
2. Ensure the correct **Date** and **Time** is showing, and adjust if necessary.

Systems with a Time Server

If using a Time Server, the time provided is always UTC (Coordinated Universal Time) which has no time zone and is not subject to any daylight saving time rules. This means that you must correctly configure the daylight savings settings, the Time Server, **and** the time zone that the controller is operating in. Failure to configure any of these correctly will result in the time being inaccurate.

1. Navigate to **Scheduling | Time**
2. Ensure the IP address of the Time Server is set correctly and that the Time Zone selected matches the daylight savings period entered.

Schedules

Schedules enable a function or access level to operate only within certain scheduled periods. Each schedule contains up to 8 periods that can have various times and days programmed. Holiday groups can also be selected to allow a schedule to function when a holiday is active.

- **Name:** The name of the schedule.
- **Period 1-8**: Time periods for the schedule. Enter a start and finish time for each period and select which days you want the schedule to operate by checking the appropriate boxes.
- **Holiday Mode**: Defines how the schedule will operate during a holiday period. Choose from:
  - **Disabled on Holiday**: When selected the period will **not** make the schedule valid on a holiday. In other words, if a door is programmed to unlock by this schedule it will **not** unlock on a holiday if Disabled on Holiday is selected. This is the default mode of operation for schedules.
  - **Enabled on Holiday:** When selected the period will only ever make the schedule valid **on** a holiday.
  - **Ignore Holiday:** When selected the period will make the schedule valid **regardless** of whether the day is a holiday or not.
- **Graphics View**: The Graphics View provides a visual representation of the schedule periods. Each day of the week is represented by a 24 hour time line with the times when the schedule is active indicated by blue sections. The Graphics View is read-only and as such times cannot be adjusted from this screen.

Schedules | Options

- **Validate Schedule if Qualify Output On**: When enabled the schedule will only be valid while the qualify output is ON and all other time, day and holiday conditions are met.
- **Validate Schedule if Qualify Output Off**: When enabled the schedule will only be valid while the qualify output is OFF and all other time, day and holiday conditions are met.
- **Qualify Output**: The schedule can be qualified using an output. This means that even if the time, day and holiday conditions are met, the schedule will be considered invalid unless the qualify output also meets programmed conditions. This can be used to change the way a reader functions when the area arms. The qualify schedule output can be used to prevent access to a door if a specific output has been activated.

Schedules | Holiday Groups

Holiday Groups: The holiday groups for which the schedule is to apply. Select which holidays groups are required by clicking **Add** and selecting them from the list.

Expanders Menu

The Expanders menu contains the settings required to connect and configure the various expander modules available that extend your Protege WX system.

This Option:	Is Used To:
Keypads	Configure the keypads attached to your system
Analog Expanders	Configure the analog expanders used to connect industrial automation devices to your Protege WX system
Input Expanders	Configure the input expanders used to extend the number of inputs available within the system
Output Expanders	Configure the output expanders used to extend the number of outputs available within the system
Reader Expanders	Configure the reader expanders used to extend the number of reading devices and locking inputs available within the system
Smart Readers	Configure standalone locking devices and ICT RS-485 readers
Expander Addressing	View the hardware that is connected to the system network, and set the addresses of the modules that have auto-addressing capability

Keypads

Keypads are used for all functions within the Protege system and are typically located near an entrance or door to allow areas within the system to be armed and disarmed.

General

- **Name**: The name of the keypad.
- **Physical Address**: The network address of the keypad.

Display

- **Default Display Line One** defines the name or description displayed on line one of the keypad display, up to 16 characters. As this is what a user sees on a keypad it should be as descriptive as possible to ensure items are easily identifiable.
- **Default Display Line Two**: line two of the keypad display, as above.

Commands

- **Commands***: Used to send manual commands to a device.

Keypads | Configuration

Configuration

- **Area this LCD belongs to:** The primary area for the keypad is the area that the keypad will display first on all area display modes. The primary area should belong to the keypad's area group if any area actions are to be performed on the keypad.
- **Max Invalid PIN Entry Attempts**: Defines the maximum number of invalid PIN entries allowed before the user is locked out of the keypad.
- **Lockout Keypad Time (seconds)*:** If the **Lock Keypad On Excess Attempts** option (under Options 1) is enabled for the selected keypad and the maximum number of incorrect user codes is reached (3 times), the lockout time programmed here defines how long the keypad will be locked out. During this period the keypad will display the lockout message and ignore all key entries or login attempts by any user.
- **Door Connected to Keypad:** The door which is connected to the keypad.
- **Menu Group For This Keypad*:** Users can only access a menu assigned to the keypad if the same menu is also assigned to the user. This is also applicable if a menu is assigned to a user, but not to the keypad, the user cannot have access to the menu on the keypad.
- **Area Group for this Keypad:** Users can only access an area assigned to the keypad if the same area is also assigned to the user's arm and/or disarm area group.
- **Smoke Reset Output/Output Group:** The output (or output group) that is programmed as the keypad smoke detector reset output will be activated when a user presses the CLEAR + ENTER keys together.
- **Time User Is Logged In (seconds):** When the user does not perform any action on the keypad for the programmed time, the keypad will automatically log the user out. Programming the option 'Never Logout' should be avoided unless for training or demonstration purposes.

Keypads | Options 1

Display Options

- **Display Custom Message (lines 1 and 2):** When enabled the keypad will display the text programmed in the Controller settings.
- **Display Primary Area Status:** When enabled the keypad will display the status of the primary area that is assigned to the keypad.

- **Display Scrollable Area Group:** When enabled the keypad will display the status of the area's that are assigned in the area group.
- **Display Trouble Message:** When enabled the keypad will display the trouble input(s) when a failure has occurred.
- **Display Bypass Message:** When enabled the keypad will display the message input(s) bypassed when an input has been bypassed in the system or primary area if the Display Primary Area Messages Only option is also enabled.
- **Display Alarm Message:** When enabled the keypad will display the message alarm(s) in memory.
- **Display Primary Area Messages Only:** When enabled in conjunction with the Display Alarm Message option, the keypad will only display the bypassed input status and alarm memory for the primary area of the keypad. Setting this option means that only the primary area's alarms are shown, in which case the alarm message is cleared only if the primary area's memory is acknowledged. If this option is not enabled any area that has an alarm stored in memory is shown and all the area's memory must be acknowledged before this message is cleared.
- **Display Defer Area Warning Messages*:** When enabled the keypad will allow defer messages to be shown on the keypad for any area that is in the defer mode and the keypad is part of the defer warning keypad group.

Access Options

- **Function Key Unlocks Door When Logged In (REX):** When enabled allows the user to unlock the controlled door by pressing the FUNCTION key when they are logged in.
- **Keypad Can Access Only Primary Area:** When enabled the keypad will only allow the user to access the keypad's primary area.
- **Allow Area Group Selection Access:** When enabled the keypad will allow the area group access screen to be accessed by the user.
- **Allow 24HR Area Access:** When enabled the keypad will allow the 24HR status screen of an area to be accessed by the user. The user must have the 24HR menu option set.
- **Function Key Unlocks Door When Logged Out (REX):** When enabled allows the user to unlock the controlled door by pressing the FUNCTION key when they are logged out.
- **Auto Logout After User Arming:** When this option is enabled, the keypad will automatically log the user out when an area is successfully armed or disarmed. This can prevent third parties from accessing the keypad if the user forgets to log out.
- **Lock Keypad On Excess Attempts:** When enabled the keypad will lock if a user makes 3 invalid attempts to log on.
- **Activate Access Level Output*:** When enabled the keypad will activate the output assigned to the user's access level upon a valid user code being entered.

Keypads | Options 2

Offline Options

- **Allow Access to the Trouble View Menu:** When enabled the keypad will allow access to the View Trouble Menu if no user is logged in.
- **Allow Access to the Event Review Menu:** When enabled the keypad will allow access to the Event Review Menu if no user is logged in.
- **Allow Access to the Information Menu:** When enabled the keypad will allow access to the Keypad Information menu is no user is logged in.
- **Keypad Login Requires Card:** When enabled the keypad will require access card verification along with a user code before the user login can succeed.
- **Offline Access to Automation Menu*:** When enabled the keypad will allow access to the Automation Menu if no user is logged in.

In addition to the offline options outlined above, it is also possible to view any open inputs in the primary area in the offline menu, using the command `OfflineInputView = true`. To view all inputs in the primary area, also include the command `ClosedInputsInOfflineView = true`.

General Options

- **Disable the LCD Keypad Beeper:** When enabled the keypad will not beep when a key is pressed.
- **Duplex Inputs (4 Keypad Inputs):** When enabled the keypad will enable the Duplex Input option making it possible to connect four inputs to the keypad.
- **Beep On Communication Failure:** When enabled the keypad will beep on a communication failure.
- **Clear Key Can Disable Keypress Beeper:** When enabled the CLEAR key can disable the keypad beeper.
- **Virtual Module*:** When enabled a physical module cannot register at this address. This is used to protect inputs, outputs, etc. that are used by functions.

Output Options

- **Activate Access Level Output Only on Valid Access*:** When enabled the user's access level output will activate after they have logged into the keypad, only if they have a valid menu group and can remain logged in to the keypad.
- **Always Activate Access Level Output*:** When enabled the user's access level output will activate after they have logged into the keypad, even if they do not have a valid menu group or the ability to control other features through the keypad.

Analog Expanders

Analog Expanders are used to connect industrial automation devices to your Protege system.

Configuration

- **Invert Device Tamper**: When enabled the analog expander will invert the module tamper input allowing a normally open tamper switch to be used. When disabled the analog expander will use the standard normally closed tamper switch.
- **Virtual Module*:** When enabled a physical module can't register at this address. This is used to protect inputs, outputs, etc. that are used by functions. When disabled modules can register as normal.
- **Physical Address**: The device address of the Analog Expander.

Commands

- **Commands***: Used to send manual commands to a device.

Analog Expanders | Channel 1-4

This feature is only available in Advanced mode.

Options

- **Enable Channel:** When enabled the analog expander will process messages according to the options configuration and module type. When disabled the channel will perform no function.
- **Channel Uses 0-20mA Input (Disabled uses 0-10V):** When enabled the input or output will operate in Current Mode and use the 0-20mA or 4-20mA interface. When disabled the channel will operate in 0-10V input or output mode.
- **Preset DAC Output Power Up:** When enabled the analog expander module is a DAC module and the output will be preset when it powers up to the setting in Preset To 100 percent (Disabled Preset to 0). When disabled the DAC output will be set to the last known value that it received.
- **Preset To 100 percent (Disabled Preset to 0):** When enabled in conjunction with the Preset DAC Output Power Up option, the DAC output will be set to the maximum or full scale deflection. When disabled and the Preset DAC Output Power Up option is enabled, the DAC will output an analog value of 0 on the voltage or current outputs.
- **Send ADC Value In Diff Mode:** When enabled the Analog input channel will constantly monitor the analog input value for any variance greater than the configured differentiate value set for the channel and then send an update to the system controller. When disabled the Input Channel will be sent based on the period configured in the channel time setting.
- **Log Channel Data:** When enabled the analog expander channels, when updated either as an input or an output, will trigger a log in the event screen with the exact raw value. This is ideal for fault finding but should not be left on in a live system as it will fill the event review rapidly. When disabled the data is not logged to the review screen.

Channel Settings

- **Channel Update Time:** When the analog expander is used the channel will generate analog information that is stored in the variable associated with the analog expander. The data can be programmed to be set to various incremental values. As many elements that are monitored by sensors operate slowly, we recommend using the longest times possible. This also reduces the risk of disturbances due to interference as the input is averaged over the period of time being sampled.
- **Channel Diff Comparison Value:** The value that is configured is constantly monitored against the last value that is sent to the system controller, and if a change has occurred greater than the amount programmed and 'Send ADC Value in Diff Mode' is enabled for the channel, an update will be sent to the controller.

Input Expanders

Input Expanders extend the number of inputs available within the system.

Configuration

- **Physical Address**: The device address of the Input Expander.

Commands

- **Commands***: Used to send manual commands to a device.

Output Expanders

Output Expanders extend the number of outputs available within the system.

Configuration

- **Physical Address**: The device address of the Analog Expander.

Commands

- **Commands***: Used to send manual commands to a device.

Reader Expanders

Reader expanders extend the number of reading devices and locking inputs available within the system.

Configuration

- **Offline Operation**: This field defines how the reader expander will operate when it loses connection with the controller, enabling the reader to operate autonomously. The options are:
  - **No Users**: The reader expander will not grant access to any users.
  - **Any Card**: The reader expander will grant access to any card that can be read. This will allow anyone with a card in the correct format to gain access to the door, even if the card is not programmed in the system.
  - **First 10 Users Plus Cache**: When this option is enabled the reader expander will store a certain number of cards and grant access to those cards when it is offline. All other cards will be denied access.
    - The reader expander will grant access to the first 10 users downloaded to the controller. These are the first 10 users by database ID with access to anything on the controller, regardless of whether they have access to the doors on this expander. Only the first programmed card will be recognized.
    - In addition, the reader expander will store the most recent 150 cards which have gained access at this expander. These users will have access to both doors, regardless of their normal level of access.

  When the reader expander is offline, each time access is granted the reader will beep four times. PIN use is not supported by offline reader expanders, and all doors will allow card only access.
- **Slave Comm Operation**: This is a legacy option that has no effect.
- **Elevator Floor Split***: This is a legacy option that has no effect.
- **Physical Address**: The network address of the module on the controller network.

  The maximum physical address available for reader expander modules is 64.
- **Port 1/2 Network Type**: These fields determine how each reader port will operate (i.e. what kind of data it will send and receive). The options are:
  - **ICT RS-485**: Used for card readers wired in RS-485 configuration (recommended).
  - **Wiegand**: Used for any standard Wiegand reader.
  - **OSDP**: Used when connecting OSDP readers. When you select this option the system will automatically create two smart readers in **Expanders | Smart Readers** to represent the entry and exit OSDP readers on the port. For more information, see Application Note 254: Configuring OSDP Readers in Protege.
  - **Aperio**: Used to connect up to 15 Aperio communication hubs via RS-485, which can control up to 60 wireless locks (configured as smart readers). For more information, see Application Note 155: Protege WX Aperio RS-485 Hub Integration.
  - **Salto SALLIS**: Used to connect a SALLIS RS-485 router, which can control up to 16 wireless locks (configured as smart readers). For more information, see Application Note 140: Protege WX Salto SALLIS Integration.
  - **Allegion**: Used to connect Allegion PIMs (supporting up to 16 wireless locks) or wired locks. For more information, see Application Note 272: Allegion Integration with Protege WX.
  - **Third Party Generic**: This option allows you to configure the reader expander to recognize third-party readers or other generic sources of serial data on this reader port (See the **Third Party Generic** options in the **Reader 1/2** tab). For more information, see Application Note 218: Configuring Credential Types in Protege WX.
- **Ethernet Network Type**: When this reader expander record is used for the controller's onboard reader expander you can set the function of the ethernet port here. This is used when a third-party system is sending reader data to the controller. The options are:
  - **Disabled**: The ethernet port is not used for reader data. This does not affect the controller's connection to the IP network.

- **SALLIS**: Used to connect a SALLIS POE router, which can control up to 64 wireless locks (configured as smart readers). Smart readers are required to configure door control. For more information, see Application Note 140: Protege WX Salto SALLIS Integration.
- **Third Party Generic**: Allows you to connect custom data sources to the controller for use as readers, via the IP network. Any data input that can be configured as a credential type can be used, along with a smart reader to configure door control. For more information, see Application Note 218: Configuring Credential Types in Protege WX.

- **Ethernet Port**:
  - When the **Ethernet Network Type** above is set to Third Party Generic this field defines the TCP/IP port which the controller will communicate over. This port is used by smart readers to receive data from third-party 'readers'.
  - When the **Ethernet Network Type** above is set to SALLIS this field defines the port used to communicate with the SALLIS router.

  If the controller needs to listen on multiple ports for different data sources, enter the command `SmartReaderPortOffset = true` in the **Commands** field below. The port used by each smart reader corresponds to the **Ethernet Port** plus the **Configured Address** (**Expanders | Smart Readers | General**).
- **SALLIS Router IP**: When the **Ethernet Network Type** above is set to SALLIS this field defines the IP address used to communicate with the SALLIS router.

Options

- **Multiple Reader Input Port 1:** When enabled the reader will process the multiplexed reader inputs on Port 1 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader. When disabled the reader port 1 interface will operate as a single reader input. Only visible when the 'Port Type' is set to Wiegand.
- **Multiple Reader Input Port 2:** When enabled the reader will process the multiplexed reader inputs on Port 2 so that dual readers can be connected for entry and exit processing. The duplex reader that is connected will always operate as the exit reader. When disabled the reader port 2 interface will operate as a single reader input. Only visible when the 'Port Type' is set to Wiegand.

Ethernet Card Data Options

- **Card Data AES Encryption Key**: Salto SALLIS cards can be encoded with site/card information via the Encoder Client. This defines the decryption key used with these cards. This option only applies to the RS-485 implementation of SALLIS.

Commands

- **Commands***: Used to send manual commands to a device.

OSDP Install Mode

When the selected reader expander has at least one **Port 1/2 Network Type** set to OSDP the **OSDP Install Mode** icon in the toolbar will be enabled. If the selected reader expander does not have any ports configured for OSDP the icon is disabled and cannot be selected.

Click the **OSDP Install Mode** icon to put the reader expander into OSDP installation mode, allowing it to pair with any connected OSDP card readers which are also in installation mode. The reader expander and card reader will establish a shared encryption key to enable secure channel communication.

For more information, see Application Note 254: Configuring OSDP Readers in Protege.

Reader Expanders | Reader 1-2

Configuration

- **Reader Format:** The reading format used to inform the reader expander what type of card readers are connected to the reader port. The reader expander supports nearly all publicly available protocols and some special protocols. Any 26 or 37 bit card reader that conforms to the standard format specification will work on the Reader Expander.
- **Reader Location:** The reader location informs the reader expander which location of the door the reader is installed at, which is connected to the reader expander port. The reader expander uses this information to pass the correct direction of travel to the door control functions. For an access door this should be set to 'Entry' reader.

  When using the reader with a door that controls an inside or outside area for arming or disarming the ENTRY and EXIT configuration must be set correctly to ensure the correct action is taken by the reader expander.
  - **Exit**: The reader is located on the inside of the door and is used to exit out of the area that is being protected by the door.
  - **Entry**: The reader is located on the outside of the door and is used to enter in to the area that is being protected by the door. This is the default setting and should be set for all general access doors (single reader).

    If the reader expander is configured for multiplex reader mode the multiplexed reader is ALWAYS the EXIT reader.
- **Reader Mode:** The reader expander port mode.
  - **Access**: The reader expander port is used to control access through doors. You must configure the door that is controlled by this reader expander.
  - **Elevator***: The reader expander is used to control access to floors within an elevator. You must configure the elevator number that is connected to the reader.
  - **Area Control***: The reader expander input is used to ONLY control an area for arming and disarming. Please note that this can be achieved using the Access Mode as well by integrating the alarm and access control systems.
- **Reader Door:** The reader controlled door setting sets the door that the reader on port one will provide card and control information to. It is possible that more than one reader has the same controlled door (Entry and Exit reading configuration).
- **Reader Keypad Type:** The keypad operation mode programmed for the reader on a port determines if the reader port has a pin entry device attached or uses a local LCD keypad.
  - **LCD keypad**: This option allows you to associate an LCD keypad module with this reader port (the **Keypad to use for PINs reader 1/2** below). When a user badges at the reader the keypad will prompt them to enter their PIN and press the **[FUNCTION]** key to unlock the door.

    To unlock the door the user **must not press [ENTER]** after entering their PIN. The **[FUNCTION]** key must immediately follow the PIN code. If the user presses **[ENTER]** the keypad will log them in (see below).

    In addition, this option allows you to use two factor authentication for keypad access. This is required when **Keypad login requires card** (**Expanders | Keypads | Options 2**) is enabled. When the user badges their card they can enter their PIN and press **[ENTER]** to log in to the keypad.
  - **26 Bit (Site 0)**: A 26 Bit Wiegand Keypad is connected in parallel with the Reader Device and has a site code of 0 set for the unit.
  - **ARK-501**: A Motorola® Format the ARK-501 outputs 8 bits of data for each key that is pressed consisting of the first 4 bits being inverted from the remaining 4. This format requires the user to press the '#' key on completion of the PIN entry.
  - **4 Bit**: 4 Bits of data is output for each pressed key.
  - **4 Bit Parity**: 5 Bits of data is output for each pressed key with the last bit being ODD parity on the first 4 bits.
  - **4 Bit Buf**: The number of bits that are sent relate to the key presses multiplied by 4. The data is buffered and only sent when the user of the keypad press's the Enter key on the keypad.

- **4 Bit Buf and Par**: The number of bits that are sent relate to the key presses multiplied by 5. Each key press is 4 bits followed by a last parity bit. The data is buffered and only sent when the user of the keypad presses the Enter key on the keypad.
- **36 Bit (IEI Site 0)**: A 36 Bit Wiegand Keypad format typical of an IEI keypad which can be set to decode PIN numbers from 0-999999.
- **None**: There is no keypad device connected to or associated with this reader input device.

When a Wiegand 26 Bit or 36 Bit Keypad is used PIN numbers that are prefixed with a 0 cannot be used and a maximum pin number of 65533 can be used for 26 Bit and 999999 for 36 Bit. This is a limitation of the 26 Bit and 36 Bit Format and not the Reader Expander. To utilize the full 8 digit capacity for the PIN number of a user and allow prefixed PIN numbers select a PIN device that supports the ARK-501 or Bit Buffered Outputs.

- **Keypad to use for PIN's reader:** If the keypad operation mode is set to use one of the selected LCD keypads, you can program the address of the keypad to use for PIN entry. When using this mode of operation the LCD keypad will present a login message when a valid card is presented that requires PIN entry.
- **Reader Arming Mode:** The reader port can perform various operations when a user badges their card multiple times. The list below details the modes this can operate in.

  When a multi badge operation has taken place the reader expander will beep the buzzer output four times. In area control, if the area is already armed the reader will only beep twice.
  - **Do Nothing**: No action will be taken by the system for arming an area associated with the door.
  - **Arm Area on 2 Reads**: Two successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
  - **Read and Input 4 of Expander**: Pressing and holding Input 4 (RDXXX:04) while presenting a card will begin arming. Input 4 must be in an area that is armed to ensure the input information is transmitted to the system controller. The area armed will depend on the card reader type setting.

    This option cannot be used for the PRT-RDM2-DIN-485 as Input 4 is not available on that module. Use another arming method or use the PRT-RDS2 or PRT-RDI2.
  - **Arm Area on 3 Reads**: Three successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
  - **Toggle Function Output on 3 Reads**: Three successive reads from the same user will result in the function output state being toggled. If the output is currently on it will be turned off and if it is off it will be turned on.
  - **Activate Function Output on 3 Reads**: Three successive reads from the same user will result in the function output state being turned on.
- **Reader Area Control Area***: The reader controlled area setting sets the area that the reader on port one will control if the reader mode is set as area control. If area control is selected the reader cannot be used for other functions.
- **Reader Elevator***: The reader elevator car is used when the reader port 1 mode of operation is configured for Elevator Control mode. When configuring the elevator control mode you must also configure the elevator number for the reader expander that the floor control relays are located on. This is typically the same reader expander that the card reader is connected to.
- **Reader Secondary Format:** The secondary reading format is used to program an alternate format for the reader expander and has the same options as the standard reader selection. The secondary format will only be used if the first format cannot decode the card information that is received by the reader interface.
- **Reader Function Output/Output Group***: The output/output group that the reader expander port is associated with.
- **Dual Authentication Pending Output**: Defines the output that activates when the first credential is presented.
- **Dual Authentication Wait Time**: Defines the maximum time allowed between presenting the two credentials.

Reader Options

- **Allow Reading Opened/Unlocked:** When enabled the reader expander will send card information to the system controller when a door is unlocked or opened. This option is set by default and should be left set if the door control areas or time and attendance events are required from the reader port. When disabled the reader performs no action when a card is presented and the door is unlocked or opened.

- **Send Format Errors:** When enabled the reader expander will send detailed format errors to the system controller if it receives information from the reader that does not comply with programmed format. Format errors include bit count, byte count, parity, checksum and LRC calculation failures. When disabled the reader will silently discard any format error. The format error will still be indicated on the reader input data LED.
- **Intelligent Reader Tamper Mode:** When enabled the reader expander will assume that the external device has smart messaging that allows a communication path to be formed from the reading devices (card reader) to the reader expander. When disabled the intelligent reader mode is disabled.

Card Data Options

- **Card Data AES Encryption Key**: Salto SALLIS cards can be encoded with site/card information via the Encoder Client. This defines the decryption key used with these cards. This option only applies to the RS-485 implementation of SALLIS.

Misc Options

- **Disarm Area For Door On Access:** When enabled the reader process will disarm the area designated by the reader type (Entry or Exit) and the door configuration programmed (if it has an area on the inside or outside assigned). When disabled the reader will not perform any disarm functions.
- **Allow Access When Area Armed:** When enabled the user will be granted access based on the access control configuration only and the area status will not be checked against the user's ability to disarm the area. When the option is disabled and the user who is attempting access to a door that has an area assigned that is armed, and the user cannot disarm the area, the user will be denied entry to the door even though they may have the correct door and schedule settings.
- **Disarm Users Area On Valid Card**: When enabled the reader will disarm the user's area when access is granted to the door they are attempting to access. The users must still be available in the user area group assigned to the user's access level. When disabled the reader will not perform any user area functions.
- **Log Reader Events:** When enabled the reader events will be logged to the event review log. When disabled the reader will not log the events to the event review log.
- **Swap lock LED display**: This option is not used.
- **Activate Access Level Output:** When enabled the reader expander will activate the output assigned to the user's access level that gained access to the door or reader. When disabled the reader will not perform any action on the access level output. For this option to work, the Reader Access Activates Output option must be enabled under Users | Access Levels.
- **Display Card Detail When Invalid:** When enabled the reader expander will display the actual card data received from the reader when the card number is not known. This option is enabled by default and can be used to identify facility and card number details before adding card data to a user. When disabled the reader will display the card number not found message.
- **Arm Users Area**: When enabled the reader will arm the user's area when they perform a dual presentation of their card to the associated reader. The user's area must still be available in the user area group assigned to the user's access level for this to correctly operate. When disabled the reader will not perform any user area arming functions.
- **Enable Enhanced Smart Reader Outputs**: When enabled allows for control of LED and buzzer outputs of an RS-485 reader as independent outputs when connected to the specified reader port.

Reader Expanders | Reader 1-2 Options

Options

- **Invert Floor Relays:** This is a legacy option which does not function. If necessary, relays assigned to elevator control can be inverted individually under **Programming | Outputs | Options**.
- **Control Relays On Comm Failure*:** When enabled the output expander used for elevator control will control the state of the relays when they go offline. When disabled the output expander used for elevator control will not change the state of the relays when they go offline.

- **Relays Activated In Comm Failure***: When enabled the output expander will activate the relays when they go offline. When disabled the output expanders will deactivate the relays when they go offline.
- **Disable Red LED Processing:** When enabled the reader expander will not control the Red LED (L2) and the output can be used for another function. This is particularly useful if the attached proximity reader LED's is controlled with one wire. When disabled the reader will turn on the Red LED when the door is locked.
- **Disable Green LED Processing:** When enabled the reader expander will not control the Green LED (L1) and the output can be used for another function. This is particularly useful if the attached proximity reader LED's is controlled with one wire. When disabled the reader will turn on the Green LED when the door is unlocked.
- **Disable Buzzer Processing:** When enabled the reader expander will not control the Buzzer Output (BZ) and the output can be used for another function. When disabled the reader will control the buzzer output.
- **Use Programmed Card Expiry:** Used for short term users (such as visitors or hotel guests) that will be configured with a start (check in) and end (check out) time. These options are designed to work with Hotel card readers and allow the reader port to alter the access control decision of a user based on the data sent from the guest card.

Offline Options

- **Door Sense Enabled:** When enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control). This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the Door Sense function for normal operation refer to the Inputs tab of the Doors menu.
- **Bond Sense Input Enabled:** Enables the magnetic bond sense functions. The magnetic bond sense is a contact that indicates if the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used and the generation of door events should be processed using both inputs. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the Bond Sense function for normal operation refer to the Inputs tab of the Doors menu.
- **REX Enabled:** When enabled the reader expander will generate request to exit events from the REX input on the reader expander. When disabled the keypad will not generate any REX events. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the REX function for normal operation, refer to the Inputs tab of the Doors menu.
- **REN Enabled:** When enabled the reader expander will generate request to enter events from the REN input on the reader expander. When disabled no action will be taken for the Request To Enter function. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the REN function for normal operation refer to the Inputs tab of the Doors menu.
- **Enable Beam Function On Input:** When enabled the reader expander will process the sense input for beam control. Beam control allows the reader expander to control an automatic gate which must have its contacts held open even if the pathway is blocked. When disabled the reader will not perform beam processing.
- **Invert Door State Control:** When enabled the door contact input is inverted. This does not affect the input functionality if it is being used. When disabled door contact functions normally.
- **Invert Sense State Control:** When enabled the reader will invert the bond sensing input. When disabled bond sensing will operate normally.
- **Invert REX Input:** When enabled the reader will invert the request to exit input. When disabled REX input will operate normally.
- **Invert REN Input**: When enabled the reader will invert the request to enter input. When disabled REN input will operate normally.
- **Always Allow REX:** When enabled the reader will always allow a request to exit event even if the door is forced open. This will not restart the forced door or the door alarm operation. When disabled REX input will operate only when the door is closed.
- **Recycle Door Open Time on REX:** When enabled the reader will extend the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the request to exit once the door has been open too long will require that the door be

closed. This option will not affect the ability for the request to exit action to unlock the door. When disabled REX input will not alter the door open time once the door has been opened.

- **Forced Door Sends Door Open:** When enabled the reader expander will process door forced open events as door open events. When disabled the reader will process forced door events as normal.
- **Recycle REX Time**: When enabled the door open time will restart when the door is held open and the REX is pressed at each point the pre-alarm starts, silencing the pre-alarm and restarting the open timer. This allows a door to be held while furniture is being moved or to provide extended access for mobility users.

Reader Expanders | Reader 1-2 PIM Config

Panel Interface Modules (PIMs) and ENGAGE Gateways (GWEs) are used as the communication interface between wireless locks and Protege controllers for Allegion wireless locking integration. These tabs allow you to add and configure the PIMs and GWEs connected to the reader expander ports for the integration.

These tabs are only visible when the corresponding **Reader 1/2 Network Type** is set to Allegion. For more information and programming instructions, see Application Note 272: Allegion Integration with Protege WX.

Configuration

- **PIM Address**: The address of the PIM/GWE connected to the reader port.
- **APM Start Address**: This defines the value set for the Low APM Range of the PIM/GWE connected to the reader port, which determines the address of the first wireless lock assigned to the device.
- **Number Of APMs**: Defines the number of wireless locks connected to the PIM/GWE.

  A maximum of 16 locks can be connected to a PIM. A maximum of 10 locks can be connected to a GWE.

Smart Readers

Smart readers can be wireless locking devices or ICT RS-485 readers.

Configuration

- **Expander Address**: The address of the reader expander that the smart reader is connected to.
- **Expander Port**: The reader port used by the smart reader.
- **Configured Address**: The address assigned to the smart reader.
- **Linked RSD Address**: Used for Allegion wireless lock integrations to define the **PIM Address** of the PIM record that the lock is linked to.

  For more information and programming instructions, see Application Note 272: Allegion Integration with Protege WX.

Commands

- **Commands***: Used to send manual commands to a device.

Smart Readers | Reader

Smart Readers can be wireless locking devices or RS-485 readers.

Configuration

- **Reader Format:** The reading format used to inform the reader expander what type of card readers are connected to the reader port.
- **Reader Location:** The reader location informs the reader expander which location of the door the reader is installed at, which is connected to the reader expander port. The reader expander uses this information to pass the correct direction of travel to the door control functions. For an access door this should be set to 'Entry' reader.

  When using the reader with a door that controls an inside or outside area for arming or disarming the ENTRY and EXIT configuration must be set correctly to ensure the correct action is taken by the reader expander.

  - **Exit**: The reader is located on the inside of the door and is used to exit out of the area that is being protected by the door.
  - **Entry**: The reader is located on the outside of the door and is used to enter in to the area that is being protected by the door. This is the default setting and should be set for all general access doors (single reader).

  If the reader expander is configured for multiplex reader mode the multiplexed reader is ALWAYS the EXIT reader.
- **Reader Mode:** The reader expander port mode.
  - **Access**: The reader expander port is used to control access through doors. You must configure the door that is controlled by this reader expander. This mode should also be used if control of a lobby or elevator call button is required. To control an elevator car use the Elevator Mode.
- **Reader Door:** The reader controlled door setting sets the door that the reader on port one will provide card and control information to. It is possible that more than one reader has the same controlled door (Entry and Exit reading configuration).
- **Reader Keypad Type:** The keypad operation mode programmed for the reader on a port determines if the reader port has a pin entry device attached or uses a local LCD keypad.
  - **LCD Keypad**: An LCD keypad is used for PIN entry. PIN entry is only possible with the Card and PIN configuration when using an LCD Keypad. To unlock in the PIN Only or Card or PIN modes the unlock shortcut key can be used. The LCD Keypad Address is configured in the next screen.

- **LCD keypad**: This option allows you to associate an LCD keypad module with this reader port (the **Keypad to use for PINs reader** below). When a user badges at the reader the keypad will prompt them to enter their PIN and press the **[FUNCTION]** key to unlock the door.

  To unlock the door the user **must not press [ENTER]** after entering their PIN. The **[FUNCTION]** key must immediately follow the PIN code. If the user presses **[ENTER]** the keypad will log them in (see below).

  In addition, this option allows you to use two factor authentication for keypad access. This is required when **Keypad login requires card** (**Expanders | Keypads | Options 2**) is enabled. When the user badges their card they can enter their PIN and press **[ENTER]** to log in to the keypad.
- **26 Bit (Site 0)**: A 26 Bit Wiegand Keypad is connected in parallel with the Reader Device and has a site code of 0 set for the unit.
- **ARK-501**: A Motorola® Format the ARK-501 outputs 8 bits of data for each key that is pressed consisting of the first 4 bits being inverted from the remaining 4. This format requires the user to press the '#' key on completion of the PIN entry.
- **4 Bit**: 4 Bits of data is output for each pressed key.
- **4 Bit Parity**: 5 Bits of data is output for each pressed key with the last bit being ODD parity on the first 4 bits.
- **4 Bit Buf**: The number of bits that are sent relate to the key presses multiplied by 4. The data is buffered and only sent when the user of the keypad presses the Enter key on the keypad.
- **4 Bit Buf & Par**: The number of bits that are sent relate to the key presses multiplied by 5. Each key press is 4 bits followed by a last parity bit. The data is buffered and only sent when the user of the keypad presses the Enter key on the keypad.
- **36 Bit (IEI S0)**: A 36 Bit Wiegand Keypad format typical of an IEI keypad which can be set to decode PIN numbers from 0-999999.

  When a Wiegand 26 Bit or 36 Bit Keypad is used PIN numbers that are prefixed with a 0 cannot be used and a maximum pin number of 65533 can be used for 26 Bit and 999999 for 36 Bit. This is a limitation of the 26 Bit and 36 Bit Format and not the Reader Expander. To utilize the full 8 digit capacity for the PIN number of a user and allow prefixed PIN numbers select a PIN device that supports the ARK-501 or Bit Buffered Outputs.

- **Keypad to use for PINs reader:** If the keypad operation mode is set to use one of the selected LCD keypads you can program the address of the keypad to use for PIN entry. When using this mode of operation the LCD keypad will present a login message when a valid card is presented that requires PIN entry.
- **Reader Arming Mode:** The reader port can perform various operations when a user badges their card multiple times. The list below details the modes this can operate in.

  When a multi badge operation has taken place the reader expander will beep the buzzer output four times. In area control if the area is already armed the reader will only beep twice.
  - **Do Nothing**: No action will be taken by the system for arming an area associated with the door.
  - **Arm Area on 2 Reads**: Two successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
  - **Read and Input 4 of Expander**: Pressing and holding Input 4 (RDXXX:04) while presenting a card will begin arming. Input 4 must be in an area that is armed to ensure the input information is transmitted to the system controller. The area armed will depend on the card reader type setting.

    This option is not available for the PRT-RDM2-DIN-485, as Input 4 is not available on that module. Use another arming method, or use the PRT-RDS2 or PRT-RDI2.
  - **Arm Area on 3 Reads**: Three successive reads from the same user will result in the inside or outside area (depending on the card reader type configuration) starting the arming process.
- **Reader Area Control Area:** The reader controlled area setting sets the area that the reader on port one will control if the reader mode is set as area control. If area control is selected the reader cannot be used for other functions.
- **Reader Elevator:** The reader elevator car is used when the reader port 1 mode of operation is configured for Elevator Control mode. When configuring the elevator control mode you must also configure the elevator

number for the reader expander that the floor control relays are located on. This is typically the same reader expander that the card reader is connected to.

- **Reader Secondary Format:** The secondary reading format is used to program an alternate format for the reader expander and has the same options as the standard reader selection. The secondary format will only be used if the first format cannot decode the card information that is received by the reader interface.
- **Reader Function Output/Output Group:** The output or output group which the reader expander port is associated with.

Reader Options

- **Allow Reading Opened/Unlocked:** When enabled the reader expander will send card information to the system controller when a door is unlocked or opened. This option is set by default and should be left set if the door control areas or time and attendance events are required from the reader port. When disabled the reader performs no action when a card is presented and the door is unlocked or open.
- **Door Sense Enabled:** When enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control).
- **Bond Sense Input Enabled:** Enables the magnetic bond sense functions. The magnetic bond sense is a contact that indicates if the magnetic bond between the electromagnet and the clamp is complete. It is used when a separate door contact and bond sense input are to be used and the generation of door events should be processed using both inputs.
- **REX Enabled:** When enabled the reader expander will generate request to exit events from the REX input on the reader expander. When disabled the keypad will not generate any REX events.
- **REN Enabled:** When enabled the reader expander will generate request to enter events from the REN input on the reader expander. When disabled no action will be taken for the Request To Enter function.
- **Intelligent Reader Tamper Mode:** When enabled the reader expander will assume the external device has smart messaging, allowing a communication path to be formed from the reading devices (card reader) to the reader expander. When disabled the intelligent reader mode is disabled.
- **Send Format Errors:** When enabled the reader expander will send detailed format errors to the controller if it receives information from the reader that does not comply with programmed format. Format errors include bit count, byte count, parity, checksum and LRC calculation failures. When disabled the reader will silently discard any format error. The format error will still be indicated on the reader input data LED.

Misc Options

- **Disarm Area For Door On Access:** When enabled the reader process will disarm the area designated by the reader type (Entry or Exit) and the door configuration programmed (If it has an area on the inside or outside assigned). When disabled the reader will not perform any disarm functions.
- **Allow Access When Area Armed:** When enabled the user will be granted access based on the access control configuration only and the area status will not be checked against the user's ability to disarm the area. When the option is disabled and the user attempts access to a door with an area assigned that is armed, and the user cannot disarm the area, the user will be denied entry to the door even though they may have the correct door and schedule settings.
- **Disarm Users Area On Valid Card:** When enabled the reader will disarm the user's area when access is granted to the door they are attempting to access. The users must still be available in the user area group assigned to the user's access level. When disabled the reader will not perform any user area functions.
- **Log Reader Events:** When enabled the reader events will be logged to the event review log. When disabled the reader will not log the events to the event review log.
- **Swap lock LED display**: This option is not used.
- **Activate Access Level Output:** When enabled the reader expander will activate the output assigned to the user's access level that gained access to the door or reader. When disabled the reader will not perform any action on the access level output.
- **Display Card Detail When Invalid:** When enabled the reader expander will display the actual card data received from the reader when the card number is not known. This can be used to interface with custom third-

party applications that require their own processing of card information. This option is enabled by default and can be used to identify facility and card number details before adding card data to a user. When disabled the reader will display the message: card number not found.

- **Enable Beam Function on Input:** When enabled the reader expander will process the sense input for beam control. Beam control allows the reader expander to control an automatic gate which must have its contacts held open even if the pathway is blocked. When disabled the reader will not perform beam processing.
- **Always Allow REX:** When enabled the reader will always allow a request to exit event even if the door is forced open. This will not restart the forced door or the door alarm operation. When disabled REX input will operate only when the door is closed.
- **Recycle REX Time:** When enabled the door open time will restart when the door is held open and the REX is pressed at each point the pre-alarm starts, silencing the pre-alarm and restarting the open timer. This allows a door to be held while furniture is being moved or to provide extended access for mobility users.

Expander Addressing

The Expander Addressing option is used to view the hardware connected to the system network and to set the addresses (see page 153) of the modules that have auto-addressing capability. This page displays the details of all modules currently connected or that have registered previously but may currently be offline.

Listed for each module is:

- The module type
- The serial number
- Current firmware version
- The current address of the module
- Whether the module is registered with the Controller
- Whether the module is currently online

Automation Menu

This feature is only available in Advanced mode.

Functions relating to building control and automation are found under the Automation menu.

This Option:	Is Used To:
Automation	Configure automation points used to control devices that are required to be operated regularly, such as lighting or HVAC systems
Programmable Functions	Configure programmable functions to perform special processing of actions when a particular event or operation occurs, such as unlocking doors in the event of a fire alarm

Automation | General

Automations are used to control devices that are required to be operated regularly by a user. For example outdoor lighting, irrigation or HVAC (heating ventilation and air conditioning) systems can be connected to automation outputs.

Configuration

- **Automation Output Time:** You can override the programmed activation time for an output or the group of outputs by setting an activation time.
- **Automation Output/Output Group:** The automation entry will control the output or output group that is assigned to the control output option.
- **C-Bus Application Code:** The Clipsal C-Bus application number is used to link this automation point to a C-Bus Application that is communicating with the system controller. For example if you want to link this automation point to activate when a Lighting, Switching and Load Control application command is generated for a particular Group Address set the Application Type to 056 (056 or $38 Hex is the Lighting, Switching and Load Control application. Refer to the Clipsal C-Bus Application Specifications and related documents).
- **C-Bus Group Code:** The Clipsal C-Bus group address is the number used to identify the group within the C-Bus network. This typically ranges from 0-255. A group allows any output in the Protege system to either control a C-Bus group as the result of a change within the system or to change based on a C-Bus group being activated. For example when a user presses a Goodbye Button on a C-Bus keypad this can activate an output that is used to ARM an Area in the Protege system. The outputs can also be used to allow doors to Unlock/Lock based on the C-Bus events.

Automation | Options

- **Display Inverted Status:** When enabled the Automation display will show the automation status as inverted. Set this option when an output or output group operates inverted to the normal state.
- **Enable C-Bus Automation Functions:** When enabled the Automation point will be included in the C-Bus processing and used to control or be controlled by a C-Bus automation point.
- **C-Bus Automation Output:** When enabled the Automation point will generate a C-Bus message on the C-Bus system when the status of the Automation point changes. For example manually controlling the Automation point will send the Application Id and Group Address to the C-Bus interface.
- **Use Output Status In C-Bus Function:** When enabled the Automation point will use the programmed output directly rather than using the automation point status or setting. This allows any output in the system to be programmed for the automation point without it actually being controlled by the automation point.
- **C-Bus Operates On Rising Edge:** When enabled the C-Bus processing will only activate on the rising edge of a change in the Automation Point or output state. For example the Automation point changing from Off to On.
- **C-Bus Operates On Falling Edge:** When enabled the C-Bus processing will only activate on the falling edge of a change in the Automation Point or output. For example the Automation point changing from On to Off.

Programmable Functions

Programmable functions are used to perform special processing of actions when a particular event or operation occurs. For example unlocking doors in the event of a fire alarm. Functions are a vital component of the Protege system and allow many variations of logic, process and automation to be performed.

Type

- **Type:** The type of function that is programmed will determine the operation that this function will perform. This will also determine the programming screens that follow in each of the sub sections as the programming of functions can contain many features and options dependent on this selection. The following section includes an explanation of each function type that is programmable in the Protege system.
  - **None:** The function will perform no actions and controls no resources. This function cannot be started or halted.
  - **Logic Control:** Performs logic operations on Programmable Outputs. Can be used to AND, OR, XOR, FOLLOW, NOT FOLLOW the programmable outputs and activate a programmable output as a result of function. When using logic control that will follow a status the system will activate the associated output as a result of the logic function. However if the output is changed from the state it will be updated 30 seconds later. This prevents endless loops from occurring while still ensuring an output will result in it being maintained.
  - **Area Control:** Can be used to arm or disarm an area based on the status of an output. This can only check the area status in follow mode every 60 seconds.
  - **Ripple Output:** Ripples on and ripples off up to 8 outputs from an enabled output. Ideal for staging on large current devices and multiple lighting circuits.
  - **Door Control:** Can be used to lock and unlock a door or door group based on the status of an input.
  - **Virtual Door:** Enables setup of defined inputs and outputs to operate as a door.
  - **Input Follows Output:** Enables an input to be controlled using an output.
  - **Elevator Control:** Can be used to lock or unlock elevator floors based on the state of an output.
- **Mode:** The mode determines how this function operates with the system controller. By default a function is set to Normal operation. Normal operation will mean the function is started if it was running when the system restarts or is completely powered down (AC Failure and Battery Failure). The Run Once mode of operation will mean the function will only run once and then wait to be stopped and started by the user or operator.
- **State**: Used to set the state of the programmable function (Running or Halted).

Logic Control

Logic Control is used to perform logic operations such as OR, AND, NOR, NAND, XOR and Follow on outputs. Logic Control evaluates the states of one or two outputs (depending on the selected function mode) and controls a single output or an output group as a result.

- **Logic Function Mode:** All control functions have a Function Mode which defines how the controlled output/output group is evaluated. There are eleven different options for the logic control function.
  - **Follow and Test**: This mode is used when the function requires the controlled output to mimic the checked output and follow any state changes. In between state changes the controlled output state is continually tested at approximately 30 second intervals. If the controlled output state has been changed by an external operation the programmable function will update its state.
  - **Inverted Follow and Test:** This mode is used when the function requires the controlled output to do the opposite of the checked output. In between state changes the controlled output state is continually tested at approximately 30 second intervals. If the controlled output state has been changed by an external operation the programmable function will update its state.
  - **Follow Pulse On**: This function will turn the controlled output ON only when the checked output transitions from an OFF to an ON state. No further testing of the output states will occur, allowing full control by other functions, processes and manual control commands.

- **Inverted Follow Pulse On:** This function will turn the controlled output ON only when the checked output transitions from an OFF to an ON state. No further testing of the output states will occur, allowing full control by other functions, processes and manual control commands.
- **Follow Pulse Off**: This function will turn the controlled output OFF only when the checked output transitions from an ON to an OFF state. No further testing of the output states will occur, allowing full control by other functions, processes and manual control commands.
- **Inverted Follow Pulse Off**: This function will turn the controlled output OFF only when the checked output transitions from an ON to an OFF state. No further testing of the output states will occur, allowing full control by other functions, processes and manual control commands.
- **Follow Logic OR**: This function will perform a logical OR operation on output 1 and 2 with the controlled output changing state according to the result. This function will result in the controlled output turning on if at least 1 of the checked outputs is on. The controlled output will only turn off if both of the checked outputs are off.
- **Follow Logic AND:** This function will perform a logical AND operation on output 1 and 2 with the controlled output changing state according to the result. The controlled output will only be turned on if both of the checked outputs are also on. The controlled output will be turned off if either/both of the checked outputs are off.
- **Follow Logic NOR:** This function will perform a logical NOR operation on output 1 and 2 with the controlled output changing state according to the result. The controlled output will only be turned on if both of the checked outputs are off. The controlled output will be turned off if either of the two checked outputs are turned on.
- **Follow Logic NAND:** This function will perform a logical NAND operation on output 1 and 2 with the controlled output changing state according to the result. The controlled output will be turned on if none, or only 1 of the checked outputs is on. If both of the checked outputs are on, the controlled output will be turned off.
- **Follow Logic XOR:** This function will perform a logical XOR operation on output 1 and 2 with the controlled output changing state according to the result. The controlled output will be turned on if only 1 of the checked outputs is on. The controlled output will be turned off if both or neither of the checked outputs are off.

- **First Output to Check**: Defines the first checked output for the logic process that is being programmed. All logic control functions use at least 1 output. The output selected must be valid.
- **Second Output to Check**: Defines the output for the logic process that is being programmed when 2 outputs are used to control another output.
- **Output to Control**: Defines the output to control as a result of the logic function.
- **Output Group to Control**: Defines the output group to control as a result of the logic function. Selecting both an output and an output group will result in only the output being controlled and the output group being ignored.

Area Control

The Area Control function can be used to arm or disarm an area based on the status of an output.

- **Area Function:** The Area Function determines what action is performed on the area or area group as a result of the output changing state. For key switch arming or simple arming of an area from an input use the area control options in the input type configuration.
  - **Follow and Test Output:** The area/area group's status follows the programmed output's state. If the output turns on the controlled area/area group will arm, and if the output turns off the controlled area/area group will disarm. In between state changes the controlled area/area group state is continually tested at approximately 30 second intervals. If the area/area group's state has been changed by an external operation the programmable function will restore it.
  - **Inverted Follow and Test Output:** Performs the same function as above however the output is inverted (NOT). If the output turns on the controlled area/area group will disarm, and if the output turns off the controlled area/area group will arm. In between state changes the controlled area/area group state is

continually tested at approximately 30 second intervals. If the controlled area/area group's state has been changed by an external operation the programmable function will restore it.

- **Follow Pulse On Output**: This function arms the controlled area/area group only when the checked output transitions from an OFF to an ON state, As the Follow Pulse On function is only evaluated at the ON edge, when the output turns off the area/area group will not be disarmed.
- **Inverted Follow Pulse On Output**: This function disarms the controlled area/area group only when the checked output transitions from an OFF to an ON state. As the Inverted Follow Pulse On function is only evaluated at the ON edge, when the output turns off the area/area group will not be armed.
- **Follow Pulse Off Output**: This function arms the controlled area/area group only when the checked output transitions from an ON to an OFF state. As the Follow Pulse Off function is only evaluated at the OFF edge, when the output turns on the area/area group will not be disarmed.
- **Inverted Follow Pulse Off Output:** This function disarms the controlled area/area group only when the output transitions from an ON to an OFF state. As the Inverted Follow Pulse Off function is only evaluated at the OFF edge, when the output turns on the area/area group will not be armed.

- **Output to Check:** Defines the output that the area control function will check.
- **Area to Control:** Defines the area to control as a result of the action being performed by the programmable function.
- **Area Group to Control**: Defines the area or area group that can be controlled by the output. Selecting both an area and an area group will result in only the area being controlled and the area group being ignored.

Ripple Output

Ripples on and ripples off up to 8 outputs from an enabled output. Ideal for staging on large current devices and multiple lighting circuits.

- **Output to Enable this Function:** When enabled the control output is used to operate the ripple output function in the STEP UP mode when it is activated, and in the STEP DOWN mode when the Enable Output is deactivated. If no enabled output is set the function will never run the ripple stages.
- **Stage 1 Output/Output Group:** The first output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 2 Output/Output Group:** The second output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 3 Output/Output Group:** The third output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 4 Output/Output Group:** The fourth output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 5 Output/Output Group:** The fifth output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 6 Output/Output Group:** The sixth output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 7 Output/Output Group:** The seventh output in the 8 outputs that can be programmed for the ripple control function.
- **Stage 8 Output/Output Group:** The eighth output in the 8 outputs that can be programmed for the ripple control function.
- **Inter Stage On Ripple Time:** The ripple on time determines the time that each output will be delayed before being activated when the ripple control function is stepping the outputs up.
- **Inter Stage Off Ripple Time:** The ripple off time determines the time that each output will be delayed before being deactivated when the ripple control function is stepping the outputs down.

Door Control

The Door Control function can be used to lock and unlock a door or door group based on the status of an output.

- **Door Function Mode**: The function mode determines what action is performed on the door or door group that is programmed as a result of the output state. A function mode MUST be selected for the programmable function to operate correctly. The actions performed on the door will vary based on the Door Control Mode.
  - **Follow and Test Output:** This mode is used when the state of the door is required to follow the state of the checked output. If the checkout output turns on the controlled door/door group will unlock (or lock down), and if the checkout output turns off the controlled door/door group will lock (or clear the lockdown). In between state changes the door/door group's state is continually tested at approximately 30 second intervals. When the door/door group's state is changed by an external operation the programmable function will restore it.
  - **Inverted Follow and Test Output:** This is the same as the Follow and Test Output function, however the output is inverted (NOT). If the checked output turns on the controlled door/door group will lock (or clear the lock down), and if the checked output turns off the controlled door/door group will unlock (or lockdown). In between state changes the door/door group's state is continually tested at approximately 30 second intervals. When the controlled door/door group's state is changed by an external operation the programmable function will restore it.
  - **Follow Pulse On Output:** The Follow Pulse On Output action will unlock (or lockdown) the door only when the checked output has transitioned from an OFF to an ON state. When the checked output turns off the door state will not change as this function is only evaluated at the ON edge.
  - **Inverted Follow Pulse On Output:** The Inverted Follow Pulse On Output action will lock the door (or clear the lockdown) only when the output one has transitioned from an OFF to an ON state. When the checked output turns off the door state will not change as this function is only evaluated at the ON edge.
  - **Follow Pulse Off Output**: The Follow Pulse Off Output action unlock or lockdown the controlled door only when the checked output has transitioned from an ON to an OFF state. When the checked output turns off the state of the door will not change as this function is only evaluated at the OFF edge.
  - **Inverted Follow Pulse Off Output:** The Inverted Follow Pulse Off Output action will lock or clear the lockdown on the controlled door only once the checked output has transitioned from an ON to an OFF state. When the checked output turns off the state of the door will not change as this function is only evaluated at the OFF edge.
- **Door Control Mode:** The control mode sets how the door/door group will be controlled. This allows a door/door group to be unlocked for the door unlock time, unlock latched, or unlocked in the fire alarm mode. This must be selected for the programmable function to operate properly.
  - **Emulate Unlock Menu:** With the Emulate Unlock Menu mode selected the door will be unlocked for the duration of the Lock Activation Time programmed from the Protege WX interface when the output changes state. This has the same effect as a valid card badge or REX.

    This mode will only function correctly when used with any of the Pulse function modes. Using this mode with a Follow and Test function mode will result in a latching behavior.
  - **Latch Door Unlock:** The door will be latched in the unlocked state and will remain unlocked until controlled from:
    - A Keypad
    - The Protege interface
    - Scheduled Action
    - Change in Area State
    - A Programmable Function.
  - **Fire Control Door Unlock:** The door will be latched in the fire control unlock state and will remain unlocked until controlled from:
    - A Keypad
    - The Protege interface
    - A Programmable Function that is programmed to deactivate the fire alarm control.

    This mode is a higher priority version of the Latched Unlock mode.
  - **Door Lockdown (Deny Entry + Exit):** This mode forces all unlocked doors to lock. Entry and Exit requests are denied.

- **Door Lockdown (Allow Entry):** This mode forces all unlocked doors to lock. Entry is allowed. Exit is denied.
- **Door Lockdown (Allow Exit):** This mode forces all unlocked doors to lock. Exit is allowed. Entry is denied.
- **Door Lockdown (Allow Entry + Exit):** This mode forces all unlocked doors to lock. Entry and Exit requests are allowed.

  Door Lockdown modes can be overridden by manually controlling the door from the Protege WX interface and by unlocking the door from a keypad.

- **Output to Check**: Defines the output that will control the door/door group. All door functions use one output. If the output selected is not valid, the function will be suspended upon startup.
- **Door to Control**: Defines the door to control as a result of the action being performed by the programmable function.
- **Door Group to Control**: Defines the door group to control as a result of the action being performed by the programmable function. Selecting both a door and a door group will result in only the door being controlled and the door group being ignored.

Virtual Door

This function enables you to setup defined inputs and outputs to operate as a door.

An example of this is where a roller door requires a REX button and DOTL monitoring, but has no reader on the outside. This can be achieved using spare inputs and outputs on expanders other than reader expanders.

- **Request to Exit Input:** The Request to Exit (REX) Input is connected to the Virtual Door's REX Input. When this input is closed the Lock output is activated and the door can be opened for the Max Open time when no alarms are being generated. This input should be configured as a digital input, therefore disable the "EOL Resistor on input" option. If a Normally Closed REX button is used the input inverted option should be set for the input to ensure pushing the button will generate the REX event. This input must also be placed in an armed area for the Virtual Door to operate.
- **Door State Input:** The Door Position input is connected to the Door State Input. This should be configured so that when the door opens the input opens. It may be necessary to invert the input to ensure this operation. This input should be configured as a digital input, therefore disable the "EOL Resistor on input" option. This input must also be placed in an armed area for the Virtual Door to operate.
- **Door Left Open Input to Control:** When programmed this input is controlled by the Virtual Door Function such that when the door is left open longer than the Max Open time and a Door Left Open event is generated this input will be opened. When the door closes the input will also close. Place this input in a reportable area to enable reportable events from the virtual door.
- **Forced Door Input to Control:** When programmed this input is controlled by the Virtual Door Function such that when the door is forced open and a Door Forced Open event is generated this input will be opened. When the door closes the input will also close. Place this input in a reportable area to enabled reportable events from the virtual door.
- **Unlock Time:** The unlock time determines how long the lock that controls the virtual door will remain unlocked for when a user access's the door.
- **Max Open Time:** The maximum open time is programmed to allow the door to be left open for a certain period before it will generate a door left open condition. When the left open condition is reached this will activate the alarm output and open the left open input.
- **Lock Output/Output Group:** You can assign an output or output group that controls the physical electric lock for the door.
- **Alarm Output/Output Group:** You can assign an output or output group that will activate when the door goes into either a left open or forced condition. Use this to warn the user to close the door.
- **Activate Alarm Output on Door Left Open:** When enabled the Alarm output will be activated when the door is left open beyond the Max Open time.
- **Pulse Alarm Output on Door Left Open:** When enabled the Alarm output will be activated with a pulse time on and off.

- **Activate Alarm Output on Door Forced:** When enabled the Alarm output will be activated when the door is forced open.
- **Pulse Alarm Output on Door Forced:** When enabled the Alarm output will be activated with a pulse time on and off.
- **Log Door Left Open Input Event:** When enabled the input will report events when the door is left open.
- **Log Door Forced Input Event:** When enabled the input will report events when the door is forced open.
- **Link to Door**: Defines the actual door to be controlled.

Input Follows Output

This function enables an input to be controlled using an output.

- **Input Follows Output:** The control input's state will be set to opened or closed according to the start of the Control Output. If the output is OFF the input will be closed. If the output is ON, TIMED ON or PULSED ON the input will be open. The input must be placed in an armed area to use it for control or reporting.
- **Output to Follow:** The control output's state will be followed by the control input.
- **Log Input Events:** When enabled the input will report events when the input changes state.

Elevator Control

The Elevator Control function can be used to lock or unlock elevator floors based on the state of an output.

- **Elevator Function Mode:** Determines which action is performed on the elevator group as a result of the output state. An action MUST be selected for the programmable function to operate correctly.
  - **Follow and Test:** The floor group status follows the programmed output state and will retest at 30 second intervals, changing the floor group state accordingly. In between state changes the floor group's state is continually tested at approximately 30 second intervals. When the floor group's state is changed by an external operation the programmable function will restore it.
  - **Invert Follow and Test:** Performs the same function as above however the output is inverted. This logic action is a test action. Consult the follow and test action for an explanation of the Test Function.
  - **Pulse On:** The pulse on action will unlock the floor group only when the output has transitioned from an off to an on state. The floor group will not be modified further from this state and will not be modified if it is turned OFF by another function.
  - **Invert Pulse On:** The not pulse on action will lock the door only when the output has transitioned from an off to an on state. The door will not be modified further from this state and will not be modified if it is turned ON by another function.
  - **Pulse Off:** The pulse off action will unlock the floor group only when the output has transitioned from an ON to an OFF state. The floor group will not be modified further from this state and will not be modified if it is turned OFF by another function.
  - **Invert Pulse Off:** The not pulse off action will unlock the floor group only when the output has transitioned from an ON to an OFF state. The output will not be modified further from this state and will not be modified if it is turned ON by another function.
- **Elevator Control Mode:** The control mode selects how the floor group will be controlled. This allows the floors to be unlocked for the token time, unlock latched or unlocked in the fire alarm mode.
  - **Emulate Unlock Menu:** The floor group will be unlocked for the token time that is programmed. Use this mode when you want to unlock the door for a defined time. The floors will lock after the token time has expired.
  - **Latch Elevator Unlock:** The floor group will be latched in the unlocked state and will remain unlocked until controlled from:
    - A keypad
    - The Protege interface
    - A scheduled action
    - A change in area status
    - A programmable function

- **Fire Control Elevator Unlock:** The floor group will be latched in the fire control unlock state and will remain unlocked until controlled from:
  - A keypad
  - The Protege interface
  - A programmable function that is programmed to deactivate the fire alarm control

- **Output to Check:** Defines the output that is used to control the elevator group.
- **Elevator Group:** Defines the elevators to control as a result of the selected function.
- **Floor Group:** Defines the floors that will be activated on all of the elevators in the elevator group as a result of the selected function.
- **Token Time:** The period of time the floor group will be activated for.

System Menu

The System menu is used to configure system settings, backup programming and update firmware.

This Option	Is Used To:
Settings	Configure the Controller settings including the IP address
Operators	Create and manage the operators that can access Protege WX to maintain and monitor the system
Roles	Configure the operator roles and the access they have
Backup	Backup and restore Controller programming
Firmware	View current version information and update firmware

System Settings

This page can be saved or refreshed using the toolbar buttons in the top right. The **Restart** button can be used to reboot the controller, which is required to apply any changes to the fields marked with an asterisk *.

System Settings | General

General

- **Name**: The controller name is programmed to identify the panel to the operator or system user. Ideally the name should describe the premises or the building where the controller is installed. The name is also used within the IP and SMTP mail services to identify the controller to the email recipient.
- **Serial Number**: The serial number of the controller.
- **HTTP Port***: The TCP/IP port that will be used for HTTP connection to the controller. The default port is 80. This can be changed to any network port that is not occupied.

  IMPORTANT: If this field is set to no value (which is converted to an invalid 0 value), the controller will no longer be accessible via the web interface and will require defaulting the IP address in order to connect.

HTTPS

Protege controllers have HTTPS connection enabled by default with a pre-loaded certificate. However, an alternative certificate can be installed if preferred.

For older controllers not equipped with a default certificate, ICT strongly recommends that all live Protege sites establish an HTTPS connection between the controller web interface and the web browser. This is especially important if the controller can be accessed onsite via a router, or externally via the internet.

If the controller is factory defaulted, any user-created HTTPS certificates are removed and the default certificate is reloaded. Custom certificates will need to be reinstalled.

- **Use HTTPS**: ICT controllers come preconfigured with a pre-loaded certificate and HTTPS enabled by default, however an alternate certificate can be installed if preferred.
- **HTTPS Port***: The TCP/IP port that will be used for HTTPS connection to the controller. The default port is 443. This can be changed to any network port that is not occupied.
- **Use HTTPS Certificate**: This option will be illuminated when Use HTTPS is selected, to signify that HTTPS is enabled. The HTTPS certificate can be the default factory certificate, a third-party certificate obtained from a Certificate Authority, or a self-signed certificate.
  - **Load Validation File**: Click to browse and upload a validation file (.txt format) provided by the Certificate Authority. This will be used by the CA to validate your domain name. Validating the domain this way requires your controller to be externally accessible via a hostname on external port 80.

    This step is not required when installing a self-signed certificate.
  - **Install Certificate**: Click to browse and upload an HTTPS certificate in .pfx format. If the file is secured with an export password you will be prompted to enter it. **Restart the controller** to implement or update HTTPS.

Cloud

- **Enable Cloud**: Enable this option to allow the controller to pair and connect to the Protege X cloud platform. For more information about pairing the controller, see the Protege X Online Help.

  This feature is only available to customers with a Protege X subscription. For more information, contact ICT Sales.

- **Status**: This field displays the status of the controller's connection to the Protege X system. For more information, see the Troubleshooting section of the Protege X Online Help.

Commands

- This field is used to send programming commands to the device. It should only be used when specifically advised by ICT documentation or technical support.

System Settings | Adaptor - Onboard Ethernet

Onboard Ethernet

- **Enable Onboard Ethernet***: This option configures the controller to communicate via its onboard ethernet communication link.

  This option is enabled by default.

Onboard Ethernet Configuration

- **Enable DHCP**: When enabled, the controller will use DHCP to dynamically allocate an IP address instead of using a static IP address.

  To use this there must be a DHCP server on the network you are attempting to connect to.

  When DHCP is enabled, the IP information below will not be updated and will therefore continue to display the last static IP configuration.

- **IP Address***: The controller has a built-in TCP/IP ethernet device and it must be programmed with a valid TCP/IP address to allow communication. By default the IP address is set to **192.168.1.2**.
- **Subnet Mask***: Used in conjunction with the IP address, a netmask 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**.
- **Default Gateway***: Used in conjunction with the IP address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the controller is connected. By default this is set to a value of **192.168.1.254**. Set this to **0.0.0.0** to prevent any external communication.
- **DNS Server***: The IP address of the DNS server being used by the controller. This is required if a DNS name is being used for the connection.

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.

Hostname

- **Controller Hostname**: If the controller is accessible via an external hostname it can be entered here.

  This is only required if the DDNS or HTTPS options are being used.

Dynamic DNS

- **Enable DDNS***: The controller has an in-built DDNS (Dynamic Domain Name Server) application, which allows it to dynamically connect to an external hostname even if its external IP address is not static. Enable this option and enter the required details to activate DDNS.
- **DDNS Server**: Enter the name of the DDNS server which is being used.

  Currently Duck DNS (www.duckdns.org) and No-IP (www.noip.com) are supported DDNS providers.

- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS

account.

- **No-IP**: The username and password are the credentials used to log in to your No-IP account.

System Settings | Adaptor - USB Ethernet

USB Ethernet

- **Enable USB Ethernet***: This option configures the controller to communicate via an ethernet adaptor connected to its USB port. This is used for connection to the Protege DIN Rail Cellular Modem.

Connection

- **Cellular Modem**: This option configures the controller to communicate with the Protege DIN Rail Cellular Modem connected to its USB port. This is currently the only USB Ethernet connection option.

  When this option is enabled the details of the cellular connection will be displayed.

For cellular modem information and programming instructions, see the Protege DIN Rail Cellular Modem Installation Manual and Protege DIN Rail Cellular Modem Configuration Guide, available from the ICT website.

Cellular Network Connection

- **Cellular APN***: The APN (Access Point Name) defines the network path for cellular data connectivity. The APN is specified by the mobile network operator (MNO) and is unique to that network, so it is important to use the correct APN for the cellular service required.
- **Cellular Username***: The username for the cellular network account.
- **Cellular Password***: The password for the cellular network account.

Cellular Options

- **Enable Debug***: When enabled, debug events are logged to the event log to help diagnose setup issues with the cellular modem. This would generally be enabled only during initial configuration or troubleshooting and should be disabled during standard operation.
- **Enable Watchdog***: When enabled, this option will prompt an automatic restart of the controller in the event that a critical fault is detected with the cellular modem that cannot be resolved. This option would typically only be enabled during fault finding.

Cellular Information

The cellular information section displays the cellular network connection status and details.

- **External Modem Detected**: Indicates whether the controller is able to communicate with the cellular modem connected to its USB port.
- **SIM Detected**: Indicates whether the controller is able to detect the cellular modem's SIM.
- **SIM Provider**: Displays the provider of the SIM, if detected.
- **Signal Strength**: The current strength of the wireless connection.

  The signal strength can only be displayed once a connection to a cell tower is established. When the cellular modem is performing initial configuration, has been automatically reset, or is initially searching for a network, Signal Not Measured will be displayed. This does not indicate a problem with the signal.

- **Network Registration Status**:
  - Registered (home): Displayed when the cellular modem is successfully connected to a network inside the SIM home region.
  - Registered (roaming): Displayed when the cellular modem is successfully connected to a network outside the SIM home region.
  - Not registered: Displayed when the cellular modem is detected but no connection has been established.
  - Not registered, seeking: Displayed when the cellular modem is actively seeking a network to connect to.

  - Denied: The network actively refused the connection attempt by the cellular modem.
  - Unknown: The cellular modem cannot currently determine network connection status.
- **Current Network Provider**: The mobile network operator that the cellular modem is currently connected to.
- **Current Technology**: The cellular technology that the cellular modem is connected with.
- **Internet Connection Status**: Identifies whether the cellular modem's internet connection is valid.
- **IP Address**: The IP address assigned to the cellular modem by the network provider.

If there is an error with the cellular connection the controller may automatically reset the modem to attempt to resolve the connection. When this occurs the controller interface will momentarily display the External Modem Detected disconnected icon. This is expected and only indicates a problem if it remains disconnected .

Cellular Hostname

- **Hostname**: If the controller is accessible via an external hostname (over the cellular modem connection) it can be entered here.

  This is only required if the cellular DDNS options are being used.

Cellular Dynamic DNS

- **Enable DDNS***: The controller has an in-built DDNS (Dynamic Domain Name Server) application, which allows it to dynamically connect to an external hostname even if its external IP address is not static. Enable this option and enter the required details to activate DDNS.
- **DDNS Server**: Enter the name of the DDNS server which is being used.

  Currently Duck DNS (www.duckdns.org) and No-IP (www.noip.com) are supported DDNS providers.
- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS account.
  - **No-IP**: The username and password are the credentials used to log in to your No-IP account.

System Settings | Configuration

Configuration

- **Test Report Time (HH:MM):** Used in conjunction with the Test Report Time is Periodic option (defined under Settings | Options (see next page)) to set the time of the day or the period that the test report trouble input activates. When the Test Report Time is Periodic option is enabled the time programmed will be used as a period between reports in hours and minutes, otherwise it is treated as a time of day.
- **Automatic Offline Time**: Allows the panel to update the users and other offline parameters on all intelligent modules at a set time of the day.
- **Module UDP Port**: Some modules, such as the Protege Module Network Repeater, can communicate with the controller over an ethernet connection using the UDP protocol. This field defines the UDP port that will be used for these communications. The default port is 9450. If this port is changed at the controller it must also be updated at all relevant modules.

  After changing this port you must restart the controller for the setting to take effect.

  Module Comms UDP/TCP (9450) is disabled by default. It can be enabled by adding `EnableModuleUDP = true` or `EnableModuleTCP = true` to the **Commands** field in the controller programming as required.
- **Default Keypad Language**: Defines the language selection for keypad displays. Select from English, Czech, Dutch, Estonian, Finnish, French, German, Greek, Italian, Norwegian, Polish, Romanian, Russian, Spanish, Swedish.
- **Touch Screen UDP Port**: This is the UDP port that a Protege touch screen will communicate over.

Touch Screen Comms UDP (9460) is disabled by default. It can be enabled by adding `EnableTLCDCommsUDP = true` to the **Commands** field in the controller programming.

Note: Ping is disabled by default for the onboard ethernet connection. It can be enabled by adding `EnablePing = true` to the **Commands** field in the controller programming.

System Settings | Options

Options

- **Test Report Time is Periodic:** When enabled the test report trouble input will be activated at the frequency defined by the **Test Report Time**. When disabled the test report trouble input will be activated at the specified time of day.
- **Generate Input Restore On Test Report Input:** When enabled the controller will generate a restore event for the trouble input test report input restoring. This occurs one minute after the trouble input has been activated.
- **Enable UL Operation Mode**: When this option is enabled, the Protege WX system runs in UL compliance mode.

  This setting has the following effects:
  - Adds a 10 second grace period following a failed poll before a module is reported as offline.

    Each module sends a poll message to the controller every 250 seconds. The module will be reported as offline if no poll has been received for the duration of this poll time plus the 10 second grace period.
  - Suppresses reporting of all alarms and/or reportable events to a monitoring station within the first two minutes of the controller powering up. The system will continue to send poll messages as usual.
  - Reports 'Input Tamper' events as 'Input Open' events when the area that the input is assigned to is armed. If the area is disarmed an 'Input Tamper' message will be sent.
  - Limits the **Dial attempts** for reporting services to a maximum of 8.

Misc Options

- **Enable Automatic Offline Download:** When this option is enabled, the controller will automatically update the users and other offline parameters on legacy intelligent expander modules at the **Automatic Offline Time** (**Configuration** tab). This option is not used for DIN rail modules.
- **Log All Access Level Events:** When enabled the controller will generate events, including the reason a user was denied access if they do not have the required access rights.
- **Do Not Wait for Dial Tone When Modem Dials Out:** When enabled the modem dials out without waiting for a dial tone.

  This setting is only supported by controller models with onboard modem dialers.
- **Enable VOIP Integration**: When this option is enabled the controller will allow the Protege Vandal Resistant Touchscreen Entry Station to retrieve user records for directory integration. For more information, see the Protege Vandal Resistant Touchscreen Entry Station installation Manual.

  Controllers on HTTPS currently do not support this feature. This is a known issue.
- **Purge Old Events**: When enabled the controller periodically deletes all events older than a specified number of days (14 days by default) from the event log. This is required by local legislation in some countries.

System Settings | Email Settings

Email on event enables you to trigger an email that is sent automatically when specific events occur. This feature can be configured to operate on area or input records.

Important: For emails to be sent, a valid DNS and gateway configuration is required.

This functionality supports TLS connection up to TLS 1.3. Insecure connection protocols are **not** supported.

This feature is only available in Advanced Mode.

Configure your Email Server Settings

Currently the following email servers are supported:

- Microsoft Exchange Server 2016
- Gmail when configured for less secure apps (see this link)
- Yahoo

Email SMTP Settings

- **SMTP Mail Server**: The address of the outgoing SMTP mail server.
- **SMTP Port**: The port used for outgoing mail connections. Typical numbers include 25 and 587.
- **Use SSL**: When this option is enabled, Protege WX will use TLS 1.2 to transmit emails to the SMTP server. Both the host OS and the SMTP server must support TLS 1.2, and the **SMTP Port** above must be changed to a TLS-enabled port (e.g. 587, 2525). When this option is disabled, no encryption will be used.
- **SMTP Logon**: The logon for the outgoing SMTP mail server.
- **SMTP Password**: The password for the outgoing SMTP mail server logon.
- **SMTP Timeout**: Defines how long (in seconds) before the connection times out.
- **Sender Email Address**: The email address used when sending outgoing mail.
- **Sender Display Name**: The display name used when sending outgoing mail. If a display name is not entered, the sender email address is used.

Test Settings

- **Test Email Address**: Enter an email address to test notifications.
- **Test Email Settings**: Click **Test** to check your configuration.

Add a Recipient Email Address

Navigate to **Programming | Areas** or **Programming | Inputs**.

- For an area, select the **Configuration** tab and add a recipient email address to the command window and use the format: `email:yourname@yourdomain.com`
- For an input, navigate to the command window for your selected input and use the format: `email:yourname@yourdomain.com`

System Settings | Custom Reader Format

This feature is only available in Advanced mode.

A custom reader format can be defined and used if the available preset formats do not meet your needs.

Custom Reader Configuration

- **Custom Reader Type**: Defines the reader type. The data can either be output as Wiegand (D0 and D1) or Magnetic Data (Clock and Data).
- **Bit Length**: The total number of bits that are sent by the card reader for each card badge.
- **Site Code Start**: The index where the site code data starts in the data transmitted. The count starts at zero.
- **Site Code End**: The index where the site code data ends in the data transmitted. The count starts at zero.
- **Card Number Start**: The index where the facility code data starts in the data transmitted. The count starts at zero.
- **Card Number End**: The index where the facility code data end in the data transmitted. The count starts at zero.

- **Data Format**: Defines how the card number that is received from the card reader is handled. If the size of the site code and card number are less than 16 bits (e.g. Site Start – Site End is less than 16 bits) use 16 bit, otherwise use 32 bit. If unsure, use 32 bit.

Parity Options (1-4)

There can be up to 4 blocks of parity calculated over the received data.

- **Parity Type**: The parity type defines the method of calculating the parity for the block. This is either Even or Odd Parity.
- **Parity Location**: The parity location defines the location of the parity bit in the received data.
- **Parity Start**: Defines where the location of the parity block starts in the received data.
- **Parity End**: Defines where the location of the parity block ends in the received data.

Bit Options (1-4)

- **Set Bit**: A set bit defines a location in the received data that must always be set (or a logical '1'). The set bit defines the location of the bit in the received data.
- **Clear Bit**: A clear bit defines a location in the received data that must always be cleared (or a logical '0'). The clear bit defines the location of the bit in the received data.

System Settings | Security Enhancement

- **Require Dual Credential for Keypad Access**: When enabled, a preconfigured numeric credential type labeled User ID will be automatically added to the **Credentials** tab of each existing and new user. When adding or updating a user, the presence of a valid unique User ID will be enforced. Both the User ID and the user's PIN will be required for the user to gain access to a keypad.
- **Allow PIN Duplication**: When enabled, this option allows more than one user to have the same PIN. This is only available when the **Require Dual Credential for Keypad Access** mode has been enabled.
- **Default PIN length**: Defines the length of PIN that will be generated by the system. If the **Default PIN length** is 6 and the **Minimum PIN length** is 4, the system will first generate new PINs 6 digits in length. Once those are depleted it will generate PINs with 7 digits, then 8 digits, then 5 digits, and finally 4 digits.
- **Minimum PIN length**: The minimum number of digits (options between 1-8) that will be permitted when manually entering PINs and when PINs are automatically generated.
- **Maximum Sequential Digits**: The maximum number of sequential digits (options between 2-4) that will be permitted or generated for PINs. For example, selecting 4 will allow a numerical sequence of 1234 or 4321 but not 12345. Selecting <not set> will allow a numerical sequence of more than 4 digits, for example 12345.
- **Maximum Repetitive Digits**: The maximum repetitive digits (options between 2-4) allowed for a user PIN. Selecting <not set> allows more than 4 repetitive digits, for example 11111.
- **PIN Expiry Time**: The frequency at which users will be prompted to reset their PIN at a keypad.

  NOTE: When PIN expiry is enabled, regardless of the expiry time, **ANY** PIN created or edited through the user Interface will immediately expire on first use. The user will be required to set their own permanent PIN when next logging in at a keypad. This ensures that only the user knows their PIN.

Operators

An operator is a person who uses Protege WX for maintaining the system and monitoring the site.

General

- **Name**: The name of the operator. This is the name displayed in the status bar at the top of the page.

  Do not enter more than **40 characters** for the operator name. This is the maximum supported length.

Configuration

- **Username**: This is the name used by the operator when logging in.
- **Password**: The password of the operator. Operators can change their own password from the Home Page once logged in.
- **Role**: Select the appropriate role to determine what access the operator has once logged in.
- **Default Language**: This sets the language of the user interface displayed to the operator.

Operator Timeout

- **Enable Operator Timeout**: Select this option to automatically log the operator out after a period of inactivity as defined in the Operator Timeout setting below.
- **Operator Timeout**: Defines the inactivity period, after which Protege WX will time out and the operator will be prompted to log in again to continue.

Roles

To control access to the Protege WX system, each operator must be assigned a role. The role determines which pages are visible to the operator when they are logged in. If an option is enabled, that page will be visible. If it is disabled, the page is hidden.

The system comes programmed with three preset roles. These roles can be customized to meet your specific requirements, however caution should be taken when making changes as removing permissions can prevent an operator from accessing the system.

Operator Role	Function
User	Can monitor the system and perform basic user configuration.
Master	Can perform actions required to program and configure the system.
Installer	Can perform all actions without any restrictions. This role cannot be edited.

By default, no operators are permitted to view user PINs after they have been saved. To allow operators to view user PINs, enable the **Show PIN number for Users** option.

Password Policy

A password policy represents a set of guidelines designed to enforce a higher level of security. Protege systems enable you to define your own password policy that other users of the system are required to follow.

Configuration

- **Minimum Password Length**: Defines the character length required for a password. If this option is activated and a minimum of eight letters are required, the password test is invalid and the password testtest is valid.
- **Minimum Number Of Uppercase Characters**: Defines the minimum number of uppercase characters required for a password. This includes all accented French, Spanish, Polish and Estonian characters. If this option is activated and a minimum of three capital letters are required the password test is invalid and the password TeST is valid.
- **Minimum Number Of Digits**: Defines the minimum number of digits required for a password. If this option is activated and a minimum of three digits are required the password t35t is invalid and t&$t!ng is valid.
- **Minimum Number of Special Characters**: Defines the minimum number of ASCII characters (@$,<>#:`~!-+%'"|\.(){}=?_*&) required for a password. If this option is activated and a minimum of three special characters are required the password t&$t is invalid and the password t&$t!ng is valid.
- **Compare Against Username**: Passwords are checked against the username to ensure that they are unique. This option splits the username by space, period, comma, hyphen or underscore to ensure that no parts of the username (more than two characters) exist in the password. If this option is activated and your username is test.operator the passwords testing and operator1234 are invalid.

Maintaining Your System

This section covers system maintenance, including how to back up and restore controller programming and update firmware.

Changing Operator Passwords

For security reasons, you may want to change operator passwords periodically.

Only operators with sufficient security permissions will have access to changing passwords for other operators. Any operator can change their own password on the Home Page.

1. Navigate to **System | Operators** and select the operator to update.
2. Click **Change Password**.
3. Enter and confirm the new password, then click **OK**.
4. Click **Save**.

Backing Up and Restoring Controller Programming

Creating backups of your controller programming is good practice to ensure you are protected against damage in the event of hardware failure or malfunction.

The Protege WX interface provides a simple export tool for backing up the system to a proprietary encrypted backup file (*.bak). This file works as a snapshot of your current system, enabling you to later restore and retain the programming at the same point as you exported it. You can even backup programming from one controller and restore it to another. This can be useful when running a test environment, or for pre-programming a system prior to deployment at a client site.

1. Navigate to **System | Backup**.
2. To create a backup, select **Backup Controller**. This creates a copy of the controller's programming, which may then be restored at a later date.

   Depending on your browser settings you may be prompted to save the file. Otherwise, it is automatically downloaded to your Downloads folder.

3. To restore programming select **Choose File** to browse to a .bak file created using the backup option, then select **Restore Controller** to import a copy of the programming.

Upgrading Application Software and Module Firmware

From time to time ICT releases new updates with changes and enhancements to system features. To ensure your installation is running at optimal performance we recommend that all installed modules utilize the latest updates.

Controllers do not support defaulting and firmware upgrade at the same time. Before you upgrade the controller firmware, ensure that the wire link used to default the controller is **not** connected.

1. From the main menu, select **System | Application Software**. This page provides details about the current Protege WX version that is installed.
2. Click the **Choose File** button and browse to the supplied update file.
3. Click **Upload** to commence the upgrade procedure.
4. The controller will automatically create a backup of the programming. Depending on your browser settings you may be prompted to save the file. Otherwise, it is downloaded automatically to your **Downloads** folder.
5. Progress is shown as the new application software is installed. The controller then restarts.

   This process can take up to 5 minutes to complete, so we recommend that upgrades are performed when the site is closed for maintenance or at times of low activity. The controller will not be able to perform its normal function while being upgraded.
6. After the upgrade is complete, log on to the controller to review and resolve any health status messages to resume normal operation. You may need to perform module updates, re-arm areas and re-enable the 24HR portions, and start services and programmable functions.

Update Module Firmware

- **Module**: This section is used to update the firmware of any module connected to the controller. Select the connected module that requires a firmware update from the dropdown.
- **BIN File**: Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the new firmware on the selected module.

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.

Force Update

In situations where a module becomes stuck in the bootloader mode and the application is not running, it may become necessary to perform a force update.

This hidden feature in the Update Module Firmware section of the web interface provides the ability to update module firmware on an inoperable module where it is not possible through the regular update process.

Clicking **Module** will expand the hidden section, making the **Force Update** panel available.

1. Select the **Force Update - Module**, carefully selecting the module type and model.
2. Select the **Force Update - Address**, which is the configured **Physical Address** of the module.
3. The **Skip Verification** option will bypass the firmware check and allow firmware that does not match the module type of the module to be loaded.

   This option should only be selected at the direction of ICT Technical Support .
4. Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the firmware on the selected module.

Note: The maximum address that can be selected for force update is 32. If the module has an address greater than 32 it cannot be upgraded via this method. You will need to contact ICT Technical Support for assistance.

Addressing Expanders

The Expander Addressing option is used to view the hardware connected to the system network and to set the addresses of DIN rail modules which have auto-addressing capability. This page displays the details of all modules currently connected or those that have registered previously but may currently be offline.

Listed for each module is:

- The module type
- The serial number
- Current firmware version
- The current address of the module
- Whether the module is registered with the controller
- Whether the module is currently online

When connecting a module to the network it must be added to Protege WX and allocated a unique physical address. By default all DIN rail modules are shipped from ICT with the address of 254 and without changing this address the module will not be able to register with the controller.

For older legacy PCB modules, the address is configured via DIP switches. Refer to the relevant Installation Manual for instructions on configuring the address of the module.

To Set the Network Address of a Module:

1. Ensure the controller is correctly powered.
2. Connect the module(s) that require addressing to the module network. Make sure that the power light on each module is on and that the status light begins flashing rapidly.
3. Allow some time for the module(s) to attempt to register with the controller.
   - If the module has the default address of 254 or has the same address as another module, the **fault** light will be constantly on and the **status** indicator will be flashing red with an error number.
     - For an unaddressed module, the status indicator will flash in **three** flash bursts.
     - If the address is already in use by another module, the status indicator will flash in **four** flash bursts.
   - If the module has been previously addressed and is not a duplicate, then it will succeed in registering and the **status** light will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the module addressing window by selecting **Expanders | Expander Addressing**.
5. Enter an address for the relevant module(s) by selecting an option under the **Address** column then click **Save** to save the address and restart the module.
6. Allow around 5 seconds per module for the new address to be sent and registered then click **Refresh** to update the list and display the new addresses.
   - If the address has not changed, check that the module is online and communicating and has finished attempting to register.
   - If the address has changed but the module is not shown as registered, check that the address is in the valid address range and is not a duplicate of another modules address.

Once all modules are online and registered with the desired addresses, the addressing process is complete.

Maximum Module Addresses

The Protege controller has a set limit on the number of modules of each type that it can support. This applies to both physical and virtual modules. The maximum addresses available for each type of module are outlined in the table below:

Module Type	Maximum Address
Keypad	200
Input Expander	248
Reader Expander	64
Output Expander	32
Analog Expander	32
Smart Reader	248

Any module with an address higher than these limits will not come online to the controller. A message will be generated in the controller's health status.

Configuring the IP Address

The controller must be programmed with a valid IP address to allow communication. By default this is set to **192.168.1.2** but can be adapted to suit your network requirements and addressing scheme.

If the IP address has been configured previously and you are not sure what it is, you can temporarily default it to 192.168.111.222. For more information, see Temporarily Defaulting the IP Address.

1. Log in to the controller and navigate to **System | Settings**.
2. In the **Adaptor - Onboard Ethernet** tab, enter the required connection settings:
   - **Enable DHCP**: When the option is enabled, the controller will use DHCP to dynamically allocate an IP address instead of using a static IP address.

     To use this feature, there must be a DHCP server on the network you are attempting to connect to.
   - **IP Address**: This is the IP address that the controller is currently using. By default this is set to **192.168.1.2**.
   - **Subnet Mask**: Used in conjunction with the IP address, a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to **255.255.255.0**.
   - **Default Gateway**: Used in conjunction with the IP address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the controller is connected. By default this is set to **192.168.1.254**.

     Set this field to **0.0.0.0** to prevent any external communication.
3. Click **Save**.
4. Click **Restart** in the toolbar to restart the controller and implement the changes.

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.

Setting the IP Address from a Keypad

If the current IP address of the controller is not known it can be viewed and changed using a Protege keypad.

1. Connect the keypad to the module network.
2. Log in to the keypad using any valid installer code. The default installer code is 000000.
   If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

   Note that this will erase **all** existing programming as well as setting up the default installer code.
3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

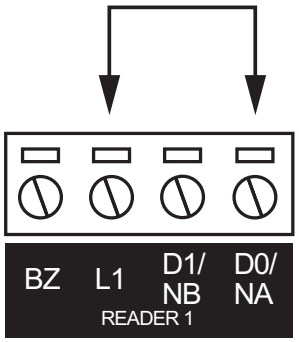
Temporarily Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it. This will also temporarily disable HTTPS security, which may help resolve some connection issues.

This defaults the IP address for as long as power is applied, but does not save the change permanently. Once the link is removed and power is cycled to the unit the configured IP address is used.

Defaulting the IP Address of a Two Door Controller

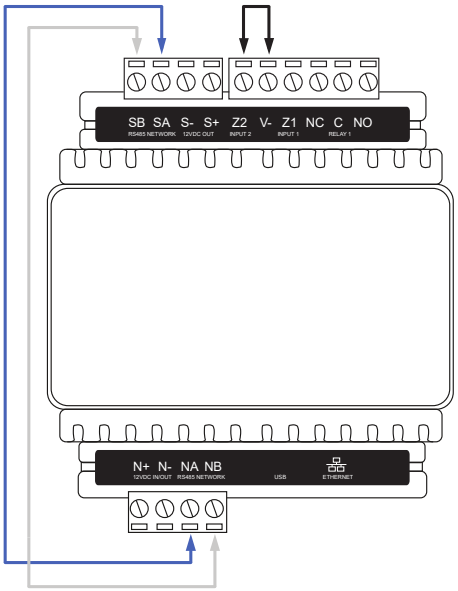
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Defaulting the IP Address of a Single Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

5. When the controller starts up it will use the following temporary settings:
   - **IP Address**: 192.168.111.222
   - **Subnet Mask**: 255.255.255.0
   - **Gateway**: 192.168.111.254
   - **DHCP**: Disabled
   - **Use HTTPS**: Disabled
6. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.

7. Remove the wire link(s) and power cycle the controller again.
   The controller will now use the configured network settings.

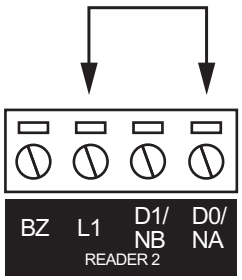
Defaulting a Controller

The controller can be factory defaulted, which resets all internal data and event information. This allows you to remove all programming and start afresh.

Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2

Defaulting a Two-Door Controller

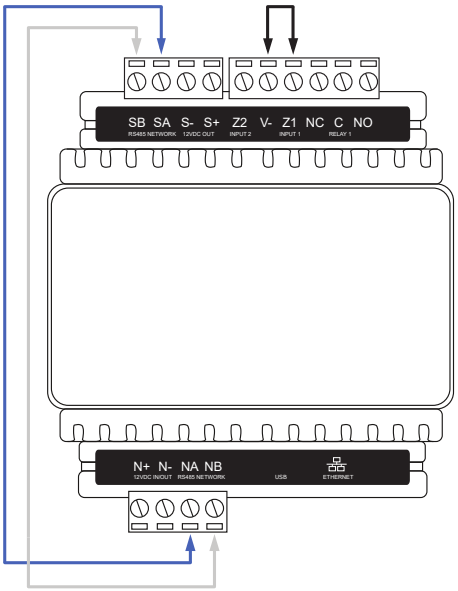
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link **before making any changes to the controller's configuration**.

Defaulting a Single-Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.
6. Remove the wire links **before making any changes to the controller's configuration**.

The system will now be defaulted with all programming and **System Settings** returned to factory configuration, including resetting the IP address and all network configuration, and removing all operator records.

- Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2.

  Earlier versions of the controller firmware do not reset the IP address. If the controller is not available on 192.168.1.2 you will be able to connect to it via its previous IP address.

- Any configured system settings (e.g. **Default Gateway**, **Event Server**) are reset to their default values.
- Any custom HTTPS certificates are removed and the default certificate is reinstalled.

  Earlier versions of the controller do not have a default HTTPS certificate installed. If the controller is not available via HTTPS, connect to it via HTTP.

- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

After Defaulting a Controller

Before making any changes to the controller's configuration or upgrading the firmware, **remove the wire link used to default the controller**.

After defaulting a controller a number of essential steps will need to be performed to resume normal operation. Not all of the following steps will necessarily be required, depending on your site configuration:

1. Connect to the controller's web interface using HTTPS, unless it is an older controller with no default certificate loaded, then it will connect using HTTP.
2. Recreate the admin operator and log in to the controller's web interface.

   If you are not prompted to create the admin operator, the default username is admin with the password admin.

3. Reset the controller's IP address to its previous value.
4. Reconfigure any additional network settings.
5. Reinstall previously installed custom HTTPS certificates.
6. Restore any other system settings as required by your site configuration.

Troubleshooting

This section includes helpful troubleshooting information.

Common Health Status Messages

The Health Status is displayed on the Home Page and provides details of the overall status of the system and can be useful in identifying any problem areas that need to be addressed.

It lists any problems that the Controller has with its current configuration. This includes:

- Modules that require a restart
- Modules that are offline
- Areas that require rearming due to input changes
- Areas where the tamper area (24 hour monitoring) is disarmed
- Inputs that have been assigned to an area, but not assigned a type
- Items that can't fit in the internal database

Essentially, anything that has been configured but that is not operating according to that configuration is shown in this list.

Modules that Require a Restart

Typical Health Status Message

Reader Expander Warehouse Reader requires a module restart

Cause

Modules need to be restarted whenever a programming change is made that requires the hardware to physically function in a different manner.

Solution

1. Navigate to the appropriate Expander menu (for example Expanders | Reader Expander).
2. Select the module that is listed in the health status message, then click the Restart button on the toolbar.

You can also restart the Controller from the System | Settings page which updates **all modules** connected to the system.

Modules that are Offline

Typical Health Status Message

Reader Expander Warehouse Reader is offline

Cause

This can occur when the module has been added, but the address has not been correctly set.

Note that if you have recently cycled power to the Controller it can take up to 250 seconds for the module to come back online.

Solution

1. If you have cycled power to the Controller, ensure you have allowed enough time for the module to come online.
2. Navigate to the appropriate Expander menu (for example, Expanders | Reader Expander).
3. Check that the **Physical Address** allocated on the General tab matches that allocated under Expanders | Expander Addressing.
4. If the problem continues, check that the module is wired correctly.
5. Check the LED indicators of the module. If the fault light is on and the status light is flashing red, the number of sequential flashes will indicate an error code.

Areas Requiring Rearming due to Input Changes

Typical Health Status Message

Area Warehouse requires rearming due to Input Warehouse PIR changes

Cause

The 24 hour portion of an area must be rearmed when programming changes result in the input functioning in a different manner. This is to prevent inadvertent changes to a live system that could result in an undetected security breach.

Solution

1. Navigate to Monitoring | Areas and click Controls to open the manual control window.
2. Click Disarm 24 to disarm 24 hour monitoring, then Arm 24 to enable it.

Areas with the Tamper Area Disarmed

Typical Health Status Message

Area Warehouse has its Tamper Area disarmed

Cause

Every Area created in Protege WX is actually made up of two areas: The main area that monitors devices (such as PIRs) only when it is armed, and the 24 hour (or Tamper) area that monitors for a tamper or short condition on devices (such as PIRs) 24/7.

The 24 hour tamper area is armed automatically when the main area is armed.

Solution

1. Navigate to Monitoring | Areas and click Controls to open the manual control window.
2. Click Arm 24 to enable 24 hour monitoring.

Inputs Assigned an Area but no Input Type

Typical Health Status Message

Input Warehouse PIR has an Area but no Input Type assigned

Cause

An input has been assigned to an area but the system has not been instructed on what to do if the input is activated.

Solution

1. Navigate to Programming | Inputs and select the input listed in the message.
2. Click the Areas and Input Types tab, then select an Input Type from the dropdown.
3. Save your changes.

Items that Can't Fit in the Database

Typical Health Status Message

Input Warehouse PIR will not fit into the internal database

Cause

Each module has only a set number of inputs and outputs. For instance, the Protege WX Controller has 8 inputs and 3 outputs, whereas a Reader Expander has 8 inputs and 8 outputs. If you add a record where the address is higher than the maximum allowed for that Expander (such as adding an input to a Controller with a Module Input of 9 or higher where the Controller only has 8 physical inputs), it cannot be added to the system.

Solution

Ensure the Module Input address physically exists.

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