PRT-WX-DIN

Using Protege WX

Programming Reference Manual

Last Published: 23-May-25 11:12 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.

  It also has a USB port which enables offsite communication via cellular network with connection to a Protege DIN Rail Cellular Modem.

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 reader port supports two readers, with the wiring or address determining which is the entry and which the exit reader.

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.

Complete the Protege WX Level 2 training course to unlock **WXpert mode** (otherwise known as advanced mode), which includes enhanced access and intrusion functionality as well as building automation and elevator control. For more information about these advanced features, request the Protege WX WXpert Mode Guide from your ICT representative.

Throughout this manual, settings marked with an asterisk ***** are only available in advanced mode.

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/cUL 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.

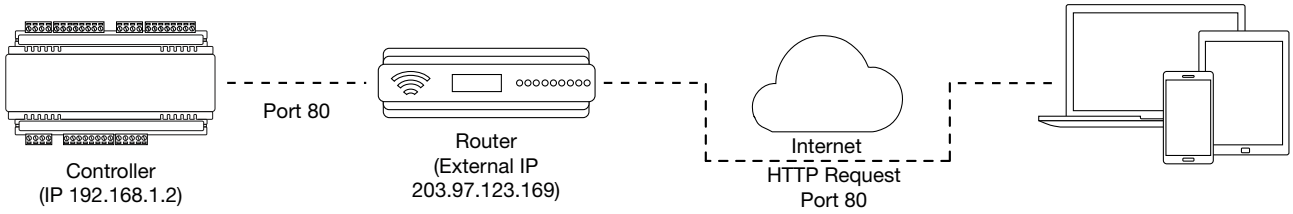
More Information

- 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.

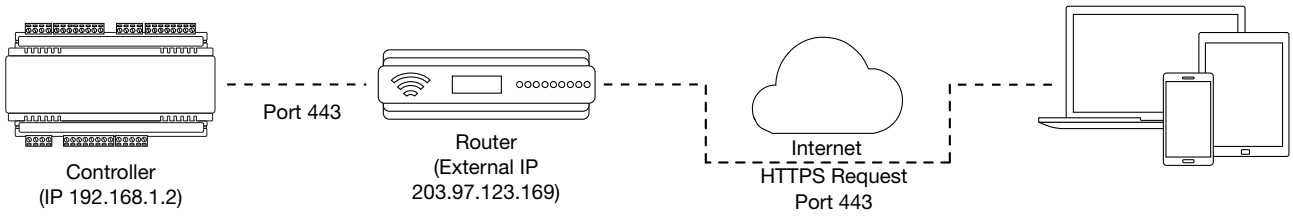
External access via HTTP is only required in order to validate and install your certificate. Once the certificate has been installed, HTTP access will be disabled because the more secure HTTPS connection is available. Therefore it will no longer be necessary to forward external port 80 to the controller.

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

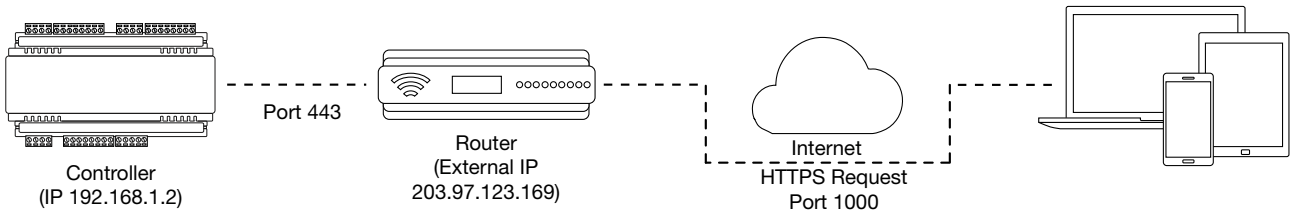
After you have installed a certificate and established an HTTPS connection to the controller, you may wish to continue accessing the controller over the internet. To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed 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.

   Always include the `-certpbe`, `-keypbe` and `-nomac` arguments so that the certificate is encrypted in a way that the controller can interpret. This does not affect the encryption of the HTTPS connection.

   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
   ```

   Always include the `-certpbe`, `-keypbe` and `-nomac` arguments so that the certificate is encrypted in a way that the controller can interpret. This does not affect the encryption of the HTTPS connection.
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, along with their corresponding inputs, outputs and trouble inputs. You can even use it to program modules that are not physically available yet.

1. Connect any new modules to the RS-485 network.
2. Click **Step 2- Auto Detection** to continue. The wizard automatically detects and displays new and existing modules.

   Each module is assigned a name automatically. These can be renamed as required for easier identification.
3. Click **Step 3- Additional Modules** to continue.
4. Review the **Existing Modules** information. Modules that are being connected to the system for the first time are automatically assigned the next available address. You can change these addresses later in **Expanders | Expander Addressing**.
5. If required, add additional modules for any hardware that is not yet connected to the network.
6. 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 65) 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. In the **Reporting Services** tab, select the primary reporting service for the area (usually ReportIP).
4. 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.
5. Click **Save** to finish creating the area.

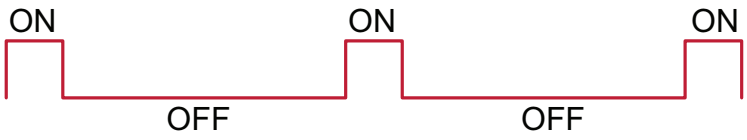
For a full list of the available properties and a description of what they do, refer to the Property Reference Guide (see page 47).

Pulse Times

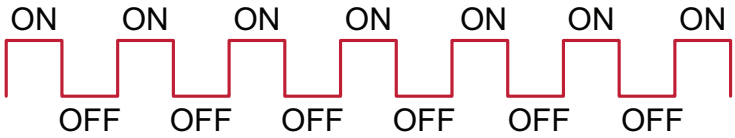
Pulse times allow an output or group of outputs to be pulsed for the duration of an area state. For example, the keypad beeper can be used to make short beeps for an exit delay, then a long continuous beep for entry delay.

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

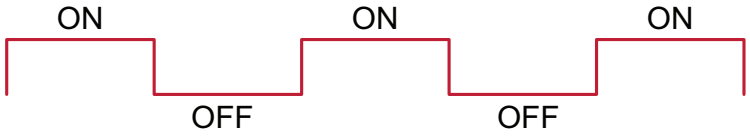
Setting the **Pulse On** to **1** and the **Pulse Off** to **9**, provides a short pulse (such as a short beep or flash) every second.



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 | Access Levels

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

User 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

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.
  - **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.

  Controllers support all credential type formats via either RS-485 or ethernet. Reader expanders only support Wiegand credential types.
- **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**: The door type assigned to a door controls the credentials required for access, as well as antipassback and dual authentication operation. Different door types can be scheduled for different times of day. For more information, see **Programming | Door Types**.
- **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/Outside Door**: These fields allow you to set the areas that are inside and outside doors, enabling integration of the door's access control functions with area control and intrusion detection. Setting these areas allow you to use a range of features such as:
  - Unlock and lock doors automatically based on the area status (see the **Options** tab)
  - Prevent users from entering armed areas (see the **Advanced Options** tab and **Expanders | Reader Expanders | Reader 1/2**)
  - Allow users to arm or disarm areas from the entry/exit reader (see **Expanders | Reader Expanders | Reader 1/2)**
  - Antipassback (see **Entry/Exit Passback Mode** in **Programming | Door Types | General**)
  - Area counting (see **Enable User Counting** in **Programming | Areas | Options 1**)

  If there is no monitored area outside the door (i.e. the door is external) you can leave the outside area as - Not Set -.

- **Unlock Schedule**: The unlock schedule can be used to latch unlock the door, allowing free access without a credential when the schedule is valid.

  By default, the unlocking function is edge triggered: the door will latch unlock when the schedule becomes valid and lock when the schedule becomes invalid, but can be overridden by user or operator commands. This behavior can be modified using the settings in the **Options** tab.

  For example, a retail shop could set an unlock schedule so that the door is unlocked for customers during their opening hours. Outside of these hours the door is locked but can be accessed by employees using their credentials.
- **Door Pre-alarm Delay Time**: When a door is left open, after this period (in seconds) it will generate a pre-alarm. This pre-alarm generates an event and activates the **Pre Alarm Output / Output Group** (set in the **Outputs** tab), warning users that the left open alarm will soon be activated.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **Door Left Open Alarm Time**: When the door is left open, after this period (in seconds) it will activate the left open alarm. This alarm opens the Door Left Open trouble input and activates the **Left Open Alarm Output / Output Group** (**Outputs** tab).

  The left open alarm timer begins when the door is first opened, not after the pre-alarm is activated. For example, with default settings the pre-alarm will be activated 30s after the door is opened, and the left open alarm will be activated 15s later (45s total).

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **Interlock Door Group***: When a door group is assigned to this field this door cannot be unlocked unless all of the doors assigned to the interlock door group are closed and locked. This ensures that only one door in the group can be opened at any given time.

  This feature is used to prevent a free path from being opened between safe and hazardous areas. For example, it could be applied to an entry point to a clean room or secure facility.

Commands

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

Doors | Outputs

Lock Output

- **Lock Output / Output Group**: The output or output group that controls the physical door lock. These are typically the relay outputs on the reader expander, but could be any output or output group in the system.
- **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**: The door will generate a pre-alarm when a door is left open, to warn users that the door left open alarm will soon be activated. The pre alarm output or output group is activated when the **Door Pre-alarm Delay Time** (**General** tab) is reached.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **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**: When a door has been left open for too long, a door left open alarm will be generated to instruct users to close the door immediately. The left open alarm output or output group is activated when the **Door left open alarm time** (**General** tab) is reached.

  In addition, when the alarm is generated the Door Left Open trouble input is opened.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **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**: When a door is forced open without any access a door forced alarm will be generated. The forced open output or output group will be activated immediately.

  In addition, when the alarm is generated the Door Forced Open trouble input is opened.

  This feature can be disabled under specific circumstances in the **Alarm options** tab.

- **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**: This input is used to detect the position of the door. When this input is opened the door status will change to 'open', and when the input is closed the door status will change to 'closed'.

  This is also known as a door contact or reed input, as a reed switch is typically used for this function.

- **Invert Door Input**: When this option is enabled the operation of the door position input will be reversed. When the input is closed the door will be considered open. When the input is open the door will be considered closed.

  Note: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

REX Input Options

- **REX Input**: This input is used for the REX (request to exit) function. When a user activates this input it will generate a request to exit and unlock the door. When the door is unlocked by REX it uses the standard **Lock Activation Time**, unless the **REX Time Different to Lock Time** option has been enabled below.

  REX is generally used in situations where a door has entry readers but no exit readers. REX inputs are commonly buttons, so they typically have a normally open **Contact Type** (**Programming | Inputs | Options**).

  The **Unlock Door On REX** option must be enabled in the **Options** tab.

- **Invert REX Input**: When this option is enabled the operation of the REX input will be reversed. When the input is closed (deactivated) a request to exit will be generated.

  Note: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

Bond Input Options

- **Bond Sense Input**: This input is used to detect the position of the door lock. When this input is opened the door status will change to 'not locked', and when the input is closed the door status will be 'locked' (assuming the door position input is also closed).

  Door left open and forced alarms may be generated based on the position of the bond sense input.

  This feature can be used with any lock that has bond or lock sense monitoring. For example, a magnetic bond sense is a contact that indicates whether the magnetic bond between the electromagnet and the clamp is complete.

- **Invert Bond Input**: When this option is enabled the operation of the bond sense input will be reversed. When the input is closed the door will be considered not locked and vice versa.

  Note: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

REN Input Options

- **REN Input**: This input is used for the REN (request to enter) function. When the user activates the input it will generate a request to enter and unlock the door. The standard **Lock Activation Time** is used.

  REN is generally used for doors which allow free entry. Alternatively, a REN button may be placed in a guard station to allow guards to unlock a door remotely. REN inputs are commonly buttons, so they typically have a normally open **Contact Type** (**Programming | Inputs | Options**).

  The **Unlock Door On REN** option must be enabled in the **Options** tab.

- **Invert REN Input**: When this option is enabled the operation of the REN input will be reversed. When the input is closed (deactivated) a request to enter will be generated.

  Note: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

Beam Input Options

- **Beam Input**: This input is used to ensure that automatic doors remain unlocked and open when there is something obstructing the path of the door. When the beam sense input is opened (while the door is already open) the door is unlocked and the lock is held open. When the input is closed the lock output(s) will remain on for the programmed **Lock Activation Time** (**Outputs** tab) before turning off again.

  This feature is typically used with automatic doors and gates which use a door pump as a lock output. This allows the door to begin opening again when it is about to collide with something.

  The beam input does not restart the pre-alarm and left open alarm timers.

- **Invert Beam Input**: When enabled the reader inverts the beam control input. When disabled the beam control input operates normally.

  When this option is enabled the operation of the beam sense input will be reversed. When the input is closed the beam function will be triggered.

  Note: If the **Contact type** setting (**Programming | Inputs | Options**) is set to Normally open there is no need to also invert the input here.

General Options

- **Always Allow REX**: When this option is enabled the door will process a request to exit even when the door is already open. This will activate the lock but will not reset the door forced or door open too long alarms. When this option is disabled the REX function will only operate when the door is closed.

  This option is useful when the lock output is controlling an automatic door opener. This allows the door to begin opening again if the REX is pushed while it is closing; however, some locks such as maglocks should remain locked while the door is open to prevent the door from 'bouncing' when it is closed.

- **Recycle Door Open Time On REX**: When this option is enabled, users can press the REX input while the door is open to reset the time that it is allowed to be left open. If the pre-alarm has started, pressing the REX button will silence the pre-alarm; however, if the door left open alarm has already been activated, pressing the REX will not reset the timer.

  For example, if the **Door Left Open Alarm Time** is set to 45 seconds, pressing the REX button during this period will reset the timer, allowing the door to be open for an additional 45 seconds.

  The **Always Allow REX** option must also be enabled.

- **Forced Door Sends Door Open**: When this option is enabled, when the door is forced open (i.e. opened without being unlocked) it will be processed as a 'door open' status. When this option is disabled the door forced status will be processed as normal.

  This can be used in situations where the door might be opened without being controlled by the controller. For example, some doors have a physical key override to manually unlock the door, which would normally cause a door forced alarm.
- **Recycle REX Time**: When this option is enabled, pressing the REX button while the door is unlocked by REX will reset the lock activation time so that the door will remain unlocked for longer.

  For example, if the **Lock Activation Time** is set to 5 seconds, pressing the REX button during this period will reset the timer, allowing the lock to remain open for another 5 seconds.

  This feature only applies when the door has been unlocked by REX. The **Always allow REX** option must also be enabled.
- **Maintain REX**: When this option is enabled the door will remain unlocked for as long as the REX button is held down. When the REX button is released the door will lock again after the **REX Activation Time**.

  Holding down the REX button will also prevent the door left open timer from starting, so the door can be held open indefinitely without activating an alarm.
- **Pulse Reader Beeper On REX**: When this option is enabled the readers associated with the door beep twice when the REX button is pressed. When this option is disabled there is no audible response from the request to exit function.
- **REX Time Different To Lock Time**: By default, the REX activation time is the same as the **Lock Activation Time** (**Outputs** tab). With this option enabled the **REX Activation Time** can be configured separately and will override the lock activation time when the REX button is pressed.

  For example, if the lock activation time is 5 seconds and the REX activation time is 10 seconds, when a user badges to enter a room the door will unlock for 5 seconds, but when they press the REX button to exit the door will unlock for 10 seconds.
- **REX Activation Time**: If the **REX Time Different To Lock Time** option is enabled above, this field sets the duration that the door lock will be activated when the REX button is pressed.

  The REX activation time cannot be set to 0.

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**: By default, doors do not generate open and close events while they are unlocked by schedule. This saves space in the controller's memory. If you need to report on these events, enable this setting to generate them.
- **Relock On Door Close**: With this option enabled the lock will relock as soon as the door closes. If the door is not closed the lock will still deactivate after the normal lock activation time.
- **Relock On Door Open**: With this option enabled the lock will relock as soon as the door opens. If the door is not opened the lock will still deactivate after the normal lock activation time.
- **Unlock Door On REX**: When this option is enabled, opening the **REX Input** (set in the **Inputs** tab) will unlock the door.

When this option is disabled the door does not automatically unlock when the REX input is pressed, but temporarily enters a 'free egress' state, suppressing door forced alarms for the normal REX activation time. This allows the use of mortise locks with a free egress handle which mechanically unlocks the door.

- **Unlock Door On REN**: When this option is enabled the **REN Input** (set in the **Inputs** tab) can be used to unlock the door using the request to enter function. Disable this option to disable REN processing for this door.
- **Schedule Operates Late To Open**: When this option is enabled the door will not latch unlock when the schedule is valid until a user or operator unlocks the door. This can be used to prevent the door from automatically unlocking on days when nobody arrives on site.

  This option overrides the **Always Check Unlock Schedule** option above.

Door Options 2

- **Door Lock Follows Inside/Outside Area**: Enable one of these options to select whether the **Area Inside Door** or **Area Outside Door** (**General** tab) will be used with the area control options below.
- **Prevent Slave Unlock On Inside Area**: If there is a **Slave door** set in the **General** tab, by default the slave door will always follow the state of the primary door when it unlocks on access. This option prevents the slave door from following the primary door when the slave door's inside area is armed, preventing false alarms. This option must be enabled in the slave door's programming.

  This feature does not work with the `SlaveREX = true` command. When the primary door is unlocked by REX, REN or manual commands the slave door will be unlocked regardless of area status.

- **Prevent Unlock On Schedule If Inside/Outside Area Armed**: When one of these options is enabled, if the unlock schedule becomes valid but the door's inside or outside area is still armed the door will not unlock. This can be used to prevent a door from unlocking on days when no one arrives to disarm the area.
- **Area Disarmed AND Schedule Valid Unlock Door**: When this option is enabled the door will automatically latch unlock when both the unlock schedule is valid and the relevant area is disarmed. When the schedule becomes invalid or the area is armed the door automatically locks.

  If the door is latch unlocked or locked by any other feature it will immediately be returned to the correct state.

  The relevant area is determined by the **Door lock follows inside area** or **Door lock follows outside area** options above.

- **Area Disarmed OR Schedule Valid Unlock Door**: When this option is enabled the door will automatically latch unlock when either the unlock schedule is valid or the relevant area is disarmed. When both the schedule is invalid and the area is armed the door automatically locks.

  If the door is latch unlocked or locked by any other feature it will immediately be returned to the correct state.

  The relevant area is determined by the **Door lock follows inside area** or **Door lock follows outside area** options above.

- **Enable Access Taken On REX/REN Events**: With this option enabled, when a REX or REN is registered at the door the system will record whether the requested access was taken or not taken. For example, if the REX button is pressed and then the door is opened a 'Request to Exit Taken' event will be logged. If the door is not opened a 'Request to Exit Not Taken' event will be logged.

Doors | Advanced Options

Advanced Options

- **Update User Area When Passback Disabled *** : By default, unless antipassback is enabled the system does not keep track of which area a user is in when they pass through the door. With this option enabled the controller will update the area the user is in even when antipassback is disabled on this door. This feature is useful on sites where some doors have antipassback enabled but others do not.

  This setting is not related to the **User Area** in **Users | Users | General**.

- **Lock Out REX When Inside Area Armed**: When this option is enabled the door will deny any request to exit made when the inside area has been armed. This can be used to prevent people from exiting an armed area. Users can still exit with a valid credential.
- **Deny Entry if Inside Area is Armed**: When this option is enabled the door will deny entry to all users when the door's inside area is armed.

  This option overrides the **Disarm area for door on access** option in the **Expanders | Reader expanders | Reader 1/2** programming, so users will be locked out even if they have access to disarm the area.

- **Deny Exit if Outside Area is Armed**: When this option is enabled the door will deny exit to all users when the door's outside area is armed.

  This option overrides the **Disarm area for door on access** option in the **Expanders | Reader expanders | Reader 1/2** programming, so users will be locked out even if they have access to disarm the area.

- **Prompt User for Access Reason Code**: With this option enabled, users who request access at the door must enter an access reason code at an associated keypad before the door will be unlocked.

  When the user badges their card the keypad will prompt them to enter an Area from 001-009, then press **[Enter]**. When they do, access will be granted and an event will be logged in the format: 'User Unlocked Door By Type [XX]'. The Type code in the event corresponds to the Area reason code minus 1, so that the codes Area 001-009 correspond to Type 00-08.

  Use of this feature requires the following settings in the **Expanders | Reader Expanders | Reader 1/2** programming:

  - **Reader 1/2 Keypad Type**: LCD keypad
  - **Keypad to Use for PINs Reader 1/2**: Select a keypad adjacent to the door

  This feature is not supported with card and PIN operation.

- **Enable Access Taken on Door Unlock Events**: With this option enabled, when a user is granted access at the door the system will record whether the requested access was taken or not. For example, if a card is badged and then the door is opened an 'Access Taken' event will be logged. If the door is not opened an 'Access Not Taken' event will be logged.

  When this option is not enabled the system will not indicate whether or not access was taken.

Extended Access Time Options

The antipassback options below apply when the door type associated with the door has antipassback settings configured (**Programming | Door Types | General**).

- **Door Extended Access Time**: The duration (in seconds) that the door will remain unlocked for users who require extended access times. This will override the **Lock Activation Time** for any users with the **User operates Extended Door Access Function** option enabled (**Users | Users | Options**).
- **Antipassback Entry/Exit User Reset Time***: If **Enable Timed User Antipassback Reset** is enabled below, these fields define the period (in minutes) for resetting the antipassback status of all users who have entered or exited the door.
- **Reset Antipassback Status On Schedule *** : With this option enabled, the antipassback status of all users who have accessed this door will be reset whenever the **Antipassback Reset Schedule** below changes states (i.e. becomes valid or invalid).
- **Enable Timed User Antipassback Reset *** : With this option enabled, the antipassback status of all users who have accessed this door will be reset periodically. The period is set in the **Antipassback Entry/Exit User Reset Time** fields above.

  For example, if the entry reset time is set to 120 minutes, every 2 hours the system will reset the antipassback status of all users who have entered the door during this time.
- **Antipassback Reset Schedule**: If **Reset Antipassback Status On Schedule** is enabled, this field defines the schedule used to reset antipassback status.

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 that the input is physically connected to (e.g. controller, input expander).
- **Module Address Input**: The **Physical Address** of the module that the input is connected to.
- **Module Input**: The index of the input on the connected module. See the relevant module installation manual for wiring instructions.

Configuration

- **Control Output/Output Group**: You can set an output or output group that is controlled by this input ('output follows input' control), which has a wide variety of applications. For example, you could set up a key switch that will unlock a specific door (one-to-one control) or configure a group of lights to turn on when the REX button is pressed (one-to-many control).

  The relationship between the input state and the output state must be configured in the input type programming (**Programming | Input Types | Options 3 | Control Options**).

  Alternatively, you can set a **Control Output / Output Group** in the input type programming, allowing many-to-one and many-to-many control (**Programming | Input Types | General**).

  > You must assign an area to the input and the area's 24hr portion must be armed to enable the control function. This is typically a dedicated 'control area'.

- **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's Reporting ID is the zone number which will represent that input to the monitoring station. Each newly created input will automatically be assigned a unique ID. Alternatively, you can manually assign an ID to each input, allowing a high amount of flexibility in input reporting. For example, if two inputs have the same Reporting ID they will both report as the same input.

  If an input has been assigned a number higher than the maximum that can be reported to a particular service, the highest possible number will be reported. Inputs and trouble inputs share the same range of zone numbers.

  > You can export Reporting IDs from **Monitoring | Events | Central Station Report**. For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

- **Alarm Input Speed**: This setting determines how long an input must be open before the system will register that it has been opened (alarmed). For example, if this is set to 30 seconds the input must be open for 30 seconds before an 'Input Opened' event will be generated.

  The alarm input speed can be set between 0 seconds and 1 hour. Shorter times are useful for inputs which require a rapid response, such as REX buttons. Longer times can be used to prevent alarms from being triggered by small amounts of movement.

  > If the alarm input speed is set to 0 seconds the restore input speed cannot be set below 100ms.

  > A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

- **Restore Input Speed**: This setting determines how long an input must be closed before the system will register that is has been closed (restored). For example, if this time is set to 30 seconds the input must be closed for 30 seconds before an 'Input Closed' event will be generated.

  The restore input speed can be set between 0 seconds and 1 hour.

If the alarm input speed is set to 0 seconds the restore input speed cannot be set below 100ms.

A module update will be required whenever this setting is changed. If the controller is registered as a reader expander this option must be set in the programming for the controller input, not the reader expander input.

- **Enable Input Lockout**: When this option is enabled, the input will lock out after a certain number of activations (the **Input Lockout Count**) to reduce false alarms.

  The activation counter is incremented every time the input is opened while the area is armed (regardless of whether it causes an alarm). Once the counter reaches the limit, the input is locked out and further activations will not cause alarms. The lockout is reset when the area is disarmed and rearmed again.
- **Input Lockout Count**: If this input uses the **Enable Input Lockout** feature above, this setting defines the number of times the input can be opened before it is locked out.

Commands

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

Inputs | Areas and Input Types

Much of an input's functionality is controlled by the areas and input types associated with it. The input type describes how the input will function in each area: for example, a door contact input might activate the entry delay in one area and instantly generate an alarm in another. Inputs can be programmed into up to four different areas, allowing the same input to be used for a variety of intrusion detection, control and automation functions in the system.

Changes to settings on this tab may require you to disarm and rearm the affected areas before they come into effect. You must rearm both the main and 24hr portions of the area. The controller will generate a health status message if rearming is required.

Assigned Areas

- **Area**: The area that monitors this input. Each input can be programmed into up to four different areas and perform different functions in each.
- **Input Type**: The input type defines how the input will operate in a particular area. A wide variety of options and preconfigured input types are available for functions such as intrusion detection, tamper detection, smoke/fire detection and automation/control.

  For example, the preconfigured Instant input type will cause the area alarm to activate immediately when the input is opened, while the Delay input type will cause the area's entry delay to start. For more, see **Programming | Input Types**.
- **KLES Input LED**: This is a legacy option that has no effect.

Inputs | Options

Options 1

- **Log to Event Buffer**: When this option is enabled the input will generate an event whenever it is opened, closed, tampered or shorted. Disable this option to prevent input events from being generated. The controller will still report alarms, restores and tampers to the monitoring station (as configured in the input type).

  It may be useful to disable event logging for inputs that are primarily used for automation or control to reduce their impact on event storage.
- **Test For Trouble Condition**: This is a legacy option that has no effect. Input trouble conditions (tamper and short) are generated and reported based on the settings in the input type (see **Generate 24hr Alarms** and **Report Tampers** in **Programming | Input Types | Options 1**).

- **Bypassing Not Allowed**: When this option is enabled the input cannot be bypassed (either temporarily or permanently) to arm an area. This should be used for high security inputs that should not be left open and unsupervised when an area is armed.

  This option will not prevent the area from being force armed when the input is open. To prevent this, ensure that the **Force input** option is disabled in the assigned input type (**Programming | Input Types | Options (1)**).

- **Latch Bypassing Not Allowed**: When this option is enabled the input cannot be latch bypassed (i.e. bypassed permanently); however, it can be bypassed temporarily until the area is next disarmed.

  This option will not prevent the area from being force armed when the input is open. To prevent this, ensure that the **Force input** option is disabled in the assigned input type (**Programming | Input Types | Options (1)**).

- **Tamper Follows Bypass State**: With this option enabled (by default) you can bypass a tampered input to allow the area to arm. With this option disabled the tamper condition cannot be bypassed, so you will not be able to arm an area with a tampered input.
- **No Bypass If Any Area Armed**: When this option is enabled this input cannot be bypassed if any of the four areas assigned in the **Areas And Input Types** tab are 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 this option is enabled if the expander module drops offline the controller will report that the input has a tamper condition. This only occurs if the module was previously registered and online with the controller.

Options 2

- **Input End of Line (EOL)**: The EOL resistor configuration used in the physical wiring for this input should be entered here. This determines whether the system can monitor the tamper and short conditions as well as open and closed. See the relevant installation manual for compatible EOL resistor configurations.

  A module update will be required whenever this setting is changed.

- **Contact Type**: The contact type used in the physical wiring for this input should be entered here. Inputs can be wired Normally Closed (default) or Normally Open. This setting determines how the input will be processed by the system.

  For example, REX inputs (buttons) are typically wired with a normally open contact. With this field set to Normally Open, when the button is not pressed the input will be marked as Closed/Off and when the button is pressed it will be marked as Open/On.

  A module update will be required whenever this setting is changed.

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 operating schedule determines when this particular door type is active. When this schedule is valid the settings in this door type will be used for those doors. When the schedule is invalid the settings in the **Secondary Door Type** set below will be used instead.

  For example, you might configure a door type so that Card only access is allowed during working hours. Outside of working hours the door uses the secondary door type with Card and PIN access to improve security.
- **Secondary Door Type**: The door type that is used when the **Operating schedule** set above is invalid. All settings from this door type are used (including e.g. antipassback settings).
- **Fallback Door Type**: This door type provides a fallback set of credentials that can be used to gain access to a door at any time.

  For example, if a carpark gate is configured to grant access based on license plate recognition it is helpful to have a traditional card reader available in case users need to open the gate without a car.

  Only the entry/exit credentials from the fallback door type are used, not other settings such as antipassback.

Entry / Exit

- **Entry/Exit Passback is Qualified with Door Opening***: By default, the user's current area is updated as soon as they are granted access to a door. With this option enabled the current area and antipassback status is not updated unless the user opens the door after being granted access.
- **Entry/Exit Passback Mode***: This field allows you to enable antipassback for this door type (in the entry and exit directions respectively). Enabling antipassback for a door allows it to monitor the areas that users are currently in, based on the **Area Inside/Outside Door** (which must be set in **Programming | Doors | General**).

  If a user attempts to move through a door from the wrong area they are violating the antipassback rules. The option selected here determines what happens in that situation:
  - **Hard Passback**: The user will be denied access until they enter the correct area or their antipassback status is reset.
  - **Soft Passback**: The user will not be denied access but a 'Soft Passback Violation' event will be logged.

  User antipassback status can be reset manually by right clicking on a user record or automatically on a timer or schedule using the options in **Programming | Doors | Advanced Options**.

  Antipassback has a number of applications. It is primarily used to prevent users from 'passing back' their access card or PIN to unauthorized persons, or to prevent people from 'tailgating' legitimate users. Antipassback can also improve the accuracy of area counting, muster reports and attendance reports, and allow you to manage loiter areas.

  Antipassback is global across the entire site. When a user passes through an antipassback controlled door the controller will update other controllers about the user's current area via cross controller operations. It may also be useful to enable the **Update user area when passback disabled** option in **Programming | Doors | Advanced options** for doors that are not using antipassback.
- **Entry/Exit Reading Mode**: The reading mode determines which credential or sequence of credentials the door will accept for entry or exit respectively. Even if users have valid permissions they will be denied access unless they have the correct type(s) of credential required by the door type.

  The default credentials available are: Card Only, PIN Only, Card And PIN, Card Or PIN, Card And Biometric, and Card Or biometric. Selecting Custom opens the **Entry/Exit Credential Types** tab, allowing you to enter a custom sequence of credentials.

Commands

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

Door Types | Options

Options

- **Door REX Not Allowed**: With this option enabled, REX (request to exit) operation will be disabled for any doors using this door type. This overrides the settings in the door programming.
- **Door REN Not Allowed**: With this option enabled, REN (request to enter) operation will be disabled for any doors using this door type. This overrides the settings in the door programming.
- **Requires Dual Authentication***: When this option is enabled any doors using this door type will require dual authentication (i.e. two separate user credentials) for access. To gain access, the following steps occur:
  - A user with **Dual Custody Master** enabled (**Users | Users | Options**) enters valid credentials.
  - The door activates the **Reader 1/2 Dual Authentication Pending Output** and waits for the second user. If the **Reader 1/2 Dual Authentication Wait Time** is exceeded the access request times out.

    Both options can be configured in **Expanders | Reader Expanders | Reader 1/2**.
  - A second user with **Dual Custody Master** or **Dual Custody Provider** enabled (**Users | Users | Options**) enters valid credentials.
  - Access is granted and the door unlocks.

  This feature is used for high security areas such as bank vaults or server rooms that require high levels of oversight. It can also be used to ensure there are always two people present in hazardous areas such as laboratories.
- **Dual Card Provider Can Initiate Access***: When this option is enabled, a **Dual Custody Provider** can initiate the dual authentication sequence without the requirement for a **Dual Custody Master**. Any combination of provider and master can initiate and complete the credential sequence.

Input Types

Input types define how an input operates in an area.

Configuration

- **Operating Schedule**: This schedule determines when this particular input type is active. When this schedule is valid the settings for this input type will be used. When the schedule is invalid the settings from the **Secondary Input Type** will be used instead.
- **Secondary Input Type**: When the **Operating Schedule** set above is invalid, inputs will use this secondary input type.
- **Keypad Alarm Display Group**: When an input using this input type generates an alarm only the keypads in this keypad group will display the alarm information. For example, you might want trouble input alarms to appear only on specific keypads available to installers and maintenance staff rather than regular users.

  If this field is not set all keypads will display alarms from these inputs.
- **Control Automation**: The automation that will be controlled by inputs with this input type. Automations can be used to control outputs, or can be connected to C-Bus groups for integrated building automation.

  You must assign an area to the input and the area must be armed to enable the control function. This is typically a dedicated 'control area'.

  For more information and programming instructions, see Application Note 289: C-Bus Integration with Protege GX and Protege WX.
- **Custom Reporting Code**: When this input triggers an alarm the custom reporting code determines the event code reported to the central monitoring station. It is also included as a 'Special Code' in the Protege WX event log.

  This allows you to provide more information about the type of alarm being triggered (e.g. medical alarm, smoke alarm, etc.). If this field is set to None the standard burglary code will be used.

  The custom reporting codes available here are drawn from Contact ID standard event codes. For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.
- **Control Output Time**: Inputs with this input type will activate the **Control Output / Output Group** (set below) for this period (in seconds). If this time is set to 0 the output will turn on indefinitely.

  This setting overrides the **Activation Time** set in **Programming | Outputs | General** and the **Output Time** set in **Programming | Output Groups | General**.
- **Control Output / Output Group**: This output or output group is controlled by inputs with this input type. The relationship between the input state and output state must be configured using the **Output Activation Options** (**Options 2** tab).

  This allows 'output follows input' control in a many-to-one or many-to-many configuration. For example, you might configure a group of lights to turn on when motion is detected on one of several PIRs in the room. You can also set a **Control Output / Output Group** in the input programming, allowing one-to-one or one-to-many control.

  You must assign an area to the input and the area's 24hr portion must be armed to enable the control function. This is typically a dedicated 'control area'.
- **Control Area**: This area can be force armed and/or disarmed by inputs with this input type. The relationship between the input state and the area state must be configured using the **Miscellaneous Options** in the **Options 2** tab.

  For example, this can be used to create key switches that will arm and disarm a specific area.

  The control area must have the **Enable Force Arming** option checked in **Programming | Areas | Options 2**.

Commands

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

Input Types | Options 1

Alarm options

- **Generate Alarms:** When this option is enabled, inputs using this input type will generate alarms. Alarms are generated when an input is opened in an armed area, causing the area to go into an alarm state. The bell output may be activated and the alarm may be saved to the area memory (depending on the settings in the **Options 2** tab).

  Disabling this option will prevent inputs with this input type from generating alarms. The inputs will still generate open/close events. For example, input types that are used only for automation do not need to generate alarms.
- **Generate 24HR Alarms**: When this option is enabled, inputs using this input type will generate 24hr (tamper) alarms. 24hr alarms (sometimes called tamper alarms) are generated when an input is tampered or shorted in an area with the 24hr portion armed. 24hr alarms do not put the area into alarm state or (normally) activate the bell output (but see the settings in **Options 3**).

  Trouble inputs also generate 24hr alarms when they are opened, however trouble input alarms do put the area into alarm and may activate the bell output as normal. This option should be enabled for any input type used by trouble inputs.
- **Entry Delay Input**: When this option is enabled, inputs using this input type will initiate the entry delay when they are opened in an armed area. Without this option enabled the area will go into alarm instantly without any entry delay.

  For example, this option could be enabled for inputs on external doors that are used to enter the building.
- **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 area is not in entry delay. 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**: With this option enabled, an input with this input type can be used to shorten the exit delay timer for an area. When the input is restored (closed) during exit delay the exit delay will be reduced to 5 seconds.

  For example, you might enable this option for a door contact so the area arms 5 seconds after the door is closed.
- **24hr Panic Input**: When this option is enabled, inputs with this input type will generate alarms even when the assigned area is not armed. A 'panic' action code will be included in the central station report. This allows inputs to act as 'panic buttons' and generate alarms whenever they are opened regardless of the area status.

  This feature uses 24hr tamper monitoring to generate alarms when the main area is not armed. Therefore, the following are also required:
  - The **Generate 24HR Alarms** option above must be enabled (however, **Generate Alarms** may be disabled).
  - The 24hr portion of the assigned area must be armed.

  To provide more information about the alarm you should also set the **Custom reporting code** in the **General** tab to an appropriate code.

- **Fire Input**: When this option is enabled, inputs using this input type will generate fire alarms when opened in an armed area. A 'fire' action code will be included in the central station report. It is recommended that you program any fire inputs in a dedicated fire area that is always armed.

  To provide more information about the alarm you should also set the **Custom reporting code** in the **General** tab to an appropriate code.

  Most smoke detectors use a normally open contact. Ensure that these inputs have the correct **Contact Type** and **Input End of Line (EOL)** settings (**Programming | Inputs | Options** tab).

Reporting options

- **Report alarms**: With this option enabled the controller will report all alarms generated by these inputs to the central monitoring station. In addition, a reporting event will be saved to the event log.

  The **Generate Alarms** option must be enabled for this option to function.

- **Report Tampers**: With this option enabled the controller will report all 24hr alarms (tamper alarms) generated by these inputs to the central monitoring station. This option should also be enabled to allow reporting of trouble input alarms. In addition, a reporting event will be saved to the event log.

  The **Generate 24HR Alarms** option must be enabled for this option to function.

- **Report Bypass**: With this option enabled the controller will report to the central monitoring station all instances where these inputs are bypassed to arm an area. It will also report when the bypass is removed. Reporting events will be saved to the event log.

  The **Report User Bypass** option must also be enabled in **Programming | Areas | Options 1**.

- **Report Restores**: With this option enabled the controller will report all input restore events to the central monitoring station. This occurs when an input is closed again after generating either an alarm or a 24hr alarm. Reporting events will be saved to the event log.
- **Stay Input**: When this option is enabled inputs with this input type will be monitored when the assigned area is stay armed. Inputs with this option disabled will not be monitored when the area is stay armed.

  For example, you may wish to stay arm an area to supervise the perimeter while people are still inside. In this case the **Stay Input** option should be enabled for perimeter inputs such as door contacts, and disabled for internal PIRs and other inputs.
- **Force Input**: When this option is enabled, inputs using this input type can be forced. This means that the assigned area can be force armed when these inputs are open without bypassing them. The inputs are still supervised and can still generate alarms if closed and opened again.

  If this option is disabled these inputs cannot be forced, however this can be overridden by the **Use Unattended Brute Force Arming** option in **Programming | Areas | Options 1**.

  You may need to bypass inputs when they are force armed to generate bypass reports. Enter one of the following commands in the **General** tab:

  - `EnableForceBypass = true` (bypasses the input until the area is disarmed)
  - `ForceSendsBypass = true` (bypasses the input until it is closed)
- **Exit Alley Input Do Not Test It**: Inputs with this option enabled will not be tested when the assigned area is arming. This means that the area can be armed even if these inputs are open and not bypassed.

  This should be used for inputs such as PIRs that overlook keypads and other arming points, which would otherwise need to be bypassed every time the area is armed. It should be used alongside the **Exit Delay Input** option.
- **Recycle Input Alarm on Exit Delay End**: By default, inputs with the **Exit Delay Input** feature do not generate alarms if they remain open after the exit delay ends. An alarm would only be generated if the input closes and opens again after arming. When this option is enabled any input that is still open at the end of the exit delay will be recycled (closed and opened again), generating an alarm.

  Use this feature for inputs that may be breached during exit delay, such as window or door contacts.

Input Types | Options 2

Miscellaneous Options

- **Activate Bell Output**: With this option enabled, when an input or trouble input with this input type generates an alarm the bell output for the assigned area is activated. This may be disabled in cases where a silent alarm is required (e.g. duress inputs).

  For regular inputs this option does not normally apply to 24hr / tamper alarms, but the **24hr Generates Bell if Armed** or **24hr Always Generates Bell** settings (**Options 3**) may be enabled as required.

- **Retrigger Bell Time**: When this option is enabled these inputs can retrigger the area's alarm/bell timer. If the alarm has already been activated when the input is opened the alarm timer will be reset to extend the time the bell output is activated.
- **Save To Area Memory**: When this option is enabled, alarms generated by these inputs will be saved to the area's alarm memory. The alarm memory can be viewed and acknowledged in the View menu of a keypad (**[Menu] [5] [1]**). Alarms in the memory are cleared the next time the area is armed.

  Disable this option to prevent alarms from being saved to the alarm memory.
- **Disarm Control Area On Input Restore**: When this option is enabled the **Control Area** set in the **General** tab will be disarmed when any input with this input type is closed (restored).
- **Arm Control Area On Input Alarm**: When this option is enabled the **Control area** set in the **General** tab will be armed when any input with the input type is opened (alarmed).

  It is not necessary to activate the area alarm to perform the control function.

- **Toggle Control Area On Input Alarm**: When this option is enabled, whenever an input with this input type is opened the state of the **Control Area** set in the **General** tab will be toggled. This means that each time the input is opened the area will switch from disarmed to armed, or vice versa.

  It is not necessary to activate the area alarm to perform the control function.

- **Allow Force Arming Of Tampered Input**: By default, areas cannot be force armed if they contain an input which is in a tamper state. With this option enabled, areas can be force armed even if inputs with this input type are tampered.

  The **Force Input** option must also be enabled in the **Options 1** tab.

- **Activate entry output on bell time**: This is a legacy option that has no effect.

Output Activation Options

- **Activate Bypass Output**: With this option enabled these inputs can activate the area's **Bypassed Inputs Output / Output Group**. This is activated when the area is armed with bypassed inputs in it, and deactivated when the area is disarmed.
- **Activate 24HR Tamper Output**: With this option enabled these inputs can activate the area's **Tamper Alarm Output / Output Group**. This is activated when an input generates a 24hr (tamper) alarm and deactivated when the area's 24hr portion is disarmed.
- **Activate Memory Output**: With this option enabled these inputs can activate the area's **Alarm Memory Output / Output Group**. This output is activated when an alarm occurs in an area and remains on until the area is disarmed.

  This feature can be used to indicate to users that there has been an alarm, preventing them from entering potentially insecure areas.
- **Input Retriggers Output Time**: When this option is enabled these inputs can be opened/closed a second time to restart the **Control Output Time** (**General** tab) so that the control output remains on for longer.

  For example, this can enable motion controlled lights to stay on for longer when a second person triggers the motion sensor.

  This feature also works with the **Control Output / Output Group** set in the input programming. The **Use Input Type Output Time** option must be enabled in the **Options 3** tab.

This option only functions correctly when the area assigned to the input is armed.

- **Activate Control Output On Alarm***: With this option enabled the **Control Output / Output Group** will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Activate Control Output On Restore***: With this option enabled the **Control Output / Output Group** will be activated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the input type programming (**General** tab).

- **Deactivate Control Output On Alarm***: With this option enabled the **Control output / output group** will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate Control Output On Restore***: With this option enabled the **Control Output / Output Group** will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the input type programming (**General** tab).

- **Toggle Control Output State On Alarm*:** With this option enabled the **Control Output / Output Group** will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the output will switch from off to on, or vice versa.

  This option refers to the control output set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

Input Types | Options 3

Automation Options

- **Activate Automation On Alarm**: With this option enabled the **Control Automation** will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Activate Automation On Restore**: With this option enabled the **Control Automation** will be activated whenever an input with this input type is closed (restored).

  This option refers to the control automation set in the input type programming (**General** tab).

- **Deactivate Automation On Alarm**: With this option enabled the **Control Automation** will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate Automation On Restore**: With this option enabled the **Control automation** will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control automation set in the input type programming (**General** tab).

- **Toggle Automation State**: With this option enabled the **Control Automation** will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the automation will switch from off to on, or vice versa.

  This option refers to the control automation set in the input type programming (**General** tab). It is not necessary to activate the area alarm to perform the control function.

- **24HR Generates Bell If Armed**: When this option is enabled, inputs with this input type can activate the area's bell output on a 24hr / tamper alarm, but only when the area is armed. The **Activate Bell Output** option must be enabled in the **Options 2** tab.

  This option is not required for trouble inputs.

- **24HR Always Generates Bell**: When this option is enabled, inputs with this input type will always activate the area's bell output on a 24hr / tamper alarm. The bell will be activated even if the area is not armed. The **Activate Bell Output** option must be enabled in the **Options 2** tab.

  This option is not required for trouble inputs.

Control Options

- **Use Input Type Output Time**: This option allows the **Control Output / Output Group** set in the input programming to use the **Control output time** set in the input type programming. When the control output is activated it will turn off after the period set in the input type.
- **Toggle Input Output State**: With this option enabled the **Control Output / Output Group** set in the input programming will be toggled whenever an input with this input type is opened (alarmed). This means that each time the input is opened the output will switch from off to on, or vice versa.

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

- **Activate Input Control Output On Alarm**: With this option enabled the **Control Output / Output Group** set in the input programming will be activated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

- **Activate Input Control Output On Restore**: With this option enabled the **Control Output / Output Group** set in the input programming will be activated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**).

- **Deactivate Input Control Output On Alarm**: With this option enabled the **Control Output / Output Group** set in the input programming will be deactivated whenever an input with this input type is opened (alarmed).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**). It is not necessary to activate the area alarm to perform the control function.

- **Deactivate Input Control Output On Restore**: With this option enabled the **Control Output / Output Group** set in the input programming will be deactivated whenever an input with this input type is closed (restored).

  This option refers to the control output set in the programming for each individual input (**Programming | Inputs | General**).

Input Types | Options 4

General Options

- **Always Log Input Event**: When this option is enabled, inputs with this input type will always generate events, regardless of whether the **Log to Event Buffer** option is disabled in the input programming (**Programming | Inputs | Options**).
- **Use Alternate Entry Time**: With this option enabled, whenever an input with this input type initiates an entry delay it will use the **Alternate Entry Time** set in **Programming | Areas | Configuration**. For example, you might use this for the door contact on a rear entry or a garage door to allow the user more time to reach the keypad.

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)**: The duration of the area's entry delay, in seconds. If an entry delay input is triggered while the area is armed the area will go into entry delay. If the area is not disarmed before this period elapses the alarm will be activated.

  If this time is set to 0 the area will immediately go into alarm, regardless of the input that is activated.

  For an input to begin the entry delay it must have **Entry Delay Input** enabled in the input type (**Programming | Input Types | Options 1**).

  The remote notify delay feature allows you to delay offsite reporting of alarms which occur during the entry delay. For more information, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

- **Alternate Entry Time (seconds)**: An alternative duration for the area's entry delay, in seconds. This will be used if the entry delay is triggered by an input with the **Use Alternate Entry Time** option enabled in the input type (**Programming | Input Types | Options 4**).

  This can be used to grant users a longer time to disarm the system when they enter through an alternative entrance, such as a garage or back door.

- **Exit Time (seconds)**: The duration of the area's exit delay, in seconds. Whenever the area is armed the exit delay will begin, giving users time to exit the area before it is armed. When the exit delay time elapses the area will be armed. If this time is set to 0 the area will arm immediately.

  During the exit delay, inputs with the **Exit Delay Input** option enabled (**Programming | Input Types | Options 1**) will not generate alarms. This should be used for any inputs that users may trigger as they exit the area (e.g. PIRs, door contacts).

- **Alarm Time (minutes)**: The duration (in minutes) that the bell output will stay on when the area alarm is activated. The minimum alarm time is 1 minute.

  Some areas may have limitations on how long a bell or siren can be activated. Ensure you check your local regulations before setting this field.

- **Smart Input Timer (seconds)***: The smart input feature prevents false alarms in areas by counting multiple unique input activations before activating the alarm. When an input is opened the alarm will not activate unless one or more additional inputs open within the period defined here (in seconds).

  To use this feature check the **Enable Smart Inputs** option in the **Options 2** tab. The number of inputs is defined by the **Smart Input Count** below.

- **Rearm Area Time (minutes)**: If the **Re-Arm Enabled** option is checked in the **Options 1** tab, whenever this area is disarmed it will automatically rearm after the time defined here (in minutes). If this time is set to 0 the area will rearm after 1 minute.

- **Vault Disarm Delay (minutes)***: If the **Vault Control Area** option is enabled in the **Options 2** tab, whenever a user attempts to disarm the area from a keypad there will be an additional delay before the area is disarmed. This field defines the delay time (in minutes). If this time is set to 0 the area will be disarmed immediately.
- **Vault Dual Code Delay (seconds)***: If the **Dual Code Vault Control** option is enabled in the **Options 2** tab the area will require two user codes to disarm. This field defines the time limit (in seconds) in which a second user must log in to the keypad and disarm the area, after the vault disarm delay period has elapsed. If the second user does not enter a PIN within this time, the disarming process will expire.
- **Recent Closing Time (seconds)**: This time (in seconds) defines how long after arming an area is considered to be 'recently closed'. If an alarm is generated in the area within this period (in seconds) a Recent Close message will be sent to the monitoring station along with the alarm message. This option will only function when the **Report Alarms** option is enabled for the relevant input in **Programming | Input Types | Options 1**.

  The alarm will be activated regardless of whether the area has been recently armed or not.

Schedule

- **Arm/Disarm Schedule**: This schedule can be used to arm and disarm an area automatically. The function depends on the options selected below. See also **Always Verify Area Schedule** in the **Options 2** tab.
- **Disarm Area When Schedule Starts**: When this option is enabled the area will automatically disarm when the **Arm/Disarm Schedule** above becomes valid.

  Use this option with caution, as the area will be disarmed regardless of whether there are any authorized users present.

- **Arm Area When Schedule Ends**: When this option is enabled the area will automatically arm when the **Arm/Disarm Schedule** above becomes invalid. This can be used to ensure that the area is secured each day even if the users forget to arm it.

  This feature force arms the area, so the **Enable force arming** option must be enabled (**Options 2** tab).

Setup

- **Child Area**: A child area may be armed and disarmed automatically based on the state of one or more parent areas. The relationship between the child and parent area status is based on the options selected in the **Options 1** tab.

  Since multiple parent areas can be applied to a single child area, this feature can be used to create a 'common area' that is dependent on a number of other areas.
- **Maximum Bypass Input Count**: The maximum number of inputs that can be bypassed within the programmed area. If more than this number of inputs have been bypassed the area cannot be armed. When this field is set to 0 there is no limit on the number of bypassed inputs.
- **Max User Count***: If the **Enable User Counting** option is selected (**Options 1** tab) this field allows you to set the maximum number of users who can be in the area at the same time. For example, if the user limit is set to 10 the 11th user who attempts to enter the area will be denied access.

  This feature is useful when there is a fire, security or health and safety code limiting the number of people allowed in a certain area, or to limit the number of users entering a carpark. You can set a **User Count Reached Output** (**Outputs** tab) that will be activated when the area is at its maximum user count.

  This field must be set to a value above zero to enable area counting. If there is no limit on the number of users allowed in the area you can set this field to the maximum value (65535).

- **Client Code**: This code represents the area in reports to the central monitoring station. This is typically a hexadecimal number but the format may depend on the receiver compatibility. If the client code for the area is left at the default value (FFFF) the area will use the **Client code** set in the reporting service (**Programming | Services | General**).
- It can be useful to set different client codes for each area in situations where a single Protege WX system contains multiple different tenancies, such as offices or apartments.

- **Interlock Area Group***: When an area has an interlock area group assigned it cannot be disarmed unless all other areas in the area group are armed. This can ensure that a high security area will not disarm until the areas surrounding it are secure.
- **Smart Input Count***: The smart input feature prevents false alarms in areas by counting multiple unique input activations before activating the alarm. The alarm will not be activated until this number of unique inputs have opened within a certain time.

  To use this feature check the **Enable Smart Input** option in the **Options 2** tab. The time period is set in the **Smart Input Timer** field above.
- **Reporting ID**: The area's Reporting ID is the group number which will represent that specific area to the monitoring station. The next available ID will be automatically assigned when each area is created, or you can manually assign the required IDs. If an area has been assigned a number higher than the maximum that can be reported to a particular service the highest possible number will be reported.

  You can export Reporting IDs from **Monitoring | Reporting | Central Station Report**.
- **Lock Door Group On Arming***: When this area is armed the doors in this door group will be automatically locked. This can be used to ensure that all entry doors for an area are locked when the area is armed, preventing users from accidentally entering an armed area.

Loiter

- **Loiter Time (minutes)**: This option is not used.
- **Loiter Reset Area**: This option is not used.

Defer Warning

- **Defer Warning Keypad Group***: When the area has the **Defer Automatic Arming** option enabled (**Options 2** tab) the keypads in this group will beep once and display a warning message when the area is about to arm automatically. While the message is displayed users can log in to the keypad and use the **[DISARM]** key to prevent the area from arming automatically.

  The **Display Defer Area Warning Messages** option must also be enabled for each keypad in **Expanders | Keypads | Options 1**. Higher priority messages (e.g. alarms) may override the defer arming warning.
- **Defer Warning Time (minutes)***: When the area has the **Defer Automatic Arming** option enabled (**Options 2** tab), automatic arming will be delayed by the time defined here (in minutes). Use this setting to give users sufficient time to leave the area or log in to the keypad and cancel the arming.

  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

This tab defines the primary reporting service for the area. This service will send reports for this area and any inputs or trouble inputs programmed in it.

Do not assign backup services to areas. When you assign the primary service, the area will automatically use the backup service when necessary.

Areas | Outputs

- **Bell Output / Output Group**: This output or output group is activated when an alarm is generated in the area. The bell output will remain on for the **Alarm Time** (**Configuration** tab) or until the area is disarmed.

  Whether the bell output is activated depends on the input type that generated the alarm. The **Activate Bell Output** option in **Programming | Input Types | Options 2** must be enabled.
- **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**: This output or output group is activated during the area's exit delay period. It is deactivated when the exit delay is complete or if the area is disarmed again.

  Use this output, commonly a keypad or reader beeper, to warn users to leave the area before it is armed.
- **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**: This output or output group is activated during the area's entry delay period. It is deactivated when the entry delay times out (activating the alarm) or when the area is disarmed.

  Use this output, commonly a keypad or reader beeper, to warn users to disarm the area before the alarm is activated.
- **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**: This output or output group is activated when the area is disarmed. It is deactivated when the area begins arming.

  This feature can be used to give users a visual indication when the area is disarmed (e.g. the green LED on a keypad). This could also be used to activate any lock relays that are not controlled by readers, so internal doors unlock when the area is disarmed. Disarmed outputs may also drive further processes that are activated when an area is disarmed.
- **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**: This output or output group is activated when the area is successfully armed. It is deactivated when the area is disarmed.

This feature can be used to give users a visual indication when the area is armed (e.g. the red LED on a keypad), preventing users from attempting to enter armed areas. Armed outputs are also useful for driving further processes that are activated when an area 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**: This output or output group is activated when the area is armed with one or more bypassed inputs. It is deactivated when the area is disarmed.

  This output will only be activated by inputs with **Activate bypass output** enabled in the input type (**Programming | Input types | Options 2**).

- **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**: This output or output group is activated whenever a 24hr / tamper alarm is generated in the area. It is deactivated when the area's 24hr portion is disarmed (disabled). This feature can be used to alert personnel that an input has been tampered, without activating the area's bell output.

  This output will only be activated by inputs with **Activate 24hr tamper output** enabled in the input type (**Programming | Input types | Options 2**).

- **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**: This output or output group is activated whenever an alarm is generated in the area. It is deactivated when the area is disarmed. This feature can be used to warn users when there has been an alarm, preventing them from entering a potentially insecure area.

  This output will only be activated by inputs with **Activate memory output** enabled in the input type (**Programming | Input types | Options 2**).

- **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** * : This output or output group is activated when the user count in an area reaches the **Max User Count** set in the **Configuration** tab. It is deactivated when the area no longer contains the maximum number of users. For example, this could be used in a carpark to activate a 'Carpark Full' sign when there are no more parks available.

  Enable User Counting must be selected in the **Options 1** tab.

- **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** * : This output or output group is activated whenever the area defers automatic arming. It is deactivated when the **Defer Warning Time** (**Configuration** tab) expires and the area arms or when the arming is canceled at a keypad. Use this feature to notify users in the area that it is about to start arming.

  Defer Automatic Arming must be enabled in the **Options 2** tab.

- **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**: This output or output group is activated for 5 seconds whenever the area fails to arm (for example, because there are inputs that have not been bypassed).
- **Ready output / output group**: This output or output group is activated when all of the inputs and trouble inputs programmed in the area are closed, signaling that the area is ready for arming. It is deactivated when the area is armed or when an input or trouble input is opened and the area is no longer ready to arm.

Areas | Options 1

General Options

- **Input Restore on Bell Cut-Off**: With this option enabled, when this area goes into alarm any inputs that are open enter a 'siren lockout' state. This means that if the inputs are restored (closed) or reopened it will not be reported to the monitoring station until the bell times out or is silenced.

  This option prevents the **Retrigger Bell Time** feature in **Programming | Input Types | Options 2** from functioning.

- **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 this option is enabled, whenever this area finishes arming the **Child Area** (**Configuration** tab) will be armed.

This option must be enabled in the parent area(s).

- **Arm Child If All Other Areas Are Armed**: When this option is enabled the **Child Area** (**Configuration** tab) will be armed whenever this area is armed, provided that all other parent areas are already armed. The **Arm Child Area** option above must also be enabled.

  For example, there may be three areas; A, B and C, where C is a child area of A and B. By default, C will be armed whenever either A OR B is armed. With this option enabled, area C will be armed when both A AND B are armed.

  This option must be enabled in the parent area(s).

- **Disarm Child Area**: When this option is enabled, whenever this area finishes disarming the **Child Area** (**Configuration** tab) will be disarmed.

  This option must be enabled in the parent area(s).

- **Disarm Child If All Other Areas Are Disarmed**: When this option is enabled the **Child Area** (**Configuration** tab) will be disarmed whenever this area is disarmed, provided that all other parent areas are already disarmed.

  For example, there may be three areas; A, B and C, where C is a child area of A and B. By default, C will be disarmed whenever either A OR B is disarmed. With this option enabled in both A and B, C will be disarmed when both A AND B are disarmed.

  This option must be enabled in the parent area(s).

- **Use Unattended Brute Force Arming**: Typically an area cannot be force armed if there are open inputs with the **Force Input** option disabled (**Programming | Input Types | Options 1**). Enabling this option allows you to 'brute force arm' the area using unattended or remote methods even if these inputs are open.

  Use this option to ensure that the area can always be force armed by the system (e.g. on schedule or automatic rearm), an operator or a user at a card reader. This will not allow users at a keypad to brute force arm the area.

  By default, when an area is brute force armed the status is set to Armed. To use Force Armed for the status, enter the `UnattendedForceArm = true` command.

Reporting Options

- **Report Arming**: With this option enabled, whenever this area is armed a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the arming. Disable this option when these reports are not required (e.g. for virtual control areas).
- **Report Disarming**: With this option enabled, whenever this area is disarmed a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the disarming. Disable this option when these reports are not required (e.g. for virtual control areas).
- **Report 24HR Area Disarming**: With this option enabled, whenever the 24hr portion of this area is disarmed (disabled) a report will be sent to the monitoring station and saved to the event log. This report includes the user who initiated the disarming. There is no equivalent report available for arming / enabling the 24hr portion of the area.
- **Report User Bypass**: With this option enabled, whenever this area is armed it will report all bypassed inputs in the area. The reports will be sent to the monitoring station and saved to the event log. The **Report Bypass** option must also be enabled for the relevant input(s) in **Programming | Input Types | Options 1**.
- **Report Entry Alarm Immediately**: When this option is enabled, if an entry input opens in an armed area a report will be sent to the monitoring station and the event log immediately, even though the area is in entry delay. A second report will be generated if the area goes into alarm. When this option is disabled an input opening that triggers entry delay will not be reported.

  This option applies to inputs with the **Entry Delay Input** and **Report Alarms** options enabled in the input type (**Programming | Input Types | Options 1**).

- **Enable User Counting***: With this option enabled the system will count the number of users in the area. When a user enters the area the count is increased by one, and when they exit the count is decreased by one.

  This feature should only be used in areas serviced by doors that have both entry and exit readers, as REX and REN will not alter the user count. The **Area inside/outside door** must be set correctly in **Programming | Doors | General**. It is recommended that user counting is used alongside antipassback (see **Programming | Door types | General**) to ensure that user counts are accurate.

  A number of features are available with user counting:

  - **Max User Count** (**Configuration** tab)

    This option must be set to a non-zero value for user counting to function.

  - **User Count Reached Output / Output Group** (**Outputs** tab)
  - **Arm On User Count At 0** (**Options 1** tab)
  - **Clear User Count When Armed** (**Options 1** tab)
  - **Prevent Arming On Count Not Zero** (**Options 2** tab)
- **Arm On User Count At 0***: When **Enable User Counting** is selected above, this feature causes the area to automatically arm when the user count reaches zero. This feature ensures the area will be secured when the last user leaves, regardless of whether they have actively armed it. This is especially useful in large office environments where it is not practical for users to check whether there is anyone else in the area.

  It is recommended that this feature is used alongside antipassback settings to ensure that the user count is accurate. If not, the area may arm while there are still people inside.
- **Clear User Count When Armed***: When this option is enabled (by default) the user count for the area (see **Enable User Counting** above) will be cleared / set to zero when the area is armed. When this option is disabled the user count will not be cleared.

Areas | Options 2

Advanced Options

- **Enable Stay Arming**: When an area is stay armed only inputs with the **Stay Input** option enabled (**Programming | Input Types | Options 1**) will be monitored. For example, this allows you to arm the perimeter of an area without arming the internal sensors, so that users can remain securely inside. With this option disabled the area cannot be stay armed.
- **Enable Force Arming**: When an area is force armed it is armed without testing the inputs. The area will be armed even if there are inputs open, provided that the inputs have the **Force input** option enabled (**Programming | Input Types | Options 1**). When this option is disabled the area cannot be force armed.

  See also **Use unattended brute force arming** below.
- **Enable Instant Arming**: When an area is instant armed it arms immediately with a 1 second exit delay. Also, all inputs that would normally initiate the entry delay instead trigger the alarm immediately (i.e. all inputs are treated as 'instant' inputs). When this option is disabled the area cannot be instant armed.

  Areas can be instant armed or instant force armed from the software, and instant stay armed or instant force armed from a keypad.
- **Do Not Arm if Trouble Condition**: When this option is enabled the area will be prevented from arming if there is any trouble input open in the system. This ensures that all trouble conditions are resolved before the area is armed.

  This is useful for high security areas which should not be vacated before all troubles are resolved.
- **Prevent Arming On Count Not Zero**: When user counting is enabled (**Options (1)** tab), this option prevents the area from arming when the user count is not zero. This ensures that the area cannot be armed (manually or automatically) when there are still users in the area.

It is recommended that this feature is used alongside antipassback settings to ensure the user count is accurate. If there is an error in the user count it may become impossible to arm the area even after all users have left.

- **Always Verify Area Schedule**: By default, the area only checks the **Arm/Disarm Schedule** (**Configuration** tab) on edges, i.e. when the schedule becomes valid or invalid. This means the area can be disarmed or armed manually regardless of the status of the schedule.

  When this option is enabled the area will verify the schedule every minute. If the area is not in the armed/disarmed state required by the schedule it will change to the correct state.
- **Area can be Reset**: When this option is enabled the area can be rearmed from a keypad without being disarmed first. This means that an area that goes into alarm can be reset (silencing the bell output) without being disarmed. Use this option for areas that should not be disarmed after an alarm.
- **Vault Control Area***: When this option is enabled the area will not disarm until the defined delay period elapses. The **Vault Disarm Delay** is set in the **Configuration** tab. This ensures that very high security areas such as bank vaults cannot be disarmed quickly in the case of a hold up.

  For more information and programming instructions, see Application Note 338: Programming Protege Keypads.
- **Dual Code Vault Control***: When this option is enabled two separate users must log in to a keypad and press the disarm button in order to disarm the area. After the first user presses disarm, the vault disarm delay must expire before the second user can enter their code. The time allotted for the second user to disarm the area is the **Vault Dual Code Delay** set in the **Configuration** tab.

  The **Vault Control Area** setting above must also be enabled.
- **Enable Smart Input***: By default, an area will go into alarm based on a single input activation. In smart input mode multiple unique inputs must be activated before the area will activate the alarm. This is useful for preventing false alarms.

  When an input is opened in the armed area a timer starts based on the **Smart Input Timer** (**Configuration** tab). The area will count unique input activations (reactivating the same input will not increase the counter). If the number of activations reaches the **Smart Input Count** (**Configuration** tab) the alarm will be activated. The same number of activations is required to initiate the entry delay.

  The response of the area depends on the input type of the final input that is triggered. For example, if the first input would start the entry delay but the last causes an instant alarm the area will go into alarm instantly.

  Smart inputs can be used alongside the remote notify delay feature to send confirmed alarm reports to the monitoring station. For more information, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

Arming Options

- **Always Force Arm Using Card Reader**: When this option is enabled, whenever a user arms an area using a card reader the area will be force armed. If this option is disabled open inputs can prevent the area from being armed.

  Options for arming using a card reader can be found under **Reader Arming Mode** in **Expanders | Reader Expanders | Reader 1/2**.
- **Disable Exit Output on Stay Arming**: When this option is enabled the **Exit Delay Output / Output Group** (**Outputs** tab) will not be activated when the area is stay armed. This is useful when there is no need to prompt users to leave the stay armed area.
- **Clear Alarm Memory after Arming**: When this option is enabled (by default) the area's alarm memory is cleared every time the area is armed. When it is disabled alarms will remain in the alarm memory until a user acknowledges them at a keypad (**[MENU] [5] [1]**).

- **Enable Late Arm Report**: When this option is enabled the system will generate a report for the monitoring station and event log whenever the area is armed later than expected. The report is generated if the area is still disarmed when the **Normal Arm Schedule** set below becomes invalid. This ensures that operators and monitoring stations are alerted to any anomalies.
- **Enable Early Disarm Report**: When this option is enabled the system will generate a report for the monitoring station and event log whenever the area is disarmed earlier than expected. The report is generated if the area is disarmed before the **Normal Disarm Schedule** set below becomes valid. This ensures that operators and monitoring stations are alerted to any anomalies.
- **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**: With this option enabled, when certain users disarm the area it will automatically rearm in stay mode after a period of time. Users must have the **Rearm Area In Stay Mode** option enabled in **Users | Users | Options**. The area will remain disarmed for the length of time specified in the **Rearm Time** setting (**Configuration** tab).

  This option is useful for allowing users to enter the building to temporarily disarm the area and remain inside while the perimeter is secured again.

  Stay arming must be enabled (above).

- **Defer Automatic Arming***: When this option is enabled, whenever the area begins arming automatically by a schedule the arming can be deferred (delayed) for a defined period of time. Users will receive notice that the area is about to arm, allowing them to leave the area or log in to the keypad and press the disarm key to defer the automatic arming.

  The **Always Verify Area Schedule** option (see above) **must be disabled** as it will override any defer arming.

  The following settings are available:
  - The **Defer Warning Time** (**Configuration** tab) determines how long the area will display the warning before beginning to arm.
  - You can give users a visual and/or audible indication that the area is about to arm using the **Defer Warning Keypad Group** (**Configuration** tab) and **Area Defer Arming Started Output / Output Group** (**Outputs** tab).
  - When a user defers arming from the keypad, the **Rearm Area Time** (**Configuration** tab) defines how long the area will wait before attempting to arm again.
  - Alternatively, the `AskForDeferTime = true` command allows users to specify the number of hours that arming will be deferred for when they cancel the arming at the keypad.
  - The `ReArmAsDeferArea = true` command allows the area to defer automatic rearming, so that defer arming can be used alongside the **Re-Arm Enabled** feature (**Options 1** tab).

  For more information and programming instructions, see Application Note 338: Programming Protege Keypads.

Squawk Options

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

- **Bell Squawk On Arming Start**: When this option is enabled the area's **Bell Output** (**Outputs** tab) will squawk (sound briefly) when the area begins arming.
- **Bell Squawk On Arming Complete**: When this option is enabled the area's **Bell Output** (**Outputs** tab) will squawk (sound briefly) when the area successfully finishes arming.

- **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.

  One or more of the other **Squawk Options** must also be enabled.

- **Bell Squawk On Disarm**: When this option is enabled the area's **Bell Output** (**Outputs** tab) will squawk twice when the area is disarmed.
- **Bell Squawk On Successful Report**: When this option is enabled the area's **Bell Output** (**Outputs** tab) will squawk when a successful 'Area Armed' report has been sent and acknowledged by the reporting service.

Schedule

- **Normal Disarm Schedule**: This schedule defines when the area is expected to be disarmed on any given day. Along with **Enable Early Disarm Report** above this allows you to generate reports if the area is disarmed earlier than expected.

  For example, you might set the normal disarm schedule to 8:30-9:30am every weekday. This represents when you expect the area to be disarmed for the first time. If the area is disarmed at 7:00am (before this schedule becomes valid) an event will indicate that the area is 'Early to Disarm'.
- **Normal Arm Schedule**: This schedule defines when the area is expected to be armed on any given day. Along with **Enable Late Arm Report** above this allows you to generate reports if the area is armed later than expected.

  For example, you might set the normal arm schedule to 4:30-5:30pm every weekday. This represents when you expect the area to be armed for the last time. If the area is still disarmed at 5:30pm (when the schedule becomes invalid) an event will indicate that the area is 'Late to Arm'.

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 that the output is connected to (e.g. keypad, output expander).
- **Module Address**: The **Physical address** of the module that the output is connected to.
- **Module Output**: The index of the output on the connected module. See the relevant module installation manual for wiring instructions.

Configuration:

- **Activation Schedule**: This schedule is used to automatically turn the output on and off. When the schedule becomes valid the output is activated. When the schedule becomes invalid the output is deactivated.

  By default, the activation schedule only controls the output when the schedule changes state (becomes valid or invalid). The output can still be controlled by other methods between these times. To ensure the output remains in the scheduled state enable **Always verify schedule** below.
- **Always Verify Schedule**: With this option enabled the output will verify the schedule every minute. If the output is not in the correct state it will be activated or deactivated to match the state of the schedule.
- **Activation Time (seconds)**: The duration (in seconds) that the output will stay on when it is activated. This applies to most methods of activation (e.g. manual activation, activation schedule, programmable function, automation). The output status will be shown as 'On Timed' on the monitoring page.

  If the activation time is set to 0 the output will remain on continuously until it is deactivated by any method.

  Some methods of output activation (e.g. output group, input type, access level) have specific times which may override the activation time.
- **Activation Retrigger**: With this option enabled, if an output is activated a second time when it is already 'On Timed' the activation time will restart. This allows outputs such as lights to stay on for longer when they are retriggered.

Commands

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

Outputs | Options

General

- **Log Output Events**: When this option is enabled the output will generate an event whenever it is activated or deactivated. Disable this option to prevent output events from being generated.

  You may disable event logging for outputs that are primarily used for automation or control (such as virtual outputs) to reduce their impact on event storage.
- **Invert Output**: When this option is enabled the output activation will be inverted. For example, if a light output is inverted deactivating the output will turn the light on and activating the output will turn the light off.

  A module update will be required whenever this setting is changed.

  If the output is on the controller, after changing this setting you must manually activate and deactivate the output.

Preset State

- **Preset Controller Power Up**: With this option enabled the output will be set to a specific state when the controller is restarted or powered on for the first time. If not, the output will be reset to its last known state.
- **Output Turns On When Controller Powers Up**: This option defines the initial state of the output when the controller powers up. With this option enabled the output turns on. With this option disabled the output turns off.
- **Preset Module Power Up**: With this option enabled the output will be set to a specific state when the module it is connected to is powered up. This will override the last known state of the output and the **Preset Controller Power Up** setting above.

  A module update will be required whenever this setting is changed.

- **Output Turns On When Module Powers Up**: This option defines the initial state of the output when the connected module powers up. With this option enabled the output turns on. With this option disabled the output turns off.
- **Preset Module Offline**: With this option enabled the output will be set to a specific state when the connected module goes offline. For example, this could be used to turn on an indicator light or beeper when a module goes offline, or ensure that emergency lighting turns on if a connection is damaged.

  A module update will be required whenever this setting is changed.

- **Output Turns on When Module Offline**: This option defines the state of the output when the connected module goes offline. With this option enabled the output turns on. With this option disabled the output turns off.

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.
- **Operating schedule**: The operating schedule determines when this particular menu group is active in an access level. When the schedule is valid the settings in this menu group will be used. When the schedule is invalid the settings from the **Secondary menu group** below will be used.
- **Secondary menu group**: When the **Operating schedule** above is invalid the secondary menu group will be used by access levels.

Settings

- **Area (1)**: When this option is enabled, users can access the area menu by pressing **[MENU] [1]** on the keypad. This menu allows users to arm and disarm areas.
- **User (2)**: When this option is enabled, users can access the user menu by pressing **[MENU] [2]** on the keypad. This menu allows users to change their own PIN and edit user records.
- **Events (3)**: When this option is enabled, users can access the events menu by pressing **[MENU] [3]** on the keypad. This menu allows users to view events saved on the controller.
- **Installer (4)**: When this option is enabled, users can access the installer menu by pressing **[MENU] [4]** on the keypad. This menu allows users to view and control the status of devices in the system and change the IP address of the controller.
- **View (5)**: When this option is enabled, users can access the view menu by pressing **[MENU] [5]** on the keypad. This menu allows users to view and control the alarm memory, system troubles and some device statuses.
- **Time (6)**: This is a legacy option that has no effect.
- **Bypass (7)**: When this option is enabled, users can access the bypass menu by pressing **[MENU] [7]** on the keypad. This menu allows users to bypass inputs.
- **System (8)**: This is a legacy option that has no effect.
- **Extended time menus (6, 2-4)**: This is a legacy option that has no effect.
- **Bypass trouble input (7, 2)**: This is a legacy setting that should not be used.

  It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

- **Area group control allowed**: When this option is enabled, users can press the **[RIGHT]** arrow key from the area menu to arm/disarm the keypad's area group.

  The keypad must have an **Area group for this keypad** set (**Expanders | Keypads | Configuration**) and **Allow area group selection access** enabled (**Expanders | Keypads | Options 1**).

- **Tamper area control allowed**: When this option is enabled, users can press the **[LEFT]** arrow key from the area menu to arm/disarm the 24hr portion of each area.

  The keypad must also have **Allow 24hr area access** enabled (**Expanders | Keypads | Options 1**).

- **Stay arming**: When this option is enabled, users can stay arm areas by pressing the **[STAY]** key. The area(s) must have stay arming enabled in **Programming | Areas | Options 2**.
- **Force arming**: When this option is enabled, users can force arm areas by pressing the **[FORCE]** key. The area (s) must have force arming enabled in **Programming | Areas | Options 2**.
- **Instant arming**: When this option is enabled, users can instant arm areas by holding the **[STAY]** key (instant stay arm) or **[FORCE]** key (instant force arm) for two seconds. The area(s) must have instant arming enabled in **Programming | Areas | Options 2**.

Menu Groups | Keypad Groups

You can assign keypad groups to a menu group to restrict the menu permissions to those keypads only. This allows you to grant users specific permissions at different keypads by assigning multiple menu groups to a single access level.

If there are no keypad groups assigned here the menu group applies to all keypads on this site.

It is important that there is only one menu group applied to each keypad that a user can access. If multiple menu groups are available for a keypad the controller will not know which permissions should be presented to the user. This can result in undefined system operation.

Menu Groups | Options

- **User advanced menu**: This is a legacy option that has no effect.
- **Installer menu group**: This option can be enabled for menu groups used by site installers and technicians. When a user with this menu group logs into the keypad the Installer Logged In trouble input is opened.

  In addition, users with this menu group assigned can stay logged in to the keypad indefinitely, regardless of the **Time user is logged in** setting in **Expanders | Keypads | Configuration**. This is convenient for installers who will be commissioning and maintaining the site.
- **Show user greeting**: Enable this option for the keypad to display a personal greeting to the user when they log in. For example, when the user John Smith logs in to the keypad at 9am it will display the message, 'Good Morning John Smith'. This option may be disabled to decrease the time it takes to log in to a keypad.

  This option is equivalent to the **Show a greeting message to user** option in **Users | Users | Options**. The greeting will be displayed if either option is enabled for the user.
- **User can acknowledge alarm memory**: When this option is enabled, users with this menu group assigned are able to acknowledge alarms in the alarm memory. Users can access the alarm memory by pressing **[MENU] [5] [1]**. The user must also have access to the **View** menu (**General** tab).

  When this option is disabled, users can view alarms but cannot acknowledge them.

  This option is equivalent to the **User can acknowledge alarm memory** option in **Users | Users | Options**. Alarms can be acknowledged if either option is enabled for the user.
- **Show user alarm memory on logon**: When this option is enabled the keypad will automatically display the alarm memory for the keypad's primary area to the user when they log in to the keypad. The user must also have access to the **View** menu (**General** tab).

  This option is equivalent to the **Show alarm memory on login** option in **Users | Users | Options**. The alarm memory will be shown if either option is enabled for the user. The keypad's primary area can be set as the **Area this LCD belongs to** (**Expanders | Keypads | Configuration**).

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 device that the trouble input is associated with (e.g. controller, reader expander, door).
- **Module Address Input**: The **Physical address** of the module or name of the door that the trouble input is associated with.
- **Module Input**: The index of the trouble input on the associated module. This determines what system trouble the trouble input monitors and the event code that is sent to the monitoring station when this trouble input generates an alarm. For example, trouble input 3 on an analog expander opens when there is a 'Battery Low / Missing' condition, and sends an event code of 302.

  See the Trouble Inputs section of the relevant installation manual for a full list for each module.

Configuration

- **Trouble Group**: The trouble groups and associated **Trouble group options** below determine how trouble conditions will be displayed on the keypad. Setting these fields will allow this trouble input to be displayed on the keypad in the Installer View menu, which is useful for technicians checking the system for issues. In addition, a custom message based on the selected trouble group option will be displayed in the Trouble View menu, and if enabled on the keypad, also in the Offline Trouble View menu.

  There is typically no need to edit the trouble groups as they are automatically set for each trouble input.

  The available trouble groups are as follows:
  - **0 - None**: This trouble input does not fall under any of the categories below and will not be displayed on the keypad. This option is used for trouble inputs that technicians on site do not need to be aware of (e.g. 'Installer Logged In').
  - **1 - General**: This trouble group consists of troubles that are relevant to the general operation of the system. This includes conditions such as AC failure, reporting issues and input faults.
  - **2 - System**: This trouble group is used for module related troubles (e.g. module tamper).
  - **3 - Access**: This trouble group is used for troubles that are related to access control and door operation (e.g. forced door, too many access attempts).

  Users can access the Trouble View menu by logging in to a keypad and pressing **[MENU] [5] [2]**, and the Installer View menu by pressing **[MENU] [4] [1] [2]**. Here they can view the current system troubles.

  If enabled on the keypad (**Expanders | Keypads | Options 2**), the Offline Trouble View menu can be accessed by pressing **[MENU] [2]**, without logging in to the keypad.

  These fields do not affect the event codes used for reporting.
- **Trouble Group Options**: The trouble group option determines what message will be displayed on keypads when this trouble input is open. Each option that can be selected has one or more variants, depending on the **Trouble Group** selected above. If the trouble group is set to 1 the first entry in each option will be used, and so on.

  There is typically no need to edit the trouble group options as they are automatically set for each trouble input.
- **Reporting ID:** The trouble input's reporting ID is the **Zone ID** index which will represent that trouble input to the monitoring station. You can manually assign an ID to each input, allowing a high amount of flexibility in input reporting. For example, if two inputs have the same Reporting ID they will both report as the same input.

Every trouble input must have a reporting ID assigned, so each newly created trouble input will be automatically assigned the lowest available ID. If a trouble input has been assigned a number higher than the maximum that can be reported to a particular service the highest possible number will be reported.

You can export Reporting IDs from **Monitoring | Reporting | Central Station Report**. Inputs and trouble inputs share the same range of Zone IDs but trouble inputs typically use higher indexes.

Commands

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

Trouble Inputs | Areas And Input Types

Like inputs, trouble inputs can be assigned to up to four areas, with a separate input type programmed in each. The input type defines how the trouble input will function in that area.

By default, trouble inputs are assigned to the predefined System Area with the Trouble Silent input type.

Assigned Areas

- **Area**: Each trouble input can be programmed into up to four different areas. Typically trouble inputs are assigned to a 'system area' which is used to monitor system troubles.
- **Input Type**: The input type defines how the trouble input will operate in that particular area. For example, the Trouble Silent input type will allow the trouble input to generate 24hr / tamper alarms without activating the area's bell output, while the Trouble Bell input type will cause the bell output to be activated.

Trouble Inputs | Options

General Options

- **Log to Event Buffer**: When this option is enabled (by default) the trouble input will generate an event whenever it is opened or closed. Disable this option to prevent trouble input events from being generated, reducing their impact on event storage. Reports will still be sent to the monitoring station.
- **Bypassing Not Allowed**: It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.
- **Latch Bypassing Not Allowed**: It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

Advanced Options

- **No Bypass If Any Area Armed:** It is possible to bypass trouble inputs from the keypad, but the bypass can only be removed by power cycling the controller. Therefore, it is recommended that you disable bypassing for trouble inputs.

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 building.

For more information and instructions, see Application Note 248: Low Level Elevator Control in Protege GX and Protege WX.

Configuration

- **Reader Expander**: Elevator cars must be associated with the reader expander that is used to control user access in that car.

  The **Reader 1/2 Mode** and **Reader 1/2 Elevator** must also be set correctly for that reader expander (**Expanders | Reader expanders | Reader 1/2**).

- **Reader Port**: The reader expander port that controls access in this elevator car.
- **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)**: This option is not used.
- **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**: Destination reporting allows the system to track which floor a user has selected. When a user is granted access, instead of immediately unlocking all floors the system will wait for an input activation. The user can select a single floor that they have access to, and only that floor will be unlocked. In addition, an event will be logged recording the specific floor the user has selected.

  This is useful for higher security situations where it may be important to know specifically which floors users are traveling to. It also prevents users pressing multiple floor buttons after gaining access.

  Destination reporting has specific wiring requirements which are different from those for basic elevator control.

Authentication Mode

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

This tab allows you to add the floors that are accessible from this elevator car, and configure how that floor will operate.

Click **Add** to add a new floor to the elevator car, and set the following:

- **Schedule**: This field sets an unlock schedule for the floor. When this schedule is valid the floor can be accessed freely from this elevator car without credentials. When the schedule is invalid credentials are required to access the floor.

  By default, the unlock schedule only controls the floor when the schedule changes state (becomes valid or invalid). The floor can still be controlled by other methods between these times. To ensure the floor remains in the scheduled state enable **Verify**.
- **Area**: This field sets the inside area for this floor (i.e. the area that users enter when they disembark from the elevator car). The inside area must be set to allow integration of area control with elevator access using the **Follow Area** and **Disarm Area** options.
- **Late To Open**: With this option enabled, when the **Schedule** becomes valid the floor will not unlock until a user has successfully gained access. This prevents floors from unlocking on schedule on days when no one arrives.

  This feature requires destination reporting.
- **Verify**: With this option enabled the floor state will be checked every minute and updated to match the schedule. If the schedule is valid the floor will be unlocked. If the schedule is invalid the floor will be locked.
- **Follow Area**: When this option is enabled the floor will follow the status of the assigned **Area**. If the area is armed the floor will lock. If the area is disarmed the floor will unlock.
- **Input**: The input set here corresponds to the floor select button in the elevator car. This is a required setting for destination reporting. This field is not required if destination reporting is not in use.
- **Output**: The relay output set here corresponds to the floor select button in the elevator car. One output is required per controlled floor in every elevator car, but not for uncontrolled floors (always unlocked). This is required configuration for both basic control and destination reporting.
- **Disarm Area**: When this option is enabled the **Area** for this floor will be automatically disarmed whenever a user with sufficient permissions is granted access. In addition, if the area is armed and the user does not have sufficient permissions to disarm it the user will be denied access.

  This feature requires destination reporting.

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).

For more information and instructions, see Application Note 248: Low Level Elevator Control in Protege GX and Protege WX.

General

- **Name**: The name of the floor.
- **Floor Relay**: The floor relay represents the level of the floor as programmed in the system. Floor relays must be unique, programmed in numerical order (starting at 1), and start at the lowest accessible floor, including any basement floors. Rear elevator doors should be programmed with floor relays starting from 65.

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**: This schedule determines when this phone number can be called. When the schedule is valid the phone number set in this record will be called. When the schedule is invalid the secondary phone number will be called. This allows you to set an alternative phone number to call after hours.
- **Secondary Phone Number**: This phone number record will be used when the **Operating Schedule** is invalid. The operating schedule of the secondary phone number must be valid.
- **Phone Number**: The telephone number that will be used by this record.

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**: This reporting service sends alarms, tests and other events to a monitoring station over a phone line using the controller's onboard modem dialer. Reports are sent in the standard Ademco Contact ID format.

    Phone line reporting is only available for controller models with onboard modem dialers.
  - **Report IP**: This reporting service sends alarms, tests and other events to a monitoring station over an IP connection. 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. This allows the Protege system to be monitored and controlled externally through custom made applications.
  - **C-Bus *** : Provides integration with building control and automation products using the Clipsal C-Bus protocol.
- **Service Mode**: Determines how the service will start. The Manual mode setting ensures that the service will only start by manual command from an operator (right clicking on the record). The Start with controller OS setting configures the service to start automatically when the controller boots up.

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.

For more on the Contact ID format see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

Contact ID | General

- **Client Code**: This code represents the controller or site in reports to the central monitoring station. This is typically a hexadecimal number with 4 digits but the format may depend on the receiver compatibility. This will be issued by the monitoring station.

  Client codes can also be set for individual areas in **Programming | Areas | Configuration**.
- **PABX number**: If the controller is connected to an internal phone network it will first dial this number to gain an external phone line. If the PABX number is disabled by an **Operating schedule** (**Programming | Phone numbers | General**) the external number will be dialed immediately.
- **Phone number 1**: The primary phone number for the monitoring station. The controller will dial this number first to report events.
- **Phone number 2**: This phone number is used when the controller cannot make a connection with either **Phone number 1** or the **Phone backup**.

- **Phone backup**: This phone number is used when the controller cannot make a connection with **Phone number 1**. The sequence of dialing attempts depends on whether **Use alternate dialing method** is enabled in the **Options** tab.

Contact ID | Options

- **Use Alternate Dialing Method**: This option determines the order in which the service will try the various phone numbers programmed in the **General** tab if **Phone number 1** fails.

  The options are:

  - **Sequential** (this option disabled): When **Phone number 1** fails the service continues to try this phone number until it reaches the maximum **Dial attempts** (**General** tab). If all attempts fail the service repeats this process with the **Phone backup**, then with **Phone number 2**.
  - **Alternate** (this option enabled): When **Phone number 1** fails the services tries the **Phone backup** once, then tries **Phone number 1** again, then repeats in an alternating fashion. When both numbers have reached the maximum **Dial attempts** the service tries **Phone number 2** until it also reaches the maximum number of attempts.

  When all numbers have reached the maximum dial attempts the Reporting Failure trouble input is opened.
- **Pause After PABX**: When this option is enabled the dialer will insert a pause of 2.5 seconds after dialing the PABX number.
- **Report open**: When this option is enabled the service will report disarming (opening) for all areas using this service.
- **Report close**: When this option is enabled the service will report arming (closing) for all areas using this service.
- **Report alarms**: When this option is enabled the service will report input alarms.
- **Report tampers**: When this option is enabled the service will report input tampers and trouble input alarms.
- **Report restore**: When this option is enabled the service will report input restores.
- **Report bypass**: When this option is enabled the service will report input bypasses.
- **Service operates as backup**: When operating as a backup the service will not begin reporting unless it is initiated by another service that has failed to report. This service will report any messages from the primary service which failed to send, and then return operation to the primary. The backup service starts and stops at the same time as the primary service.

  Only Report IP services have the option to set a **Backup service** (**General** tab).
- **Log modem events to event buffer**: When this option is enabled, detailed events describing the call progression will be saved to the event log for every report. This can be used for troubleshooting issues but should be turned off during normal operation as large numbers of events will be generated.

Contact ID | Settings

- **Dial Attempts**: Determines how many times the controller will attempt to dial each number before moving on to the next backup number. This limit applies even when the report was successful.

  For UL/ULC installations (with **Enable UL Operation Mode** enabled in **Sites | Controllers | Options**) the controller will not allow values above 8.
- **Port Attempts**: Determines how many times the service will attempt to gain access to the onboard modem before reporting a communications failure. This may occur when another service is using the same port for communications.
- **Report count**: Determines how many reports the service can send in each call to the monitoring station. When set to 0, all pending reports can be sent in one call. This is acceptable for most scenarios, but confirm with your central monitoring station.

  When using multiple reporting paths that can report the same event to multiple locations, a limit of 8-16 is recommended. If the limit is reached, the controller will dial out again to send any remaining messages.

- **Handshake Time**: The length of time (in seconds) that the controller will wait to receive a handshake message response from the remote receiving unit. This can be adjusted if a longer than normal call completion time is required.
- **Dial Time**: The length of time (in seconds) that the controller will wait following a failed reporting attempt before redialing or dialing a backup number. The minimum value is 10 seconds.
- **Off Hook Output / Output Group**: This output or output group is activated when the service begins using the modem and is deactivated when the communication is completed. It can be used with remote exchange systems that require ground start communication connections.
- **Report OK Output / Output Group**: This output or output group is activated when the service successfully completes a report. It is not deactivated automatically, and should be programmed with an **Activation time** (**Programming | Outputs**) to ensure that it is turned off between reports.

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**: This code represents the controller or site in reports to the central monitoring station. An account code for Report IP can be up to 8 digits. Any leading zeros will be truncated so that the minimum number of digits possible is sent (e.g. 004311 is shortened to 4311). If the client code is longer than the reporting format allows it will be truncated.
- **Reporting Protocol**: The Report IP Service supports a number of reporting formats. This includes versions of traditional formats that can be sent over an IP connection, providing maximum flexibility.
  - **Armor IP**: ArmorIP is a proprietary IP reporting protocol by ICT. Reports are sent to an installed ArmorIP server which provides a standard Ademco 685 output and allows routing and redirection of messages to other receivers. This format provides full textual transmission that includes the names of the records (user, area, input) that generated the report and additional information such as field time and controller name. It also includes standard ContactID codes for automation.

    ArmorIP reporting is available in both UDP and TCP modes, and either encrypted or unencrypted.

For more information, see the ArmorIP Version 3 Internet Monitoring Application User Manual.

  - **SIA over IP (DC09)**: Communicates in the SIA Level 2 format using the SIA DC09 specification for digital communication.
  - **CID over IP**: Communicates in the Contact ID format using the SIA DC09 specification for digital communication.
  - **CSV IP**: CSV IP is an IP reporting protocol used by Alarm New Zealand. This is a generic ASCII protocol which takes the form: username, password, client code, message. This service sends report messages in Contact ID format.
  - **Patriot LS30**: Patriot LS30 is a proprietary IP reporting protocol by Patriot Systems. This service sends report messages in a variant of the Contact ID format.
- **CSV-IP Username/Password**: The username and password required for the CSV-IP protocol.
- **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 time (in seconds) between polling messages sent from the controller to the receiving server. The polling message format depends on the **Reporting Protocol** set above.

  Ensure that the same poll time is set at both the controller and the receiver.

- **Backup Service**: The backup service will be used when the Report IP service suffers a communication loss. It is useful to select a service that connects over the phone line to ensure that reports can be sent over an alternative connection when there is a cable failure or internet outage.

  The service selected here must have **Service Operates As Backup** enabled in the **Options** tab.

- **Time Before Switching to Backup (seconds)**: If a **Backup service** is configured above, this field defines the length of time (in seconds) that the IP connection must be lost before the service will activate the backup.

Primary / Secondary Channel Settings

The secondary channel provides a backup path for communication with the monitoring station should the primary channel fail. If the primary channel cannot be used the service will try the secondary channel before starting the backup service.

The two channels should at minimum have different IP addresses and/or port numbers. For higher reliability use two different mediums for internet access, such as both wired and wireless connections.

- **IP Address / Host Name**: The address of the receiver that messages are sent to.
- **IP Port Number**: The port used for communication with the receiver. This will depend on the configuration of the receiver software or hardware.
- **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 attempt to open the communications port before logging a communication failure and switching to the other channel or a backup service. To bypass this setting use the **Switch Secondary IP Immediately** option (**Options** tab).
- **Ack Wait Time**: The length of time (in seconds) that the service will wait for an acknowledgement (ACK) packet from the receiver before resending the report.
- **Report Fail Output / Output Group**: This output or output group is activated when the service experiences a communication failure. It is deactivated when communication is restored.
- **Enable Offline Polling**: Offline polling occurs when the service is not normally in use, i.e. operating as a backup. If the backup service loses connection the Reporting Failure trouble input will open and a report will be sent to the monitoring station. This ensures that any issues are detected before the backup service is required.
  - **Communication Failure Report Code/Group/Number**: The Contact ID event code, group number and zone number sent when the offline polling fails.

- **Offline Poll Count**: The number of offline polls that must fail before the connection failure is reported.
- **Offline Test Report Time**: The time between offline polls, in minutes.

Report IP | Options

- **Switch Secondary IP Immediately**: With this option enabled, when the primary channel fails to connect the service will immediately attempt the secondary channel instead of making multiple attempts to connect over the primary (i.e. the **Port Open Attempts** setting is ignored).
- **Report open**: When this option is enabled the service will report disarming (opening) for all areas using this service.
- **Report close**: When this option is enabled the service will report arming (closing) for all areas using this service.
- **Report alarms**: When this option is enabled the service will report input alarms.
- **Report tampers**: When this option is enabled the service will report input tampers and trouble input alarms.
- **Report restore**: When this option is enabled the service will report input restores.
- **Report bypass**: When this option is enabled the service will report input bypasses.
- **Log Acknowledge Response**: When this option is enabled, an event will be logged whenever an acknowledgment (ACK) packet is received from the monitoring receiver. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log Polling Message**: When this option is enabled, an event will be logged whenever a polling message is sent to the monitoring receiver. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log Message Retries**: When this option is enabled, an event will be logged whenever the service resends a failed message.
- **Log Reporting Failure**: When this option is enabled, an event will be logged whenever communications have failed completely and the service is waiting to make another attempt.
- **Service operates as backup**: When operating as a backup the service will not begin reporting unless it is initiated by another service that has failed to report. This service will report any messages from the primary service which failed to send, and then return operation to the primary. The backup service starts and stops at the same time as the primary service.

  Only Report IP services have the option to set a **Backup service** (**General** tab).

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**: The TCP/IP port that the service will use to communicate.
- **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.
- **Checksum Type**: Sets the type of checksum 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**: The default method of sending multi byte numbers is Little Endian (least significant byte first). With this option selected, multi byte numbers will be sent as Big Endian (most significant byte first).
- **Allow Status Requests When Not Logged In**: When this option is enabled the external program connected to the service can request and receive status updates (e.g. area status) without logging in. The program cannot send control commands (e.g. disarming the area) without logging in with a valid user PIN.
- **Use Logon Lock Out Timer if Incorrect PIN is Supplied**: When this option is enabled, if an incorrect PIN is supplied three times in a row the service will block further attempts for 60 seconds.
- **Ack Commands**: With this option enabled the service will send an acknowledgment (ACK) packet to the external program after it successfully receives a control command.
- **Expect Ack For Status Monitoring**: With this option enabled the service will expect an acknowledgment (ACK) packet to be returned after it sends a status update. If no ACK is returned within 3 seconds the status update will be resent.
- **Resend Status Monitoring If Not Ack after 5 Attempts**: If **Expect ACK For Status Monitoring** is enabled above, this option controls the cut off criteria for unacknowledged status updates.

  When this option is enabled the service will resend each status message until it receives an ACK from the external program. When this option is disabled the service will stop sending a status update if it has not been acknowledged after 5 attempts.
- **Expect Ack for Events**: With this option enabled the service will expect an acknowledgment (ACK) packet to be returned after it sends an event. If no ack is returned within 3 seconds the event will be resent.
- **Resend Events if not Ack after 5 Attempts**: If **Expect ack for events** is enabled above, this option controls the cut off criteria for unacknowledged events.

  When this option is enabled the service will continue sending each event until it receives an ACK from the external program. When this option is disabled the service will stop sending an event if it has not been acknowledged after 5 attempts.

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 C-Bus network interface that the controller is communicating with.
- **CNI Port**: The IP port used to communicate with the C-Bus network interface. This should be the same port used for communications between the CNI and the C-Bus Toolkit software.
- **Communication Failure Output / Output Group**: This output or output group is activated when there is a communication failure with the CNI.

Options

- **Enable Text Output**: Enable this option to convert communications from the controller to a human readable format. This allows for debugging if a monitoring device is used in place of the CNI; however, the integration will not function with this option enabled.
- **Add CR to Text Output**: When **Enable Text Output** is in use, enabling this option adds a carriage return character onto the end of each message.
- **Add LF to Text Output**: When **Enable Text Output** is in use, enabling this option adds a line feed character onto the end of each message.

- **Log C-BUS PCI Failure Message**: With this option enabled, error events will be logged when the CNI fails to initialize. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log C-BUS ACK Message**: With this option is enabled, events will be logged for each acknowledgement (ACK) packet received from the CNI. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.
- **Log C-BUS Data Activity**: With this option enabled, events will be logged for all packets sent to and received from the CNI. This option may be useful for initial configuration and troubleshooting but should be disabled during normal operation to save event storage.

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 monitor power supplies
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 OSDP readers and standalone locking devices
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** * : Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.

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 monitor the power supplies connected to your Protege WX system.

Configuration

- **Invert Device Tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.
- **Virtual Module** * : Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Physical Address**: The device address of the analog expander.

Commands

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

Analog Expanders | Channel 1-4

The options in this tab are not used.

Input Expanders

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

Configuration

- **High Charge Current**: This is a legacy option that has no effect.
- **Virtual Module** * : Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Invert Device Tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open 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

- **High Charge Current**: This is a legacy option that has no effect.
- **Virtual Module** * : Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Invert Device Tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.
- **Physical Address**: The device address of the output 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.
- **High Charge Option**: This is a legacy option that has no effect.
- **Virtual Module** * : Enable this option to register the module as a virtual module. Virtual modules act as placeholders in the system, allowing you to program virtual inputs and outputs for use with programmable functions and other advanced features.
- **Invert Device Tamper**: When this option is enabled the module's tamper input will be inverted. This should be enabled when the tamper switch has a normally open configuration.

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 4/8 of Expander**: Users can hold input 4 (for reader port 1) or input 8 (for reader port 2) and enter their credentials to arm the associated area.

    If input 4/8 is monitored by the area that is being armed, arming may fail because the input is open. To prevent this ensure that **Exit alley input do not test it** is enabled in the input type (**Programming | Input types | Options (1)**).

  - **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 reader expander will activate the relays when they go offline. When disabled the reader expander 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 OSDP 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

Configuration

- **Reader Format**: The type of credential data received, determined by the third-party device or application. Commonly for smart readers the format is set to Custom Credential, which represents a specific credential type:
  - For RS-485 connected smart readers the custom credential is determined by the credential type(s) set in the door type.
  - For ethernet connected smart readers the custom credential is set in the **Reader credential match types** field below.
- **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).
- **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.
- **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 Secondary Format**: The secondary format should be set to Custom Credential.

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 163) 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 special automated processes that can be programmed in the Protege WX system. Generally these processes have a trigger - such as an output turning on - which causes the controller to activate the process.

These functions present an extensive variety of applications for control and automation. For example, you might use them to arm an area based on the state of an output, operate a complex series of devices each time a specific door is unlocked, or unlock the doors in the event of a fire alarm.

Type

- **Type**: The type of programmable function determines what kind of operation it will perform. Each type of function has different programming and options available.
  - **None**: The function will perform no action.
  - **Logic Control**: Controls an output or output group based on the state of one or two triggering outputs. Several logical operations are available.
  - **Area Control**: Arms or disarms an area or area group based on the state of an output.
  - **Ripple Output**: Activates a series of outputs in a ripple pattern based on a single triggering output. This can be used to stage large current devices and multiple lighting circuits.
  - **Door Control**: Locks or unlocks a door or door group based on the state of an output. Can also be used to initiate emergency egress or door lockdown.
  - **Virtual Door**: Enables defined inputs and outputs to act as a door without programming a door record. Useful for doors that do not have readers and are not monitored by a reader expander but require some door processing.
  - **Input Follows Output**: Controls an input based on the state of an output. Can be used to activate alarms based on an output state.
  - **Elevator Control**: Locks or unlocks floors for an elevator car or elevator group based on the state of an output.
- **Mode**: Determines how the system controller operates this function.
  - When this option is set to Normal the programmable function will run every time its triggering conditions are met.

    If the controller is restarted the function will start again.
  - When set to Run Once Only the programmable function will run once when its triggering conditions are met, then stop.

    It will not run again unless started by an operator.
- **State**: This is a legacy option that has no effect.

Logic Control

A logic control function evaluates the status of one or two outputs and applies a logical operation to control the state of another output or output group (called the control output). A range of logical programming is available including follow/inverted follow (with continuous and pulsed options), OR, AND, NOR, NAND and XOR.

- **Logic Function Mode**: This field determines the type of logical operation that will be used to control the state of the control output or output group.

  The control mode may be continuous or pulsed. Continuous control modes check the output state every 30 seconds. If the state is not correct the function reasserts control and turns the output on/off. Pulsed or edge triggered modes only change the output state when the triggering conditions are met, and do not affect it at other times.

  The available control options are:

- **Follow and test**: The control output continuously follows the state of the first output. When the first output is ON, the control output is ON. When the first output is OFF, the control output is OFF.
- **Inverted Follow and Test**: The control output continuously follows the state of the first output in an inverted manner. When the first output is ON, the control output is OFF. When the first output is OFF, the control output is ON.
- **Follow Pulse On**: The control output follows the rising edge of the first output. When the first output turns ON, the control output turns ON.
- **Inverted Follow Pulse On**: The control output follows the rising edge of the first output in an inverted manner. When the first output turns ON, the control output turns OFF.
- **Follow Pulse Off**: The control output is activated on the falling edge of the first output. When the first output turns OFF, the control output turns ON.
- **Inverted Follow Pulse Off**: The control output is deactivated on the falling edge of the first output. When the first output turns OFF, the control output turns OFF.
- **Follow Logic OR**: The function performs a logical OR operation to determine the state of the control output. If either the first or second output is ON, the control output is ON. If both the first and second output are OFF, the control output is OFF.

First Output	Second Output	Control Output
✓	✓	✓
✓	✗	✓
✗	✓	✓
✗	✗	✗

- **Follow Logic AND**: The function performs a logical AND operation to determine the state of the control output. If both the first and second output are ON, the control output is ON. If either the first or second output is OFF, the control output is OFF.

First Output	Second Output	Control Output
✓	✓	✓
✓	✗	✗
✗	✓	✗
✗	✗	✗

- **Follow Logic NOR**: The function performs a logical NOR operation to determine the state of the control output. If either the first or second output is ON, the control output is OFF. If both the first and second output are OFF, the control output is ON.

First Output	Second Output	Control Output
✓	✓	✗
✓	✗	✗
✗	✓	✗
✗	✗	✓

- **Follow Logic NAND**: The function performs a logical NAND operation to determine the state of the control output. If both the first and second outputs are ON, the control output is OFF. If either the first or second output is OFF, the control output is ON.

First Output	Second Output	Control Output
✓	✓	✗
✓	✗	✓
✗	✓	✓
✗	✗	✓

- **Follow Logic XOR**: The function performs a logical XOR operation to determine the state of the control output. If both the first and second outputs are in the same state (both ON or both OFF), the control output is OFF. If the first and second outputs are in different states (one ON, one OFF), the control output is ON.

First Output	Second Output	Control Output
✓	✓	✗
✓	✗	✓
✗	✓	✓
✗	✗	✗

- **First Output to Check**: The first output that is used to set the control output state. This field must be set for all logic function modes.
- **Second Output to Check**: The second output that is used to set the control output state. This field is not required for pulse modes.
- **Output / Output Group to Control**: This output or output group is the control output for the logic control function. It is activated and deactivated based on the states of the first and second outputs and the **Logic Function Mode** selected above.

  If you set both an output and an output group, both will be controlled by the function.

Area Control

Area control programmable functions can arm and disarm an area or area group (called the control area) based on the state of an output. You can configure either continuous control (the function always checks the output state and maintains the area status) or pulse control (the function only controls the area status when the output changes state).

This can be used for applications such as arming an area after a period of inactivity or using a key switch to disarm an area.

- **Area Function**: This field determines how the control area or area group will be controlled based on the state of the output.

  The control mode may be continuous or pulsed. Continuous control modes check the area state every 30 seconds. If the state is not correct the function reasserts control and arms/disarms the area. Pulsed or edge triggered modes only change the area state when the triggering conditions are met, and do not affect it at other times.

  - **Follow and Test Output**: The control area continuously follows the state of the output. When the output is ON, the control area is ARMED. When the output is OFF, the control area is DISARMED.

- **Inverted Follow and Test Output**: The control area continuously follows the state of the output in an inverted manner. When the output is ON, the control area is DISARMED. When the output is OFF, the control area is ARMED.
- **Follow Pulse On Output**: The control area is armed on the rising edge of the output state. When the output turns ON, the control area is ARMED.
- **Inverted Follow Pulse On Output**: The control area is disarmed on the rising edge of the output state. When the output turns ON, the control area is DISARMED.
- **Follow Pulse Off Output**: The control area is armed on the falling edge of the output state. When the output turns OFF, the control area is ARMED.
- **Inverted Follow Pulse Off Output**: The control area is disarmed on the falling edge of the output state. When the output turns OFF, the control area is DISARMED.

- **Output to Check**: The output that is used to set the control area state.
- **Area / Area Group to Control**: This area or area group is the control area for the programmable function. It is armed or disarmed based on the state of the **Output to Check** and the **Area Function** selected above.

  You can set either an area or an area group. If both are set only the area will be controlled by the function.

Ripple Output

This programmable function ripples a series of outputs on or off when a triggering output changes state. It is ideal for staging large current devices or multiple lighting circuits.

- **Output to Enable this Function**: When this output is activated the function activates the controlled outputs in sequence (step up). When this output is deactivated the function deactivates the controlled outputs in sequence (step down).
- **Stage 1-8 Output / Output Group**: These fields define up to 8 outputs or output groups that are controlled by this function. When the **Output to Enable this Function** is activated the function turns these outputs on in sequence from 1 to 8, separated by the **Inter Stage On Ripple Time**. When the **Output to Enable this Function** is deactivated the function turns these output off in reverse sequence from 8 to 1, separated by the **Inter Stage Off Ripple Time**.
- **Inter Stage On Ripple Time**: When the controlled outputs are being stepped up, this is the delay between each output activation (in seconds).
- **Inter Stage Off Ripple Time**: When the controlled outputs are being stepped down, this is the delay between each output deactivation (in seconds).

Door Control

The door control programmable function allows you to lock and unlock a door or door group based on the status of an output. It is also used for implementing fire drop (emergency egress) and lockdown states on a door or door group.

The Door Function Mode activates or deactivates the Door Control Mode based on the state of the Output to Check. The door control mode then determines what action the door or door group will take.

You can configure either continuous control (the function always checks the door state and maintains its status) or pulse control (the function only controls the door status when the output changes state).

- Continuous modes check the door state every 30 seconds. If the state is not correct the function reasserts control and updates the door state.
- Pulsed or edge triggered modes only change the door state at the time when the control mode changes state, and do not check or control it at other times.

Configuration

- **Door Function Mode**: This field determines the control response to the output status, i.e. whether the output turns the chosen **Door Control Mode** on or off.

  The available door function mode options are:

- **Follow and Test Output**: The door control mode continuously follows the state of the output.

  When the output is ON, the door control mode is ON. When the output is OFF, the door control mode is OFF.
- **Inverted Follow and Test Output**: The door control mode continuously follows the state of the output in an inverted manner.

  When the output is ON, the door control mode is OFF. When the output is OFF, the door control mode is ON.
- **Follow Pulse On Output**: The door control mode is activated on the rising edge of the output.

  When the output turns ON, the door control mode turns ON.
- **Inverted Follow Pulse On Output**: The door control mode is deactivated on the rising edge of the output.

  When the output turns ON, the door control mode turns OFF.
- **Follow Pulse Off Output**: The door control mode is activated on the falling edge of the output.

  When the output turns OFF, the door control mode turns ON.
- **Inverted Follow Pulse Off Output**: The door control mode is deactivated on the falling edge of the output.

  When the output turns OFF, the door control mode turns OFF.

- **Door Control Mode**: This field defines what action the door or door group takes when the door control mode is activated or deactivated.
  - **Emulate Unlock Menu**: When the door control mode is activated the door will be unlocked for the duration of the **Lock Activation Time** (**Programming | Doors | Outputs**). This has the same effect as unlocking the door via REX or credential. When the door control mode is deactivated the door is locked.

    When the **Door Function Mode** is set to a continuous mode, once every 30 seconds the door will unlock for its normal unlock time.
  - **Latch Door Unlock**: When the door control mode is activated the door will be latch unlocked. When the door control mode is deactivated the door will be locked.
  - **Fire Control Door Unlock**: When the door control mode is activated the door will be latch unlocked indefinitely. This command overrides other features that might be holding the door locked, such as area status. When the door control mode is deactivated the door will return to its previous state.
  - **Door Lockdown (Deny Entry + Exit)**: When the door control mode is activated the door will be locked down and deny access to all users in both directions. When the door control mode is deactivated the lockdown will be cleared and the door will return to its previous state.
  - **Door Lockdown (Allow Entry)**: When the door control mode is activated the door will be locked down. Access will be allowed in the entry direction only (including REN). When the door control mode is deactivated the lockdown will be cleared and the door will return to its previous state.
  - **Door Lockdown (Allow Exit)**: When the door control mode is activated the door will be locked down. Access will be allowed in the exit direction only (including REX). When the door control mode is deactivated the lockdown will be cleared and the door will return to its previous state.
  - **Door Lockdown (Allow Entry + Exit)**: When the door control mode is activated the door will be locked down. Access will be allowed in both directions (including REX and REN). When the door control mode is deactivated the lockdown will be cleared and the door will return to its previous state.
- **Output To Check**: The output used to control the door or door group. The relationship between the output and the door control mode is determined by the **Door Function Mode** above.
- **Door / Door Group To Control**: This door or door group is controlled by the programmable function. Door behavior is determined by the **Door Control Mode** above.

  Programmable functions can control either a door or a door group. If both are set only the door will be controlled by the function.

Virtual Door

This function enables you to set up defined inputs and outputs to operate like a door. This is useful when some aspects of door processing are required but no readers or reader expander ports are available. For example, roller doors with no readers may require locks, a REX button and left open monitoring. It is also possible to link a virtual door to a regular one, allowing two doors to be controlled from the same reader.

Configuration

- **Request to Exit Input**: When this input is opened a REX (request to exit) is sent to the virtual door. This causes the programmable function to activate the lock output and grant access.

  The programmable function inverts the REX input by default. Therefore, the **Contact Type** in **Programming | Inputs | Options** should be set to the opposite of the physical wiring. If the REX input is wired normally open the **Contact Type** should be set to Normally Closed. If the REX input is wired normally closed, it should be set to Normally Open.

- **Door State Input**: This input represents the door contact or door position input for the virtual door. When the input is opened, the door is considered open. When the input is closed, the door is considered closed.
- **Door Left Open Input to Control**: This input is opened when the door has been left open for too long (as defined by the **Max Open Time** below). It can be programmed with an area and input type to allow it to report door left open events from the virtual door (in place of the trouble input available on a regular door).

  A virtual input should be used for this purpose rather than a physical one.

- **Forced Door Input to Control**: This input is opened when the door is forced open. It can be programmed with an area and input type to allow it to report door forced events from the virtual door (in place of the trouble input available on a regular door).

  A virtual input should be used for this purpose rather than a physical one.

- **Unlock Time**: The duration (in seconds) that the lock will be activated when the virtual door is unlocked.
- **Max Open Time**: The duration (in seconds) that the virtual door can be open before it enters a left open state.
- **Lock Output / Output Group**: This output or output group controls the physical lock for the door.
- **Alarm Output / Output Group**: This output or output group is activated when the virtual door enters a left open or forced condition. This should be a beeper or other audible/visible output that can warn users to close the door. It is deactivated when the door is closed.

  The required **Activate Alarm Output** options must be enabled below.

- **Activate Alarm Output on Door Left Open**: When this option is enabled the **Alarm Output / Output Group** will be activated when the door is left open too long.
- **Pulse Alarm Output on Door Left Open**: By default, the alarm output is activated continuously while the door is left open. When this option is enabled it will pulse on and off in 5 seconds intervals.

  Activate Alarm Output on Door Left Open must also be enabled.

- **Activate Alarm Output on Door Forced**: When this option is enabled the **Alarm Output / Output Group** will be activated when the door is forced open.
- **Pulse Alarm Output on Door Forced**: By default, the alarm output is activated continuously while the door is forced open. When this option is enabled it will pulse on and off in 5 seconds intervals.

  Activate Alarm Output on Door Forced must also be enabled.

- **Log Door Left Open Input Event**: This is a legacy option that has no effect. An event is always logged when the virtual door is left open too long.
- **Log Door Forced Input Event**: This is a legacy option that has no effect. An event is always logged when the virtual door is forced open.
- **Link to Door**: This option allows you to associate the virtual door with a regular door. Whenever the regular door is unlocked by access, a keypad or an operator, the virtual door is also unlocked. Whenever the virtual

door is unlocked by REX the regular door is also unlocked. This allows two doors to be controlled from a single reader.

Input Follows Output

This function allows an input to be triggered by an output. This is useful for generating alarms based on the state of an output rather than a physical input.

- **Input Follows Output**: This control input is opened when the **Output to Follow** is activated, and closed when the output is deactivated. By programming the input into an area with an input type it can be used for alarm reporting.

  A virtual input should be used rather than a physical one.

- **Output to Follow**: This output is monitored by the function and controls the state of the control input. This can be set to any physical or virtual output that should trigger an alarm state.
- **Log Input Events**: When this option is enabled an event will be generated whenever the input changes state due to this programmable function. When this option is disabled no events will be generated.

Elevator Control

This type of programmable function is used to lock and unlock selected floors for a specific elevator group based on the state of an output. It is also used to implement the fire drop (emergency egress) state on floors.

The Elevator Function Mode activates or deactivates the Elevator Control Mode based on the state of the Output to Check. The elevator control mode then determines what action the floors will take.

You can configure either continuous control (the function always checks the floor state and maintains its status) or pulse control (the function only controls the floor status when the output changes state).

- Continuous modes check the floor state every 30 seconds. If the state is not correct the function reasserts control and updates the floor state.
- Pulsed or edge triggered modes only change the floor state at the time when the control mode changes state, and do not check or control it at other times.

Configuration

- **Elevator Function Mode**: This field determines the control response to the output status, i.e. whether the output turns the chosen **Elevator Control Mode** on or off.

  The options are:

  - **Follow and Test**: The elevator control mode continuously follows the state of the output.

    When the output is ON, the elevator control mode is ON. When the output is OFF, the elevator control mode is OFF.
  - **Invert Follow and Test**: The elevator control mode continuously follows the state of the output in an inverted manner.

    When the output is ON, the elevator control mode is OFF. When the output is OFF, the elevator control mode is ON.
  - **Pulse On**: The elevator control mode is activated on the rising edge of the output.

    When the output turns ON, the elevator control mode turns ON.
  - **Invert Pulse On**: The elevator control mode is deactivated on the rising edge of the output.

    When the output turns ON, the elevator control mode turns OFF.
  - **Pulse Off**: The elevator control mode is activated on the falling edge of the output.

    When the output turns OFF, the elevator control mode turns ON.
  - **Invert Pulse Off**: The elevator control mode is deactivated on the falling edge of the output.

    When the output turns OFF, the elevator control mode turns OFF.

- **Elevator Control Mode**: This field defines what action the floor group takes when the elevator control mode is activated or deactivated.
  - **Emulate Unlock Menu**: When the elevator control mode is activated the floor group will be unlocked for the duration of the **Token Time** (below). When the elevator control mode is deactivated the floor group is locked.

    This setting is not compatible with continuous elevator function modes.

  - **Latch Elevator Unlock**: When the elevator control mode is activated the floor group will be latch unlocked. When the elevator control mode is deactivated the floor group will be locked.
  - **Fire Control Elevator Unlock**: When the elevator control mode is activated the floor group will be latch unlocked indefinitely. This command overrides other features that might be holding the floors locked, such as area status. When the elevator control mode is deactivated the floor group will return to its previous state.
- **Output To Check**: The output used to control the floor group. The relationship between the output and the elevator control mode is determined by the **Elevator Function Mode** above.
- **Elevator Group**: The floors controlled by this function will be locked/unlocked for the elevator cars in this elevator group only.

  For example, a programmable function might be used to latch unlock the floors in the public elevators but not the maintenance elevators.
- **Floor Group**: The floors in this group are controlled by the programmable function. Floor behavior is determined by the **Elevator Control Mode** above.
- **Token Time**: If the **Elevator Control Mode** is set to Emulate Unlock Menu the floors will be unlocked for this length of time when the elevator control mode is activated.

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 (requires an app password - see this help page)
- 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. For Gmail accounts this is the email address that you used to generate the app password.
- **SMTP Password**: The password for the outgoing SMTP mail server logon. For Gmail accounts this is your app password.
- **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

This feature is only available in Advanced mode.

- **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.

  The PIN only and Card or PIN door types are not compatible with duplicate PINs, as there is no way to uniquely identify the user who is requesting access.

- **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

If you update these fields while the operator is active, the changes will not come into effect until that operator logs out and in again.

- **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 **Restore Controller**. Browse to the backup file you wish to restore, then click **Open** to upload it.

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.

Before Upgrading Firmware

- This process will take approximately 10 minutes and the controller will not be able to perform its normal functions during this period. It is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity.
- Ensure that the controller does not lose power during the firmware upgrade process.
- Ensure that there is a stable network connection to the web interface before you begin uploading the firmware.
- 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.
- We strongly recommend having a technician on site during the firmware upgrade process to respond to any issues that might arise.

Losing power or network connection during the upgrade process or upgrading with a default link connected can cause the controller to become inoperable.

Upgrade Firmware

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.
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 modules connected to the controller. You can also view the serial number and firmware version of card readers connected to the network by ICT RS-485 or OSDP and update TSL reader firmware. 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. This warning does not apply to TSL readers, which do not put the network into maintenance mode.

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.

This feature is not available for card readers. Contact ICT Technical Support for assistance.

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.

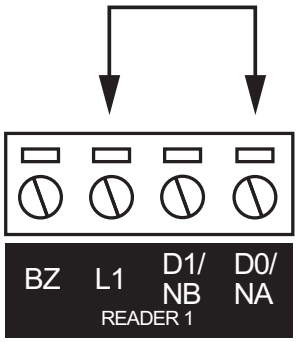
Temporarily Defaulting the IP Address

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

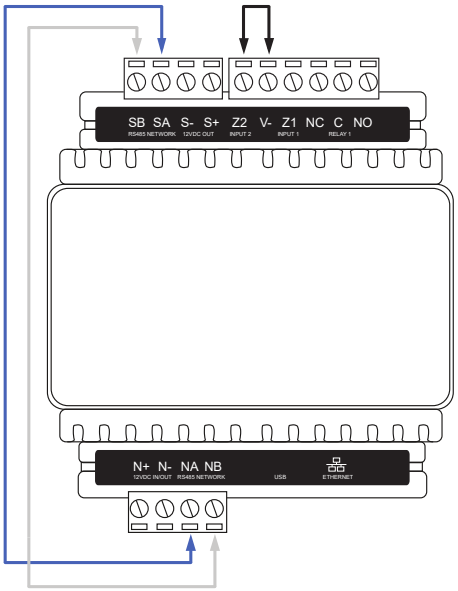
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



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.

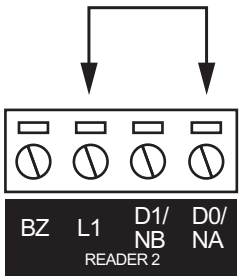
Defaulting a Controller

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

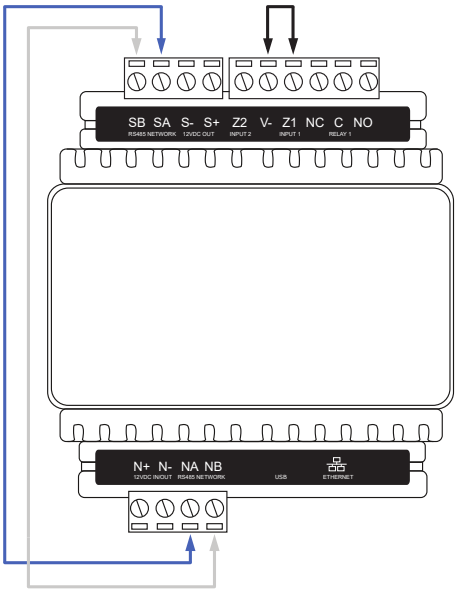
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



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 encryption keys used for secure sessions and pairing are deleted. This includes:
  - OSDP secure channel encryption keys for the controller **and** connected reader expanders
  - Protege wireless lock encryption keys
  - Pairing with Protege GX extended services
  - Pairing with Protege X
- 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. If you were using OSDP secure channel, put **all** OSDP card readers connected to the controller **and** its reader expanders into installation mode. Initiate installation mode on the controller and all connected reader expanders to re-establish the secure channel.

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.

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