Protege WX Integrated System Controller

Configuration Guide

Last Published: 19-May-23 11:53 AM

Contents

Introduction

This configuration guide provides programming instructions and system communication information for Protege WX controllers. For installation instructions and technical specifications, see the appropriate controller installation manual, available from the ICT website.

Controller Editions

This configuration guide includes programming instructions for the following Protege WX controller models:

Product Code	Controller Module
PRT-WX-DIN-IP	Protege WX DIN Rail Integrated System Controller (IP only)
PRT-WX-DIN	Protege WX DIN Rail Integrated System Controller
PRT-WX-DIN-1D	Protege WX DIN Rail Single Door Controller

About This Module

The Protege WX controller is the central processing unit responsible for the control of security, access control and building automation in the Protege WX system. It communicates with all system modules, stores all configuration and transaction information, processes all system communication, and reports alarms and system activity to a monitoring station or remote computer.

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 module network. Up to 250 modules can be connected to the Protege system in any combination to the network, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

Current Features

The current features of the Protege WX controllers include:

Features	PRT-WX-DIN-IP	PRT-WX-DIN	PRT-WX-DIN-1D
Internal industry standard 10/100 ethernet	✓	✓	✓
32 Bit RISC processor with 2GB total memory	✓	✓	✓
Encrypted module network using RS-485 communication	✓	✓	✓
NIST Certified AES 128, 192 and 256 Bit encryption	✓	✓	✓
Factory loaded HTTPS certificate	✓	✓	✓
OSDP configurable RS-485	✓	✓	✓
Reader ports	2	2	1
High security monitored inputs	8	8	2
Open collector outputs	4	4	-
Form C Relay outputs	2	2	1
Bell Output	✓	✓	✗
USB Port	✓	✓	✓
Built-in offsite communications dialer (Contact ID or SIA)	✗	✓	✗
Industry standard DIN rail mounting	✓	✓	✓

Configuring a Controller via the Web Interface

The controller's built-in web interface allows you to configure specific communication settings including IP address, subnet mask, gateway and DNS settings. In addition, you can load security certificates, update the controller firmware and/or the firmware of connected expander modules from this interface, and control operator access to the controller.

When the controller is connected to the computer's network, the web interface can be accessed by entering its current IP address into the address bar of a browser, then logging in with valid credentials for that controller.

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.

Logging In for the First Time

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.

Older one-door controllers may require additional steps to access the web interface (see next page).

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.

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.

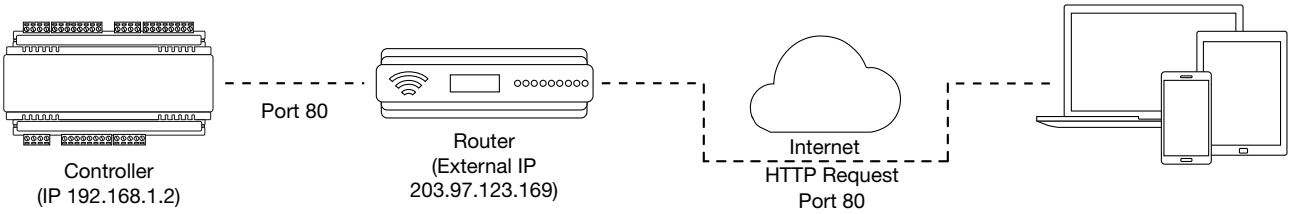
More Information

- 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.

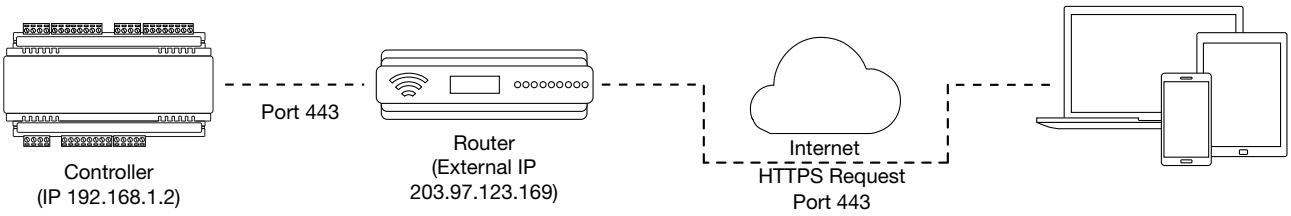
External access via HTTP is only required in order to validate and install your certificate. Once the certificate has been installed, HTTP access will be disabled because the more secure HTTPS connection is available. Therefore it will no longer be necessary to forward external port 80 to the controller.

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

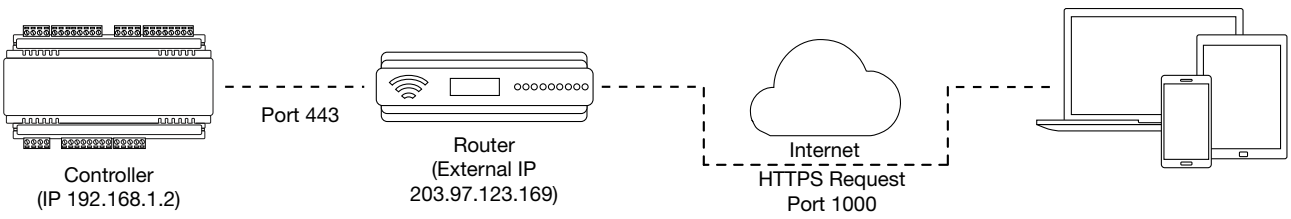
After you have installed a certificate and established an HTTPS connection to the controller, you may wish to continue accessing the controller over the internet. To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed 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 11) can be used to assign this hostname.

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

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

Creating a Private Key and Certificate Signing Request

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

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

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

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

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

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

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

   Some details are optional. Confirm with your CA which fields are required.
6. **Save** both files in a safe, known location, as both are required for the following steps. It is especially important that the private key is not publicly accessible.

Purchasing a Certificate

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

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

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

   DO NOT change the name or contents of this file.

Authenticating the Certificate

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

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**.

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

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

Converting the Certificate Format

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

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

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

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

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

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

   Android devices will fail to connect if intermediate certificates are not included in the certificate loaded onto the device.
3. Enter the **passphrase** for the private key (set above) to continue.

   Note that passphrase characters will not be displayed in the console.
4. Enter an **export password** when requested. This will be required when installing the certificate on the controller.
5. This process will generate a [name].pfx file in the current OpenSSL directory. This is your third-party certificate. Store this file in a safe, known location.

Installing the Certificate on the Controller

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

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

refresh.

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

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

Self-Signed Certificate

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

Requirements for Self-Signed Certificates

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

Generating a Self-Signed Certificate with OpenSSL

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

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

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

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

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

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

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

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

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

Installing the Self-Signed Certificate to the Controller

1. Access the controller's web interface by typing its **IP address** into the address bar of a web browser, then log in with your username and password.
2. Navigate to the **System Settings**.
3. In the **General** tab, select the **Use HTTPS** checkbox (if not already enabled).
4. Enter an appropriate **HTTPS Port**. The default is port 443, which is commonly used for this purpose. You should retain the default port unless you are required to use another port by your system administrator.
5. Click **Install Certificate** and browse to the .pfx certificate file to install it on the controller.

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

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

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

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

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

Additional Controller Programming

This section outlines additional controller programming requirements and options.

Programming the Onboard Reader

The onboard reader is programmed in exactly the same way as any other reader module. It can be thought of as if it were a normal reader expander module on a separate circuit board. The onboard reader of a Protege WX controller is programmed as a reader expander with an address of 1.

Two-Door Controllers

For two-door controllers, the onboard reader uses inputs 1-4 and 5-8 as its door contact, REX, bond sense and REN inputs respectively.

The default settings are shown in the following table:

Input	Access Control Function	Default Setting
Input 1	Door Contact, Port 1	Door Contact, Port 1
Input 2	REX Input, Port 1	REX Input, Port 1
Input 3	Bond Sense, Port 1	General Purpose Input
Input 4	REN Input, Port 1	General Purpose Input
Input 5	Door Contact, Port 2	Door Contact, Port 2
Input 6	REX input, Port 2	REX Input, Port 2
Input 7	Bond Sense, Port 2	General Purpose Input
Input 8	REN Input, Port 2	General Purpose Input

One-Door Controllers

For one-door controllers, the onboard reader uses inputs 1 and 2 as its door contact and REX respectively.

The default settings are shown in the following table:

Input	Access Control Function	Default Setting
Input 1	Door Contact, Port 1	Door Contact, Port 1
Input 2	REX Input, Port 1	REX Input, Port 1

Any inputs that are not configured for use with the onboard reader may be used as general purpose inputs. If you wish to use an access control input as a general input, you will need to disable the associated function input in the door programming section of the Protege user interface.

Programming Controller Inputs

Two-door controllers have 8 onboard inputs and one-door controllers have 2 onboard inputs for monitoring the state of devices such as magnetic contacts and motion detectors.

Any inputs that are not configured for use with the onboard reader may be used as general purpose inputs. If you wish to use an access control input as a general input, you will need to disable the associated function input in the door programming section of the Protege user interface.

Input Duplexing

Input duplexing allows the controller to support twice the number of inputs, wired in duplex configuration.

1. To enable this feature, navigate to **System | Settings** and enter the following command:
   `DuplexZones = true`
2. In addition, you will need to manually add the additional input records in **Programming | Inputs** with the correct addresses as outlined below.

Enabling duplex inputs will not change the programming of any existing inputs. These must be reprogrammed to match the new addressing scheme.

Two-Door Controllers

The following table indicates the position and resistor configuration corresponding to each input address for two-door controllers:

Input Address	Position	Resistor
1	Z1	1K
2	Z1	2K4
3	Z2	1K
4	Z2	2K4
5	Z3	1K
6	Z3	2K4
7	Z4	1K
8	Z4	2K4
9	Z5	1K
10	Z5	2K4
11	Z6	1K
12	Z6	2K4
13	Z7	1K
14	Z7	2K4
15	Z8	1K
16	Z8	2K4

One-Door Controllers

The following table indicates the position and resistor configuration corresponding to each input address for one-door controllers:

Input Address	Position	Resistor
1	Z1	1K
2	Z1	2K4
3	Z2	1K
4	Z2	2K4

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 table details the trouble inputs that are configured in the controller and the trouble groups that they are associated with.

Two-Door Controllers

Input Number	Description	Default Trouble Group	Default Trouble Group Option
CP001:01	Reserved	-	-
CP001:02	12V Supply Failure	General	AC Failure
CP001:03	Reserved	-	-
CP001:04	Real Time Clock Not Set	General	RTC/Clock Loss
CP001:05	Service Report Test	-	-
CP001:06	Service Report Failure to Communicate	General	Reporting Failure
CP001:07	Phone Line Fault (modem model only)	General	Phone Line Lost
CP001:08	Auxiliary Failure	General	Power Fault
CP001:09	Bell Cut/Tamper	General	Bell/Output Fault
CP001:10	Reserved	-	-
CP001:11	Bell Current Overload	General	Bell/Output Fault
CP001:12	Reserved	-	-
CP001:13	Module Communication	System	Module Loss
CP001:14	Module Network Security	System	Module Security
CP001:15	Reserved	-	-
CP001:16	Reserved	-	-
CP001:17	Reserved	-	-
CP001:18	Reserved	-	-
CP001:19	Reserved	-	-

Input Number	Description	Default Trouble Group	Default Trouble Group Option
CP001:20	Report IP Reporting Failure	System	Hardware Fault
CP001:21	Reserved	-	-
CP001:22	Modbus Communication Fault	System	Hardware Fault
CP001:23	Protege System Remote Access	System	Hardware Fault
CP001:24	Installer Logged In	System	Hardware Fault
CP001:25	Reserved	-	-
CP001:26	Reserved	-	-
CP001:27	Reserved	-	-
CP001:28	Reserved	-	-
CP001:29	System restarted	System	Hardware Fault
CP001:30	Reserved	-	-
CP001:31	Reserved	-	-
CP001:32	3G Modem Link Lost (legacy 3G modem model only)	System	Hardware Fault
CP001:33	Controller Group Link Lost	System	Hardware Fault
| | | |	| |	|	|
CP001:64	Reserved	-	-

One-Door Controllers

Input Number	Description	Default Trouble Group	Default Trouble Group Option
CP001:02	12V Supply Failure	General	AC Failure
CP001:04	Real Time Clock Not Set	General	RTC/Clock Loss
CP001:05	Service Report Test	-	-
CP001:08	Auxiliary Failure	General	Power Fault
CP001:13	Module Communication	System	Module Loss
CP001:14	Module Network Security	System	Module Security
CP001:20	Report IP Reporting Failure	System	Hardware Fault
CP001:22	Modbus Communication Fault	System	Hardware Fault
CP001:23	Protege System Remote Access	System	Hardware Fault
CP001:24	Installer Logged In	System	Hardware Fault
CP001:29	System restarted	System	Hardware Fault
CP001:30	PoE Connection Lost (legacy PoE model only)	General	Power Fault
CP001:31	Output Over-Current Failure (legacy PoE model only)	General	Power Fault

Input Number	Description	Default Trouble Group	Default Trouble Group Option
CP001:33	Controller Group Link Lost	System	Hardware Fault

Onboard Reader Trouble Inputs

The onboard reader expander can monitor up to 16 trouble inputs used to report associated trouble conditions.

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

Input Number	Description	Default Trouble Group	Default Trouble Group Option
RDxxx:01-11	Reserved	None	None
RDxxx:12	Reader 1 Tamper	System	System Tamper
RDxxx:13	Reader 2 Tamper	System	System Tamper
RDxxx:14	Door 1 Lockout	Access	Too Many Attempts
RDxxx:15	Door 2 Lockout	Access	Too Many Attempts
RDxxx:16	Module Offline	System	Module Offline

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

Door Trouble Inputs

In addition to the trouble inputs of the module itself, the onboard reader can also monitor trouble inputs associated with connected doors. These are used for monitoring and reporting door troubles such as door forced and duress conditions.

Input Number	Description	Default Trouble Group	Default Trouble Group Option
Door xxx 01	Door Forced	Access	Forced Door
Door xxx 02	Door Left Open	Access	Left Open
Door xxx 08	Door Duress	None	None

'xxx' refers to the **Name** of the door in the Protege system.

Configuring the Cellular Modem Connection

Cellular modem connection requires the controller to be operating firmware version 4.00.1241 or higher.

1. Log in to the controller web interface and navigate to the **System Settings** page.
2. In the **Adaptor - USB Ethernet** tab, check **Enable USB Ethernet** to configure the controller to look for an ethernet adaptor connected to its USB port.
3. If not automatically enabled, set the **Connection** to Cellular Modem to configure the controller to communicate with the cellular modem connected to its USB port.

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

4. Configure the **Cellular Network Connection**:
   - **Cellular APN**: The APN is specified by the mobile network operator (MNO) and is unique to that network. 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.
5. Click **Save**.
6. **Restart** the controller.

Establishing the Connection

After the controller restarts it will automatically detect the modem and connect to the cellular network. The connection status and details will be updated in the Cellular Information section.

It can take a minute or two for the modem to connect to the cellular network and obtain an IP address, and the page may display 'Not registered' while the modem is initially starting up.

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.

Maintaining Your System

This section covers system maintenance, including how to back up and restore controller programming and update firmware.

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 8).

Home Page

Controller Status

- **Health**: Displays the health status of the controller.
- **Voltage**: Shows the voltage passing through the controller.
- **Memory Usage**: Shows the current memory usage of the controller, along with a breakdown of what that memory is being used for.
- **Status**: Displays the current serial number of the controller.

Operator Details

- **Logged on as**: Shows the username of the current operator.
- **Logged on at**: Shows the time and date this operator logged in.

Options

- **Display Theme**: Switch between the dark (dark background, white text) and light (white background, dark text) display themes for the web interface.
- **Display Color**: Select the display color used for the web interface. This selection will persist whenever this operator logs in to the controller with the same web browser.
- **Logout**: Log out and return to the login screen.
- **Change Password**: Change the password used by this operator.

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.

Commands

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

System Settings | Adaptor - Onboard Ethernet

Onboard Ethernet

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

  This option is enabled by default.

Onboard Ethernet Configuration

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

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

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

- **IP Address***: The controller has a built-in TCP/IP ethernet device and it must be programmed with a valid TCP/IP address to allow communication. By default the IP address is set to **192.168.1.2**.
- **Subnet Mask***: Used in conjunction with the IP address, a netmask must be configured to allow access to the appropriate node on the subnet. By default this is set to a value of **255.255.255.0**.
- **Default Gateway***: Used in conjunction with the IP address, the gateway can be configured to allow access to a router for external communications beyond the subnet to which the controller is connected. By default this is set to a value of **192.168.1.254**. Set this to **0.0.0.0** to prevent any external communication.
- **DNS Server***: The IP address of the DNS server being used by the controller. This is required if a DNS name is being used for the connection.

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

Hostname

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

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

Dynamic DNS

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

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

- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS account.
  - **No-IP**: The username and password are the credentials used to log in to your No-IP account.

System Settings | Adaptor - USB Ethernet

USB Ethernet

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

Connection

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

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

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

Cellular Network Connection

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

Cellular Options

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

Cellular Information

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

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

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

- **Network Registration Status**:
  - Registered (home): Displayed when the cellular modem is successfully connected to a network inside the SIM home region.
  - Registered (roaming): Displayed when the cellular modem is successfully connected to a network outside the SIM home region.
  - Not registered: Displayed when the cellular modem is detected but no connection has been established.
  - Not registered, seeking: Displayed when the cellular modem is actively seeking a network to connect to.
  - Denied: The network actively refused the connection attempt by the cellular modem.
  - Unknown: The cellular modem cannot currently determine network connection status.
- **Current Network Provider**: The mobile network operator that the cellular modem is currently connected to.
- **Current Technology**: The cellular technology that the cellular modem is connected with.
- **Internet Connection Status**: Identifies whether the cellular modem's internet connection is valid.
- **IP Address**: The IP address assigned to the cellular modem by the network provider.

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

Cellular Hostname

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

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

Cellular Dynamic DNS

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

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

- **DDNS Username/Password**: Enter the required credentials for your DDNS provider.
  - **Duck DNS**: The username should be left blank. The password is the **Token** generated by your Duck DNS account.
  - **No-IP**: The username and password are the credentials used to log in to your No-IP account.

System Settings | Configuration

Configuration

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

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

  Module Comms UDP/TCP (9450) is disabled by default. It can be enabled by adding `EnableModuleUDP = true` or `EnableModuleTCP = true` to the **Commands** field in the controller programming as required.

- **Default Keypad Language**: Defines the language selection for keypad displays. Select from English, Czech, Dutch, Estonian, Finnish, French, German, Greek, Italian, Norwegian, Polish, Romanian, Russian, Spanish, Swedish.
- **Touch Screen UDP Port**: This is the UDP port that a Protege touch screen will communicate over.

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

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

System Settings | Options

Options

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

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

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

Misc Options

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

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

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

System Settings | Email Settings

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

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

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

This feature is only available in Advanced Mode.

Configure your Email Server Settings

Currently the following email servers are supported:

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

Email SMTP Settings

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

Test Settings

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

Add a Recipient Email Address

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

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

System Settings | Custom Reader Format

This feature is only available in Advanced mode.

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

Custom Reader Configuration

- **Custom Reader Type**: Defines the reader type. The data can either be output as Wiegand (D0 and D1) or Magnetic Data (Clock and Data).
- **Bit Length**: The total number of bits that are sent by the card reader for each card badge.
- **Site Code Start**: The index where the site code data starts in the data transmitted. The count starts at zero.
- **Site Code End**: The index where the site code data ends in the data transmitted. The count starts at zero.
- **Card Number Start**: The index where the facility code data starts in the data transmitted. The count starts at zero.
- **Card Number End**: The index where the facility code data end in the data transmitted. The count starts at zero.
- **Data Format**: Defines how the card number that is received from the card reader is handled. If the size of the site code and card number are less than 16 bits (e.g. Site Start – Site End is less than 16 bits) use 16 bit, otherwise use 32 bit. If unsure, use 32 bit.

Parity Options (1-4)

There can be up to 4 blocks of parity calculated over the received data.

- **Parity Type**: The parity type defines the method of calculating the parity for the block. This is either Even or Odd Parity.
- **Parity Location**: The parity location defines the location of the parity bit in the received data.
- **Parity Start**: Defines where the location of the parity block starts in the received data.
- **Parity End**: Defines where the location of the parity block ends in the received data.

Bit Options (1-4)

- **Set Bit**: A set bit defines a location in the received data that must always be set (or a logical '1'). The set bit defines the location of the bit in the received data.
- **Clear Bit**: A clear bit defines a location in the received data that must always be cleared (or a logical '0'). The clear bit defines the location of the bit in the received data.

System Settings | Security Enhancement

- **Require Dual Credential for Keypad Access**: When enabled, a preconfigured numeric credential type labeled User ID will be automatically added to the **Credentials** tab of each existing and new user. When adding or updating a user, the presence of a valid unique User ID will be enforced. Both the User ID and the user's PIN will be required for the user to gain access to a keypad.
- **Allow PIN Duplication**: When enabled, this option allows more than one user to have the same PIN. This is only available when the **Require Dual Credential for Keypad Access** mode has been enabled.
- **Default PIN length**: Defines the length of PIN that will be generated by the system. If the **Default PIN length** is 6 and the **Minimum PIN length** is 4, the system will first generate new PINs 6 digits in length. Once those are depleted it will generate PINs with 7 digits, then 8 digits, then 5 digits, and finally 4 digits.
- **Minimum PIN length**: The minimum number of digits (options between 1-8) that will be permitted when manually entering PINs and when PINs are automatically generated.
- **Maximum Sequential Digits**: The maximum number of sequential digits (options between 2-4) that will be permitted or generated for PINs. For example, selecting 4 will allow a numerical sequence of 1234 or 4321 but not 12345. Selecting <not set> will allow a numerical sequence of more than 4 digits, for example 12345.
- **Maximum Repetitive Digits**: The maximum repetitive digits (options between 2-4) allowed for a user PIN. Selecting <not set> allows more than 4 repetitive digits, for example 11111.
- **PIN Expiry Time**: The frequency at which users will be prompted to reset their PIN at a keypad.

  NOTE: When PIN expiry is enabled, regardless of the expiry time, **ANY** PIN created or edited through the user Interface will immediately expire on first use. The user will be required to set their own permanent PIN when next logging in at a keypad. This ensures that only the user knows their PIN.

Operators

An operator is a person who uses Protege WX for maintaining the system and monitoring the site.

General

- **Name**: The name of the operator. This is the name displayed in the status bar at the top of the page.

  Do not enter more than **40 characters** for the operator name. This is the maximum supported length.

Configuration

- **Username**: This is the name used by the operator when logging in.
- **Password**: The password of the operator. Operators can change their own password from the Home Page once logged in.
- **Role**: Select the appropriate role to determine what access the operator has once logged in.
- **Default Language**: This sets the language of the user interface displayed to the operator.

Operator Timeout

- **Enable Operator Timeout**: Select this option to automatically log the operator out after a period of inactivity as defined in the Operator Timeout setting below.
- **Operator Timeout**: Defines the inactivity period, after which Protege WX will time out and the operator will be prompted to log in again to continue.

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**.

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.

Backing Up and Restoring Controller Programming

Creating backups of your controller programming is good practice to ensure you are protected against damage in the event of hardware failure or malfunction.

The Protege WX interface provides a simple export tool for backing up the system to a proprietary encrypted backup file (*.bak). This file works as a snapshot of your current system, enabling you to later restore and retain the programming at the same point as you exported it. You can even backup programming from one controller and restore it to another. This can be useful when running a test environment, or for pre-programming a system prior to deployment at a client site.

1. Navigate to **System | Backup**.
2. To create a backup, select **Backup Controller**. This creates a copy of the controller's programming, which may then be restored at a later date.

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

3. To restore programming select **Choose File** to browse to a .bak file created using the backup option, then select **Restore Controller** to import a copy of the programming.

Upgrading Application Software and Module Firmware

From time to time ICT releases new updates with changes and enhancements to system features. To ensure your installation is running at optimal performance we recommend that all installed modules utilize the latest updates.

Controllers do not support defaulting and firmware upgrade at the same time. Before you upgrade the controller firmware, ensure that the wire link used to default the controller is **not** connected.

1. From the main menu, select **System | Application Software**. This page provides details about the current Protege WX version that is installed.
2. Click the **Choose File** button and browse to the supplied update file.
3. Click **Upload** to commence the upgrade procedure.
4. The controller will automatically create a backup of the programming. Depending on your browser settings you may be prompted to save the file. Otherwise, it is downloaded automatically to your **Downloads** folder.
5. Progress is shown as the new application software is installed. The controller then restarts.

   This process can take up to 5 minutes to complete, so we recommend that upgrades are performed when the site is closed for maintenance or at times of low activity. The controller will not be able to perform its normal function while being upgraded.
6. After the upgrade is complete, log on to the controller to review and resolve any health status messages to resume normal operation. You may need to perform module updates, re-arm areas and re-enable the 24HR portions, and start services and programmable functions.

Update Module Firmware

- **Module**: This section is used to update the firmware of any module connected to the controller. Select the connected module that requires a firmware update from the dropdown.
- **BIN File**: Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the new firmware on the selected module.

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

Force Update

In situations where a module becomes stuck in the bootloader mode and the application is not running, it may become necessary to perform a force update.

This hidden feature in the Update Module Firmware section of the web interface provides the ability to update module firmware on an inoperable module where it is not possible through the regular update process.

Clicking **Module** will expand the hidden section, making the **Force Update** panel available.

1. Select the **Force Update - Module**, carefully selecting the module type and model.
2. Select the **Force Update - Address**, which is the configured **Physical Address** of the module.
3. The **Skip Verification** option will bypass the firmware check and allow firmware that does not match the module type of the module to be loaded.

   This option should only be selected at the direction of ICT Technical Support .
4. Click **Upload Firmware** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the firmware on the selected module.

Note: The maximum address that can be selected for force update is 32. If the module has an address greater than 32 it cannot be upgraded via this method. You will need to contact ICT Technical Support for assistance.

Addressing Expanders

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

Listed for each module is:

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

When connecting a module to the network it must be added to Protege WX and allocated a unique physical address. By default all DIN rail modules are shipped from ICT with the address of 254 and without changing this address the module will not be able to register with the controller.

For older legacy PCB modules, the address is configured via DIP switches. Refer to the relevant Installation Manual for instructions on configuring the address of the module.

To Set the Network Address of a Module:

1. Ensure the controller is correctly powered.
2. Connect the module(s) that require addressing to the module network. Make sure that the power light on each module is on and that the status light begins flashing rapidly.
3. Allow some time for the module(s) to attempt to register with the controller.
   - If the module has the default address of 254 or has the same address as another module, the **fault** light will be constantly on and the **status** indicator will be flashing red with an error number.
     - For an unaddressed module, the status indicator will flash in **three** flash bursts.
     - If the address is already in use by another module, the status indicator will flash in **four** flash bursts.
   - If the module has been previously addressed and is not a duplicate, then it will succeed in registering and the **status** light will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the module addressing window by selecting **Expanders | Expander Addressing**.
5. Enter an address for the relevant module(s) by selecting an option under the **Address** column then click **Save** to save the address and restart the module.
6. Allow around 5 seconds per module for the new address to be sent and registered then click **Refresh** to update the list and display the new addresses.
   - If the address has not changed, check that the module is online and communicating and has finished attempting to register.
   - If the address has changed but the module is not shown as registered, check that the address is in the valid address range and is not a duplicate of another modules address.

Once all modules are online and registered with the desired addresses, the addressing process is complete.

Maximum Module Addresses

The Protege controller has a set limit on the number of modules of each type that it can support. This applies to both physical and virtual modules. The maximum addresses available for each type of module are outlined in the table below:

Module Type	Maximum Address
Keypad	200
Input Expander	248
Reader Expander	64
Output Expander	32
Analog Expander	32
Smart Reader	248

Any module with an address higher than these limits will not come online to the controller. A message will be generated in the controller's health status.

Hardware Configuration

Setting the IP Address from a Keypad

If the current IP address of the controller is not known it can be viewed and changed using a Protege keypad.

1. Connect the keypad to the module network.
2. Log in to the keypad using any valid installer code. The default installer code is 000000.
   If the default code has been overridden and you do not know the new codes you will need to default the controller (see Defaulting the Controller in this document) to reset the code.

   Note that this will erase **all** existing programming as well as setting up the default installer code.
3. Once logged in select **Menu 4** (Install Menu) then **Menu 2** (IP Menu) and view or edit the IP address, network mask, and gateway as required.

Once the settings have been changed you must save the settings by pressing the **[Arm]** key. You will be prompted to confirm the changes by pressing **[Enter]**. You must then restart the controller, either through the menu **[4], [2], [2]** or by cycling the power, for the settings to take effect.

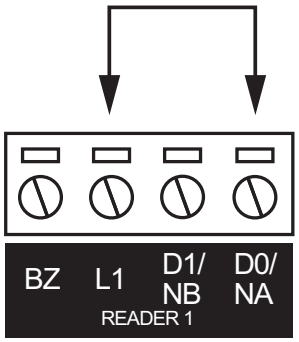
Temporarily Defaulting the IP Address

If the currently configured IP address is unknown it can be temporarily set to 192.168.111.222 so that you can connect to the web interface to view and/or change it. This will also temporarily disable HTTPS security, which may help resolve some connection issues.

This defaults the IP address for as long as power is applied, but does not save the change permanently. Once the link is removed and power is cycled to the unit the configured IP address is used.

Defaulting the IP Address of a Two Door Controller

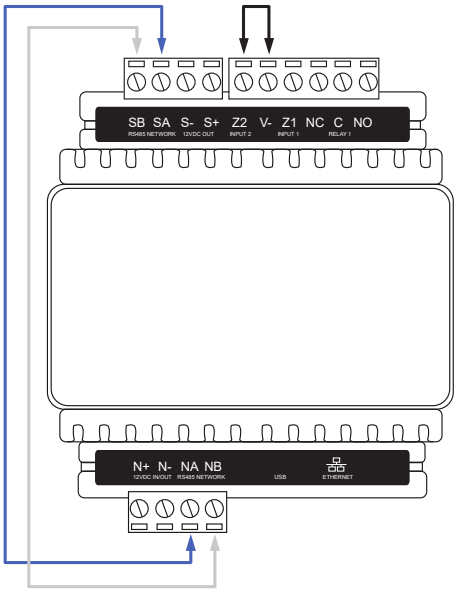
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.

Defaulting the IP Address of a Single Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 2** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.

Accessing the Controller

5. When the controller starts up it will use the following temporary settings:
   - **IP Address**: 192.168.111.222
   - **Subnet Mask**: 255.255.255.0
   - **Gateway**: 192.168.111.254
   - **DHCP**: Disabled
   - **Use HTTPS**: Disabled
6. Connect to the controller by entering http://192.168.111.222 into the address bar of your web browser, and view or change the IP address and other network settings as required.

   Remember to change the subnet of your PC or laptop to match the subnet of the controller.

7. Remove the wire link(s) and power cycle the controller again.
   The controller will now use the configured network settings.

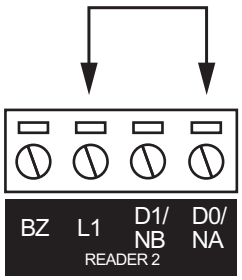
Defaulting a Controller

The controller can be factory defaulted, which resets all internal data and event information. This allows you to remove all programming and start afresh.

Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2

Defaulting a Two-Door Controller

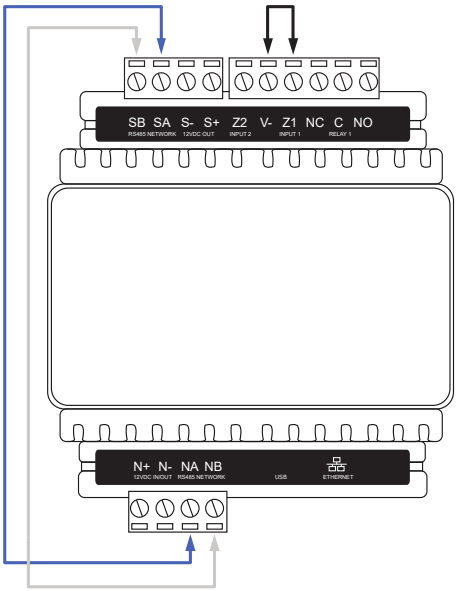
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



4. Power up the controller. Wait for the status indicator to begin flashing steadily.
5. Remove the wire link **before making any changes to the controller's configuration**.

Defaulting a Single-Door Controller

1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **NA** of the module network and **SA** of the reader network, and between **NB** of the module network and **SB** of the reader network.
4. Connect **Input 1** to ground.



5. Power up the controller. Wait for the status indicator to begin flashing steadily.
6. Remove the wire links **before making any changes to the controller's configuration**.

The system will now be defaulted with all programming and **System Settings** returned to factory configuration, including resetting the IP address and all network configuration, and removing all operator records.

- Defaulting the controller resets the IP address to the factory default IP of 192.168.1.2.

  Earlier versions of the controller firmware do not reset the IP address. If the controller is not available on 192.168.1.2 you will be able to connect to it via its previous IP address.

- Any configured system settings (e.g. **Default Gateway**, **Event Server**) are reset to their default values.
- Any custom HTTPS certificates are removed and the default certificate is reinstalled.

  Earlier versions of the controller do not have a default HTTPS certificate installed. If the controller is not available via HTTPS, connect to it via HTTP.

- All operator records are removed and the admin operator must be recreated.
- All other programming is removed.

After Defaulting a Controller

Before making any changes to the controller's configuration or upgrading the firmware, **remove the wire link used to default the controller**.

After defaulting a controller a number of essential steps will need to be performed to resume normal operation. Not all of the following steps will necessarily be required, depending on your site configuration:

1. Connect to the controller's web interface using HTTPS, unless it is an older controller with no default certificate loaded, then it will connect using HTTP.
2. Recreate the admin operator and log in to the controller's web interface.

   If you are not prompted to create the admin operator, the default username is admin with the password admin.

3. Reset the controller's IP address to its previous value.
4. Reconfigure any additional network settings.
5. Reinstall previously installed custom HTTPS certificates.
6. Restore any other system settings as required by your site configuration.

Disclaimer and Warranty

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

For warranty information, see our Standard Product Warranty.

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