Protege GX Integrated System Controller

Configuration Guide

Last Published: 06-Sep-22 02:04 PM

Contents

Introduction

This configuration guide provides programming instructions and system communication and troubleshooting information for Protege GX 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 GX controller models:

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

About This Module

The Protege GX controller is the central processing unit responsible for the control of security, access control and building automation in the Protege GX 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.

Protege GX is an enterprise level integrated access control, intrusion detection and building automation solution with a feature set that is easy to operate, simple to integrate and effortless to extend.

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 GX controllers include:

Features	PRT-CTRL-DIN-IP	PRT-CTRL-DIN	PRT-CTRL-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 settings in order to get the controller online with a Protege GX server. These settings include:

- IP addressing, including IP address, subnet mask, gateway and DNS settings
- Event server connections
- Event, control and download port 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

Protege controllers have a built-in web interface which can be accessed via your web browser. However, due to ongoing changes in internet security and controller technology you may encounter some error messages as you attempt to log in to your controller.

To access your controller for the first time:

1. Open a web browser and into the URL bar enter https:// followed by the IP address of the controller.
   If you are logging in for the first time this will be: **https://192.168.1.2**

   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.

2. If the connection is **successful** the browser will warn you that the connection may not be secure. For example, you may see a message similar to the following:
   - Chrome: "Your connection isn't private " (NET::ERR_CERT_AUTHORITY_INVALID)
   - Edge: "Your connection isn't private " (NET::ERR_CERT_AUTHORITY_INVALID)
   - Firefox: "Warning: Potential Security Risk Ahead" (MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT)

   This warning is displayed because the default security certificate on the controller is self-signed, and therefore not trusted by the web browser. The connection is still encrypted.

3. To access the controller, click **Advanced**, then select the option to proceed to the controller's IP address. You will then see the controller's login page.

   This also adds a security exception for the controller, allowing you to access the web interface in future without a warning.

4. If the connection has **failed** you may see an error message similar to the following:
   - Chrome: "This site can't be reached. 192.168.1.2 refused to connect." (ERR_CONNECTION_REFUSED)
   - Edge: "Hmmm... can't reach this page. 192.168.1.2 refused to connect." (ERR_CONNECTION_REFUSED)
   - Firefox: "Unable to connect. An error occurred during a connection to 192.168.1.2."

   When you see this error, remove the https:// prefix from the URL. For example, for a controller with a default IP address this would be: **192.168.1.2**

5. Alternatively, if the connection has **failed** you may see a message similar to the following:
   - Chrome: "This site can't provide a secure connection. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
   - Edge: "The connection for this site is not secure. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
   - Firefox: "Secure Connection Failed. Peer using unsupported version of security protocol." (SSL_ERROR_UNSUPPORTED_VERSION)

   The error messages you receive may differ depending on your server security settings.

   In this case, additional configuration is required to allow the connection. See the instructions for Browsing to Less Secure Controllers below.

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.

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 Less Secure Controllers

Some controllers use older hardware types or operating systems which do not support more recent security protocols and cipher suites. Most web browsers will not allow users to access the web interface of these controllers, even if users trust the site and accept the risk.

If you see one of the following errors when browsing to the controller, it means that the controller has an HTTPS security certificate installed, but only supports the older TLS 1.0 protocol.

The error messages you receive may differ depending on your server security settings.

- Chrome:
  - "This site can't provide a secure connection. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
  - "This site can't be reached. 192.168.1.2 unexpectedly closed the connection." (ERR_CONNECTION_CLOSED)
- Edge:
  - "The connection for this site is not secure. 192.168.1.2 uses an unsupported protocol." (ERR_SSL_VERSION_OR_CIPHER_MISMATCH)
  - "Hmmm... can't reach this page. It looks like 192.168.1.2 closed the connection." (ERR_CONNECTION_CLOSED)
- Firefox:
  - "Secure Connection Failed. Peer using unsupported version of security protocol." (SSL_ERROR_

UNSUPPORTED_VERSION)
- "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 controllers.

1. Download and install Firefox from the Mozilla website if you do not have it already.
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 less secure controllers 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.

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.

1. Log in to the controller web interface and navigate to the **System Settings** page.
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** 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

For two-door controllers, 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

One-door controllers currently support self-signed certificates only. Third-party certificates are not supported.

Protege controllers have HTTPS connection enabled by default with a pre-loaded certificate. 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 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 on-site 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.

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).

For configuration and version requirements refer to AN-314: HTTPS Connection to the Protege GX 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.

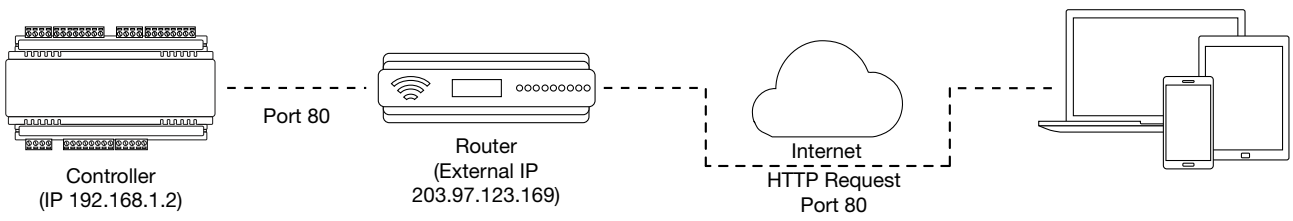
Operating on an active network requires knowledge of the configuration and structure of the network. Always consult the network or system administrator before you begin.

For detailed networking information, see the Protege GX Network Administrator 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.

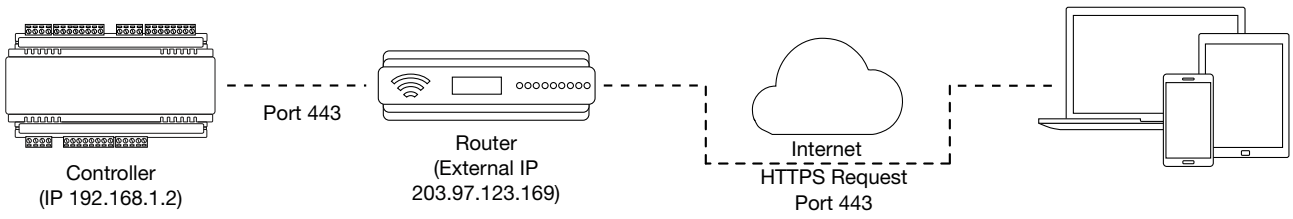
External access via HTTP is only required in order to validate and install your certificate. Once the certificate has been installed, HTTP access will be disabled because the more secure HTTPS connection is available. Therefore it will no longer be necessary to forward external port 80 to the controller.

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

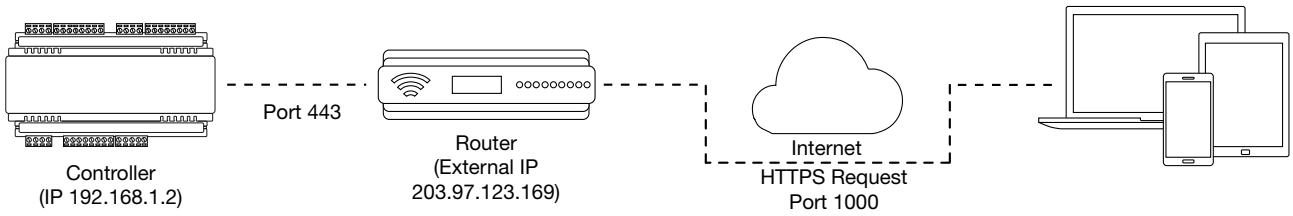
After you have installed a certificate and established an HTTPS connection to the controller, you may wish to continue accessing the controller over the internet. To achieve this, the controller must be accessible via its HTTPS port. The default HTTPS port is **internal port 443**, but this can be changed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

One-door controllers currently support self-signed certificates only. Third-party certificates are not supported.

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 support third-party certificates. One-door controllers and two-door controllers without USB ports do not support these 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.

If you receive an error message when browsing to the controller, some additional configuration may be required to allow access. For more information, see Browsing to Less Secure Controllers (page 8).

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.

If you receive an error message when browsing to the controller, some additional configuration may be required to allow access. For more information, see Browsing to Less Secure Controllers (page 8).

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.

If you still cannot browse to the controller, additional web browser configuration may be required. For more information, see Browsing to Less Secure 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.

Communications: Event Servers

The event server manages communication from the controller to the Protege GX server. The event server is configured in Protege GX and the controller settings determine communication with the event server.

- **Event Server 1***: The primary event server connection settings.
  - The IP address or DNS name for connection to the event server.
  - **Primary Adaptor**: The controller's adaptor connection to the event server, via either the **Onboard** ethernet connection or **USB Ethernet** port.
  - **Secondary Adaptor**: The controller's backup adaptor connection to the event server (optional).
- **Event Server 2/3***: Alternative paths to the event server (optional).

Communications: Ports

- **Event Port***: The default port is **22000**. This must match the port defined in **Global | Event server** in the Protege GX software.
- **Download Port***: The default port is **21000**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.
- **Control Port***: The default port is **21001**. This must match the port defined in **Sites | Controllers | General** in the Protege GX software.

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.

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.

  The **Dynamic IP address update** option must also be enabled for this controller in Protege GX (**Sites | Controllers | General**).

  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 .

Operators

Operators can be created, deleted and saved using the toolbar buttons at the top right. Note that these are operators for the controller's web interface and do not correspond to operators in the Protege GX software.

- **Name**: A name for the operator record in the web interface.

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

Configuration

- **Username/Password**: The operator's login credentials for the controller's web interface.
- **Change Password**: Click this button to change the password of the operator.

  It is recommended that you give each operator a secure password. Passwords must comply with password policy requirements.

- **Default Language**: Select a default language for the operator. This language will be displayed when the operator uses the web interface.

Operator Timeout

- **Enable Operator Timeout**: When this option is enabled, the operator will be automatically logged out of the web interface after a defined period of inactivity.
- **Operator Timeout**: Set the length of time in minutes before the operator will be automatically logged out.

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.

  In the future this will be configurable, but is currently fixed at 8 characters.

- **Minimum Number Of Uppercase Characters**: This option is reserved for future development.
- **Minimum Number Of Digits**: This option is reserved for future development.

- **Minimum Number of Special Characters**: This option is reserved for future development.
- **Compare Against Username**: This option is reserved for future development.

Application Software

Controller Software

- **Current Version**: Displays the current firmware version of this controller. Click on this field to display further version information.

Update Application Software

- **BIN File**: This section is used to update the firmware of the controller. Click **Upload** to browse to the firmware file (.bin format) supplied by ICT, and open the file to install the new firmware on the controller.

  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.

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.

Configuring a Controller via the Protege GX Software

To add a controller to the Protege GX system, navigate to **Sites | Controllers** and click **Add**. Several options are available, allowing you to define which records will be created alongside your controller.

- **Use the controller wizard**: The controller wizard allows you to specify the inputs, outputs, doors and expander modules that are required by your site. Some additional options can also be configured. The selected default records are automatically added to the database with the controller.
- **Just add a controller**: Only the controller record itself is added to the database. All other records must be programmed separately.
- **Add new controller based on an existing controller**: The controller record and all connected programming are duplicated from an existing controller. This includes devices such as expander modules, inputs, outputs and doors.

  It may be convenient to create a 'template' controller record as a base for adding new controllers.

Once the controller record has been created, bring it online by entering the **Serial number**, **IP address**, **Download port**, **Download server** and **Control and status request port** in the **General** tab. If the controller does not come online, you will need to troubleshoot the connection (see page 49).

Adding a Controller with Default Records

When you select **Use the controller wizard**, the **Add controller** configuration window is displayed. This allows you to automatically add default records (inputs, outputs, expander modules, doors) alongside the controller. The records have default names and settings, and can be renamed, edited or deleted as required.

General

- **Name**: The name of the controller in the Protege GX software.
- **Count**: The number of controllers that will be added with the same default records. If more than one controller is added the subsequent controllers will be assigned default names that can be edited later.
- **Prepend controller name to added records**: When this option is enabled, all new records generated by the wizard will include the controller name at the start of the record name. For example, if the controller is named Office, the first output on the controller will have the name Office CP1 Bell 1.

Controller

- **Type**: The model code of the controller that is being added to the system. This is displayed on the upper right of the controller face.
- **Inputs**: The number of onboard inputs that will be created for the controller. This is set automatically based on the **Type** of controller selected.

  Not all controller inputs may be required if the onboard reader expander is being used, as the inputs can be assigned to the reader expander record.

- **Outputs**: The number of onboard outputs that will be created for the controller. This is set automatically based on the **Type** of controller selected.

  This number includes only the bell and relay outputs (outputs 1, 3 and 4). Reader outputs are assigned to the onboard reader expander record (even if not used for connected readers).

  Controller output 2 only exists on legacy hardware. This address is skipped when the wizard automatically adds the default records.

- **Add trouble inputs**: Enable this option to automatically add the trouble inputs associated with the controller.

Keypads, Input expanders, Reader expanders, Output expanders and Analog expanders

Enter the **Type** and number of each expander module that should be added to this controller. The number of inputs and outputs required should be set automatically. Enable **Add trouble inputs** to include the trouble inputs for each module.

If the controller's onboard reader expander is being used it should be included in the number of reader expanders so that the relevant programming can be created.

Options

- **Create "Installer" menu group**: Creates a menu group with every menu enabled for use by site installers.
- **Create floor plan**: Creates a floor plan including all inputs and outputs on the controller. This is useful for small sites with only a few inputs and outputs. For larger sites it is generally better to create the floor plans manually.
- **CID report map**: The Contact ID report map that will be used for assigning the **Reporting ID** to each input. The options are:
  - **Standard**: Suitable for small burglary and access control installations.
  - **Large**: Suitable for intrusion detection installations with a large number of input expanders.
  - **SIMS II**: A variant of the Contact ID format which can send a much larger number of inputs. For this mapping to function correctly the service must also be configured for SIMS II by setting the **Cid mapping** option for a Contact ID service, or the **CID map settings** option for a Report IP service.

  For more information, see Application Note 316: Contact ID Reporting in Protege GX and Protege WX.

Doors

- **Doors**: Automatically creates the defined number of door records. Typically this should be 2 doors per reader expander.
- **Assign to reader expanders**: Automatically assigns the doors to reader expander ports, in order of creation.
- **Add door trouble inputs**: Creates the relevant trouble inputs for each door record.
- **Assign reader lock output to door configuration**: Automatically sets the **Lock output** for each door to the relay output on the associated reader expander.
- **Assign reader beeper to door alarm configuration**: Automatically sets the **Pre alarm output**, **Left open alarm output** and **Door forced output** for each door to the beeper output on the associated reader expander.

Adding a Controller Based on an Existing Controller

When you select **Copy an existing controller**, the **Copy controller** configuration window is displayed. This allows you to select the controller to copy, and configure some options.

The copied records include inputs, outputs, doors, areas and groups associated with that controller.

The new controller record will have a blank **Serial number**, **IP address** and **Download server**.

- **Site (copy from)**: Defines the site that the programming will be copied from.
- **Controller (copy from)**: Defines the controller that the programming will be copied from.
- **New controller name**: The name of the new controller in the Protege GX software.
- **Name (second language)**: The name of the new controller in the second language.
- **Prepend controller name to all record names**: When this option is enabled, all new records generated by the copy process will include the new controller's name at the start of the record name. This means all new records will have the same name as those on the original controller, with the new controller's name added.

  If the original records included the controller's name, this name will still be included in the new records (i.e. will not be replaced by the new name).

- **Copy access levels**: When this option is enabled the access levels of the original controller are copied for the new controller. The new access levels are assigned the equivalent doors, areas and other records from the new controller, but are not assigned to any users.
- **Copy global records**: When this option is enabled, site-wide records such as schedules and function codes will be copied for use with the new controller.

Configuring a Controller

Once added, the controller needs to be configured to define settings including the serial number and communication parameters.

Controllers | General

General

- **Name**: The name of the record in English. This name is used everywhere the record appears in the English version of the software.
- **Name (second language)**: The name of the record in the second language (as installed with the software). This name is used everywhere the record appears in the second language version of the software. Alternatively, additional information about the record may be included in this field.
- **Record group**: The record group this item belongs to. This allows records to be organized by categories such as building, branch or company. Using roles and security levels, you can restrict operator access so that operators can only see or control the records in specific record groups.

  Some record types, such as outputs, inputs, trouble inputs and expander modules, inherit the record group assigned to the controller.

Communications

- **Serial number**: The serial number of the controller. This can be obtained from the configuration page of the built-in web interface, or the label on the side of the controller.
- **IP address**: The IP address of the controller. The default IP address is 192.168.1.2, which can be changed via the built-in web interface.

  In general the IP address should be the same here and in the controller web interface. Alternatively, if the controller is external to the server network you may need to enter the external IP address of the router which is forwarding traffic to the controller.

  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.
- **Dynamic IP address update**: When this option is enabled the software automatically detects the IP address of the controller from incoming messages and updates the **IP address** field automatically. Use this for situations where the controller's IP address may change unexpectedly, or when the controller is configured to use DHCP.
- **Username / Password**: If the single record download service is in use, you must enter a username and password for the controller so that the service can make a connection. These must match an operator in the controller's web interface.

  Ensure that the **Username** is entered in all lowercase letters, otherwise the connection will fail.

  These fields are not required when the single record download service is not in use.
- **Download port**: The TCP/IP port that is used by the download service to send programming downloads to the controller. By default, this is port 21000.
- **Single record download port**: The TCP/IP port that will be used by the single record download service (if in use) to send programming downloads to the controller. This should match the **HTTPS Port** of the controller. By default, this is port 443.
- **Download server**: Defines the download server which will send downloads to the controller. If this field is <not set> the controller will not receive any downloads.
- **Control and status request port**: This field specifies the port that will be used to send manual commands and status requests to the controller over TCP/IP. By default, this is port 21001.

- **Last known IP address**: Shows the last IP address that the controller used to communicate with the server (read only).
- **Last downloaded**: Shows the date and time of the last download to the controller (read only).

Display

- **Panel name**: The name used to identify the controller to IP reporting services.

Diagnostic windows

- **Open download server diagnostic window**: Opens a window listing transactions between the controller and the download server. This can be useful for checking whether recent programming changes have been downloaded successfully.
- **Open event server diagnostic window**: Opens a window showing the current status of the event server. This can be useful for diagnosing controller connection issues.

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.

Download binary blob

- **Set the download binary blob from a file**: This feature allows you to select a binary blob file and download it to the controller. This is required for some specific transitions and integrations.

  Do not use this feature unless specifically advised by ICT.

- **Database data length (bytes)**: The size of the file that has been selected for download.

Record history

Each record displays its programming history, including the time and date it was created, the time and date it was last modified and the operator who last modified it.

Controllers | Configuration

Configuration

- **Test report time (HH:MM)**: The controller periodically tests the reporting service by opening the predefined Service Report Test trouble input. This field sets the time of day the trouble input will be opened.

  When the **Test report time is periodic** option is enabled in the **Options** tab, 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**: The time of day when the controller will update the users and other offline parameters on legacy intelligent expander modules. The **Enable automatic offline download** option must be enabled. This option is not used for DIN rail modules.
- **AC restore delay time**: The time, in seconds, that the AC Failure trouble input will remain open after an AC failure before restoring. This setting is only relevant to legacy hardware which is supplied by an AC power source.
- **AC fail time**: The time, in seconds, that the AC mains voltage must have failed before the AC failure trouble input will be opened. This setting is only relevant to legacy hardware which is supplied by an AC power source.
- **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.

From controller firmware version 2.08.886 module UDP/TCP communications are disabled by default. You can re-enable communications by entering the following commands in the **Commands** field (**General** tab): `EnableModuleUDP = true` and `EnableModuleTCP = true`.

- **Modem country**: This option affects the number of dial attempts made by phone line reporting services, and may override the **Dial attempts** setting in the reporting service. It is recommended to test the number of dial attempts to ensure that you comply with regional requirements.

  This setting is only supported by controller models with onboard modem dialers.

- **Modem backup phone number**: If ethernet communication fails, the controller's onboard modem will dial this number to report events. The **Module backup if IP fails** option must be enabled (**Options** tab).

  This setting is only supported by controller models with onboard modem dialers.

- **Default language**: The default language displayed on the keypad for users who have no language selected and for any events generated by a serial printer service (see **Programming | Services | Serial printer**).
- **Download retry delay**: This field allows you to set a minimum delay period (in seconds) between downloads to this controller. After the download server has completed a download it will not attempt to download to this controller again until the delay has elapsed, except in the following circumstances where the download server will send the download as soon as possible without waiting for the delay period:
  - When a **Force download** command is sent
  - When changes are made to hardware devices that are hosted by the controller (e.g. expanders, inputs, outputs)
  - When the single record download service triggers a full download

  The minimum retry delay is 10 seconds.

- **Register as reader expander**: The module address assigned to the controller's onboard reader expander. You can program the onboard reader expander by creating a record with the same address in **Expanders | Reader expanders**.

  This address must not be the same as that of any physical reader expander.

- **Onboard reader lock outputs**: This option determines which outputs on the controller are mapped to the onboard reader expander's lock outputs. This should generally be set to Controller relay 3/4 outputs, which maps controller outputs 3 and 4 to reader expander outputs 1 and 2. If the controller is not being used for door control this option may be set to None.
- **Touch screen UDP port**: The UDP port that a Protege Touchscreen will communicate over.

  From controller firmware version 2.08.886 touchscreen communications are disabled by default. You can re-enable communications by entering the following command in the **Commands** field (**General** tab): `EnableTLCDCommsUDP = true`.

- **Maximum packet size**: The maximum packet size that can be downloaded to the controller.
- **Controller offline grace time**: If a controller drops offline there is a fixed grace period of 1 minute before Protege GX begins indicating that the controller is offline. This option allows you to extend this grace period by a number of minutes. This should be used in situations where the controller periodically drops offline and comes online again, allowing you to avoid unnecessary alerts.

Encryption

- **Initialize controller encryption**: Enables encryption of the messages sent between the controller and the Protege GX server. Selecting this option initiates a one-off process that randomly generates a 256 bit AES encryption key. Using an RSA algorithm, this key is exchanged and stored in both the controller and the Protege GX database.
- **Disable controller encryption**: Instructs the software to stop using encryption. To prevent encryption from being disabled accidentally or maliciously, this option will not change the encryption setting in the controller itself. You must hardware default the controller to fully disable encryption and allow communications.
- **Encryption enabled**: Read only field that indicates whether encryption is enabled.

HTTPS public key

- **HTTPS public key**: If the single record download service is in use this field displays the public key of the controller's HTTPS certificate. This is automatically populated when the single record download service connects to the controller for the first time. If the certificate is changed or the controller is defaulted you must delete the information in this field to allow the single record download service to reconnect.

Version 3 settings

This section displays settings which were used in software version 3 and earlier. These settings do not require configuration in version 4 or later.

Controllers | Options

Options

- **Test report time is periodic**: When this option is enabled the **Test report time** set in the **Configuration** tab will be treated as a frequency rather than a time of day. For example, a Test Report Time of 12:00 AM will cause the Service Report Test trouble input to be opened every 12 hours if this option is enabled, or every day at 12AM if this option is disabled.
- **Weekly test report**: When this option is enabled the test report is sent once a week based on the day of the week selected. The Service Report Test trouble input will be opened at the time specified in the **Test report time** field in the **Configuration** tab. When this option is disabled the trouble input will be opened once a day.
- **Day of the week**: Defines the day of the week that the weekly test report is sent.
- **Troubles require acknowledge**: System troubles are displayed in the trouble view menu of the keypad (**[Menu] [5] [2]**). Normally if the trouble condition ends (i.e. the trouble input closes) the trouble is no longer included in this list; however, with this option enabled the trouble condition remains in the list until it is acknowledged by an authorized user.

  Users must have **Acknowledge system troubles** enabled in **Users | Users | Options** and access to the **View (5)** menu from their menu group.

- **Generate input restore on test report input**: When this option is enabled the controller will generate a restore event for the Service Report Test trouble input closing after the regular test report. This occurs one minute after the Service Report Test trouble input has been activated.
- **Report short duration module communication failure**: When this option is enabled the controller will always generate trouble events for any module communications failure, without allowing any grace period for the module to come back online.
- **Advance UL operation**: When this option is enabled the Protege GX 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.

  This setting must be used in conjunction with the other configuration requirements in the controller installation manual.

- **Duplex inputs**: With this option enabled the controller can support twice the number of inputs, wired in duplex configuration. For more information, see the relevant controller installation manual.

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.
- **Modem backup if IP fails**: When this option is enabled the controller will dial out through the onboard modem if it cannot connect to the software via ethernet to report events. The **Modem backup phone number** must be set in the **Configuration** tab.

  This setting is only supported by controller models with onboard modem dialers.
- **Backup only alarm events**: With this option enabled, when the controller has lost ethernet connection it will only report alarms and other reportable events over the phone line. All stored events will be reported when the ethernet link is restored.

  This setting is only supported by controller models with onboard modem dialers.
- **Invert controller tamper input**: When this option is enabled the controller will invert the module tamper input allowing a normally open tamper switch to be used. This setting is only relevant to older hardware which includes an onboard tamper input.
- **Log all access level events**: This is a legacy option that has no effect.
- **Do not wait for dial tone when modem dials out**: When this option is enabled, modem dialing occurs even when no dial tone is detected.

  This setting is only supported by controller models with onboard modem dialers.

Controllers | Time update

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.
Daylight savings settings can be configured in **Programming | Daylight savings**.

- **Automatically synchronize with an internet time server**: Select this option to automatically synchronize the controller's internal clock with an internet time server.
- **Primary SNTP time server**: The IP address of the primary SNTP time server that the controller will use to update its time.
- **Secondary SNTP time server**: The IP address of the secondary (backup) SNTP time server that the controller will use to update its time. This time server will be used if the controller cannot connect to the primary server.
- **Time zone**: The current time zone that the controller is stationed in. Each time zone is described via its offset from GMT and relevant regions.

Controllers | Custom reader format

This tab allows you to define a custom reader format (Wiegand or Magnetic) which is available for use by reader expanders connected to the controller. To use this format, set the **Reader format** (**Expanders | Reader expanders | Reader 1/2**) to Custom format.

See **Sites | Credential types** for alternative options for configuring custom credentials.

Custom reader configuration

- **Custom reader type**: Defines the reader type. The data can be output as Wiegand (D0 and D1) or Magnetic (Clock and Data).
- **Bit length**: The total number of bits that are sent by the card reader for each credential.

- **Site code start**: The index where the site/facility code data starts in the transmitted credential data. The count starts at zero.
- **Site code end**: The index where the site/facility code data ends in the transmitted credential data. The count starts at zero.
- **Card number start**: The index where the card number data starts in the transmitted credential data. The count starts at zero.
- **Card number end**: The index where the card number data ends in the transmitted credential data. The count starts at zero.
- **Data format**: This field describes how to handle the site/facility code and card number received from the reader. If the size of the site/facility code is smaller than 16 bits and the size of the card number is smaller than 16 bits, set the data format to 16 Bit Data. Otherwise use 32 Bit Data.

Parity 1-4 options

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

All parity options that are not in use must be set to 255.

- **Parity type 1-4**: The method of calculating the parity for the block. This is either even or odd parity.
- **Parity location 1-4**: The position of the parity bit in the received data. The count starts at zero.
- **Parity start 1-4**: The index where the parity block starts in the received data. The count starts at zero.
- **Parity end 1-4**: The index where the parity block ends in the received data. The count starts at zero.

Bit options

All bit options that are not in use must be set to 255.

- **Set bit 1-4**: The index of a set bit (a logical '1') in the received data. The count starts at zero.
- **Clear bit 1-4**: The index of a clear bit (a logical '0') in the received data. The count starts at zero.

Card data options

- **Card data AES encryption key**: Salto SALLIS and Aperio cards can be encoded with site/card information via the ICT Encoder Client. This field defines the decryption key so that Protege GX can decrypt data from these cards.

  For more information, see Application Note 147: Protege GX Aperio Integration or Application Note 148: Protege GX Salto SALLIS Integration.

  This field sets the card data AES encryption key for all reader ports associated with this controller.

Manual Controller Commands

Right clicking on a controller record (**Sites | Controllers**) displays a menu with manual commands for that controller.

Set controller date time

If you are not using a time update server to synchronize the controller time (see **Sites | Controllers | Time update**) you can update the time and date manually using this command. To manually update the time on a controller:

1. Right click on the controller record in **Sites | Controllers**.
2. The **Time** field displays the current date and time at the server. If you need to change these, enter new values in the field or click on the clock icon to use the time and date picker.
3. Click **Set controller date time** to send the entered time to the controller.

Update modules

Programming changes that alter the way hardware will operate require a module update to download the hardware-specific settings. A module update command causes the module to restart.

Use this option to perform a module update on the controller and all connected modules.

Warning: Sending this command will cause the controller and every connected module to temporarily go offline as they restart. This option should **not** be used in an active system.

To update only a specific module (such as a keypad or reader expander), right click on the specific record in the **Expanders** programming and click **Update module**.

Force download

In normal operation the download service checks each controller for changes in order by Database ID. If any changes are detected the services downloads the changes to that controller, then continues on to the next controller.

An operator can use the **Force download** command to increase the priority of a specific controller, so that it will be next in line after the previous controller has been completed. The **Download retry delay** period will be ignored so that the download is sent as soon as possible.

In addition, the download service will download to the controller even if no changes are detected.

Get health status

The **Get health status** function sends a command to the controller to retrieve its current health status. The health status window will open, displaying any notices or issues relating to the controller or its module network.

The **Clear** button can be used to clear some notices which do not require action (e.g. 'The Controller has been restarted').

The health status window is static. Resolving or clearing notices will not cause the status to update until the **Get health status** command is sent again.

Module addressing

The **Module addressing** command is used to view the hardware that is connected to the system network, and to set the addresses of modules. Selecting this option opens a window showing the details of all modules that are currently connected, as well as those that have registered previously but are currently offline.

By default, Protege modules are shipped from the factory with an address of 254. This is outside the range that the controller will accept, so the address must be set by the installer. For some modules, such as keypads, the network address can be set in the module itself (see the relevant installation manual). For most Protege modules the address is set in the **Module addressing** window.

The address of the controller's onboard reader expander is set by the **Register as reader expander** setting in **Sites | Controllers | Configuration**.

Setting Module Network Addresses

1. Ensure the controller is correctly powered and is communicating with the Protege GX software.
2. Connect the module(s) that require addressing to the module network. Make sure the power light on each module is on and that the status indicator 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 indicator will begin flashing an error code.
   - If the module has been previously addressed and is not a duplicate then it will succeed in registering and the status indicator will begin flashing at 1 second intervals.
4. Once all modules have completed the registration process (successful or not), open the Protege GX software and navigate to **Sites | Controllers**.
5. Right click on the controller record and select **Module addressing** to open the module addressing window. This window displays all of the modules that are connected to the controller with the following information:
   - The module type (e.g. controller, keypad, etc.)
   - The serial number
   - Current firmware version and build number
   - The current module address
   - Whether the module address can be changed (for example, the controller's address cannot be changed)
   - Whether the module has successfully registered with the controller
   - Whether the module is currently online

   The controller's onboard reader expander will appear on this list as a reader expander with the same serial number as the controller. The address of this reader expander must be set in the **Register as reader expander** field (**Configuration** tab).
6. Before assigning addresses to modules you may need to identify specific physical modules:
   - For DIN rail modules, click the **Find** button to activate identification mode for the specified length of time. In identification mode the status and fault indicators flash in an alternating pattern, allowing you to identify the specific module.
   - For all modules, compare the **Serial** column with the serial number of each module (found on the module label).
7. For each module set the network address in the **Address** column. The new addresses will be displayed in **bold**, indicating that they have not yet been updated in the modules.
8. Push the addresses to the modules either by clicking **Update** for each individual module or by clicking **Update all**. Allow approximately 5 seconds for the module to re-register with the controller at the new address.
9. Click **Refresh**. The new addresses should change from bold to normal font and the newly addressed modules should be online.
   - If the address has not changed, check that the module has finished attempting to register with the controller.
   - If the address has changed but the module is not registered or online, check the address is in the valid address range and that it is not a duplicate of another module address.

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

Legacy Protege PCB modules cannot be addressed by this process. They must be addressed using DIP switches as described in the relevant installation manual.

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.

Update firmware

Use the **Update firmware** option to update the firmware of one or more controllers.

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. Click on the ellipsis **[...]** button and browse to the .bin firmware file. Click **Open**.
2. Check the boxes of the controller(s) that you wish to update.
3. Click **Update**.

This process will take approximately 10 minutes per controller and it is recommended that firmware updates 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 firmware is being updated.

A popup message may appear in the user interface with the message 'Update Interrupted'. This is expected behavior for some firmware versions and does not indicate that the update has failed.

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. By default the onboard reader is disabled. To enable it, configure the address at which you want it to register using the Protege user interface. Note that any physical reader expander module that is connected with the same address will be treated as a duplicate and will fail to register, so care should be taken to ensure the address is unique.

Enabling the Onboard Reader Expander

To enable the controller's onboard reader expander, complete the following steps:

1. Navigate to **Sites | Controllers** and select the controller.
2. In the **Configuration** tab, set the **Register as reader expander** field to any address that is not currently being used by a reader expander.
3. Click **Save**.
4. Navigate to **Expanders | Reader expanders**. Select the relevant **Controller** in the toolbar.
5. **Add** a new reader expander and set the **Physical address** to the address selected above.
6. Click **Save**.
7. In the **Module configuration** window, review the settings to create the inputs, outputs, trouble inputs and doors associated with the onboard reader expander.
8. Click **Add now**.

Two-Door Controllers

For two-door controllers, the onboard reader can use 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 can use 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 using 1K and 2K4 resistors. For more information about the wiring requirements, see the relevant installation manual.

1. To enable this feature, check the **Duplex inputs** option in **Sites | Controllers | Options**.
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 type and group that they activate.

Two-Door Controllers

Input Number	Description	Type	Group
CP001:01	Reserved	-	-
CP001:02	12V Supply Failure	Power Fault	General
CP001:03	Reserved	-	-
CP001:04	Real Time Clock Not Set	RTC/Clock Loss	General
CP001:05	Service Report Test	-	-
CP001:06	Service Report Failure to Communicate	Reporting Failure	General
CP001:07	Phone Line Fault (modem model only)	Phone Line Lost	General
CP001:08	Auxiliary Failure	Power Fault	General
CP001:09	Bell Cut/Tamper	Bell/Output Fault	General
CP001:10	Reserved	-	-
CP001:11	Bell Current Overload	Bell/Output Fault	General
CP001:12	Reserved	-	-
CP001:13	Module Communication	Module Loss	System
CP001:14	Module Network Security	Module Security	System
CP001:15	Reserved	-	-
CP001:16	Reserved	-	-
CP001:17	Reserved	-	-
CP001:18	Reserved	-	-
CP001:19	Reserved	-	-
CP001:20	Ethernet Link Lost	Hardware Fault	System
CP001:21	Reserved	-	-

Input Number	Description	Type	Group
CP001:22	ModBUS Communication Fault	Hardware Fault	System
CP001:23	Protege System Remote Access	Hardware Fault	System
CP001:24	Installer Logged In	Hardware Fault	System
CP001:25	Reserved	-	-
CP001:26	Reserved	-	-
CP001:27	Reserved	-	-
CP001:28	Reserved	-	-
CP001:29	System restarted	Hardware Fault	System
CP001:30	Reserved	-	-
CP001:31	Reserved	-	-
CP001:32	3G Modem Link Lost (legacy 3G modem model only)	Hardware Fault	System
CP001:33	Controller Group Link Lost	Hardware Fault	System
| | | |	| |	|	|
CP001:64	Reserved	-	-

One-Door Controllers

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

Configuring the Cellular Modem Connection

Cellular modem connection requires the controller to be operating firmware version 2.08.1271 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.

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.

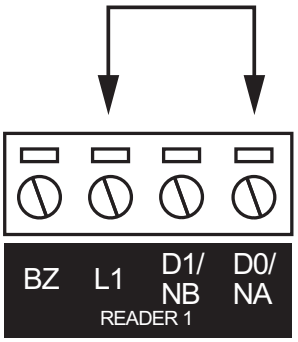
Temporarily Defaulting the IP Address

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 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

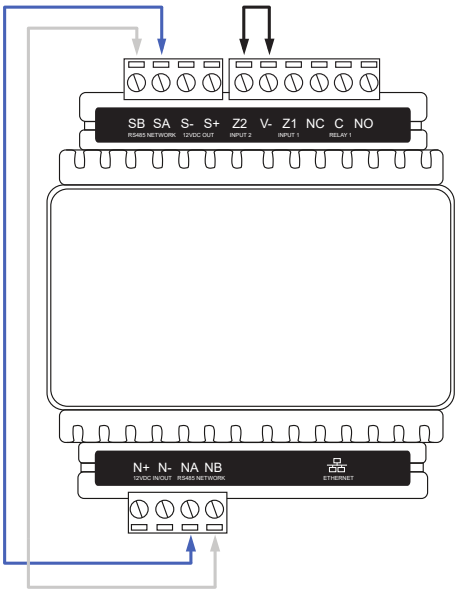
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between **Reader 1** D0 input and **Reader 1** L1 output.



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.

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
6. Connect to the controller by entering https://192.168.111.222 into the address bar of your web browser, and view or change the IP address 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.

   You can now connect to the controller using the configured IP address.

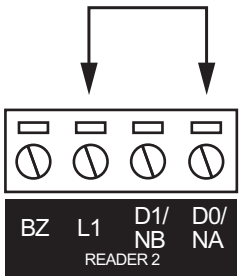
Defaulting a Controller

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

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

Defaulting a Two-Door Controller

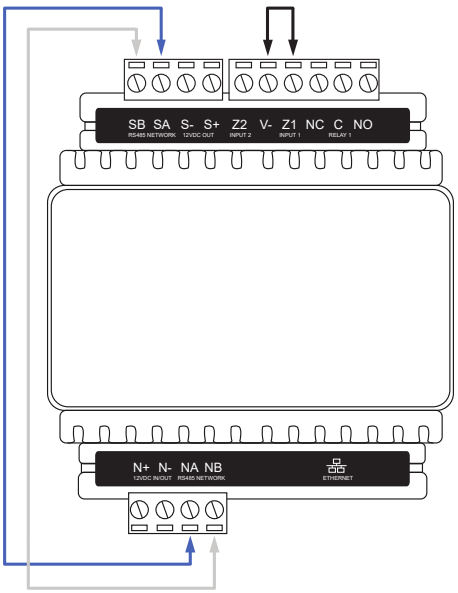
1. Remove power to the controller by disconnecting the 12V DC input.
2. Wait until the power indicator is off.
3. Connect a wire link between the **Reader 2** D0 input and the **Reader 2** L1 output.



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

Defaulting a Single-Door Controller

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



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

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

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

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

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

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

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

After Defaulting a Controller

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

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

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

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

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

Troubleshooting Controller Connectivity

The following section provides useful troubleshooting steps for situations where the controller and server are not communicating.

For a demonstration, see Bringing a Protege GX Controller Online on the ICT YouTube channel.

Communication Requirements

For the server and controller to communicate, the following are required:

1. The controller must be physically networked to the server, or connected over the web.
2. The Protege GX services must be running.
3. The server must have the correct IP address for the controller.
4. The server must have the correct controller serial number to properly identify incoming messages from it.
5. The controller must have the event server IP address and port set correctly (port 22000 by default).
6. The controller must be contactable on the download and control ports (ports 21000 and 21001 by default).
7. Protege GX must have the correct computer name configured for the download and event servers.
8. The Protege GX software and databases must have the same database version.
9. Encryption must either be disabled at both ends or enabled at both ends with the correct encryption key.

Check that the Services are Running

The simplest and first thing to check is that the Protege GX services are running.

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Scroll down to the Protege GX services. Ensure that the following services are running:
   - Protege GX Data Service
   - Protege GX Download Service
   - Protege GX Event Service
   - Protege GX Update Service
3. If any service is not running, right click on it and click **Start**.

If any services will not start there may be another issue with your installation. For example, the database version may be incompatible (see page 52).

Confirm Controller IP Address

For the server to be able to contact the controller it must have the correct IP address programmed and be able to reach that IP address.

1. In Protege GX, navigate to **Sites | Controllers**.
2. In the **General** tab, highlight and copy (CTRL + C) the **IP address**.
3. Paste (CTRL +V) the IP address into the address bar of a web browser on the server, with the prefix https:// (e.g. https://192.168.1.2).

   You may be presented with a certificate security warning on connection.
4. If you cannot connect, remove the https:// prefix and try again (e.g. 192.168.1.2) as your controller may not be configured for HTTPS.
5. If the controller is reachable using this IP address you should be presented with a simple login screen.
6. Log in to the controller using admin credentials.

If you are unable to web browse to the controller you may not have the correct IP address. If the IP address is unknown you will need to view/change it from a keypad or default the controller's IP address (see below).

If you do have the correct IP address then it is likely that you have a network problem. Ensure that the server and controller are on the same subnet, or have correct port forwarding configured at the router.

From firmware version 2.08.911 controller ping is disabled by default. If the controller is receiving downloads you can allow ping by adding the command `EnablePing = true` in the controller commands.

Unknown Controller IP Address

If the currently configured IP address is unknown:

- It can be viewed and/or changed using a Protege keypad. For more information, see Setting the IP Address from a Keypad (page 44).
- 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. For more information, see Temporarily Defaulting the IP Address (page 45).

Confirm Controller Serial Number

Incoming messages from the controller to the server are identified by the controller's serial number.

1. In the controller web interface, navigate to the **Settings** page.
2. Highlight and copy the **Serial number**.
3. In Protege GX, navigate to **Sites | Controllers | General**.
4. Paste into the **Serial number** field.

Duplicate IP Address or Serial Number

Although the software warns you, it is possible to save two controllers with the same IP or serial number. In this case, the controller created first takes priority.

- Confirm you haven't created a controller with a duplicate IP address or serial number. Check all of your sites.
- If you have created a site for templates, these should be left with zero IP addresses and serial numbers.

If you have two controllers with the same IP address or serial number anywhere on your server, there will be communication problems with at least one of them.

Confirm the Event Server is Functioning

To confirm the event server is functioning and listening on the correct port for incoming events, open the event server diagnostic window.

1. In Protege GX, navigate to **Sites | Controllers | General** and expand the **Diagnostic windows** section.
2. Select **Open event server diagnostic window**. You should see a message that reads 'Listening on Port : 22000'.

   The default event server port is **22000**, but this can be changed in **Global | Event servers**.
3. If the event server diagnostic window shows messages about an unknown serial number, events are being received from a controller with the serial number listed in the message. This also means the event server is accepting incoming events.
4. In the controller web interface, ensure that the **Event Port** matches the port set in Protege GX.
5. If you change the event port you must **save** and **restart the controller** using the icons in the upper right before your changes will take effect.

If the event server diagnostic window contains no text there is a problem with the configuration of the event server. This means the event server is **not** accepting incoming events. This can sometimes be resolved by restarting the Protege GX Event Service:

1. Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
2. Locate the Protege GX Event Service. Right click on the service and select **Restart**.

Confirm Event Server IP Address

For messages to get from the controller to the server, the controller must have the correct IP address for the event server.

1. On the server computer, open a command prompt. Enter the command `ipconfig` and press **[Enter]**.
2. You will be presented with the status and details of the server on various sub networks. Locate and copy the **IPv4 Address** for the sub network that the controller is connected to.

   For more complex networks it may be preferable to open a command prompt on a machine the controller is directly connected to and use the `ping` command to ascertain the external IP address of the server.
3. In the controller web interface, on the **System Settings** page, check that **Event Server 1** has the correct IP address. Paste in the address located above if it does not match.

   There are three spaces for entering the event server IP. This is for situations where controllers have multiple paths to the server. In most cases the second and third event server IP addresses should be left as all zeros or all 255s.

Confirm Ports

Next, ensure that the download and control ports set on the server match those set in the controller interface.

1. In Protege GX, navigate to **Sites | Controllers | General** and check these values:
   - **Download port** (default 21000)
   - **Control and status request port** (default 21001)
2. In the controller web interface, on the **System Settings** page, ensure that the **Download Port** and **Control Port** match those defined in the software.

3. If you have changed any settings on the controller, save your changes and restart the controller for the changes to take effect.

Check Computer Name

The download and event servers must have a correct computer name that matches the server machine. This usually only changes when you have restored a database from a different PC.

IMPORTANT: The computer name must be no longer than **15 characters**, or downloads will fail.

1. On the server computer, open **Control Panel > All Control Panel Items > System** to view computer information.
2. Copy the **Computer Name**.
3. In Protege GX, navigate to **Global | Download server** and check that the **Computer name** matches the name of the server machine. If not, paste in the name copied earlier.
4. Navigate to **Global | Event server** and again check and correct the **Computer name**.
5. If you have changed the computer name for either server, you must restart the corresponding service.

   Open the **Services** snap-in by:
   - Pressing the **Windows + R** keys
   - Typing **services.msc** into the search bar and pressing **Enter**
6. Locate the Protege GX services. Right click on the download service and/or event service and click **Restart**.

Repair Database Compatibility

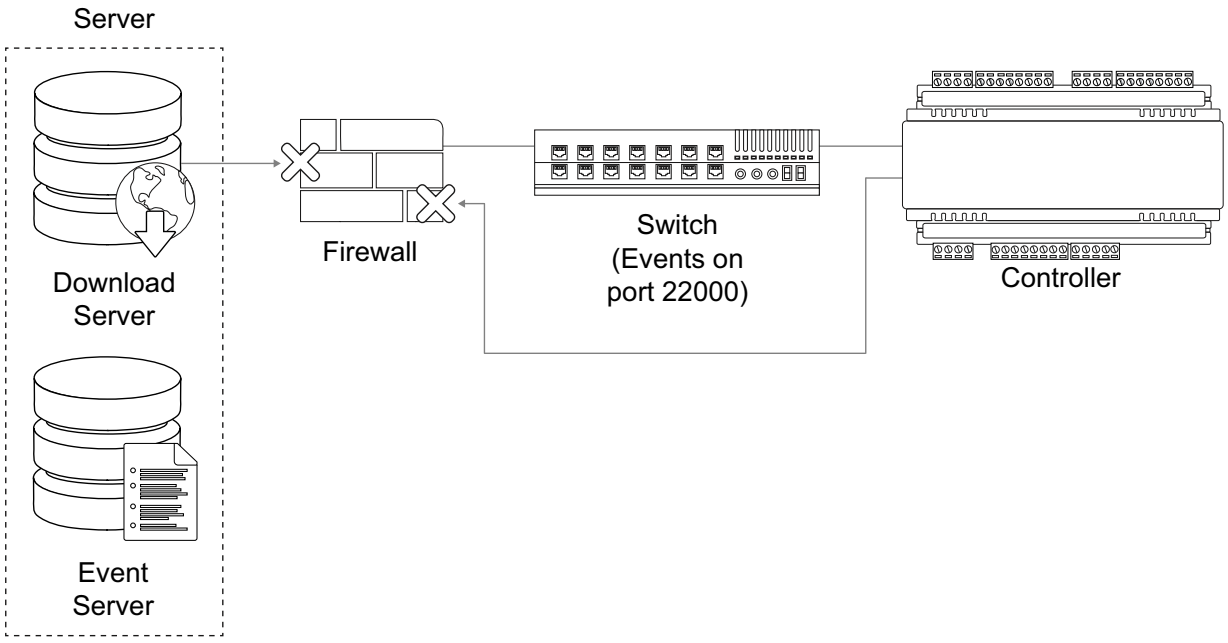
If you have restored a database from an older version of Protege GX, there may be a mismatch between the software and database versions. In this case the Protege GX Data Service will fail to start, the download and event server diagnostic windows will both remain blank, and no downloads will be passed to the controller.

To resolve this issue you must **uninstall and reinstall** Protege GX. This will prompt a database upgrade.

A backup taken from a newer version of Protege GX cannot be restored to an older version.

Windows Firewall

When the controller and server are on the same local network the only place a firewall can be blocking messages is on the server machine itself. This is called the Windows Firewall.



1. Open the Windows Firewall settings at **Control Panel > All Control Panel Items > Windows Firewall**. If the firewall is on, it is shown in green.
2. To eliminate the Windows Firewall as a cause of communication problems, turn it off temporarily by clicking **Turn Windows Defender on or off** at the left of the screen. Disable the firewall for each network location.

   Check whether this resolves the issue. If so, you can turn the Firewall back on and allow the Protege GX services through the Firewall.
3. Click the **Allow an app or feature through Windows Defender Firewall** link on the left of the screen.

   Third-party antivirus or firewall software may prevent modification of Windows Firewall rules. If this is the case, refer to the third-party manufacturer for details on allowing programs through the firewall.
4. Select **Allow another app...** to add a program as an exception.
5. Click **Browse...**, then navigate to the Protege GX installation directory.

   The default installation directory is C:\Program Files (x86)\Integrated Control Technology\Protege GX.
6. Select (double click or select and **Open**) the executable that you want to allow, then click **Add**.

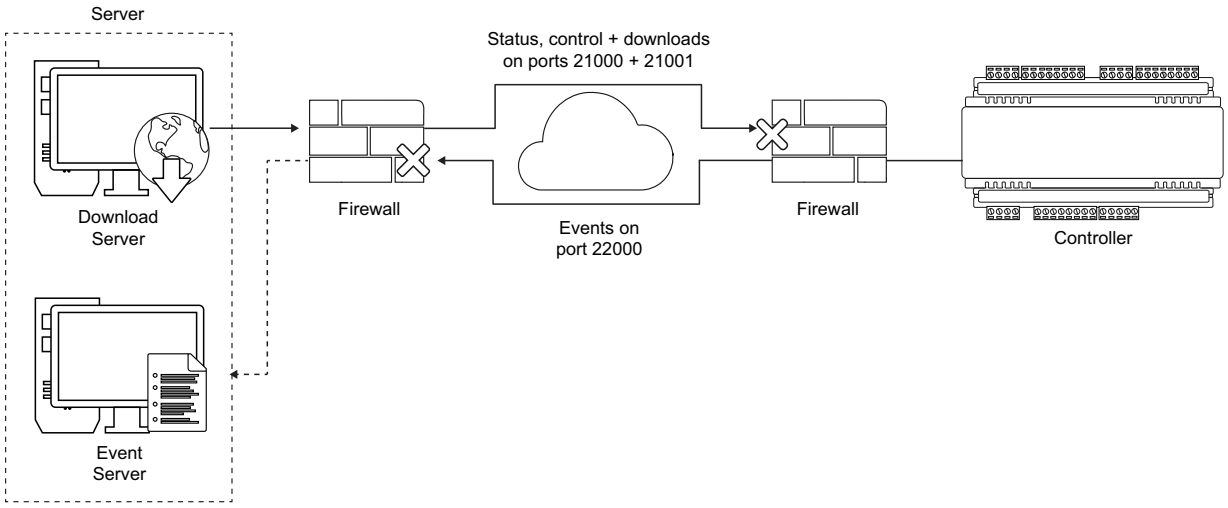
   Add the following Protege GX executables, one by one:
   - GXSV.exe
   - GXSV2.exe
   - GXSV3.exe
   - GXPI.exe
   - GXEvtSvr.exe
   - GXDVR1.exe
   - GXDVR2.exe

   This allows the necessary Protege GX services access through the Windows firewall.

   The above process will only allow access through your primary network connection. If you have multiple networks connected you will need to manually allow access (tick the checkbox in the network column) for each additional network that the Protege GX executable requires access through.

Multiple Firewalls

On corporate networks there can be multiple firewalls.



To ensure these are configured correctly, provide the Protege GX Network Administrators Guide to the appropriate IT staff member. This document is included in the software installation pack.

Encryption

Both Server and Controller Encryption Enabled

Encryption relies on a shared key that both the sender and receiver of a message know. The message is encrypted using the key, then decrypted by the receiver using the same key. If the message is intercepted, it will make no sense to anyone without the encryption key.

Server Enabled, Controller Disabled

If for some reason the receiver loses the key, it is unable to decrypt incoming messages. In this case, the message is rejected.

Server Disabled, Controller Enabled

If the sender loses the key, the message is sent in plain text. The receiver, expecting to receive encrypted events, will also reject the message as it may be of a malicious nature.

Server and Controller with Different Encryption Keys

If the sender and receiver have different keys, the message can still not be decrypted by the receiver. This also results in the receiver rejecting incoming messages.

Each time encryption is enabled at the server, a new encryption key is generated. Each controller has a unique key, independent from all other controllers. If encryption for a controller is disabled then enabled again, the key is changed. If encryption for a controller is disabled at the server, the controller must be defaulted. It is not possible to re-enable encryption without first defaulting the controller.

Both Server and Controller Encryption Disabled

If encryption is disabled at both the sender and receiver, received messages are accepted. The downside with this scenario is that anyone 'listening' between the sender and receiver can also receive the messages.

Disabling Encryption

Defaulting the controller is the only way to remove the encryption key. This is by design and intended as a security feature. It means that physical access to the controller must be gained before encryption can be disabled.

If you are unsure of the state of encryption of either the server or controller, disable encryption at the server, then default the controller. This ensures that neither is encrypted and rules this out as a cause of communications problems. Encryption should then be re-enabled once communications are established.

1. Disable encryption at the server.
   Navigate to **Sites | Controllers | Configuration** tab and click **Disable controller encryption**.
   The software warns you prior to disabling encryption.
2. Default the controller (see Defaulting a Controller).

Telnet

To confirm a network path exists from the server to the controller and the correct ports are open, you can telnet to the controller on the download port (by default port 21000).

1. If the Telnet feature is not turned on, open the **Control Panel > All Control Panel Items > Programs and Features**.
2. Click **Turn Windows features on or off**. Locate the **Telnet Client**, check the box next to it and click **OK**.
3. Open a command prompt and attempt to telnet to the controller.
   For example, enter the command `telnet 192.168.1.2 21000`
   - If the controller can accept the connection, a clear screen appears with a cursor blinking in the top left corner.
   - If there is no connection, a message will advise there is still a problem between the server and controller. If you can web browse to the controller, it is likely a firewall is blocking the connection somewhere.

Finally, to confirm the event server is able to accept connections, configure a laptop with the same IP settings as the controller.

1. Remove the ethernet plug from the controller and plug into your laptop.
2. Try to telnet to the server IP address on the event server port (22000 by default):
   `telnet 192.168.1.100 22000`
   - If the server is able to accept connections, the clear screen and blinking cursor appear.
   - If the server is not reachable, a message will advise there is still a problem, indicating a firewall is blocking port 22000 to the server.

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.