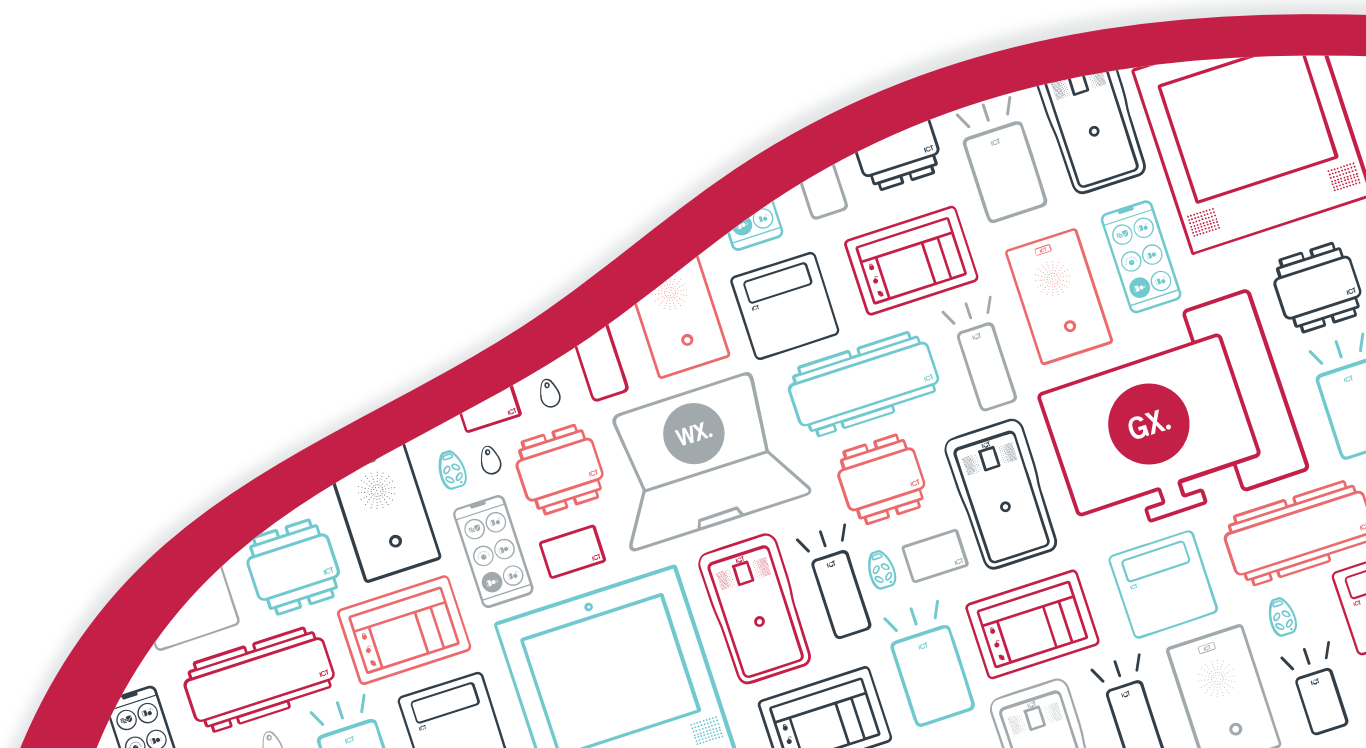
PRT-GX-SRVR

Protege GX System Hardening Guide



Last Published: 06-Dec-24 4:43 PM

Contents

Introduction

Protege GX is a complex and powerful system which is central to the functioning of the facilities where it is installed. It provides centralized control over building security and automation, and often contains a large amount of personal user data. All of this can make the Protege GX system a valuable target for malicious parties, such as external hackers or dishonest employees.

To mitigate the risk of a security incident or data breach, ICT strongly recommends that you proactively harden the Protege GX system before an incident occurs. System hardening is a process of identifying and mitigating potential vulnerabilities to reduce the 'attack surface' of the entire system. This should ideally be carried out by the security system installer or network administrator during the initial installation, and reviewed at regular intervals to ensure that best practices are still being met.

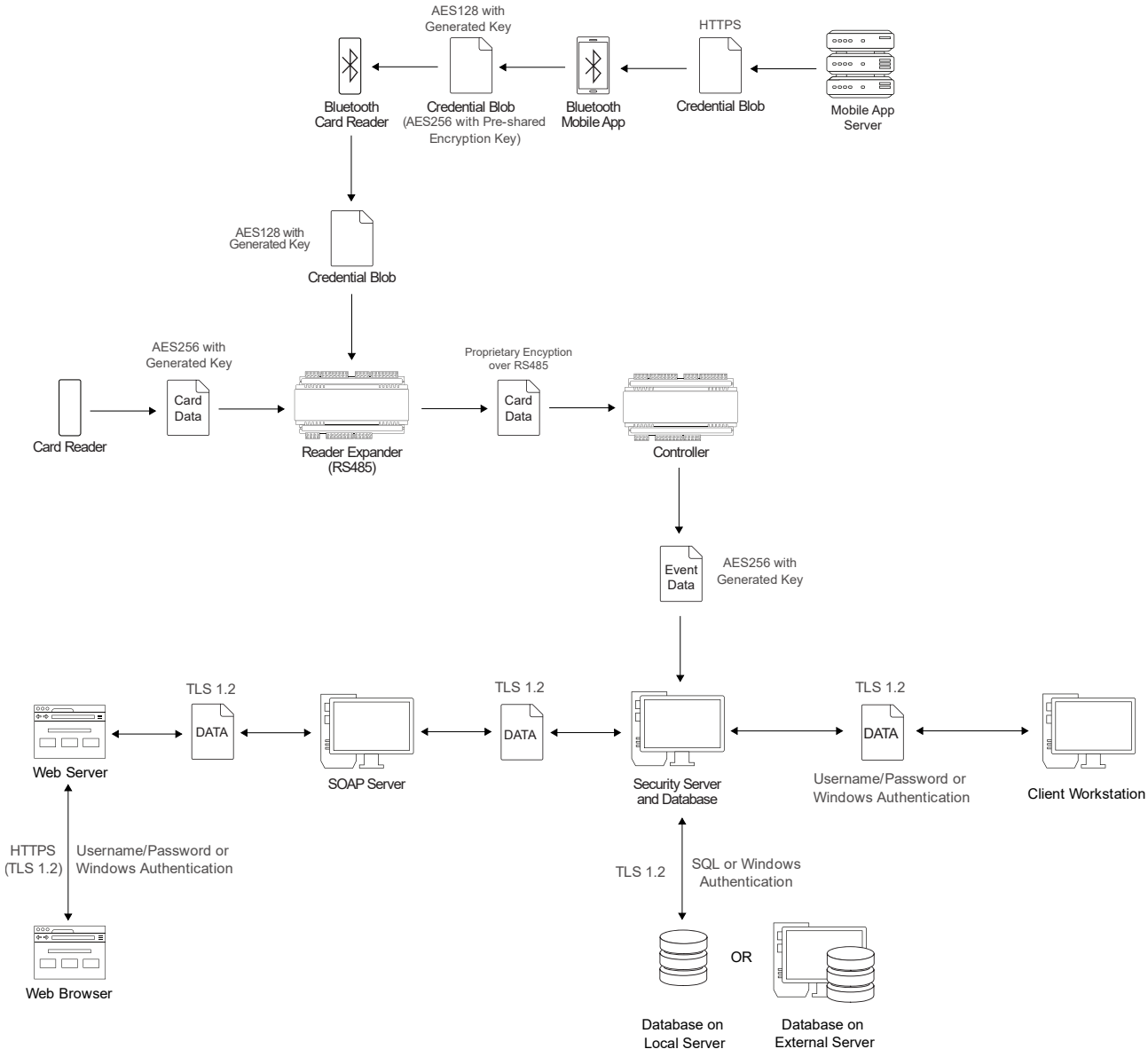
This document is intended to provide a useful reference guide for hardening the Protege GX system. It includes:

- Overviews of the system architecture, including details about the protocols and ports which may be used by the Protege GX server and controller.
- Guidelines and recommendations for improving system security.
- References to other documents (such as installation manuals and application notes) which contain instructions for enabling Protege GX security features.

Additionally, you should ensure that you follow all security recommendations included in the Protege GX and SOAP Service installation manuals.

Secure Architecture

The Protege GX system is secure by design and features end-to-end encryption of data. The diagram below shows how each part of the communication chain is encrypted in a standard installation.



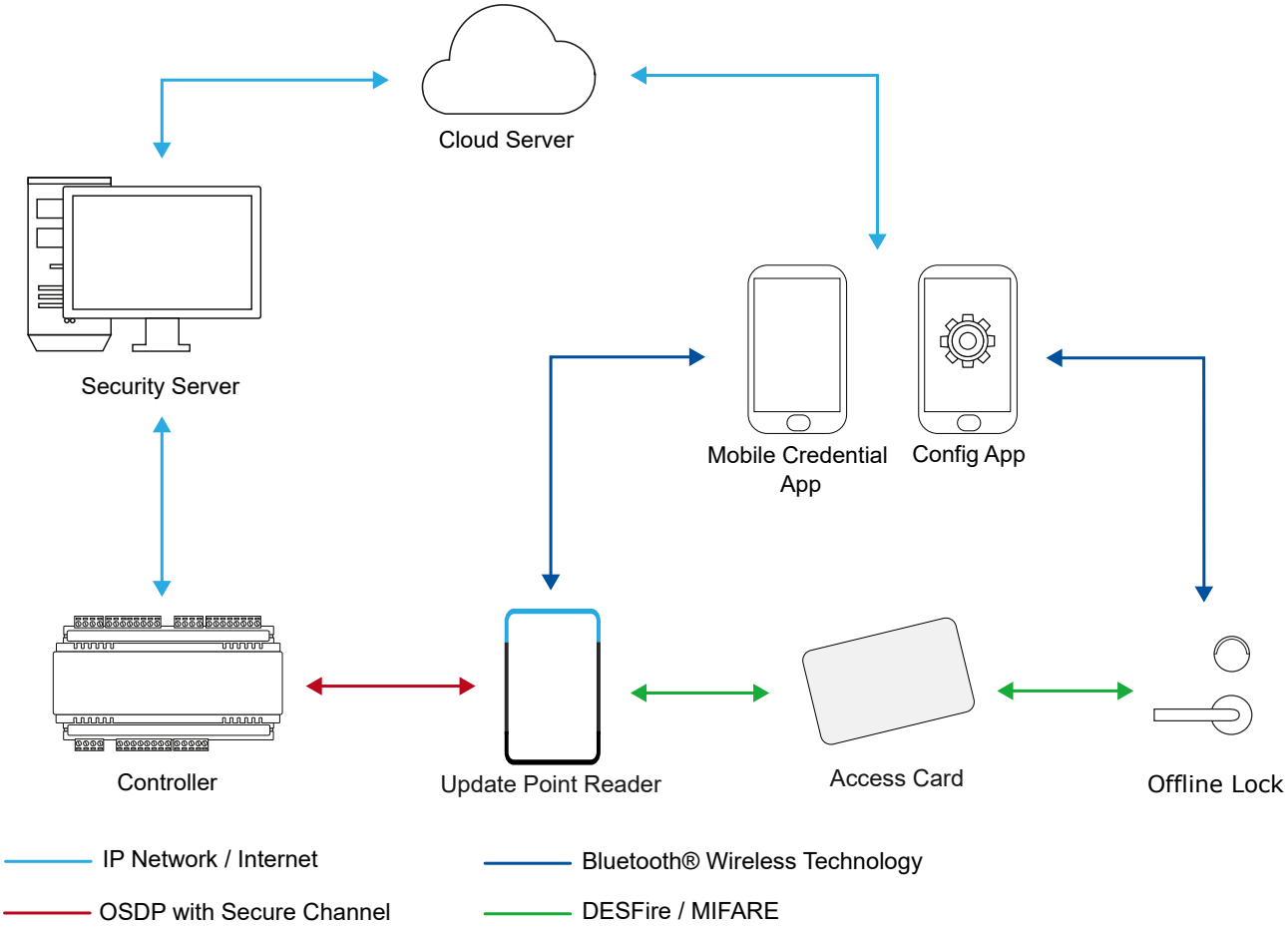
Some encryption features must be enabled separately or are only available in certain configurations. For more information, see Secure Communications (page 23).

Wireless Locks

The ICT wireless locking system is **end-to-end encrypted** with a minimum of 128-bit encryption* at every step in the chain of communication. All encryption keys are uniquely generated for every site and shared between components using industry-standard methods. The wireless lock itself contains a Secure Access Module (SAM), an isolated chip which handles all key storage, encryption and decryption to provide the highest level of security for encryption keys.

* Only applies when using DESFire cards and/or mobile credentials for access. MIFARE Classic cards do not provide the same level of security.

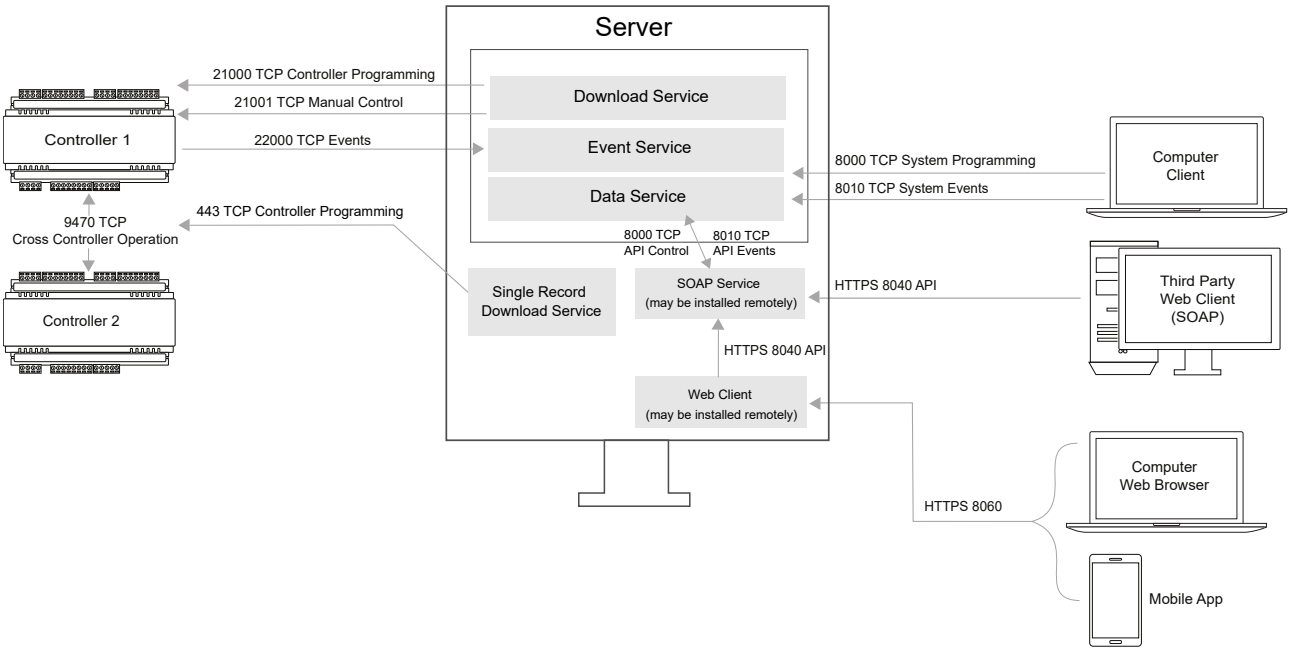
Offline Wireless Lock System Architecture



Server Networking Overview

The Protege GX server communicates with a number of components, including:

- Controllers, either on the same network or over the internet.
- The SQL databases for saving and retrieving configuration and events.
- Local and remote client software.
- Via the Protege GX SOAP service:
  - The Protege GX web client and Protege mobile app.
  - The ICT Data Sync Service.
  - Third-party web clients and other components required for specific integrations.



Server Communications

The communication paths listed below may need to be opened or forwarded in the firewall for Protege GX to function correctly.

Server-Database Communications

From	To	Default Port	Protocol	Description
Data Service	SQL Server	1433	TCP	Store programming in SQL database. Transfer programming to controllers. • Port is configurable by editing the config file for the service. See the Protege GX Server Installation Manual.
Data Service	SQL Server	1434	UDP	On a server behind a firewall you must enable port 1434 for SQL Server to listen on.

From	To	Default Port	Protocol	Description
Event Service	SQL Server	1433	TCP	Store system events and status updates in SQL database. • Port is configurable by editing the config file for the service. See the Protege GX Server Installation Manual.
Event Service	SQL Server	1434	UDP	On a server behind a firewall you must enable port 1434 for SQL Server to listen on.
Download Service	SQL Server	1433	TCP	Store programming in SQL database. Transfer programming to controllers. • Port is configurable by editing the config file for the service. See the Protege GX Server Installation Manual.
Download Service	SQL Server	1434	UDP	On a server behind a firewall you must enable port 1434 for SQL Server to listen on.
Single Record Download Service	SQL Server	1433	TCP	Store programming in SQL database. Transfer programming to controllers. • Port is configurable by editing the config file for the service. See the Protege GX Server Installation Manual.
Single Record Download Service	SQL Server	1434	UDP	On a server behind a firewall you must enable port 1434 for SQL Server to listen on.

Server-Client Communications

From	To	Default Port	Protocol	Description
Client	Data Service	8000	TCP	Communications between client and server for logging in to, programming and controlling the system. • Port is configurable during installation of Protege GX.
Client	Data Service	8010	TCP	Communications between client and server for retrieving report data. • Port is configurable during installation of Protege GX.

Server-Controller Communications

From	To	Default Port	Protocol	Description
Download Service	Controller	21000	TCP	Download system programming to controllers. • Port is configurable in the software and controller settings.

From	To	Default Port	Protocol	Description
Download Service	Controller	21001	TCP	Download manual control commands to controllers. • Port is configurable in the software and controller settings.
Controller	Event Service	22000	TCP	Send system events and status to the event server. • Port is configurable in the software and controller settings.
Single Record Download Service	Controller	443	TCP	Download system programming to controllers. • Port is configurable in the software and controller settings. • When connecting to an older controller, port 80 is used temporarily to upgrade the controller from HTTP to HTTPS.

SOAP and Web Client Communications

From	To	Default Port	Protocol	Description
SOAP Service	Data Service	8000	TCP	Communications between SOAP service and server for logging in to, programming and controlling the system. • Port is configurable during installation of Protege GX.
SOAP Service	Data Service	8010	TCP	Communications between SOAP service and server for retrieving report data. • Port is configurable during installation of Protege GX.
Web Client	SOAP Service	8030	HTTP TCP	Web interface for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the SOAP service.
Third-Party Web Client (SOAP)	SOAP Service	8030	HTTP SOAP	Custom application for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the SOAP service.
ICT Data Sync Service	SOAP Service	8030	HTTP SOAP	Application for synchronizing the Protege GX system with external data. • Port is configurable during installation of the SOAP service.
Web Client	SOAP Service	8040	HTTPS TCP	Web interface for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the SOAP service.

From	To	Default Port	Protocol	Description
Third-Party Web Client (SOAP)	SOAP Service	8040	HTTPS SOAP	Custom application for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the SOAP service.
ICT Data Sync Service	SOAP Service	8040	HTTPS SOAP	Application for synchronizing the Protege GX system with external data. • Port is configurable during installation of the SOAP service.
Web Browser	Web Client	8050	HTTP TCP	Web interface for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the web client.
Mobile App	Web Client	8050	HTTP TCP	Mobile app for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the web client.
Web Browser	Web Client	8060	HTTPS TCP	Web interface for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the web client.
Mobile App	Web Client	8060	HTTPS TCP	Mobile app for viewing, controlling and programming Protege GX systems. • Port is configurable during installation of the web client.

Integration Communications

From	To	Default Port	Protocol	Description
Data Service	DVR Service B	8020	TCP	Manage video integrations. • Port is configurable by editing the config files for the services. • DVR Service B can be turned off if video integrations are not in use.

Each integration has its own specific architecture and requirements. For more information, see the relevant application note. Ports and protocols used for integrations are disabled by default.

Miscellaneous

From	To	Default Port	Protocol	Description
Data Service	SMTP Mail Server	25	SMTP	Send emails from the Protege GX server. • Port is configurable in the software.

From	To	Default Port	Protocol	Description
Client	SIP Server	5060	UDP	Connect to a PBX SIP server to make and receive calls. • Port is configurable in the software.

Controller Networking Overview

Physical Network Connections

Protege controllers incorporate two main networking technologies - ethernet and RS-485 - and several supplementary technologies. Below is a summary of the externally available network ports on Protege controllers.

Physical Network Connection	Notes
RJ45 ethernet port	• Single 10/100 base T ethernet connection. • Available on all controller variants. • PoE available on some variants.
USB	• Single USB port capable of supporting a single secondary physically connected ethernet adaptor. • Capable of supporting an external 4G cellular modem providing wireless ethernet connectivity.
3G cellular modem	• Internal 3G cellular modem providing wireless ethernet connectivity. • Factory option, not available on all models.
RS-485 port 1	• RS-485 network dedicated to communicating with ICT module hardware using a proprietary protocol.
RS-485 port 2	• RS-485 network dedicated to communicating with ICT card reader hardware using a proprietary protocol. • Can be configured to communicate with industry standard Wiegand or OSDP card readers. • Can also be configured to communicate with specific third-party hardware using proprietary protocols.
RS-485 port 3	• RS-485 network dedicated to communicating with ICT card reader hardware using a proprietary protocol. • Can be configured to communicate with industry standard Wiegand or OSDP card readers. • Can also be configured to communicate with specific third-party hardware using proprietary protocols.
PSTN modem	• Provided on some models for dial out only. There is no dial in ability provided by the controller. • Use is restricted to sending Contact ID or SIA messages to security monitoring stations. • Not available on all models.

Ethernet Connectivity

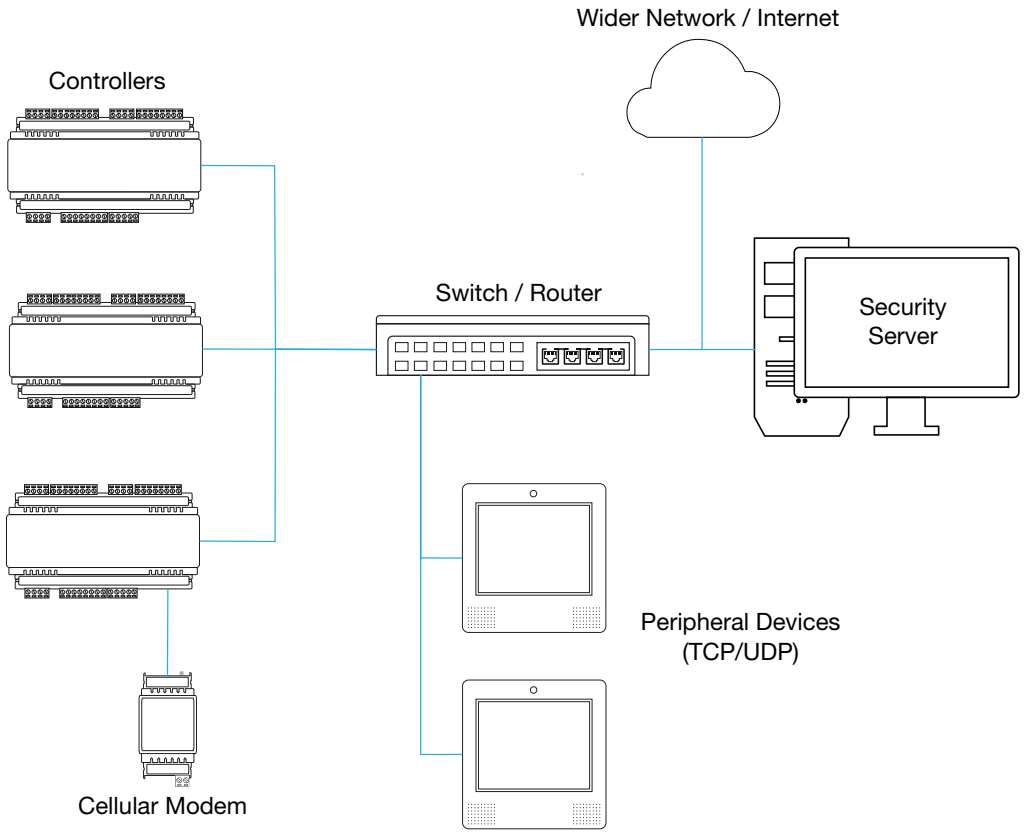
Protege controllers use ethernet to communicate with a server for system configuration, with other controllers, and with proprietary user interface hardware.

- Controllers incorporate the Embedded Compact 7 variant of the Microsoft Windows operating system. All ethernet network activity is managed through the operating system's underlying protocol stack.
- The Microsoft Windows firewall is enabled and active on all interfaces.
- All ethernet interfaces have promiscuous mode disabled by default. Promiscuous mode will be enabled only if the onboard RJ45 interface is configured to support the Otis high level elevator protocol.

- Controllers are configured with IPV4 addresses only. Each controller is shipped with the default IP address 192.168.1.2.

Physical Connection

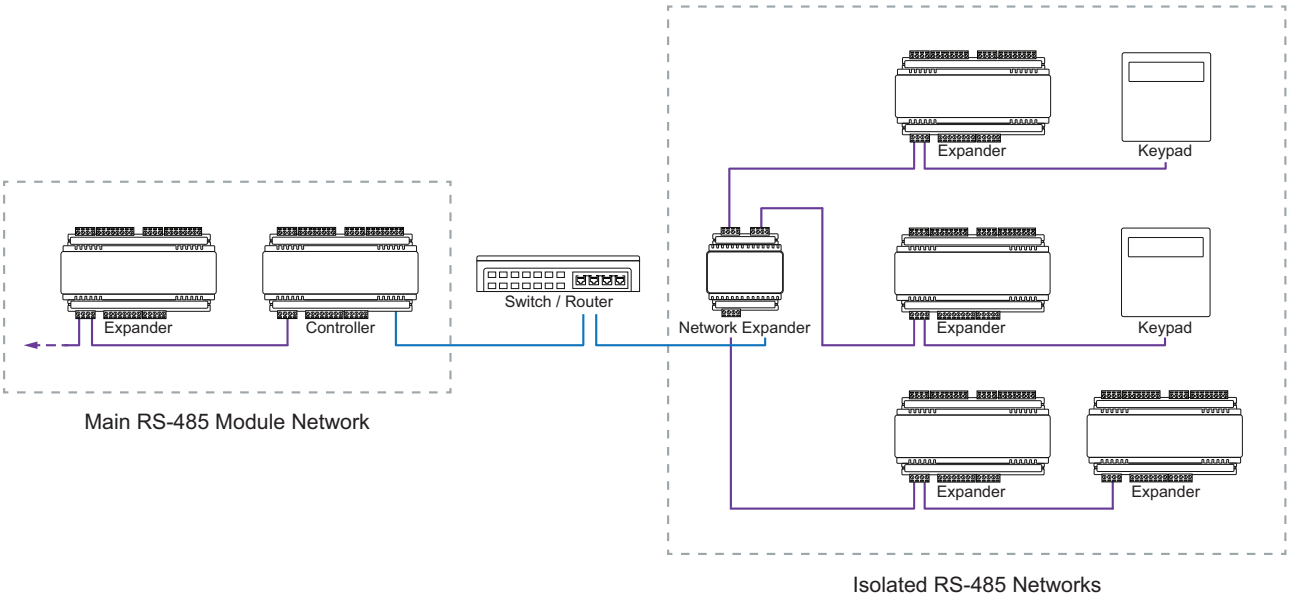
Typically controllers are connected through a network switch to a host server. The network frequently includes peripheral devices such as entry stations. Depending on the network configuration, the controllers may also be exposed to a wider network or the internet.



On a small system the controller may be connected directly to the host PC or server.

Network Expansion

The PRT-MNR2-DIN network repeater module may be used to expand the controller's module network. The network repeater module provides a UDP interface to the controller for connection with a remote RS-485 module network. The network repeater recognizes only a single proprietary protocol for communicating with ICT peripheral modules.



Supported Protocols

The following communication protocols are supported on the controller.

Standard Protocols

Protocol	Default Port	Description / Notes
TCP		
UDP		
ICMP		Ping functionality is disabled by default.
Telnet	23	From firmware version 2.08.1221, Telnet is permanently disabled on the controller. Prior to this version, Telnet is disabled by default. It may be intentionally enabled during non-standard system analysis to provide access to the Windows console and shell.
FTP	21	From firmware version 2.08.1221, FTP is permanently disabled on the controller. Prior to this version, FTP is disabled by default. It may be intentionally enabled during non-standard system analysis to provide access to the underlying file system of the controller.
DNS	53	
DDNS	80/443	Disabled by default. Port depends on the HTTP or HTTPS port.
DHCP	67/68	
NTP	123	

Protocol	Default Port	Description / Notes
HTTP	80	The controller incorporates a built-in web server used for some system configuration. HTTPS is the factory default protocol for this interface. • Port is configurable in the controller web interface
HTTPS	443	Factory default for the built-in web interface using TLS 1.2. Custom third-party or self-signed HTTPS certificates can be installed by the user. • Port is configurable in the controller web interface • The controller's advertized ciphers are: - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521 For more information, see Application Note 314: Configuring HTTPS Connection to the Protege GX Controller.

Protege GX System Protocols

Protocol	Default Port	Description / Notes
ICT download	21000	Proprietary protocol for downloading programming from the host Protege GX server to the controller. • TCP/IP • Port is configurable in the software and controller settings.
ICT event/status	22000	Proprietary protocol for exchange of event and status information from the controller to the Protege GX software. • TCP/IP • Port is configurable in the software and controller settings.
ICT control	21001	Proprietary protocol for downloading manual control commands from the host Protege GX server to the controller. • TCP/IP • Port is configurable in the software and controller settings.
ICT single record download	443	Uses HTTPS to download programming from the host Protege GX server to the controller. • TCP/IP • Port is configurable in the software and controller settings.
Cross controller communication	9470	Proprietary protocol for exchange of system state information between controllers. • TCP • Port is configurable via controller command • AES256 encrypted
TCP module communication	9450	Proprietary protocol for exchange of system information between a controller and ICT peripheral input/output device. • Disabled by default • TCP • Port is configurable in the software
UDP module communication	9450	Proprietary protocol for exchange of system information between a controller and ICT peripheral input/output device. • Disabled by default • UDP • Port is configurable in the software
UDP touchscreen communication	9460	Proprietary protocol for exchange of system information between a controller and ICT touchscreen peripheral device. • Disabled by default • UDP • Port is configurable in the software

Protocol	Default Port	Description / Notes
Automation and control	-	Proprietary protocol for exchange of system information and control commands between controllers and custom third-party applications. • Disabled by default • TCP • Port is configurable in the software
Link Me	-	Proprietary protocol for exchange of system information between controllers. • Disabled by default • UDP • Port is configurable in the software

Reporting Protocols

Protocol	Default Port	Description / Notes
Armor IP	-	Proprietary protocol for sending messages from the controller to security monitoring stations. • Disabled by default • TCP or UDP • Port is configurable in the software • Optional AES encryption • Only used for outbound connections, does not listen for connections
SIA	-	Industry standard protocol for sending messages from the controller to security monitoring stations. Uses the SIA DC-09 specification for digital communication. • Disabled by default • TCP • Port is configurable in the software
Contact ID	-	Industry standard protocol for sending message from the controller to security monitoring stations. Uses the SIA DC-09 specification for digital communication. • Disabled by default • TCP • Port is configurable in the software
Patriot LS30	-	Proprietary third-party protocol for sending message from the controller to security monitoring stations. • Disabled by default • TCP • Port is configurable in the software
CSV-IP	-	Proprietary third-party protocol for sending message from the controller to security monitoring stations. • Disabled by default • TCP • Port is configurable in the software

Integration Protocols

Each integration has its own specific architecture and requirements. For more information, see the relevant application note.

Protocol	Default Port	Description / Notes
BACnet	4708	Industry standard BACnet protocol. • Disabled by default • UDP
VizIP	-	Proprietary third-party protocol for communicating with DVR equipment. • Disabled by default • UDP • Port is configurable in the software
Serial printer	-	Proprietary third-party protocol for sending system information to a dumb terminal or printer. • Disabled by default • TCP • Port is configurable in the software
Modbus	-	Industry standard protocol for communication with automation modules. • Disabled by default • TCP • Port is configurable in the software
C-Bus	-	Proprietary third-party protocol for communication with automation modules. • Disabled by default • TCP • Port is configurable in the software
Intercom	-	Proprietary third-party protocol for communication with intercom modules. • Disabled by default • UDP • Port is configurable in the software
Fanvil intercom	-	Proprietary third-party protocol for communication with intercom modules. • Disabled by default • TCP • Port is configurable in the software
KONE elevator HLI	-	Proprietary third-party protocol for communication with an elevator control system. • Disabled by default • TCP • Port is configurable in the software

Protocol	Default Port	Description / Notes
ThyssenKrupp elevator HLI	-	Proprietary third-party protocol for communication with an elevator control system. • Disabled by default • TCP • Port is configurable in the software
Otis elevator HLI	-	Proprietary third-party protocol for communication with an elevator control system. • Disabled by default • TCP • Port is configurable in the software
Schindler elevator HLI	-	Proprietary third-party protocol for communication with an elevator control system. • Disabled by default • TCP • Port is configurable in the software
MCE elevator HLI	-	Proprietary third-party protocol for communication with an elevator control system. • Disabled by default • TCP • Port is configurable in the software
Aperio	-	Proprietary third-party protocol for communication with wireless locking devices. • Disabled by default • TCP • Port is configurable in the software
Salto SALLIS	-	Proprietary third-party protocol for communication with wireless locking devices. • Disabled by default • TCP • Port is configurable in the software
ASSA ABLOY DSR	-	Proprietary third-party protocol for communication with a wireless locking server. • Disabled by default • TCP • Port is configurable in the software
Vingcard	-	Proprietary third-party protocol for communication with a wireless locking server. • Disabled by default • TCP • Port is configurable in the software

Protocol	Default Port	Description / Notes
Third-party generic	-	Generic interface for receiving credential data in standard formats, e.g. numeric, ASCII, UTF8. • Disabled by default • TCP • Port is configurable in the software • Multiple ports can be opened

Unused UDP Ports

When you port scan the controller, UDP ports 500 and 4500 appear to be Open/Filtered. However, these ports are not used and the controller will not respond to requests over these ports.

This is a feature of the Windows operating system that cannot be deactivated. These open ports do not pose a cybersecurity risk.

Security Guidelines

This section provides recommendations for hardening your Protege GX system against attack.

These are general guidelines only, and cannot account for every security requirement in your installation. When planning the system, ensure that you consider company policy and any relevant legislation in your country. Guidelines issued by your country's cybersecurity or privacy authorities can be a useful resource to supplement this document.

In addition, Protege GX integrates with a wide range of third-party systems, which may not all be compatible with security best practices. Make sure you take into account the security profile of any integrations you may be using, and follow any guidelines provided by third-party manufacturers.

For additional guidance on managing privacy requirements, see Application Note 258: Protege GX Compliance with GDPR.

Software and Firmware Updates

New cybersecurity vulnerabilities and threats arise frequently. It is recommended that you keep all software up-to-date to gain the protection of the latest security patches and features.

- The following Protege GX components should all be kept up to date:
  - Protege GX server/client software
  - Controller firmware
  - SOAP service, web client and data sync software

  Instructions for updating software and firmware versions are included in the release notes for each new version.
- Always apply Windows security updates to your server and client machines.

Network Configuration

There are a number of good security practices that can harden the ethernet network against attack.

- Use a dedicated, segmented network for the security system, with firewalls preventing access from other networks.
- Do not connect the Protege GX server and controllers to other networks.
- If it is necessary to connect to the security network remotely, use secure methods such as VPNs.
- When configuring firewall and port forwarding settings, only open the ports which are required for the system to function. For example, to enable communications between server and controllers, you only need to open the download, control and event ports.
- Do not expose devices to the internet unless necessary, as this increases the possibility of attack.
- If devices must be exposed to the internet or other networks, implement protections on the network to mitigate common attack types. For example, use rate limiting to prevent denial of service (DOS) attacks.

Systems Configuration

There are a number of steps you can take to prevent or mitigate attacks against server and client machines. In addition, if an incident does occur it is vital to have comprehensive logs of system activity.

- Do not install any software or services on the Protege GX server machine except for the minimum required.
- Install an approved antivirus solution on the server and client machines to ensure that they are not vulnerable to malware.

- Use a strong password or pass phrase for access to the server (both for the OS and SQL server). Use two-factor authentication where possible. Restrict who has access to the server.
- Run the Protege GX services under a dedicated domain account. The minimum required permissions for SQL server are documented in the Protege GX Server Installation Manual.

  Using a restricted account for the services may lead to some configuration difficulties in setting up Windows Authentication for Protege GX operators. Consult your IT professional for assistance.
- Set the server and client computers to automatically lock their screens after 15 minutes of inactivity or less.
- Disable autoplay on the server so that USB devices cannot automatically run software when they are plugged in.
- Make sure that event logging is enabled on both the server and the Protege GX application. Logs should be stored securely and reviewed at regular intervals.
- Ensure that all computer clocks in the system are synchronized to a network time server. If clocks in the system are desynchronized it can be very difficult to locate and compare event logs from the time of the incident.

  Controllers can be synchronized to an SNTP time server in the **Sites | Controllers | Time update** tab.
- Encrypt the programming and event databases using Transparent Data Encryption (TDE). This protects the data even if attackers gain access to backup files or physical media. For more information, see the Protege GX Server Installation Manual.
- You can encrypt user PIN codes and prevent operators from viewing them by enabling **Encrypt user PINs** in **Global | Global settings | General**. For more information, see Application Note 306: User PIN Encryption and Advanced PIN Management in Protege GX.

Physical Security

Good physical security is required to prevent malicious parties from gaining physical access to the Protege GX server machine. It is also important to protect the server from physical damage and ensure that it can be restored quickly if damaged or destroyed.

- Make sure that the server machine is physically secure so that unauthorized parties cannot gain physical access. The door to the server room should use strict access control.
- Encrypt the server's hard drive using the Windows BitLocker feature. This further protects the data on the device even if it is stolen or accessed physically. For more information, see the Windows documentation.
- The server should be stored in a climate-controlled room to prevent environmental damage.
- Take regular backups of both the server machine and the Protege GX databases. Store these backups in a secure, off-site location so that they are available if the server is damaged, stolen or destroyed.
- Do not connect portable devices such as laptops or USB drives to the security network without scanning and sanitizing them beforehand.

Secure Communications

As shown in the Secure Architecture diagram (see page 5), Protege GX features end-to-end encryption. However, some parts of the Protege GX system require specific configuration to enable secure, encrypted communications.

The table below outlines what actions must be taken to ensure that each part of the installation is secure.

Communication	Encryption	Recommendation
Between server and thick client / SOAP / database	TLS 1.2	Enable TLS 1.2 on the Protege GX server. If you are logging in to the Protege GX server from a remote client workstation (outside the firewall), install an SSL certificate signed by a trusted certificate authority on the Protege GX server. Enable service certificate validation to prevent man-in-the-middle attacks. For instructions, see Application Note 277: Configuring Protege GX to use TLS 1.2.
Between server and controller	Proprietary 256 bit AES with generated key	Enable encryption for each controller by clicking **Initialize controller encryption** in **Sites | Controllers | Configuration**. **Note**: Once controller encryption has been enabled, it cannot be disabled without physically defaulting the controller.
Between server and SMTP email server	TLS 1.2	Check the **Use SSL** option in **Global | Global Settings | Email settings** to enable TLS 1.2 encryption (as long as both the host OS and SMTP server support TLS 1.2). In addition, you must change the default mail port (25) to a TLS-enabled port. This can differ between mail servers, but is commonly 587 or 2525.
Server	-	Disable insecure cipher suites and protocols on the Protege GX server. We recommend using the **PCI 3.2** setting in IIS Crypto by Nartac Software. For more information, see the Protege GX Server Installation Manual.
Between controller and web browser	HTTPS	Current Protege GX controllers have a self-signed HTTPS certificate pre-installed at the factory. This is sufficient to provide an encrypted connection. However, it is recommended to install a custom certificate signed by a trusted certificate authority. Controllers manufactured before April 2021 do not have a factory certificate. It is strongly recommended to install an HTTPS certificate. For instructions, see Application Note 314: HTTPS Connection to the Protege GX Controller.
Between controller / reader expander and card readers	OSDP Secure Channel	For best security, use card readers in OSDP mode with secure channel communication enabled. This provides AES 128-bit encryption with uniquely generated encryption keys. For more information, see Application Note 254: Configuring OSDP Readers. ICT RS-485 is ICT's proprietary connection method. This method uses a fixed AES 256-bit encryption key, and so is not as secure as OSDP secure channel. Wiegand reader connection does not provide encryption between the card reader and reader port.

Communication	Encryption	Recommendation
Between card and card reader	-	Use MIFARE DESFire card technology for bi-directional, encrypted communications and resistance to cloning. Do not use cards which are unencrypted or easy to clone (e.g. 125kHz, MIFARE Classic). Standard cards and card readers provided by ICT use default encryption keys which are publicly available. We recommend using custom encryption keys that are unique to the site. For more information, see Application Note 352: Setting Up Custom Credential Encryption.
Between SOAP service and web client	HTTPS	A self-signed SSL certificate is generated during installation of the SOAP service. To improve security, install an SSL certificate signed by a trusted certificate authority on the ProtegeGX site in IIS. Disable insecure cipher suites and protocols on the SOAP server. We recommend using the **PCI 3.2** setting in IIS Crypto by Nartac Software. For instructions, see the Protege GX SOAP Service Installation Manual.
Between SOAP service and data sync service	HTTPS	As above, ensure that a trusted SSL certificate is installed for the SOAP service, and insecure cipher suites and protocols are disabled. In the data sync service configuration tool, set the **SOAP Server Address** to the HTTPS endpoint of the SOAP service. This requires you to enter the fully qualified domain name of the SOAP server (instead of localhost) and connect over the HTTPS port (port 8040 by default).
Between SOAP service and integrations	HTTPS	As above, ensure that a trusted SSL certificate is installed for the SOAP service, and insecure cipher suites and protocols are disabled. Ensure that any integration connects to the HTTPS endpoint of the SOAP service (port 8040 by default).
Between web client and web browser	HTTPS	Install a trusted SSL certificate for the ProtegeGXWeb site in IIS. Ensure that operators connect to the web client via HTTPS (port 8060 by default). Set the secure flag to ensure that session cookies are sent over HTTPS only. For instructions, see the Protege GX Web Client Installation Manual.
Between web client and mobile app	HTTPS	As above, install a trusted SSL certificate for the web client. Ensure that the mobile app is connected to the web client via HTTPS (port 8060 by default). For instructions, see Application Note 210: Securing the Protege Mobile App.
Wireless locks		Use DESFire cards and/or mobile credentials instead of MIFARE Classic cards to prevent card cloning and achieve minimum 128-bit encryption across the system. All communications are automatically encrypted (see page 5).

Operator Access

Protege GX operators typically have extensive control over the security system and access to sensitive data. Controlling operator access to the Protege GX server and controller can greatly reduce the risk of data breaches and security incidents. Proper access control and reporting also makes it possible to identify who has accessed the system in the case of a security incident.

- **Operator logins**:
  - One operator should be created per person who needs to access the system. This allows you to report accurately on which individuals are logged in to the system and who has edited a particular record.
  - All operators should use strong passwords or pass phrases. Passwords should not be shared with others.
  - Alternatively, it is possible to integrate Protege GX with Windows Active Directory, allowing operators to log in to the client and web client without entering a separate username and password (single sign-on). This reduces the number of passwords that operators need to remember and allows you to easily set a password policy for the whole organization.

    Active Directory integration is a separately licensed feature. For more information, see Application Note 288: Using Active Directory in Protege GX and Application Note 299: Using Windows Authentication with the Protege GX Web Client.
- **Operator auditing**:
  - By default, any time an operator edits a record an event is saved to the Protege GX events database. This allows you to report on any unexpected changes to records and identify which operator made the change. Ensure that **Save operator events to event database** is enabled in **Global | Global Settings**.

    Changes for individual records are saved in the **History** tab for that record.
  - Enable the **Save failed operator login events to event database** option. This allows you to detect and report on unexpected failed login attempts.
- **Operator access to records**:
  - Ideally, each operator should only be able to view, edit and control the records which are required for their job, and should have restricted access to all other records. Roles and security levels allow you to control what operators can see and do in the Protege GX interface:
    - Restrict access based on sites or record groups.
    - Select which menus the operator has read/write, read only or no access to.
    - Set which devices the operator can control.
  - Prevent operators from viewing user PIN codes by disabling the **Show PIN numbers for users** option in **Global | Operators**. This is not required when PIN codes are encrypted in the database (see page 21).
  - In addition, each SOAP integration which accesses the system should use a unique operator with only the permissions that are required. SOAP operators use the same permissions as normal Protege GX operators.

For more information about programming roles and security levels, see Application Note 191: Programming Operator Roles in Protege GX.

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.

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