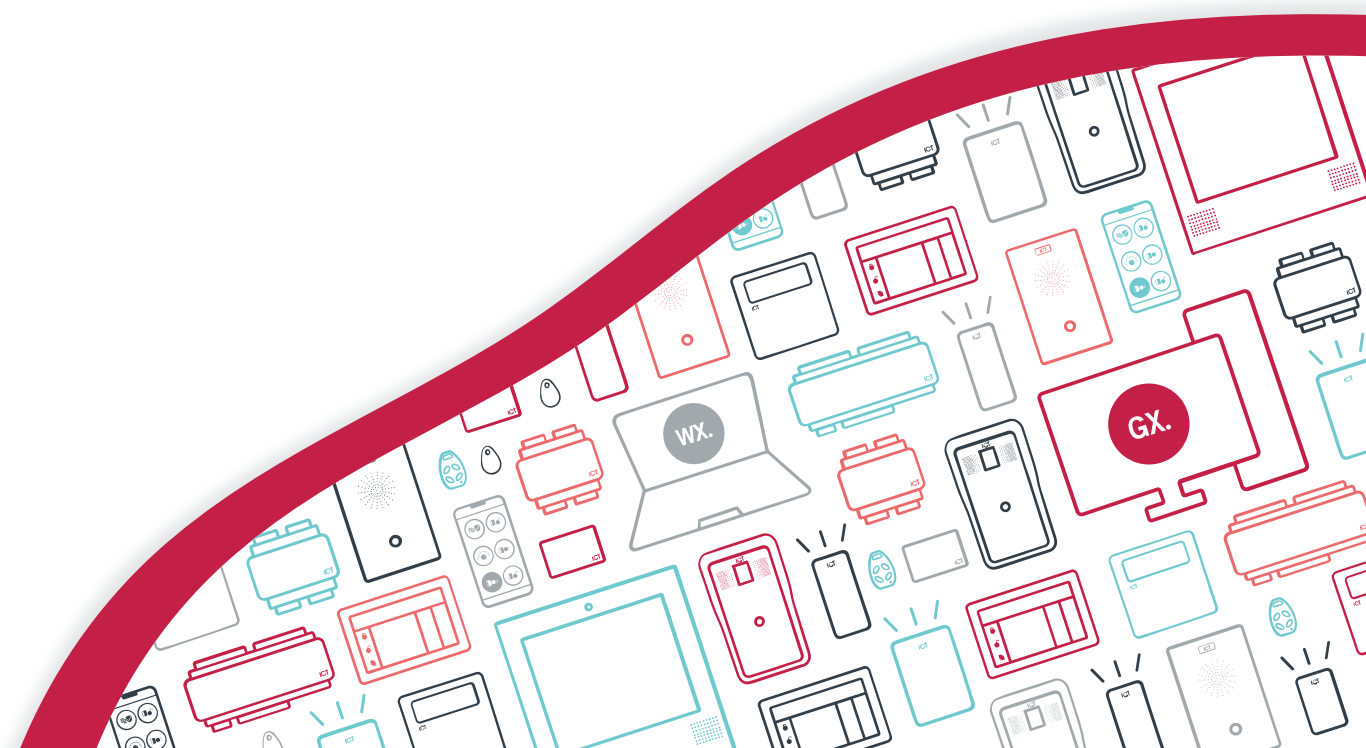
Integrated Control Technology

Protege GX Controller Firmware

Release Notes | Version 2.08.1411



Last Published: 14-Nov-23 8:42 AM

Contents

Introduction

This document provides information on the new features, enhancements and resolved issues released with:

- Protege GX controller firmware version 2.08.1411

A full release history for previous versions is also included.

This version includes important cybersecurity changes to the controller's operation. If your site uses the single record download service, you **must** upgrade this service alongside the controller firmware (see page 7).

Supported Hardware

This firmware is supported in the following Protege GX controller modules:

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

Older Controller Limitation

Due to physical technology limitations, older controller hardware is currently not capable of loading the latest firmware versions.

Controller models without physical USB ports may not support newer firmware files. If your controller does not have a USB port, **do not** attempt to upgrade it to the current version without confirming compatibility.

In particular, controllers manufactured prior to **December 2015** use an older operating system which is not compatible with firmware versions higher than **2.08.1002**. There are two methods for checking your controller's manufacture date:

- The warranty sticker on the back of the controller shows the month and year of manufacture.
- Contact ICT support with a list of controller serial numbers to check.

It may be possible to upgrade the operating system of the controller and allow use of the latest firmware versions. Contact ICT support for more information.

Upgrading Firmware

Upgrading controller firmware can be carried out from the Protege GX user interface. It is also possible to upgrade the firmware of individual controllers from the **Application Software** section of the controller web interface.

PCB and DIN controllers run completely different firmware. **Deploying incorrect firmware to a controller will result in total failure.** This can be corrected, however the process to do so is time consuming. Please ensure you download and install the correct firmware for your device.

Upgrading Firmware from the Protege GX User Interface

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. Open and log in to the Protege GX application and ensure that you have a connection to the controller that you wish to upgrade.
2. From the main menu, select **Sites | Controllers**.
3. Right click on a controller and select **Update firmware**.
4. Click the **[...]** button and browse to the supplied firmware (.bin) file.
5. Choose which controller(s) to update by selecting the **Include** option. Only the selected controller(s) will be updated.
6. Click **Update** to commence the firmware upgrade procedure.
   The upgrade can take up to 10 minutes per controller to complete. Once complete, the controller is automatically restarted.
7. On completion of a firmware upgrade a download is required to update controller programming. Right click on the controller record and select **Force download**.

Protege GX Controller Firmware 2.08.1411

Cybersecurity Enhancements (2.08.1411)

This firmware release includes extensive cybersecurity enhancements to the controller, protecting against a range of cyberattacks.

- Protects against clickjacking, where attackers can attempt to steal your operator credentials.
- Protects against session hijacking, where attackers spoof the ID of the operator who is currently logged in.
- Protects against man-in-the-middle attacks, where attackers can intercept and view traffic between you and the controller over the HTTPS connection.
- Addresses vulnerabilities in the web interface by upgrading all web components.
- Improves the selection of cryptographic protocols that are used to communicate with the web browser, following NIST recommendations.

Important Notes

- If your site uses the Protege GX Single Record Download Service, you must also upgrade it to **version 1.0.1.1 or higher**. Earlier versions are not compatible with this controller firmware release.
- Although some protection is offered by the new firmware version, for full protection you also need to **upgrade the controller's operating system to version 2.0.32 or higher**. Contact ICT Technical Support for more information about this process.

  The OS upgrade is only required for sites that need the cybersecurity enhancements listed above. The other updates described in these release notes do not require an OS upgrade.

- If you upgrade the controller's firmware and operating system and later wish to downgrade, you may need to clear the site data for the controller's web interface.

Feature Enhancements (2.08.1411)

The following enhancements have been made to existing features in this release.

Access Events

- Added new events that are used when a user attempts to gain access at a door or elevator car, but does not have any access levels which allow access to that record. The events are:
  - User John Doe Door Not Allowed Office Door Using any Access Level
  - User John Doe Access Level Schedule Not Valid Office Door Using any Access Level
  - User John Doe Denied by Elevator Group at South Elevator Using any Access Level

  This feature requires Protege GX software version 4.3.344.12 or higher.

Credential Types

- Added the ability to descramble card data using a custom Wiegand format programmed in the credential type. This makes it easier to transition sites using legacy card formats to new card readers.

  Contact ICT Technical Support for assistance with this feature.

Otis Compass Integration

- Added the ability to define up to four reader formats for Otis Compass integrations.

  For more information and programming instructions, see Application Note 174: Protege GX Otis Compass HLI Integration.

Schindler Integration

- Added the ability to use ICT card readers to travel directly to a home floor instead of selecting a floor.

  Some additional configuration is required to enable this feature. For instructions, see Application Note 196: Protege GX Schindler HLI Integration.

Allegion Integration

- Added apartment mode functionality for Allegion LE series locks. This allows users to toggle the door lock using their card, the inside push button or the deadbolt. When the user exits using the inside handle, the door is latch unlocked.

  For more information, see Application Note 182: Allegion Integration with Protege GX.

Issues Resolved (2.08.1411)

The following issues were resolved with this release.

- Resolved an issue where duplex inputs did not work on one-door controllers.
- Resolved an issue with the Allegion integration where using the mechanical REX often resulted in an unexpected door forced alarm. The controller now has a four second grace period before activating the forced door alarm for Allegion locks to prevent false alarms.

  You can override this delay by entering the **`DoorForcedStateDelay = #`** command in the door programming, where **#** is the number of seconds to delay to door forced alarm for.

- Resolved an issue where toggling a timed output off before the end of its activation period would cause it to display an 'Error' status.
- Resolved an issue where the Automation and Control Service took longer to log out than expected.
- Resolved an issue where temporary bypasses on inputs were not removed when the area was disarmed.
- Resolved an issue where bypasses were sometimes removed from inputs when an unrelated area was disarmed.
- Resolved an issue where some device and function states were not restored correctly when the controller was power cycled or the firmware was upgraded.
- Resolved an issue where the **Schedule operates late to open** feature could override lockdowns.
- Function codes for unlocking doors now follow the same lockdown rules as card badges.
- Resolved an issue where an entry delay input was only reported to the monitoring station once, even if it was restored and opened again after the alarm had been activated.
- Resolved an issue where the **Preceding characters** setting in credential types was not working correctly. Preceding and trailing characters can now be used for all formats except for Wiegand.
- Resolved a cybersecurity issue where sending specific packets to the TCP manual control port could cause the controller to reboot or stop responding.
- Resolved an issue with the Schindler HLI integration where fixed bits were not applied to pure Wiegand custom credential types.

  Existing sites which have a workaround for this issue will not be affected by the firmware upgrade. If you wish to remove the workaround, contact ICT Technical Support for assistance.

- Resolved an issue where some Polish special characters were not displayed correctly in events and health status.
- Resolved an issue where some buttons could not be clicked on the corners.
- Resolved an issue with sequential output activation where bookings with earlier end times could override bookings with later end times that had already been activated.
- Resolved an issue where **Relock on door close** did not work when the door was unlocked with an extended access time.

- Resolved an issue where programmable functions did not arm/disarm an area group immediately when the output changed state.
- Resolved an issue where reader expanders with OSDP readers connected would generate unnecessary 'Module update required' messages in the health status.

Known Issues (2.08.1411)

ICT would like to make you aware of the following known issues in this version:

- ASCII credentials such as license plates received over the controller's ethernet connection are not processed correctly. This issue was discovered in version 2.08.1360.

Previous Release History

Protege GX Controller Firmware 2.08.1360

New Features (2.08.1360)

The following new features have been included with this release.

OSDP 2.2 Support

The controller and connected reader expanders are now compliant with OSDP 2.2.

- Protege modules now support OSDP installation mode, allowing them to establish a secure channel session with readers using a randomly generated encryption key. After putting the card reader into installation mode, simply right click on the reader expander record and select **Activate OSDP install mode**. This prompts the module to initiate an OSDP session with the card reader, in which it will negotiate an encryption key for a secure session.
- Alternatively, it is possible to manage custom encryption keys manually if preferred. One unique encryption key can be programmed per reader, and the key will be diversified by the controller to establish a secure session with the card reader.
- Protege modules now support encryption key rotation, whereby a new key is negotiated between the devices within the existing secure session. A new session is then established using the new key.
- Protege modules will now automatically detect the baud rate of an OSDP reader, so this no longer needs to be configured in the programming. The module will alternately send polling messages at the supported baud rates of 9600 baud, 19200 baud, and 38400 baud until it receives a response from a reader on one of these baud rates. Once a reader comes online the module will stop cycling through baud rates and communicate on the same baud rate as the reader.
- A number of issues and inconsistencies in the previous iteration of OSDP support have been resolved.

For complete prerequisites and programming instructions, see Application Note 254: Configuring OSDP Readers in Protege. If you have previously programmed OSDP readers using commands, it is recommended that you remove these commands and replace them with the new programming available in the UI.

Modbus Client Integration

In addition to the existing Modbus server integration the Protege GX controller can now act as a Modbus client . This can be used to monitor and control analog registers, coils and digital inputs from connected server devices such as temperature sensors and lighting controls.

For more information and programming instructions, see Application Note 353: Protege GX Modbus Client Integration.

Feature Enhancements (2.08.1360)

The following enhancements have been made to existing features in this release.

Offsite Reporting

- It is now possible to delay reporting of alarms which occur during an area's entry delay. This helps to minimize false alarm reporting and is a required component of BS 8243 compliance.

  To enable this feature, enter the command **`RemoteNotifyDelay = #`** in the area programming, where **#** is the number of seconds to delay the reporting for.

  For more information and programming instructions, see Application Note 312: Minimizing Offsite Reporting of False Alarms in Protege GX and Protege WX.

- Added reporting codes for Burglary Verified alarms in SIA (BV) and Intrusion Verifier alarms in Contact ID (139). These require both the remote notify delay and smart input features to be enabled.
- Added the option to append extended data to SIA reports over IP using the DC09 protocol. This enables you to add the names of the relevant input, area and/or user to every report.
- Added further custom event codes for input types, which can be used to override the default event codes for input and trouble input alarms in SIA DC09 reporting.

  For more information, see Application Note 317: SIA L2 Reporting in Protege GX and Protege WX.

Module Support

- This controller version supports Protege cellular modems manufactured after 1st October 2022. The new modem firmware will not function with previous controller firmware versions.

Aperio Integration

- Added the ability to read Aperio cards with a reverse byte order. To enable this setting, enter the following command in the smart reader programming for each Aperio lock:

  `ReverseByteOrder=True`

Cellular DDNS

- Added the ability to configure the controller's hostname and DDNS settings for the USB ethernet adaptor. This allows you to use a hostname instead of an IP address with the Protege DIN Rail Cellular Modem.

PoE Controllers

- Added the ability to disable a PoE (power over ethernet) controller's regular battery test. This can prevent some issues with smart power supplies.

  To disable the battery test, add the following command in the controller programming:

  `DisableBattTest = true`

Issues Resolved (2.08.1360)

The following issues were resolved with this release.

- Resolved an issue where the controller would periodically poll for a cloud connection.
- Resolved an issue with the Allegion integration where MIFARE UIDs would be interpreted as invalid PIN codes.

  When you upgrade the controller to this firmware version, you must also change the settings on any Allegion locks with keypads.

  In the Schlage Utility software, navigate to the lock's **Device Properties** and change the following settings:
  - **Keys Buffered**: Change from 8 to 1
  - **Output Format**: Change from 9 to 1

  For more information, see Application Note 182: Allegion Integration with Protege GX.
- Resolved an issue with the Allegion integration where a forced door would generate two 'Door Forced' events. Also resolved a related issue where the system would report 'Door Forced' and 'Door Left Open' events when the PIM was powered on.
- Resolved an issue where activating duress at a door programmed on a smart reader would instead open the duress trouble input for the door programmed on the reader expander port. This resulted in duress being reported for the incorrect door or not at all.
- Resolved an issue where the controller would generate a large number of "Battery OK" events from Inovonics transmitters, even when the state had not changed.

- Resolved an issue which occurred when one user's duress PIN was the same as another user's regular PIN (while duplicate PINs were enabled). If the first user entered their duress PIN at a door set to Card and PIN operation it would be interpreted as the second user's regular PIN, causing access to be denied with no duress response.
- Resolved an issue in the controller's web interface where the clickable area of some buttons was smaller than the visual size of the button.
- Resolved an issue where the single record download service did not restart the controller after installing an HTTPS certificate, leading to the HTTPS connection failing.
- Resolved an issue in SIA reporting where bypass restore events were incorrectly reported as BR. They are now correctly reported as BU.

  If your site uses SIA reporting, before upgrading to this firmware version it is recommended that you contact your central monitoring station and inform them of the code change.

- Introduced a number of performance improvements to the controller firmware, which will mitigate timing issues on sites with large numbers of modules and extensive cross-controller operations.

  For best results, it is recommended that you use reader expander firmware version 1.12.585 or higher.

- Resolved mapping and configuration issues with the Modbus server integration.

  For more information on programming and using this integration, see Application Note 023: Protege GX Modbus Server Integration.

- When a KONE controller comes online, Protege GX will now only send global masks to that controller.

  Previously when a KONE controller came online Protege GX would send global masks to all KONE controllers. To reinstate this behavior, enter the following command in the controller programming: `FilterHLIMasks = false`
- When a global COP mask is changed, Protege GX will update only the global COP masks in the KONE controllers, and similarly for global DOP masks.

  Previously when a global COP or DOP mask was changed Protege GX would update all global masks in KONE controllers. To reinstate this behavior, enter the following command in the controller programming: `FilterHLICOPDOPMasks = false`
- Resolved an issue where, after the controller was power cycled, Verex POD inputs would report the incorrect state or become non-responsive.
- Resolved an issue where custom Wiegand credentials were treated as case sensitive. They are now case insensitive.
- Resolved an issue where EOL resistor configuration with hysteresis was not correctly switching to falling edge hysteresis.

Known Issues (2.08.1360)

ICT would like to make you aware of the following known issues in this version:

- When using the new extended data feature for SIA DC09 reporting, be aware that special characters in record names may not be decrypted correctly by Patriot receiver software. Patriot has confirmed that only ASCII characters are supported when using encryption.
- The SIA reporting format incorrectly sends MA/MH for door forced and analog expander trouble inputs.
- The duplex inputs feature is currently non-functional on one-door controllers in firmware versions above 2.08.1247.

Protege GX Controller Firmware 2.08.1309

New Features (2.08.1309)

The following new features have been included with this release.

Aperio IP Multi-Hub Integration

Protege GX controllers are now able to integrate with up to four Aperio IP hubs over the ethernet network. Each hub can control up to 16 locks, allowing integration with a total of 64 wireless locks per controller.

- Both Gen 3 and Gen 5 AH40 hubs are supported, along with a range of Aperio wireless locks.
- The integration supports a number of card formats including MIFARE Classic with sector data and ICT encrypted DESFire.
- Unique trouble inputs are available to monitor a range of status conditions for each individual door, including door forced/left open, lock tamper, low battery and offline states.
- Privacy mode is supported on compatible locks.

For more information and programming instructions, see Application Note 343: Protege GX Aperio IP Hub Integration.

Feature Enhancements (2.08.1309)

The following enhancements have been made to existing features in this release.

Antipassback in Elevator HLI Integrations

- Added support for antipassback in elevator high level interface integrations. This is available in any HLI integration which utilizes card readers connected to Protege GX controllers and reader expanders.

  Antipassback is useful in preventing users from passing their card back to allow an unauthorized person to call an elevator in scenarios where the elevator lobby has a turnstile or security gate with entry and exit readers.

  For more information, see the relevant elevator HLI application note.

Force Arming

- Typically when an area is force armed, any inputs which are currently open will not prevent the area from arming, but can cause an alarm if closed and opened again. With this firmware version, you can report on these open inputs as if they had been bypassed.

  Enter the following command in the input type programming:

  `ForceSendsBypass = true`

  With this setting enabled, when the area is force armed any open inputs are bypassed. This is shown in the input status, event log and message to the monitoring station. The bypass will be removed when the input is closed, so the input will activate the alarm if it is opened again.

  In contrast, the existing `EnableForceBypass` command allows forced inputs to be bypassed until the area is disarmed.

- When the **Use unattended brute force arming** option is enabled, you can now enable the area to use the Force Armed status rather than the regular Armed status.

  To enable this setting, enter the following command in the area programming:

  `UnattendedForceArm = true`

  This is useful alongside other options such as `EnableForceBypass` and `ForceSendsBypass` above.

Aperio RS-485 Hub Integration

- Aperio lock tamper monitoring is now supported. To monitor the lock tamper state, program a trouble input with a **Module type** of Door (DR) and a **Module input** of 3.

Dual Authentication

- Added the ability to configure dual authentication settings for doors controlled by the controller's ethernet port. The following commands are available in **Expanders | Reader expanders**:

- `DualAuthOutputEth = X`

  Sets the output that will be activated when the first user enters their credentials at the door, where **X** is the output's Database ID.
- `DualAuthTimeEth = Y`

  Sets the time that the door will wait for a second credential, where **Y** is the time in seconds.

These commands affect all doors on the controller's onboard ethernet port. Doors cannot be configured separately.

Issues Resolved (2.08.1309)

The following issues were resolved with this release.

- Resolved an issue where the KONE integration would prompt for floor selection instead of calling an elevator for the home floor. The `DontSendAccess` command is no longer required to troubleshoot this issue.
- Resolved several buffer overflow vulnerabilities.
- The clock in the top right of the controller's web interface now displays in 12HR or 24HR times based on the browser's location settings.
- Resolved an issue where hashed operator passwords could potentially be exposed.
- Resolved an issue where session IDs were not sufficiently random.
- Resolved an issue where reader expanders would not recognize alternative PIN formats when credential types were in use.
- Resolved an issue where the controller displayed noon/12PM as 0PM when 12 hour time was in use.
- Resolved an issue where the network settings would become blank in the UI after a firmware update.

In this version you will see the message "(Unpaired)" beside the current version in the **Application Software**. This message is related to future functionality and will not affect the controller's operation.

Protege GX Controller Firmware 2.08.1271

Feature Enhancements (2.08.1271)

The following enhancements have been made to existing features in this release.

Otis Compass Integration

- Added the ability to physically separate the Protege GX and Otis Compass networks, preventing networking issues. This enables the controller to communicate with the Otis network over the RJ45 onboard ethernet port, and the Protege GX network over USB ethernet.

  For more information and programming instructions, see Application Note 174: Protege GX Otis Compass Integration.

Issues Resolved (2.08.1271)

The following issues were resolved with this release.

- Mitigated an issue where RS-485 readers on the onboard reader expander would drop offline and fail to recover. Readers will now recover within 10 seconds.
- Resolved an issue with the Otis integration where the default floor was not being sent correctly for rear doors. This fix allows the configuration of DEC operation modes 1 and 4. For more information, see Application Note 174: Protege GX Otis Compass HLI Integration.
- Resolved an issue where the controller would deactivate the cellular modem immediately when power began to drop. The modem will now remain operational until power is completely lost.

- Resolved an issue where the Redwall integration was not working after firmware version 2.08.849. Some additional configuration is required. For more information, see Application Note 181: Protege GX Redwall Integration.
- Resolved an issue where changing the controller's IP address or event server could cause the web interface to become inaccessible from the server.
- Resolved an issue where the controller's IP address could not be set via the keypad.

Protege GX Controller Firmware 2.08.1255

New Features (2.08.1255)

The following new features have been included with this release.

USB Cellular Modem Support

This firmware version includes support for the new Protege DIN Rail Cellular Modem. This 4G modem connects to the controller via the USB port and provides an alternative communication pathway between the controller and central monitoring station or Protege GX server.

- The 4G modem is designed for reporting of events and alarms to the central monitoring station. This is ideal for replacing existing phone lines for backup reporting services.
- The controller is also capable of connecting to the Protege GX server over the 4G cellular network for sending events and receiving downloads and manual commands. This enables you to extend the reach of your Protege GX system to areas without physical network infrastructure.

  This feature requires a SIM card that supports inbound data connections.

- Additional tabs have been added to the **System Settings** in the controller's web interface, allowing you to configure the onboard ethernet and 4G modem (USB ethernet) connections separately and define which adaptor will be used by each event server path.

For more information on the Protege DIN Rail Cellular Modem and configuring it for use with Protege GX, see the relevant product documentation.

Feature Enhancements (2.08.1255)

The following enhancements have been made to existing features in this release.

EOL Resistor Programming

- Added support for 3 Resistor EOL input doubling with 6 states.

  The feature can be used on any input and is set up using the physical input and another input record which is offset by the total physical inputs of the device. The 6 states are then translated to input states for both.

For more information and programming instructions, see Application Note 303: Configuring Protege Input EOL Resistors Using Commands.

Issues Resolved (2.08.1255)

The following issues were resolved with this release.

- Resolved an issue where the **Bell squawk only when unattended** feature did not work as expected. Now, arming and disarming by card reader or function code will not cause a squawk when this feature is active.
- Resolved an issue where latch unlocking a door group would not unlock any doors that were momentarily unlocked by access.
- Resolved an issue where the PRT-ZX1 firmware could not be upgraded from the controller web UI.

Known Issues (2.08.1255)

ICT would like to make you aware of the following known issues in this version:

- When the **Entry/Exit reading mode** is set to Custom and the card and biometric credential types are selected, the door does not correctly accept the biometric credentials and denies access.
- When door's lock time is recycled by a user with **User operates extended door access function** enabled, the door's standard lock time is used instead of the extended lock time.

Protege GX Controller Firmware 2.08.1244

New Features (2.08.1244)

The following new features have been included with this release.

Function Outputs

Function outputs provide an alternative method of controlling outputs based on the door state. When the door is unlocked, up to three function outputs or output groups can be activated. These operate independently of the lock outputs, allowing you to control connected devices such as automatic door pumps, chair lifts and bypass shunts.

- Program up to three separate function outputs or output groups for each door, each with a different activation time.
- Activate the function output every time the door is unlocked, or only when the door is unlocked by access or REX/REN. Activation can also be restricted to people with disabilities for control of accessibility devices.
- Outputs can be deactivated when the door is opened or closed.
- Outputs can be recycled by user access or REX/REN, allowing users to keep the output activated for longer.

This feature requires Protege GX software version 4.3.317.10 or higher. For more information and programming instructions, see Application Note 336: Programming Function Outputs in Protege GX.

Feature Enhancements (2.08.1244)

The following enhancements have been made to existing features in this release.

Disable Remote Area Arming, Disarming and 24hr Disarming

- Added the ability to disable remote arming and disarming of an area.
  This is achieved by adding the appropriate command(s) to the programming of each required area.
  - Add the command **`NoRemoteArm = 1`** to disable remote arming.
  - Add the command **`NoRemoteDisarm = 1`** to disable remote disarming.
  - Add the command **`No24hrRemoteDisarm = 1`** to disable remote 24hr disarming.

This feature supports ULC Standard S302 which limits arming and disarming of a Security Level 3 or Level 4 Area to only the local system keypad(s).

These protection requirements are applicable for safes, ATMs, CDUs, CRUs, night depositories and vaults.

For information on how to configure this feature, see Application Note 326: Disabling Remote Area Arming and Disarming.

Area Counting Options

- A new **Area Count on Door Opening** option has been added. When this option is enabled the area count is not incremented/decremented by the user merely being granted access, but will be updated only if the door has been opened after entry/exit is granted.
  To enable the option, add to the area programming the command: **`AreaCountOnDoorOpening = true`**

For more information see Application Note 205: Area Counting.

Controller Password Policy

- This version includes the initial implementation of a password policy for controller operators. All new operator passwords are now required to have 8 characters or more. Existing passwords are not affected.

  Further functionality is in development.

Cybersecurity Enhancements

- Removed insecure FTP and Telnet protocols from the controller.
- Removed an insecure debug mechanism.

Otis Compass HLI Integration

- Increased the number of floors supported by the Otis HLI integration from 64 to 128. This can be implemented by entering the following commands in the controller programming:
  - `HLI_128_FLOORS = true`
  - `HLI_MAX_FLOORS = 128`

Language Support

- Updated translations on the controller web interface.
- Added Turkish as a selectable language on the controller.

Issues Resolved (2.08.1244)

The following issues were resolved with this release.

- Resolved an issue where multiplexed Wiegand readers were not able to read custom credentials.
- Resolved an issue where badging custom credentials multiple times at multiplexed Wiegand readers could cause a controller crash.
- Resolved an issue where areas could not be armed using card read and input 8 of a reader expander using RS-485 readers.
- Resolved an issue with the ASSA ABLOY DSR integration where door status was not being displayed correctly.
- Resolved an issue with the ASSA ABLOY DSR integration where PIN and credential expiry did not work.
- Resolved an issue with the ASSA ABLOY DSR integration which could cause a controller crash if no smart reader records were assigned to the DSR locks.
- Corrected an issue in the ASSA ABLOY DSR integration where an unexpected response from the DSR could cause the controller to crash.
- Resolved an issue where the **Always log input event** option was not enabled/disabled correctly when the input type was changed by an operating schedule.
- Resolved an issue which was causing persistent memory leak in 3G-enabled controllers. This could prevent operators from accessing the controller's web interface, with the following error message: 'The Web Server is too busy, cannot handle any more connections.'
- Resolved an issue where the HTTP port for the controller's web interface could be set to 0 or other restricted ports. Added an error messages to notify operators when the selected port is not valid.
- Corrected an issue where, when HTTPS was enabled, an HTTP connection could still be established on one randomly chosen port.
- Resolved an issue where the LEDs of OSDP readers connected to a reader expander did not function correctly if the controller's onboard reader was not also configured for OSDP.
- Removed a vulnerability where programming information was visible on legacy controller web pages.
- Resolved an issue where single door controllers did not detect the defaulting link on power up.
- Resolved an issue where deleting a programmed elevator record could cause the controller to restart on a card badge.

- Resolved an issue in the Otis MLI integration where the controller was not sending 'Set Access' packets to the elevator controller.
- Resolved an issue with the Otis MLI integration where the last elevator car on each interface was displaying 'Floor Unknown' for all floors.
- Resolved an issue in the Otis MLI integration where, when a user gained access to a floor, the event log would report the incorrect floor number.

  To implement this fix, enter the command **AEAFloorOffset=X** in the controller programming. **X** is a value from -8 to 8 that will be added to the floor relay values for the purpose of event reporting.
- Resolved an issue where controller operators could not be deleted.
- Resolved an issue where 'Access denied by door type' events were not displayed correctly when access was denied due to an incorrect credential type.
- Resolved an issue where the controller could not process osdp_RAW packets received from Idesco readers.
- Resolved an issue where, if a user had two credentials with the same facility/card number but different credential types, the last used time would be updated for both credentials whenever one credential was used.
- Fixed an issue where it was not possible to search for operators that contained an ampersand and/or equals sign in the record name.
- Resolved an issue where PINs entered at a 4 bit HID PIN pad could fail if entered immediately after a card read at another reader (using multiplexed Wiegand readers on the onboard reader expander).
- Fixed an issue where areas could be incorrectly disarmed by schedules that crossed over midnight.
- Improved the controller firmware update process. This mitigates an issue where the software incorrectly reports that the firmware update has been interrupted.
- Added the ability to introduce a regular time correction to the controller's internal clock. This mitigates an issue where controllers running in offline mode for long periods can experience time drift.

  To implement this fix, add the following command in the controller programming:

  TimeDriftComp = X, Y

  Where **X** is the frequency for applying the time correction (in days), and **Y** is the amount of the time correction (in seconds). For example, the command **TimeDriftComp = 2, 10** will add 10 seconds to the controller's clock every 2 days.
- Resolved an issue with card readers configured for card and PIN authentication where the card could be entered at the entry reader and the PIN at the exit reader, and vice versa.
- Resolved an issue where unaddressed modules were not displayed in the module addressing window after the controller restarted.
- Resolved an issue where function codes could not be used on smart readers.
- Resolved an issue that was exacerbating clock drift.
- Resolved an issue where the **Disable green LED processing** option in the reader expander programming did not work for readers connected in RS-485 configuration.

  Limitation: This feature is not available for smart readers.
- Resolved an issue with the KONE Destination 880 integration where commands programmed for Group 1 and Group 2 would be overridden by UI programming if it was present.
- Resolved an issue with the KONE Destination 880 integration where "RCGIF" as part of a command was interpreted as an entire command and resulted in the service stopping.
- Resolved an issue where turnstiles were not correctly calling an elevator for the home floor.
- Modified the KONE Destination 880 integration to accommodate some KONE group controllers that do not follow the recommended heartbeat protocol.
- Resolved an issue where the controller's **Settings** page was not displayed correctly when non-English characters were used in some record names.
- Resolved an issue where areas would not arm correctly on schedule when successive days ending in midnight in the same period were checked.
- Resolved an issue where it was not possible to enter a hostname in the event server address fields.

- Resolved an issue where access was denied incorrectly for doors with the Card and PIN door type while locked by calendar action.
- Resolved an issue where the time displayed in the web interface would drift backwards when the browser tab was not focused, so that it did not accurately display the controller time.
- Resolved an issue where multiplexed Wiegand readers connected to a reader expander would not produce 'Exit Granted' events for custom credential types.
- Resolved an issue with the ASSA ABLOY DSR integration where the controller could restart during initial synchronization.
- Resolved an issue where it was not possible to access the keypad using the default installer code after defaulting the controller.
- Verex Transition:
  - Resolved an issue where the controller did not process all four inputs on legacy Verex keypads correctly.
  - Resolved an issue where the arm function display did not line up with the correct function key.

Protege GX Controller Firmware Version 2.08.1140

New Features (2.08.1140)

The following new features have been included with this release.

Controller Default Security Upgrades

This release includes significant changes to the process of setting a password and defaulting the controller. These changes ensure that Protege GX is compliant with Title 1.81.26: Security of Connected Devices, enacted by the State of California.

Upon firmware upgrade, you will be asked to change your password if it is still the default. Defaulting a controller now resets all settings to the factory default, including IP and login information.
In the future, new controllers shipped from the factory will have HTTPS enabled by default and require you to set a custom login username and password.

In the past, when a controller was defaulted, only the programming database was deleted. With this version, the controller is entirely reset to factory default, with the following effects:

- The IP address is reset to the default address (192.168.1.2).
- Any custom HTTPS certificate uploaded by an operator is deleted and must be reloaded.
- All other **System Settings** (e.g. HTTP Port, DNS Server, Event Servers) revert to their default values.
- All programming is deleted, including all operators.

  When you access the web interface after defaulting the controller, you will be required to create a new username and password for the administrator operator.

Protege GX ASSA ABLOY DSR Integration

This release introduces the Protege GX ASSA ABLOY DSR integration. The integration provides the ability for Protege GX to connect and communicate with IP-enabled ASSA ABLOY locks, via the ASSA ABLOY DSR (Door Service Router) system.

In this integration, a single Protege GX controller communicates with the ASSA ABLOY DSR server, which in turn communicates with up to 1024 IP-enabled locks over WiFi or ethernet. Protege GX controls and maintains all access control functions and receives alarms and events from the DSR server.

For integration details and configuration information, refer to AN-311: Protege GX ASSA ABLOY DSR Integration.

User Interface Improvements

This version features improvements to the controller's user interface.

- Switch between light and dark display themes to reduce eye strain.
- Pick the display color used for the header bar and other interface elements. Your selection will persist whenever you log in to the controller from the same browser.

Feature Enhancements (2.08.1140)

The following enhancements have been made to existing features in this release.

LED Color Support

- Added support for LED colors and patterns on OSDP readers connected to the onboard reader expander.
- Added the ability to define the L1 and L2 LED colors using the corresponding reader output in the software. This is available for both ICT RS-485 and OSDP readers.

  To set the LED color, add the following command to the output programming: `LEDColour = X`, where `X` corresponds to a color code from the table below.

  This command can be used with the following outputs on a reader expander or controller onboard reader expander:
  - Output 3 (Green LED Port 1)
  - Output 4 (Red LED Port 1)
  - Output 6 (Green LED Port 2)
  - Output 7 (Red LED Port 2)

  The following color codes are available:

Number (X)	Color	Supported Reader(s)
1	Red	ICT RS-485, OSDP
2	Amber	ICT RS-485, OSDP
3	Orange	ICT RS-485
4	Yellow	ICT RS-485
5	Lime	ICT RS-485
6	Green	ICT RS-485, OSDP
7	Mint	ICT RS-485
8	Turquoise	ICT RS-485
9	Cyan	ICT RS-485
10	Sky Blue	ICT RS-485
11	Cobalt	ICT RS-485
12	Blue	ICT RS-485, OSDP
13	Violet	ICT RS-485
14	Purple	ICT RS-485, OSDP
15	Magenta	ICT RS-485
16	Crimson	ICT RS-485

This feature is only supported on card readers with RGB LEDs.

Custom LED colors may not function correctly when enhanced reader outputs are enabled and one output is activated on the reader port. This is a known issue. This operation has not yet been validated with area status display functionality, function codes, and 'LED follows lock' functionality (i.e. when the door's lock output is not the default reader port lock output) handled by the controller.

Low Level Elevator Integration

- The controller now indicates which of the user's cards was presented when accessing an elevator.

ThyssenKrupp HLI Integration

- Extended the ThyssenKrupp HLI integration to support up to 128 floors instead of 64.

For information on how to configure this feature, see Application Note 169: Protege GX ThyssenKrupp HLI Integration.

Cybersecurity

- Improved web security by preventing cross-site scripting.
- Upgraded jQuery to 3.5.1 to include a security patch from jQuery.

Door Forced Alarms

- Added the ability to delay door forced alarms, allowing the door to be in the 'open' state for a specified length of time before the audible alarm and door forced trouble input are activated.

  For more information, see Application Note 304: Delaying Door Forced Alarms.

Aperio Integration

- Added the ability to process ICT encrypted DESFire cards presented at an Aperio lock.

Trouble Inputs

- Added the ability to set alarm and restore speeds for trouble inputs. This allows you to prevent a trouble input from triggering an alarm until it has been present in the system for a set time.

  For more information, see Application Note 305: Trouble Input Alarm and Restore Speeds.

Schindler PORT HLI Integration

- Added the ability to set a home floor for a user.
- Added support for the 'Pure Wiegand' site code format.
- Updated the process for sending users to the Schindler database, so that the user's ID is sent instead of the name.

For more information, see Application Note 196: Protege GX Schindler HLI Integration.

Elevator HLI

- Added the ability to process the door lock output / output group (if configured) in elevator HLI integration.
- Added the ability to process ASCII card reads from the Otis elevator integration.

Expander Module Support

- Added support for updating the firmware of the PRT-TS50 module.

Issues Resolved (2.08.1140)

The following issues were resolved with this release.

- Resolved an issue with the Otis AEA Type B and EMS elevator integrations where timers were not reset on all the elevator cars in the elevator group, if the group had been marked as offline.
- Resolved an issue where the onboard reader expander's port 1 exit reader was not restoring beeper operations correctly after an access granted event.
- Resolved a reporting issue where, when the primary channel failed, the trouble input ReportIP Reporting Failure would not open after the message retry attempt limit was reached.

- Resolved an issue where door lockdown could be overridden by an unlock schedule if a manual unlock command was sent while the schedule was valid.
- When changing a user's PIN from the keypad, there is now a check against existing user duress PINs when the **Treat User PIN Plus 1 as Duress** option is enabled.
- Resolved an issue where changing a user's PIN from the keypad caused the controller to restart.
- Resolved an issue where a keypad's firmware could not be updated if it did not have a corresponding module record configured.
- Resolved an issue where performing a module update after a firmware update caused an error to be displayed.
- Resolved an issue where elevator floors were not relocking after the **Unlock Access Time** had expired.
- Resolved an issue where authentication files loaded to the controller could not be validated by third-party certificate authorities.
- Resolved an issue where updating a user PIN from the keypad in a large database could cause the controller to restart.
- Resolved an issue where the controller would not correctly clear the session key stored on a reader expander when its network port type was no longer configured for OSDP.
- Removed a security vulnerability where the controller would send the session key to a reader expander even if the session key had not changed.
- Resolved an issue where the **Relock on Door Close/Open** function was not working correctly when using additional lock outputs with no activation delays configured.
- Resolved an issue where cards greater than 32 bits were being incorrectly truncated when presented at Aperio locks.
- Resolved an issue where the lockdown state of a door was not restored when the controller was restarted.
- Resolved an issue where a crash could occur when a user with more than 255 access levels was denied access at a door.
- Resolved an issue with the Otis EMS integration where floors were not relocked correctly after the floor selection had timed out.
- Resolved an issue where the Otis EMS integration was not correctly processing the response frames for dispatch reporting.
- Resolved an issue that was causing incorrect REX/REN detection when the controller powered up.
- Resolved an issue with the Inovonics integration where pressing multiple buttons at the same time could cause an 'Error 036' event.
- Resolved an issue where, when Contact ID is used as a backup service to Report IP, the Contact ID service would not attempt to dial out after a power cycle.
- Resolved an issue where area status LED changes could cause the onboard reader's enhanced outputs to not reactivate correctly when the reader or controller was power cycled.
- Resolved an issue with the ThyssenKrupp HLI integration where the kiosk on floor 64 was not receiving the correct floor map updates.
- Resolved an issue with the ThyssenKrupp HLI integration where the maximum floor configured was not reloaded correctly if the integration was already running.
- Resolved an issue with the ThyssenKrupp HLI integration where the front and rear designation for landing based kiosks was not set correctly.
- Resolved an issue where area status LEDs were not controlled correctly when enhanced outputs were active.
- Resolved an issue where a card reader beeper could be deactivated by badging a card once at the exit reader or pressing a key on the keypad, without changing the status of the output in the system.

  Note: The fix requires the following command to be entered in the programming of each reader expander: `ForceRestoreBeeper=true`. This command causes the reader expander to reactivate the output regularly until it is legitimately deactivated.
- Resolved an issue where Wiegand readers connected to reader ports 1 and 2 and processing the same door did not synchronize their LED operation correctly. This caused the port 2 reader L2 to remain on for too long after repeated card badges.
- Resolved a reader expander LED glitch which occurred when the door relocked.

- Resolved an issue where area status LED functionality was not always respecting standard reader LED output activation.
- Resolved an issue where the RS-485 module network would reboot periodically after the controller was powered up without an ethernet connection.
- Resolved an issue where a door using additional lock outputs, that were set to unlock with the same activation time and no delays, did not have its status updated correctly when relocked after a fire control unlock.
- Resolved an issue where a controller would not successfully boot up on OS version 2.0.16 with the ethernet cable connected.
- Resolved an issue with RGB readers connected to the controller's onboard reader in RS-485 configuration. When the reader temporarily lost connection while the door was unlocked, upon reconnection the green LED was incorrectly stuck in the 'on' state. This was resolved for the case where the door's lock output was the Lock 1 output on the onboard reader expander.
- Resolved an issue with OSDP reader LEDs not synchronizing correctly during standard door operation when configured with custom color codes.
- Resolved an issue with credentials longer than 48 bits being truncated incorrectly when presented at ICT RS-485 or OSDP readers on the controller's onboard reader expander.
- Resolved an issue where the **Tamper Input if Module Offline** option did not work correctly.
- Fixed a regression where HTTPS would be disabled on controller startup.
- Resolved an issue which occurred when two ports of a reader expander were both set for card and PIN operation. If a card was badged at one reader and an incorrect PIN entered at the other, access would be denied on the first reader.
- Resolved an issue where a 'Read Control Error' could be generated if two packets were received from PIN pads on the same reader port in quick succession.
- Resolved an issue where an output that was turned 'off timed' would not return to the correct state if it was off before the command was received.
- Resolved an issue where controllers running the Allegion integration could enter a restart loop.
- Resolved an issue where Wiegand reader LEDs which were pulsing were not restored to the correct state after the door was unlocked.
- Resolved an issue where the **Panel Name** in the System Settings could be edited, which caused incorrect settings data to be saved. The **Panel Name** is now read only.

Protege GX Controller Firmware Version 2.08.1002

New Features (2.08.1002)

The following new features have been included with this release:

Fast User Disable

With this firmware version and the accompanying software version (4.3.285), when a user record is disabled in the software, a 'User Disabled' command will be sent directly to the controller without waiting for a regular controller download. This will cause the controller to update the user record directly in its internal database, disabling the user's access rights almost immediately.

Compliance Types

With this firmware version and the accompanying software version (4.3.285), Protege GX's Credential Type functionality has been extended to include custom Compliance Types. For more information, see the software release notes.

Cybersecurity Enhancement

The list of ciphers advertised for use in the HTTPS negotiation process has been updated so that TLS_ECDHE_RSA ciphers are prioritized over TLS_RSA ciphers.

Otis EMS (Elevator Management System) Integration

Protege GX now has the ability to integrate with the Otis EMS Interface.

For more information, see Application Note 298: Protege GX Otis Elevator Management System Integration.

Ask for Defer Time

The command **`AskForDeferTime = true`** has been added to the Area commands. This allows users to specify the number of hours to defer area arming for, when logged into a keypad.

Alternative REX Input

The command **`AltREX = #`** has been added to the door commands. This specifies the input to be used as a secondary REX input, which operates using the extended REX time instead of the standard door lock time.

Aperio Integration: Privacy Mode

Privacy mode has now been enabled for the Aperio integration. When the inside push button is pressed on an IN100 device, Protege GX will deny user access until privacy mode has been released by a request to exit (turning the inside handle), or canceled by a user with super user rights. Events will be generated in the event log whenever privacy mode is activated or deactivated.

Feature Enhancements (2.08.1002)

The following enhancements have been made to existing features in this release:

Reader Expanders

- Updated OSDP functionality, including Secure Channel and OSDP reader support on Reader Expander modules.

  For more information on supported features, see Application Note 254: Configuring OSDP Readers in Protege GX.

Function Codes

- Updated the Function Code feature to work with Door Types using custom Credential Types. Function Codes can now be implemented by Custom Credential + PIN or Custom Credential only.

Commend Integration

- Updated the Commend integration to handle inputs programmed without the 'D' or 'A' prefix.
- Updated the Commend integration to handle the tamper alarm, duress button and door release messages.

Schindler HLI Integration

- Extended the Schindler Elevator HLI to allow for additional ports to be opened for the Call and Life Reporting interfaces.
- Extended the Schindler Elevator HLI to allow the use of ICT readers for Schindler elevator access.

Issues Resolved (2.08.1002)

The following issues have been resolved in this release.

- Fixed a bug in the KONE HLI service which would cause it to crash if the service was enabled but there was no other KONE programming.
- Fixed an issue with the count on access functionality for areas causing the controller to crash if it was supplied with two or fewer entries.
- Fixed an issue with Sunday schedule periods not working at the programmed times.
- Fixed an issue with the version number of devices populating in the Module Addressing window.

- Fixed an issue with the onboard RS-485 reader's offline Trouble Inputs being opened automatically when a module update was performed.
- Fixed an issue with credential events showing the actual PIN entered by the user.
- Fixed an issue where a 'Smart Reader raw credential' event was being incorrectly displayed instead of a Reader Expander raw credential event for Wiegand credentials on Reader Expanders.
- Fixed an issue where an area arming via user count reaching zero was not displaying the correct door reference in the relevant events.
- Fixed an issue with the Otis integration where the last eight floors (of 64) were not being processed correctly when there were basement (negative) floors present.
- Fixed an issue with Otis Authorized Floor V2 Packet not setting the 'Special Features' byte for the user correctly by default for Otis readers.
- Fixed an issue with 'entry granted' events showing when the reader port was configured as an exit.
- Fixed an issue with reader expanders incorrectly setting a door as forced open after a module update.
- Corrected an issue where configuring an input's EOL settings using commands could result in it flagging the module it is assigned to as requiring a module update after every download.
- Fixed an issue where custom credentials could not be presented out of sequence.
- Fixed an issue with the population of account number information in SIA/CID over IP poll messages.
- Fixed an issue with SIA/CID over IP encryption not working.
- Fixed an inconsistency with the Aperio integration, so that now when the inside handle is turned only a REX event is generated without an unlock command, as the physical mechanism is internally handled by Aperio.
- Fixed an issue with the Allegion AD-series integration incorrectly sending through a locking packet when an invalid format card is presented.
- Fixed an issue with the Allegion AD-Series integration not correctly locking/unlocking via manual commands for any lock after the first eight that are linked to a PIM.
- Fixed an issue with the Allegion AD series integration not resetting the left open trouble input when the door closes.
- Fixed an issue with EOL thresholds not working for reader expanders beyond module address 8.
- Fixed an issue with the Forced Open alarm not disabling the assigned output when the Forced Alarm Operating Schedule becomes invalid.
- Fixed an issue where the door lock output time was unexpectedly extended with dual credential access.
- Fixed an issue where the dual authentication output did not deactivate according to the specified timeout.
- Fixed an issue with detailed credential events not correctly displaying all credentials presented.
- Fixed an issue with REX and REN not being processed on the initial trigger following a restart of the controller.
- Improved security by removing the server name that is used when the web server generates HTTP response headers.
- Fixed an issue with generic input reporting for the Commend integration.
- Fixed an issue where card reader area status LEDs were not working when enhanced smart reader outputs were enabled.
- Fixed an issue where a controller that was simply polling the status port could take longer than the software to decide that the connection has been lost.
- Fixed an issue with Door Alarms not working correctly when the Operating Schedule for Pre Alarms and Left Open Alarms are both invalid.
- Fixed an issue where firmware could not be updated on controllers.
- Resolved an issue where setting daylight savings time could cause the controller's internal clock to regularly skip an additional hour ahead.

Protege GX Controller Firmware Version 2.08.911

New Features (2.08.911)

New Look Web Interface

- New look web pages including multilingual operators.
- Ability to update firmware via web pages.

HTTPS Support

- There is now support for HTTPS connection to the controller's web interface. This provides an improved level of security by encrypting communications between controller and web browser.
- ICT **strongly recommends** that HTTPS connection is established on all live Protege sites, especially where the controller's web interface can be accessed over the internet.
- These certification methods are available:
  - Validating and installing a third-party certificate obtained from a certificate authority.
  - Installing a self-signed certificate (recommended for testing only).

For more information on configuration and operation of this feature, please see Application Note 314: Configuring HTTPS Connection to the Protege GX Controller.

Wiegand Formats Defined as Custom Credential Types

- Wiegand formats can now be specified using customized credentials allowing up to 32 formats to be recognized per reader port.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Offline Access to Input Status at Keypad

- The command `OfflineInputView = true` has been added to the Keypad commands. This will allow users to view the state of the inputs belonging to the primary area of the keypad, via the offline menu. The list of inputs available for viewing will be filtered to only include those which are not sealed.
- The command `ClosedInputsInOfflineView = true` has been added to the Keypad commands to work in conjunction with the new offline access to the input view menu described above. When enabled, all inputs associated with the keypad's primary area will be available to view in the offline menu irrespective of the input state.

Area Status – Visual Feedback

- It is now possible to control the color of a reader LED via commands, based on the status of up to 4 system areas that the reader is monitoring. This gives users visual feedback to indicate the current status of any one of these system areas, depending on which area status has the highest priority.

  Note: This feature requires card readers with RGB LEDs.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Ademco Vista Integration

- It is now possible to integrate with Ademco Vista-128BP/Vista—250BP panels via commands.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Area counting

The command **`CountOnAccess = DV,AL,AL,AL...`** has been added to the Area programming which allows a data value (DV) to be incremented or decremented each time a user with one of the specified access levels (AL) enters or leaves the area. Up to four of these commands can be used per area.

Expander Module Support

- Added Support for the 2nd Generation of Intercom modules.

Feature Enhancements (2.08.911)

The following enhancements have been made to existing features in this release:

Controller Network Security Enhancements

- Module Comms UDP/TCP (9450) has been disabled by default. It can be re-enabled via Controller commands:
  - `EnableModuleUDP = true`
  - `EnableModuleTCP = true`
- Touch Screen Comms UDP (9460) has been disabled by default. It can be re-enabled via Controller commands:
  - `EnableTLCDCommsUDP = true`
- Inter-Controller Comms TCP (9470) has been disabled by default. It will only be enabled if Protege GX has told the controller it is part of a controller group.
- Ping is disabled by default for the onboard Ethernet connection. It can be re-enabled via Controller Commands:
  - `EnablePing = true`

  If you have any modules installed that utilize Module Comms (port 9450) or Touch Screen Comms (port 9460) over Ethernet you will need to add the above commands to the controller or these modules will not be able to communicate with the controller.

Doors

- The command **`LockOutAttempts = #`** configures the number of retries allowed before the 'Too Many Attempts' trouble input is generated for the door. In the Door commands, add this line with your required value of retries in place of the # symbol.
- The command **`AlwaysAllowREN = true`** has been added to the Door commands which will allow Requests to Enter to be actioned, even when the door is open, similar to what is available for Requests to Exit functionality.
- Added ability to configure when Pre-Alarm, Left Open and Forced Open alarms are suppressed, such as when unlock schedules are valid, or when doors are unlocked by programmable functions, area control or calendar actions.
- The command **`SlaveREX = true`** has been added to the Door commands. This will allow a slave door to follow its primary door whenever Requests to Exit/Enter or manual commands are actioned on the primary, in addition to Access Granted actions.
- The command **`AccessDeniedTime = #`** has been added to the Door commands which will specify the duration in seconds that an output or output group will be activated for when access to the door has been denied. This must also be paired with one of the following 2 commands in order for the functionality to occur.
- **`AccessDeniedOutput = #`** has been added to the Door commands which will specify the output that will be activated when access to the door has been denied.
- **`AccessDeniedOutputGroup = #`** has been added to the Door commands which will specify the output group that will be activated when access to the door has been denied.
- Included the lock state as well as the door state in the multi state value that is returned when using the BACnet service.

Salto SALLIS Integration

- The Salto SALLIS Integration can now support locks equipped with keypads.
- Added ability to process ICT encrypted DESFire cards presented at a SALLIS lock.

High Level Elevator Integrations

- Up to 128 front and rear floor openings can now be supported for the KONE Elevator HLI.

Input/Output/Door Status

- Improved efficiency of restoring statuses and events by controllers after losing connection with Protege GX for a significant amount of time.

Elevators

- The command `EntryMode = #` has been added to the Elevator Car commands. This configures the type of authentication that must be used to gain access to the elevator car. The **#** symbol should be replaced with your required type of authentication as follows:

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

Readers

- Added the ability to trigger a duress trouble input from a reader's keypad.

OSDP Support

- Controller reader ports now support the following functionality, conforming to a subset of the OSDP Version 2.1.5 specification:
  - Manual Commands
  - Function Codes (multi-color LED indication is not currently supported)
  - Beep on REX
  - Custom Credentials
  - LED Sync on Connection

Note: OSDP is not currently supported on reader expander reader ports.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Allegion Integration

- Added ability to handle AD300/301 locks for the Allegion AD-Series Integration.
- Added generation of connection status events for the Allegion AD-Series
- Added ability to handle deadbolt state changes for the Allegion AD-Series Integration.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Aperio Integration

- The command `HasAperioDeadbolt = true` has been added to the Door commands. This will allow users to define whether an Aperio lock is physically fitted with a deadbolt, which is used for processing the deadbolt functionality. By default, all Aperio locks are assumed to NOT be fitted with a physical deadbolt.

Language Support

- Added language support for Czech, Dutch and German.

KONE Elevator Integration

- Added the ability to handle the Destination 880 protocol.

Issues Resolved (2.08.911)

The following issues have been resolved in this release.

- Fixed an issue with the controller not being able to handle more than 256 doors within a single access level.
- Fixed an issue where the on-board reader expander would not recognize PIN entries when set to Casi-Rusco format.
- Fixed an issue of incorrectly displaying duplicate areas when navigating through a keypad module's area group.
- Fixed an issue with card readers operating in RS-485 mode occasionally dropping offline when readers with different firmware versions were wired in a multiplexed configuration on the Onboard Reader Expander.
- Fixed an issue in the BACNet service where setting the present value of a multi-state value would always set the value of the object with an index to zero.
- Improved the time synchronization between linked controllers when one has a time zone configured and one doesn't.
- Fixed an issue where OSDP readers would not read HID iClass reader PINs correctly.
- Fixed an issue with Pre-Alarm and Left Open events not being generated for the Allegion AD-Series Integration.
- Fixed an issue with Smart Reader Tamper, RF Loss and Low Battery events being incorrectly generated for the Allegion AD-Series Integration.
- Fixed an issue with the Low Battery and Tamper trouble input restoring incorrectly for the Allegion AD-Series Integration.
- Fixed an issue with Commend Integration not fully updated to handle Commend Input IDs starting with 'A'.
- Fixed an issue with the MODBUS door register write not working properly.
- Fixed an issue with operator triggered arm/disarm of Apartment areas not displaying the correct operator reference.
- Fixed an issue with REX/REN not working for the first time after a controller restarts, if the 'Invert REX/Invert REN' option is not enabled.
- Fixed an issue where PINs with leading zeros would not work when using dual authentication to log into a keypad.
- Fixed an issue where the BACnet service could fail to respond due to an invalid broadcast address.
- Resolved issue with Access Taken and Access Not Taken events not always displaying the correct user reference.
- Fixed issue with control of Area, Trouble Inputs and Elevator Floors via BACnet not working as intended.
- Resolved issue with user's access level expiry not being taken into consideration when checking the user's access to a door.
- Fixed issue with potential Receive Buffer overflow for BACnet service.
- Fixed a regression that stopped the Keypad Login Requires Card option from working.

Protege GX Controller Firmware Version 2.08.0848

New Features (2.08.0848)

The following new features have been included with this release.

Resistor Values

Added the ability to individually specify the resistor values connected to monitored Inputs and to specify more than two resistors if required.

Issues Resolved (2.08.0848)

The following issues have been resolved in this release.

- Fixed issue with Function Codes not correctly checking the entry/exit mode of the door type when configured to be usable for both Entry and Exit directions on the door.
- Improved the module update process to eliminate any input or output glitching when an update is performed.

Protege GX Controller Firmware Version 2.08.0843

New Features 2.08.0843

The following new features have been included with this release.

Additional Lock Outputs

Up to an additional 5 lock outputs or output groups can now be assigned to a door. Each additional lock output or output group can be configured with their own individual lock activation time, as well as a delay before activation time. This delay would allow the additional lock outputs to be activated in a staggered sequence. For information on configuring the additional Lock Outputs, please refer to the Protege GX Operator Reference Manual.

Feature Enhancements 2.08.0843

The following enhancements have been made to existing features in this release:

Doors

- Doors can now be associated with a new trouble input, Door Duress, when either a duress user's PIN or when a duress PIN code has been entered into the reader at the door. For information on configuring the Trouble Inputs, please refer to the Protege GX Operator Reference Manual.
- The command `DualCredPendingTime = #` configures the timeout for supplying credentials for authenticating a user, such as Card and PIN. In the Door commands, add this line with your required value of timeout in place of the # symbol.

Keypads

- Improved process for bypassing inputs and trouble inputs when logged into a keypad.
- Improved process for viewing doors, inputs, trouble inputs and outputs when logged into a keypad.

Inovonics Integration

- The Inovonics Integration can now support the Inovonics Repeater Module. For information on configuring the inputs and trouble inputs of the Inovonics Repeater Module, please refer to the Inovonics Wireless Receiver Module Installation Manual.

Services

- Improved feedback to the monitoring station for Report IP services configured with 'Enable Offline Polling', when the 'Report IP Reporting Failure' trouble input has been generated.

Dual Custody

- The command `CustodyPairEnforced = true` has been added to the Door Type commands which will update the antipassback status for both the Dual Custody Master and Dual Custody Provider. In addition, both the Dual Custody Master and Dual Custody Provider will be included in the area counting process.

Access Level Outputs

- Access level outputs can now be toggled between activations.
- Access level outputs can now be activated when reader port operates under 'Area Control' mode.

Issues Resolved 2.08.0843

The following issues have been resolved in this release:

- Resolved issue with the Log Message Retries and Log Reporting Failure options not working correctly for the Report IP service.
- Resolved issue with Modbus service unable to deactivate an input.
- Keypad no longer displaying incorrect language when accessing certain offline menus.
- Resolved issue with Defer Automatic Arming not working when deferring using a card badge.
- Activate Access Level Output now works correctly for reader port 2 when configured for Elevator Mode.
- Resolved issue with card readers operating in RS-485 mode not generating the Door Too Many Attempts trouble input correctly.
- Resolved issue with card readers connected to the onboard reader expander momentarily dropping offline after programming is downloaded.
- Improved efficiency of sending via backup service for Report IP when all channels have been determined as offline.
- Resolved issue with invalid PINs entered via readers reporting as raw card read events.
- Access level outputs now activate correctly as per configurations when triggered via Smart Readers.
- Corrected an issue where certain combinations of username and password supplied for CSV IP service would cause the controller to crash.

Protege GX Controller Firmware Version 2.08.0825

New Features (2.08.0825)

The following new features have been included with this release.

Card Usage Counting for Access Limits

User Cards can now be limited to a certain number of Access Granted swipes for a particular time period. This can be used to enable scenarios such as cafeteria line access or clubroom access based on membership policies. To enable this functionality, enter **`LimitUsage=true`** into the Access Level Commands.

- The command **`UsesBeforeDisable = #`** configures the number of uses for the Access Level before its disabled. In the Access Level Commands, add this line with your required value of uses in place of the # symbol.
- The command **`UsageResetType = #`** configures how long the Access Level usage will be Disabled for in terms of minutes (m/M), hours (h/H) or days (d/D). In the Access Level Commands, add this line with your required reset type in place of the # symbol.
- The command **`UsageResetPeriod = #`** configures the frequency on when the access level usage will be reset. In the Access Level Commands, add this line with your required value reset period in place of the # symbol.

Door Type Override in Access Levels

A new feature has been added to the system to allow a given Access Level to override the Door Type. The Doors in the Access Level will all use the Door Type specified in the Access Level, instead of the Door Type specified in the Door. This allows certain User or groups of Users to, for example only require a PIN at a door that would normally require Card and PIN.

- To enable this functionality, enter **`AllowOverrideDoorType = true`** into the Access Level Commands.
- The command **`OverrideDoorType = #`** can then be added to Door Type Commands. This specifies the Door Type to be used as the overriding Door Type.

Sequential Access Level Output Activation

Access Level Outputs are typically used to activate a specific feature in the building for a User or group of Users. A new feature has been added to allow multiple Access Level Output activations from a single card swipe, as long as the Access Level Start and End Expiry times create a continuous time period. This feature can be used to enable a variety of booking system scenarios where a User may request multiple bookings for all or parts of a facility in the same day.

For more information on configuration and operation of this feature, please see the relevant Application Note available on the ICT Website (www.ict.co).

Feature Enhancements (2.08.0825)

The following enhancements have been made to existing features in this release:

Elevators

- The command `FloorAccessCheckCar = true` has been added to the Controller commands which allows Floor access to be granted based on all of the User's Access Levels, as well as the Elevator being used.

Inovonics Integration

- The Inovonics Integration can now associate low battery states for wireless devices with Trouble Inputs, as well as generating Events. For information on configuring the Trouble Inputs, please see the Inovonics Integration Module Installation Guide.

Access Level Outputs

- Currently active Access Level Outputs will now be turned off if the Access Level is removed from the User that activated the Output, or if the Expiry Time is updated to be outside the current time.

Issues Resolved (2.08.0825)

The following issues have been resolved in this release:

- Fixed an issue where a Report IP service that fails over IP and switches to PSTN for back-up would not correctly open the "Report IP reporting failure" trouble input.
- Fixed an issue where users with credential programming that varied greatly in length from the credentials of other users would not always be found when their credentials were submitted. This did not affect facility/card numbers or PINs, nor credentials of similar length.
- Fixed an issue where under certain conditions, if a user badged at a door to which they did not have access the controller would restart.
- Stay Arming from a keypad is now possible when Inputs have been bypassed.
- Resolved an issue with a 'Module requires an update' being generated incorrectly for Outputs and Inputs in a Cross Controller Configuration.
- Function Codes now work correctly when the Door Type has been set to Card and PIN.
- Modules are now able to register successfully behind the Module Network Repeater after it was previously registered directly with the controller (and vice versa).
- Schedules now work correctly for those that are valid across the midnight threshold.
- Inputs 9 through to 16 now working correctly for the F/2F module after performing a module update.
- Resolved an issue where processing a numeric credential greater than half the length defined in the Credential Type would cause a Controller restart.
- Over Current Trouble Input is no longer triggered incorrectly on the Single Door Controller with PoE.
- Feedback is now provided when a User fails to gain access after validating against the Fallback Door Type.
- The Inovonics Integration Module Input States are now being set correctly after a module update for the first 8 inputs.
- Valid Credentials are no longer interpreted as Raw Credential reads under certain conditions.

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