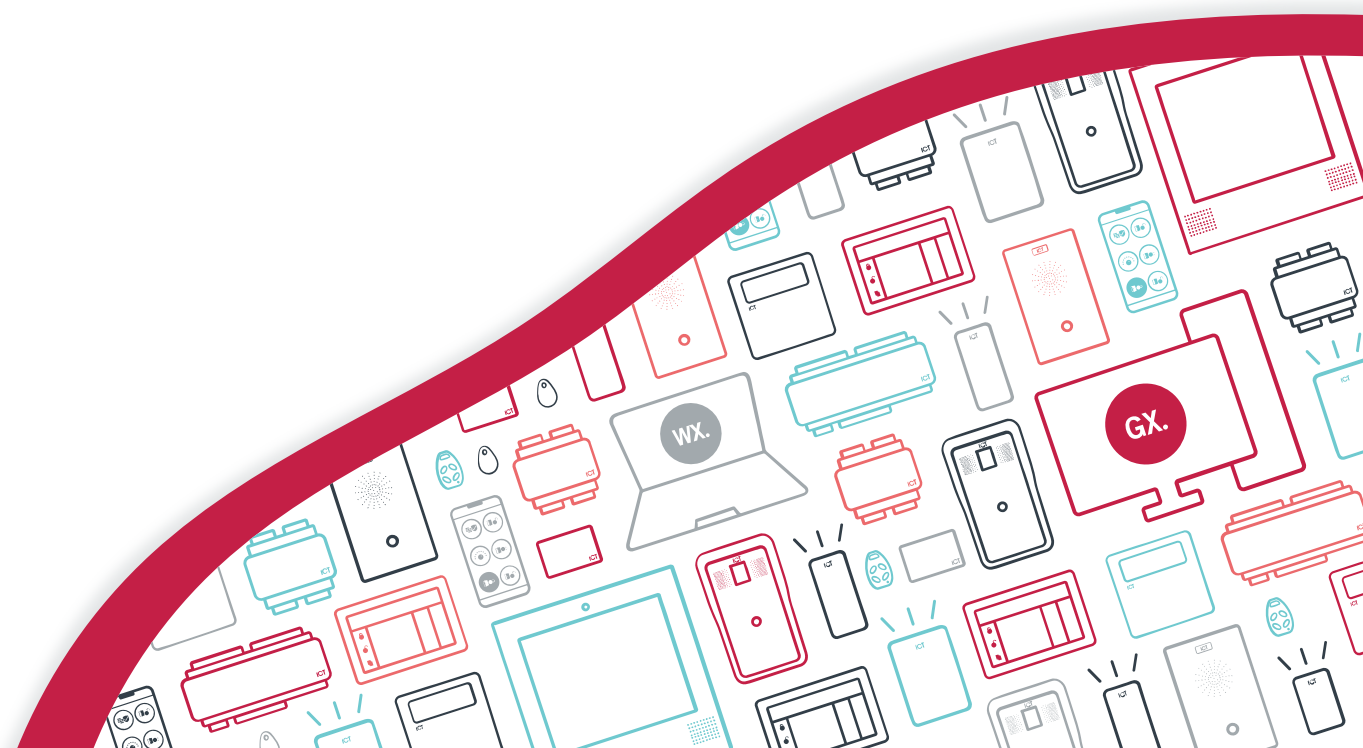
Integrated Control Technology

Protege GX Controller Firmware

Release Notes | Version 2.08.1487



Last Published: 16-Apr-25 3:38 PM

Contents

Introduction

This document provides information on the feature enhancements and resolved issues released with:

- Protege GX controller firmware version 2.08.1487

A full release history for previous versions is also included.

This firmware version includes changes to some reporting codes in the SIA L2 protocol (see page 8). If your site uses this reporting protocol, ensure that you contact your central monitoring station to make any required updates to automation mappings.

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 Controller 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.

Before Upgrading Firmware

- This process will take approximately 10 minutes per controller and it is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity. The controller will not be able to perform its normal function while firmware is being updated.
- Ensure that the controller does not lose power during the firmware upgrade process.
- Ensure that there is a stable network connection between the controller and the Protege GX server before you begin upgrading the firmware. If the network connection is unstable, we recommend upgrading locally from the controller's web 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.
- We strongly recommend having a technician on site during the firmware upgrade process to respond to any issues that might arise.

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

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

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 2.08.1487

New Features (2.08.1487)

The following new features have been included with this release.

Door Bypassing

It is now possible to bypass a door or virtual door, allowing the door position and bond sense inputs to be left open without triggering door forced or left open alarms. This is useful in situations where a door is broken and must be left open until it can be fixed.

- To bypass a door, enter the command **`Bypass = true`** in the door programming. This will bypass the inputs and prevent all door forced or left open alarms from that door. Remove this command or set it to **`false`** to remove the bypass.

  You must also remove the bypass from the inputs separately.

- To suppress door alarms from a specific input, enter the command **`InhibitBypassMode = true`** in the input programming. When you bypass this input, it will not trigger area alarms or door alarms.

Feature Enhancements (2.08.1487)

The following feature enhancement has been included with this release.

Site Code Mode

It is now possible to allow door access to any card with a correct site code, even if the user does not exist in the system or does not have access to that door. This can be used to temporarily loosen access restrictions on a room, such as for special events.

To program this feature:

1. Create a door type with the **Entry/Exit reading mode** set to Card only.
2. Enter the command **`SiteCodeModeList=x,y,z`**

   You can enter up to 8 site codes in a comma-separated list.

3. Assign the door type to a door, or set it as the **Secondary door type** for another door type to enable it on a schedule.

When a card with a matching site code is presented at the door, the door will unlock. You will receive a user event if the user exists in the system, or a REN and 'Read Raw Data' event if they do not.

Issues Resolved (2.08.1487)

The following issue was resolved with this release.

- Resolved an issue where ASCII credentials such as license plates received over the controller's ethernet connection were not processed correctly.
- Resolved an issue where output follows input control did not function unless the control area was armed. Now only the 24hr portion of the area needs to be armed to enable output control.
- Resolved an issue with custom EOL resistor configuration where the programmed hysteresis was not being used for controller inputs.
- Resolved an issue with the Allegion integration where the operation of the deadbolt was incorrect. Previously when the deadbolt was extended, all access was denied. Now access will be granted as normal, unless the lock is in privacy mode or apartment mode.

- Resolved an issue where the controller could not detect a SIM unless it was present in the cellular modem when the controller first started up. It is no longer necessary to restart the controller to detect the SIM.
- Resolved an issue where update point readers used for exit showed entry events.
- Resolved an issue where, if the controller had a custom HTTP port configured, it would revert back to port 80 when it was restarted, then back to the custom port the next time it restarted.
- Resolved an issue where assigning the same elevator car to two reader expanders generated a misleading health status message.
- Resolved an issue where OSDP readers in secure channel mode would periodically drop offline.
- Resolved an issue where the PRT-ZX8-DIN could report incorrect input states to the controller after a module update.
- Improved the resilience of the control port, TCP and UDP functions to denial of service.

SIA Protocol Updates (2.08.1487)

This firmware version includes corrections to some trouble alarm and restore codes in the SIA L2 protocol. If your site uses SIA L2 over phone or IP, you must contact your central monitoring station when you upgrade the controller firmware to update the required automation mappings.

The following alarm and restore codes have been updated:

Description	Trouble Input Address	New Alarm Code	New Restore Code
Bell Siren Tamper/Cut	Controller 9	YA	YH
PSU Module Tamper	Analog Expander 1	TA	TH
PSU Mains Failure	Analog Expander 2	AT	AR
PSU Battery Low/Missing	Analog Expander 3	YT	YR
PSU Module Offline	Analog Expander 8	EM	EN
Door Forced Open	Door 1	DF	DR
Door Left Open	Door 2	DM	DH
Door Duress	Door 8	HA	HH

In addition, this firmware version resolves an issue where trouble inputs configured to activate the normal area alarm (instead of the 24hr alarm) sent the incorrect alarm/restore codes. Now all alarm and restore codes are the same regardless of whether the normal alarm or the 24hr alarm is activated.

For more information about this reporting protocol and all alarm/restore codes, see Application Note 317: SIA L2 Reporting in Protege GX and Protege WX.

Known Issues (2.08.1487)

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

- When you upgrade from version 2.08.1378 or earlier to this version, OSDP readers using secure channel may drop offline. If you observe this issue, you must put the card readers into installation mode, then activate installation mode on each reader expander to re-establish the secure channel.

Previous Release History

Protege GX Controller Firmware 2.08.1453

Protege Wireless Lock Support

This Protege GX software and firmware release introduces support for Protege wireless locks operating in offline mode.

Offline wireless locks are an integrated part of your Protege GX security system, even with no active connection to the network. All access and event data is carried on user cards and mobile devices and periodically synchronized with Protege GX when the user badges at a wired update point reader such as the front door of the building.

Doors, door groups, schedules and holidays can be programmed in Protege GX as normal and transferred to the offline locks over Bluetooth® using the Protege Config App.

Offline Wireless Lock Features

- Control user access based on **access levels, doors, door groups, schedules and expiry dates**. All of this information is stored on the user's card or mobile phone when they badge at an update point reader, allowing the lock to make access decisions without input from the controller.
- **Events** from wireless locks are stored on user cards and uploaded to the system via the update point reader, allowing you to monitor and report on access events and the lock's battery status.
- Deleted cards and users are added to the **blocklist**, which is stored on all user cards and circulated to offline locks throughout the system. This reduces the chance that an unauthorized credential can be used to gain access at offline locks, even if that credential hasn't been updated at an update point reader yet.
- Offline locks support several convenient **operating modes**:
  - **Standard**: When you gain access, the door unlocks temporarily.
  - **Unlock on schedule**: The door unlocks based on a specific schedule (e.g. working hours). Optionally, you can enable 'late to open' operation, so that the lock will not unlock until the first user arrives in the morning.
  - **Office unlock**: Any authorized user can unlock the door temporarily, but specific users (e.g. managers) can unlock the door indefinitely by holding down the inside handle and presenting a credential to the reader. Repeat the process to relock the door.
  - **Toggle**: Whenever any authorized user accesses the door, the lock will toggle on/off.
  - **Exit leaves door unlocked**: When someone exits the door using the inside handle, it will remain unlocked. Depending on the settings, it will either lock again after a set length of time or remain unlocked until someone badges a card.
- The **Emergency Open** feature grants one-off access to unlock a door using the config app - perfect for helping a user who has locked themselves out.
- From the server to the lock, the offline wireless locking system is **end-to-end encrypted** using industry-standard encryption protocols.

See the Protege Wireless Lock Configuration Guide for all features, requirements and programming instructions for Protege wireless locks.

Issues Resolved (Controller Firmware 2.08.1453)

The following issues were resolved with this release.

- Resolved an issue where changing the access level's expiry time to a time before the present would not cause access level outputs to deactivate.
- Resolved an issue where the controller could not communicate with the ThyssenKrupp system over the onboard ethernet connection.

- Resolved an issue where gaining access via a PRT-TS35 would cause the controller to reboot.
- Resolved an issue where the keypad's Installer menu did not display the correct IP address of the controller.
- Resolved an issue with the KONE HLI integration where the call types programmed in Protege GX were not sent to the KONE system.

  If your site has an additional controller programmed with the Otis HLI integration as a workaround, this record can now be deleted. Ensure that the user records are programmed correctly for the KONE integration.
- Resolved an issue where the 4G modem could become stuck in the 'Not Registered - Seeking' state indefinitely.
- Resolved an issue with low level elevator integration where elevators would deny access to any credential programmed in the second row of access cards.
- Resolved an issue where custom HTTPS certificates with intermediate certificates could not be loaded onto the controller.
- Resolved an issue where controllers would fail to come back online with the Report IP server after a disconnection.
- Resolved an issue where the 'System Restarted' trouble input did not open after a system restart.
- Resolved an issue where there was no reader feedback when a user was denied access by interlock.
- Resolved an issue where controllers would not recognize door inputs on other controllers after a power cycle.

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.

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.

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