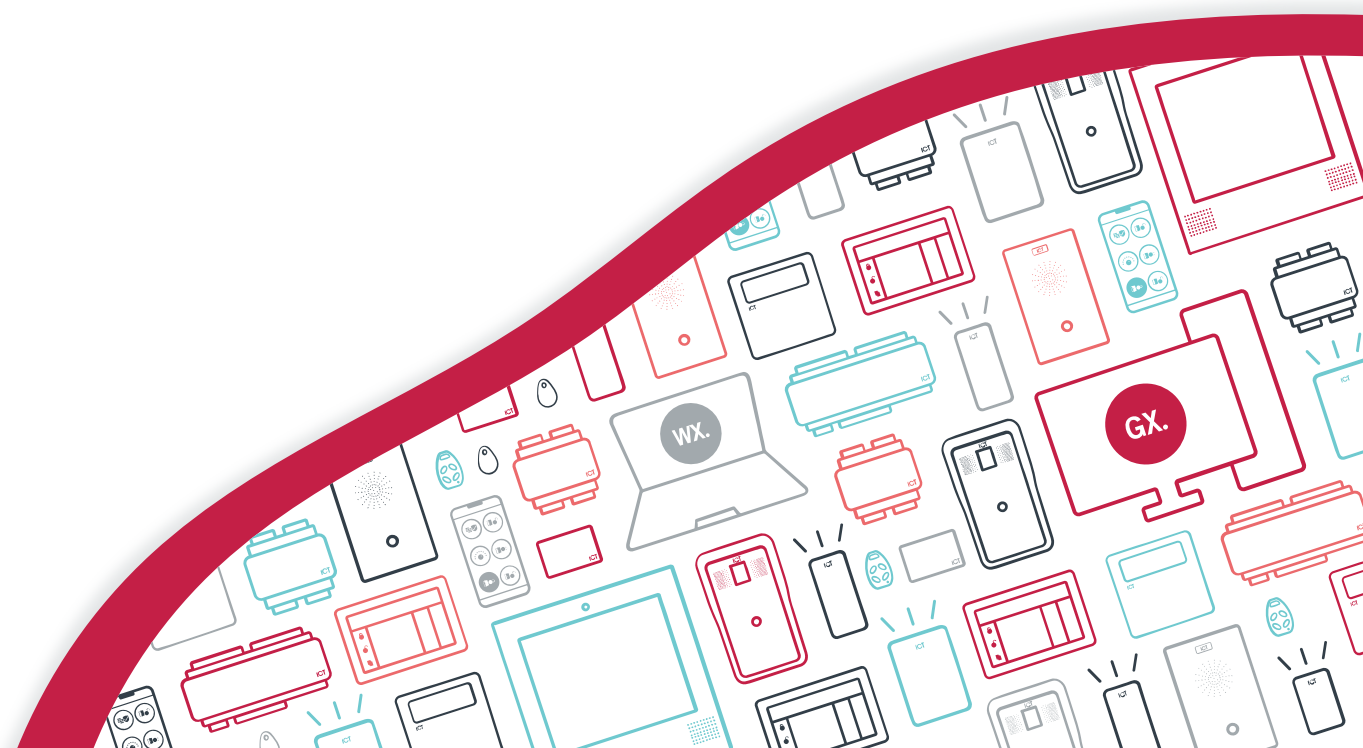
Integrated Control Technology

Protege GX Controller Firmware

Release Notes | Version 2.08.1543



Last Published: 08-Sep-25 10:02 AM

Contents

Introduction

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

- Protege GX controller firmware version 2.08.1543

A release history for previous versions is also included.

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 2.08.1543

New Features (2.08.1543)

The following new features have been included with this release.

USB Ethernet

You can now connect the controller's USB port to wired and wireless networks using a USB-Ethernet adapter. This alternative network connection is useful for:

- Backup reporting networks
- Remote access to the web interface

This feature has been validated with the following hardware:

- **USB-Ethernet Adapter**: The controller supports USB-Ethernet adapters with the following chipsets:
  - ASIX AX88772B1
  - ASIX AX88772C_xxxx

  ICT supplies the Protege USB-Ethernet Adapter, which can be purchased using the order code PRT-USB-ETH.
- **Mobile Internet Modem**: Validated with Teltonika RUT241 and RUT200 modules. ICT cannot guarantee functionality with other modems or network switches.

See the Protege GX Controller Configuration Guide for more information and instructions for setting up mobile internet.

Over-the-Network Firmware Updates for TSL Readers

You can now upgrade TSL readers over the network from the controller's web interface - no need to remove card readers from the wall, reconfigure the wiring or schedule downtime. Card readers continue to operate normally through almost the entire upgrade process, only rebooting quickly at the end to implement the new firmware.

To view the card readers that are available to update, log in to the controller's web interface, navigate to **Application Software** and open the **Module** dropdown. The controller will display all card readers connected by ICT RS-485 or OSDP. Select an available reader and upload a firmware file to upgrade it.

Although tSec readers do not support over-the-network updates, you can now view their serial numbers and current firmware versions in the **Module** dropdown as well.

This feature requires the following firmware versions:

Component	Minimum Firmware Version
Protege GX Controller	2.08.1498
Protege WX Controller	4.00.2261
Reader Expander	1.12.605
TSL Reader	1.05.382

Readers connected by Wiegand cannot be displayed or updated over the network.

If the reader expander's address has changed since it was connected to the network, you must power cycle the reader expander before the card readers will appear in the web interface. This is a known issue that will be resolved in a later release.

Enterprise Download Server Support

This version of the Protege GX firmware supports the Protege GX Enterprise Download Server. The enterprise download server is an efficient and scalable solution for downloading programming to controllers in medium and large Protege GX systems. It is built with enterprise-scale platforms and architecture, offering massive improvements over the standard download service in terms of speed and capacity.

The enterprise download server is a forthcoming feature that is still in development. For more information, get in touch with ICT.

Feature Enhancements (2.08.1543)

The following feature enhancement has been included with this release.

Power Supply Support

This version of Protege GX supports two new power supply modules that are forthcoming from ICT.

- PRT-PSU-DIN-5A: ProtegeDIN Rail 5A Intelligent Power Supply
- PRT-PSU-DIN-10A: ProtegeDIN Rail 10A Intelligent Power Supply

To support the new power supplies, you must also upgrade Protege GX to version 4.3.390 or higher.

Access Denied Events

Previously, some types of 'Access Denied' events displayed the reader expander port where access was denied instead of the door. These now display the door's name and Database ID, making it easier for operations teams to understand where the incident occurred.

The updated events now display the following text:

- User Jane Smith (UN175) Record Expired At Door Front Door (DR12)
- User Jane Smith (UN175) Record Expired At Door Front Door (DR12) Using Credentials 100:4306
- User Jane Smith (UN175) Record Disabled At Door Front Door (DR12)
- User Jane Smith (UN175) Record Disabled At Door Front Door (DR12) Using Credentials 100:4306
- User INVALID USER PIN Not Valid at Door Front Door (DR12)

You must add the new events to your **event filters** to ensure that they appear in relevant event reports and status pages. After upgrading to this version, navigate to **Events | Event filters** and add the new events to any event filters that contain the 'Record Expired', 'Record Disabled' or 'PIN Not Valid' events.

To receive these new events, you must also upgrade Protege GX to version 4.3.390 or higher. If either the software or the controller does not support the new events, you will continue to receive the existing events.

In addition, the 'Door Unlocked by Access' event is no longer generated by default each time the door is unlocked. Suppressing this event saves event storage, especially on busy sites.

If you wish to re-enable this event, enter the following command in **Sites | Controllers | General**:
`EnableUnlockByAccessEvent = true`

Issues Resolved (2.08.1543)

The following issues were resolved with this release.

- Resolved an issue where the **Allow reading opened/unlocked** setting did not work when using credential types instead of cards.
- Resolved an issue where the **Door REX not allowed** setting in the door type did not override free egress operation. Now when REX is disabled in the door type and the door programming, the door does not provide free egress and will raise a 'Door Forced' alarm if forced open.

- Resolved an issue where the REN input did not consistently trigger a request to enter. This could cause issues with unlocking doors from intercoms.
- Resolved an issue where cards that did not match a card profile could not gain access at update point readers.
- Resolved an issue where access levels with more than 255 doors or door groups assigned to them were not correctly downloaded to the controller by the standard Protege GX Download Service.

  This does not resolve download capacity issues when using the single record download service. If you experience these issues, we recommend that you upgrade to this firmware version **and** deactivate access level downloads in the single record download service. See Application Note 309: Single Record Downloads in Protege GX for instructions. This issue does not affect the enterprise download server.
- Removed a session hijacking vulnerability from the controller's web interface.
- Resolved an issue where the area count was not being incremented for both dual authentication users when both `CustodyPairEnforced` and `AreaCountOnDoorOpening` commands were in use.
- Resolved an issue where OSDP card readers using secure channel could drop offline after a controller firmware upgrade.
- Resolved an issue where bypass messages on the keypad could prevent other messages, such as time and attendance, from being displayed.
- It is now possible to disable privacy mode on Allegion locks, preventing users from locking themselves out. To achieve this, enter the following command in the smart reader programming:

  ```
  DisablePrivacyMode = true
  ```
- When an operator changes their password in the web interface, now all concurrent sessions are logged out instead of just the session where the password was changed.
- Improved the stability of OSDP secure sessions with third-party readers.
- Resolved an issue where it was not possible to force a firmware update from the controller to modules with addresses above 32.
- Resolved an issue where Any Bit (Raw) credentials were not processed correctly.
- Resolved an issue where manual command events sometimes displayed the wrong Operator ID.
- Resolved an issue where controllers using NTP could experience time skips, potentially missing schedule changes. This could cause doors to stay locked or unlocked even when the schedule changed.
- Changed how controllers in cross controller systems synchronize times. Previously, all linked controllers would send time updates to each other, causing time skips. Now only controllers connected to NTP servers will send time updates, and only controller without NTP servers will accept updates.
- Resolved an issue where wireless doors connected to an Aperio IP hub would not unlock after granting access.
- Resolved an issue where controllers using DHCP could fail to come back online after the DHCP server dropped and then recovered.
- Resolved an issue with the KONE integration where events from KSP833 DOPs did not show the correct destination floor. If your site uses KSP833s, add the following command in **Sites | Controllers**:

  ```
  KoneKSP833Present = true
  ```
- Resolved a memory leak that could cause controllers using the single record download service to restart unexpectedly.
- Resolved an issue where some users could temporarily be lost from the controller's database if a download failed halfway through. This could cause unexpected failed card reads with 'Read Raw Data' events.

Input Controls Output Changes

Resolved an issue where it was not possible to disable output control by disarming an area. The behavior for inputs controlling outputs is now consistent, as follows:

- **Input controls output**: Both the 24hr area and main area must be armed to control the output. Disarm the area to disable the output control.
- **Input type controls output**: Both the 24hr area and main area must be armed to control the output. Disarm the area to disable the output control.

- **Twenty four hour panic input**: When this setting is enabled, only the 24hr area needs to be armed to control the output.

We recommend assigning all inputs that control outputs to a dedicated control area that can be armed and disarmed as required.

Previous Release History

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.

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.

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