Integrated Control Technology

Protege WX

Release Notes | Version 4.00.2510

Last Published: 08-Sep-25 10:05 AM

Contents

Introduction

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

- Protege WX version 4.00.2510

A release history for previous versions is also included.

This firmware version includes changes to some reporting codes in the SIA L2 protocol (see page 9). 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 update is supported in the following Protege WX controller modules:

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

Older Controller Limitation

Controller models without physical USB ports do not support this firmware version. If your controllers do not have USB ports, **do not upgrade the firmware to this version**. Instead, use the long term support release version, available from the ICT website.

If you need help determining the hardware type of your controllers, contact ICT support with a list of controller serial numbers.

Upgrading to the Latest Version

Before Upgrading Firmware

- This process will take approximately 10 minutes and the controller will not be able to perform its normal functions during this period. It is recommended that firmware updates are performed when the site is closed for maintenance or at times of low activity.
- Ensure that the controller does not lose power during the firmware upgrade process.
- Ensure that there is a stable network connection to the web interface before you begin uploading the firmware.
- 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.

Upgrade Firmware

1. From the main menu, select **System | Application Software**. This page provides details about the current Protege WX version that is installed.
2. Click the **Choose File** button and browse to the supplied update file.

3. Click **Upload** to commence the upgrade procedure.
4. The controller will automatically create a backup of the programming. Depending on your browser settings you may be prompted to save the file. Otherwise, it is downloaded automatically to your **Downloads** folder.
5. Progress is shown as the new application software is installed. The controller then restarts.
6. After the upgrade is complete, log on to the controller to review and resolve any health status messages to resume normal operation. You may need to perform module updates, re-arm areas and re-enable the 24HR portions, and start services and programmable functions.

Version 4.00.2510

New Features (4.00.2510)

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 WX 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 **System | 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.

Door Bypassing

It is now possible to bypass a door or virtual door, allowing the door 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 bypass a specific door or bond sense input, enter the command `InhibitBypassMode = true` in the input programming, then send a **Bypass** command. This will prevent that input from triggering door alarms while it is bypassed.

Feature Enhancements (4.00.2510)

The following enhancements have been made to existing features in 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: Protege DIN Rail 5A Intelligent Power Supply
- PRT-PSU-DIN-10A: Protege DIN Rail 10A Intelligent Power Supply

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

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 **System | Settings | General**:

```
EnableUnlockByAccessEvent = true
```

In addition, the maximum length of event descriptions has been extended to 1024 characters.

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 (4.00.2510)

The following issues were resolved with this release.

- Resolved an issue where the Report IP service would not successfully reconnect to the primary reporting channel after a connection issue was resolved.
- 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 no events were recorded when an operator instant force armed or instant stay armed an area.
- 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 events were not displayed in Swedish.
- 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, 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 adding a card to a user record from the event log could overwrite the user's PIN code.
- Resolved an issue with Protege X where the controller would fall back to 4G after losing ethernet connection, but would not return to the primary channel when ethernet connection was restored.
- 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.
- Resolved an issue where the **Door Extended Access Time** was set to 0 by default. This is now set to 10 seconds by default for new doors (existing doors are not affected).
- Improved the resilience of the TCP and UDP functions to denial of service.
- 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 the live events page (**Monitoring | Events**) could fail to export events spanning multiple months.
- 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 the user count for areas would be lost when the firmware was updated.
- 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.
- When a user is denied exit due to not having the correct credential type, the event now displays "Waiting for credential" instead of "Waiting for bio". In addition, this type of event now includes the phrase "User Denied Entry/Exit".
- 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.
- Resolved an issue where wireless doors connected to an Aperio IP hub would not unlock after granting access.
- Resolved an issue where users created by the users wizard had their Reporting IDs set to 0 instead of the next sequential ID.
- Resolved an issue where controllers using DHCP could fail to come back online after the DHCP server dropped and then recovered.
- Resolved a memory leak that occurred when the controller received API requests with strings longer than the maximum supported length. This could cause the controller to restart.
- Resolved an issue where OSDP readers would drop offline after new expanders were added via the Expanders Wizard.

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.

SIA Protocol Updates

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

Description	Trouble Input Address	New Alarm Code	New Restore Code
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 WX DLL API Updates

String Lengths

The API now rejects any new records or updates containing strings that are more than 50 characters long. It will return the following error message: "Command Failed (18) Submitted record name is too long."

The exceptions to this rule are as follows:

- User names (**First Name**, **Last Name** and **Display Name**) are capped at 32 characters. This is due to memory considerations on sites with large numbers of users.
- Custom credential definitions (e.g. Wiegand formats) have no length limits, as these typically exceed 50 characters.
- Commands have no length limits, as a single record may need multiple commands.
- The bulk user submission feature does not apply any length limits. However, if a user record created by bulk submission has a name that is too long, any further changes to that record will be rejected until a shorter name is submitted.

Event Length

The maximum event length returned by the API (and displayed in the Protege WX UI) has been extended to 1024 characters.

Previous Release History

Version 4.00.1969

Cybersecurity Enhancements (4.00.1969)

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

- 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 are using the Protege Mobile App to monitor and control the Protege WX system, you must upgrade your mobile app to version 1.0.9. Earlier mobile app versions will no longer connect to the controller.
- 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.
- Direct camera monitoring is not compatible with the cybersecurity improvements and has been removed from Protege WX in this release. If you need to use direct camera integration, you must remain on the previous Protege WX release.
- This release introduces a new help documentation format which is compatible with the cybersecurity restrictions. Now when you click the **Help** button:
  - If the controller has access to the internet, it will open the new Protege WX Online Help: https://doc.ict.co/wxhelp/index.htm.
    This online documentation offers improved navigation and search functionality and does not require a login, so you can bookmark this page for easy viewing on any device.
  - If the controller does not have access to the internet, it will open a PDF copy of the help documentation which is saved on the controller. This gives you all of the detailed information you need even when there is no internet access.
- There are some changes to the process of logging on with the Protege WX API. If you have an API integration, see the API documentation for more information on what needs to be updated.

Feature Enhancements (4.00.1969)

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

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.

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 272: Allegion Integration with Protege WX.

Issues Resolved (4.00.1969)

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 the controller's web interface would occasionally fail to load the users or events pages and redirect to the login screen.
- Resolved an issue where "Read Raw Credential Data" events with large credential bit counts would cause the controller to stop sending events over the API.

  > Any credential up to 200 bits long will be displayed with the correct bit pattern. However, note that events have a maximum length of 105 bits. Anything longer than that will be truncated.

- 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.
- 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 an issue where the central station report displayed all trouble inputs with an event code of 145. The report now displays the correct event codes (for example, the Module Offline trouble input now correctly uses event code 143).
- Resolved an issue where the User ID credential type was not automatically added when there was a large number of users.
- Resolved an issue where it was not possible to program a hostname for Report IP services.

- Resolved an issue where imported users could have undefined start and expiry dates.
- Resolved an issue where backing up very large databases would fail.
- 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.
- Resolved an issue where the controller could crash on start up when there was a large number of users with phonebook integration enabled.
- Resolved an issue where the offline menu did not show the correct IP address for the controller.
- Resolved an issue where new users added via the keypad always had their **Reporting ID** set to 0. Now they will correctly have the next available Reporting ID.
- Resolved an issue where the event incorrectly stated that an expired user had used a card to attempt access, when they had actually used a PIN.
- 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.

Protege X Updates (4.00.1969)

The following changes apply to controllers that are connected to Protege X:

- You can now easily pair a controller with Protege X using the new **Enable Cloud** checkbox in **System | Settings | General**. The **Status** field shows the current pairing status of the controller to help with troubleshooting any connection issues.
- Resolved an issue where controllers could not be registered or update their licenses after they were paired with Protege X.
- Resolved an issue where large records could block the controller's download queue, preventing it from receiving downloads.
- Resolved an issue where controllers could occasionally lose pairing with Protege X.

Version 4.00.1505

New Features (4.00.1505)

The following new features have been included with this release.

OSDP 2.2 Support

Protege WX now supports the OSDP 2.2 standard. This includes a number of changes which make setting up OSDP card readers quicker and easier.

- When you set the **Port 1/2 Network Type** of the reader expander to OSDP, the system automatically creates two smart readers to represent the entry and exit readers connected to that reader port.
- 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 select the reader expander record then click the **OSDP Install Mode** icon in the toolbar. 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.
- ICT 485 smart reader licenses are no longer required to connect OSDP readers.
- 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.

Feature Enhancements (4.00.1505)

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 (4.00.1505)

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 272: Allegion Integration with Protege WX.
- 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 where the clickable area of some buttons was smaller than the visual size of the button.
- 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.
- Resolved an issue where it was not possible to create trouble inputs for modules with an address above 32.
- Resolved an issue where, when the operator's language was set to a language other than English, the final user in the user list was not displayed.
- Introduced a number of performance improvements to the controller firmware, which will mitigate timing issues on sites with large numbers of modules.

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

Version 4.00.1234

New Features (4.00.1234)

The following new features have been included with this release.

Aperio IP Multi-Hub Integration

Protege WX 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 344: Protege WX Aperio IP Hub Integration.

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 users with the extended door access function enabled, allowing you to limit 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.

For more information and programming instructions, see Application Note 336: Programming Function Outputs in Protege GX and Protege WX.

Feature Enhancements (4.00.1234)

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

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 supported 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.

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

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

  ```
  UnattendedForceArm = true
  ```

Firmware Upgrade

- Protege WX now automatically creates and downloads a backup of the programming when you trigger a firmware upgrade.

Issues Resolved (4.00.1234)

The following issues were resolved with this release.

- Resolved an issue where inputs bypassed by a service generated a 'bypass restore' event instead of a 'bypass' event.
- Resolved several buffer overflow vulnerabilities.
- Resolved an issue where session IDs were not sufficiently random.
- Resolved an issue where hashed operator passwords could potentially be exposed.
- Resolved an issue where some drop downs in the access levels programming were not expanding to fill the page.
- Resolved an issue where the **Test Report Time** and **Automatic Offline Time** could not be set to PM values.
- Resolved an issue where saving a user record using an operator without permission to view PINs would cause the PIN to become blank.
- Resolved an issue where reader expanders would not recognize alternative PIN formats when credential types were in use.
- Resolved an issue where the admin operator would not be restored correctly when the controller was defaulted.
- Resolved an issue where the controller displayed noon/12PM as 0PM when 12 hour time was in use.
- Resolved an issue where the PIN expiry field could not be updated by operators without permission to view PINs.
- 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.

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

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.