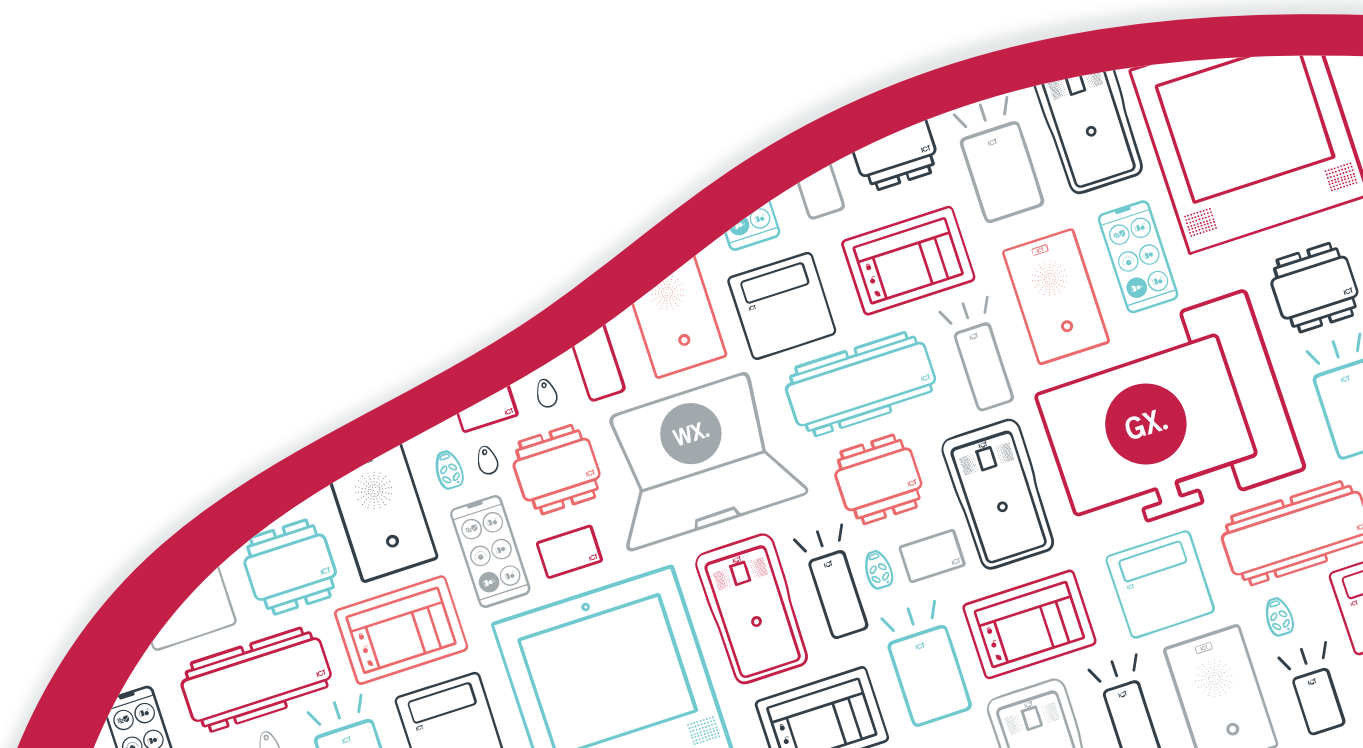
Integrated Control Technology

Protege WX

Release Notes | Version 4.00.1505



Last Published: 27-Apr-23 3:07 PM

Contents

Introduction

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

- Protege WX version 4.00.1505

A full release history for previous versions is also included.

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

Due to technological limitations, some 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 **4.00.427**. 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 to the Latest Version

Controllers do not support defaulting and firmware upgrade at the same time. Before you upgrade the controller firmware, ensure that the wire link used to default the controller is **not** connected.

1. 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.

   This process can take up to 5 minutes to complete, so we recommend that upgrades 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 being upgraded.
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 4.00.1505

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.

Known Issues (4.00.1505)

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.

Previous Release History

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.

Version 4.00.1096

New Features (4.00.1096)

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.

- 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 and connecting locations which do not have wired internet access.
- 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.

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

Feature Enhancements (4.00.1096)

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

EOL Resistor Programming

- Added support for input doubling using 3 resistor EOL configuration 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.

Protege WX only supports up to 16 inputs on any one module, regardless of whether input doubling is configured. This is a known issue.

Cybersecurity

- The **Show PIN Numbers for Users** option is now disabled by default for the Installer and Master roles.

  The roles will not be altered when the firmware is upgraded. When the controller is defaulted this option will be disabled.

Issues Resolved (4.00.1096)

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.

- 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 where the **Display Site Name** option on the **License Update** page did not function. Now the site name will be displayed in the top right of the UI.
- Resolved an issue where the elevator and floor record names were not limited to 50 characters.
- Resolved an issue where access levels with large numbers of doors and schedules assigned would respond slowly in the UI.
- Resolved an issue where selecting and editing multiple inputs could cause their names to revert to the default names.
- Resolved an issue where event reports did not handle time picking correctly when the system was set to 24 hour time.
- Resolved a textual issue in the **Channel 1/2/3/4 Update Time** fields in the analog expander programming.

Version 4.00.965

Issues Resolved (4.00.965)

The following issues were resolved with this release.

- Resolved a regression where changes to a user's access levels would not be saved if an access level assigned to that user had previously been deleted.

Version 4.00.938

Feature Enhancements (4.00.938)

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

Cybersecurity Enhancements

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

Issues Resolved (4.00.938)

The following issues were resolved with this release.

- Resolved an issue where controller models without USB ports could not be updated past version 4.00.840.

  Some older controllers are still not compatible with current firmware. Ensure that your controller is compatible before upgrading (see page 6).

- 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 where areas would not arm correctly on schedule when successive days ending in midnight in the same period were checked.
- Resolved an issue where the date/time picker displayed 12-hour time even when the browser's location settings specified 24-hour time.
- Resolved an issue where invalid date formats in a user import CSV were not handled correctly in the user expiry fields, resulting in those fields becoming uneditable.
- Resolved an issue where the access control wizard would hang endlessly when attempting to rename the maximum number of doors (128).

- Resolved an issue where the ellipsis button next to the **Alarm Operating Schedule** fields for door left open and door forced open did not link to the correct page.
- Resolved an issue where the output's 'activate timed' feature displayed the time of day instead of length of time to activate.
- 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.

Known Issues (4.00.938)

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.
- When an access level is deleted, any user that has that access level assigned when it is deleted will be unable to have any other access level added to the user record. This can be prevented by removing the access level from all associated user records **before deleting the access level**.

Version 4.00.864

New Features (4.00.864)

The following new features have been added in this release.

Controller Default Security Upgrades

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

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

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

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

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

PIN Security Enhancements

Site security enhancements provide greater control over the PIN codes available to users, and enable sites to require dual credentials (PIN and User ID) to authenticate users at the keypad. These options are available in the **System | Settings | Security Enhancement** tab, allowing you to configure the following:

- Require each user to enter a unique User ID as well as their PIN when they log in to a keypad. The User ID field is added to all new and existing users, and can be populated with unique values by the operator.
- Force users to set their own PIN the first time they use a keypad, so that only the user knows their permanent PIN.
- Set default PIN expiry periods to ensure that user PINs are changed regularly.
- Set complexity requirements for PINs, such as minimum length, maximum sequential digits and maximum repeated digits.

This feature is only available in Advanced mode.

Editing User Records from a Keypad

This release adds the ability to create and edit user records from a Protege keypad, increasing convenience for installers and end users on site.

- Modify existing user records. You can configure the following:
  - Name
  - Default language
  - The first facility and card number
  - The first assigned access level
  - PIN number
  - User ID (if site security enhancements are in use)
  - Many useful options from the **Options** tab, such as **User Has Super Rights And Can Override Antipassback** and **User Operates Extended Door Access Function**.
- Create new blank user records and configure them immediately for use.
- Delete obsolete user records.

Access to edit user records from the keypad is restricted to users with the **User (2)** option enabled in the **Menu Groups** programming and the **User Can Edit User Settings from Keypad** option enabled in **Users | Users | Options**.

For more information, see the relevant keypad user manual.

User Interface Improvements

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

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

Alternative REX Input

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

Aperio Integration: Privacy Mode

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

Ask for Defer Time

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

HTTPS Support

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

For more information on configuration and operation of this feature, please see Application Note 280: Configuring HTTPS Connection to the Controller Web Interface.

Offline Access to Input Status at Keypad

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

Area Status - Visual Feedback

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

  Note: This feature requires card readers with RGB LEDs.

For more information on configuration and operation of this feature, please see Application Note 271: Configuring Area Status LED Functions.

Expander Module Support

- Added support for the 2nd generation of intercom modules.

Feature Enhancements (4.00.864)

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

Password Policy Violation Messages

- Detailed messages have been added to the password creation process which inform operators specifically which configuration parameter(s) have not been met.

Allegion LE and NDE Networked Wireless Locks Support

- The Allegion integration has been extended to support Allegion LE and NDE wireless locks and the associated GWE ENGAGE Gateway modules. For more information, see AN-272: Allegion Integration with Protege WX.

Smart Reader Custom Credentials

- Added the ability to select custom credentials in the reader formats for smart readers.

All Users Antipassback Reset

- This firmware version introduces the ability to rest the antipassback status for all users. This function is performed through the Protege WX API. For more information, see the Protege WX API documentation.

Area User Count

- Added a new **Area Count on Door Opening** option. 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 AN-205: Area Counting.

- This firmware version introduces the ability to view the user count for an area. The **Enable User Counting** option needs to be enabled for each required area, and the current user count can then be viewed through the Protege WX API area status codes.

Expanders Wizard

- Added the ability to select the **Port 1 Network Type**, **Port 2 Network Type** and **Ethernet** settings when creating a reader expander.

OSDP Readers

- Added OSDP as a **Port 1/2 Network Type** option in the reader expander programming.

Door Alarm Options

- Added a new **Alarm Options** tab to door programming to provide extended alarm options for pre-alarm, left open and forced open events.

  Pre-Alarm Options
  - Enable Pre-Alarm Alarms
  - Disable During Unlock Schedule
  - Disable During Manual Commands
  - Disable During Calendar Actions
  - Disable Whilst Unlocked By Area
  - Disable Whilst Unlocked by Programmable Function
  - Disable Whilst Unlocked by Fire Drop
  - Alarm Operating Schedule

  Left Open Options
  - Enable Left Open Alarms
  - Disable During Unlock Schedule
  - Disable During Manual Commands
  - Disable During Calendar Actions
  - Disable Whilst Unlocked By Area
  - Disable Whilst Unlocked by Programmable Function
  - Disable Whilst Unlocked by Fire Drop
  - Alarm Operating Schedule

  Forced Open Options
  - Enable Forced Open Alarms
  - Alarm Operating Schedule

Note: This tab replaces the **Enable Pre-Alarm Events** and **Enable Left Open Events** options, which have been removed from the **Options** tab.

For information about the above options and their operation, refer to the Protege WX Programming Reference.

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.

LED Color Support

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

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

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

  The following color codes are available:

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

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

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

Low Level Elevator Integration

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

Cybersecurity

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

Event Reports

- Improved the handling of event reports with large numbers of records. The event report page can now accept up to 1500 records, and gives a warning if more than that number is selected.

Limitations

- Protege WX is no longer limited to 128 records for area groups, door groups, output groups, keypad groups and menu groups.

Credential Types

- Added the ability to program HID 37-Bit Wiegand H10302 cards as a credential type. When creating a credential type, set the **Format** to Wiegand and enter the required **Wiegand or TLV Format**.

Door Forced Alarms

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

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

Aperio Integration

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

Expander Module Support

- The PRT-TS50 module can now be addressed as a keypad in Protege WX.
- Added support for updating the firmware of the PRT-TS50 module.

Reporting

- Added the ability to enable encryption for SIA over IP reporting.

Controller Network Security Enhancements

- Module comms UDP/TCP (9450) has been disabled by default. It can be re-enabled via controller commands:
  - `EnableModuleUDP = true`
  - `EnableModuleTCP = true`
- Touch screen comms UDP (9460) has been disabled by default. It can be re-enabled via controller commands:
  - `EnableTLCDCommsUDP = true`
- Ports 9470, 21000 and 21001 have been turned off for Protege WX.
- Ping has been disabled by default for the onboard ethernet connection. It can be re-enabled via controller commands:
  - `EnablePing = true`

  If you have any modules installed that utilize module comms (port 9450) or touch screen comms (port 9460) over ethernet you will need to add the above commands to the controller or it will not be able to communicate with these modules.

Doors

- The command `SlaveREX = true` has been added to the door commands. This will allow a slave door to follow its primary door whenever requests to exit/enter or manual commands are actioned on the primary, in addition to access granted actions.

Salto SALLIS Integration

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

Elevators

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

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

Allegion Integration

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

For more information on configuration and operation of this feature, please see Application Note 272: Allegion Integration with Protege WX.

Aperio Integration

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

Access Level Outputs

- Access level outputs can now be toggled between activations.

System Settings

- Added the ability to restart the controller from the web interface.

Programmable Functions

- Extended the maximum value configurable for 'Token Time' to be 65535 for elevator control.

Languages

- Updated translations for supported languages.

Issues Resolved (4.00.864)

The following issues were resolved with this release.

- Resolved an issue with credential events incorrectly displaying user PIN codes.
- Resolved an issue with the 'Credential Disabled' event referencing the incorrect user.
- Fixed the issue where the trouble input for tamper/missing was incorrectly triggering when a module update was performed on the onboard reader expander using ICT RS-485 readers.
- Resolved an issue with DDNS not working with No-IP.
- Resolved an issue where the controller would not start up correctly if the ethernet cable was disconnected on power up.
- Fixed an issue displaying duplicate areas when navigating through a keypad module's area group.
- Fixed an issue with card readers operating in RS-485 mode occasionally dropping offline when readers with different firmware versions were wired in a multiplexed configuration on the onboard reader expander.
- Fixed an issue with pre-alarm and left open events not being generated for the Allegion AD-Series integration.
- Fixed an issue with smart reader tamper, RF loss and low battery events being incorrectly generated for the Allegion AD-Series Integration.
- Fixed an issue with the low battery and tamper trouble inputs restoring incorrectly for the Allegion AD-Series Integration.
- Fixed an issue with REX/REN not working the first time after a controller restarts, if the **Invert REX** / **Invert REN** option is not enabled.
- Resolved an issue with 'Access Taken' and 'Access Not Taken' events not always displaying the correct user reference.
- Resolved an issue with user access level expiry not being observed when checking the user's access at a door.
- Fixed an issue with the elevator status list incorrectly processing the fifth elevator twice.
- Fixed a memory leak related to using the email on event functionality with a misconfigured email server.
- Fixed a regression which prevented the keypad login requires card functionality from working.
- Fixed an issue which could stop services from automatically restarting after a firmware update.
- Enhanced the firmware update process for modules to include support for PRT-HRDM-DIN, PRT-HZX16-DIN and PRT-HPX8-DIN.
- Fixed an issue where the Contact ID service would not restart correctly after a power cycle.
- Fixed an issue where not all **Misc Options** were being displayed for smart readers under the **Reader** tab.
- Resolved an issue where it was possible to create duplicate expanders using the expanders wizard.
- Resolved an issue where using the Enter key while naming an area group could produce an error.
- Fixed an issue with inputs incorrectly reporting 'Module Input already in use' under certain conditions.
- Resolved an issue with the web interface not displaying the correct **Module Type** for all controller inputs and outputs.
- Resolved an issue with the **Disable Green LED Processing** option being incorrectly hidden when a reader expander's reader port has been configured for ICT RS-485 mode.
- Corrected an issue with the welcome message not displaying correctly if the language is non-English.
- Fixed an issue with the change password functionality not working correctly when initiated from the Home page.

- Fixed an issue of incorrectly displaying a smart reader raw credential event instead of a reader expander raw credential event for Wiegand credentials on reader expanders.
- Fixed an issue where an area arming via user count reaching 0 would not display the correct door reference in the relevant events.
- Fixed an issue where if two card reads were received from the same port of the same reader expander in quick succession, the second card read would not be processed.
- Improved robustness of processing credential packets received on reader expanders configured using the Third Party Generic network type.
- Fixed an issue where using sequential credentials as fallback door types could lead to the controller crashing.
- Resolved an issue with 'Entry Granted' events being displayed when the reader port is configured as an exit.
- Fixed an issue with PRT-PSU-DIN-8A not displaying correctly in module addressing.
- Fixed an issue with the change password function on the Home page not working correctly.
- Resolved an issue with the **Events** tab on programming pages not listing the events in the correct chronological order.
- Improved the functionality of the Protege WX wizards so that they function effectively over slower connections (e.g. HTTPS connections). This resolved the following issues:
  - Resolved an issue where expander modules were not added correctly by the expanders wizard.
  - Resolved an issue where schedules and inputs were not created correctly by the security wizard.
- Fixed an issue with reader expanders incorrectly setting a door as forced open after a module update.
- Corrected an issue where configuring an input's EOL settings using commands could result in it flagging the module it is assigned to as requiring a module update after every download.
- Fixed an issue where custom credentials could not be presented out of sequence.
- Fixed an issue with the population of account number information in SIA/CID over IP poll messages.
- Fixed an inconsistency with the Aperio integration, so that now when the inside handle is turned only a REX event is generated without an unlock command, as the physical mechanism is internally handled by Aperio.
- Fixed an issue with the Allegion AD-series integration incorrectly sending through a locking packet when an invalid format card is presented.
- Fixed an issue with the Allegion AD-Series integration not correctly locking/unlocking via manual commands for any lock after the first eight that are linked to a PIM.
- Fixed an issue with the Allegion AD series integration not resetting the left open trouble input when the door closes.
- Fixed an issue with EOL thresholds not working for reader expanders beyond module address 8.
- Fixed an issue where the door lock output time was unexpectedly extended with dual credential access.
- Fixed an issue where the dual authentication output did not deactivate according to the specified timeout.
- Fixed an issue with detailed credential events not correctly displaying all credentials presented.
- Fixed an issue with REX and REN not being processed on the initial trigger following a restart of the controller.
- Improved security by removing the server name that is used when the web server generates HTTP response headers.
- Fixed an issue where card reader area status LEDs were not working when enhanced smart reader outputs were enabled.
- Fixed an issue where firmware could not be updated on controllers.
- Resolved an issue where setting daylight savings time could cause the controller's internal clock to regularly skip an additional hour ahead.
- Resolved an issue where the custom reader format tab was not available.
- Resolved an issue where the onboard reader expander's readers were not restoring beeper operations correctly after an access granted event.
- Resolved a reporting issue where, when the primary channel failed, the trouble input ReportIP Reporting Failure would not open after the message retry attempt limit was reached.
- Resolved an issue where the keypad options **Allow Area Group Selection Access** and **Allow 24Hr Area Access** were reversed in the UI.

- Resolved an issue where the CSV event export had corrupt and missing data.
- Resolved issues with handling of special characters in record names.
- Resolved an issue where the **Use DHCP** option was missing a checkbox.
- Resolved an issue where door lockdown could be overridden by an unlock schedule if a manual unlock command was sent while the schedule was valid.
- When changing a user's PIN from the keypad, there is now a check against existing user duress PINs when the **Treat User PIN Plus 1 as Duress** option is enabled.
- Resolved an issue where changing a user's PIN from the keypad caused the controller to restart.
- Resolved an issue where a keypad's firmware could not be updated if it did not have a corresponding module record configured.
- Resolved an issue where performing a module update after a firmware update caused an error to be displayed.
- Resolved an issue where elevator floors were not relocking after the **Unlock Access Time** had expired.
- Resolved an issue where authentication files loaded to the controller could not be validated by third-party certificate authorities.
- Resolved an issue where updating a user PIN from the keypad in a large database could cause the controller to restart.
- Resolved an issue where cards greater than 32 bits were being incorrectly truncated when presented at Aperio locks.
- Resolved an issue where the lockdown state of a door was not restored when the controller was restarted.
- Resolved an issue where the bulk user import allowed you to load more users than permitted by your licensing.
- Resolved an issue where a crash could occur when a user with more than 255 access levels was denied access at a door.
- Resolved an issue where the live events page did not load consistently.
- Resolved an issue where unassigned credential types appeared in the user records.
- Resolved an issue where searching the user list was not returning the correct users.
- Resolved issue where the credential types on the users page were not displayed correctly.
- Resolved an issue where the door states were not displayed on the door status page.
- Resolved an issue where outputs and doors could not be set on programmable functions.
- Resolved an issue where areas could not be created.
- Resolved an issue that was causing incorrect REX/REN detection when the controller powered up.
- Resolved an issue where, when Contact ID is used as a backup service to Report IP, the Contact ID service would not attempt to dial out after a power cycle.
- Resolved an issue where area status LED changes could cause the onboard reader's enhanced outputs to not reactivate correctly when the reader or controller was power cycled.
- Resolved an issue where area status LEDs were not controlled correctly when enhanced outputs were active.
- Resolved an issue where a card reader beeper could be deactivated by badging a card once at the exit reader or pressing a key on the keypad, without changing the status of the output in the system.

  Note: The fix requires the following command to be entered in the programming of each reader expander: `ForceRestoreBeeper=true`. This command causes the reader expander to reactivate the output regularly until it is legitimately deactivated.
- Resolved an issue where Wiegand readers connected to reader ports 1 and 2 and processing the same door did not synchronize their LED operation correctly. This caused the port 2 reader L2 to remain on for too long after repeated card badges.
- Resolved a reader expander LED glitch which occurred when the door relocked.
- Resolved an issue where area status LED functionality was not always respecting standard reader LED output activation.
- Resolved an issue where the RS-485 module network would reboot periodically after the controller was powered up without an ethernet connection.

- Resolved an issue where a controller would not successfully boot up on OS version 2.0.16 with the ethernet cable connected.
- Resolved an issue with RGB readers connected to the controller's onboard reader in RS-485 configuration. When the reader temporarily lost connection while the door was unlocked, upon reconnection the green LED was incorrectly stuck in the 'on' state. This was resolved for the case where the door's lock output was the Lock 1 output on the onboard reader expander.
- Resolved an issue with OSDP reader LEDs not synchronizing correctly during standard door operation when configured with custom color codes.
- Resolved an issue with credentials longer than 48 bits being truncated incorrectly when presented at ICT RS-485 or OSDP readers on the controller's onboard reader expander.
- Resolved an issue where the **Tamper Input if Module Offline** option did not work correctly.
- Fixed a regression where HTTPS would be disabled on controller startup.
- Resolved an issue which occurred when two ports of a reader expander were both set for card and PIN operation. If a card was badged at one reader and an incorrect PIN entered at the other, access would be denied on the first reader.
- Resolved an issue where a 'Read Control Error' could be generated if two packets were received from PIN pads on the same reader port in quick succession.
- Resolved an issue where an output that was turned 'off timed' would not return to the correct state if it was off before the command was received.
- Resolved an issue where controllers running the Allegion integration could enter a restart loop.
- Resolved an issue where Wiegand reader LEDs which were pulsing were not restored to the correct state after the door was unlocked.
- Resolved an issue where deleting a user incorrectly reset the next database ID to use for new records back to 0.
- Fixed the intelligent reader tamper functionality for OSDP and ICT RS485 readers to match behavior of Wiegand readers.
- Resolved an issue where reader expanders with an address of 1 would not appear in the module addressing window, preventing the address from being changed.
- Resolved an issue where the expanders wizard could create records with duplicate reporting IDs.
- Resolved an issue which prevented holiday groups from being updated and produced a 'Command Failed' error.
- Resolved an issue where multiplexed Wiegand exit 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 where arming with read and input 4/8 could not be done on the controller's onboard reader.
- Resolved an issue where system records could be deleted via the bulk user submission.
- Corrected licensing default settings for ICT RS485 readers.
- Addressed an issue which prevented adding more than 30 expanders through the expanders wizard.
- Resolved an issue where adding multiple expanders through the expanders wizard could result in duplication of records.
- Resolved an issue where the access control wizard required users to click **Save and Return to Menu** twice before saved changes were displayed.
- Resolved an issue where the security wizard did not correctly save all applied settings.
- Corrected an issue in the site security enhancements dual credential functionality where a user ID would not be automatically assigned to a user unless the **Allow Duplicate PIN** option was selected.
- Resolved an issue where entering 46 or more special characters in the name of some record types would cause other records to not be displayed correctly.
- Resolved an issue where the **Events** button on the door monitoring page did not display the correct information.

- Resolved an issue on the schedules page where times could not be entered via the keyboard.
- Resolved an issue where the **Reader Credential Types** tab in the smart reader programming did not display consistently.
- Resolved an issue where the user search filter did not appear in the light theme.
- Resolved an issue where the Refresh button on the daylight savings and camera programming pages did not work correctly.
- Resolved an issue where the schedule dropdown menus on the access level doors and floors tabs could not be selected in Microsoft Edge browsers.
- Fixed the security wizard to correctly close the 'Re-enabling 24hr' popup message and redirect to the home page.
- Resolved an issue where the **Module Type** field for trouble inputs, inputs and outputs could be incorrectly disabled when set to Controller.
- Restored the ability for the UI to update only the changed content in records as opposed to updating the complete record.

  Note: This functionality does not apply to user records.
- Addressed an issue where new smart reader records would be assigned an invalid record ID and fail to function when added manually after auto-generated smart readers are added.
- Improved the reliability of firmware updates over the web interface when using HTTPS on OS 2.0.20.
- Resolved an issue with record selections in the list view not highlighting correctly on initial page loading and when any record on the page has been updated.
- Corrected an error preventing users being added correctly from a read raw event.
- Addressed the health status text not being cleared after the controller's health status has been resolved.
- Addressed an issue where importing users via CSV takes an extremely long time.
- Addressed an issue where access levels were not correctly assigned when importing via CSV.
- Corrected an issue where deletion/update of multiple records did not work correctly.
- Reinstated the missing **Menu Group** dropdown list on the menu groups page.
- Resolved an issue where after restoring a database from an earlier version, new records could overwrite existing records.
- Resolved an issue where changing the **Physical Address** on an output expander could cause some fields to reset and an endless loading screen.
- Resolved an issue where smart reader records could be deleted when changes were made to the reader expander programming.
- Resolved an issue where operators could be saved with only spaces for the name or username.
- Resolved an issue where popup windows were not centered.
- Resolved an issue where restoring an older backup could result in the door alarm settings being changed.
- Fixed an issue where, when HTTPS was enabled, an HTTP connection could still be established on one randomly chosen port.
- Resolved an issue where the HTTP port for the controller's web interface could be set to 0 or other restricted ports. Added error messages to notify operators when the selected port is not valid.
- Resolved an issue where the Report IP service could become corrupted when saved.
- 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.
- 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 where the firmware could not be updated when 100,000 users were programmed on the controller.

- Resolved an issue where the event report did not display all events on the on-screen display.
- Corrected an issue in door monitoring which caused the Door Lockdown Deny Entry and Exit status to be displayed as undefined.
- Corrected the area programming **Arm/disarm schedule** default selection. It now displays **Always**, where previously it incorrectly displayed **-Not set-**.
- Addressed an issue which caused the door left open pre-alarm and alarm to trigger when a door was latched unlocked and held open.
- Corrected the intelligent tamper operation. It is now permanently enabled for RS-485 capable readers connected to the controller's onboard reader expander.
- Resolved an issue where updating settings for reporting services instead created an additional record.

  Note: To correct reporting service records affected by this issue, make and save a change to the original record, after the firmware has been updated.

- Resolved an issue where the **Always log input event** option for input types did not correctly follow the operating schedule configuration.
- Resolved an issue where some controller configurations could exhaust their HTTP connections.
- Resolved an issue where, after restoring a database from an earlier version, new records could overwrite existing records.
- Resolved an issue where PIN entry could grant access on a reader that did not initiate a card and PIN access sequence. This could occur if the door type was **Card+PIN** and a card was presented at the entry reader then a PIN entered at the exit reader, the door would unlock.
- Resolved a number of issues with schedules that cross over midnight.
- 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).
- Corrected an issue with alarm options for records not updating correctly after a firmware upgrade.
- Resolved an issue where record searches would fail when entering more than 32 characters in the search string.
- Resolved an issue where the onboard reader expander could fail to process raw read events for OSDP readers with certain formatting configurations.
- Corrected an issue where incorrect access denied events could be generated when the credential type being used for attempted access was not valid for the door type, and the event generated should be **Access Denied by Door Type**.
- Addressed an issue which prevented searching for users and operators that contain ampersand (&) and/or equals sign (=) in their name.
- Corrected the controller health status list displaying one item only.
- Addressed an issue where, when adding multiple new floors to a new access level, the floor schedule would be left empty instead of defaulting to Always.
- Resolved a problem with the events report not correctly displaying the prompt to load the next 1500 records.
- Corrected the user page not maintaining focus on the search record when clearing the search field.
- Resolved an issue in the expanders wizard where the duplicate address error would be displayed any time the physical address was set before the module type was selected.
- Resolved an issue in the expanders wizard where duplicate expander records could be created if the same module type records were added with the same physical address.
- Addressed an issue when using multi-select to update large numbers of output records, where the progress window could hang and the update would fail to complete.
- Corrected an issue with operators not being deleted correctly.
- Corrected expiry settings for default users, which were missing default values for expiry date and time.
- Resolved an interface issue which prevented adding floors to elevators.
- Resolved an issue which could cause the **Events** tab on the users page to become inaccessible.
- Resolved an issue which could cause additional characters to be added to the end of the names of expanders added through the expanders wizard.

- Corrected an issue which would prevent access to the **Credential Types** tab for a user if all credential types were deleted for that user.
- Resolved an issue where, when creating a new holiday group, holidays added to the group could not be deleted until the new holiday group was saved.
- Resolved an issue where it was not possible to select a secondary phone number while the phone number operating schedule was set to something other than Always.
- Corrected an issue where health status messages did not clear once the issue was resolved.
- Increased the speed of event report generation to resolve report failures when reporting on large numbers of records.
- Corrected an error which allowed users to be imported into the database with IDs lower than existing users and potentially overwrite existing users.
- Resolved an issue which prevented the email on event command from triggering on an area event after being saved to an input.
- Corrected a display issue when renaming multiple door records within the access control wizard, where Step 2 of the wizard displays only the first change.
- Corrected an issue when renaming schedules within the access control wizard, where not all changes would be saved.
- Addressed an issue that could cause the controller to crash when restoring a database where operators with very long names had been programmed.
- Resolved an issue which caused unaddressed modules to be forgotten by the controller if it was restarted, resulting in the modules themselves needing to be power-cycled to be recognized again.
- Resolved an issue which was exacerbating clock drift.
- Resolved an issue which caused the REX operation to be locked out for 255 seconds when older Protege WX databases were migrated to the latest build.

Known Issues (4.00.864)

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

- Preceding characters are not recognized in Unicode, UTF8, ASCII, Numeric or Hexadecimal credential types.
- Trailing characters are not recognized in Unicode, UTF8, ASCII, Numeric or Hexadecimal credential types.
- Prefixes are not recognized in Unicode, UTF8, ASCII, Numeric or Hexadecimal credential types.
- UTF8 and Hexadecimal credential types are not recognized when assigned to door types.

Version 4.00.359

New Features (4.00.359)

The following new features have been included in this release:

Localized Interface: Norwegian, Czech, Dutch and German

The user interface is now available in **Norwegian**, **Czech**, **Dutch** and **German.**

Feature Enhancements (4.00.359)

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

Doors

- The command `LockOutAttempts = #` configures the number of retries allowed for supplying credentials for authenticating a user, before triggering the Too Many Attempts trouble input. In the door commands, add this line with your required value of attempts in place of the # symbol.

- The command `AlwaysAllowREN = true` has been added to the door type commands which will allow a Request To Enter event to occur even if the door is open.

Input Expanders

- The expanders wizard now recognizes the PRT-HZX16-DIN.
- Input expanders can now be configured as virtual modules.

Reader Expanders

- The expanders wizard now recognizes the PRT-HRDM-DIN.
- Reader expanders can now be configured as virtual modules.

Output Expanders

- Output expanders can now be configured as virtual modules.

Issues Resolved (4.00.359)

The following issues have been resolved in this release:

- Resolved an issue with the controller being unable to communicate correctly with the Inovonics integration running module firmware of Build 21 and earlier
- Fixed issue with the reader expander wizard incorrectly setting the Reader 1 / Reader 2 tamper trouble input's Trouble Group and Trouble Group Options

Version 4.00.349

New Features (4.00.349)

The following new features have been included in this release:

Localized Interface: Swedish and Finnish

The user interface is now available in **Swedish** and **Finnish**.

Feature Enhancements (4.00.349)

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

Doors

- Doors can now be associated with a new trouble input, Door Duress, which is triggered when either a duress user's PIN or when a duress PIN code has been entered into the reader at the door.
- The command `DualCredPendingTime = #` configures the timeout for supplying credentials for authenticating a user, such as Card and PIN. In the Door commands, add this line with your required value of timeout in place of the # symbol.

Keypads

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

Inovonics Integration

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

Services

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

Dual Custody

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

Access Level Outputs

- Access level outputs can now be activated when the reader port operates under Area Control mode.

Issues Resolved (4.00.349)

The following issues have been resolved in this release:

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

Version 4.00.331

New Features (4.00.331)

The following new features have been included in this release:

Card Usage Counting for Access Limits

User cards can now be limited to a certain number of access granted swipes for a particular time period. This can be used to enable scenarios such as cafeteria line access or clubroom access based on membership policies. The command `LimitUsage = true` has been added to the access level commands to enable this functionality.

- The command `UsesBeforeDisable = #` has been added to the access level commands which configures the number of uses for the access level before it is disabled.
- The command `UsageResetType = #` has been added to the access level commands which configures how long the access level usage will be disabled for in either minutes (m/M), hours (h/H) or days (d/D).
- The command `UsageResetPeriod = #` has been added to the access level commands which configures the frequency that the access level usage will be reset.

This feature is only available in Advanced mode.

Sequential Access Level Output Activation

Access level outputs are typically used to activate a specific feature in the building for a user or group of users. A new feature has been added to allow multiple access level output activations from a single card swipe, as long as the access level start and end expiry times create a continuous time period. This feature can be used to enable a variety of booking system scenarios where a user may request multiple bookings for all or parts of a facility in the same day.

This feature is only available in Advanced mode.

For more information on this feature please see the Configuring Sequential Access Level Output Activation in Protege WX application note on the ICT Website (www.ict.co).

Automatically Purging Events

Added a new **Purge Old Events** option (System | Settings | Options) that causes all events older than a specified number of days (14 days by default) to be deleted from the event log. This is required by local legislation in some countries.

User Access Level Schedule

Schedules can now be added directly to the Access Level assigned to the User and can be configured from Users | Users | Access Levels.

This feature provides flexibility for Users that require the access to the same doors within a selected access level, but at different times of the day or week.

Graphical Door Display

You can now view a graphical display of door access rights per user.

Feature Enhancements (4.00.331)

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

- Added functionality/support for advanced encryption between the card readers and the onboard reader expander (requires compatible card reader firmware).
- Added support for card formats other than 26/34 bits when read with card readers in ICT RS-485 mode (requires compatible reader expander 485 firmware).
- The command `RecycleDoorTimeOnAccess = true` has been added to the door commands which gives the ability to recycle door lock activation time upon generation of access granted events.
- The command `NoAccessEventsIfUnlocked = true` has been added to the door commands which gives the ability to suppress access granted events generated whilst door is still unlocked.

Aperio Integration

- Added ability to generate the Low Battery and the Comms Offline trouble inputs for Aperio locks.
  For more information on configuring trouble inputs please see the Configuring Aperio Integration in Protege WX application note on the ICT Website (www.ict.co).
- Added ability to handle deadbolt state changes for Aperio locks.

Keypads

- The command `ConfidentialMode = true` has been added to the Keypad commands which allows confidentiality mode to be enabled for Touch Sense LCD Keypads.

Elevators

- The command `FloorAccessCheckCar = true` has been added to the controller commands which allows floor access to granted based on all of the user's access levels, as well as the elevator being used.

Inovonics Integration

- The Inovonics Integration can now associate low battery states for wireless devices with trouble inputs, as well as generating events. For information on configuring the trouble inputs, please see the Inovonics Wireless Receiver Module Installation Manual.
- Updated the CID code to be sent for low battery and poll failures reported for Inovonics Wireless Receiver Modules.

Access Level Outputs

- Currently active access level outputs will now be turned off if the access level is removed from the user that activated the output, or if the expiry time is updated to be outside the current time.

Issues Resolved (4.00.331)

The following issues have been resolved in this release:

- Resolved issue with multiple events being generated incorrectly when an area has been configured with a ready output group.
- Fixed issue with defer automatic arming and rearming not working with open, bypassed inputs.
- Fixed issue with clearing lockdown on a door with a valid schedule that does not restore the door to its expected Unlocked By Schedule state.
- Corrected an issue with the **All Elevators** option within access level incorrectly granting access to all doors under some circumstances.
- Fixed issue with credential event strings not displaying the correct credential used when the user has multiple credentials of the same type and is using multiple credential types to gain access to a door.
- Fixed issue with the ready output not working correctly for open inputs configured for **Exit Alley Input Do Not Test It**.
- Fixed issue with the ready output functionality not generating the correct output events and using the appropriate output activation time set.
- Resolved an issue with schedule checking not working correctly for end times set to 00:00.
- Fixed an issue where the Report IP service would stop if the **Time Before Switching to Backup** option was set to zero.
- Fixed issue with lock activation glitch (unlock then immediately relocking) when the door is associated with an armed area.
- Updated the handling of Inovonics Wireless Receiver Module so that a hardware tamper will result in all inputs from the associated remote device being set to the TAMPER state.
- Improved synchronization of input states when a module update is performed on the Inovonics Wireless Receiver Module or new inputs have been added to the programming.
- Stay arming from a keypad is now possible when inputs have been bypassed.
- Modules are now able to register successfully behind the module network repeater after it was previously registered directly with the controller (and vice versa).
- Schedules now work correctly for those that are valid across the midnight threshold.
- Resolved an issue where processing a numeric credential greater than half the length defined in the credential type would cause a controller restart.
- Over current trouble input is no longer triggered incorrectly on the single door controller with PoE.
- Feedback is now provided when a user fails to gain access after validating against the fallback door type.
- The Inovonics Wireless Receiver Module input states are now being set correctly after a module update for the first 8 inputs.
- Valid credentials are no longer interpreted as raw credential reads under certain conditions.
- Encoding for Protege WX email is now explicitly set to UTF-8 so that non-English text is displayed correctly.
- Fixed issue with events referencing keypad modules incorrectly displaying the record ID as the module address in Protege WX.
- Updated module registration error handling to prompt a module update if the module has changed from being connected via RS-485 to Ethernet (and vice versa).

- Fixed issue with **Deny Entry if Inside Area is Armed/Deny Exit if Outside Area is Armed** functionality blocking access if the area is disarmed but in alarm.
- Fixed issues with events `EVT_USER_ENTRY_DOOR_MODE` and `EVT_USER_EXIT_DOOR_MODE` not displaying required information in Protege WX.
- Fixed issue with **Log Message Retries** and **Log Reporting Failure** options not working correctly for Report IP service.
- Resolved an issue where, when enabled, offline user processing could cause a controller restart.
- Fixed issue with Report IP not activating the **ReportIP Reporting Failure** trouble input correctly.

Version 4.00.292

New Features (4.00.292)

The following new features have been included in this release:

Email on Event

Email on event enables you to trigger an email that is sent automatically when specific events occur. The feature can be configured to operate on Area or Input Records.

This feature is only available in Advanced mode.

1. Navigate to **Programming | Areas** or **Programming | Inputs.** Select the **Configuration** tab and add a recipient email address to the command window using the format `email:yourname@yourdomain.com`
2. Configure your email server settings under **System | Settings.**

   Currently, Microsoft Exchange Server 2016, Gmail (when configured for less secure apps) and Yahoo are supported.

   - **SMTP Mail Server:** The address of the outgoing SMTP mail server.
   - **SMTP Port**: The port used for outgoing mail connections.
   - **Use SSL**: When enabled will transmit email using the Secure Sockets Layer (SSL).
   - **SMTP Logon:** The logon for the outgoing SMTP mail server.
   - **SMTP Password:** The password for the outgoing SMTP mail server.
   - **SMTP Timeout**: Defines how long (in seconds) before the connection times out.
   - **Sender E-mail Address:** The email address used when sending outgoing mail.
   - **Sender Display Name:** The display name used when sending outgoing mail. If a display name is not entered, the sender email address is used.
   - **Test E-mail Address**: Enter an email address to test notifications then click **Test E-mail Settings** to check your configuration.

Inovonics Integration

Protege WX now interfaces with the new Inovonics Wireless Receiver Module. The module is designed to link ICT's Protege systems to wireless Inovonics devices. The new product works with the Inovonics EN4200 Echostream repeater to translate incoming signals from Inovonics wireless devices so they are understood by Protege controllers.

The Inovonics Wireless Receiver Module is not a licensed feature.

Login Timeout

If you repeatedly enter incorrect passwords at the Protege WX login window, you will be forced into a login stand down. Three consecutive incorrect login attempts will result in the login process being locked for 5 seconds. If another three login attempts fail, the login process will be locked for 60 seconds between all subsequent attempts until a valid login is made. An operator cannot disable this.

Export User Fields

The new User Search export button provides a quick and easy way of taking a list of all user programming out of your system and using it elsewhere. The exported CSV file can be opened in an Excel spreadsheet or similar.

1. Navigate to **Users | User Search** and press the **Export** button.

   Fields exported to the CSV file include:
   - Display Name
   - Reporting ID
   - Default language
   - Phone extension
   - Pin code
   - User area
   - Start date
   - Expiry date
   - Credential type
   - Credential
   - Access levels
   - Facility code
   - Card number
   - Disable user
   - Show a greeting message to user
   - Go directly to the menu on login
   - User can acknowledge alarm memory
   - Show alarm memory on login
   - Turn off the primary area if user has access on login
   - Turn off the user area on login if user has access
   - Acknowledge system troubles
   - Treat user pin +1 as duress
   - User has super rights and can override antipassback
   - User operates extended door access function
   - User loiter expiry count enabled
   - User is a duress user
   - Rearm area in stay mode
   - Dual custody master
   - Dual custody provider

Localized Interface: Russian and Greek

The user interface is now available in **Russian** and **Greek**.

The language is set at an Operator level **(System | Operators)**.

Feature Enhancements (4.00.292)

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

- A Company Name field has been added to the Users menu.
- Access levels now specify a direction (Entry, Exit or Both) in the Doors and Door Groups lists.
- An area Ready Output and/or Output Group can now be configured to indicate that all inputs in the area are closed and the area is ready for arming.
- Added SIA over IP (DC09) and CID over IP (DC09) to the ReportIP service.

- Area, User, Input and Trouble Input database IDs are now included in the packet sent to ArmorIP when reporting an event.
- Phone extensions can be non-numeric when synced with an entry station.
- If Stay arm or Force arm have been selected from a keypad, pressing each button again will switch to Instant Stay arming or Instant force arming, respectively.

Issues Resolved (4.00.292)

The following issues have been resolved in this release:

- Reporting IDs are now automatically assigned when adding users, areas, inputs or trouble inputs.
- A door type using only card or PIN can now be used as the fallback door type for doors using a credential door type.
- Fixed an issue with the Activate Access Level Output option not working when a reader expander operates under Elevator mode.
- The onboard reader expander's input LEDs now change based on their logical state instead of their physical state as per the other modules.
- Fixed an issue with credential events not displaying the correct credential data when a user has multiple credentials of the same type.
- Fixed an issue with the Fire Control programmable function not working correctly when a lock output group has been assigned instead of a single output.
- Corrected resyncing of enhanced smart reader LEDs when a module update is applied to the onboard reader.
- Removed the use of customizable codes for ReportIP background polling. An offline channel now sends a normal poll to determine if that channel has come back online.
- Fixed an issue where double and triple badging to arm an area was not working from an ICT RS-485 reader connected to a reader expander if the controller's onboard reader had not been enabled.
- Fixed an issue with the Token Time in the Elevator Control function being limited to 255 seconds.
- Access granted events for elevator access are now displayed in green.
- Fixed an issue where a door would not automatically relock if a beam input had been programmed then deleted from the programming while the beam was broken.
- Two issues resolved in the database upgrade process when updating from version 4.00.198 or earlier. The controller would not update correctly if the Lock Door Group On Arm was set to All Doors or the Keypad Alarm Display Group was set to all keypads.
- Fixed an issue where deleting a user's PIN would appear deleted but still be processed.
- Automatic licensing now operates correctly.

Version 4.00.284

Feature Enhancements (4.00.284)

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

- Added `ReArmAsDeferArea = true` to the area commands. This will allow areas to be rearmed as a deferred area.

Issues Resolved (4.00.284)

The following issues have been resolved in this release:

- Resolved issue with Patriot LS30 protocol not recovering correctly from a failed connection.
- Fixed issue with Onboard Reader LEDs not synchronizing correctly when a module update is performed.

Version 4.00.278

Feature Enhancements (4.00.278)

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

- Setting the unlock time to 0 for an Aperio Version 3 lock will now toggle the lock state.
- Credential data submitted to the Protege WX system is now displayed with many credential related events.

Issues Resolved (4.00.278)

The following issues have been resolved in this release:

- Resolved an issue with **Lock** and **Unlock** control commands not working correctly for Aperio Version 3 locks.
- Resolved an issue with **Reader Tamper/Missing** trouble events reporting incorrectly when the onboard reader expander reader ports are programmed for RS-485 operation.
- Fixed an issue where filtered events stop updating automatically when displaying live updates.
- Resolved an issue where raw credential data was always sent as lower case.
- Resolved an issue where historical events are missing or displaying incorrectly after updating to Protege WX Version 4.00.274.
- Fixed an issue with the **Inverted Follow Pulse On Output** programmable function not working correctly for door groups.
- Fixed an issue with the **Follow Pulse Off Output** programmable function not working correctly for door groups.
- Resolved an issue with operator related programmable function events incorrectly displaying the name of the operator.
- Fixed an issue with **Input Bypass Restore** events reporting incorrectly.
- Resolved an issue with RS-485 reader LEDs and buzzers not re-synchronizing correctly when the onboard reader expander is power cycled.
- Resolved an issue where setting a **Fallback Door Type** as itself could cause a lockup.
- Resolved an issue which could cause ICT RS-485 smart readers to re-synchronize with the controller every 11 minutes.
- Resolved an issue where a filtered list of user names would always include the last user.
- Resolved an issue related to an incorrect date and time display in the Protege WX interface if the current year was not a leap year.
- Resolved an issue where daylight saving adjustments could change by two hours on more recent controller variants.
- Resolved a slow memory leak related to TCP/IP communication on more recent controller variants.

Version 4.00.274

New Features (4.00.274)

The following new features have been included in this release:

HTTP Port

A new **HTTP Port** field has been added to the **Settings | General** menu. The default port is 80 but this can be changed to any network port not occupied. **Changes to this field will require the Controller to be power cycled.**

Credential Types

The **Credential Types** feature enables Protege WX to accept forms of user identification other than the existing card, PIN and biometric (created under Users | General) formats, such as vehicle license plates and bar codes. These new credential types are created under **Users | Credential Types** with fields available for defining credential type name and configuring the credential data sent to the controller. There is no limit to the number of credentials that can be added to any single user.

To be able to use the credential functionality, the third-party device or software used to collect the credential data is configured as a smart reader (**Expanders | Smart Readers**), with the data sent through to the controller via the onboard RS-485 reader ports or via Ethernet (the feature supports Unicode, UTF8, ASCII, Numeric and Hexadecimal data formats). The smart reader in this case is not a physical device but is necessary to link the credential-matching functionality to a door. The smart reader should be configured to match the correct **Expander Address** and **Expander Port** to which the third-party device is connected. Because the smart reader is not a physical device the **Configured Address** is not important but must still be set to a unique value. The smart reader must be told which credential types it can accept, as well as which door to unlock. This is programmed under the **Reader** tab.

The door must also be configured with the credential types it will respond to. This is programmed under the Door Type configuration from the **Programming | Door Types** menu. The **Entry Reading Mode** and **Exit Reading Mode** can be set to **Custom**, then an **Entry Credential Types** and an **Exit Credential Types** tab appears where one or more standard credential types can be selected. For the door to unlock, all selected credential types must be presented and if the **Sequence** option is checked, the credential types must be presented in the specified order.

See **Fallback Door Type** below for programming alternative standard credential types as a fallback door type.

Fallback Door Type

To ensure building access in cases where equipment malfunction or communication failure means a particular credential type fails (such as a DVR device reading license plates), an alternative set of (standard) entry and exit Door Type credentials can be programmed to be accepted as a fallback. For example, a door type that requires license plate recognition could be configured with a fallback door type requiring card and PIN. In this case, presenting either set of credentials would grant access to the door. The alternative door type is defined in the field **Fallback Door Type** (**Door Types | General**).

Reporting Service and Reporting ID

- Each area, input and trouble input must now have a **Reporting Service** and a **Reporting ID** assigned. When an area, input or trouble input is assigned to a reporting service and does not have a reporting ID assigned, the lowest available reporting ID is automatically assigned. This can be manually edited as required. If the primary reporting service is configured to back up to another service, only the primary service for the input, trouble input or area needs to be specified.
- Under **Users | General**, a **Reporting ID** field is now available for defining the code by which a user is reported to a monitoring station. Users' phone extensions can now be extracted (if entered in the **Phone Extension** field) when an entry station is integrated with Protege WX. A **User Area** field has also been added.
- A **Reporting Services** tab has been added to the Areas menu to define the primary reporting service for the area.
- New fields have been added to the **Services | Report IP | General** tab:
  - **Test Report CID Code** is an industry-standard three-digit code signifying the type of event.
  - **Test Report CID Group** is a two-digit reporting ID for area.
  - **Test Report CID Zone** denotes the specific reporting ID of an input, e.g. of a particular PIR.
  - The **IP Port Number** configures the TCP/IP port used.
  - The **Ack Wait Time** denotes the wait time (in seconds) for signal acknowledgment.
  - **Enable Offline Polling** enables polling to detect whether the alternative backup service is working (see Service Operates as Backup below).
- A **Service Operates as Backup** option has been added to **Services | Report ID | Options**. When enabled the service will not report messages and alarms unless it is started by another service that has failed. It will then

start reporting messages immediately from the time the other service failed to report, then return operation to the service that started. This cycle will continue until the service that failed operates normally again.

- All CID mapping options have been removed from the Services menu. Mapping is now generated using the Central Station Report function (see **Central Station Reports**).

Central Station Reports

The CID map options have been made obsolete for the ReportIP and the ContactID services. Central Station Reports have been implemented under **Monitoring | Reporting**, providing a report map for the Contact ID and Report IP services which can be supplied to the monitoring station.

Password Policy

The new **Password Policy** menu offers a set of guidelines designed to enforce a higher level of security. Protege WX enables definition of a password policy for all users of the system to follow. Fields enable configuration options for password length and characters, and an option for passwords to be checked against user names to ensure they are unique.

Door Inputs

An **Inputs** tab has been added to the **Programming | Doors** menu so that any input from within the Protege WX system can be assigned to a door for the REX, REN, door sense, bond sense, and beam sense functions. The original settings in the **Expanders | Reader Expanders** menu are now only relevant to the offline operation of the reader expander. Unexpected behavior may occur if default reader inputs are not assigned for these door functions when the expander goes offline. Fields from the Reader Expander menu now configurable under **Doors | Inputs** are:

- **Door Input** (with **Invert Input** option)
- **REX Input** (with **Invert Input** option)
- **Bond Input** (with **Invert Input** option)
- **REN Input** (with **Invert Input** option)
- **Beam Input** (with **Invert Input** option)
- **Always Allow REX**
- **Forced Door Sends Door Open**
- **Recycle REX Time**

Door Trouble Inputs

All door-related Trouble Inputs have been removed from the Reader Expander programming and are now assigned directly to the door. A Door (DR) option can now be selected from the Module Type drop-down menu for each of the door trouble inputs. When this option is selected, the Module Address field is updated to allow selection of the door the Trouble Input is associated with.

Menu Group Changes

A **Keypad Groups** tab has been added to the **Menu Groups** menu to filter menu groups based on the keypad group assigned to them.

User Search

The new **User Search** feature enables operators to easily locate users within Protege WX based on details such as card numbers, access levels and other options attributed to users.

Feature Enhancements (4.00.274)

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

- New options have been added to **Users | Options**:
  - **Turn Off the User Area on Login if User Has Access**: When enabled the area programmed in the user's global area will be turned off when the user logs into a keypad.
  - **Treat User PIN+1 As Duress**: When enabled, the user can enter a duress code, allowing access but sending a silent alarm to the offsite monitoring station. The duress code is the last digit of a user's PIN plus 1. For example, if the user's PIN is 1234 but the PIN is entered as 1235, it will be processed as a duress code. (Note: the plus 1 counter applies to the last digit only. This means if the user PIN is 1239, the PIN to trigger a duress code is entered as 1230).
- The **Include All** options have been removed from the various Door Groups, Area Groups, Floor Groups and Elevator **Groups** menus and are now configurable within **Users | Access Levels**:
  - **Include All Doors**
  - **Include All Areas**
  - **Include All Arming Areas**
  - **Include All Disarming Areas**
  - **Include All Floor Groups**
  - **Include All Elevator Groups**
- New options have been added to **Doors | Inputs**:
  - **Recycle Door Open Time On REX**: When enabled the reader extends the door open time when the REX is received. The REX must be received during the normal open time or during the pre-alarm time for the timer to be recycled. Pressing the Request to Exit once the door has been open too long requires the door to be closed. This option will not affect the ability of the Request to Exit action to unlock the door. When disabled, REX input will not alter the door open time once the door has been opened.
  - **Maintain REX**: When enabled the door stays unlocked for as long as the REX button is held down.
  - **Pulse Reader Beeper On REX**: When enabled the reader associated with the door produces a double beep when the REX button is pressed.
  - **REX Time Different To Lock Time**: When enabled the REX Activation Time field appears, allowing for specification of duration for unlocking the door using the REX button. This overrides the time set for the Lock Activation Time (under **Doors | Outputs**).
- A **Relock on Door Open** option has been added to **Doors | Options**. If enabled, the door lock reactivates when the door sense detects that the door is open.
- New options have been added to **Doors | Advanced Options**:
  - **Reset Antipassback Status On Schedule**: When enabled Antipassback is reset according to the Antipassback Reset Schedule.
  - **Enable Timed User Antipassback Reset**: When enabled Antipassback is reset according to **User Reset Time**.
- An **Enable Input Lockout** option has been added to **Inputs | General**. When enabled the Input Lockout Count increments each time an alarm is triggered. Once this exceeds the **Zone Lock Out** count, the input is locked out and further activations are ignored. The counter is reset when the area is disarmed and rearmed and the input is permitted to trigger the alarm again. This is ideal for an input in a position where it may occasionally falsely trigger an alarm.
- A **KLES Input LED** field has been added to each assigned area under **Inputs | Areas and Input Types**. It defines the LED of the Protege Eclipse Keypad used to display the state of the input in the specified area. If a Protege Eclipse LED keypad is used, the area selected can be assigned to one of the keypad's LEDs. Any area assigned to LEDs 9 or higher is displayed on the keypad with a 0 representing the '10s' digit. For example, when the number 15 is displayed, the 0 and 5 will flash.
- New fields have been added to **Expanders | Keypads | General**:
  - **Default Display Line One** defines the name displayed on the keypad. As the first 16 characters are what a user sees from a keypad, these characters should be as descriptive as possible to ensure items are easily identifiable.
  - **Default Display Line Two**: as above
- New fields have been added to **Expanders | Keypads | Configuration**:

- **Max Invalid PIN Entries** defines the maximum number of invalid PIN entries allowed before the user is locked out of the keypad.
- The **Lockout Keypad Time (seconds)** now handles values over 4 minutes. To use this feature, enable **Lock Keypad On Excess Attempts** under the Options 1 tab.

- New fields have been added to the **Expanders | Reader Expanders | Reader 1/2**:
  - **Reader 1/2 Dual Authentication Pending Output** defines the output that activates when the first credential is presented.
  - **Reader 1/2 Dual Authentication Wait Time** defines the maximum time allowed between presenting the two credentials.
  - **Card Data AES Encryption Key**: Salto SALLIS cards can be encoded with site/card information via the ICT Encoder Client. This defines the decryption key used with these cards. Please contact ICT for additional information. This option only applies to the RS-485 implementation of SALLIS.
  - **Disarm Users Area On Valid Card**: When enabled the reader will disarm the users area when access is granted to the door the user is attempting to access. The users must still be available in the user area group assigned to the users access level. When disabled the reader will not perform any user area functions.
  - **Activate Access Level Output**: When enabled the reader expander will activate the output assigned to the users access level that gained access to the door or reader. When disabled the reader will not perform any action on the access level output.
  - **Arm Users Area**: When enabled the reader will arm the users area when they perform a dual presentation of their card to the associated reader. The area must still be available in the user area group assigned to the user's access level for this to operate correctly. When disabled the reader will not perform any user area arming functions.
  - **Enable Enhanced Smart Reader Outputs**: When enabled allows for control of LED and buzzer outputs of an RS-485 reader as independent outputs when connected to the specified reader port.
- The options under **Expanders | Reader Expanders | Reader 1/2 Options** have been split between two headings: **Options** and **Offline Options**. The following are new fields under Offline Options:
  - **Door Sense Enabled**: When enabled the reader will send door events when the door input is opened or closed. This is enabled by default but should be disabled on at least one reader port if both reader ports are controlling the same door (ENTRY and EXIT access control). This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the Door Sense function for normal operation, refer to Doors | Inputs.
  - **Bond Sense Input Enabled**: Enables the magnetic bond sense functions. It is used when a separate door contact and bond sense input are to be used and the generation of door events should be processed using both inputs. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the Bond Sense function for normal operation, refer to Doors | Inputs.
  - **REX Enabled**: When enabled the reader expander will generate request to exit events from the REX input on the reader expander. When disabled the keypad will not generate any REX events. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the REX function for normal operation, refer to Doors | Inputs.
  - **REN Enabled**: When enabled the reader expander will generate request to enter events from the REN input on the reader expander. When disabled no action will be taken for the Request To Enter function. This option is ignored during normal operation and is only relevant for the offline operation of the reader expander. To program the REN function for normal operation, refer to Doors | Inputs.
- The option **Read Non ICT Programmed Sector Data** has been added to Expanders | Smart Readers | Reader under the heading Card Data AES Encryption Key. When enabled, it allows for the reading of card sector data not programmed by ICT.
- The Alarm NZ IP reporting protocol is now referred to as CSV-IP. By default the CSV-IP service will use the Contact ID reporting format. Information is sent using a login, password and event information in an ASCII comma separated values (CSV) format.

- Blind dialing (to CID modules that can't provide a dial tone) is now possible with the **Do Not Wait For Dial Tone When Modem Dials Out** option added to **System | Settings | Options**. When enabled the modem dials out without waiting for a dial tone.
- Pages will now resize to display based on size of browser window.
- Multi-selecting records is now available.

Issues Resolved (4.00.274)

The following issues have been resolved in this release:

- The **Door Left Open Alarm Time** now handles values over 4 minutes (**Doors | General**).
- Blind dialing (to CID modules that can't provide a dial tone) is now possible with the **Do Not Wait For Dial Tone When Modem Dials Out** option added to **System | Settings | Options**. When enabled the modem dials out without waiting for a dial tone.
- Previous issues with events not displaying on the **Door Status List** have been resolved. Now when unlocking a door via manual command the system generates events in the **All Events** page, and also lists them under **Events** on the **Door Status List** page.
- The problem of not being able to set a value greater than 64 for the **Configured Address** field in the Smart Readers menu has been fixed. It is now configurable to up to 255.

The issues with saving selected options in **Programming | Doors | Advanced Options** have been corrected.

- All expanders can now be created with the **Physical Address** defined as **Not Set**. The field will now display **Not Set** instead of **Error Duplicate Address**.
- The **Smart Reader Card Data AES Encryption Key** value now saves correctly.
- Reader 1 and Reader 2 format will now default to **HID 26/34 Bit** (Expanders).
- Resolved issue of being unable to add cards from events page when utilizing an operator language other than English.

Version 2.20.198

New Features (2.20.198)

The following new features have been added in this release:

- A **Deny Entry and Deny Exit** option has been added for door lockdown.
- Non ICT programmed sector data cards are now processed when presented to Aperio locks.

  To configure this option, enter `NonICTSectorProgram = true` into the Commands section of the Smart Readers page.
- Added a feature that enables you to assign a separate unlock time for REX operation.

  To configure this option, enter `REXTime = #` into the Commands section of the Doors page.
- Added a feature that unlocks the door for as long as the REX button is held down.

  To enable this option, enter `MaintainREX = true` into the Commands section of the Doors page.
- Door locks can now reactivate when the door sense detects that the door is open.

  To enable this option, enter `RelockOnOpen = true` into the Commands section of the Doors page.
- Added the ability to force all PSTN modem dialing to commence without the need to detect a dial tone.

  To enable this option, enter `BlindDial = true` into the Commands section of the System Settings page.
- Updated the Report IP service to allow for poll times of up to 24 hours.
- You can now add phone extensions to user records.
- Operator events now reference the operator logged into the system at the time.
- Language support has been added for Greek and Russian.

Issues Resolved (2.20.198)

The following issues have been resolved in this release:

- Resolved an issue with the Protege Eclipse Keypad not being able to unlock a door after logging into the keypad and pressing the Menu key.
- Corrected an issue where a user with the right to disarm an area was not able to arm the area when badging at a card reader.

Version 2.20.162

Feature Enhancements (2.20.162)

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

- Protege WX is now able to support 32 floors and 8 elevator cars.

Issues Resolved (2.20.162)

The following issue has been resolved in this release:

- Fixed an issue with smart readers not operating correctly.

Version 2.20.154

Issues Resolved (2.20.154)

The following issues have been resolved in this release:

- The **Log to Event Buffer** option in the **Inputs | Options** menu is now disabled by default.

Version 2.20.145

Issues Resolved (2.20.145)

The following issues have been resolved in this release:

- Corrected an issue where Low Battery Trouble events for SALLIS Locks were not reporting correctly.
- Events now display correctly in the **Monitoring | Events** page when viewed in Estonian.
- Resolved an issue where the Unlock For Time function for elevators was operating incorrectly.

Version 2.20.139

Issues Resolved (2.20.139)

The following issues have been resolved in this release:

- Resolved an issue that prevented subsequent NTP time requests from occurring after the first request.
- Resolved an issue where a user configured to disarm the primary area of a keypad upon logging in may sometimes disarm another area they have access to.
- Resolved an issue where if there is any text in the Commands section of the Programming | Inputs menu, the Input Lockout function would automatically enable with a value of 1. This issue allowed the input to trigger the alarm when first activated, but prevented any subsequent activations until the area rearmed.

Version 2.20.138

Feature Enhancements (2.20.138)

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

- HTML special characters now display correctly for record groups.
- You can now move the Monitoring | Event Report overlay window freely across the screen (and off screen).
- The Reader tabs in the Expanders | Reader Expanders menu are now hidden if the associated Port Network Type option is set to SALLIS or Aperio.

Issues Resolved (2.20.138)

The following issues have been resolved in this release:

- The Alert Operator but Allow Access option no longer overrides the Hard Antipassback option.
- The controller no longer fails to rearm areas following a full power cycle.
- The Token Time for the Elevator Control programmable function now uses the correct value.
- Timed outputs no longer intermittently remain on for twice the programmed time.
- SALLIS Ethernet router settings can no longer be overwritten if Commands have been parsed to the reader expander.
- Corrected the door processing functionality that returns doors to schedule processing following a manual control command. Doors now return to operating on a schedule irrespective of whether the Always Check Schedule option is enabled.
- Door Left Open alarms are now correctly generated for Allegion integration.
- Improved the time sync issues seen with the SALLIS RS-485 and SALLIS Ethernet implementations.
- The process used to check the state of Allegion controlled doors has been enhanced to avoid inconsistent LED flashing.
- Door state change events for Allegion integration now display the correct reader addresses.
- Event numbers and formatted text are now included in the event strings sent to the Protege WX DLL.
- FTP and Telnet passwords are now forced to the Protege WX version every time a Protege WX controller is powered up.
- The EVT_CARD_READ_CARD_BY_DOOR, **EVT_CARD_READ_PIN_BY_DOOR** and **EVT_CARD_FORMAT_ERR_BY_DOOR** events now display correctly in Protege WX.
- The firmware version number for the Protege WX DIN Rail 8 Input Expander is now displayed correctly when initially registered with an invalid module address.
- The Include All Outputs option in the Programming | Output Groups | Outputs menu has now been removed.

Version 2.20.132

New Features (2.20.132)

The following new features have been included in this release:

System Capacity Expansion

This release of Protege WX offers an extended system capacity with original hardware and record limitation being lifted, making Protege WX suitable for a wider range of installations.

The Protege WX system is now able to support up to:

- **248 Input Expanders**

  To accompany the release of the Protege Single Input Expander, the limit on input expanders has been increased from 32 to 248. This enables use of single input expanders without hitting the ceiling too soon.

- **200 Keypads**

  To accommodate the growing use of the Protege Keypad App for iOS and Android, we've extended Protege WX's keypad capacity from 32 to 200. Using the Protege Keypad App you are able to arm and disarm an area or group of areas, control doors and monitor the status of any input, output, schedule or door directly from a compatible mobile device.
- **64 Reader Expanders**

  More reader expanders means more doors. With up to two hardwired doors per reader expander, the Protege WX system is now able control up to a total of 128 individual doors. This further enables you to scale your system as your requirements change and ensures an accommodating migration path from Protege SE.

To apply these changes, install the latest Protege WX Application Software file, ensure that your controller is registered, and download a new license.

Antipassback

This feature is only available in Advanced mode.

In many high security or hazardous environments, maintaining an accurate record of who went where and when is critical. Using Antipassback you are able to prevent users from passing their credentials to another user and to stop users from entering areas by following or tailgating another user.

When combined with other features found in Protege WX, Antipassback provides the perfect solution for the following scenarios:

Hazardous Areas

- Hazardous areas have strict requirements around user training and certification for entry and safe operation. Use Antipassback to ensure only authorized users are entering an area.

High Security Areas

- Some industries have requirements around the level of security provided in certain environments. Combine Antipassback with dual authentication to ensure there are always two people in an area.

Car Parks

- To ensure accuracy in carpark counting, use Antipassback together with area counting to prevent too many cars from entering the area and to automatically illuminate a 'Car Park Full' sign.

For more information about Antipassback, refer to the ICT website (www.ict.co).

Raw Card Data Functionality

From the users menu you are now able to open a new dialog window that picks up any raw card data that is recorded by the system (once the window has opened). Once displayed, you are able to apply the card information to a new or existing user. A similar feature is also available from the Events list. Clicking a raw data event that has a + sign next to it enables you to add the card number to an existing user, or to create a new user with the card number.

This reduces data entry and administration time, and enables you to quickly and accurately add card data to users on the fly.

TCP/IP Protege Keypad Application Support

The Protege Keypad Application for iOS and Android is now able to connect to Protege WX using TCP/IP (using UDP/IP as a fall back). This ensures the reliability of the Protege Keypad Application for internet connected devices.

Localized Interface: Italian

The user interface is now available in **Italian**.

The language is set at an operator level (System | Operators):

Feature Enhancements (2.20.132)

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

- When updating a license, you can now select either Automatic Licensing or Manual Licensing.
- You are no longer required to power cycle your controller when updating application software.
- The registered and online status icons in the expander addressing page are now automatically updated every five seconds.
- The expander wizard now correctly displays the number of doors assigned to a reader expander.
- Jump [...] buttons have been added to various areas within the UI.
- All references to controller firmware within the UI have been changed to application software.
- The name of the site has been added to the header bar within the UI. When logging in this is displayed above the ICT logo. When you are logged in this is displayed beside the Protege WX logo. This option can be enabled/disabled from the Licensing | License Update menu.
- The administrator operator now has its username and role set to read only.
- Removed the Not Set option from the schedule list in the Users | Access Levels menu.
- Adjusted the timing to speed up the dialing process of the SIA reporting service.
- Trouble inputs have been added to the Automation & Control service.
- Added an option that allows a schedule to override a latched unlocked door.

  To enable this option, enter **`ScheduleOverridesLatch = true`** into the Commands section of the Doors menu.
- The Emulate Unlock Menu option for the Door Control programmable function can now be applied to SALLIS locks.
- The retry time for TCP/IP module communications is now incremental. This allows the ICT Phone app to use TCP/IP, enabling ICT customers to install the keypad app on their phone and log into their system from anywhere in the world.
- When a user logs in at a keypad, all valid menu groups from all valid access levels are now used to determine what the user has access to.
- Added the ability to manually set the number of invalid attempts allowed at a keypad.

  To configure this option, enter **`MaxInvalidPinEntry = x`** into the Commands section of the Keypads menu.
- The maximum Lockout Keypad Time is now 65535 seconds (approximately 18 hours).

  To configure this option, enter **`ENKeypadLockoutTime = x`** into the Commands section of the Keypads Menu.
- Support for the Zone Lockout functionality is now available.

  To enable this, enter **`ZoneLockout = true`** and **`ZoneLockoutCount = x`** into the Commands section of the relevant input where x is any number between 1-255. This sets the alarm trigger count limit. After this time has elapsed, the input no longer triggers the generating of any alarm reports for the area that it belongs to following the area being armed. This option resets once the area is disarmed. To test this:
  - Place the input with the zone lockout setting into an area.
  - Arm the area.
  - Trigger an alarm on the area via the input configured.
- The ability to trigger trouble inputs on short duration module communication faults is now available.

  To configure this option, enter **`ReportShortModCommFault = true`** into the Commands section of the System Settings page.
- You are now able to view time and attendance details from a keypad. This feature is used to provide visual feedback to a user to verify a successful card read when signing in or out using an ICT card reader. When a user badges at the reader their name, along with the recorded time and date, displays on a keypad located beside the reader

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

- Events displayed in the Monitoring | Events list and in Event Reports are now color coded.
- Test reports are now able to occur on a weekly basis. To enable this option, enter `TestReportDayOfWeek = x` into the Commands section of the System Settings Page where x is any number from 1 (Monday) through to 7 (Sunday). This works in conjunction with the time configured for the Test Report Time option located under the Configuration tab of the System Settings page.
- The Controller is now able to interpret SEOS cards presented to Aperio locks.
- Added a **User Loiter Expiry Count Enabled** option to the Users | Options menu.

  This feature is only available in Advanced mode.

- Increased the speed of batch importing of users.
- Added a single 5k6 and a 5k6/5k6 resistor option to the Input EOL options.
- Added a Loiter section to the Areas | Configuration menu. This section includes a Loiter Timer in Minutes option and a Loiter Reset Area option.

  This feature is only available in Advanced mode.

- The Protege Single Zone Input Expander has been added to the expanders wizard and the firmware and expander addressing pages.
- In the Inputs | Options menu the Input Inverted checkbox has now changed to a Contact Type dropdown. This enables you to select whether an Input is Normally Open or Normally Closed.
- In the Users | Options menu the User Has Super Rights checkbox has now been changed to User Has Super Rights And Can Override Antipassback.

Issues Resolved (2.20.132)

The following issues have been resolved in this release:

- The Access Control Wizard now supports accented characters.
- The Reader Format field is now visible for smart readers regardless of the selected expander format.
- Resolved an issue where duplicate PINs were not being found during user import if the **Treat PIN + 1 as Duress** option was selected.
- If a Door is linked to a Virtual Door Programmable Function the unlock time programmed for the Door is now overridden by the unlock time programmed for the Virtual Door.
- A Reporting ID of 0 (the default) for Areas and Users will now send the Area or User index rather than the value 1.
- Resolved an issue where all doors were being processed regardless of whether they had been programmed.
- Resolved an issue where if the TCP module communications transmit buffer gets more than ten seconds behind and stops accepting registration packets, it could cause data to be aborted due to the discarded registration packet being used later.
- Resolved an issue where the Smart Reader process could use the incorrect reader port when determining the door status of a Smart Reader when both reader ports are in use.
- Corrected an issue where Aperio could incorrectly determine that a non-existent lock was online.
- Resolved an issue where a lock state change packet sent from an Aperio lock with no door programming could cause the controller to restart.
- Increased the size of Default Display Line One and Default Display Line Two from 16 to 32 bytes in order to accommodate 16 accented UTF-8 characters.
- The Report User Bypass Option is now recognized correctly when a user bypasses an input.
- The Automation and Control Service no longer turns off encryption for the service after you log out.
- Bell Squawk now occurs at the correct time during an Area's arming sequence.
- Resolved an issue where disabled users were still granted access via PIN entry on reader keypads.
- The Door Lockdown function now correctly checks the entry/exit configuration of readers in multiplex mode.
- Corrected an issue where the token time for the elevator control function was not using the correct value.
- When a door is manually locked via a UI command while the door is unlocked by a schedule, then manually

unlocked again, it now returns to the unlocked by schedule state.
- Elevator Floors are now saved correctly.

Version 2.20.101

New Features (2.20.101)

The following new features have been added in this release:

- Support for the Protege Eclipse LED Keypad has been added, including setup within the Expander Wizard.

  For more information on how to setup and configure a Protege Eclipse LED Keypad in Protege WX, please refer to the application note: AN-157 Eclipse LED Keypad Protege WX Integration available from the ICT Website (www.ict.co).
- Support for the RS-485 enabled Protege DIN Rail 2 Door Expander has been added, including setup within the Expander Wizard.
- A "Deleting programming... please wait" dialog box is now displayed when deleting expander programming.
- Protege WX exported event lists are now sorted from newest to oldest.
- Intelligent Tamper Trouble Inputs now work for Wiegand Readers that are connected to the Onboard Reader Expander. When upgrading, these records need to be added manually as they do not exist in the system by default.

  For more information, please refer to the application note AN - 158 Creating Intelligent Tamper Trouble Inputs for the Onboard Reader available from the ICT Website (www.ict.co.
- Added the ability to handle iClass cards parsed from any Aperio iClass Locks.
- Defaulting the controller now defaults the Licensing Site Details.
- The CSV User Import function now creates all unrecognized access levels found in a batch .csv file.

Issues Resolved (2.20.101)

The following issues have been resolved in this release:

- On-screen event reports are now displayed consistently between browsers.
- Resolved an issue where single quotation marks (') used in Area names could cause problems in the Security Wizard.
- Dynamic search now supports unicode characters.
- Unique identifiers are now appended to URLs to prevent browser caching.
- The correct translation is now used in the Username field of the Operators menu.
- The Activate Access Level Output option now works correctly for Smart Readers.

Version 2.20.082

Issues Resolved (2.20.082)

The following issues have been resolved in this release:

- Corrected an issue where under certain circumstances the creating of the first Event Report record or the first Smart Reader record could result in a 'Failed to Save' message appearing. This issue affected firmware release 2.20.076.

Version 2.20.76

New Features (2.20.76)

The following new features have been added in this release:

- An 'Enable UL Operation Mode' has been added to the **Settings | Options** page .
- A 'Confirm Password' field has been added to the Change Operator Password process. This ensures that the password entered is correct and is a minimum of four characters long.

  Instructions for changing an Operator's password can be found in the Protege WX Getting Started Guide.
- Module firmware updates can now be carried out from the 'Firmware' page.
- A module's build number can now be viewed alongside its firmware version from the 'Expander Addressing' page and from 'Step 2' of the 'Expanders Wizard'.

Issues Resolved (2.20.76)

The following issues have been resolved in this release:

- Viewing and exporting filtered event reports now correctly uses the configured 'End Date'.
- Saving a record maintains correct 'Not Set' text for areas, phone numbers and input types.
- Default Gateway and IP Address verification now looks at the Subnet Mask.
- Reader expander port 2 arming mode values have been corrected.
- Meta tags have been added to Protege WX to prevent search engine indexing.
- Badging an invalid card no longer generates incorrect 'Router Offline/Online' events with the RS-485 implementation of SALLIS.
- Badging an invalid card with a non-matching card format on any Aperio lock no longer generates an event that displays incorrect Site Code and Card Number information.
- When a record is deleted, all fields that relied on it are now automatically set to <Not Set>.
- The maximum activation time for an Output Group has been changed from 255 seconds to 65535 seconds (approximately 18 hours).
- The maximum Control Output Time for an Input Type has been changed from 255 seconds to 65535 seconds (approximately 18 hours).

Version 2.20.074

Issues Resolved (2.20.074)

The following issues have been resolved in this release:

- Unlock schedules now work correctly with both the Ethernet and RS-485 implementations of SALLIS.
- Viewing and exporting filtered event reports now correctly uses the configured 'End Date'.
- The Report IP Service no longer pads out Account Codes that are less than 4 digits long.
- Resolved an issue where adding and deleting of 16 ReportIP services could result in the Controller failing to allow any more services to be added, even after all services had been deleted.

Version 2.10.068

New Features 2.10.068

The following new features were added in this release:

Event Reports

Event Reports allow an operator to create, view and export customized reports based on users, doors and areas.

To create an Event Report:

- Navigate to **Monitoring | Reporting | Event Reports**.
- Enter a **Name** for the report if saving is required.
- Enter a valid **Start Date** and **End Date**.
- To include **all events** click **Save**, **View** or **Export**.
- To filter based on Users, Door and/or Areas, use the additional tabs. Some common reporting scenarios and the filter criteria required are outlined in the following topic.
- Clicking **View** displays the relevant events.
- The report can also be exported in CSV format enabling you to extract event data which can then be formatted and manipulated as required.

  Depending on your browser settings you may be prompted to save the file, otherwise it is downloaded automatically to your Downloads folder.

The following scenarios cover common reporting requirements and the options to select:

To view what a particular user or group of users has accessed on site:

1. Define the date/time range
2. Select the user(s)
3. Select View or Export

To view which users have been through a specific door, or group or doors:

1. Define the date/time range
2. Select the door(s)
3. Select View or Export

To view whether an individual user has been through a particular door:

1. Define the date/time range
2. Select the user
3. Select the door
4. Select View or Export

To view which user has armed an area:

1. Define the date/time range
2. Select the area
3. Select View or Export

To view whether an individual user has disarmed a particular area:

1. Define the date/time range
2. Select the user
3. Select the area
4. Select View or Export

Central Station Reports

Central Station Reports provide a report map for the Contact ID and Report IP services that can be supplied to the monitoring station.

To export a Report Map

1. Navigate to **Reporting | Central Station Reports**
2. Click **Export** for either of the two services to generate a CSV format report that can be forwarded to your monitoring station.
3. Depending on your browser settings you may be prompted to save the file, otherwise it is downloaded automatically to your Downloads folder.

Cameras

Cameras are a separately licensed feature.

Protege WX supports the monitoring of IP cameras that allow direct URL access to either a static JPG image feed or a streaming MJPG video feed. If you are able to paste a URL into your browser and view the raw camera image, then your camera is supported by Protege WX.

To add a Camera:

1. Navigate to **Programming | Cameras** and click **Add**.
2. Enter a **Name** for the camera and select the **Door** it is associated with.
3. To automatically setup your camera, click **Configure**.
4. Enter the **Manufacturer** and **IP address** of the camera.
5. If authentication is required, enter the **Username** and **Password**.

   If the camera you are using does not appear in the list, you can use the **Manual Configuration** section.

6. Enter the **Static image URL** and/or **Streaming MJPG URL**.

   If authentication is required to view the camera feed, the URL entered must contain the login details.

7. The **Refresh Rate** defines how often the Static Image is refreshed. The default is 400ms.
8. Once the camera has been configured, a preview of its stream is displayed under the **Camera Preview** Section. Alternatively, a live camera feed can be viewed from the **Door Monitoring** page by clicking the **Controls** button. Multiple camera feeds can be viewed simultaneously.

The camera function is only supported when the Protege WX interface is not being port forwarded externally to the internet through a router.

Feature Enhancements (2.10.068)

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

- Events can now be viewed from Area and Door Status Lists.
- An Events tab has been added to the Users, Doors and Areas menus.
- Licenses can now automatically be downloaded and installed from the Protege WX interface.
- An Elevator Monitoring page has been added that displays a list of all elevators and their current status.

  This feature is only available in Advanced mode.

- 128 Holidays can now be added to a Holiday Group.
- The hours, minutes, and seconds can now be set from the Time menu.
- A new field has been added to the Output Groups menu to allow you to specify an output activation time.

- There is now an option to select all outputs when creating an Output Group.
- The following Biometric Reader events have been added:
  - Door # waiting for biometric input from user #
  - Door # biometric timeout by user #
  - Door # biometric canceled by user #
- Users can now be a Dual Custody Master or a Dual Custody Provider.
- The Automation and Control service now references records in the order they are displayed in the browser. For example, if a door is displayed as the third door in the list, it will be referenced as Door 3.

  To implement this, navigate to **System | Settings** and enter `ACPUseDisplayOrder = true` into the **Commands** section and click **Save**.

Issues Resolved (2.10.068)

The following issues have been resolved in this release:

- Elevator and Area Control reader modes can no longer be selected when WXpert is not enabled.
- Accented characters in user names are now displayed correctly on the LCD keypad.
- Resolved an issue where the Keypad Red LED Output and Keypad Green LED Output where being incorrectly assigned by the Expanders Wizard.
- The Roles menu now displays all page names correctly.
- When setting the expander port for a smart reader that is connected to a 1D controller, the option to select port 2 is no longer displayed.
- Resolved an issue where the use of a 1D controller prevented the Reader 2 and Reader 2 Option tabs from being displayed for any additional reader expanders.
- The sitedetails.xml file is now removed when a Protege WX Controller is defaulted.
- When an area is armed/disarmed automatically, the event now states that it was armed/disarmed by the System User.
- Resolved an issue where schedules were not being correctly identified and populated in an access level.
- An issue regarding the possibility of the controller crashing during an offline user download has been resolved.
- The Expanders Wizard now correctly displays the names of existing modules.
- Resolved an issue where the Expanders Wizard labeled keypad outputs by number, not by function.
- Resolved an issue where user Start/Expiry Dates could be edited without the options being enabled.
- Open doors that have been unlocked by a schedule now trigger a 'Left Open Alarm' when they remain open following the end of the schedule.
- The event log can now correctly display the read mode used at Biometric Reader.
- Multiple Protege WX operators can now view live events from different browser sessions simultaneously without interference.
- Resolved an issue where debug and assertion events were omitted from exported event lists.
- The Contact ID and Report IP services can now differentiate between a standard analog expander and a PSU analog expander and can send the correct trouble zone codes for each.
- Resolved an issue where the 'Deny Exit if Outside Area is Armed' and 'Deny Entry if Inside Area is Armed' options were ignored if REX or REN was initiated.
- Resolved an issue where if the 'Treat Users PIN + 1 as Duress' option is enabled, a duplicate PIN check was not run. A pre-scan of all users is now performed and any potential PIN conflicts are brought to the attention of the operator.
- OS Services that are unused by Protege WX (e.g. SNMP - Simple Network Management Protocol) are now turned off by default. This prevents the controller from potentially crashing when Protege WX is used alongside network scanning software and further ensures the security of the Protege WX system.
- System assertion events no longer occur following the linking of an elevator record to a reader expander.
- Changes have been made to ensure that the naming conventions for all door lockdown options are consistent.

- Improvements have been made to the Automation and Control service that allows it to properly identify the status of its connection. These improvements prevent the service from locking up and denying connections when its initial connection has been lost.
- An undefined user is now recorded as an INVALID USER in the Protege WX event log.
- Contact ID is now the only service that can be selected as the backup for the Report IP service.

Version 2.10.060

Issues Resolved (2.10.060)

The following issue has been resolved in this release:

- Access Level programming now contains a **Time To Activate Output** setting to define the period the access level output is activated for.

Version 2.10.056

Feature Enhancements (2.10.056)

- Significant improvements to the Expanders Wizard, including the ability to program any module (including PCB hardware) using the Expander Wizard.
- New field added to the Expanders Wizard to allow you to specify the number of doors to be created.
- If an addressed module is found without programming, you are now given the option to program it.
- Output and Output Group tabs now added to the Access Levels page (Advanced mode only) to define the output that is activated when using the Reader Access Activates Output / Keypad Access Activates Output options when a user presents a valid card to a card reader or enters a valid user code at a keypad.
- Activate Access Level Output options now added to Reader1 and Reader2 tabs (Advanced mode only).
- When in the Security Wizard, the client codes now appear at the top of the respective Contact ID and Reporting IP sections.
- Language support has been added for Estonian.
- Self-aware card/PIN duplicate checking has been added to User Wizard and User pages.
- The Database ID is now visible under Menu Groups and Areas enabling you to view the ID when programming items using a Touchscreen.
- The maximum number of Automation points has been increased from 32 to 248.
- When deleting an Expander module you are now prompted whether you would also like to delete the associated programming.
- The Slave Comm option for Reader Expanders is now visible when in Basic mode.
- Service names are now shown in the Protege WX events list instead of the Record IDs.

Issues Resolved (2.10.056)

- If an invalid username or password is entered, the correct error message is now displayed.
- Resolved an issue where some doors would not unlock in offline mode if the Controller had not been defaulted prior to downloading the new programming.
- Resolved an issue where badging at a reader while it was beeping to indicate exit delay could silence the reader beeper.
- Adjusted the timing of the UDP module communications to address an issue where a heavily loaded slave network on an RDE2 could experience significant delays when all modules attempted to register at once.
- Resolved a timing issue where door unlock on schedule occasionally failed. This problem only existed in build 191 of the firmware and could be worked around by enabling the 'Always check unlock schedule' option.

- Corrected an issue with extracting information from a Lock State packet received from a SALLIS Ethernet/RS-485 Router, causing troubles zone for Door Forced/Left Open linked to SALLIS Doors to trigger incorrectly within Protege WX.
- All SALLIS Ethernet router and door online and offline events are now monitored by the Reader 1 Tamper Trouble Zone (12) for the Onboard Reader.
- All SALLIS 485 router and door online and offline events are now monitored by the Reader 2 Tamper Trouble Zone (13) for the Onboard Reader.
- Resolved an issue where SALLIS doors above address 10 would prevent all SALLIS operation.
- Door lockdown now works correctly for Exit doors. Previously it would only check Entry doors.
- Corrected an issue where a user could always arm/disarm the area assigned to a keypad regardless of their assigned access levels.
- An intermittent problem that could result in a script error when logging in has been resolved.
- Toggle Function Output on 3 Reads and Activate Function Output on 3 Reads options have been read as Arming Modes when programming a Reader Expander.
- If the access level is omitted from an imported CSV file, users are no longer automatically given installer access.
- The Parity options under Custom Reader Format are now applied correctly.
- The Onboard Reader beam detection on Inputs 3 and 7 now works correctly.
- Defaulting a controller now correctly defaults the operator list to a single admin operator.
- The Expanders Wizard now checks that a module has been correctly created before creating the module programming.
- The Reader Location is now correctly programmed by the Access Control Wizard.
- The Users wizard no longer adds 'All Areas' to a new access level when no areas are selected.
- The Reader Location programmed in the Access Control Wizard now saves on completion of the wizard process.
- An issue with the SALTO fields randomly populating in the Expander Wizard has now been fixed.
- The Door Unlocked/Locked by Schedule events are now hidden when the Enable Open/Close Events On Schedule option is enabled.
- The Always Check Unlock Schedule option now works correctly.
- Corrected an issue where a UDP Report IP service would potentially block other UDP Report IP services if it couldn't open a port.
- Moved the 'System started' event to before all other events.
- A health status message now appears if the port hardware type is changed, prompting you to update the reader expander.
- Corrected a problem with UDP responses slowing down over time which resolves connectivity issues with SALLIS Routers.
- Resolved an issue with Door Pre-Alarm/Door Left Open processing not working correctly with Aperio locks
- Online and offline detection events now included for the SALLIS 485 Router.
- All SALLIS door low battery events are now monitored by Trouble Zone 3 for the Onboard Reader.
- Resolved and issue with incorrect health status messages.
- Added the ability to correctly handle correctly HID Prox 125kHz cards parsed from any SALLIS 125kHz Locks via both the Ethernet and the RS-485 version of SALLIS routers.

Version 2.10.044

New Features (2.10.044)

The following new feature has been added in this release:

Localized Interface: Polish

The user interface is now available in **Polish**.

The language is set at an Operator level (System | Operators):

Issues Resolved (2.10.044)

This is a key update that addresses a known issue with IP Monitoring, and contains improvements to RS-485 module communication on large or high-traffic networks.

Anyone using IP Monitoring, or experiencing module offline issues, using PSU or ADC module analog channel logging, or with a system larger than 32 modules should apply this upgrade to enhance network stability.

Other issues addressed include:

- Substantial performance improvements when importing users from a CSV file.
- License details are now automatically removed when defaulting a controller.
- Duplicate address checking now works correctly when creating a new Input, Output or Trouble Input.
- When programming a Door the Area Disarmed AND Schedule Valid Unlock Door and Area Disarmed OR Schedule Valid Unlock Door options are now mutually exclusive, meaning you cannot incorrectly enable both options.
- The minimum user PIN length has been removed.
- When adding a new user the surname field is now optional.
- Trouble Inputs can now be created correctly.
- Pressing the Enter key to login when using IE8 now works correctly.
- When importing users from a CSV file the PIN is now optional.
- An interment issue where the final step of the Security wizard failed to complete has been resolved.
- Several cosmetic issues around translation of the user interface have been resolved.
- When restarting a controller following a firmware update the progress indicator now displays correctly in Google Chrome.
- All options related to Loiter functionality have been removed from the UI as they are not relevant to Protege WX.

Version 2.10.039

New Features (2.10.039)

The following new feature was introduced in this release:

Localized Interface: French and Spanish

The user interface is now available in **French** and **Spanish**.

The language is set at an Operator level (System | Operators):

Feature Enhancements (2.10.039)

- Inputs and Input Types now have a Control Automation field enabling you to define the automation point that is activated when an input opens or closes. This can be used for various functions such as gardening irrigation, lighting circuits, etc.

  You must also configure the appropriate options under the Input Type (Options 3 tab) in order to trigger the automation point.

Issues Resolved (2.10.039)

- When exporting events the date format no longer includes the day of the week (e.g. Tue 16/07/2013) making it possible to now sort the events by date.
- The module type is now displayed correctly when programming an input.

- When programming a Smart Reader, if values are defined in any of the following fields they are now saved correctly:
  - Keypad to use for PINs Reader 1
  - Reader One Area Control Area
  - Reader One Elevator
  - Invert Floor Relays
  - Control Relays On Comm Failure
  - Relays Activated In Comm Failure
- Floor details are now saved correctly when programming Elevators.
- If non-numerical characters are entered in the Facility/Card number fields they are now removed automatically.
- If a user has more than one card the system now performs duplicate checking on all card details.

Version 2.10.036

Feature Enhancements (2.10.036)

- **Firmware Version**: Protege WX consists of multiple modules, each of which has its own version number. These are now combined into one firmware version number, which is displayed on the firmware page. If at any time you need to view the module version number, click the Current Firmware text and a full list will be displayed.
- **Licensing:** The Site/Installer details form has been moved into the License Update tab, and a new Protege WX registration page has been added to the website (www.ict.co/wx) to make the process more intuitive.
- Additional **User Has Super Rights And Can Override Antipassback** option added (Users | Options). When enabled, the user is deemed to be a super user and can unlock doors in a lockdown situation.

Issues Resolved (2.10.036)

- Progress bars continue to move correctly if the user navigates to a different tab.
- Menu Groups can now be removed from an Access Level.
- Registration page corrected for operation with IE8.

Version 2.10.030

New Features (2.10.030)

The following new features have been added in this release:

Advanced Mode

Available to users that undertake optional WXpert training, Advanced Mode unlocks more comprehensive access control and intrusion detection features, as well as additional functions around building control and automation:

- Separate Arming and Disarming groups in Access Levels enabling you to differentiate between the areas a user is allowed to arm or disarm.
- The addition of Floors, Floor Groups and Elevator Groups in Access Levels enabling you to define which floors and elevator cars a user has access to.
- Additional Door options:
  - Slave Door option to provide the ability to set a door so it follows another door when it locks and unlocks. For example, this can be used to lock/unlock internal office doors automatically when the main entry door is locked or unlocked.
  - Interlock Door Group option that enables you to deny access to a door when other doors are not secure. Sometimes referred to as a mantrap or sally port system, this provides a controlled passageway where only one door can be opened at a time. Often used to separate non-secure areas from secure areas and

prevent unauthorized access, or in high tech manufacturing to provide entry and exit chambers for clean rooms.

- Area Counting functionality enabling you to control access to carparks and other building areas that require limited staff access.
- The addition of the Commands option which can be used in conjunction with ICT Support to send manual commands to a device.
- Elevator Control (low level only) to restrict a user's ability to select floors in an elevator car.
- Automation & Control and C-BUS Services (requires an Automation license), providing a generic interface for integration with third party automation products such as Savant and those that use the Clipsal C-Bus protocol.
- Custom Reader Format enabling you to define a custom Wiegand Reader format if none of the available preset options meet the format required.
- A range of Programmable Functions allowing you to perform specific processing when a particular event or operation occurs, including:
  - Logic Control
  - Area Control
  - Door Control
  - Elevator Control
  - Virtual Door
  - Ripple Output
  - Input follows Output

Unlocking Advanced Mode

Protege WX launches in basic mode. You must undertake an optional training course to become a 'WXpert' and unlock the advanced features.

To find out more about training, please contact ICT or your local distributor.

Once training has been completed, you will be given a new license file. Follow the steps for registering your Controller to complete the process.

Operators and Roles

You are now able to define your own Operators and assign Roles to determine which pages are visible to the operator when they are logged in.

To Add an Operator:

- Navigate to **System | Operators** and click **Add**.
- Enter the operators credentials including a username and password:
- Select the appropriate **Role** to determine what access the operator has once logged in.
- Click **Save** to finish adding the Operator.

The system comes programmed with three preset roles: User, Master and Installer. These roles can be customized to meet your specific requirements by enabling/disabling certain pages, however caution should be taken when making changes (particularly to the Installer role), as removing permissions can prevent an operator from accessing the system.

To Edit a Role

- Navigate to **System | Roles** and select the Role to edit.
- Enable/disable options as required. If an option is enabled, that page will be visible. If it is disabled, that page is hidden.

SALLIS Integration

SALLIS integration is a licensed feature that enables you to use SALTO standalone online devices within the Protege WX system, using SALLIS wireless technology.

SALLIS locks communicate via Nodes which are connected to a PoE Router. The Router communicates with Protege WX via the Ethernet.

- Select the Onboard Reader Expander and enable the **Enable Ethernet Router** option:
- Enter the **Port** and **IP Address** of the SALLIS Router.
- Each wireless lock must then be configured as a Smart Reader (Expanders | Smart Readers).
  - Set the **Expander Address** to 1 (the Onboard Reader)
  - Set the **Expander Port** to Ethernet
  - Enter the **Address** of the lock (as defined in SALLIS)

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

CSV User Import

The User Import feature enables you to transfer user data from an external source into Protege WX, automatically mapping the user information to the corresponding fields in Protege WX.

Important: The CSV file must be in the following format:

```
FirstName,LastName,FullName,Facility,Card,PIN,AccessLevel
```

The following rules apply:

- Each field must have a value, however the firstname/lastname can be omitted if the fullname is used, and vice versa.
- The facility can be omitted **if** it is prepended to the card number and separated with a colon (e.g. 123:4567).
- The Access Level must exist before import. If a match is not found, the access level is not assigned.
- The PIN and Card must be unique for each user.
- The file cannot contain a header row.

The following are valid examples:

```
Joe,Stanley,Joe Stanley,123,4587,1418,Warehouse Staff
Georgia,Smith,,123,4654,6884,Warehouse Staff
,,Billy Randall,123,4727,3492,Warehouse Staff
Frank,Powell,,,123:4639,3160,Warehouse Staff
```

To Import Users From a CSV File:

- Navigate to **Users | Users** and select the Import button from the toolbar.
- Browse to and select the CSV File you wish to import the users from, then click **OK**.
- The Users records are created and a message displayed to indicate the action was successful.

CSV Event Export

The Event Export feature enables you to extract event data as a CSV file which can then be formatted and manipulated as required to create custom reports.

To Export Events:

- Navigate to **Monitoring | Events** and select the Export button from the toolbar.
- Select the date range you wish to include events from, then click **OK**. A CSV file is created.

  Depending on your browser settings, you may be prompted to save the file otherwise it is downloaded automatically to your Downloads folder.

Feature Enhancements (2.10.030)

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

- The input limit/maximum length for both Facility Codes and Card Numbers is now set to 10.
- CTRL+Click and Shift+Click selection has been implemented for:
  - Access Level (Area Groups, Doors, Door Groups, Floor Groups, Elevator Groups, Menu Groups)
  - Area Groups (Areas)
  - Door Groups (Doors)
  - Output Groups (Outputs)
  - Schedules (Holiday Groups)
  - Users (Access Levels)
  - Holiday Groups (Holidays)

  This allow you to select multiple items that have been assigned to the record (such as the number of doors assigned to a door group) and delete them in one action rather than having to delete each item individually

Issues Resolved (2.10.030)

This release resolves a number of issues:

- Clicking Live View on the All Events page no longer causes the clock to speed up.
- If a door has been deleted it no longer appears as 'undefined' in the User Wizard .
- Area status is now correctly displayed when an area is in Exit Delay.
- When programming a Phone Number, the Secondary Phone Number field is now disabled/dimmed out unless an operating schedule has been defined.
- When programming the Contact ID Service through the Security Wizard the second phone number is now correctly labeled and linked to the Backup Phone Number.
- Changing the Controller time to 12:00 noon now displays the time correctly as 12:00pm and not 12:00am.
- Setting he Controller time to use the time and date of the PC now sets the clock to the current second, not just the current minute.
- The Logged on at field on the home page now uses the same data format as the Protege WX clock.
- When assigning an operating schedule to a menu group, the secondary menu group is now activated when the schedule ends.
- Addresses are only marked as duplicates under the Expander Addressing when both the expander type and address match.
- When adding a keypad through the wizard only 2 keypad inputs are now created.
- A number of minor/cosmetic corrections to the user interface.

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