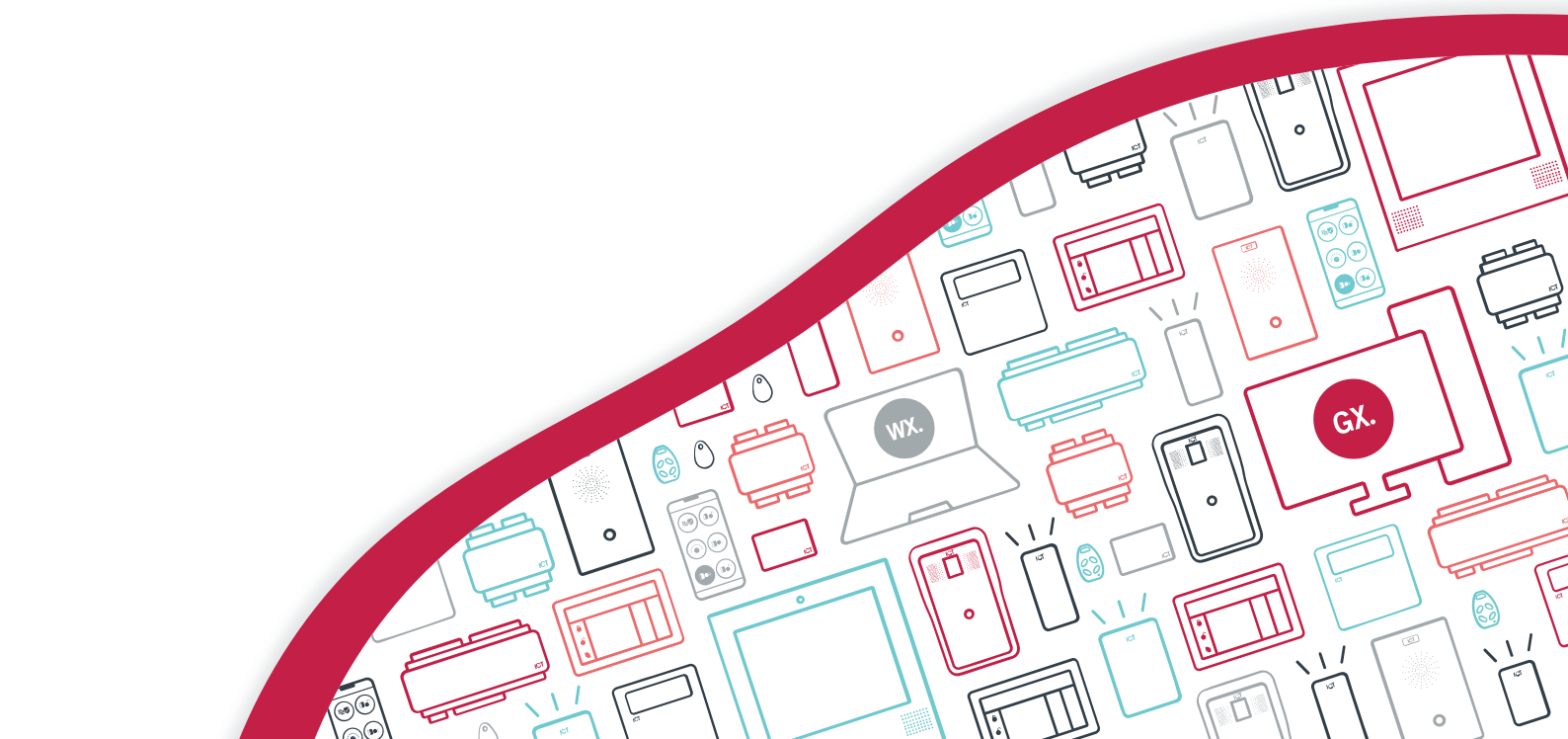
Integrated Control Technology

Protege GX Offline Wireless Lock Support

Release Notes | Protege GX 4.3.361 and Firmware 2.08.1453



Last Published: 31-May-24 3:18 PM

Contents

Introduction

ICT is excited to announce software and firmware support for Protege wireless locks operating in offline mode. The following versions are intended to be used together as part of the offline wireless locking system:

- Protege GX software version 4.3.361
- Protege GX controller firmware version 2.08.1453

This document includes all changes since the previous releases:

- Protege GX version 4.3.342
- Protege GX controller firmware version 2.08.1411

For a full release history of previous changes, see the release notes for those versions on the ICT website.

Get in touch with your ICT sales representative to discuss whether wireless locks are right for your site.

Changes to Supported Versions

In this version, ICT is dropping support for some Windows operating systems and SQL Server versions. These versions have reached end-of-life and are no longer supported by Microsoft.

- Windows 8.1 (Microsoft ended support in January 2023)
- Windows Server 2012 (Microsoft ended support in October 2023)
- SQL Server 2008 (Microsoft ended support in September 2019)
- SQL Server 2012 (Microsoft ended support in July 2022)

ICT recommends upgrading to the latest supported versions (see below) to ensure that your site receives cybersecurity updates, bug fixes and features from Microsoft and ICT.

New software versions, including this one, will not be tested on unsupported Windows and SQL Server versions. Sites may continue to use these unsupported versions, but upgrading the Protege GX software is at the customer's own risk and new features may not work correctly. ICT Technical Support reserves the right to request that any issues be replicated on a supported operating system and/or SQL Server version.

Supported Operating Systems

Operating System	Edition	Architecture
Microsoft Windows Server 2022	Standard, Datacenter	64-bit
Microsoft Windows Server 2019	Standard, Datacenter	64-bit
Microsoft Windows Server 2016	Standard, Datacenter	64-bit
Microsoft Windows 11	Pro, Business, Enterprise	64-bit
Microsoft Windows 10	Professional, Enterprise	32 / 64-bit

SQL Server Compatible Versions

The Protege GX application uses a non-proprietary open SQL database engine to store and share information. The software is compatible with SQL 2014, 2016, 2017 and 2019 in Standard, Express, and Enterprise editions.

The Express edition is a scaled down, free edition of SQL Server that includes the core database engine and functionality. The Express version of SQL supports a database size of up to 10 GB.

To obtain either SQL or SQL Express, download the appropriate installer from the Microsoft website. It is also recommended to download SQL Server Management Studio from Microsoft in order to configure SQL. Download the latest general availability (GA) version of SSMS from the Microsoft website.

Note: SQL Server 2014 (SP2) for 32-bit installation or SQL 2016 (SP2) for 64-bit installation.

Supported Hardware

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

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

Older Controller Limitation

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

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

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

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

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

Upgrading Protege GX to the Latest Build

To upgrade to the latest version, you may be required to uninstall the previous version first. The installer will inform you if this is the case.

1. Prior to performing an upgrade, you should always back up your database:
   - Open the Protege GX application and log in using an operator account with administrative permissions, or at minimum the ability to perform system functions.
   - Select **Global | Global settings** from the main menu.
   - Under the **Main database backup** options, select **Backup now**.

   Wait for the backup to be completed before proceeding.
2. Run the installation for the server:
   - Run the supplied setup file (setup.exe) and follow the onscreen instructions.
   - When the installer is launched it looks for the previous version of Protege GX installed on the local workstation and upgrades it to the latest build.
   - Progress is displayed as the database is upgraded and the application installed.
3. Run the installer again on each client machine to update the client interface.

Detailed installation instructions can be found in the Protege GX Installation Manual.

Upgrading Firmware

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

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

Upgrading Firmware from the Protege GX User Interface

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

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

Protege GX 4.3.361 and 2.08.1453

Protege Wireless Lock Support

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

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

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

Offline Wireless Lock Features

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

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

Feature Enhancements (4.3.361)

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

Access Events

- Added new events that are used when a user attempts to gain access at a door or elevator car, but does not have any access levels which allow access to that record. The events are:

- User John Doe Door Not Allowed Office Door Using any Access Level
- User John Doe Access Level Schedule Not Valid Office Door Using any Access Level
- User John Doe Denied by Elevator Group at South Elevator Using any Access Level

You may need to edit existing event filters to ensure that these events are displayed in reports and status pages.

Performance Improvements

- The door and access level lists are now paginated, improving the loading times for pages when there are large numbers of records.
- Added a search bar to the door and access level pages for quickly filtering the record list.
- Improved the loading times for the doors and access levels pages and system navigator.

Language Support

- The Protege GX thick client now supports Traditional Chinese.

Issues Resolved (Protege GX 4.3.361)

The following issues were resolved with this release.

- Resolved an issue where the single record download service would trigger a download when a user record was saved without any changes, or with changes only to fields that are not downloaded to the controller. Now user downloads are only triggered when there are changes to fields which need to be downloaded to the controller.
- Resolved an issue where running an event report for a period which had no events would return an error. Now it returns an empty event report.
- Resolved an issue where the **Detach** (breakout) button did not have a tooltip.
- Resolved an issue where the default schedule for elevator floors was displayed as Always instead of Never.
- Resolved an issue where the **Access direction** dropdown in **Users | Access levels | Door groups** was not populated when it was first opened.
- Resolved an issue where the incorrect Site ID was used when deleting smart readers, causing the delete event to not appear in reports for that site.
- Resolved an issue with custom reader formats where the even and odd parity settings were reversed.
- Resolved an issue where Salto door groups could not be added to access levels.
- Resolved an issue where the module addressing window would crash when there were a large number of modules connected.
- Resolved an issue where Protege GX installations using SQL Server versions older than 2016 could not download to the controller, add/edit door groups, or add/edit access levels containing door groups after upgrading to version 4.3.341.5.
- Resolved an issue where muster reports did not complete when there were a large number of access events with custom credentials in the reporting period.
- Resolved an issue where opening a user from an event could open the wrong user record if the list was paginated.
- Resolved an issue where the default inactivity periods were not being applied when a user was added from a credential event.
- Resolved an issue where status pages did not display the record names of muster reports.
- Fixed a visual issue with the pagination and quick search features in detached windows.
- Resolved an issue where the maximum value for the **Function 3 activation time** was incorrectly set to 128. It is now correctly set to 86,400.
- Resolved an issue where doors were assigned an incorrect host controller based on an unrelated output group.
- Resolved an issue where attendance reports did not deduct the early in time if the user was also late out.
- Resolved an issue where the **Forced open output** was not assigned to doors when a reader expander was added manually.

- Resolved an issue where the Door Duress trouble inputs were not created when a door was added manually.
- Resolved an issue where calendar actions were not filtered by record groups in the web client.
- Resolved an issue where logging in with Windows Authentication randomly failed approximately 25% of the time.

  If your site uses Windows Authentication, when you upgrade to this version of the Protege GX software you must also upgrade the Protege GX Web Client to version 1.47.1.3.
- Resolved an issue where upgrading a system with PIN encryption enabled would cause errors in the database.
- Resolved an issue where the download service would crash when there were a large number of users to download.
- Resolved performance issues with the data service in large systems.
- Resolved download service crashes in large systems.
- Resolved an issue where changing an output group from the areas page could cause the **Bell output group** to be reassigned to the **Exit delay output group**.
- Resolved an issue where navigating from the **Function outputs** tab to another door record tab would remove the outputs assigned in the **Outputs** tab.
- Resolved an issue where the users page would show a 'Save Changes' prompt when navigating away from the first user, even if no changes had been made.
- Resolved an issue where only the first custom alarm sound would be played, even when multiple custom sounds were programmed.
- Resolved an issue where saving a programmable function would blank out the **Door to control**, and saving a second time would remove the door record.
- Resolved an issue where deleting a door record would automatically delete its associated trouble inputs, but no 'Trouble Input Deleted' events were logged.
- Resolved an issue where changing an operator with the No Access role caused a network error.
- Resolved an issue with the Finnish language version where the controller wizard did not add reader expanders if a keypad was also added.
- Resolved an issue with the Schindler integration where it was not possible to select the controller used for the integration in the SOM output programming.
- Resolved an issue where visitor notification emails failed to send, preventing visitors from signing in.
- Resolved an issue where the Salto SHIP integration periodically went offline and the Protege GX download server crashed.
- Resolved an issue where controllers would drop offline and come back online regularly.
- Resolved an issue where entry and exit events using credential types were not included in the **Users | Users | Attendance** tab.
- Resolved an issue where clicking **Refresh** on the module addressing page would cause an error or crash the client.
- Resolved an issue where operators without the default Administrator role could not get card templates or floor plans via the SOAP API.
- Resolved an issue where only the default Admin operator could add in/out events in the **Users | Users | Attendance** tab.
- Resolved an issue where multi-selecting and editing doors or access levels from a tab other than **General** could cause some fields to be cleared.

High Data Usage on 4G Modems

In some recent versions of Protege GX there is unexpectedly high data usage on controllers connected by 4G modems. This can be caused by the Protege GX regularly contacting all controllers to improve status reporting from the event service.

If you are experiencing high data usage on metered (low data) connections, you can turn off these regular "check-ins". Be aware that this may increase the chance of controllers dropping offline.

1. Stop the Protege GX services.
2. In the File Explorer, navigate to the installation directory: C:\Program Files (x86)\Integrated Control Technology\Protege GX
3. Open GXSV.exe.config.

   Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

4. Directly under the **<configuration>** tag, add the following code:

```
<appSettings>
    <add key="gx:EnableUnknownStatusMitigation" value="false" />
</appSettings>
```

5. Save the file.
6. Open GXEvtSvr.exe.config.
7. Directly under the **<appSettings>** tag, add the following code:

```
<add key="EnableControllerConnectionWatchdog" value="0" />
```

8. Save the file.
9. Restart the Protege GX services.

Issues Resolved (Controller Firmware 2.08.1453)

The following issues were resolved with this release.

- Resolved an issue where changing the access level's expiry time to a time before the present would not cause access level outputs to deactivate.
- Resolved an issue where the controller could not communicate with the ThyssenKrupp system over the onboard ethernet connection.
- Resolved an issue where gaining access via a PRT-TS35 would cause the controller to reboot.
- Resolved an issue where the keypad's Installer menu did not display the correct IP address of the controller.
- Resolved an issue with the KONE HLI integration where the call types programmed in Protege GX were not sent to the KONE system.

  If your site has an additional controller programmed with the Otis HLI integration as a workaround, this record can now be deleted. Ensure that the user records are programmed correctly for the KONE integration.

- Resolved an issue where the 4G modem could become stuck in the 'Not Registered - Seeking' state indefinitely.
- Resolved an issue with low level elevator integration where elevators would deny access to any credential programmed in the second row of access cards.
- Resolved an issue where custom HTTPS certificates with intermediate certificates could not be loaded onto the controller.
- Resolved an issue where controllers would fail to come back online with the Report IP server after a disconnection.
- Resolved an issue where the 'System Restarted' trouble input did not open after a system restart.
- Resolved an issue where there was no reader feedback when a user was denied access by interlock.
- Resolved an issue where controllers would not recognize door inputs on other controllers after a power cycle.

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