Integrated Control Technology

Protege GX Offline Wireless Locking System

Release Notes | July 2025

Last Published: 30-Jul-25 3:56 PM

Contents

Introduction

ICT is pleased to announce a new software and firmware release package for the Protege offline wireless locking system. This includes:

- Protege GX version 4.3.387.2
- Protege Config App version 1.0.5.26
- Protege GX controller firmware 2.08.1514
- TSL card reader firmware 1.05.385
- Wireless lock firmware 1.1.098

For best performance, we recommend that you use all of these software and firmware versions together in your Protege GX offline locking system.

This document includes all changes related to the Protege GX offline locking system since its initial release in May 2024, as well as some other relevant software and firmware updates that may affect your sites.

Other Important Updates

Apart from updates to the offline wireless locking system, these versions include some significant changes that may affect your Protege GX site. Read this document carefully to understand what preparation and actions are required when you upgrade to this version.

In particular, be aware of the following changes:

- If your system uses **cross controller operations**, you must complete some additional programming when you upgrade the system. For more information, see Cross Controller Groups (page 8).
- If your system uses the **web client, mobile app or any SOAP service integration**, you must enable HTTPS before upgrading to this software version. Protege GX will no longer allow unencrypted HTTP connections. For more information, see Password Security Enhancements (page 9).
- If your system uses **SIA reporting services**, you must inform your monitoring station about some updates to reporting codes. For more information, see SIA Protocol Updates (page 11).

For more information about changes that are not related to wireless locks, contact ICT Technical Support.

Upgrading TSL Readers

The upgrade process for your TSL update point readers may differ depending on the current hardware and firmware versions used on your site. For more information, see TSL Reader Firmware Support (page 14).

Wireless Lock System Updates

Protege Rear Mount Mortise Wireless Lock

The wireless locking system now supports the Protege Rear Mount Mortise Wireless Lock. This lock has the same functionality as the Cartridge Mortise Wireless Lock but the electronics are housed in a discrete module installed on the rear side of the door, making it simple to retrofit to existing doors.

Feature Enhancements

Optional Blocklist

The blocklist is a useful tool for quickly responding to lost credentials or removing access from users, but it can be inconvenient in day-to-day operations. The new **Blocklist creation** setting (**Global | Sites | Offline wireless locks**) allows you to choose what happens when a user or credential is deleted: automatically add them to the blocklist, don't add them, or prompt the operator to choose on a case-by-case basis.

Door Open Events

Door open events are now disabled by default, saving valuable card storage space for important events and alerts. You can enable them for all locks using the **Enable door open events** setting in **Global | Sites | Offline wireless locks**, or for individual locks in **Programming | Doors | Offline wireless lock settings**.

Issues Resolved

Lock Operation

- Mitigated unexpected behavior in motorized deadbolts during locking and unlocking.
- Resolved unexpected privacy mode behavior for mortise locks.
- The LED will no longer flicker when manually toggling the motorized deadbolt.
- Wireless locks will no longer follow schedules while in toggle mode, preventing users from overriding the schedule.
- Resolved an issue where MIFARE Classic cards could be denied access due to full event storage even when the storage wasn't full yet.
- Resolved an issue where the emergency unlock feature did not work correctly when there were multiple controllers using offline wireless locks.

Software UI

- Resolved an issue where the **Connection type** field did not appear in the Find tool on the doors page.
- Improved the names for wireless lock-related settings in the user interface to make them more intuitive.
- Updated the default card profile settings for MIFARE Classic 1K credentials. These now allow space for access and events, but not the blocklist by default (as there is not enough space for all three).

Events and Status

- Resolved an issue where spurious 'Late Open' events were occasionally generated by wireless locks.
- Resolved an issue where update point readers configured as exit readers would generate 'Entry' events.
- Improved consistency of events generated by wireless locks.
- Resolved an issue where locks persistently showed the **Update required** status whenever the blocklist was empty.
- Resolved an issue where deleting data from the config app after initializing the lock would make it impossible to update the lock's status in the software.

- Resolved an issue where the lock status might not be correctly updated after initializing a lock and upgrading its firmware from an iOS device.

Update Point Reader

- Resolved an issue where cards that did not match a card profile could not gain access at update point readers.
- Improved the read/write speed for MIFARE Classic cards at the update point reader.
- Mitigated an issue where MIFARE Classic cards could become corrupted if pulled away from the update point reader too soon.
- Improved the read speed of DESFire cards at the update point reader.

Config App

- Resolved an issue where the config app could hang when updating a lock if only the blocklist had changed.
- The config app now correctly removes the encryption keys when you clear the site data.

Known Issues

ICT would like to make you aware of the following new known issues that affect the offline wireless locking system:

- 'Card Expired' events do not include the relevant card number.
- Some 'Door Locked' events may be generated twice.
- If an installer updates a lock, then deletes the data from their config app, the lock's status will remain as **Update required** indefinitely. To resolve this, use the **Force update** command and update the lock again, then badge your config app at an update point reader.

For more known issues, see the Protege Wireless Lock Configuration Guide.

Other Updates

This section covers other important updates included in the software and firmware versions that may be relevant to your system.

Cross Controller Groups

All Protege GX versions after 4.3.373 include cross controller groups, a new feature that streamlines cross controller programming and unlocks the power of the Protege GX Enterprise Download Server. With a small amount of initial preparation from the integrator, the enterprise download server can handle downloads to many linked controllers much more efficiently than the existing download service.

Cross controller groups define which controllers can use **cross controller operations**. Controllers in the same cross controller group can communicate with each other, allowing them to share inputs, outputs and other records. When you are programming the site, the user interface will only allow you to select resources in the same cross controller group. Any controllers that are not in cross controller groups will operate standalone, using only the resources available on that controller.

If the site uses cross controller operations, you must create cross controller groups when you upgrade to this version. This is required even if the site will not use the enterprise download server.

Running the Cross Controller Group Report

The Protege GX database can generate a report on the 'implicit cross controller groups' created by programming links between controllers. This report is generated by a stored procedure which is available in Protege GX version 4.3.386 and higher.

> The stored procedure can take up to a minute to run and may block some database tables during the process. We recommend you run this report during a period of low activity (e.g. immediately after upgrading the software). Alternatively, create a backup and restore it to a test machine to run the stored procedure on.

To run the stored procedure:

1. Run SQL Server Management Studio on the machine with the Protege GX databases installed.
2. Connect to the ProtegeGX server instance.
3. Expand the **Databases** node. Right click on the ProtegeGX database and select **New Query**.
4. Enter the following query:
   ```
   SET TRANSACTION ISOLATION LEVEL READ UNCOMMITTED
   EXEC ControllerGroupingReport
   ```
5. Click **Execute**.

The stored procedure will generate a report showing the following:

- **Section 1**: Number of implicit cross controller groups created by the download service based on programming links.
- **Section 2**: Number of explicit cross controller groups created by the operator.
- **Section 3**: List of the controllers in each implicit cross controller group.
- **Section 4**: List of the controllers in each explicit cross controller group.
- **Section 5**: List of the programming links between controllers, showing why two controllers are in the same implicit group.

  > Please note that some programming links may not be relevant. For example, input types may show spurious programming links based on an incorrect Host Controller assignment. You can disregard these irrelevant links.

If the report does not show any implicit cross controller groups, you do not need to program any cross controller groups.

If the report does show cross controller programming, you have two options:

- Program explicit cross controller groups that match the existing implicit cross controller groups. Any controllers without programming links should be left as standalone.
- Remove the programming links (if they were unintentional or not required).

  Protege GX will not correct any existing programming that is not consistent with the new cross controller groups.

After programming cross controller groups, you can run the stored procedure again to make sure that each implicit cross controller group has an equivalent explicit cross controller group.

Creating Cross Controller Groups

To create cross controller groups:

1. Plan out the cross controller groups required for your system.
2. In Protege GX, navigate to **Sites | Cross controller groups**.
3. Add a new cross controller group with a descriptive name (e.g. Newmarket Apartments Common Areas).
4. Click **Add** and select the controllers that will be in this group.
5. Click **OK**.
6. Click **Save**.

When you add a new controller through the controller wizard you can select a **Cross controller group** to add it to or choose not to add it to a cross controller group. You can update the cross controller groups later as the needs of your system change.

When programming the system, you will see that the **Programming mode** dropdown in the toolbar has been replaced by a **Local** checkbox. This allows you to select whether you are programming with all resources in the cross controller group or only those on the local controller. In addition, the toolbar displays which **Cross controller group** each record belongs to.

Password Security Enhancements

This version of Protege GX includes considerable improvements to the security of passwords used by system operators, following modern best practices for password construction and secure design.

In summary, the changes are:

- All operator passwords must have at least 8 characters. Blank passwords are not allowed and the default admin password must be changed on first login.
- There are no restrictions on the types of characters used within a password.
- It is no longer possible for an operator to set a permanent password for another operator. The first operator can set a temporary password that the second operator must change when they first log in.
- The new **Change password on next login** option in **Global | Operators** enables you to force another operator to change their password.
- Passwords must always be sent over encrypted connections to ensure that they are secure.
  - It is no longer possible to install Protege GX with no communication security. When upgrading or installing, you must select either TLS or Windows Authentication to provide an encrypted connection.
  - The Protege GX SOAP Service no longer allows unencrypted communications over HTTP (port 8030). Instead, use HTTPS over port 8040.
  - The Protege GX Web Client no longer allows browsers to connect over HTTP (port 8050). Instead, use HTTPS over port 8060.

- The data structure used for logging in with the SOAP API has changed: `LogonType` 1 has been deprecated and is no longer available. For more information, request an updated copy of the Protege GX SOAP API Specification from ICT.

Upgrading to this Version

This version of Protege GX requires upgrades to other software components. **You must upgrade all software at the same time.** The software is not backwards compatible.

Software	Required Version
Protege GX Server and Client	4.3.370.1 or higher
Protege GX SOAP Service	1.7.0.0 or higher
Protege GX Web Client	1.48.0.4 or higher

Before Upgrading

We recommend you complete the following changes before you upgrade any Protege GX components. This allows you to confirm that your integrations and clients can function over HTTPS before the encryption requirements are in place, so upgrading should be a seamless transition.

- All SOAP integrations that use HTTP must be updated to use HTTPS. You may need to install a trusted third-party SSL certificate on your SOAP server - see the Protege GX SOAP Service Installation Manual for instructions.
- All operators accessing the web client over HTTP must now use HTTPS. For example, you may need to update URLs and bookmarks used by end users.

  If operators were using the HTTP version of the web client previously, you may need to install a trusted third-party HTTPS certificate on the web server to enable them to securely connect over HTTPS. See the Protege GX Web Client Installation Manual for instructions.
- Update the place configuration in your Protege Mobile App to use the HTTPS URL for the web client. This will also require a third-party HTTPS certificate on the web server.
- Custom SOAP integrations may need to be updated. If `LogonType` 1 is used in the application, this must be changed to another `LogonType`.
- If your site uses a Protege Vandal Resistant Touchscreen Entry Station with Protege GX Directory Integration, **do not upgrade Protege GX**. This integration will no longer function with this software version, as the entry station is unable to connect to the SOAP service over HTTPS.

  Contact ICT to discuss options for upgrading your system.

After Upgrading

Some additional tasks are required after upgrading the Protege GX server, SOAP service and web client.

- You must upgrade the Protege GX server and all client installations at the same time. Older client versions will not function with the new server version.
- When upgrading, you must select either TLS or Windows Authentication for the security mode. None is no longer available.
- All operators will be forced to update their passwords when they first log in after the software is upgraded. This ensures that all passwords meet the new security requirements. Operators can change their passwords in either the thick client or the web client.
- Operators using the mobile app must update their passwords in the thick client or web client, then reconnect to their place in the app.
- In addition, the operator passwords used by SOAP integrations must be updated. After installing the new software, log in to Protege GX using the SOAP operator's details and update the password. Then update the password in the configuration for the service.

  This applies to the following services and integrations:

- ICT Data Sync Service
- Protege Tenancy Portal Sync Service
- Milestone Bidirectional Integration Service
- KeyWatcher Integration Service
- KeySecure Integration Service
- Any custom integration using the SOAP service

SIA Protocol Updates

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

The following alarm and restore codes have been updated:

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

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

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

Over-The-Network Upgrades for TSL Readers

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

Over-the-network upgrades are available for versions after 1.05.382. To upgrade your existing TSL readers to this version, see Upgrading TSL Readers.

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

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

This feature requires the following firmware versions:

Component	Firmware Version
Protege GX Controller	2.08.1498

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

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

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

Upgrading Software and Firmware

This section contains instructions for upgrading the software and firmware components required for this wireless lock release.

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 Controller Firmware

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

Before Upgrading Firmware

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

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

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

Upgrading Firmware from the Protege GX User Interface

1. Open and log in to the Protege GX application and ensure that you have a connection to the controller that you wish to upgrade.
2. From the main menu, select **Sites | Controllers**.
3. Right click on a controller and select **Update firmware**.
4. Click the **[...]** button and browse to the supplied firmware (.bin) file.
5. Choose which controller(s) to update by selecting the **Include** option. Only the selected controller(s) will be updated.
6. Click **Update** to commence the firmware upgrade procedure.

   The upgrade can take up to 10 minutes per controller to complete. Once complete, the controller is automatically restarted.
7. On completion of a firmware upgrade a download is required to update controller programming. Right click on the controller record and select **Force download**.

TSL Reader Firmware Support

The first hardware revision of the TSL reader does not support newer firmware. If you purchased TSL readers in 2023/2024, before upgrading you must check whether your TSL reader supports the new firmware version.

If your readers are connected by RS-485 or OSDP, you can find out this information from the controller's web interface:

1. Upgrade your controller's firmware to the latest version (2.08.1498 or higher).
2. If one or more TSL readers is connected to a reader expander, upgrade the reader expander firmware to the latest version (1.12.605).
3. Log in to the controller's web interface and navigate to **Application Software**.
4. Under **Update Module Firmware**, expand the **Module** dropdown. This allows you to see the current firmware versions of your connected TSL readers.

Current Firmware Version	Supports Upgrade?	Action
1.05.373 and earlier	No	Do not upgrade.
1.05.374-375	Depends on hardware revision	Readers with the later hardware revision can be upgraded. Make a list of the readers' serial numbers from the **Module** dropdown. Send this list to ICT Technical Support and ask which readers have the later hardware revision. For those with newer hardware, upgrade the firmware to version 1.05.382 using the separate upgrade tool provided by ICT (see next page). Do not upgrade readers with older hardware.
1.05.376-381	Yes	First, upgrade the firmware to version 1.05.382 using the separate upgrade tool provided by ICT (see next page). Then, upgrade the firmware to the latest version over the network (see next page).
1.05.382 and higher	Yes	Upgrade the firmware to the latest version over the network (see next page).

Updating TSL Reader Firmware to 1.05.382

To upgrade your TSL reader from an earlier version to 1.05.382 or higher, you must first upgrade to firmware to version 1.05.382. After this, you can upgrade the reader firmware over the network from the controller's web interface.

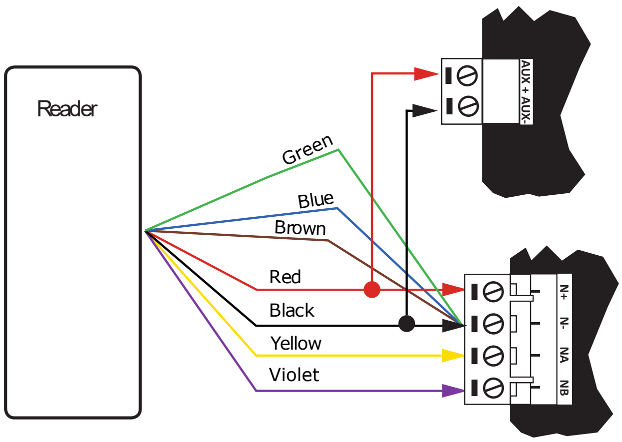
You will need a command-line tool provided by ICT, which upgrades both the application and boot firmware. You will also need an RS-485 USB Converter to connect the TSL reader to a computer.

Do not allow the TSL reader to lose power during the upgrade process. This can render the device non-functional.

To upgrade the TSL reader:

1. Plug the RS-485 USB Converter into your computer. Open the **Device Manager**. Under **Ports (COM & LPT)**, identify the serial port that the device is connected to (e.g. COM3).
2. Put the reader into boot mode by connecting the green, blue and brown wires to the black (N-) wire.

   Alternatively, you can use the Protege Config App to apply the **Device Mode: Firmware Update Mode** TLV within 2 minutes of the reader starting up.
3. Connect the reader to the RS-485 USB converter as pictured below.



4. The LEDs on the reader will flash blue and green to indicate it is starting in boot mode. The flashes will then slow to indicate the reader is now in boot mode and ready for the firmware update.

   You have approximately 30 seconds from the time you power the reader on to load the firmware.
5. **Disconnect the green, blue and brown wires from the black wire before running the upgrade tool.**
6. On the computer, open a command terminal.
7. Run the executable using a command similar to the following:

   ```
   "C:\Tools\tsl_otn_support_upgrade_tool_1_5_bd_382_P1B0.exe" --port COM3
   ```

   Ensure that you include the correct:
   - File location
   - Executable filename
   - COM port number
8. The terminal will show its progress as it upgrades the boot and application firmware. **Do not** allow the TSL reader to lose power during this process.
9. When the process is complete, disconnect the TSL reader from the converter.

Updating TSL Reader Firmware

TSL readers support over-the-network updates from the controller's web interface.

1. Connect the TSL reader to a controller or reader expander using ICT RS-485 or OSDP configuration.

   Readers connected in Wiegand configuration cannot be upgraded over the network.

2. Log in to the controller's web interface.
3. **In Protege GX**: Navigate to **Application Software**.
   In Protege WX: Navigate to **System | Application Software**.
4. Open the **Module** dropdown to view the card readers connected to the system.
   - TSL readers that support upgrade are displayed in white.
   - Readers that do not support upgrade are grayed out. This includes tSec readers, TSL readers with firmware below version 1.05.382, and third-party readers.
   - Readers are grayed out if the reader expander version is less than 1.12.605.
   - Readers connected via Wiegand are not displayed.
   - If no card readers appear in the dropdown, upgrade your controller to version 2.08.1498 (Protege GX) or 4.00.2261 (Protege WX), or higher.
5. Select the reader to upgrade.
6. Click **Upload Firmware** and select the new .bin file.
7. The web interface will show progress as the controller uploads the firmware to the reader. The reader will remain operational and respond to card badges and PINs while it is loading the new firmware.

   The warning in the **Update Module Firmware** section does not apply to TSL readers. Updating a TSL reader does not put the network into maintenance mode.

8. When the upload is complete, the reader will flash purple for approximately 10 seconds while it reboots. It will not respond to card badges or PINs during this time.
9. After rebooting, the reader will begin operating as normal with the new firmware. Click **OK** to close the window.

   You must refresh the page to see the new firmware version in the **Module** dropdown.

Upgrading Wireless Lock Firmware

Wireless lock firmware is upgraded automatically whenever you initialize or update a lock using the latest Protege Config App. To upgrade your locks:

1. Ensure that you are running the latest Protege Config App version. You can view the version in the side menu of the config app.
   If you do not have the latest app version, check for updates on the Apple App Store or Google Play Store.
2. If you are initializing new locks, simply badge the config app at an update point reader, then initialize the locks as normal.
3. If you wish to upgrade existing locks, in Protege GX navigate to **Programming | Doors**. Right click on each wireless lock and select **Force update**. Then badge the config app at an update point reader and update each lock as normal.
4. The config app will upgrade the lock's firmware before it initializes or updates it. The lock's LEDs will flash blue and red while the firmware is being upgraded. This may take a minute or two, so stay in Bluetooth® range of the lock until the lock flashes blue.
5. Repeat to upgrade each lock.
6. Return to the update point reader to upload the lock status updates to Protege GX.

We recommend that you only initialize or update up to 50 wireless locks at a time before returning to the update point reader to upload the data.