



Protege Wireless Lock

Configuration Guide



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

Last Published: 31-May-24 1:37 PM

Contents

Introduction	5
Offline Locking System Architecture	5
Offline Lock Programming Overview	6
Prerequisites	6
System Design Recommendations	8
Limitations	8
Setting up Offline Wireless Locking	9
Enabling Wireless Locks	9
Configuring Controllers	9
ICT Wireless Locking Credential Type	10
Creating Card Profiles	11
Setting up Update Point Readers	13
Configuring the TSL Reader	13
Programming the Reader Expander	14
Programming the Update Point Reader Door Type	14
Programming Offline Doors in Protege GX	16
Programming a Wireless Lock Door Type	16
Programming Doors	17
Offline Lock Limitations	17
Programming Access Records	17
Configuring Offline Locks	19
Enabling Users to Configure Offline Locks	19
Initializing an Offline Lock	19
Updating Offline Locks	20
Defaulting an Offline Lock	21
Deleting Programming from the Config App	22
Manual Commands for Offline Locks	22
Programming User Access	24
Programming Access Levels	24
Adding Users	24
Blocklist	25
Access Control Settings	26
Validating Lock Operation	27
Emergency Open	29

Additional Settings	30
Troubleshooting	32
Update Point Reader Operation	32
Update Point Reader LED and Beeper Indications	32
Lock Operation	33
Lock LED and Beeper Indications	33
User Access	35
Defaulting the System	36
System Administration	37
Backing up and Restoring the Database Encryption	37
Backing up the Certificate	37
Restoring the Certificate	38
Configuring the Single Record Download Service	38
Known Issues	40

Introduction

Protege wireless locks combine an advanced-technology, intelligent credential reader with leading locking system hardware. With no cabling necessary you can deploy integrated electronic access control in areas where traditional wired locking solutions are not possible. Wireless locks offer unprecedented flexibility, allowing businesses to significantly reduce labor and material costs.

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.

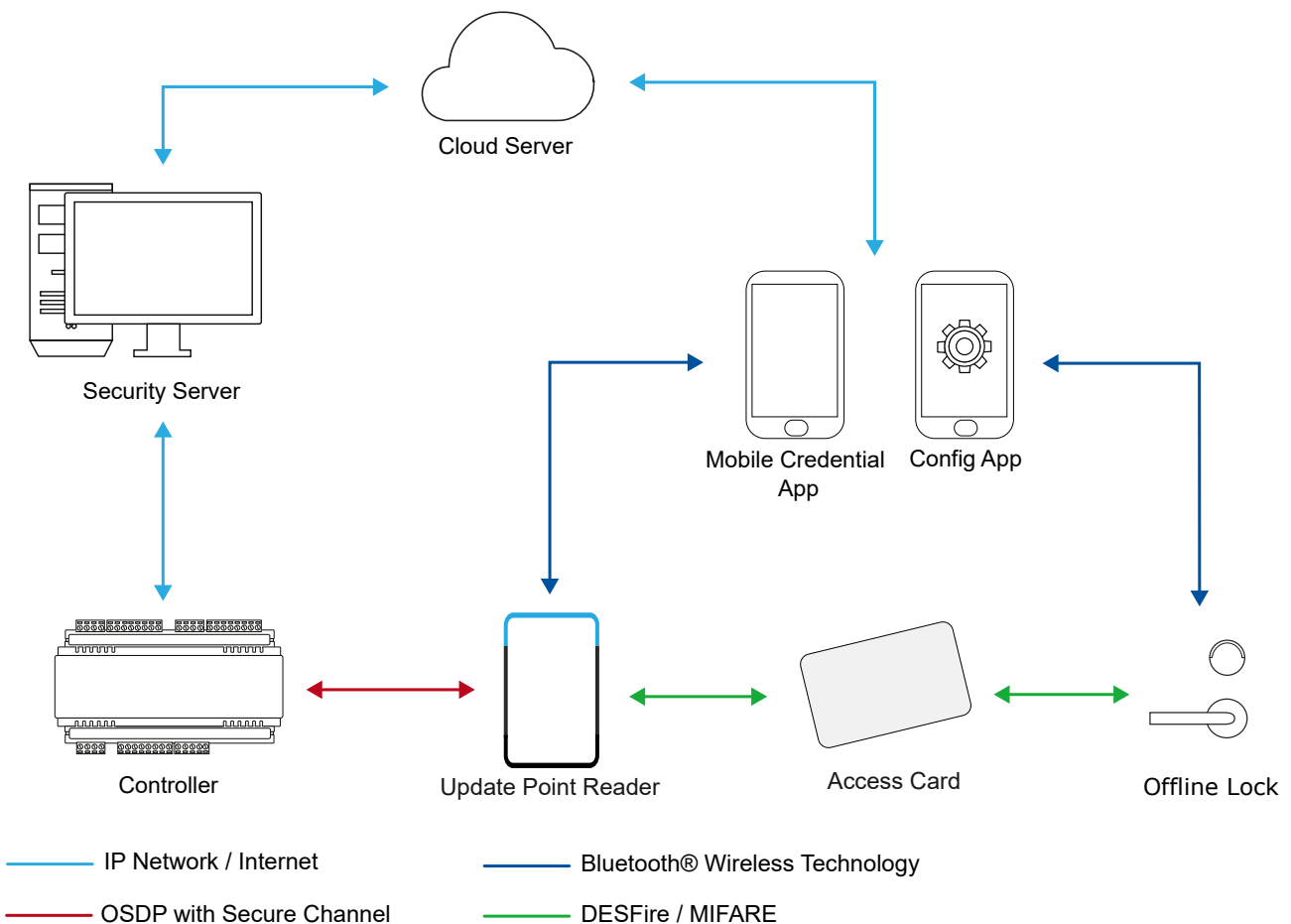
Configuration of offline locks is a simple process with the Protege Config App: program doors in the software, badge your mobile device at the update point, and download the programming to the locks using **Bluetooth® Wireless Technology**. No physical configuration or separate devices are required.

This document provides instructions for configuring, initializing and updating wireless locks, setting up update point readers and programming user access.

This document covers programming and configuration for the entire Protege wireless lock family. For physical installation instructions, see the relevant installation manual.

Offline Locking System Architecture

The offline wireless locking system uses end-to-end encrypted architecture with industry-standard communication and storage protocols.



Offline Lock Programming Overview

Because offline locks are not actively connected to the Protege system, all programming and data must be transferred from the software to the lock using the Protege Config App. The process is simple and can be easily carried out by any installer, technician or building manager with the appropriate permissions in the system.

1. Add or update doors, door types, schedules or other records in **Protege GX**.
2. Open the **Protege Config App** and badge at a **TSL update point reader** to retrieve the latest data.
3. The config app will use Bluetooth® Wireless Technology to detect nearby **offline locks** that need to be initialized or updated. Select each lock to:
 - Download the latest programming
 - Update the lock's firmware if there is a newer version available
 - Update the time on the lock
 - Retrieve the latest events
 - Retrieve the lock's battery status
4. Badge the config app at the update point reader again to upload the latest events and status to the system.

Prerequisites

All components used in the wireless lock system must use the minimum software and firmware versions described below.

Software

Component	Version	Notes
Protege GX	4.3.361.1 or higher	
SQL Server	2016 Service Pack 1 or later	
Protege Config App	1.0.4.14 or higher	You can download the Protege Config App for free from the Google Play Store or App Store. If you already have a Protege Mobile App account, the same account can be used for the config app. The app must have permission to use Bluetooth® (this may require access to your location).
Protege Mobile App	1.0.9.9 or higher	

Hardware

Component	Version	Notes
Protege GX Controller	2.08.1453 or higher	The controller must be operational and online with Protege GX.

Component	Version	Notes
TSL Reader	Update point reader firmware 1.05.373 or higher	<p>Each site needs one or more TSL readers to act as update point readers. When ordering, specify that the TSL reader will be used for offline wireless locks and the card technology in use (DESFire or MIFARE).</p> <p>Update point readers must be connected to the controller's onboard reader expander via OSDP wiring. For physical installation instructions, see the TSL Card Reader Installation Manual.</p> <p>TSL readers used as update point readers can support either DESFire or MIFARE cards, but not both. 125kHz cards are not supported on update point readers. This is under development and will be resolved with a TSL reader hardware revision.</p>
Protege Wireless Locks		<p>All wireless lock types are programmed the same way, but there are some differences in operation between mortise and deadbolt lock types.</p> <p>The config app will automatically upgrade the wireless lock firmware when a newer version is available.</p>
DESFire/MIFARE Cards or Tags	Request wireless lock credentials from ICT	<p>Wireless locks can read DESFire, MIFARE Classic and ICT Secured MIFARE cards/tags. DESFire cards are strongly recommended for improved security and resistance to cloning.</p> <p>As the offline wireless locking system uses data stored on the card, it is recommended to use cards with more storage space (4K or 8K cards).</p> <p>Due to limitations in the TSL reader, it is currently not possible to support both DESFire and MIFARE cards on the same site.</p>
Construction Card		<p>Order code: WL-CONST</p> <p>Construction cards are used to unlock locks before they are initialized and initialize them into the system. It is recommended that you have one card for each technician who will be installing locks.</p>
USB Desktop Encoder		<p>Order code: PRX-ENC-DT</p> <p>Optional component to streamline the process of enrolling users.</p>

Licensing

License	Order Code	Notes
Protege GX Door License	PRT-GX-DOR-1	1 license per wireless lock and update point reader installed in the system.
	PRT-GX-DOR-10	
	PRT-GX-DOR-50	
Mobile credentials	PRX-MCR	1 credential per installer who will be configuring wireless locks. This can be the same credential that is used for access with the Protege Mobile App.

System Design Recommendations

The offline wireless locking system relies on field components such as card readers and wireless locks with limited processing capacity. To ensure optimal performance, keep the following recommendations in mind when designing and programming the system:

- Update point readers should be connected to dedicated controllers that do not have a large number of other modules connected to them. A good rule of thumb is that each two-door controller can support two update point readers and an analog expander. Separate controllers should be used for any wired doors in the building.
- Maximum 1000 schedules (all schedules are included in this total, whether they are used by wireless locks or not).

Limitations

The wireless locking system currently has the following limitations:

- Only one update point reader can be connected to each reader port. Entry and exit readers are not supported.
- Each update point reader only supports one card technology (DESFire or MIFARE) alongside Bluetooth® wireless technology. 125kHz cards are not supported on update point readers.
- MIFARE Classic 1K cards do not support event collection due to the very small amount of data storage available on the card. Use larger cards to allow event storage and retrieval.
- The Protege GX SOAP Service can be used to make day-to-day changes to access records (users and access levels), but is not recommended for programming wireless door records or other initial configuration such as credential types and card profiles.

SOAP currently has the following limitations:

- Some initial configuration steps **must** be performed in the Protege GX client: enabling the integration in **Global | Sites | Site defaults** and configuring the reader expander.
- It is not possible to monitor wireless lock status or perform manual commands.
- It is not possible to encode user cards using a desktop encoder via SOAP. Encode cards using an update point reader instead.
- The default settings in **Global | Sites | Offline wireless locking** are not used when adding new records.
- SOAP does not apply the correct limitations to card profile records, resulting in invalid card data structures. Do not program these records via SOAP.
- It is possible to update some settings via SOAP that are not permitted in the Protege GX client. For example, records not used for wireless locks may display wireless lock-related settings and vice versa. When adding and editing records via SOAP, ensure that your program respects the rules imposed in the client software.

Validate all programming operations before deploying them to a live site. Records that are configured incorrectly must be fixed via the Protege GX client.

Setting up Offline Wireless Locking

To begin using offline wireless locks, you must enable them on your site and complete some initial setup.

Enabling Wireless Locks

When you enable wireless locks on a Protege GX site, Protege GX briefly connects to the ICT cloud server to securely generate encryption keys for use in the wireless locking system, then encrypts those keys in SQL Server.

Because of this encryption, enabling wireless locks is a permanent change and cannot be reversed without restoring a previous backup.

It is convenient to have internet access on the Protege GX server during the initial setup process, but this is not required.

1. If you have existing programming, it is recommended that you take a backup before enabling wireless lock integration.
 - In Protege GX navigate to **Global | Global settings**.
 - Under **Main database backup**, enter a **Backup path**.
 - Click **Backup now**.
2. Navigate to **Global | Sites | Site defaults**.
3. Check **Enable ICT wireless locking integration**.
4. Click **Save**.
5. A popup will warn you that this is a permanent change. Click **Yes**.
6. If the Protege GX server has internet access, it will connect to the ICT cloud server to generate encryption keys for the wireless locking system.
If the server does not have internet access, you will see a popup advising you to use manual key generation. Click **Yes**. To manually generate encryption keys:
 - Click **Generate** to generate an encryption key request file.
 - Transfer the request file to a computer that has internet access.
 - Browse to the URL shown in Protege GX and upload the request file.
 - Download the encryption key file and transfer it to a Protege GX server or client machine.
 - In Protege GX, click **Browse** and upload the encryption key file.
7. You will see a popup about the new wireless locking credential type (see next page).
8. The **Offline wireless locking** tab will now be available for this site. This tab enables you to set general options for the site, as well as the default settings for any new door and user records. For more information, see [Additional Settings](#) (page 30).

Configuring Controllers

The controllers on a wireless locking site need some specific configuration to ensure that the site functions correctly.

1. Each controller must have the correct **daylight savings and time zone settings**, as these are used to set the time on wireless locks.
2. **Encryption** must be enabled on every controller to secure communications between the controller and server.
3. Every controller with an update point reader connected must have the **onboard reader expander** enabled.

To configure the controllers:

1. If your region uses daylight savings:
 - Navigate to **Programming | Daylight savings**.
 - Using the **Controller** dropdown in the toolbar, check that every controller on site has a correct daylight savings record programmed.
 - Add any missing daylight savings records.
2. Navigate to **Sites | Controllers**.
3. In the **Configuration** tab ensure that each controller has the onboard reader expander enabled:
 - **Register as reader expander** must be set to an available address.
 - **Onboard reader lock outputs** should be set to Controller relay 3/4 outputs.
4. Ensure that **Encryption enabled** is checked for each controller. If not, click **Initialize controller encryption**.
5. In the **Time update** tab, set the **Time zone** correctly for every controller on site and save.

You must set the **Time zone** even if you are not using a time server to update the controller's time.

6. If the site does not use a time server, right click on each controller and select **Set controller date time**.

When any controller's time zone or daylight savings record is updated in Protege GX, all wireless locks will be marked as **Update required** even if they are not affected by this time change. Avoid updating time settings after the initial site setup (see previous page).

ICT Wireless Locking Credential Type

Wireless locks and update point readers use 34-bit credentials by default. When you enable wireless locking, the ICT Wireless Locking credential type is created automatically in **Sites | Credential types** with the following settings:

- **Format:** Wiegand
- **Wiegand or TLV format:**
#34bit__A, FACILITY, 16, MSB, BIN__B, CARD, 16, MSB, BIN__
PAAAAAAAAAAAAAAAAABBBBBBBBBBBBBBBB__XXXXXXXXXXXXXXXXXXXX....._
_.....XXXXXXXXXXXXXXXXXXXXO
- **Preceding characters:** 0
- **Trailing characters:** 0
- **Prefix:** None
- **Case sensitive:** Disabled
- **Wireless locking:** Enabled
- **Unique value:** Enabled

You can add alternative wireless locking credential types if a different Wiegand format is required:

1. Navigate to **Sites | Credential types**.
2. Add a new credential type.
3. Set the **Format** to Wiegand.
4. Enter the required **Wiegand or TLV format**.
5. Enable the **Wireless locking** setting.
6. Click **Save**.

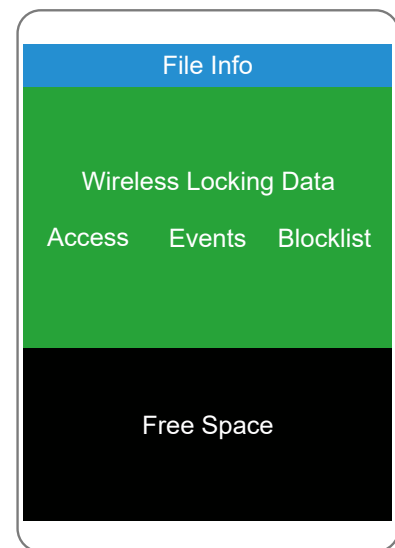
Wireless locking credential types can only be deleted once all current credentials of that type have been deleted and then expired from the blocklist. If you need to delete large numbers of credentials, you must stagger the changes to avoid reaching the maximum blocklist size (see page 25).

Creating Card Profiles

The offline wireless locking system uses DESFire and MIFARE cards to store user access data, events and the blocklist. Card profiles are templates for encoding this additional data into the space available on a card, using an update point reader or desktop encoder.

Each card is divided into three main sections:

- **File info:** Reserved system data (determined by the card format).
- **Wireless locking data:** All data used for the ICT offline wireless locking functionality.
 - **Access:** The user's facility and card numbers, doors, door groups, schedules and options. This only includes offline wireless locks, not wired doors.
 - **Events:** Events retrieved from locks.
 - **Blocklist:** The list of users and credentials which have been deleted or disabled.
- **Free space:** Any other files on the card, e.g. data for third-party systems.



Important Notes

- Both a card profile and a credential type are needed. The card profile determines how much storage is used for wireless locking data, whereas the credential type determines the format of the facility and card number.
- You must create one card profile for each card type (MIFARE/DESFire) and card size (1K/2K/4K/8K) that is used on site. This is not required for mobile credentials, as mobile phones have much more storage space than cards.

To preserve system security, **do not** create card profiles for card types that are not used on site (especially MIFARE cards).

- Once a card has been encoded, it is not possible to change the total size of the wireless locking file, the additional data section or the sectors used on a MIFARE card. However, it is possible to change the relative sizes of the separate data types within the wireless locking file (access, events, blocklist).
If the wireless locking file size changes (i.e. if you delete a card profile and create a new one for the same type of card), any cards that have already been encoded must be recalled, wiped and re-encoded.

Ensure that the card profile has been programmed correctly before encoding any cards.

- We recommend you allocate as much space as possible to wireless locking functions, as the functionality of the offline system may be limited if there is not enough space on the users' cards.
 - **Access:** If there is not enough space on the card for the user's personal access rights, encoding will fail. Avoid shrinking the access data after cards have been encoded.
 - **Events:** When the event storage is full, no more events can be stored on the card. Events can still be retrieved from locks using the config app or mobile app. Alternatively, if event collection is not required you may reduce this sector to 0 bytes.
 - **Blocklist:** If there is not enough space for the blocklist on user cards, there is a higher chance that deleted credentials will still be able to gain access to doors. The blocklist can still be propagated using the config app or mobile app.

Creating a Card Profile

1. Navigate to **Sites | Card profiles**.
2. Add a new card profile with a descriptive name (e.g. DESFire 4K Card Profile).
3. Select the **Card type**.

4. Select the **Card size** (the total amount of storage available on the card).
5. Click **Edit** to view and adjust the amount of space available on the card for access, events and blocklist. The defaults for **Access bytes**, **Event bytes** and **Blocklist bytes** are the recommended values. If required, you can adjust the available storage for each data type. For example, your site may need more **Free space** for other functions, so you could decrease the **Event bytes** value to create more space.

Some rules of thumb for programming card profiles:

- 256 bytes of access data will allow you to store about 30 records (doors, door groups and schedules) on each access card.
- Each event uses about 16 bytes of storage on the card.
- The total space used for wireless locking data must be a multiple of 16.
- If the card is not being used for other functions, you can eliminate the free space to provide more space for wireless locking.

It is currently not possible to reserve MIFARE sectors for other features. This will be addressed in future versions.

6. Click **Update**.
7. Ensure that the proportion of space used for wireless locking is correct (in the top right of the box). This cannot be changed later.
8. Click **Save**.
9. The software will warn you that the wireless locking file size cannot be changed. Click **Yes**.

Setting up Update Point Readers

Update point readers have special functionality that allows them to encode wireless lock access data and retrieve events from cards and mobile apps that are badged at the reader. They will also continue to perform standard access control functions, allowing you to install update point readers at the front door of the building or other chokepoints.

Any TSL reader connected to the controller's onboard reader expander can be used as an update point reader.

Configuring the TSL Reader

You must apply a special config to each TSL reader to configure it as an update point reader. This also sets the reader to OSDP mode.

1. Log in to the Protege Config App using your app account.
2. Navigate to **Reader Configuration**.
3. Select your **Credential Profile**.
4. Add a new **Reader Configuration** called Enable Update Point Reader.
5. Tap the **Add TLV** dropdown and select the **Device Mode** option.
6. Set the **Device Mode** to Wireless Lock Update Point Mode, then tap **Save**.

Once the required reader config is available in the config app, it can be applied to individual readers via Bluetooth® communication.

ICT card readers can only be programmed within 2 minutes of startup. In order to program the reader you will need to disconnect power and complete programming within 2 minutes of powering up.

When you view readers in the config app, each individual reader has a name based on its serial number. Most readers have a name in the format `_R<SERIALNUMBER>` (e.g. `_RF19E3331`). However, update point readers used for offline wireless locking systems have names in the format `_U<SERIALNUMBER>` (e.g. `_UF19E3331`).

Programming a Card Reader using the Protege Config App

1. Activate Bluetooth® on your device.
2. In the Config App, navigate to the **Reader Configuration** page and select the appropriate **Credential Profile**.
3. Tap the required config to apply to the reader. The selected config will be marked as ACTIVE.
4. Power cycle the reader that requires programming. The following steps must be completed in the next 2 minutes.
5. To apply the selected config to the nearest reader, place the device with the app close to the reader and tap **Scan Closest**.
 - The app should display Connecting to reader `_R<SERIALNUMBER>`. If there is no response, the device may need to be closer to the reader.
 - When programming is successful, the app will display the message Configuration of `_R<SERIALNUMBER>` successful and the reader will beep several times quickly and then restart.
 - If a power cycle is required, the app will display the message Failed to configure `_R<SERIALNUMBER>`. Configuration timeout. Please restart the reader.
6. To view and select from a list of nearby readers, tap **Select Reader**.
 - If the reader is compatible, its **Broadcast Address** (`_R<SERIALNUMBER>`) will be displayed in the list.
 - If only the reader model is displayed, this reader cannot be configured using the app.
 - The number to the right identifies the decibel response. The smaller the value (i.e. the closer to zero), the nearer the reader is to the device.

The **Bluetooth Proximity** setting in **Mobile Credential Settings** can be adjusted to exclude readers that are further away.

7. Identify the appropriate reader and tap **Apply**.
 - The app should display Connecting to reader _R<SERIALNUMBER>.
 - When programming is successful, the app will display the message Configuration of _R<SERIALNUMBER> successful and the reader will beep several times quickly and then restart.
 - If a power cycle is required, the app will display the message Failed to configure _R<SERIALNUMBER>. Configuration timeout. Please restart the reader.
 - If the reader is not compatible, the app will display the message Failed to configure <READER>. Reader disconnected.

After the reader has been updated, it will appear in the config app as _U<SERIALNUMBER> to indicate that it is an update point reader. You can still configure other functions such as the LED colors as normal.

Programming the Reader Expander

The TSL reader must be programmed as an update point reader in the reader expander module in Protege GX.

1. Navigate to **Expanders | Reader expanders**.
2. Select the controller's onboard reader expander, or add a new one at the **Register as reader expander** address (see page 9).
3. Set the **Port 1/2 network type** to ICT wireless lock update point reader (set Port 1, Port 2 or both depending on how many update point readers are connected).
4. The update point reader will use the custom credential type created above (see page 10). In the **Reader 1/2** tab, set the **Reader 1/2 format** to Custom credential.
5. Typically the update point reader is associated with a door (RD1 DR1 or DR2 by default), but it can instead be associated with an elevator car or even just used for updating cards without any additional function. If necessary, adjust the **Reader 1/2 mode** and **Reader 1/2 door** as required.
6. Click **Save**.
7. If controller encryption is not enabled, the software will enable it automatically to secure the wireless locking communications.
 - Click **Update** to enable encryption.
 - The server will enable encryption with the controller. When the message reads 'Succeeded', click **Close**.
8. Right click on the reader expander record and select **Update module**. Wait until the module update is complete, then click **Close**.
9. Right click on the reader expander again and click **Activate OSDP install mode**. This establishes secure communications between the controller and the update point reader.

Programming the Update Point Reader Door Type

If the update point reader is associated with a door, it needs a door type that will read the wireless lock credential type. This can also be used for other readers on site as required.

1. Navigate to **Programming | Door types**.
2. Click **Add** to add a new door type and give it a relevant name.
3. Set the **Entry reading mode** to Custom.
4. Under **Entry credential types**, click **Add**.
5. Select ICT Wireless Locking or another credential type you created above (see page 10) and click **OK**.
6. If the door has an exit reader, repeat the above steps for the **Exit reading mode** and **Exit credential types**.

7. Program any other settings that are needed for this door.
8. Click **Save**.
9. Navigate to **Programming | Doors**.
10. Select the door records that represent the update point readers.
11. Set the **Door type** to the one created above.
12. Click **Save**.
13. Assign the door type to any other wired doors in the system that need to read the same credential type.

Programming Offline Doors in Protege GX

Offline wireless locks are programmed in a similar way to regular doors: each lock needs a door record with a door type assigned to it.

Before you begin programming doors, you may wish to adjust the default settings in **Global | Sites | Offline wireless locking** so that the new door records have the correct defaults. Alternatively, you can program the basic door records first, then bulk update them from the site settings. For more information, see [Additional Settings](#) (page 30).

Programming a Wireless Lock Door Type

Door types determine the operating mode of each wireless lock.

1. Navigate to **Programming | Door types**.
2. Click **Add** to add a new door type and give it a relevant name (e.g. Offline Lock Office).
3. Set the **Entry reading mode** to Custom.
4. Under **Entry credential types**, click **Add**.
5. Select ICT Wireless Locking and click **OK**.
6. In the **Options** tab, set the **Lock operating mode** to determine how this lock will behave. The available lock operating modes are:
 - **Standard**: When a user gains access at the reader the door will unlock for the **Lock activation time** (**Programming | Doors | Offline wireless locking**), then lock again. Motorized deadbolts that are unlocked from the inside will also relock after the lock activation time.
 - **Office unlock**: A user with **Enable office unlock** can latch unlock the door by holding down the inside handle and badging at the reader. Once unlocked, the door will remain unlocked until the same process is repeated to lock it again.
 - **Toggle**: When any user gains access at the reader, the lock will toggle (change from locked to unlocked or back again).
 - **Exit leaves door unlocked**: The lock operates in standard mode, but when someone exits using the inside handle the door will remain unlocked. By default it will remain unlocked until someone badges their card to relock it. To automatically relock the door after a time period, enable **Exit leaves door unlocked time period** in **Programming | Doors | Offline wireless locking**.
 - **Exit leaves door unlocked + toggle**: The door operates in toggle mode and will also remain unlocked when someone exits using the inside handle.

Mortise locks support all of the above settings. Deadbolt locks only support Standard and Toggle modes.

7. Click **Save**.

Changing Operating Mode on Schedule

Wireless locks support changing the operating mode based on the time of day. For example, you may wish the door to operate in standard mode by default, but switch to office unlock mode during working hours.

To alter a lock's operating mode on a schedule:

1. Create the schedule in **Sites | Schedules**.
2. In **Programming | Door types**, create a primary door type (that will operate when the schedule is valid) and a secondary door type (that will operate when the schedule is invalid).
3. In the primary door type, set the **Operating schedule** and the **Secondary door type**.
4. Click **Save**.

Programming Doors

Each wireless lock in the system is represented by one door record in Protege GX.

1. Navigate to **Programming | Doors**.
2. Click **Add** to create a new door.
3. Enter a relevant **Name** for the wireless lock.
4. Enter a **Keypad display name**, or use the arrows to copy the name field. This is the name that will be displayed in the config app, so should succinctly describe the wireless lock's role and location.
5. Under **Setup**, set the **Connection type** to *Wireless offline*.
6. Set the **Door type** to the one created above.
7. If you want the door to unlock at specific times, set the **Unlock schedule**. During the unlock schedule the door will remain unlocked, even if a user attempts to toggle the lock back on.

Motorized deadbolt locks must be in Standard mode to use an unlock schedule.

8. In the **Offline wireless locking** tab you can program the operation of this lock.
 - **Options:** These will initially match the default options set in **Global | Sites | Offline wireless locking**. You can edit the settings for each lock separately as required. For more information, see *Additional Settings* (page 30).
 - If the door is using an unlock schedule, you can enable **Schedule operates late to open** to prevent the door from unlocking until the first user gains access.
 - Set the **Lock activation time** to determine how long the door will unlock for when the lock is in standard mode.

For motorized deadbolt locks, we recommend setting this value to 10 seconds or longer to give the user time to close the door before the bolt extends again.

- Set the **Door extended access time** to determine how long the door will unlock for when accessed by users with **User operates extended door access function** enabled.
9. Click **Save**.

Once the door has been programmed, you can see its **Status** in the record list. A new door record will display **Initialize required** until the physical lock has been initialized into the system.

Offline Lock Limitations

When programming offline locks, keep in mind that they are not connected to the rest of the system. This means that many standard Protege GX features will not work on offline locks.

As general principles, offline locks **cannot**:

- Respond to changes in other parts of the system (e.g. the door won't unlock when an area disarms).
- Affect other parts of the system (e.g. you can't disarm an area when the door is unlocked).
- Report events and alarms back to the software immediately (e.g. the lock can't raise an alarm when the door is forced).
- Act on manual commands such as lock, unlock and lockdown.

Programming Access Records

The access cards used to pass access data to offline locks have a very limited storage capacity, so they cannot carry all of the records needed for access. Because of this, some of this data must be programmed in advance and transferred to the lock using the Protege Config App.

As well as the configuration for the lock itself (i.e. door and door type settings), the following records used for user access must be programmed in advance:

- Schedules
- Holiday groups
- Door groups

We recommend that you program these records as part of the initial site setup so they will be added to the locks when you initialize them. Once you have programmed these records you can use them in access levels without updating the locks themselves.

Any schedules, holiday groups or door groups that are added or edited later cannot be used on the offline locks until they are updated using the config app (see page 20). Locks that are not updated will continue to use the previous settings and will deny access to any new records that they do not recognize.

To avoid unnecessary changes, it may be helpful to program separate records that are used only for access levels with wireless locks. That way you can update the records used for wired doors separately without triggering an update for the wireless locks.

Tip: Door groups in access levels use less storage on access cards than individual doors. If you have several communal doors in a building (e.g. ground floor facilities), program these as a door group to store access data more efficiently.

Configuring Offline Locks

When the update point reader and wireless lock programming are ready, you can initialize the locks using the Protege Config App. Once the lock has been initialized it will be able to read user cards, make access decisions, follow schedules and record events.

Because the lock is operating without an active connection to the system, whenever the programming is updated in the software an installer or technician will need to use the app to transfer the new programming to the lock.

See the [Troubleshooting](#) section for help with any issues during this process.

Enabling Users to Configure Offline Locks

Some users, such as installers and building managers, need access to initialize and update offline locks using the Protege Config App. This is managed separately from door access, allowing these users to update locks on apartments and other private areas without necessarily having access to unlock them.

First you must create an access level with access to configure wireless locks:

1. Navigate to **Users | Access levels**.
2. Add a new access level or select an existing one.
3. Check **Enable access to wireless lock config**.
4. In the **Doors** tab, add the door record associated with the update point reader.

If the update point reader is not associated with a door, add any door, area or elevator car from the same controller to the access level.

5. Click **Save**.

The access level must then be assigned to each user who will configure the locks. In addition, the user's mobile credential must be assigned to their record in Protege GX so that the system can identify the user when they badge the config app.

1. Navigate to **Users | Users** and select or add a user record.
2. Scroll down to the **Credentials** section and locate the wireless lock credential type created above.
3. Under **Credential**, enter the facility and card number of the user's mobile credential, separated by a colon (e.g. 10636:7482).

You can find this on the **Wireless Locks** page of the config app or in the wireless credential portal.

4. In the **Access levels** tab, add the access level programmed above.
5. Click **Save**.

Initializing an Offline Lock

Before a wireless lock can be used for access control, it must be **initialized** as part of the Protege system. This addresses the lock, downloads programming, and activates its Bluetooth® communications so that it can receive mobile credentials.

This process requires a **construction card** to activate the locks. These cards can also be used to unlock locks that have not been initialized yet, making it easy to move around the site.

To initialize a lock:

1. In Protege GX, you can view the doors with the **Initialize required** status in **Programming | Doors** or on a status page.

2. Ensure that your Protege GX user record has a mobile credential programmed and an access level that allows lock configuration (see previous page).
3. Turn on Bluetooth® on your mobile device.
4. Ensure that the device has internet access. This is only required the first time you log in to configure wireless locks.
5. Open the Protege Config App and log in.

If you have used this device to configure wireless locks on a different site, you may need to log out of the app, then back in.

6. Navigate to **Wireless Locks**.
7. Badge the phone at an update point reader. The controller will send the config app the latest information about the wireless locks programmed in Protege GX that need to be initialized or updated. The update point reader will rapidly flash purple while lock data is being transferred.
8. If there are a large number of locks to configure, they will be split into batches of 100. Select which batch of locks you will configure, then tap **OK**.
9. Select **New**. The app will display any doors that have been programmed in the software but not initialized.

The banner at the top of the screen displays when the lock configuration data was last updated from the software. Always make sure you have the latest programming before you begin configuring locks.
10. Locate the door record you want to program onto a lock and tap **Init + Update**.
11. Badge the construction card at the lock that needs to be initialized. This causes the lock to activate Bluetooth® and broadcast its ID for 2 minutes.
12. The config app will display all wireless locks in range that are currently uninitialized and broadcasting their IDs. If there is more than one lock in range, use the signal strength to identify the closest lock. Tap **Initialize**.
13. The app will initialize the lock, performing the following processes:
 - Check the lock's firmware version. If it is out of date and the lock has sufficient battery life remaining, install the latest firmware.

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.

- Program the lock with the settings from the door record in Protege GX, including the schedule and blocklist.
- Set the lock's time, time zone and daylight savings settings based on the controller's time.
- Record the lock's current battery status.

When this is all done, the app will notify you that the process is complete. The lock will flash white while it is updating, then flash blue to show that the update was successful and the lock is beginning normal operation. The lock is now ready to perform access control functions.

14. Badge again at an update point to upload the data from the config app back to Protege GX. This informs the system the lock has been initialized and updates its latest status.

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.

Updating Offline Locks

After they have been initialized, locks may need to be updated periodically to change their programmed settings. This follows much the same process.

1. In Protege GX, you can view the doors with the **Update required** status in **Programming | Doors** or on a status page.

Tip: Hover over the status to see whether the door needs a blocklist update. If only a blocklist update is required, the blocklist should naturally propagate through user access and there is typically no need to use the config app.

2. Ensure that your Protege GX user record has a mobile credential programmed and an access level that allows lock configuration (see page 19).
3. Turn on Bluetooth® on your mobile device.
4. Open the Protege Config App and log in.
5. Navigate to **Wireless Locks**.
6. Badge the phone at an update point reader. The controller will send the config app the latest information about the wireless locks programmed in Protege GX.
The update point reader will rapidly flash purple then flash green and unlock the door when the data transfer is complete.
7. If there are a large number of locks to configure, they will be split into batches of 100. Select which batch of locks you will configure, then tap **OK**.
8. The app will show a list of locks that need updating in the **Existing** tab. The **Update** button will turn solid blue when the corresponding lock is in Bluetooth® range.

The banner at the top of the app displays when the lock configuration data was last updated from the software. Always make sure you have the latest programming before you begin configuring locks.

9. Tap **Update** to update each lock in turn. The app will perform the following processes:
 - Check the lock's firmware version. If it is out of date and the lock has sufficient battery life remaining, install the latest firmware.
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.
 - Update the programming in the lock to match the software, including the lock's schedule and blocklist.
 - Update the lock's time, time zone and daylight savings settings based on the controller's time.
 - Record the latest events and current battery status.
10. The lock will flash white while it is updating, then flash blue to show that the update was successful and the lock is returning to normal operation.
11. Return and badge at the update point reader. This will upload the lock's latest events and status into the software.

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.

Defaulting an Offline Lock

Many lock settings, such as schedules and the name of the lock, can be updated using the normal update process. However, it may be necessary to default a lock in situations where:

- The lock is being removed from the site.
- The hardware is being replaced.
- The handing of the lock needs to be changed.

Defaulting a lock requires physical access to power cycle the lock.

1. In Protege GX, navigate to **Programming | Doors**.
2. Right click on the door that will be defaulted and select **Reinitialize**.

If this is not available, you must turn on **Enable lock reinitializing** in **Global | Sites | Offline wireless locking**.

3. Ensure that your Protege GX user record has a mobile credential programmed and an access level that allows lock configuration (see page 19).
4. Turn on Bluetooth® on your mobile device.
5. Open the Protege Config App and log in.
6. Navigate to **Wireless Locks**.
7. Badge the phone at an update point reader to retrieve the lock data.
8. Unlock the wireless lock and open the door.
9. Unscrew the battery cover and pull out one of the batteries. Wait for a few seconds and then reinsert it. After the lock restarts, it will allow defaulting for 2 minutes.
10. At the bottom of the list of locks, tap **Default**. The phone will scan for nearby locks.

All nearby locks will be displayed, but only a lock that has recently been power cycled can be defaulted.

11. Use the signal strength to identify the lock to default and tap **Default Lock**.
12. When the defaulting process is complete, the reader LED will flash white five times. The app will display "Lock Defaulted".

Deleting Programming from the Config App

The config app can only hold lock programming for one site at a time. If you are moving between sites, you need to remove the previous site from the app and badge at an update point reader to retrieve the new site's programming.

To delete the programming:

1. **Before you leave the first site**, make sure you badge your config app at an update point reader to upload the latest data. Data that has not been uploaded to the system will be lost when the config app is cleared.
2. In the config app, navigate to **Wireless Locks**.
3. Tap the **Delete** icon in the top right.
4. Select **Clear Data**.
5. Open the side menu and select **Logout**. This is needed to clear the encryption keys for the first site.

When you log in again and badge at the update point reader at the new site, the config app will retrieve the data for that site.

Manual Commands for Offline Locks

Offline wireless locks are not actively connected to the system and so do not support the standard manual commands for wired doors (e.g. lock, unlock, lockdown). However, some commands are available to help with lock administration:

- **Force update:** Changes the lock's status from **OK** to **Update required**, allowing you to update the programming with the config app. For example, this could be used to update the lock's internal clock if it is not following schedules correctly, or to collect the full event log using the config app.
- **Reinitialize:** If the **Enable lock reinitializing** setting is activated in **Global | Sites | Offline wireless locking**, you can use this command to change the lock's state to **Initialize required**. You must then default the wireless lock associated with this door record and either initialize it again or replace it with a new one.
- **Emergency open:** If the **Allow emergency openings** setting is enabled (**Offline wireless locking** tab), you can use this command to unlock the door once using the config app. Badge a config app at an update point reader to retrieve the command, move to the lock, then tap **Unlock** in the app to temporarily unlock the door.

The command expires after one hour.

For more information, see [Emergency Open](#) (page 29).

- **View recent:** Runs an event report for the most recent events from that lock.

Programming User Access

The same user records can be used for wireless and wired doors on a single Protege GX site. After you program the user record, you must initialize the user's card at an update point reader or desktop encoder to allow them to get access to wireless locks.

Keep in mind that some types of records are stored on the lock itself rather than on user cards (see page 17). When you program access levels and users, you should only use existing schedules and door groups that have already been stored on the offline locks. If you add or update any schedules or door groups, the offline locks will not be able to use these new settings until they have been updated using the config app.

Programming Access Levels

The same access levels can be used for wired and wireless doors.

1. Navigate to **Users | Access levels** and add a new access level.
2. In the **Doors** or **Door groups** tabs, add the wired and wireless doors that these users will access. Users may have access to the update point reader, but this is not necessary.
3. If you need to restrict access based on schedules, program the **Schedule** for each door and door group.

Offline locks only use the schedules programmed in the **Doors** and **Door groups** tabs. The access level's **Operating schedule** and any schedules programmed in the user record are ignored.

4. Click **Save**.

Adding Users

To add a user with access to wireless locks:

1. Navigate to **Users | Users** and click **Add**.
2. Program the user's basic settings as normal:
 - Name
 - Access levels
 - Expiry dates under **User expiry date/time** (optional)
3. The **General** tab includes some specific settings related to wireless locks. By default these will match the settings in **Global | Sites | Offline wireless locking**.
 - The **Update Period** (**General** tab) determines how frequently the user has to renew their access data by presenting their card to an update point reader. If this period expires, the user will not be able to access any offline locks until they update their card again.
 - Select **Enable office unlock** (**General** tab) to allow the user to toggle the lock when the door is in office mode.
4. The following settings in the **Options** tab may be needed for some users:
 - **User has super rights and can override antipassback** enables users to override privacy mode on mortise locks (as well as lockdown and antipassback restrictions on wired doors).
 - **User operates extended door access function** allows the user to unlock the door for longer (using the **Door extended access time** in **Programming | Doors | Offline wireless locking**).
5. Before the user can use their card or mobile credential at an offline lock, you must initialize it to download the access data. For physical cards, this encodes the wireless locking files onto the card based on the card profile (see page 11). Then it downloads the user's access data so that the card or mobile credential can be used to gain access at locks.

There are two methods for initializing a credential:

Using a desktop encoder (cards only):

- Save the user record.
- In the **General** tab, scroll down to the **Credentials** section and select the ICT Wireless Locking credential type.
- Set the **Start** and **End** expiry dates if needed.
- Place the card on the desktop encoder.
- Click **Program card**. Protege GX will encode the card, download the access data and save the facility and card number to the user record.

Using an update point reader (cards and mobile credentials):

- In the **General** tab, scroll down to the **Credentials** section and select the ICT Wireless Locking credential type.
- Under **Credential**, enter the facility and card number of the user's card or mobile credential, separated by a colon (e.g. 10636:7482).
- Set the **Start** and **End** expiry dates if needed.
- Click **Save**.
- Wait for the programming to be downloaded to the controller.
- Badge the card or mobile device at an update point reader to encode the card and download the access data.

The user now has all of the relevant access data on their card or mobile device, so they will be granted and denied access at wireless locks.

Blocklist

The blocklist is a list of credentials that are not allowed access at offline locks. When a credential is lost or stolen, you can add it to the blocklist using one of the following methods:

- When a credential is deleted from a user record, that credential is added to the blocklist.
- When a user record is deleted, all of their assigned credentials are added to the blocklist.

When any user badges at an update point reader, the latest blocklist is stored on their credential (or the config app for an installer). They will then circulate the blocklist as they travel throughout the building. 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.

Blocklisted credentials will expire in the locks 28 hours after the earlier of the **Update period** and the user/credential **End** date (if enabled). It may be an additional 24 hours before you can reassign that credential in the software. As a rule of thumb, after blocklisting a credential you should set it aside for twice the **Update period** (e.g. 60 days) before reassigning it to another user.

Using the Blocklist

The blocklist is intended to be used for rare emergency situations where a card has been lost or stolen. It is not designed to store large numbers of credentials, so it is not recommended to delete many users or credentials in a short period.

The maximum number of credentials that can be stored on the blocklist at any one time is **150**. Locks will not accept any new blocklist that is larger than this limit.

If you need to prevent users from gaining access to wireless locks but it is not an emergency, the best methods are:

- Set the **User expiry date/time** or credential **End** in **Users | Users | General** to an invalid date (e.g. yesterday).
- Remove or edit the access levels that grant access to wireless locks.








If it is necessary to delete large numbers of users, this should be staggered over a longer period so that the blocklist does not grow too large.









Users with expiry dates may not be blocklisted correctly. Disable the user's expiry date before blocklisting them.

Access Control Settings

Protege GX has various methods for scheduling, expiring and disabling user access. However, due to the inherent limitations of the offline system, wireless locks are only able to use a subset of these options. Keep this in mind when programming user records, as using the wrong settings may cause users to have access to locks when they should not.

The following table shows which user access settings can be used to restrict access on offline locks.

Type	Setting	Supported?
Schedule	Schedule Groups Door groups Doors	
	Schedule Users Access levels Doors	
	Schedule Users Access levels Door groups	
	Operating schedule Users Access levels General	
	Schedule Users Users Access levels	
Expiry	Start/End Groups Door groups Door group expiry date/time	
	Access level expires / Expiry start / Expiry end Users Access levels	
	Start/End Users Users General Credentials	
	Start/End Users Users General User expiry date/time	
Inactivity	Inactivity period Users Users General Credentials	
	Disable period Users Users General User disable/deletion	
	Delete period Users Users General User disable/deletion	 Not recommended - see below.
	Update period Users Users General Wireless lock settings	
Usage Restriction	Enable usage restriction Users Access levels Usage restriction	

Type	Setting	Supported?
Disable	Disabled Users Users General Credentials	
	Disable user Users Users Options	
Delete	Remove door from door group	 Programming change must be transferred to the lock using the config app.
	Remove door from access level	
	Remove door group from access level	
	Remove access level from user	
	Remove credential from user	 Credential is added to blocklist (see page 25).
	Delete user record	 Credential is added to blocklist (see page 25).

User Inactivity Settings

We do not recommend using the **Delete period (Users | Users | General | User disable/deletion)** in offline locking systems, as this will add all of the user's assigned credentials to the blocklist. Instead, set the **Update period** appropriately to ensure that users will lose access to wireless locks if they do not badge at an update point reader regularly.

Validating Lock Operation

Once you have programmed a user, you can validate that the lock is operating as expected.

1. Program a new user record with an access level that grants access to a wireless lock.
2. Encode the user's card using either a desktop encoder or update point reader. The update point reader will rapidly flash purple while updating the card. Once the update is complete it will grant or deny access to the door as normal.

Be patient while the update point reader updates the card. Do not remove the card until the reader stops flashing purple.

3. Badge the user's card at the lock. The lock should flash green to show that access is granted.
 - Standard, Office, Exit leaves unlocked modes: The door should unlock for a short time, then relock.
 - Toggle modes: The door should unlock and remain unlocked. Badge the card again to lock it again.
4. If the lock is in Office mode and the user has **Enable office unlock**, hold down the inside handle and badge at the reader. The door should unlock and remain unlocked until you repeat this process.
5. If the lock is in Exit leaves unlocked mode, open the door from the inside. The door should remain unlocked until you badge a card or the timer expires.
6. If the cartridge mortise lock has an inside thumbturn or key cylinder, actuate it to activate privacy mode. Badge the card at the reader. You should be denied access unless the user is a super user.

7. Return to the update point reader and badge the card. The update point reader will rapidly flash purple as it retrieves events from the card and updates the access settings and blocklist.
8. In Protege GX, navigate to **Programming | Doors**. Right click on the wireless lock you have been testing and click **View recent** to run an event report. You should see the access events that were retrieved from the lock.

Emergency Open

The emergency open command enables anyone with permission to configure locks to unlock an offline lock once. This allows a building manager to open the door when the owner or tenant locks themselves out, but does not grant them permanent access.

Emergency opening is disabled by default, but can be enabled using the **Allow emergency openings** setting in **Programming | Doors | Offline wireless locking** or **Global | Sites | Offline wireless locking**.

To perform an emergency open:

1. In Protege GX, navigate to **Programming | Doors** and locate the relevant door record.
2. Right click on the door and select **Emergency open**. This grants the ability for a config app user to unlock the lock once within one hour.
3. Ensure that your user record is permitted to configure locks using the config app (see page 19). Log in to the config app, open the **Wireless Locks** page and badge your phone at the update point reader to retrieve the command.
4. Move to the door that needs to be unlocked, then tap **Unlock** in the app.
5. The lock will unlock for its normal lock activation time, then lock again.

Additional Settings

Offline wireless locks have a wide range of additional settings to customize their operation.

General Site Settings

These settings determine the operation of the whole site.

- **Collect event log when updating locks:** With this option enabled, when the Protege Config App updates an offline lock it will also collect the lock's archived event log, including events that have been retrieved by cards in the past. The events are uploaded to Protege GX the next time the app is badged at an update point reader. This may be time consuming if there are a large number of events to retrieve.
- **Enable lock reinitializing:** When this option is enabled, you can right click on an offline door record and select **Reinitialize** to remove the lock pairing without deleting the programming. You can then either default and reinitialize the existing lock, or initialize a new lock.

Door Settings

Many wireless lock settings can be programmed in both the site (**Global | Sites | Offline wireless locking**) and the individual door records (**Programming | Doors | Offline wireless locking**).

Settings at the site level are the default settings for any new door records that are created. When you change the settings, you can also automatically apply the new defaults to every door on site. If there are different requirements for specific locks, you can override the settings in individual door records.

- **Enable lock event log:** Enable this option to allow the offline lock to store events in its internal memory. You can determine what types of events are recorded using the settings below.
- **Enable card event log:** Enable this option to allow the offline lock to transfer events to access cards and mobile devices when access is granted. The events will be uploaded to the system when the credential is badged at an update point reader. This option can be disabled when cards do not have enough storage to collect practical numbers of events (e.g. MIFARE 1K cards).

If this option is disabled, events can still be retrieved from the lock using the Protege Config App.

- **Log access granted events:** Enable this option to allow the offline lock to log access granted events.
- **Log access denied events:** Enable this option to allow the offline lock to log access denied events.
- **Log exit events:** Enable this option to allow the offline lock to log exit (REX) events.
- **Deny access when card storage is full:** With this option enabled, the lock will deny access if there is no space on the user's card to store events. The user must badge their card at an update point reader to upload their events before they can gain access. When this option is disabled, access will be granted even if there is no space for new events on the card.

Use this setting with caution, as cards with low storage space can fill up with events quickly in normal operation.

- **Enable beeper:** With this option enabled, the lock will signal with the beeper as well as the LED. This may impact the lock's battery life.
- **Enable key override indication:** With this option enabled, the reader will flash blue three times when the door is unlocked with a key. This occurs when the door latch is fully retracted (not when the deadbolt is retracted).
- **Allow emergency openings:** Enable this option to allow operators to send the **Emergency open** manual command to the door. An authorized config app user can retrieve the command from an update point reader and use it to unlock the door once. This allows a building manager to open the door when the owner or tenant locks themselves out, but does not grant them permanent access.
- **Exit leaves door unlocked time period:** When the lock is in Exit leaves door unlocked or Exit leaves door unlocked + toggle mode (**Programming | Door types | Options**), by default when someone exits the door will remain unlocked until a user badges a credential to relock it. With this option enabled, the door will automatically lock when the defined period expires. It can still be manually relocked by badging a credential.

User Settings

Some settings can be programmed in both the site (**Global | Sites | Offline wireless locking**) and the individual door records (**Users | Users | General | Wireless lock settings**). Like the door settings above, programming at the site level provides the default settings, which you can then override for specific users.

- **Update period:** The update period determines how frequently the user must update their credential at an update point reader. If they do not update their credential within this period, the access data will expire and they will not be able to access offline locks until they renew the data at the update point reader.
- **Enable office unlock:** When the **Lock operating mode** is set to Office unlock (**Programming | Door types | Options**), users with this option enabled can latch unlock the door by holding down the inside handle and badging a credential at the same time. They can relock the door using the same method.

Troubleshooting

Update Point Reader Operation

The config app does not receive any lock data when I badge at an update point reader

There are a few possible causes for this:

- Check whether Bluetooth® is turned on.
- There are no locks in the Protege GX system that need updating. If you wish to update a specific lock, navigate to **Programming | Doors**, right click on the lock and select **Force update**.
- Your access level does not have the **Enable access to wireless lock config** option enabled.
- Your config app is still using the encryption keys from a previous site. Log out of the app and then back in again.

The update point reader grants/denies access to a card, but does not encode the wireless locking files

The update point reader is failing to encode the card. This could mean:

- The system does not have a card profile for this type of card. Create a new card profile (see page 11).
- The card profile does not have enough space to encode the user's access data. Increase the space allocated for access.
- The card has been used on a different wireless locking site and has different encryption keys. It is not possible to use the same cards on multiple unique sites. Retrieve and wipe the card or issue a new one.

If you have a USB desktop encoder, the error messages in the software may give more insight into why the encoding is failing.

Update Point Reader LED and Beeper Indications

Startup Indications

When the TSL reader is in update point reader mode, whenever it powers up it will flash and beep to signal the status of each encryption key. As an initial diagnostic for any update point reader issues, power cycle the reader and observe the LEDs and beeper. For each key, there is a specific LED color and a beeper indication:

- 2 short beeps: The key is loaded correctly
- 1 long beep: The key is not loaded correctly

LED Colour	Meaning
Blue	Reader is starting up (4 short beeps)
Red	Bluetooth® session key
Green	DESFire master key
Yellow	DESFire read/write key
Mint green	MIFARE site key A
Violet	MIFARE site key B

If any of the encryption keys are not loaded correctly, you will need to default the reader using the config **Device Mode - Factory Default EEPROM**, then enable update point reader mode again (see page 13).

Credential Indications

The update point reader shows the following indications when it reads a card or mobile credential:

LED Colour	Beeper	Meaning
Blue	1 short beep	Card detected
Rapid purple flashing		Encoding data on card and retrieving events.
Green	2 medium beeps	Access granted
Blue	1 long beep	Access denied

Lock Operation

Wireless locks are unlocking at the wrong time / Events from locks have the wrong field time

The lock's internal time is based on that of the controller. Check the controller's daylight savings and time zone settings (see page 9), then update the locks using the config app.

If an initialized lock loses power for more than one minute (e.g. while the batteries are being changed), its internal clock will lose the current time. If this occurs, update the lock using the config app.

The motorized deadbolt lock emits a long beep before actuating the bolt

The long beep is the lock's collision detection warning, so check that the path of the deadbolt is not obstructed.

If not, the lock's handing may be set incorrectly. This is based on the position of the bolt when the lock is powered on in construction mode. To set the handing correctly:

1. If the lock has already been initialized, default it (see page 21).
2. Open the battery cover and remove a battery. Wait a few seconds for the lock to shut down completely.
3. **Retract** the deadbolt.
4. Insert the battery to power up the lock.
5. Reinitialize the lock into the system (see page 19). It should now lock and unlock correctly.

The lock is flashing red and blue LEDs continuously

The firmware update process has failed and the lock is stuck in boot mode. To resolve this issue:

1. In the config app, tap **Firmware Reset**.
2. The app will scan for locks in boot mode. Select the lock and tap **Update**.
3. The app will reset the lock's firmware. This may take 2-3 minutes.

Updates to locks close to the update point reader are failing

The update point reader can interfere with attempts to update locks in close proximity. On the **Mobile Credentials** page, reduce the **Bluetooth proximity** to avoid picking up nearby update point readers.

Lock LED and Beeper Indications

LED and beeper indications can help you interpret the status of the wireless locks.

The beeper will only operate when **Enable beeper** is on in **Programming | Doors | Offline wireless locking**.

Beeper Indicators

- **Short** beeps have a sound and interval duration of **100ms**.
- **Long** beeps have a sound and interval duration of **1 second**.

Low Battery Indicators

- **Yellow** flash indicates battery voltage less than 3.8V. Batteries need to be replaced within 2-3 **months**.
- **Red** flash indicates battery voltage less than 3.55V. Batteries need to be replaced within 2-3 **weeks**.

Operation	LED Indication	LED Description	Beeper
Access Granted		3 Green flashes (100ms/100ms)	2 short
Access Granted - Battery Low < 3.8V		2 Green flashes (100ms/100ms) 1 Yellow flash (200ms)	2 short
Access Granted - Battery Low < 3.55V		2 Green flashes (100ms/100ms) 1 Red flash (200ms)	2 short
Access Denied		3 Red flashes (100ms/100ms)	1 long
Access Denied - In Privacy Mode		3 Red flashes (200ms/200ms)	1 long
Access Denied - Battery Low < 3.8V		2 Red flashes (100ms/100ms) 1 Yellow flash (200ms)	1 long
Access Denied - Battery Low < 3.55V		2 Red flashes (100ms/100ms) 1 Red flash (200ms)	1 long
Construction Mode - Access Granted		3 Purple flashes (100ms/100ms)	2 short
Construction Mode - Access Granted - Battery Low < 3.8V		2 Purple flashes (100ms/100ms) 1 Yellow flash (200ms)	2 short
Construction Mode - Access Granted - Battery Low < 3.55V		2 Purple flashes (100ms/100ms) 1 Red flash (200ms)	2 short
Construction Mode - Access Denied		3 Orange flashes (100ms/100ms)	1 long
Construction Mode - Access Denied - Battery Low < 3.8V		2 Orange flashes (100ms/100ms) 1 Yellow flash (200ms)	1 long

Operation	LED Indication	LED Description	Beeper
Construction Mode - Access Denied - Battery Low < 3.55V		2 Orange flashes (100ms/100ms) 1 Red flash (200ms)	1 long
Exit Leaves Open Mode - Lock/Unlock Granted		1 Green flash (100ms)	1 short
Exit Leaves Open Mode - Lock/Unlock Denied		3 Red flashes (100ms/100ms)	1 long
Opening Not Allowed - Battery Flat		1 Red flash (20ms)	1 short
Powering Up		Flashing Blue (200ms/200ms) until ready to read (typically 1.5s)	2 short
Powering Up - Battery Low < 3.8V		Flashing Blue (200ms/200ms) until ready to read 1 Yellow flash (200ms)	2 short
Powering Up - Battery Low < 3.55V		Flashing Blue (200ms/200ms) until ready to read 1 Red flash (200ms)	2 short
Factory Reset		5 White flashes (100ms/100ms)	
Blob Version Not Supported		1 White flash (100ms)	
Blob Contains No Configuration		1 White flash (500ms)	

User Access

If a user's access rights to wireless locks seem to be incorrect, first ensure that the credential is up to date with the programming in the software.

1. Ensure that the software has downloaded all changes to the controller.
2. Badge the user's card or phone at an update point reader. This also resets the **Update period** on the credential.
3. Badge the credential at the lock to check whether the issue persists.

If the issue does persist, review the troubleshooting suggestions below.

A user was denied access at a lock

It may be useful to enable **Log access denied events** for this lock to see what events are returned when the user badges their card.

- User Jenny Taylor Door Not Allowed Apartment 102 Front Door - The door is not included in the user's access level.
Alternatively, the user's access level may contain a door group that is not stored on the lock (see page 17). In this case, access will be denied. Update the lock using the config app.
- User Jenny Taylor Schedule Not Valid Apartment 102 Front Door - The schedule on the door is invalid (**Users | Access levels | Doors / Door groups**).
Alternatively, the user's access level may contain a schedule that is not stored on the lock (see page 17). In this case, access will be denied. Update the lock using the config app.
- User Jenny Taylor Not Valid At Apartment 102 Front Door - The user record or credential has expired, not become valid yet, or has exceeded the update period. Check the **User expiry date/time** and credential **Start / End**.
- User Jenny Taylor Denied Access At Wireless Lock Apartment 102 Front Door As Privacy Mode Engaged - The door is in privacy mode.

A user gained access to a lock outside of their schedule

- The time on the lock may be set incorrectly. Check the **Field time** of the events returned from the lock. If necessary, adjust the controller's daylight savings and time zone settings (see page 9). Then update the lock using the config app.
- Not all schedule options are supported on wireless locks (see page 26). Ensure that the schedule is programmed on the doors and door groups in the access level.

An expired or disabled user gained access to a lock

Not all access settings in Protege GX can be used with offline wireless locks. Check the [Access Control Settings](#) page to ensure that the correct settings are being used.

Defaulting the System

Every communication in the wireless locking system is encrypted with unique encryption keys. This means that if any component of the system is defaulted and loses its encryption keys, some other components may need to be defaulted as well to allow them to generate new keys.

If the controller is defaulted, you must do the following to get the system working again:

1. Disable controller encryption at the server (**Sites | Controllers | Configuration | Encryption**).
2. Bring the controller back online and update all modules.
3. Re-initialize controller encryption.
4. Default the update point readers connected to the controller using the config app with the following config:
Device Mode - Factory Default EEPROM
5. Re-configure the update point readers (see page 13).
6. In **Expanders | Reader expanders**, right click on the onboard reader expander and select **Activate OSDP install mode**.

This deletes the old encryption keys on each component and generates new ones.

If you delete the Protege GX database all encryption keys in the system need to be regenerated. You will also need to default the controllers, update point readers and locks, and wipe any access cards that have already been encoded. To refresh the encryption keys in the config or mobile app, log out then in again.

You must also default any component that is being connected to a new system (e.g. moving a TSL reader from one site to another). Any cards which are transferred to a different system must be wiped and re-encoded.

System Administration

The wireless locking system uses advanced encryption for every part of the chain of communication, following industry best practices. System administrators must complete some additional configuration to ensure that the Protege GX system continues to function as expected.

Backing up and Restoring the Database Encryption

When wireless locking is enabled on a site, some database columns are encrypted to keep the data secure. We recommend that you back up the Data Service Encryption Certificate to ensure that it is not lost if the Protege GX server goes down. In addition, when you restore the Protege GX database to another server or secondary download server you must import the certificate to allow the new server to access the encrypted columns.

Backing up the Certificate

The certificate is created on the machine where the data service is installed, which may not be the same machine as the SQL server installation.

1. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
2. The tool directory will display Certificates - Local Computer.
3. Open the **Personal** folder, then click the **Certificates** sub-folder.
4. In the window displaying the certificates, scroll across to the **Friendly Name** column and locate the certificate called Data Service Encryption Certificate.
5. Right click the certificate and select **All Tasks > Export**.
6. The **Certificate Export Wizard** will open. Click **Next**.
7. You must select the **Yes, export the private key** option.

The private key is the critical component in decryption. If you do not export the private key, when the certificate is imported it will not be able to decrypt the encrypted data.

Then click **Next**.

8. Ensure that the following **Export File Format** options are selected:
 - **Include all certificates in the certification path if possible**
 - **Enable certificate privacy**

The **Delete the private key if the export is successful** option **must be disabled**.

Then click **Next**.

9. On the **Security** page, enter and confirm a strong **Password**.

This should be saved securely with important site information.

10. Set **Encryption** to AES256-SHA256, then click **Next**.
11. Specify an export **File name** and path, then click **Next**.
12. Click **Finish** to complete the certificate export.
13. When the export is complete, confirm that the certificate backup .pfx file has been exported to the file path as specified.
14. The file should be stored securely in a separate location to ensure that it is available if required.

You must back up the certificate and the password used to encrypt the private key in a secure location. If these are lost, it will not be possible to restore database backups to another server.

Restoring the Certificate

1. Ensure that the .pfx backup file is accessible from the local PC.
2. Stop all Protege GX services before initiating the import.
3. To open the Certificate Manager tool as an administrator, press the **Windows + R** keys, then type **certlm.msc** into the search bar and press **Control + Shift + Enter**.
4. The tool directory will display Certificates - Local Computer.
5. Open the **Personal** folder.
6. Right click the **Certificates** sub-folder and navigate to **All Tasks**, then select **Import**.
7. The **Certificate Import Wizard** will open. Click **Next**.
8. Click **Browse...** and locate the .pfx backup file to import, then click **Next**.

You will need to change the file type dropdown to Personal Information Exchange (*.pfx;*.p12).

9. Enter the **Password** that was created during the export process.
10. Import Options:
 - **Mark this key as exportable. This will allow you to back up or transport your keys at a later time.**
 - This option must be selected if you want to be able to export/backup the private key with this certificate in the future. This option is slightly less secure.
 - The key is more secure if this option is not selected, however you will not be able to export the private key with the certificate in the future if you lose your current .pfx backup file.
 - Ensure that **Include all extended properties** is selected.
11. Click **Next**.
12. Ensure the **Certificate store** is set to Personal, then click **Next**.
13. Click **Finish** to complete the certificate import.
14. Close the Certificate Manager tool.
15. Restart the Protege GX services.

Configuring the Single Record Download Service

Because the wireless lock feature uses column encryption in the SQL database, some additional steps are required to configure the Protege GX Single Record Download Service to work in wireless lock systems.

1. Stop the Protege GX Single Record Download Service in the Windows Services Manager.
2. In the File Explorer, navigate to the installation directory of the single record download service. The default installation directory is: C:\Program Files (x86)\Integrated Control Technology\Protege GX.
3. Open GXSV2B.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. Locate the following connection string:

```
<add name="Main" connectionString="Trusted_Connection=yes;
TrustServerCertificate=yes; Encrypt=yes; Server=[DatabaseServer];
Database=[MainDatabase]; max pool size=2000;" />
```

5. Add the text in bold:

```
<add name="Main" connectionString="Trusted_Connection=yes;  
TrustServerCertificate=yes; Encrypt=yes; Server=[DatabaseServer];  
Database=[MainDatabase]; max pool size=2000; Column Encryption  
Setting=Enabled;" />
```

6. Save the config file.
7. Start the Protege GX Single Record Download Service in the Windows Services Manager.

Known Issues

ICT would like to make you aware of the following known issues and limitations.

Programming

- When any controller's time zone or daylight savings record is updated in Protege GX, all wireless locks will be marked as **Update required** even if they are not affected by this time change. Avoid updating time settings after the initial site setup (see page 9).
- Updating the schedule assigned to a door group in **Users | Access levels | Door groups** will not change the door's status to **Update required**. To resolve this issue, right click on the lock and select **Force update**.
- The Find tool cannot filter the doors list by the **Connection type** field.
- Saving a card profile with invalid partition sizes can cause the Protege GX client to crash. Ensure that settings are correct before saving.

Update Point Reader

- Update point readers programmed as exit readers do not beep when a card is presented.
- Update point readers programmed as exit reader incorrectly generate entry events instead of exit events.

Lock Configuration

- After updating the firmware of a wireless lock, the config app sometimes fails to initialize the lock correctly and reports an error. Initialize the lock again (you may need to default it first).
- The config app may fail to update the lock's firmware on the first attempt.
- The config app will hang and fail to update the lock if there are only blocklist changes (i.e. no configuration changes). If this occurs, use the **Force update** command to trigger a configuration update.
- Door schedules do not work correctly when they contain a holiday group with more than one holiday.

Credentials

- It is not possible to use MIFARE credentials for additional applications alongside offline wireless locks, because the update point reader does not correctly reserve sectors when programming the card.

User Management

- Credentials that are encoded using a desktop encoder do not respect the credential start/end expiry dates (i.e. may be granted access before or after their expiry date). They will be denied access correctly after being updated at an update point reader.
- Wireless locks only respect the first instance of a door schedule assigned to a user. If a user has access to the same door through multiple access levels, ensure that the most permissive access level is assigned as their first access level.
- The maximum blocklist size is 150 users. Locks will not accept any new blocklist that puts them over this limit. If you encounter this issue, contact ICT Technical Support for assistance.
- Users with expiry dates may not be blocklisted correctly. Disable the user's expiry date before blocklisting them.

Monitoring and Events

- Some lock/unlock events in office unlock and exit leaves unlocked modes display the wrong user.
- The "Granted Entry" event is used for both locking and unlocking a lock in toggle mode.
- Motorized deadbolt locks occasionally fail to generate events.

- If there are multiple Protege GX sites on the same server and only some of them have the wireless locking feature enabled, sites which do not have this feature enabled may receive unnecessary "Wireless Lock Key Initialization" events from controllers.
- Some access events generated by wireless locks are duplicated.
- A maximum of 10 events can be transferred to a credential each time it is badged at a wireless lock, regardless of how much space is available.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2024. All rights reserved.

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