Protege Wireless Lock Range

Motorized Deadbolt Wireless Lock

Installation Manual

Last Published: 31-Jul-24 10:34 AM

Contents

Introduction

This installation manual provides instructions and technical specifications for installation of the Protege Motorized Deadbolt Wireless Lock.

For programming instructions, see the Protege Wireless Lock Configuration Guide.

About This Product

The Protege Motorized Deadbolt Wireless Lock combines an advanced-technology, intelligent wireless credential reader with leading motorized deadbolt locking system technology. With no cabling necessary this provides sites with the ability to deploy integrated electronic access control in areas where traditional wired locking solutions may not be possible.

Current features of the wireless lock include:

- **Bluetooth**® Wireless Technology
- MIFARE and DESFire credential reading
- Integrated LED indicator provides read response and status signaling
- Lock configuration programmable via the Protege Config App
- Efficient operation provides battery life of up to 1 year (10,000 activations)*

*Not evaluated by UL.

How Does It Work?

Online Mode

A wireless lock in online mode operates almost the same as a wired system. A wired access point acts as a network connection node, facilitating communication between the lock and the controller using Bluetooth® Wireless Technology. When a user presents their credential the lock checks their access permissions in real time via the access point. Access is granted or denied accordingly and events are communicated back to the controller.

Locks are configured for one mode or the other. When a lock in online mode loses connection to the access point or hub it does not revert to operating in offline mode ('data on card'). It will not unlock for any credential and will flash a red LED every second to indicate a lost connection.

| Wireless Lock | Access request → ← Access decision | Access Point | Access request → ← Access decision | Protege System |

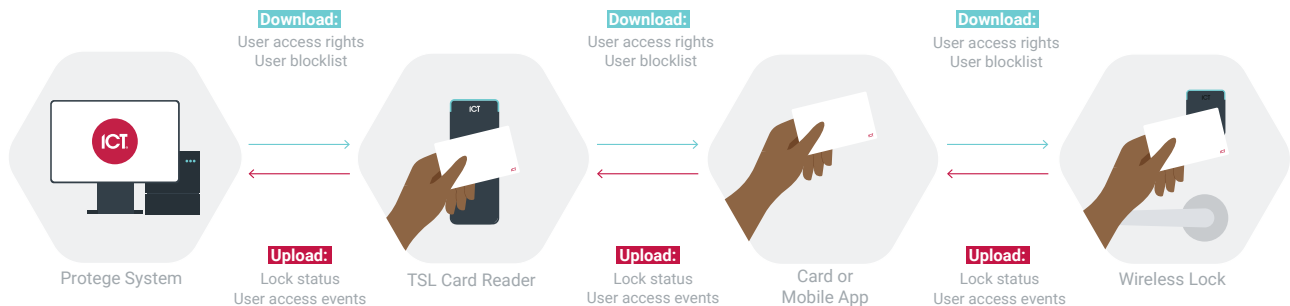When a user presents their credential at a wireless lock operating in online mode the lock sends a request via the access point to check the credential's access permissions. The controller processes the request and provides an access decision. The lock grants or denies access accordingly, then sends the related events to the controller. When the user presents their credential at the next lock the process is repeated.

Offline Mode

Unlike wired and online doors, which contact the controller to determine whether to grant or deny access, wireless locks in offline mode make access decisions based on the permissions stored on the user's credential ('data on card').

In an offline wireless locking system each user acts as a walking data store carrying access and event data to and from the locks, like a colony of ants creating a mobile data network.

When a user presents their credential at a wired update point (such as at a main entrance) the reader downloads a 'credential blob' to the card/phone. This credential blob contains encrypted information about the access rights for that specific credential, including which doors they can access and when. It also includes a blocklist of users who have recently been banned from the site.

When the user presents their credential at a wireless lock the credential blob tells the lock whether that user should be granted or denied access. All the lock has to do is follow the instructions. The blocklist is also uploaded to the lock to ensure that inactive users who have not yet had their credential blob updated can no longer gain access. At the same time the lock downloads the user's events to their credential, and when they next present at a wired update point their accumulated events are uploaded to the controller.

Access-related programming changes to access levels, schedules and so on are downloaded to the controller as normal. The next time the user presents the credential at a wired update point the credential blob is updated with any changes that affect their access for that specific credential.

A site may have a combination of locks operating in online and offline modes.

Hardware Options

The Protege Motorized Deadbolt Wireless Lock is available in two color options.

Motorized Deadbolt Wireless Lock Options

Deadbolt Lock Body	Code
Motorized Deadbolt Wireless Lock	MDB

Two keys are supplied with each lock.

Deadbolt Trim Finish	Code
Flat Black	622-FB
Satin Chromium Plated	626-SC

Construction Cards

When a Protege wireless lock is in factory default state, it can only be unlocked using a construction card provided by ICT. Construction cards are also used to initialize locks and connect them to the access control system.

Construction cards are not included with the locks and must be ordered separately. Any ICT construction card will work with any Protege wireless lock.

Card	Code
ICT Construction Card	WL-CONST

Wireless Access Points

Wireless access points are required for online operation. One access point supports up to 8 wireless locks, allowing up to 128 online locks to be connected per online hub.

Access Point	Code
Wireless Access Point	WL-AP

MIFARE Technology

About MIFARE

Based on the international standard ISO/IEC 14443 Type A, MIFARE is a technology used for contactless RFID smart card systems consisting of card and reader components.

- Fully compliant with the international standard ISO/IEC 14443 Type A
- Multi-application memory to store several services on the same card, allowing for many integration possibilities
- Fast transaction speed
- High security and fraud protection

Secured MIFARE Card Format

Secured MIFARE is the compromise between secured cards and cost. Card data is protected with a diversified authentication key and encrypted with an AES256 algorithm. These cards are not as secure as MIFARE DESFire but still provide high security against cloning. This card mode can be used on all MIFARE 1K (S50) cards and tags.

About MIFARE DESFire EV1

MIFARE DESFire EV1 is an ideal solution for multi-application smart cards in transport schemes, e-government or identity applications. It complies fully with the requirements for fast and highly secure data transmission, flexible memory organization, and interoperability with existing infrastructure.

- Fully compliant with the international standard ISO/IEC 14443 Type A 1-4
- Common Criteria EAL4+ security certified
- Secure, high speed command set
- Unique 7-byte serial number
- Open DES/3DES crypto algorithm in hardware
- Open AES 128 bit crypto algorithm in hardware

About MIFARE DESFire EV2

MIFARE DESFire EV2 delivers the perfect balance of speed, performance and cost-efficiency. For a truly convenient touch-and-go experience, MIFARE DESFire EV2 offers increased operating distance.

Based on global open standards for both air interface and cryptographic methods, it complies with all requirements for fast and highly secure data transmission and flexible application management.

- Fully compliant with all levels of the international standard ISO/IEC 14443A
- Common Criteria EAL5+ security certified
- Secure, high speed command set
- Unique 7-byte serial number
- Open DES/3DES crypto algorithm in hardware
- Open AES 128 bit crypto algorithm in hardware
- Fully interoperable with existing NFC reader infrastructure
- Backwards compatible with all previous MIFARE DESFire generations

About MIFARE DESFire EV3

The latest addition to the MIFARE DESFire product family, MIFARE DESFire EV3 offers even more advanced hardware and software implementation on a brand new internal chip, and combines enhanced performance with a greater operating distance and improved transaction speed compared to its predecessors.

Based on global open standards for both air interface and cryptographic methods, it uses the same security certification level as IC products used for banking cards and electronic passports. Featuring an on-chip backup management system and mutual three-pass authentication, EV3 supports confidential and integrity-protected communication with secure dynamic messaging and mirroring.

- Fully compliant with the international standard ISO/IEC 14443 Type A 1-4 and ISO/IEC 7816-4
- Common Criteria EAL5+ security certified for IC hardware and software
- NFC Forum Tag Type 4 certified
- Secure, high speed command set
- Unique 7-byte serial number
- Choice of open DES/2K3DES/3K3DES/AES crypto algorithms
- Open AES 128 bit crypto algorithm in hardware
- Fully interoperable with existing NFC reader infrastructure
- Transaction timer mitigates risk of man-in-the-middle attacks
- Backwards compatible with all previous MIFARE DESFire generations

MIFARE/DESFire Products

The MIFARE/DESFire products can be expanded to accommodate large numbers of modules using the encrypted RS-485 Network. ICT provides a number of reader and physical credential options in the MIFARE/DESFire range.

Physical Credentials

- Proximity clamshell card
- Proximity ISO card
- Proximity ISO dual technology card
- Proximity standard key tag
- Proximity adhesive disc
- Proximity silicone wristband

Physical credentials are available in an extensive range of technology and EEPROM size configurations. Visit the ICT website to view the full range of proximity products.

For more information on configuration options and ordering, contact ICT Customer Services.

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- UL 294 - Access Control System Units
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- UL 1034 - Burglary-Resistant Electric Locking Mechanisms
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- CAN/ULC-60839-11-1, Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- The Local Authority Having Jurisdiction (AHJ)

Installation

Installation of the wireless lock requires the following steps to be completed in the correct sequence.

1. **Install the latch** (see page 13).
2. **Install the strike plate** (see page 14).
3. **Install the outside escutcheon trim** (see page 15).
4. **Install the inside mounting plate** (see page 16).
5. **Connect the cable** (see page 17).
6. **Install the inside escutcheon trim** (see page 18).

Be careful not to overtighten screws, as this can compress precise moving parts and interfere with the lock operation. It is recommended to always perform the final 10% of tightening by hand.

What's Included?

The Protege Motorized Deadbolt Wireless Lock is supplied with the following components.

- 1 x 13.56MHz lock control card reader with Bluetooth® Wireless Technology

  The reader is built into the outside assembly.

- 1 x Grade 2 Deadbolt door latch
    - 4 x #8-32 combo screws for securing the latch and strike plate
    - 1 x Strike plate
    - 1 x Strike reinforcement plate
    - 1 x Dust box
    - 1 x ⅛" plastic filler
- 1 x Outside trim assembly with configurable handing
    - 1 x Key cylinder
    - 8-wire reader cable wiring loom with socket plug for connection to the reader
    - 1 x Rubber gasket
    - 2 x Keys
- 1 x Inside trim assembly
    - 1 x Electronic lock control board
    - 1 x Inside mounting plate
    - 1 x Rubber gasket
    - 2 x ¼"-28 x 2-¼" flat head screws for securing the mounting plate and gasket
    - 2 x M4 x 12 pan head screws for securing the inside assembly
    - 1 x M3 x 18 pan head screw for securing the battery cover
    - 4 x Alkaline LR06 AA 1.5V batteries

Door Preparation

Doors should come pre-prepped when they are ordered from the supplier, unless you are retrofitting existing doors.

Door Thickness

- 1 ¾ - 2" (larger thickness available by special order)

Door Prep

This lock uses standard 161 door prep:

- Bore Hole: 2 ⅛"
- Edge Bore: 1"
- Bolt Faceplate: 2 ¼" x 1 ⅛"

Backset Prep

- 2 ⅜" **or** 2 ¾" (the deadbolt latch is adjustable to either length)

Strike Prep

- Deadbolt Strike Plate: 2 ¾" x 1 ⅛"
- Deadbolt Throw: 1" from the edge of the door

Drill Template

Drill templates should be used to ensure correct installation. A to-scale drill template is supplied with the lock and is also available from www.ict.co/deadbolt-template.

Pilot Holes

It is strongly recommended that you pre-drill pilot holes in wooden doors to prevent the wood from splitting. This is especially important when installing the lock in a hardwood door. The table below shows recommended diameters.

| Screw Type	Pilot Hole Diameter (Hardwood)	Pilot Hole Diameter (Softwood)
#8	1/8"	3/32"

Installing the Deadbolt Latch

1. Prepare the door according to the drill template.

2. The latch can be adjusted to accommodate either a 2 ⅜″ or 2 ¾″ backset. Twist the latch and extend or retract it to the required backset position. Then twist again to set it.

3. The latch comes with a ⅛″ plastic filler behind the faceplate to fill the gap on commercial and retrofit doors which have a 1 ⅛″ edge. If you are installing on a door with a standard 1″ edge, remove the plastic filler.

4. Install the latch with the cross slot for the tailpiece towards the bottom, as shown below.

5. Using the 2 x #8-32 combo screws provided, secure the latch in position. Do not tighten the screws at this stage, as it will be easier to install the escutcheon assemblies with some movement in the latch.
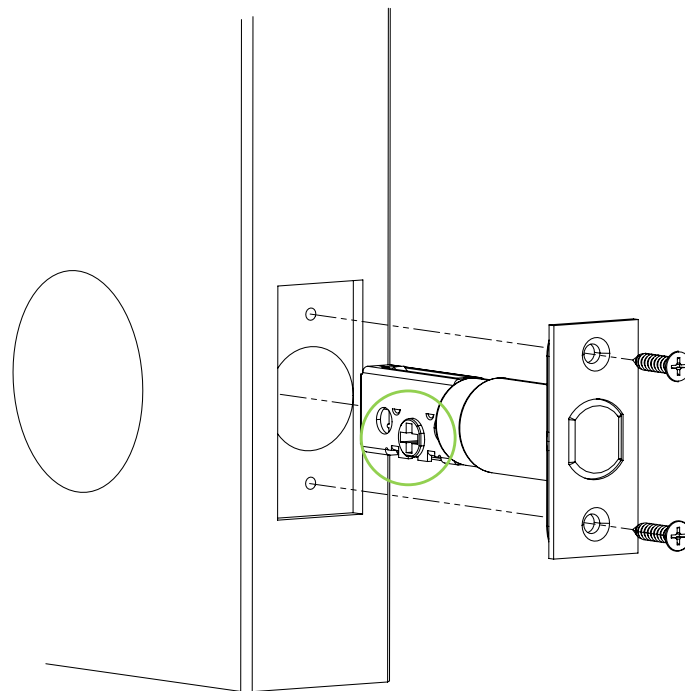
Installing the Strike Plate

1. Close the door and, using the faceplate as a guide, mark the position for the strike plate.
2. Prepare the door jamb for the strike plate.
3. Insert the dust box into the door frame cavity.
4. Position the strike reinforcement plate, then the strike plate on the door frame.
5. Using the two #8-32 combo screws provided, secure the strike plate in position.
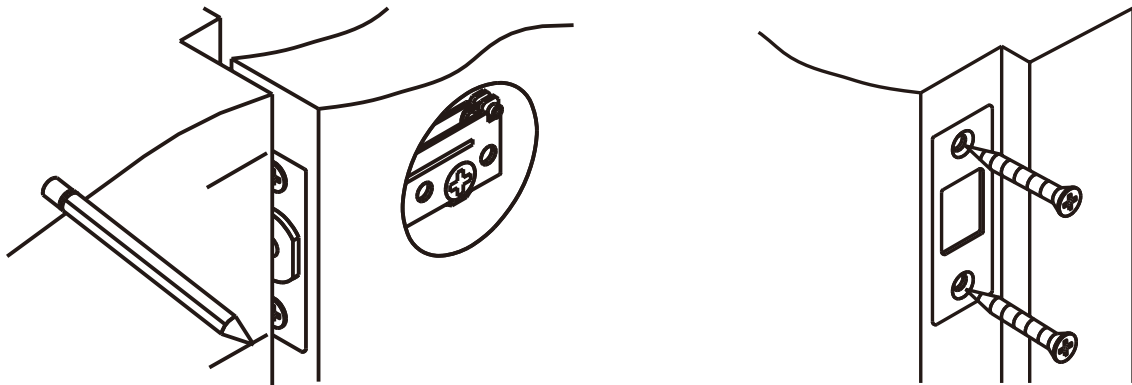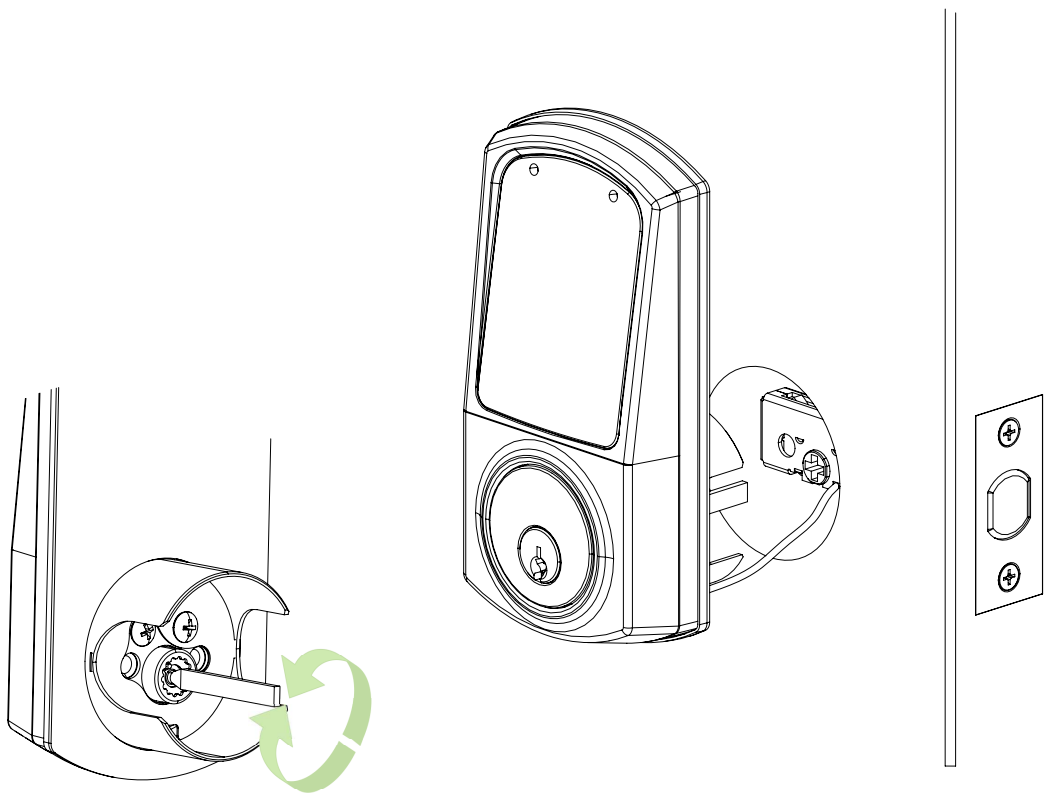
Installing the Outside Escutcheon Trim

1. To determine the handing of the door, stand on the secure side (outside). A left hand door has the hinges on the left, while a right hand door has the hinges on the right.

2. Set the handing of the outside escutcheon trim:
   - **Left Hand Door**: Rotate the tailpiece **clockwise** until it stops in the vertical orientation.
   - **Right Hand Door**: Rotate the tailpiece **counter-clockwise** until it stops in the vertical orientation.

   If the deadbolt action only moves in one direction, the handing may be incorrect.

3. From the outside of the door, feed the reader cable through the hole to the other side.

   Important: You must feed the reader cable **under** the latch.

4. Install the outside escutcheon trim assembly, guiding the tailpiece into the cross slot in the latch.

Installing the Inside Mounting Plate

1. Remove the M3 x 18 pan head screw from the battery cover and remove the cover.
2. Remove the rubber gasket and inside mounting plate assembly from the escutcheon trim assembly.
3. Feed the reader cable through the cable slot at the bottom of the rubber gasket and inside mounting plate assembly.
4. Position the gasket and mounting plate in place over the hole in the door.

   Ensure that the mounting plate is on the outside of the rubber gasket, as shown below.

5. Feed the reader cable through the cable slot at the bottom of the gasket and mounting plate, as shown below.
6. Insert the two ¼"-28 x 2-¼" flat head screws through the mounting plate and gasket into the deadbolt latch and secure the mounting plate into position.

   Do not overtighten the screws, as this can affect the deadbolt movement.

7. The outside trim may shift during assembly of the inside mounting plate, so ensure that the outside gasket is still fitted correctly around the edges and not pinched in any place.
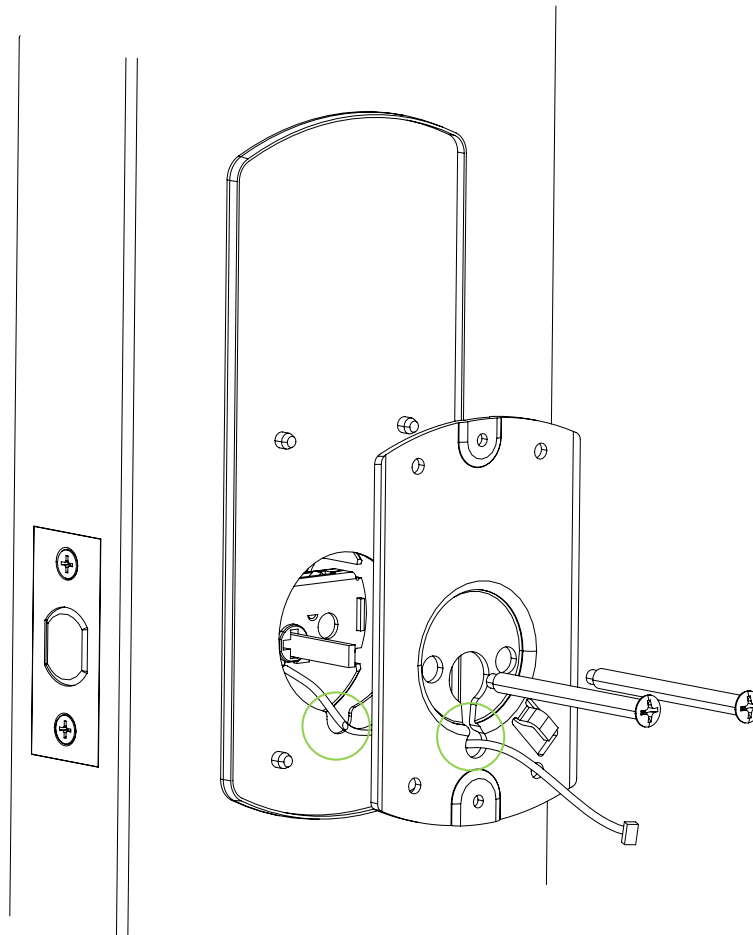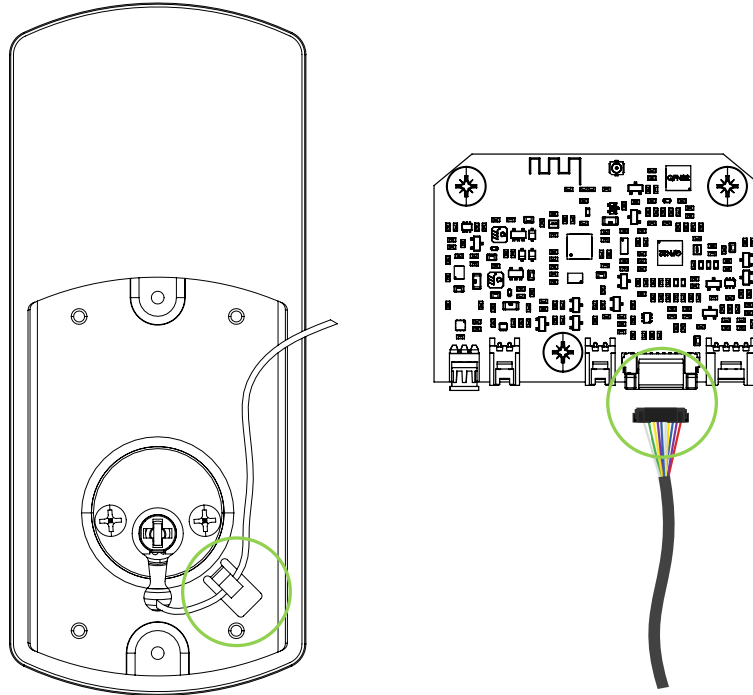
Connecting the Cable

1. Secure the reader cable through the hook in the mounting plate as shown below.

    This is an important step. The cable may become damaged if it is not properly secured.

2. Ensuring the cable is not twisted or knotted, plug the reader cable into the main socket at the bottom of the lock control board firmly so that it clicks into place.

Installing the Inside Escutcheon Trim

Both the deadbolt and the thumbturn must be in the **retracted** position when fitting the escutcheon.

1. Taking care not to pinch the cable, install the inside trim onto the door.
2. Confirm that the thumbturn correctly operates the deadbolt latch.
3. Ensure that the gasket is fitted correctly, sealed around the edges and not pinched in any place.
4. Using the two M4 x 12 pan head screws provided, secure the inside trim in position.
5. **Retract** the deadbolt before inserting the batteries. This ensures that the lock handing is set correctly.
6. Insert the four AA batteries provided. The lock should beep.

   Rechargeable batteries are not recommended due to reduced charge time and lock operation.

7. Using the M3 x 18 pan head screw provided, secure the battery cover in position.
8. With installation complete, you can now secure the deadbolt latch faceplate screws and perform a final check on all fittings and lock operation.
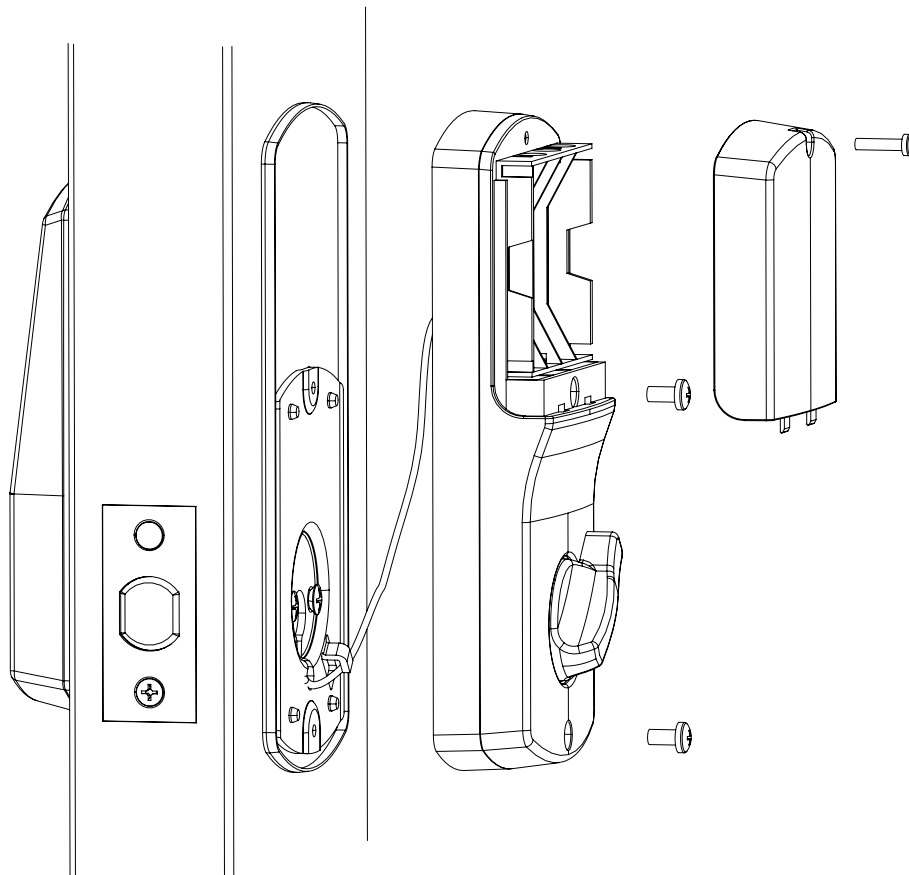
For UL installations (UL 294), UL approved batteries must be used.

For cUL installations (CAN/ULC 60839-11-1), cUL approved batteries must be used.

Approved batteries include Energizer MAX Alkaline.

Programming Locks

Wireless locks can be programmed for a wide range of functionality to meet your site's requirements.

Offline wireless locks are programmed in the Protege software. You can then use your Protege Config App to download the configuration from an update point and transfer it to the lock via Bluetooth®. Online wireless locks receive their programming from the software via the Bluetooth® access point.

For more information about setting up and programming wireless locks, see the Protege Wireless Lock Configuration Guide, available from the ICT website.

Operation

Protege wireless locks provide specific audio and visual signals to indicate read response and current status. The following table describes the available LED and beeper response signals.

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

| Operation	LED Indication	LED Description	Beeper
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
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)	

Maintenance

Protege Motorized Deadbolt Wireless Locks have an expected battery life of up to 1 year (10,000 activations), dependent on usage levels and reader configuration. Batteries should be replaced every year, or earlier if required.

In case of battery failure, emergency access can be gained via key or thumbturn.

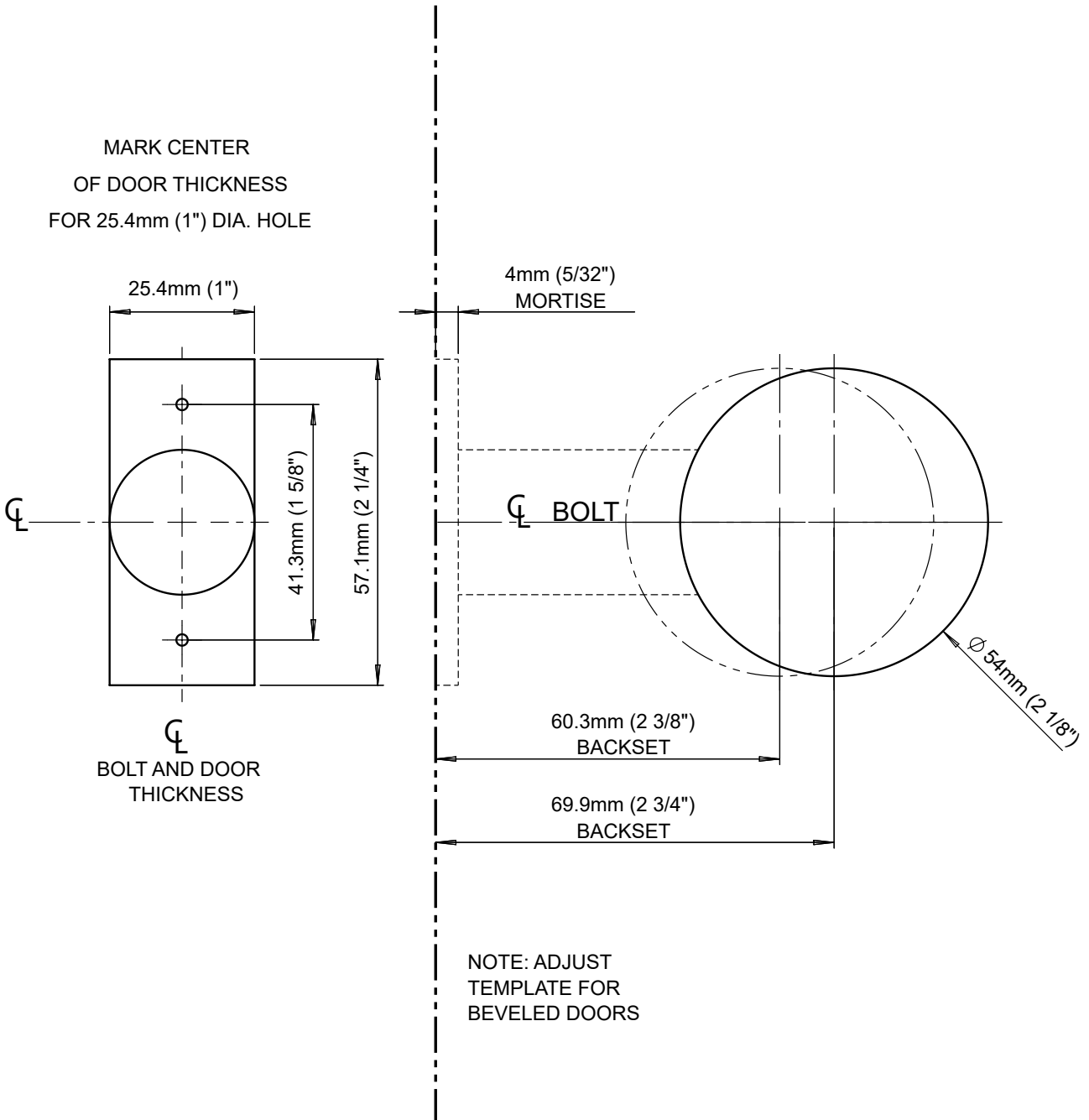Length of battery life not evaluated by UL.

Mechanical Layout

75.2mm (2.96")

148.4mm (5.84")

34mm (1.34")

27.7mm (1.09")

75.4mm (2.97")

176.3mm (6.94")
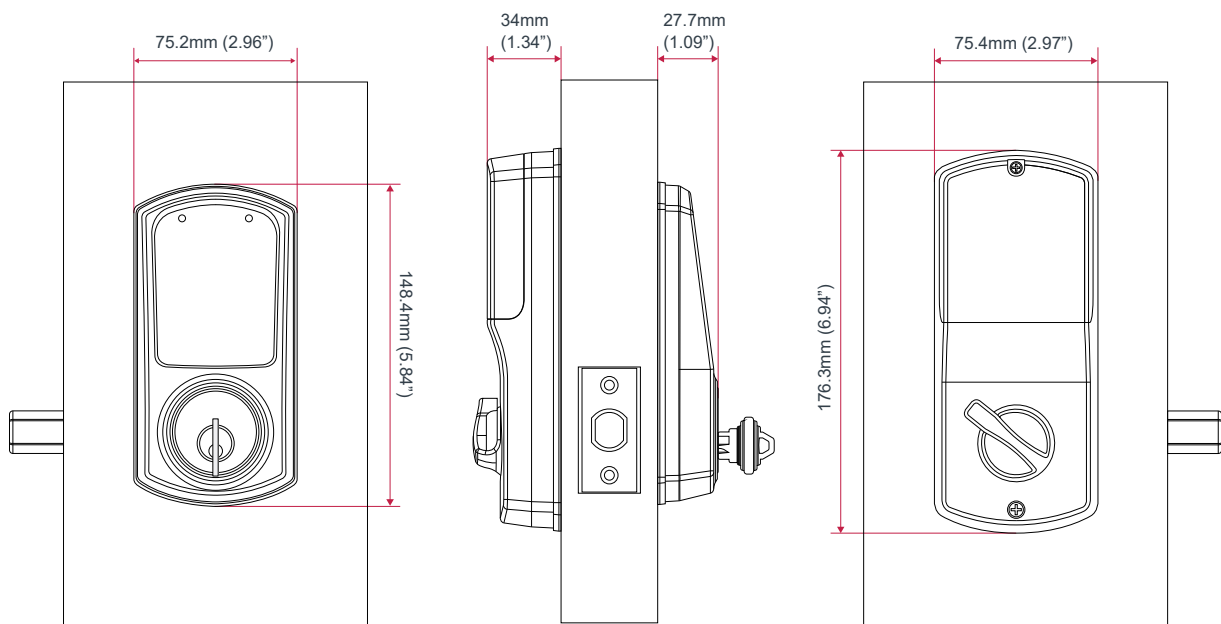
Door Template

This template is included for information only and may not be to scale. For a version of this template that can be printed to scale, go to www.ict.co/deadbolt-template

MARK CENTER
OF DOOR THICKNESS
FOR 25.4mm (1") DIA. HOLE

25.4mm (1")

4mm (5/32")
MORTISE

41.3mm (1 5/8")

57.1mm (2 1/4")

C̵L

C̵L BOLT

⌀ 54mm (2 1/8")

C̵L
BOLT AND DOOR
THICKNESS

60.3mm (2 3/8")
BACKSET

69.9mm (2 3/4")
BACKSET

NOTE: ADJUST
TEMPLATE FOR
BEVELED DOORS

Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
Order Codes	See Hardware Options
Power Supply	
Battery	Alkaline AA 1.5V (x4) UL/cUL Energizer MAX Alkaline
Expected Battery Life	Up to 1 year (10,000 activations) Length of battery life not evaluated by UL.
Operating Voltage	6V
Operating Current	900mA (Peak, Door Activation)
Average Operating Current	82µA (Standby Mode)
Memory	
Event Memory Storage	40,000 log entries
Communications	
Frequency	13.56 MHz ISO/IEC 14443 Type A
Card Read Range	20mm (0.79") (Typical)
Tag Read Range	15mm (0.59") (Typical)
Bluetooth® Wireless Technology	
Bluetooth® Read Range	Proximity mode: up to 0.5m (1.6ft) configurable Action unlock (shake): up to 5m (16.4ft) configurable
Bluetooth® Electronic Credential Transmission Technology	Bluetooth® version 5.2 compliant Proprietary data exchange protocol. AES-128 encrypted Credentials can be distinguished by unique site code and card number
Bluetooth® Wireless Device	Protege Mobile 1.0.x
Lock Specification	
Lock Type	Grade 2 heavy duty deadbolt lock
Deadbolt	Stainless steel. 25.4mm (1") throw
Latch Plate	Stainless steel. H x W 57.2 x 28.6mm (2.25 x 1.13")
Strike Plate	Stainless steel. Non-handed.
Default Keyway	Schlage C Compatible (SCC).
Default Keying	Keyed Different.
Door Thickness	44.45 to 50.8mm (1.75 to 2") standard. Larger thickness by special order
Control Hardware Dimensions	
Front (H x W x D)	148.4 x 75.2 x 27.7mm (5.84 x 2.96 x 1.09")

Back (H x W x D)	176.3 x 75.4 x 34mm (6.94 x 2.97 x 1.34")
Weights	
Net Weight	1.32kg (2.9lbs)
Gross Weight	1.68kg (3.7lbs)
Operating Conditions	
Operating Temperature	UL/cUL 0° to 49°C (32° to 120°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)
Mean Time Between Failures (MTBF)	520,834 hours (calculated using RDF 2000 (UTE C 80-810) Standard)

The **Bluetooth**® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Integrated Control Technology is under license. Other trademarks and trade names are those of their respective owners.

Integrated Control Technology continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.ict.co) for the latest documentation and product information.

UL and cUL Installation Requirements

Only UL / cUL listed compatible products are intended to be connected to a UL / cUL listed control system.

CAN/ULC-60839-11-1

- This card reader is CAN/ULC-60839-11-1 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- The card reader must be connected with shielded, grounded cable.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- **Security Grade**: 1
- **Environmental**: Indoor, dry
- **Lock Firmware Version**: 1.0.XXXX

UL 294

- This card reader is UL 294 Listed for Class 1 applications only.
- Exit devices and wiring must be installed within the protected area.
- The card reader must be connected with shielded, grounded cable.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- A means of verification shall be employed by the user to enable access to the wireless electronic device such as a PIN or biometric feature, which subsequently provides access to the credential application software present on the wireless electronic device.
- The access control system shall have the means to distinguish between the type of credential used via code or description (e.g. authentication/digital signature keys received from a physical card vs. authentication/digital signature keys received from a wireless electronic credential.)
- **Lock Firmware Version**: 1.00.XXXX

Performance Levels

- **Line Security**: Level I
- **Destructive Attack**: Level I
- **Endurance**: Level IV
- **Standby Power**: Level I

UL 1034

- **Static Strength**: 1000 pounds-force (4448N)
- **Dynamic Strength**: 50 foot-pound-force (68J)
- **Endurance**: 250,000 cycles

Note: The ICT Protege Config App is used for onsite installation, troubleshooting and programming.

Flammability Standards

- This lock has been tested and found to comply with UL 10C, UL 10B and CAN/ULC-S104.
- This lock is rated for UL 10C for up to 20 minutes when installed in a steel fire rated door.
- This lock must be installed with approved alkaline batteries for compliance with UL/cUL. Lithium batteries are **not permitted**.

FCC Compliance Statements

FCC PART 15, WARNINGS: INFORMATION TO USER

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not authorized by the party responsible for compliance could void the user's authority to operate this product.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

Disclaimer and Warranty

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.

For warranty information, see our Standard Product Warranty.