Protege Wireless Lock Range

Rear Mount Mortise Wireless Lock

Installation Manual

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: 09-Dec-24 2:30 PM

Contents

Introduction 5

About This Product 5

How Does It Work? 5

Hardware Options 7

Construction Cards 9

Wireless Access Points 9

Replacement Parts 9

Key Cylinder 9

MIFARE Technology 10

About MIFARE 10

Secured MIFARE Card Format 10

About MIFARE DESFire EV1 10

About MIFARE DESFire EV2 10

About MIFARE DESFire EV3 11

MIFARE/DESFire Products 11

Installation Requirements 12

Installation 13

Installation Overview 13

What's Included? 14

Door Preparation 14

Installing the Strike Plate 15

Installing the Lock 16

- Position the Lock Cable 16
- Secure the Lock 17

Fit the Handle and Sectional Trim 18

Key Cylinder and Privacy Thumbturn 20

Installing the Faceplate 21

Installing the Reader 22

Installing the DPS Sensor and Magnet 23

Installing the Lock Control Assembly 24

- Mount and Connect the Lock Control Assembly 24
- Insert the Batteries 27
- Secure the Cover 28

Bluetooth® Access Point Connection 29

RS-485 Connection 29
Shield Connection 30
Programming Locks 31
Operation 32
Maintenance 34
Mechanical Layout 35
Door Template 37
Technical Specifications 39
UL and cUL Installation Requirements 41
CAN/ULC-60839-11-1 41
UL 294 41
UL 1034 41
Flammability Standards 42
FCC Compliance Statements 43
Industry Canada Statement 44
Disclaimer and Warranty 45

Introduction

This installation manual provides instructions and technical specifications for installation of the Protege Rear Mount Mortise Wireless Lock.

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

About This Product

The Protege Rear Mount Mortise Wireless Lock combines an advanced-technology, intelligent wireless credential reader with leading mortise locking 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:

- Native integrated electronic access control solution
- Grade 1 electronic mortise lock meets ANSI lock standards
- Rear mount control unit is easily retrofitted to existing doors
- Sleek reader design with rectangular or circular cover available in white or black
- Integrated LED indicator provides read response and status signaling
- **Bluetooth**® Wireless Technology
- MIFARE and DESFire credential reading
- Supports online or offline operation
- Lock configuration programmable via the Protege Config App
- Advanced technology wireless operation provides battery life of up to 2 years (40,000 activations)*
- USB-C connection to supply power for emergency opening
- IP65 environmental rating allows installation both indoors and outdoors

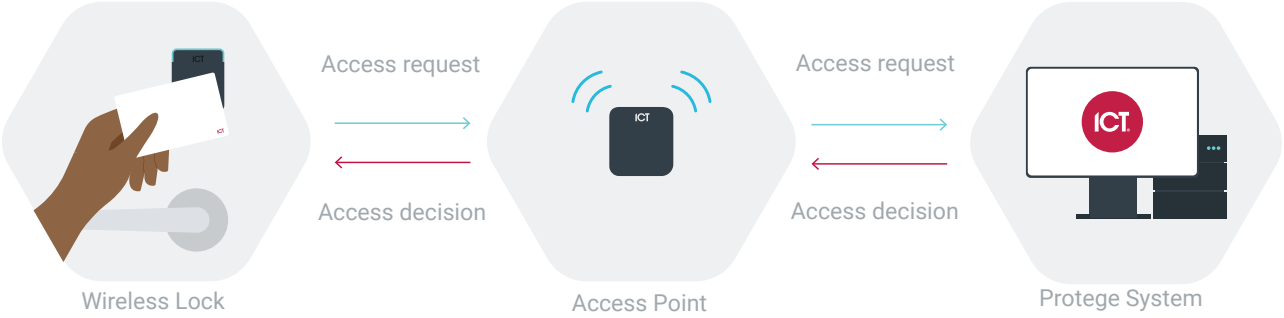
*Not evaluated by UL.

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.

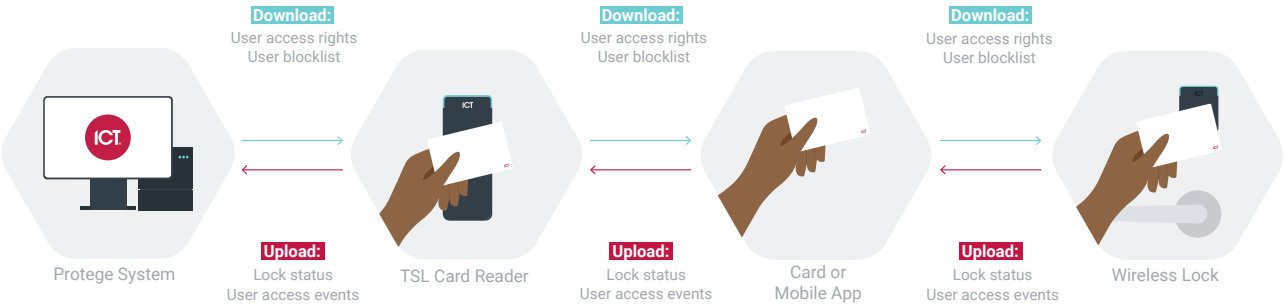


When a user presents their credential at a wireless lock operating in online mode the lock sends a request via the access point to check the credential's access permissions. The controller processes the request and provides an access decision. The lock grants or denies access accordingly, then sends 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 Rear Mount Mortise Wireless Lock offers the flexibility to create your own configuration. Simply choose your preferred components from the range of available options to compile your perfect combination.

1. Select the **Electronic Assembly**.
2. Select the **Mortise Lock Body** type.
3. Specify the **Handing**.
4. Select the optional **Thumbturn** if required.
5. Select a **Handle Set**.
6. Select the **Sectional Trim**.
7. Specify the **Finish**.
8. Specify the **Door Thickness**.
9. Optionally, order a 1 ¼″ key cylinder from a third-party supplier.

Rear Mount Mortise Wireless Lock Options

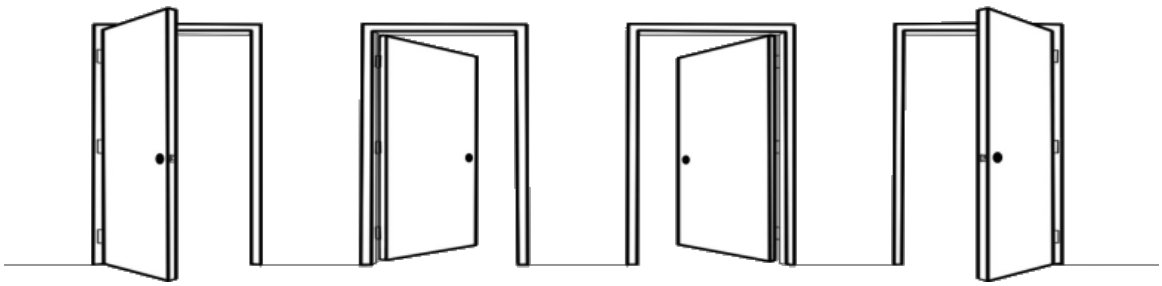
Electronic Assembly	Code
Mortise Electronic Rear Mount Assembly & Reader with Door Position Sensor	RME-DFBT

Mortise Lock Body	Code
Mortise Lock Body (with Optional Thumbturn)	MLB
Mortise Lock Body with Deadbolt and Thumbturn	MLB-DB

Handing	Code
Left Hand	LH
Right Hand	RH
Left Hand Reverse	LHR
Right Hand Reverse	RHR

Ensure that you select the correct handing when you order the locks. **Re-handing the product in the field is possible, but there is a risk of voiding the warranty.** If you do not have the correct locks for a project, we strongly recommend restocking instead of changing the handing of existing stock.

The handing of the mortise lock depends on the door orientation. To determine the handing, stand on the outside (entry side) of the door. Reach your right or left hand across your body to open the door. If the door opens inwards, it is a standard handing; if the door opens outwards, it is a reverse handing.



Left Hand Reverse (LHR) **Left Hand (LH)** **Right Hand (RH)** **Right Hand Reverse (RHR)**

For more information, see the Protege Mortise Lock Handing Change Guide, available from the ICT website.

Optional Thumbturn	Code
Mortise Thumbturn	MT

Handle Set	Code
Acadia	MH-AC
Aspiring*	MH-AS
Banff	MH-BA
Denali	MH-DE
Glacier	MH-GL
Jasper	MH-JP
Nightcap	MH-NI
Peak	MH-PE
Sequoia	MH-SE

* Handing needs to be specified when ordering the Aspiring handle set. Other handles are non-handed.

Sectional Trim	Code
Round Rose	MR-RO
Square Rose	MR-SQ

Finish	Code
Bright Brass Clear Coated	605-BB
Satin Brass Clear Coated	606-SB
Satin Bronze Clear Coated	612-SB
Oil Rubbed Bronze	613-RB
Flat Black	622-FB
Bright Stainless Steel	629-BS
Satin Stainless Steel	630-SS

Color selection applies to the faceplate, strike plate, handle, trim, thumbturn and cartridge armor plate (if applicable). By default, all parts have the same finish. For split finishes, discuss with your sales representative.

Door Thickness	Code
Standard Door: 1.75″ - 2.00″	No code required
Thick Door 1: 2.25″	TD1
Thick Door 2: 2.50″	TD2
Thick Door 3: 2.75″ - 3.00″	TD3
Greater than 3.00″ Custom order required. Please discuss with your sales representative.	CUSTOM

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

Replacement Parts

In addition to the components included in the initial installation, the following individual components may be ordered for replacement.

The required finish will need to be specified when ordering replacement parts.

Mortise Lock Strike Plate Replacement	Code
Mortise Strike Plate	SPM

Mortise Lock Faceplate Replacement	Code
Mortise Dress Plate (no Deadbolt)	DPM
Mortise Dress Plate (with Deadbolt)	DPM-DB

Key Cylinder

The mortise lock mechanism contains space for an optional key cylinder. A suitable 1 ¼″ mortise key cylinder may be obtained from a third-party supplier.

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

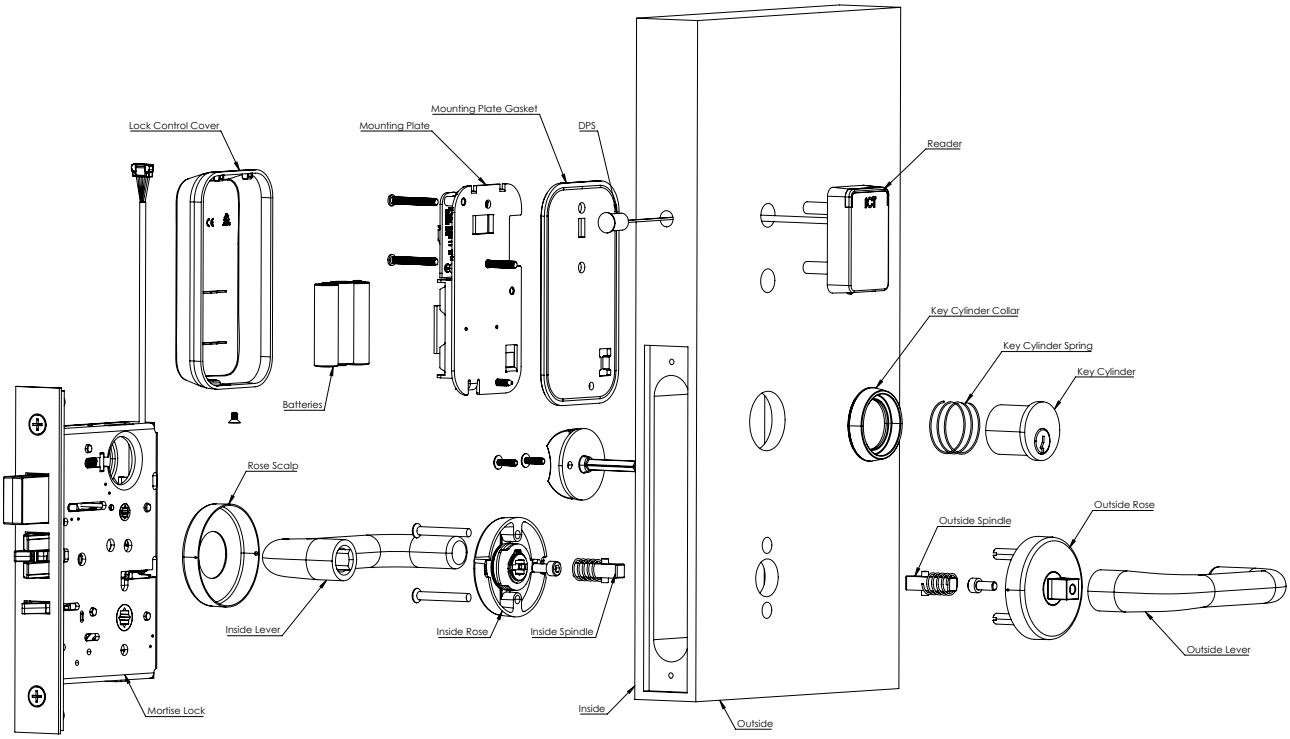
Installation of the wireless lock requires the following steps to be completed in the correct sequence.

1. **Install the strike plate** (see page 15).
2. **Install the lock**.
   - Position the lock cable (see page 16).
   - Secure the lock (see page 17).
3. **Fit the handle and sectional trim** (see page 18).
4. If included, **fit the optional key cylinder and privacy thumbturn** (see page 20).
5. **Install the faceplate** (see page 21).
6. **Install the reader** (see page 22)
7. **Install the optional door position sensor** (see page 23)
8. **Install the lock control assembly**
   - Mount and connect the lock control assembly (see page 24)
   - Insert the batteries (see page 27)
   - Secure the cover (see page 28)

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.

Installation Overview

The following image provides a general overview of the lock installation, the components and their positioning.



The above diagram is for illustration purposes only. Options such as deadbolt, thumbturn and handle style are dependent on the hardware variations installed.

What's Included?

The Protege Rear Mount Mortise Wireless Lock is supplied with the following components.

- 1 x 13.56MHz lock control credential reader with Bluetooth® Wireless Technology
- 1 x Rear mount electronic lock control assembly
  - 1 x Lock control cover
  - 1 x Silicone gasket
  - 1 x Door position sensor and magnet
  - 2 x #8-32 x 1 ¼″ pan head screws for connecting the control assembly to the card reader
  - 2 x #8-32 x 1 ⅞″ pan head screws for connecting the control assembly to the card reader
  - 1 x #5 x ½″ self-drilling pan head screw for securing the control assembly to the door
  - 1 x Countersunk #6-32 x ¼″ Phillips head screw for attaching the cover to the control assembly
  - 3 x Alkaline LR06 AA 1.5V batteries
- 1 x Grade 1 mortise lock
  - 8-wire lock cable wiring loom with socket plug for connection to the lock control cartridge
  - 1 x Faceplate
  - 2 x Countersunk #12-24 combo screws for securing the lock body
  - 2 x Countersunk #8-32 x ¼″ flat head machine screws for installing the faceplate
  - 1 x Deadlatch plate and strike plate
  - 2 x #12-24 combo screws for installing the strike plate
- 1 x Door handle kit with sectional trim
- 1 x Optional thumbturn

Door Preparation

Doors should be ordered according to the drill template so that they come pre-prepped from the supplier.

Door Thickness

1 ¾″ standard. Larger thicknesses available, see Hardware Options.

Strike Prep

The mortise lock uses a non-handed curved lip with a deadlatch plate which retracts the deadlatch. The strike prep must be prepared in accordance with the drill template.

Drill Template

Drill templates should be used to ensure correct installation. Any deviation from the template can result in the lock not functioning correctly.

A to-scale drill template is supplied with the lock and is also available from www.ict.co/rear-mount-mortise-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.

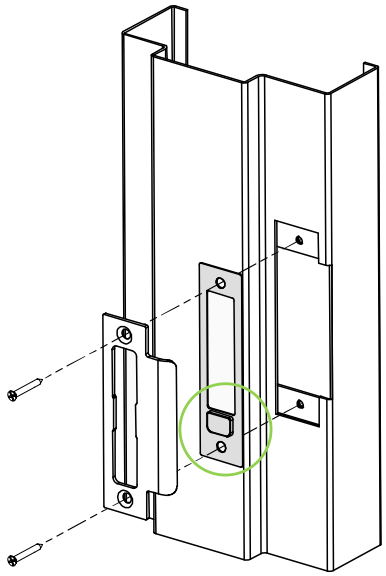
Screw Type	Pilot Hole Diameter (Hardwood)	Pilot Hole Diameter (Softwood)
#5	5/64″	1/16″
#8	1/8″	3/32″
#12	9/64″	1/8″

Installing the Strike Plate

1. Prepare the door jamb for the mortise lock strike plate.
2. Install the deadlatch plate behind the strike plate, with the **slider towards the bottom**.

   The deadlatch retracts when it hits the deadlatch plate, locking the latch in place and preventing the lock from being tampered or jimmied.

3. Using the two #12-24 combo screws provided, secure the deadlatch plate and strike plate in position.

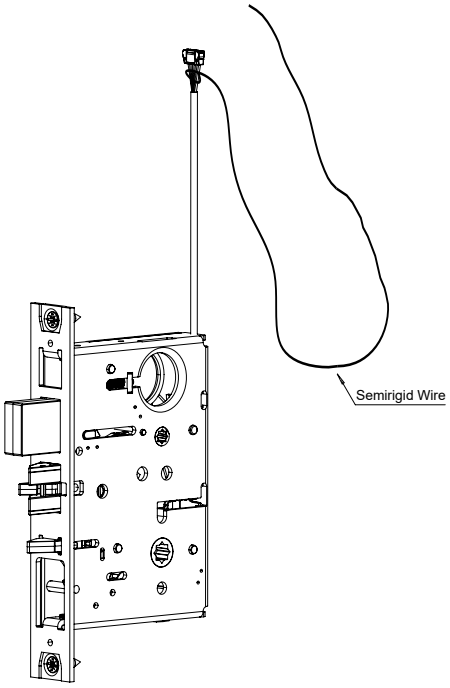


Installing the Lock

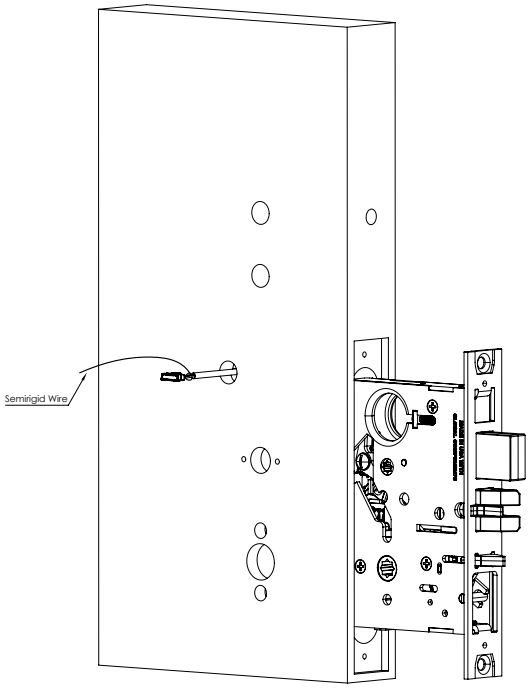
Position the Lock Cable

Before the mortise lock can be installed the lock cable needs to be threaded through the lock cavity and out the lock cable hole. This cannot be done after the lock is installed.

1. Attach a semirigid wire to the lock cable connector.
2. Feed the semirigid wire and lock cable into the lock cavity and out through the cable hole at the rear of the cavity, on the inside of the door.



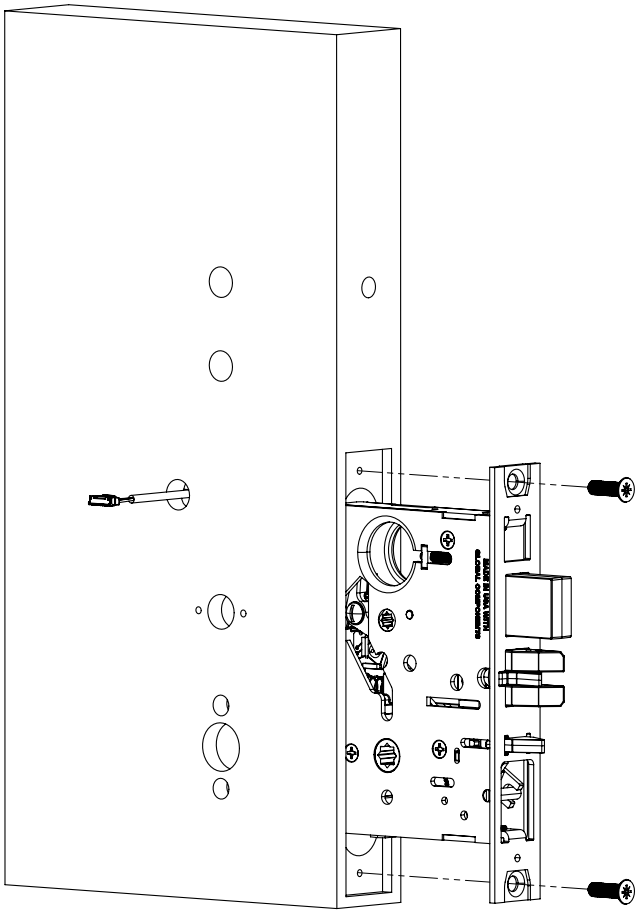
Attach the wire to the lock cable.



Pass the wire through the cable hole.

Secure the Lock

1. Insert the mortise lock cartridge into the lock cavity, ensuring the cable remains in position.
2. Using the two #12-24 combo screws provided, secure the lock body in position.

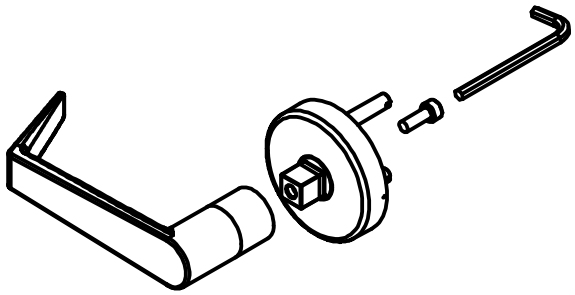


Fit the Handle and Sectional Trim

Assemble the handle and sectional trim, ensuring the correct inside/outside door and handle positions and spindle orientation.

Levers need to be firmly secured to prevent loose handles. The cap screws can be difficult to tighten sufficiently with hex keys alone, so a T-handle or pliers may be helpful for securing the handles.

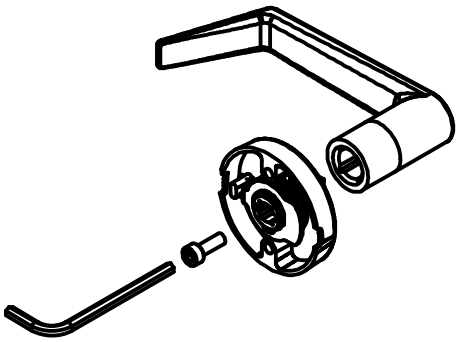
1. Assemble the outside rose.
   i. Fit the rose scalp cover onto the outside rose assembly by aligning the dimples with the slots in the rose plate. Secure by rotating clockwise until tight.
   ii. Fit the handle onto the rose assembly spindle.
   iii. Using the M5 x 0.8 x 14mm socket head cap screw and 4mm hex key provided, secure the handle.



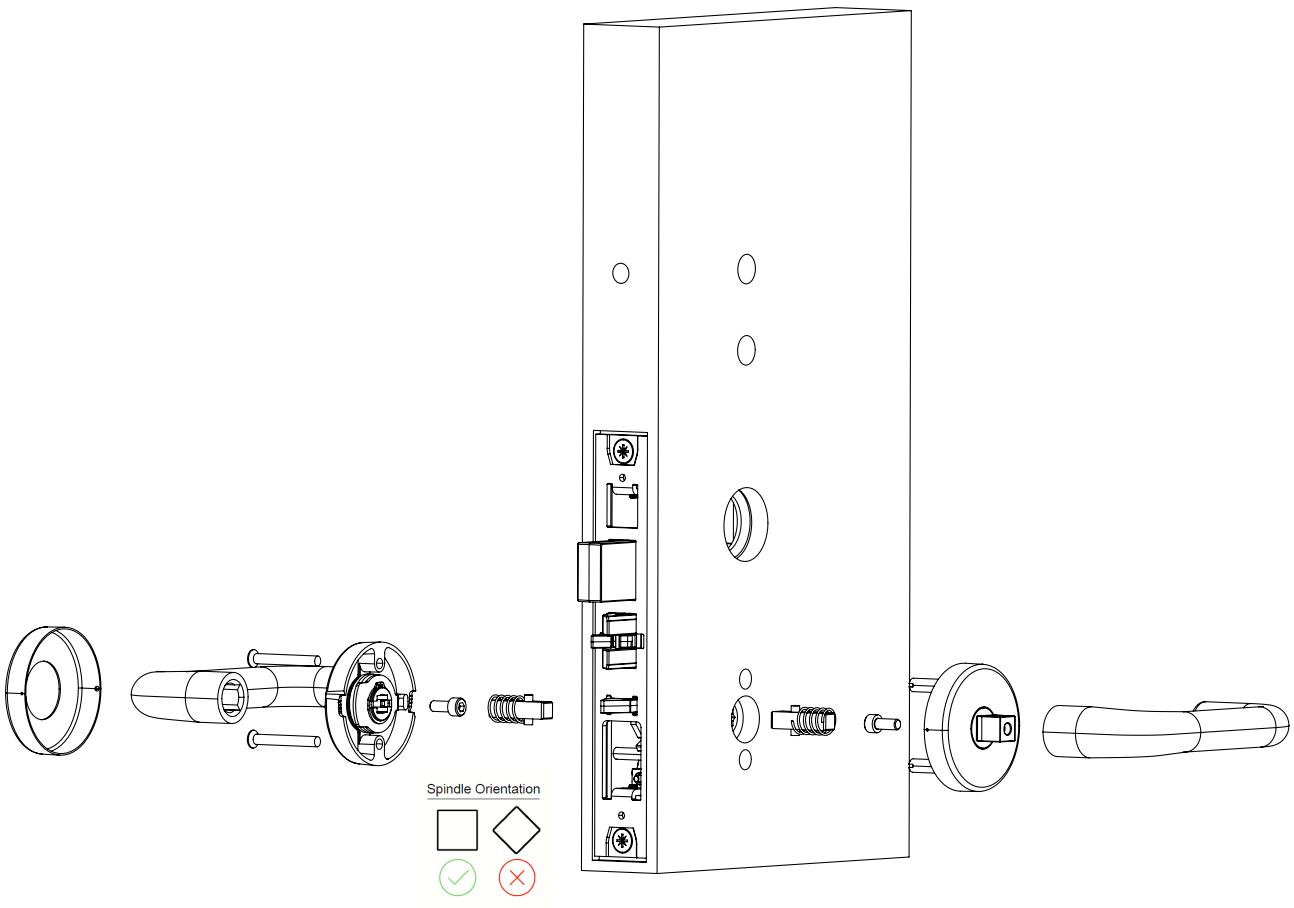
2. Assemble the inside rose.

   This step is **not required** for Aspiring and Jasper handle sets (see Step 6).

   i. Fit the handle onto the rose assembly spindle.
   ii. Using the M5 x 0.8 x 14mm socket head cap screw and 4mm hex key provided, secure the handle.



   The inside rose scalp cover should not be installed at this point.



3. Install the spindles and springs on both sides.
   - The springs and the long end of the spindles must be on the handle side (away from the door), as shown above.
   - Ensure that the spindle orientation is correct, as shown above.
4. Install the outside assembly, aligning with the spindle. Confirm spindle engagement by rotating the lever down and verifying that the latch retracts.
5. Install the inside assembly, aligning with the spindle. Confirm spindle engagement.
   i. Using the #10-24 x 1-½" flat head machine screws provided, secure the inside rose assembly.

      Do not overtighten the screws, as this can interfere with lock operation.

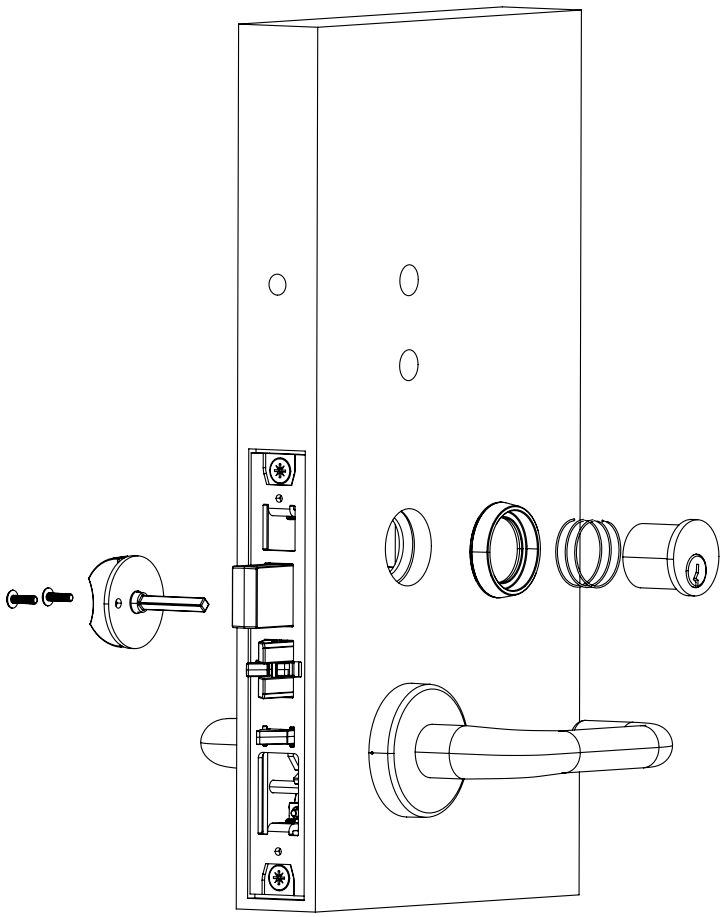
   ii. Fit the rose scalp cover onto the inside rose assembly by aligning the dimples with the slots in the rose plate. Secure by rotating clockwise until tight.
6. For Aspiring and Jasper handle sets **only**:
   i. Slide the lever onto the assembly spindle, ensuring the screw hole is on the underside of the lever.
   ii. Using the M5 x 0.8 set screw and 2.5mm hex key provided, secure the lever.

Key Cylinder and Privacy Thumbturn

The following instructions are only required if installing the optional key cylinder and privacy thumbturn.

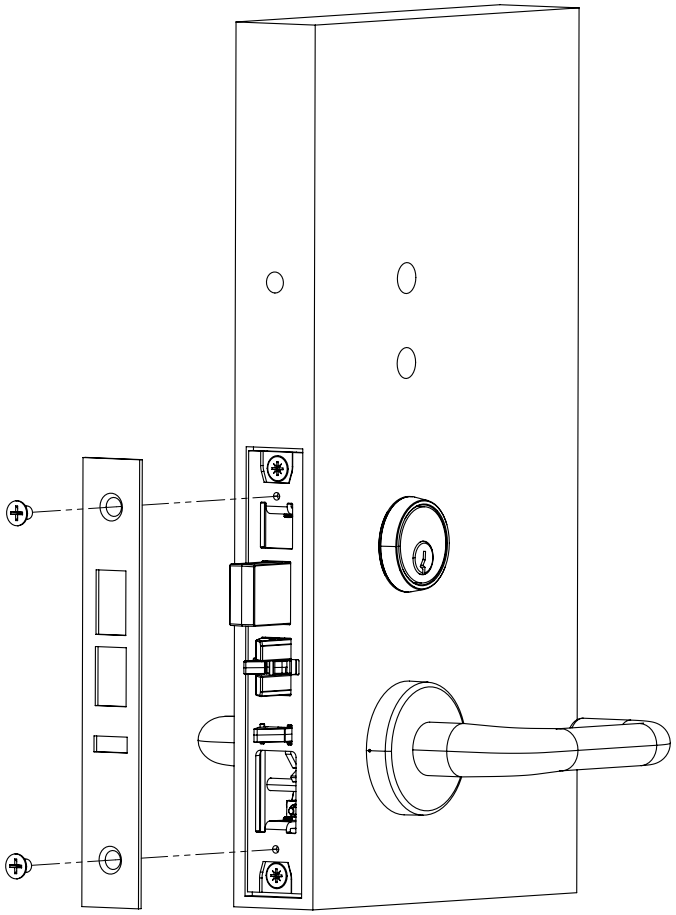
Ensure that the key cylinder is installed on the outside of the door with the thumbturn on the inside.

1. Insert the key cylinder into the collar and spring, then thread it into the lock body until the cylinder is flush or slightly recessed in the trim collar.
2. Secure the key cylinder following the manufacturer's instructions.
3. Line up the thumbturn vertically so that the mounting holes are accessible, then gently position the thumbturn spindle in the lock body spindle receiver.
4. Secure using the two stainless steel #6 x ½" truss head sheet metal screws provided.
5. Test the thumbturn operation of the deadbolt. It should turn smoothly and easily.



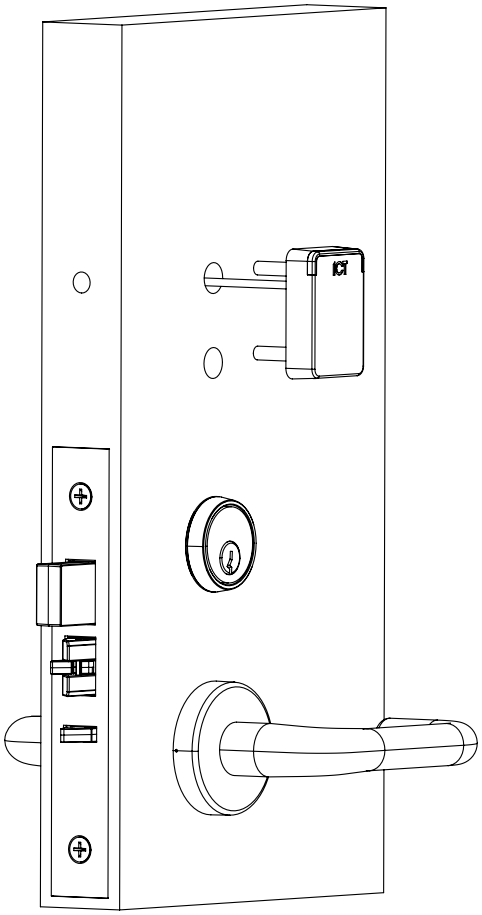
Installing the Faceplate

1. Using the two #8-32 x ¼" flat head machine screws provided, install the faceplate.



Installing the Reader

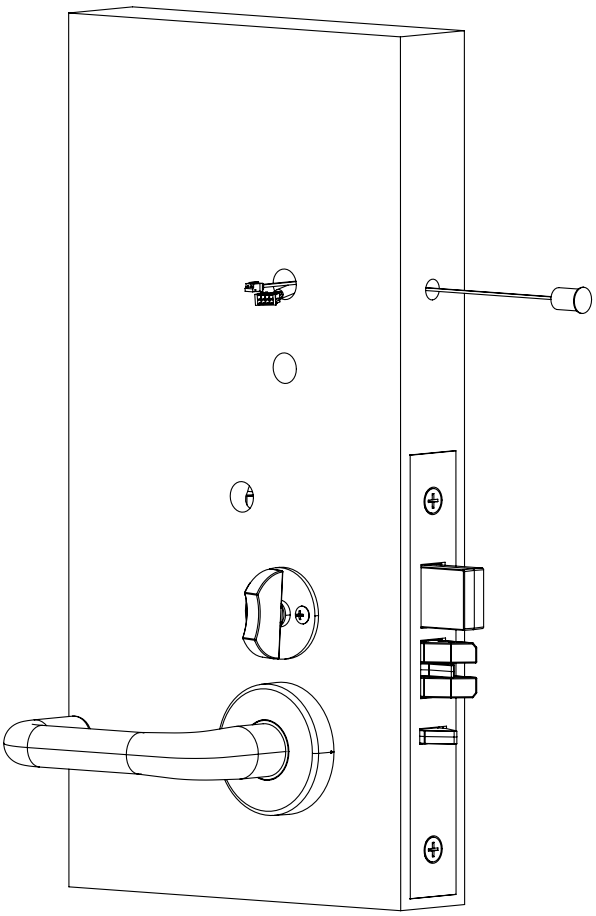
1. Thread the reader cable through the top hole in the door.
2. Slot the two screw posts into the corresponding holes.



Installing the DPS Sensor and Magnet

An optional Door Position Sensor (DPS) is provided with the lock. This is not used in offline locking systems but can be used in online systems to detect when the door is opened or forced.

1. The sensor cable includes a fireproof sleeve that needs to be at the sensor end of the cable when installed. Slide the fireproof sleeve along the cable until it is hard up against the sensor.
2. Thread the sensor cable through the hole in the edge of the door.
3. Pull the cable through the upper hole on the inside of the door, alongside the reader cable.
4. Slot the sensor into the edge of the door.
5. Install the accompanying magnet in the door jamb as directly opposite the sensor as practical. The sensor has an operating range of approximately 12mm (½") from the sensor to the magnet before contact is broken.



Installing the Lock Control Assembly

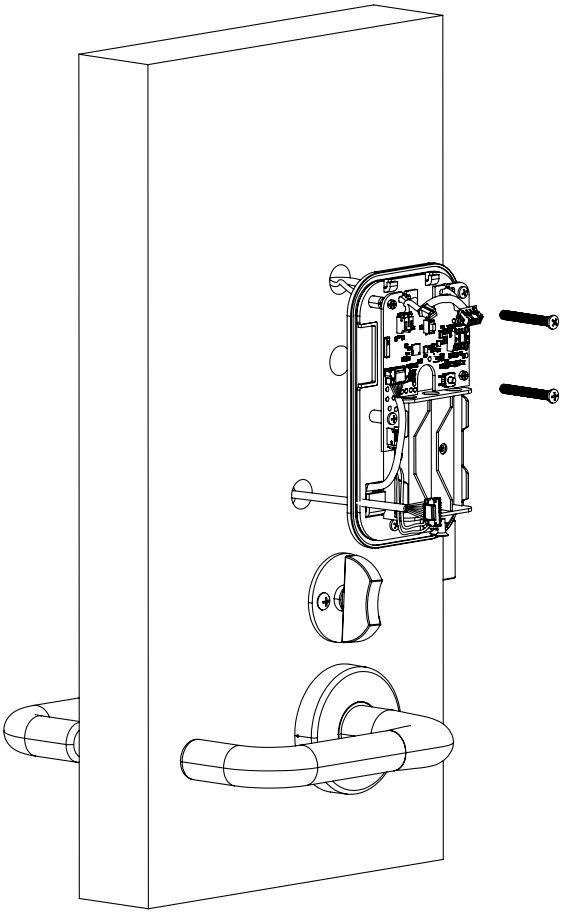
Mount and Connect the Lock Control Assembly

The lock control assembly needs to be secured in position on the door using the bolt-through fixings from the card reader. While doing this it is important that all cables are carefully positioned for connection to the lock control board.

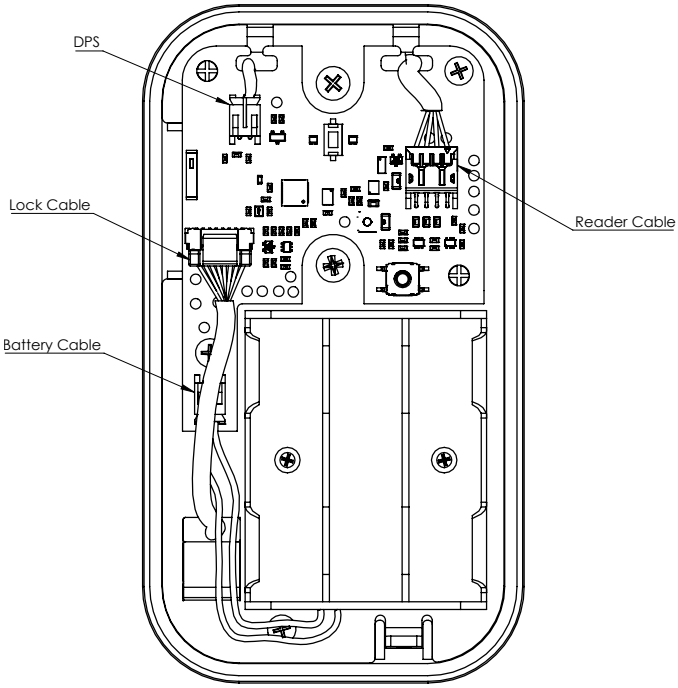
1. The lock control assembly includes a silicone gasket which sits between the mounting plate and the door. First, pass the cables through the holes in the gasket:
   - Pass the **lock cable** through the rectangular slot at the bottom left corner.
   - Pass the **reader cable** through the rectangular slot at the top center. Ensure that the black and yellow wires are on the left side of the cable so that the orientation is correct.
   - Pass the **DPS cable** (if in use) through the rectangular slot at the top center of the gasket.

   Image to be created.

2. Hold the lock control assembly in front of the gasket. Pass the cables through the matching slots on the mounting plate.
3. Slot the reader cable into the notch at the top right of the control board.
4. Slot the DPS cable into the notch at the top left of the control board.

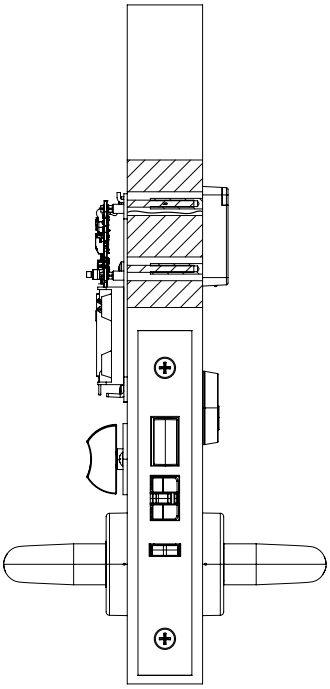


5. Connect the cables to the lock control board as shown in the diagram below.



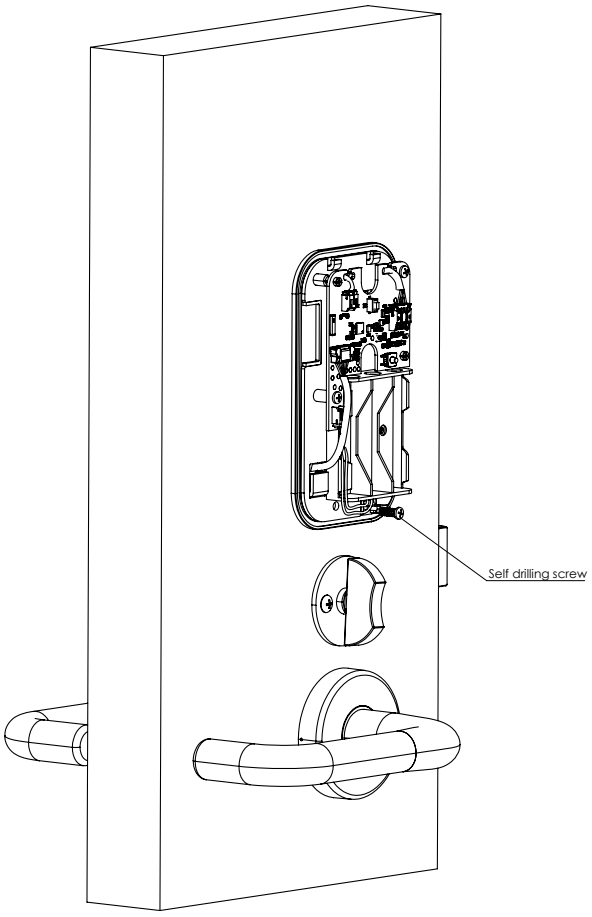
   i. Connect the **lock cable** on the left side, above the battery cable.
   ii. Connect the **DPS cable** (if used) at the top left of the board.
   iii. Connect the **reader cable** at the top right of the board.

6. Use two #8-32 pan head screws to connect the lock control assembly and gasket through to the screw posts of the card reader. 1 ¼″ and 1 ⅞″ screws are provided to account for different door thicknesses (details TBC).



7. Using the #5 x ½" self-drilling pan head screw provided, secure the bottom section of the mounting plate.

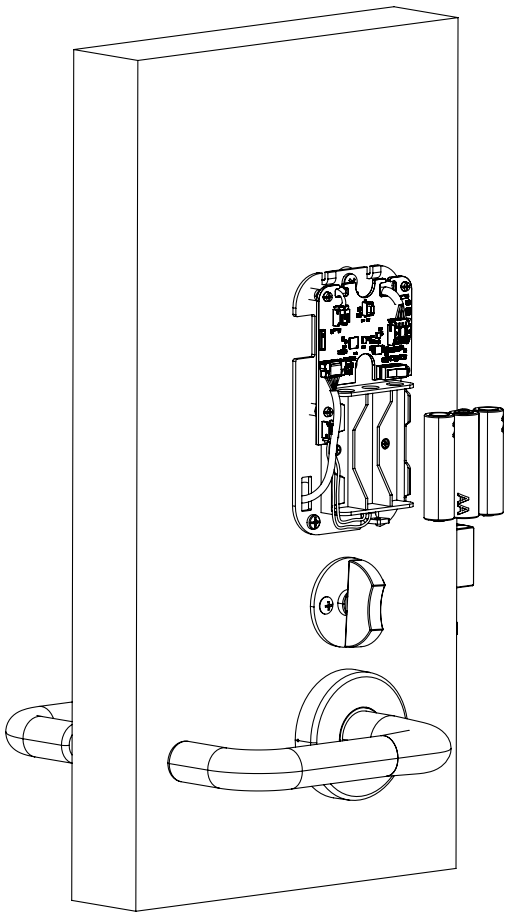
This screw is suitable for self-drilling into wood or metal doors.



Insert the Batteries

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

1. Insert the 3 x AA batteries provided.



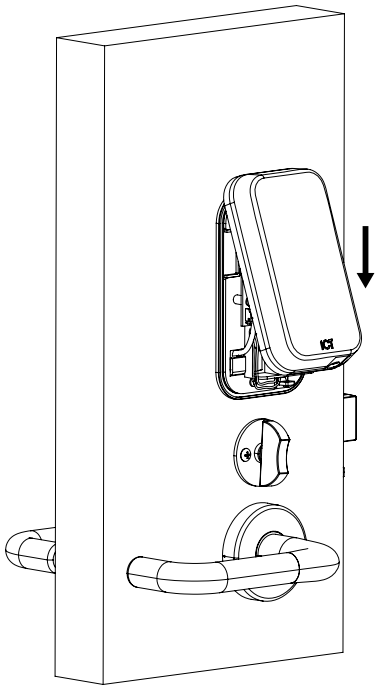
For UL installations (UL 294), UL approved batteries must be used.

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

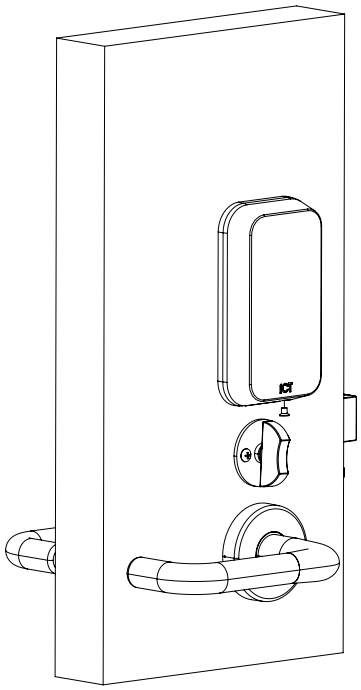
Approved batteries include Energizer MAX Alkaline.

Secure the Cover

1. Lower the lock control assembly cover onto the hooks at the top of the mounting plate, as shown below.



2. Press on the bottom of the cover until it slots over the lower rim of the mounting plate, lining up the screw hole at the bottom.
3. Secure the cover onto the mounted base using the countersunk #6-32 x 3/16″ Phillips head screw provided.



Bluetooth® Access Point Connection

Online operation is achieved using a TSL reader which has been configured as an access point. This is wired to the controller's RS-485 port to act as a network connection node between the wireless lock and the controller.

One TSL reader supports up to 8 wireless locks operating in online mode.

Using the recommended cables, splice the cable together with the pigtail of the TSL reader and seal the splice. Route the cable from the reader to the host module. Connect the cable to the module port as shown in the connection diagram that follows.

The recommended cable types for RS-485 are:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120 ohm

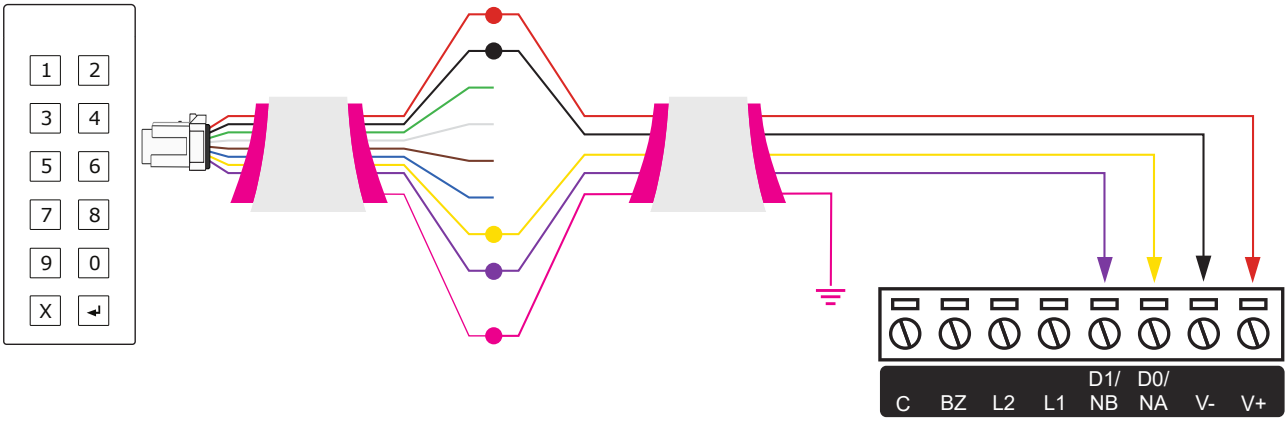
Maximum distance: 900m (3000ft)

For UL installations, a UL Listed (UL 294) Protege controller and TSL reader must be used.

For cUL installations, a cUL Listed (CAN/ULC 60839-11-1) Protege controller and TSL reader must be used.

RS-485 Connection

Connecting a TSL reader to a controller to act as a Bluetooth® access point:



Wiring Connections

Color	Wire	Connection
	Red	**V+** 12VDC positive
	Black	**V-** 12VDC negative
	Yellow	**D0/NA** RS-485 A
	Violet	**D1/NB** RS-485 B
	Shield	Shield (drain) wire. Frame grounded at one point only

Shield Connection

Connect the TSL reader pigtail shield and cable shield wires together at the reader pigtail splice. Connect the cable shield to a suitable earth point. **Do not** connect the cable shield to a ground or AUX connection. The pigtail shield wire is **not** terminated inside the reader.

Important:

- The reader must be connected to the module port using a shielded cable.
- The shield must only be connected at one end of the cable in the metallic enclosure (frame grounded).
- Do not connect the cable shield to an AUX-, 0V or V- connection on the module.
- Do not connect the cable shield to any shield used for isolated communication.
- The reader pigtail shield and cable shield wires should be joined at the reader pigtail splice.
- Do not terminate the reader shield wire inside the reader.

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

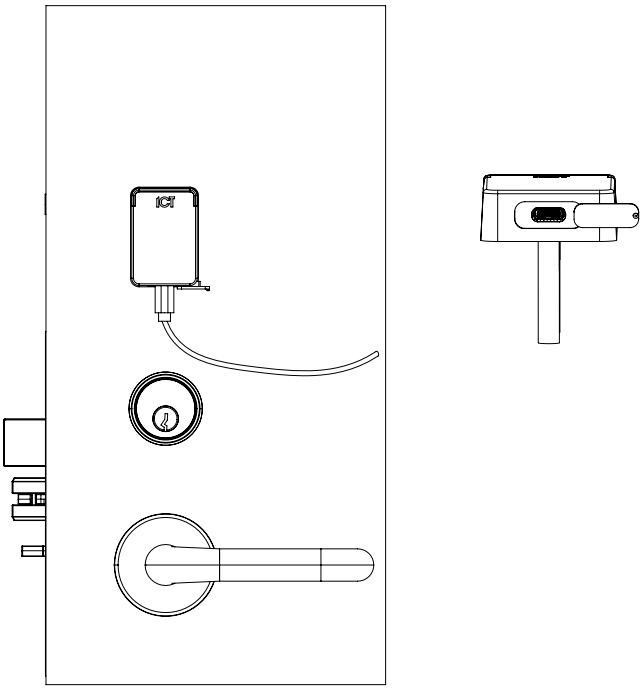
Operation	LED Indication	LED Description	Beeper
Construction Mode - Access Granted - Battery Low < 3.55V		2 Purple flashes (100ms/100ms) 1 Red flash (200ms)	2 short
Construction Mode - Access Denied		3 Orange flashes (100ms/100ms)	1 long
Construction Mode - Access Denied - Battery Low < 3.8V		2 Orange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

Rear mount mortise locks have an expected battery life of up to 2 years (40,000 activations), dependent on usage levels and reader configuration. Batteries should be replaced every 2 years, or earlier if required.

In case of battery failure, slide open the cover at the base of the reader and supply emergency power via the USB-C port.

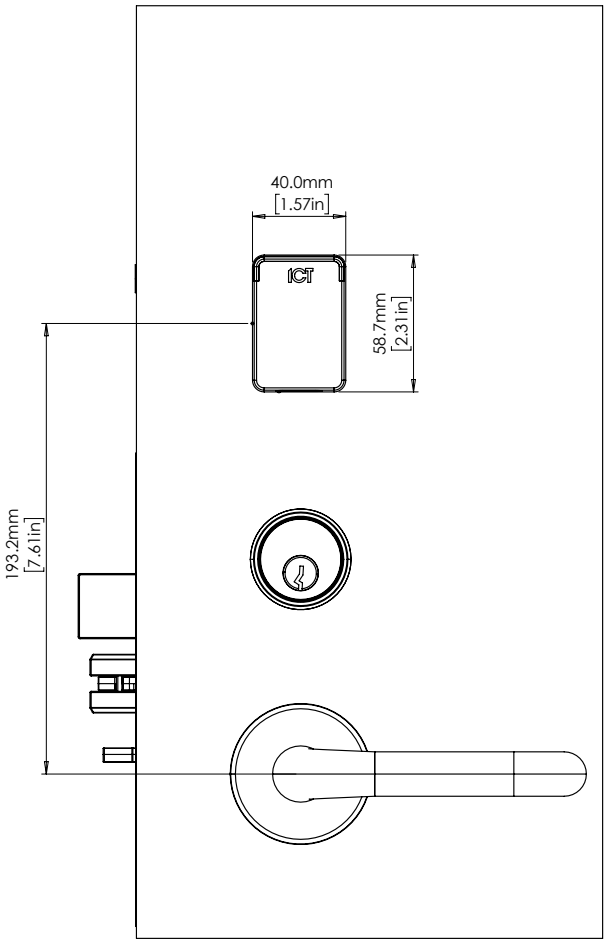
Any USB power supply unit can be used to supply emergency power to the lock.

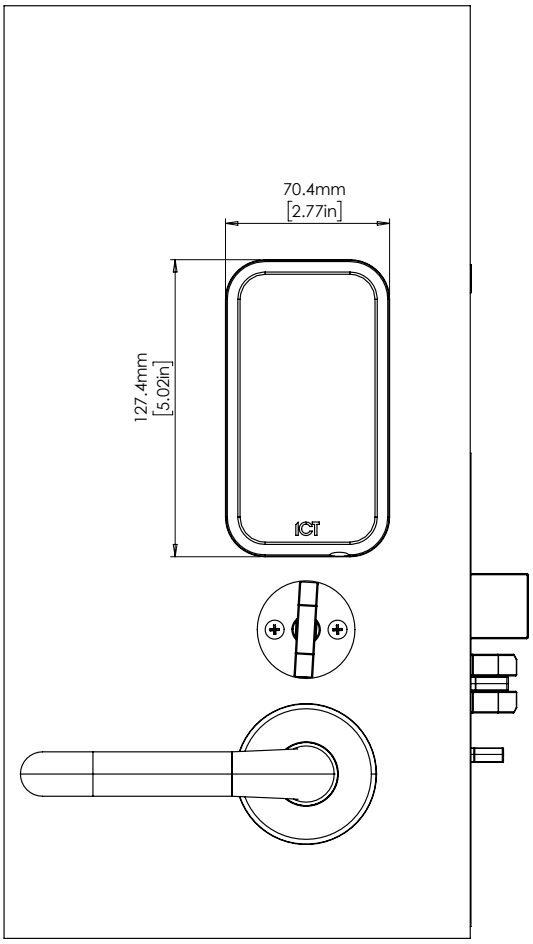


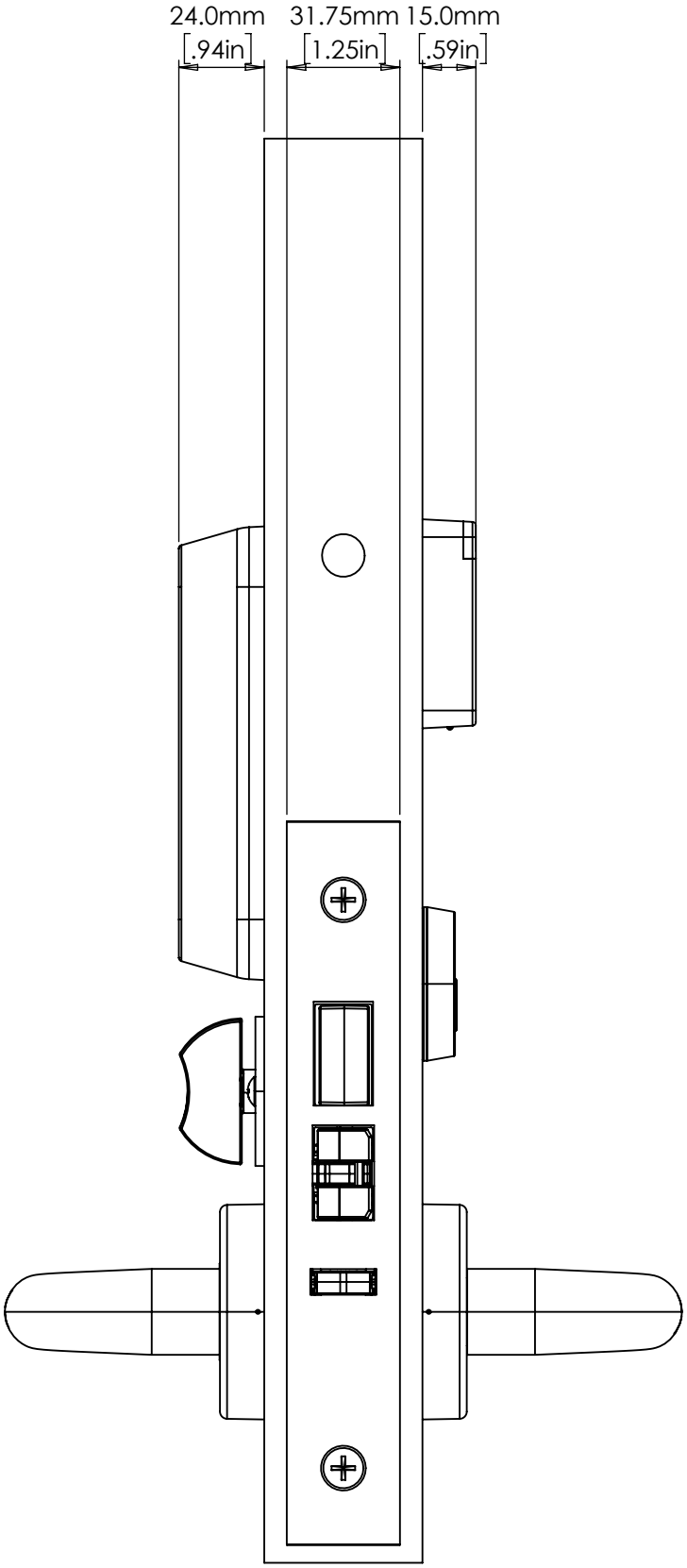
Length of battery life not evaluated by UL.

Mechanical Layout

Optional key cylinder is not supplied.

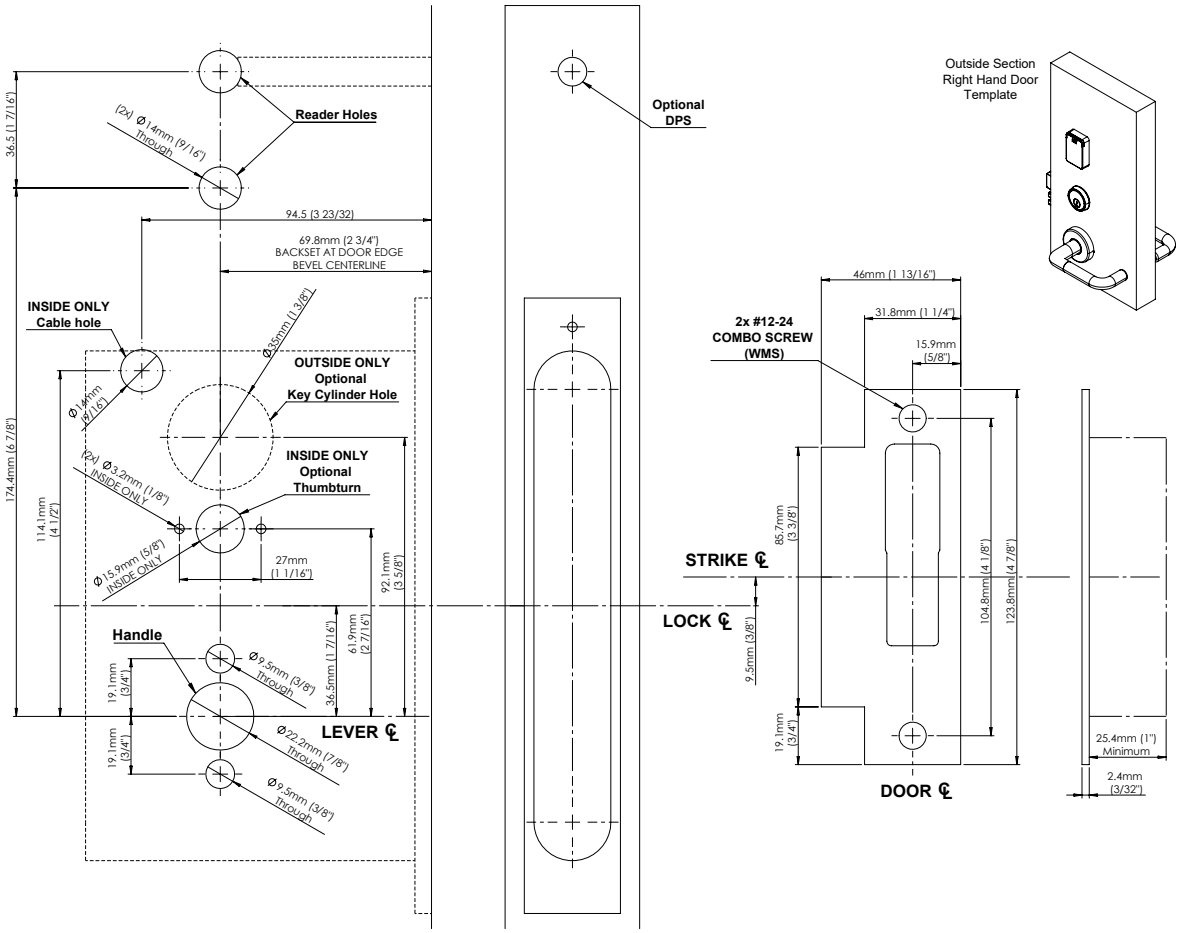


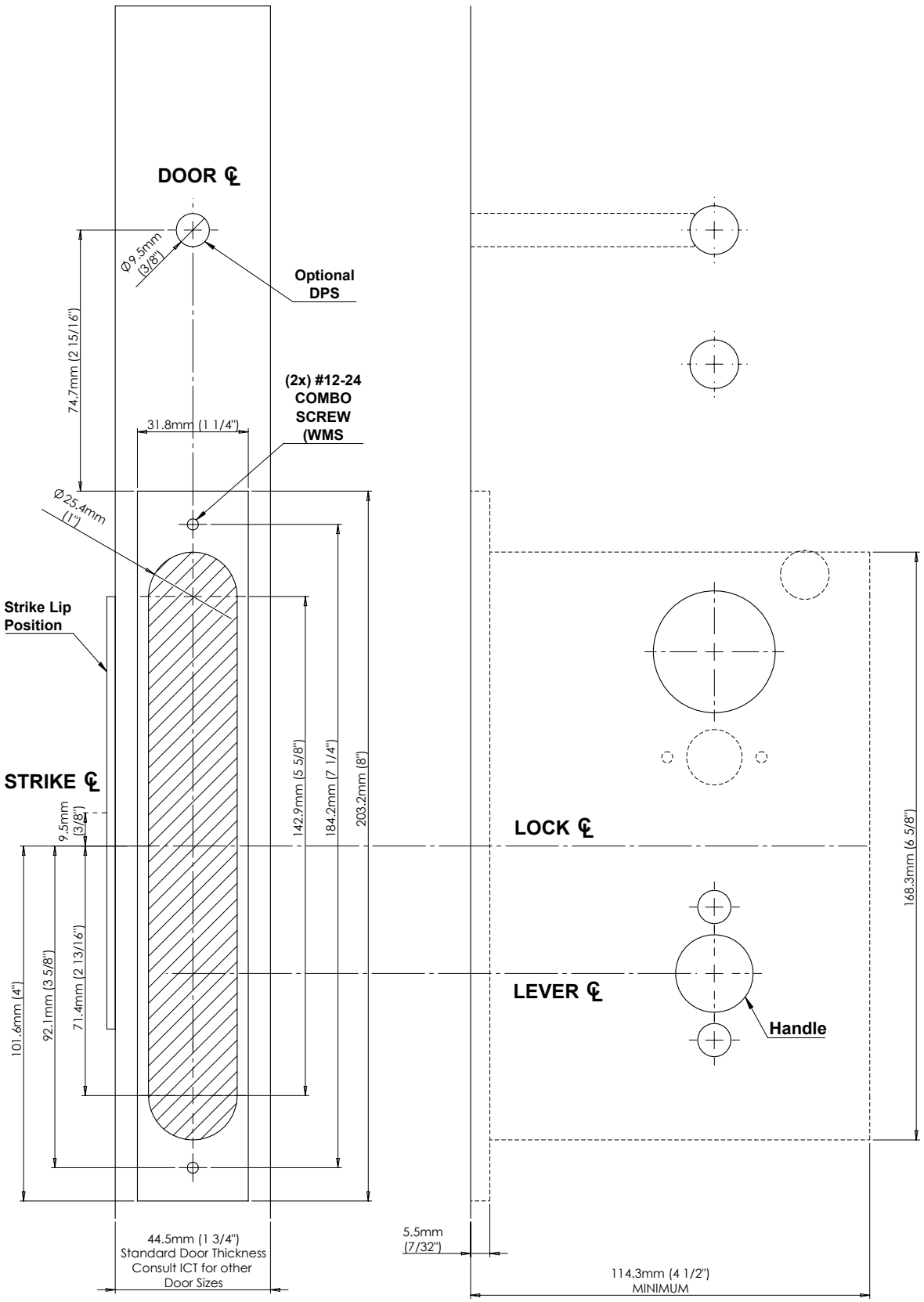



24.0mm
[.94in]
31.75mm
[1.25in]
15.0mm
[.59in]

Door Template

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




DOOR ℄
Ø 9.5mm (3/8")
Optional DPS
74.7mm (2 15/16")
(2x) #12-24 COMBO SCREW (WMS
31.8mm (1 1/4")
Ø 25.4mm (1")
Strike Lip Position
STRIKE ℄
9.5mm (3/8")
142.9mm (5 5/8")
184.2mm (7 1/4")
203.2mm (8")
LOCK ℄
168.3mm (6 5/8")
101.6mm (4")
92.1mm (3 5/8")
71.4mm (2 13/16")
LEVER ℄
Handle
44.5mm (1 3/4")
Standard Door Thickness
Consult ICT for other
Door Sizes
5.5mm (7/32")
114.3mm (4 1/2")
MINIMUM

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 (x3) UL/cUL Energizer MAX Alkaline
Expected Battery Life	Up to 2 years (40,000 activations) Length of battery life not evaluated by UL.
Emergency Power Supply	USB-C connection allows power supply for emergency opening
Operating Voltage	Rated 4.5VDC Operating range 3.83 - 4.95VDC
Operating Current	370mA (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 1 mortise lock
Casing	12 gauge heavy duty dichromated alloy steel
Faceplate	Stainless steel. Beveled. H x W 203.2 x 31.75mm (8 x 1.25")
Strike Plate	Stainless steel. Non-handed. Curved lip
Latchbolt	Stainless steel. Anti-friction. 19mm (0.75") throw
Deadbolt	Stainless steel. 25.4mm (1") throw
Handle Rotation	35 degrees

Door Thickness	1.75″ - 3.00″ (above 3.00″ available by custom order)
Dimensions	
Reader Body (H x W x D)	62 x 40 x 16mm (2.4 x 1.6 x 0.6″)
Control Assembly (H x W x D)	131 x 74 x 24mm (5.1 x 2.9 x 1.0″)
Operating Conditions	
Environment IP Rating	IP65
Operating Temperature	UL/cUL -35° to 66°C (-31° to 151°F) :
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor/outdoor use (relative humidity)

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**: Outdoor, general
- **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**: 100,000 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 3 hours when installed in a steel fire rated door.
- This lock is rated for UL 10C for up to 90 minutes when installed in a wooden 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.

Product Name: ICT Protege Rear Mount Electronic Reader

FCC ID: UAURMEDFBT

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.

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.