Wireless Lock Range

Cartridge Mortise Wireless Lock

Installation Manual

Last Published: 24-Jul-23 03:15 PM

Contents

Introduction

This installation manual provides instructions and technical specifications for installation of the ICT Cartridge Mortise Wireless Lock.

About This Product

The ICT Cartridge Mortise Wireless Lock combines an advanced-technology, intelligent wireless credential reader with leading mortise 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 lock control card reader include:

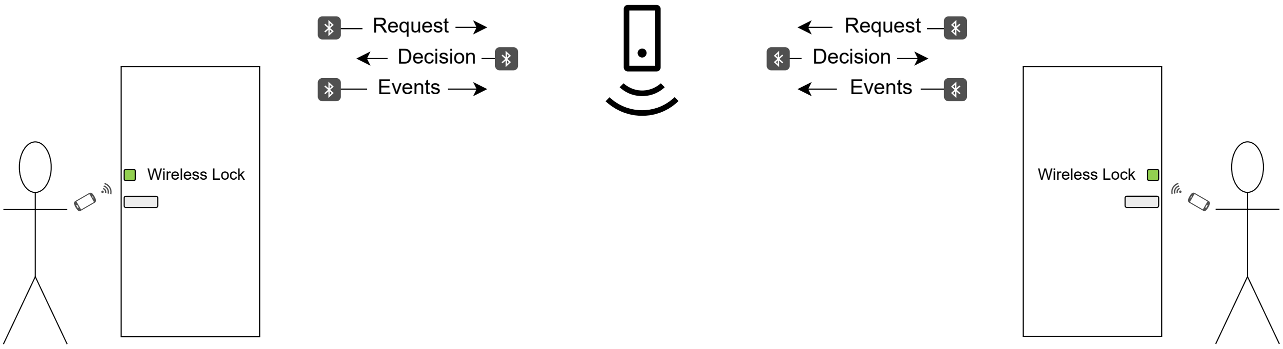
- **Bluetooth**® Wireless Technology
- MIFARE and DESFire credential reading
- Keep alive transmission every 30 seconds for intelligent tamper management
- Integrated LED indicator provides read response and status signaling
- USB-C connection to supply power for emergency opening
- Supports online or offline operation
- Reader configuration programmable via the Protege Config App
- Advanced technology wireless operation provides 2 years battery life (40,000 activations)

How Does It Work?

Online Mode

When the wireless lock is configured to operate in online mode it operates almost the same as a wired system. A wired Bluetooth® node acts as a network connection point, facilitating communication between the lock and the controller. When a user presents their credential the lock checks their access permissions in real time, via the Bluetooth® node. 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 that is configured to operate in online mode loses connection to the Bluetooth® node or hub it does not revert to operating in offline mode ('data on card'). It will flash a red LED every second to indicate lost connection. It will not unlock for any credential presented.

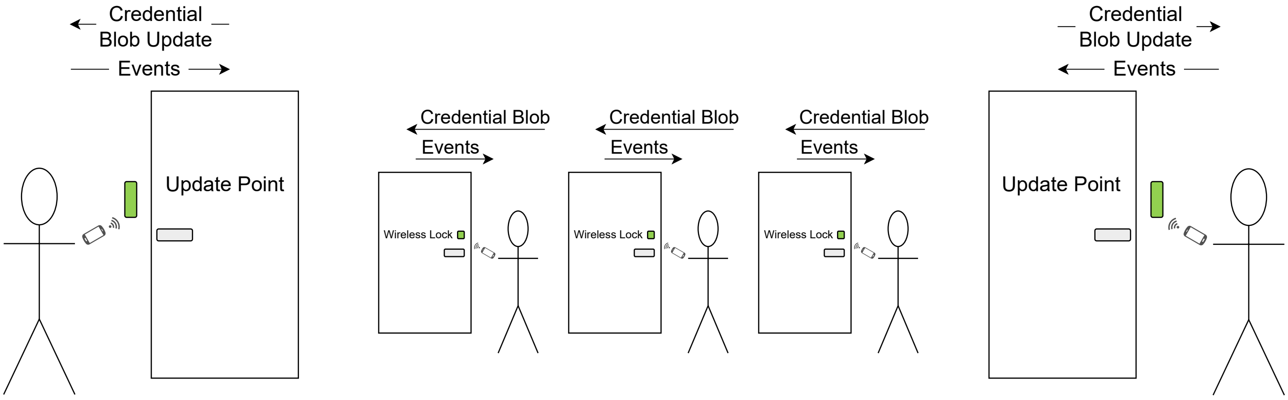


When a user presents their credential at a wireless lock operating in online mode the lock sends a request via the Bluetooth® node to check the access permissions of the supplied credential. The controller processes the request and provides an access decision response. The lock grants or denies access 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 online operation, where the lock checks with the controller to determine whether to grant or deny access, in offline wireless lock operation a user's access permissions are carried in their credential ('data on card').

When the wireless lock is configured to operate in offline mode each user acts as a walking data store, carrying their credential 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 doors, access level, 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 both locks configured to operate in online mode and locks configured to operate in offline mode .

Hardware Options

The ICT Cartridge 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. Specify the **Electronic Cartridge** configuration.
2. Choose a **Reader Cover**.
3. Select the **Mortise Lock Body** type.
4. Specify the **Handing**.
5. Select the optional **Key Cylinder** if required.
6. Select a **Handle Set**.
7. Select the **Sectional Trim**.
8. Specify the **Finish**.

Cartridge Mortise Wireless Lock Options

Electronic Cartridge	Code
Mortise Electronic Cartridge & Reader	CME-DFBT
Mortise Electronic Cartridge & Reader with Door Position Sensor	CME-DFBT-DPS

Reader Cover	Code
Black Circular	MC-BC
Black Rectangular	MC-BR
White Circular	MC-WC
White Rectangular	MC-WR

Mortise Lock Body	Code
Mortise Lock Body	MLB
Mortise Lock Body with Deadbolt and Thumbturn	MLB-DB

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

Optional Key Cylinder	Code
Key Cylinder	MK

Two keys are supplied with each lock.

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
Satin Chromium Plated	626-SC
Bright Stainless Steel	629-BS
Satin Stainless Steel	630-SS

Color selection applies to faceplate, strike plate, handle, trim, key cylinder, thumbturn and cartridge armor plate.

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.

Thumbturn Replacement	Code
Mortise Thumbturn	MT

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

Electronic Lock Control Cartridge Armor Plate Replacement	Code
Cartridge Dress Plate	DPC

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)

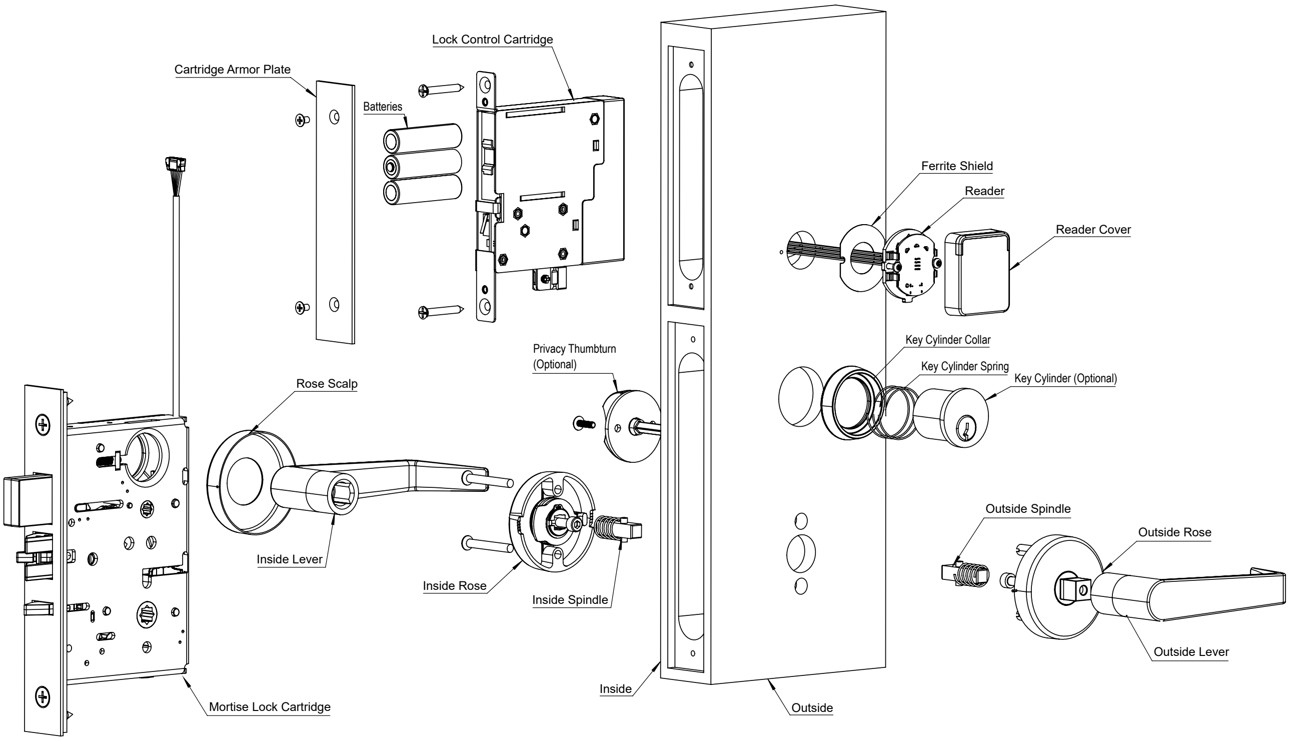
Installation

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

1. **Install the strike plate** (see next page).
2. **Install the lock**.
   - Position the lock cable (see page 15).
   - Secure the lock (see page 16).
3. **Fit the handle and sectional trim** (see page 17).
4. If included, **fit the optional key cylinder and privacy thumbturn** (see page 19).
5. **Install the faceplate** (see page 20).
6. **Install the lock control cartridge**.
   - Position the reader cable (see page 21).
   - Connect the lock cable (see page 22).
   - Secure the cartridge (see page 23).
7. **Install the reader**.
   - Attach the reader base (see page 25).
   - Connect the reader (see page 24).
8. **Insert the batteries** (see page 26).

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. Installation options such as deadbolt, key cylinder, thumbturn, handle style and reader cover options are dependent on the hardware variations installed.

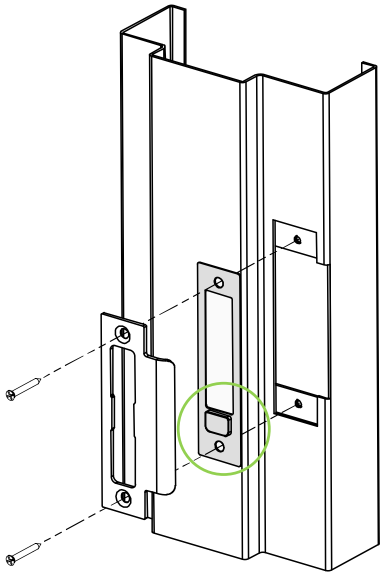
What's Included?

The ICT Cartridge Mortise Wireless Lock is supplied with the following components.

- 1 x 13.56MHz lock control credential reader with Bluetooth® Wireless Technology
    - USB-C connection to supply power for emergency opening
    - 1 x Reader cover (rectangular or circular)
    - 1 x Reader mounting base
    - 1 x Ferrite shield
    - 2 x N°4 9.5mm pan head self-tapping screws for mounting the reader base
- 1 x Electronic lock control cartridge
    - 8-wire reader cable wiring loom with socket plug for connection to the reader
    - 1 x Armor plate
    - 2 x Countersunk G8 x 3/4" flat head screws for securing the cartridge body
    - 2 x Countersunk M3.5 x 6mm Pozidriv screws for installing the armor plate
    - 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 1/4" flat head machine screws for installing the faceplate
    - 1 x Dead latch plate and strike plate
    - 2 x #12-24 combo screws for installing the strike plate
- 1 x Door handle kit with sectional trim
- Optional key cylinder

Installing the Strike Plate

1. Prepare the door jamb for the mortise lock strike plate.
2. Install the dead latch plate behind the strike plate, with the **slider toward the bottom** for dead latch.
3. Using the two #12-24 combo screws provided, secure the dead latch plate and strike plate in position.



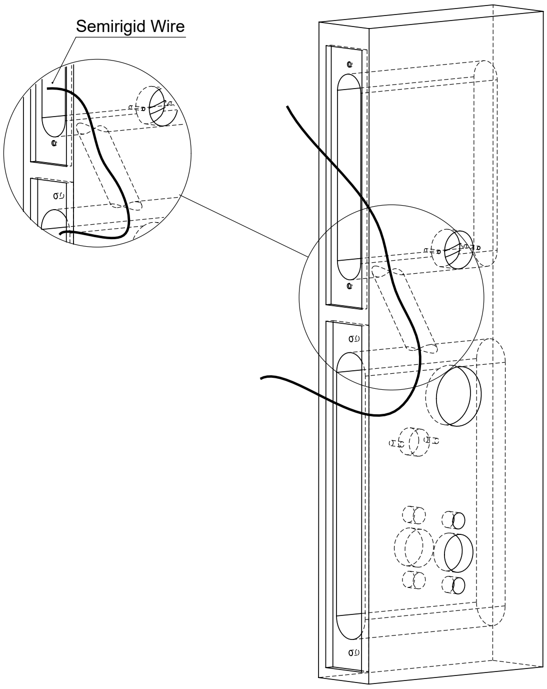
Installing the Lock

Position the Lock Cable

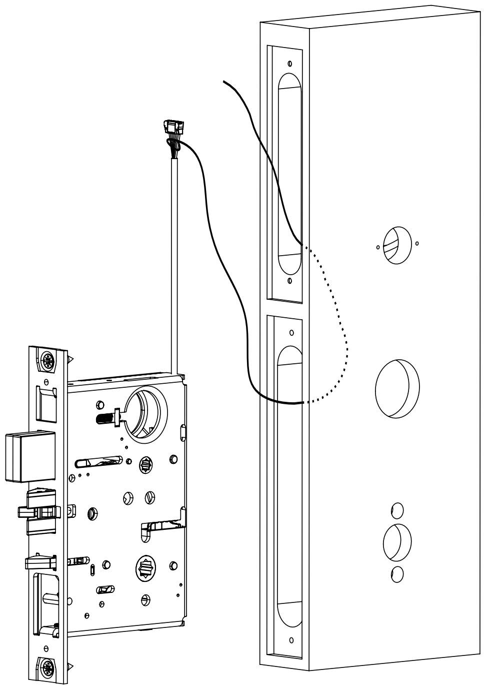
Before the mortise lock can be installed the lock cable needs to be threaded through from the lock cavity to the cartridge cavity. This cannot be done after the lock is installed.

1. Feed the lock cable in through the lock cavity and up through the cable hole into the cartridge cavity.

    It may be helpful to attach a semirigid wire to the lock cable connector plug and pull the lock cable up through the cable hole (see below).



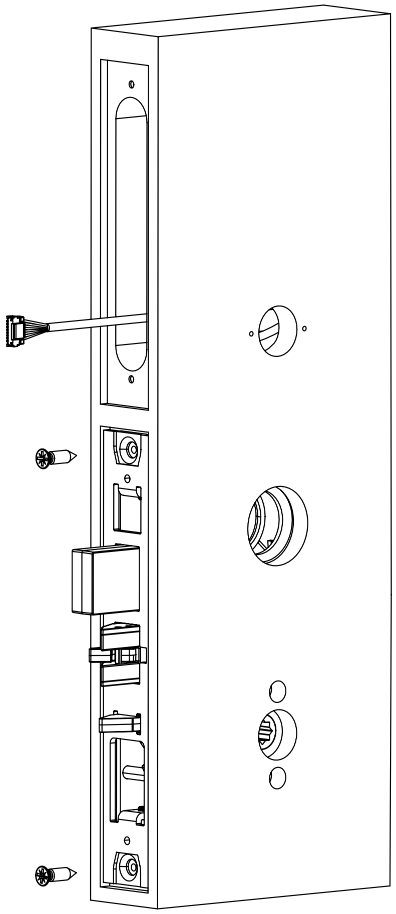
Pass the wire through the cable hole.



Attach the wire to the lock cable.

Secure the Lock

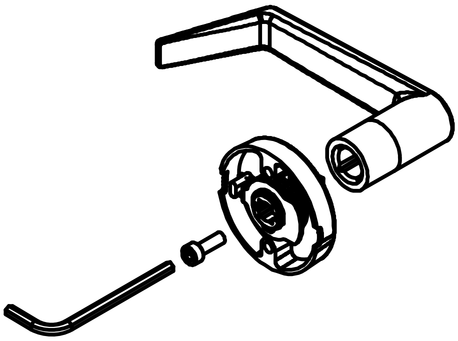
1. Insert the mortise lock cartridge into the lock cavity, ensuring the cable remains in position.
2. Using the two #12-24 combo screws provided, secure the lock body in position.



Fit the Handle and Sectional Trim

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

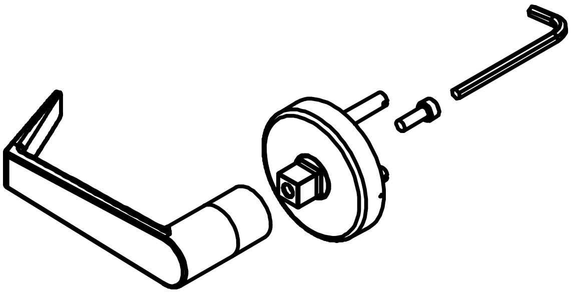
1. Assemble the outside rose.
   1. Fit the rose scalp cover onto the outside rose assembly by aligning the dimples with the slots in the rose plate. Secure by rotating clockwise until tight.
   2. Fit the handle onto the rose assembly spindle.
   3. Using the M5 x 0.8 x 14mm socket head cap screw and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



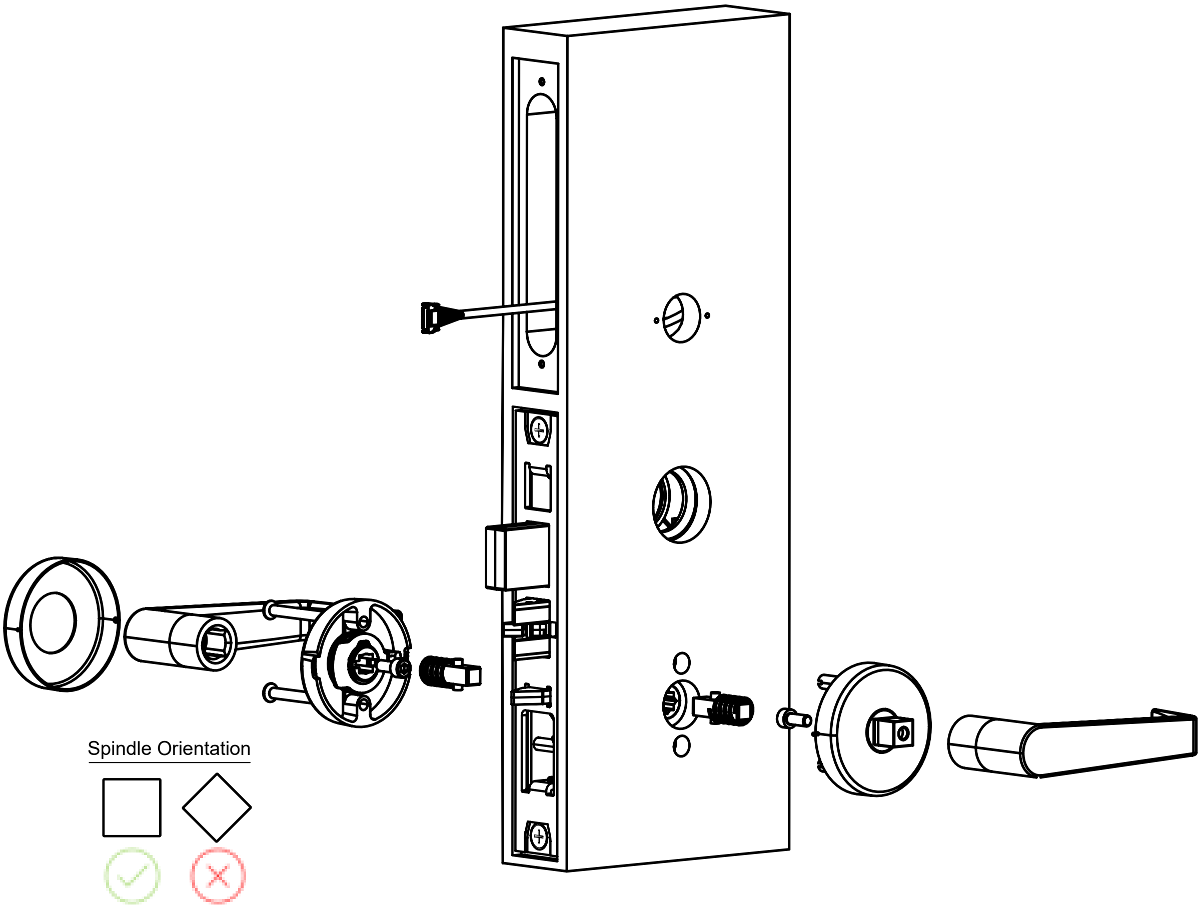
2. Assemble the inside rose.

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

   1. Fit the handle onto the rose assembly spindle.
   2. 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.



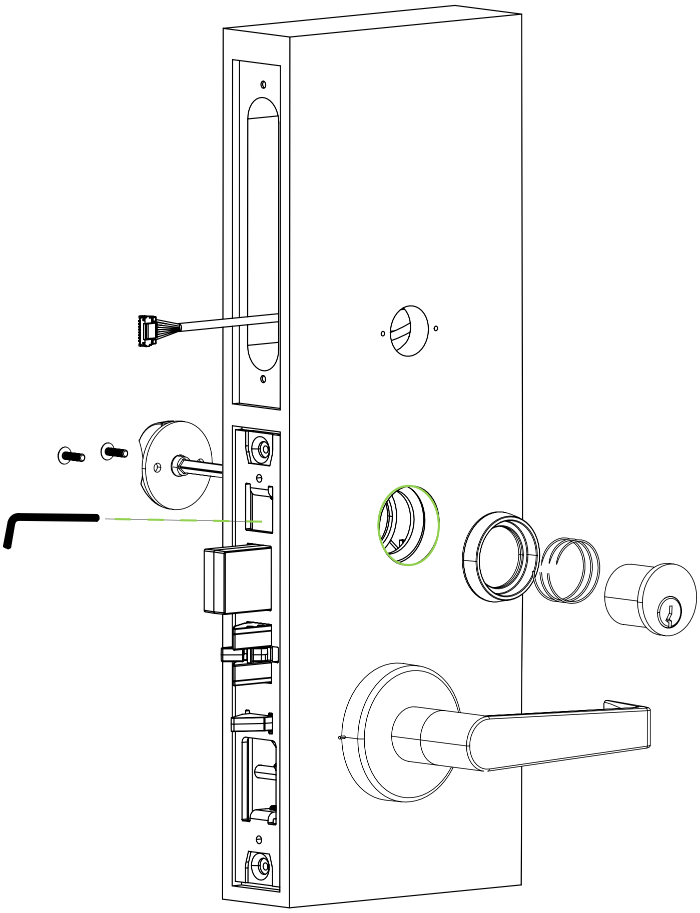
3. Install the spindles and springs on both sides, ensuring the correct **spindle orientation** (see above).
4. Install the outside assembly, aligning with the spindle. Confirm spindle engagement by rotating the lever down and verifying that the latch retracts.
5. Install the inside assembly, aligning with the spindle. Confirm spindle engagement.
   i. Using the #10-24 x 1-1/2" flat head machine screws provided, secure the inside rose assembly.
   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.

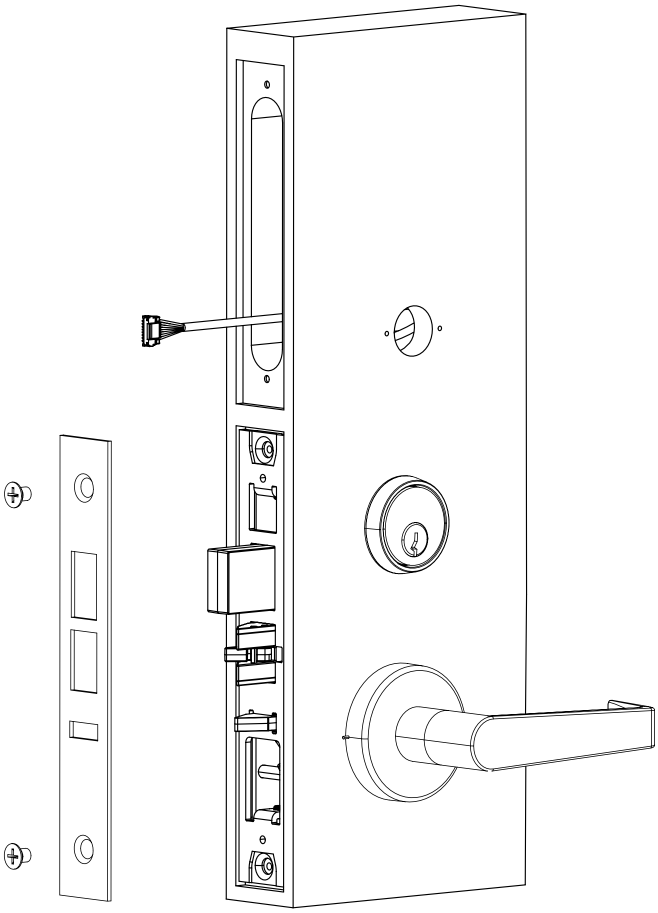
Ensure that the key cylinder is installed on the outside of the door with the thumbturn on the inside.

1. Thread the key cylinder into the lock body until the cylinder is flush or slightly recessed in the trim collar.
2. Using the 2.5mm hex key provided, through the front of the lock cartridge tighten the set screw on the side of the key cylinder to secure it in position.
3. Install the thumbturn. Secure using the two stainless steel #6 x 1/2" truss head sheet metal screws provided.



Installing the Faceplate

1. Using the two #8-32 x 1/4" flat head machine screws provided, install the faceplate.



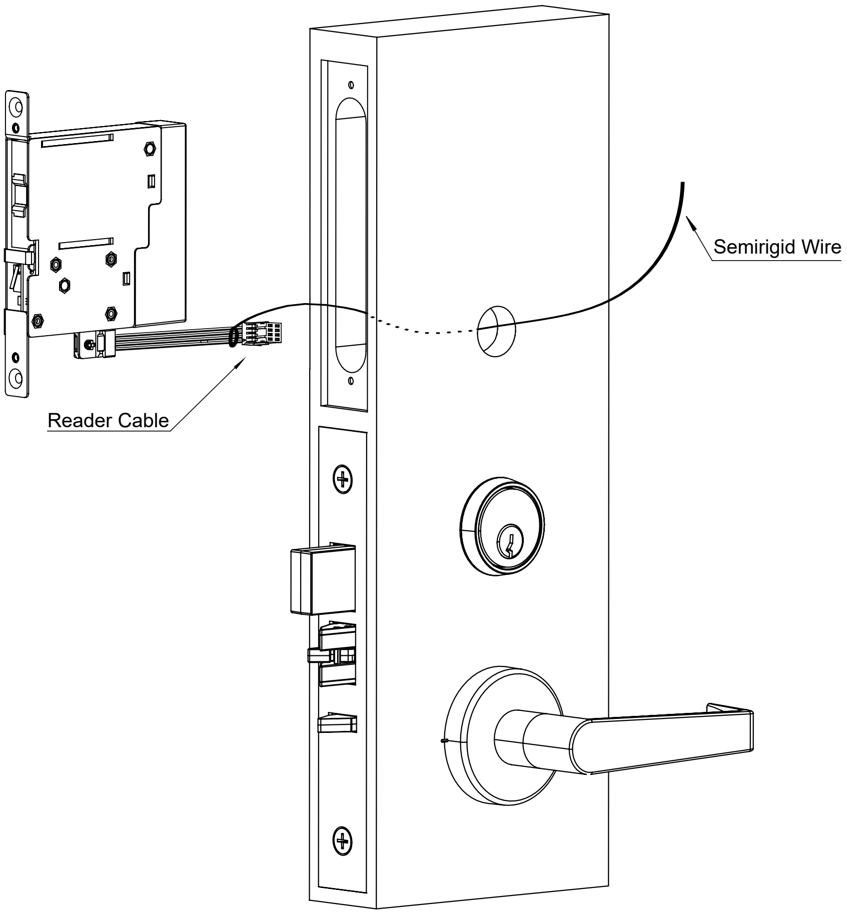
Installing the Lock Control Cartridge

Position the Reader Cable

Before the electronic control cartridge can be installed the attached reader cable needs to be secured from inside the cartridge cavity out through the reader hole using a semirigid wire.

While it may be possible to locate and pull the reader cable through the reader hole after installing the cartridge this will not be possible for some door configurations. Due to the short length of the reader cable and variable door conditions it is recommended to position the reader cable before inserting the cartridge.

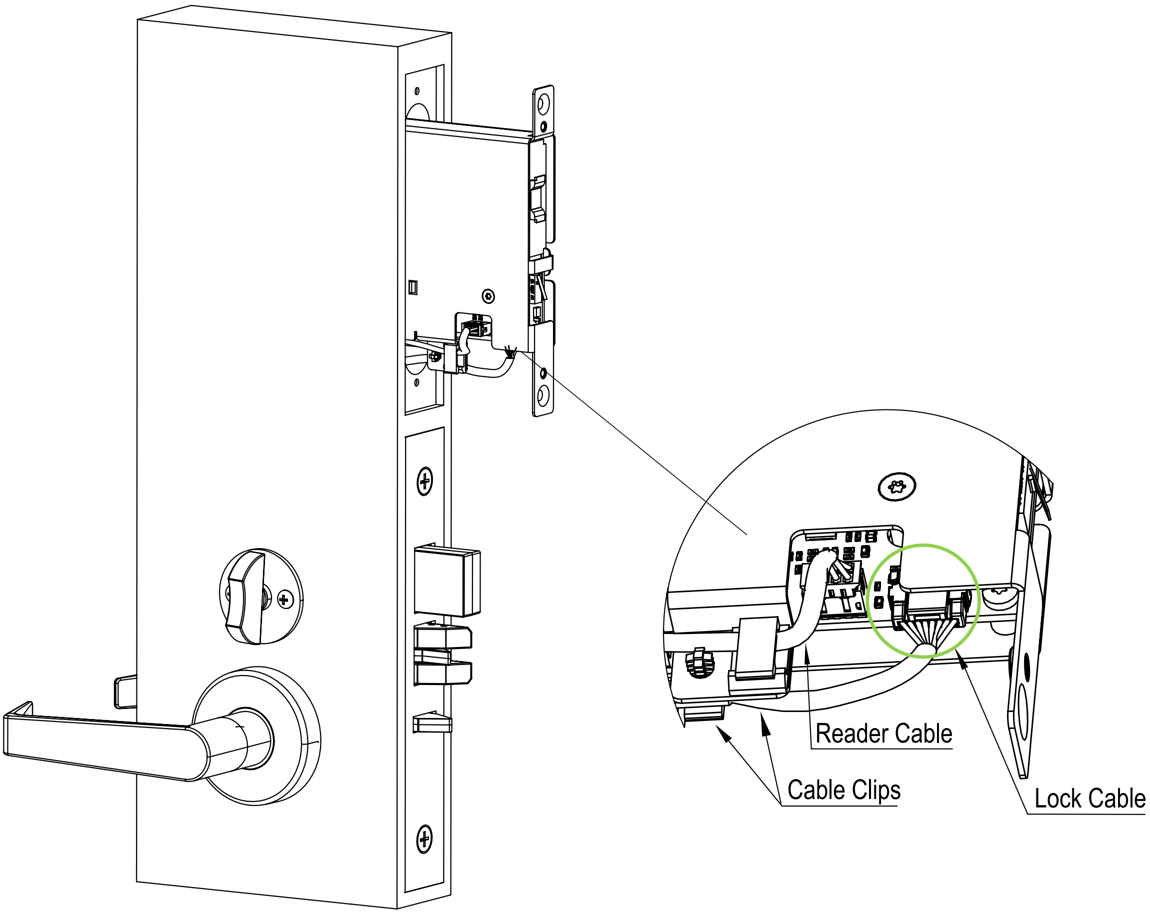
1. Attach a semirigid wire to the reader cable connector.
2. Feed the wire in through the cartridge cavity and out through the reader hole so that the reader cable can be pulled through after installing the cartridge.



Connect the Lock Cable

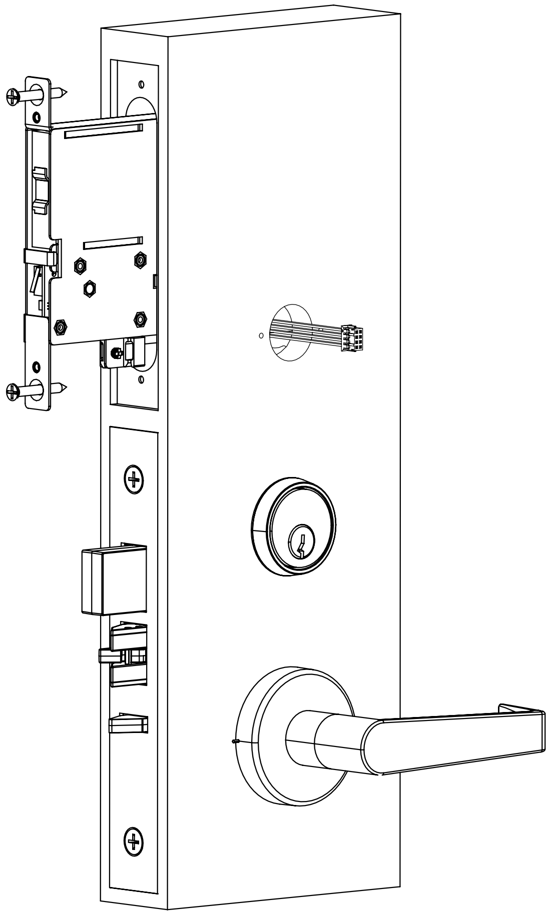
Before installing the cartridge the lock cable needs to be connected.

1. Connect the black lock cable socket plug to the black connector on the bottom of the cartridge.
2. Secure the lock cable to the spare cable clip on the underside of the cartridge.



Secure the Cartridge

1. Insert the lock control cartridge into the cartridge cavity.
2. Pull the reader cable through the reader hole.
3. Using the two G8 x 3/4" flat head screws provided, secure the cartridge in position.



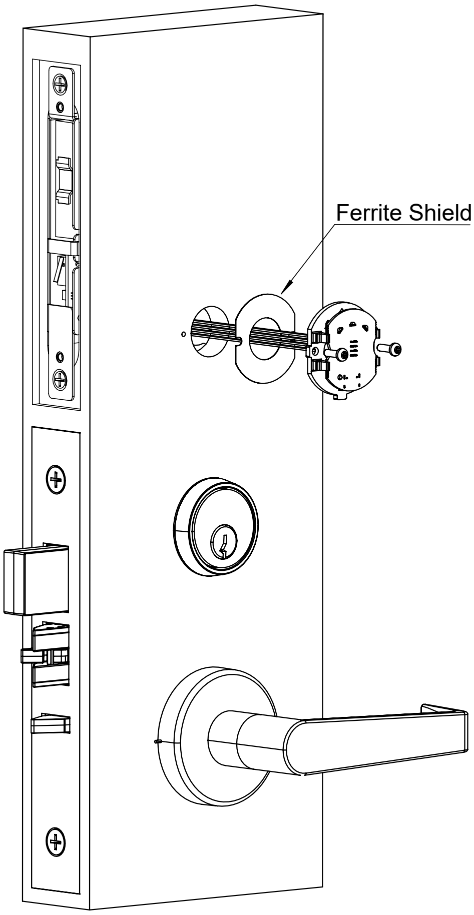
Installing the Reader

Connect the Reader

1. Using a small flat screwdriver, release the tab at the bottom of the reader to separate the reader cover from the base.
2. If mounting the reader on a metal surface it is recommended to place the optional ferrite shield (provided) onto the back side of the reader base.

   The shield is placed between the reader and the mounting surface to suppress electromagnetic interference caused by the reader's proximity to the metal surface.

3. Connect the reader cable plug to the connector on the back of the reader board.
4. Thread the other end of the reader cable through the hole in the door and out to the other side.

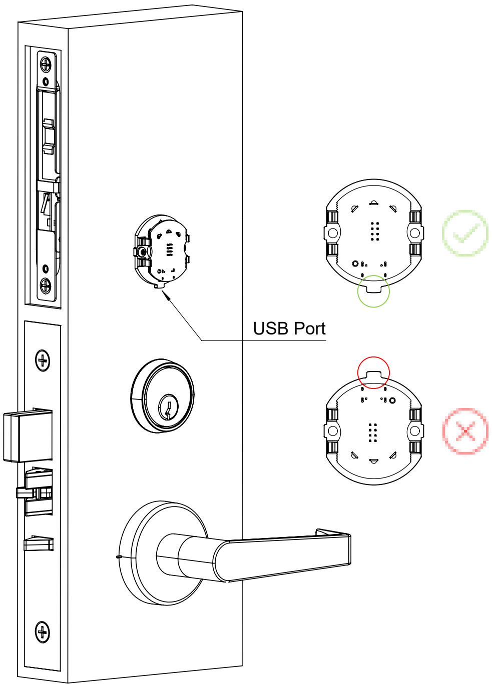


Attach the Reader

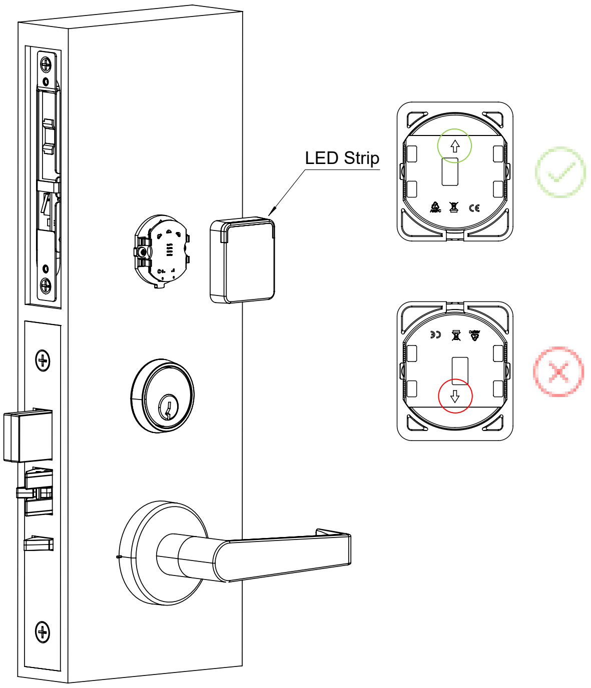
1. Position the reader onto the door, ensuring the USB port is at the bottom.
2. Using the two self-tapping N°4 9.5mm pan head screws provided, fasten the reader in position on the door.

   Do not use screws longer than 9.5mm to mount the reader.

3. Position the reader cover over the reader, with the LED strip at the top, and press firmly until the cover clips into position.



Attach the reader with the USB port at the bottom.



Attach the cover with the LED strip at the top.

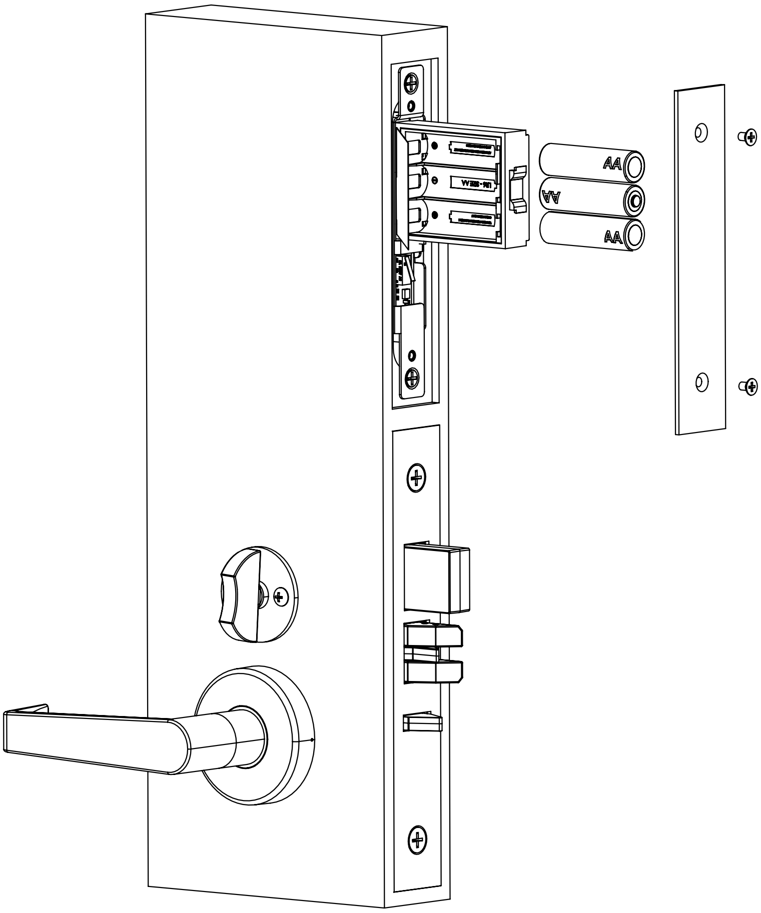
Either a rectangular or circular reader cover may be ordered. The process is the same for both covers.

It is not possible to detach the reader board from the base while it is firmly mounted in position. You will need to loosen or remove the mounting screws to allow the flex required to clip/unclip the board (e.g. for maintenance).

Inserting the Batteries

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

1. Remove the battery holder from the cartridge.
2. Lift the battery cover and insert the 3 x AA batteries provided.
3. Push the battery holder back into the cartridge.
4. Using the two M3.5 x 6mm Pozidriv machine screws provided, install the armor plate.



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

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

Approved batteries include Energizer Ultimate Lithium and Energizer MAX Alkaline.

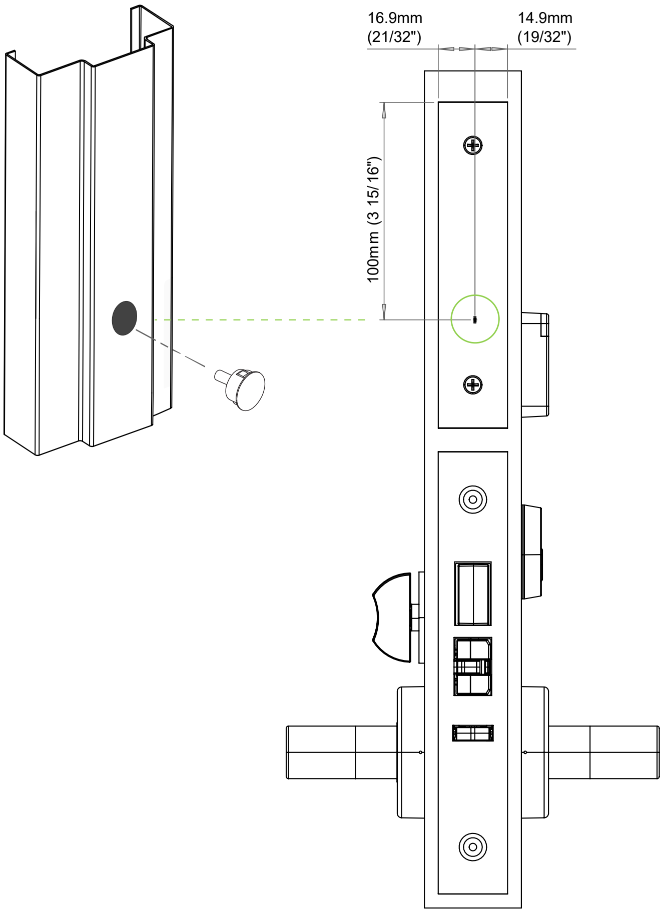
Installing the DPS Magnet

This step applies to the Mortise Electronic Cartridge & Reader with Door Position Sensor (CME-DFBT-DPS) only.

For electronic cartridge models which have a DPS (Door Position Sensor) included, the accompanying magnet needs to be installed in the door jamb as directly opposite the sensor as practical.

There is no need to install or connect the sensor itself as it is preinstalled in the electronic lock control cartridge.

The sensor is positioned 100mm from the top of the cartridge armor plate. Note that it is slightly off-center to the reader side, although this difference is negligible in door position operation. The sensor has an operating range of approximately 12mm from the armor plate to the magnet before contact is broken.



Bluetooth® Node Connection

Online operation is achieved using a Bluetooth® communication node, wired to the controller's RS-485 port to act as a network connection point between the wireless lock and the controller.

One Bluetooth® node supports up to 20 wireless locks operating in online mode.

Using the recommended cables, splice the cable together with the pigtail of the Bluetooth® node and seal the splice. Route the cable from the node 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:

- Belden 9842 or equivalent
- 24 AWG twisted pair with characteristic impedance of 120ohm

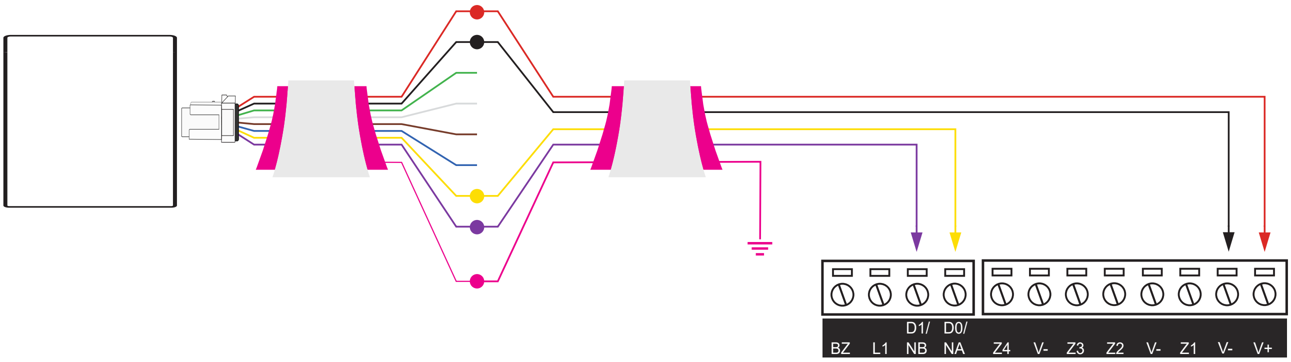
Maximum distance: 900m (3000ft)

For UL installations, a UL Listed (UL 294) node and controller must be used.

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

RS-485 Node Connection

The connection of a Bluetooth® communication node to a controller.



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

Important:

- The node 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 node pigtail shield and cable shield wires should be joined at the node pigtail splice.
- Do not terminate the node shield wire inside the node.

Programming the Reader

ICT credential readers can be programmed for a wide range of functionality to suit your site's requirements.

Programming options are dependent on hardware compatibility and firmware versions.

Readers can be programmed using a mobile device running the Protege Config App. Reader configuration is programmed by applying specific TLV (Type Length Value) settings to the reader to enable, disable and configure reader options.

Important: Readers can only be programmed within 2 minutes of startup. You will need to remove the batteries to disconnect the power supply, then apply the programming within 2 minutes of powering up.

Protege Config App

The Protege Config App provides a secure, convenient and flexible method for programming ICT credential readers.

To use the Config App you will need:

- An app account
- A mobile credential

Programming Summary

To program a reader using the Config App:

1. Log in to the app using your app account.
2. Select your **Credential Profile**.

   Your credential profile is automatically assigned to your app account with your mobile credential, and is based on the credential issuer and the site the credential was allocated to.

3. Create a **Reader Configuration** (config) comprising the required TLV settings.
4. Activate Bluetooth® on your device (if not already activated).
5. Power cycle the reader you want to program.
6. Select the **config** to program the reader with.
7. Apply the configuration to the reader, within two minutes of startup. Hold your mobile device close to the reader and tap **Scan Closest** to apply the configuration.

When programming is successful the reader will beep 4 times quickly, then restart.

For information on using the Config App, see the Protege Config App User Guide, available from the ICT website.

Operation

ICT 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)	

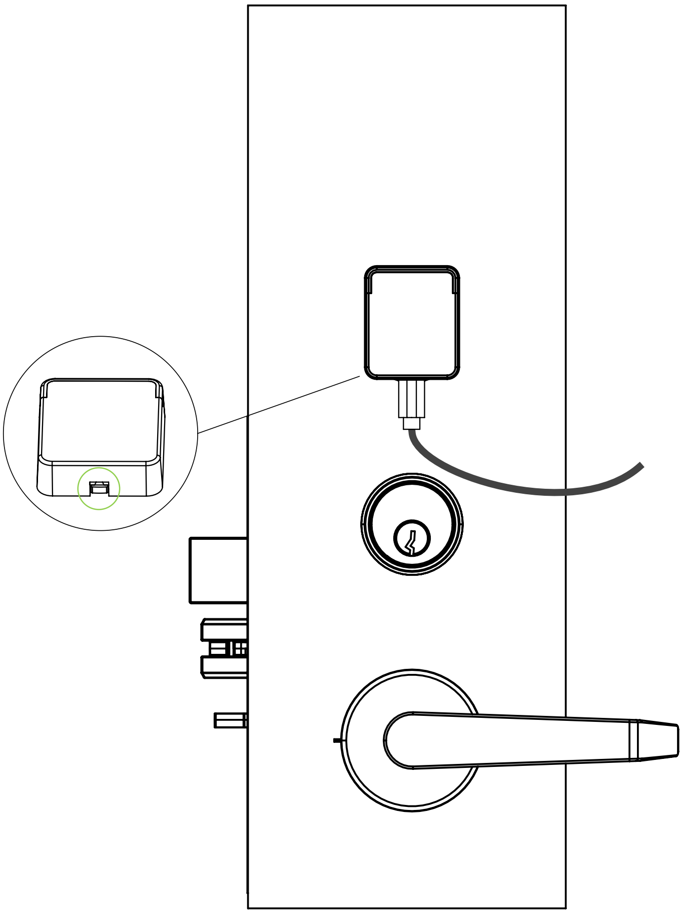
Maintenance

ICT cartridge mortise wireless locks have an expected battery life of approximately 2 years (40,000 activations), dependent on usage levels and reader configuration.

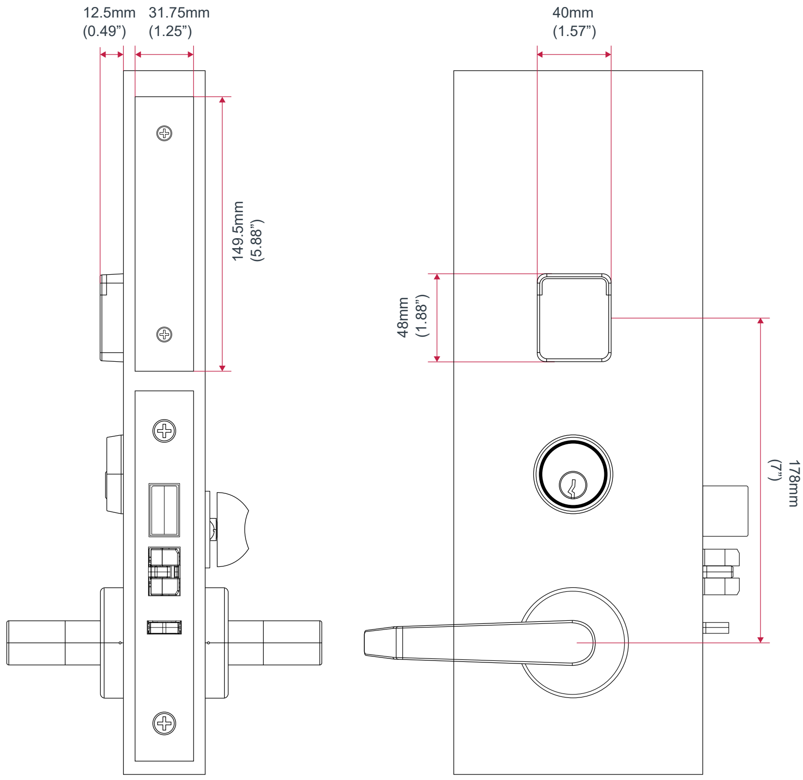
- Maximum 140,000 activation cycles with MIFARE/DESFire or NFC credentials
- Maximum 180,000 activation cycles with Bluetooth® Wireless Technology credentials

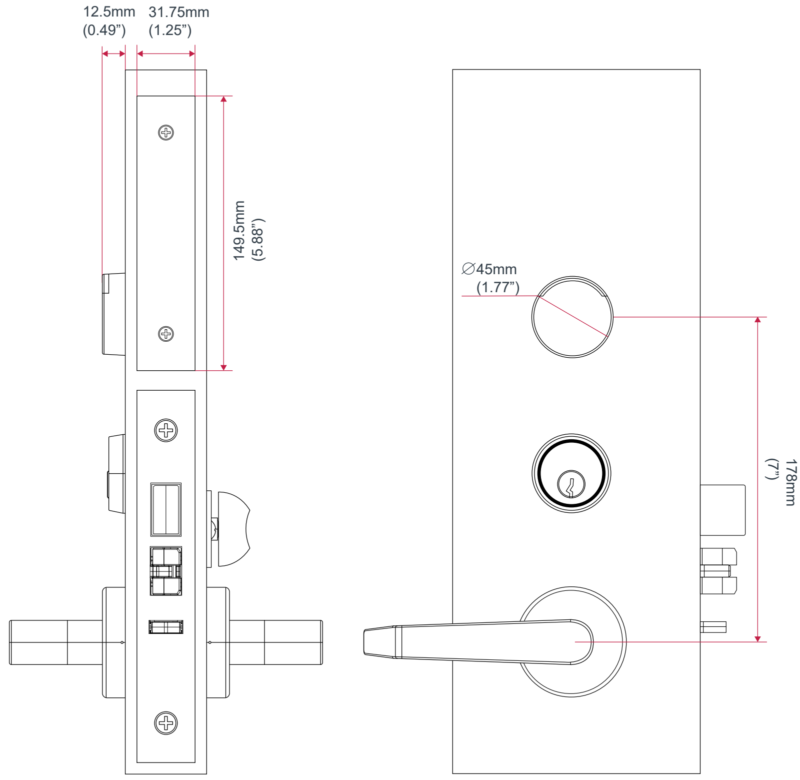
Batteries should be replaced every two years, or earlier if required.

In case of battery failure, emergency power can be supplied via the USB-C port at the base of the reader.



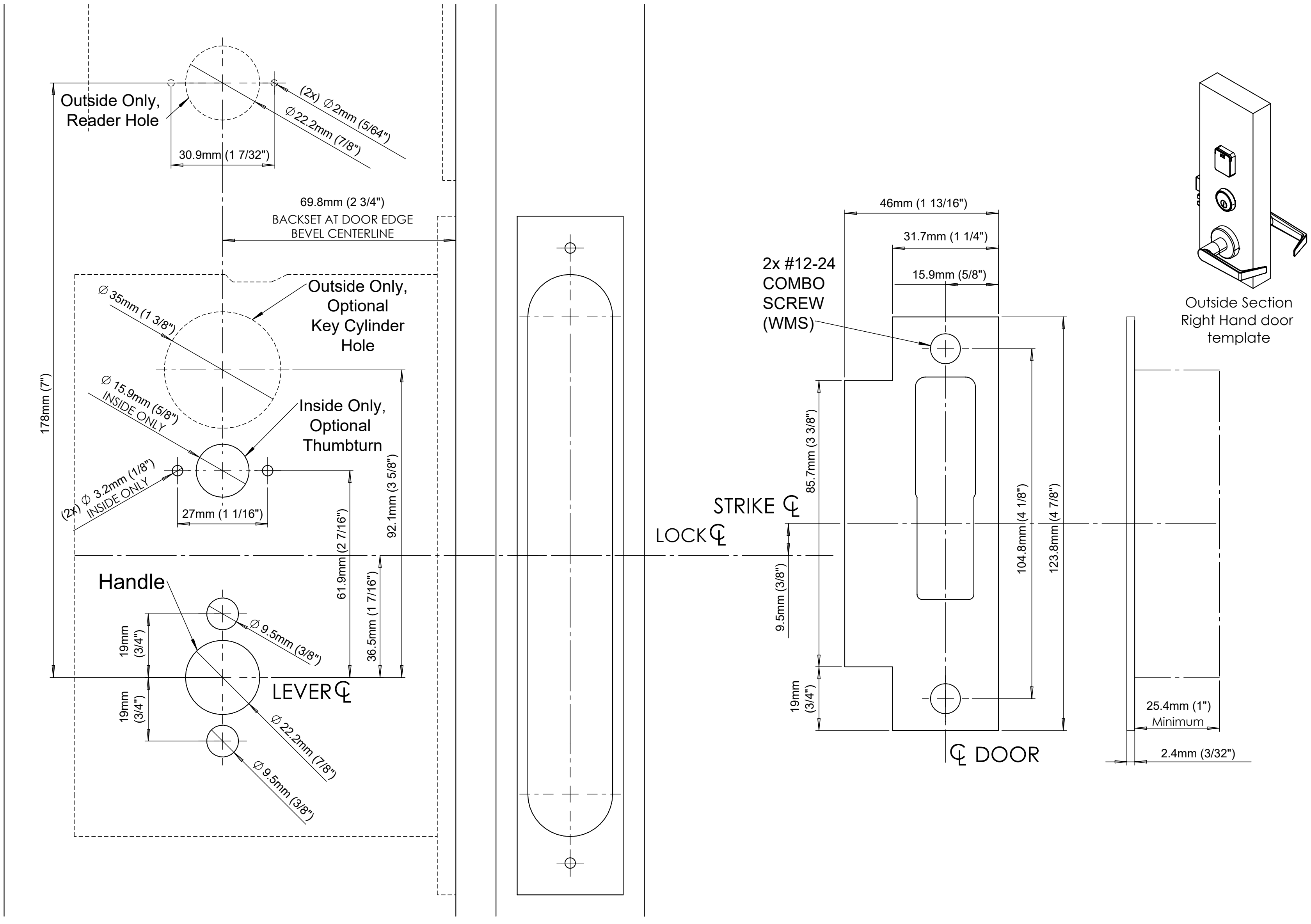
Mechanical Layout



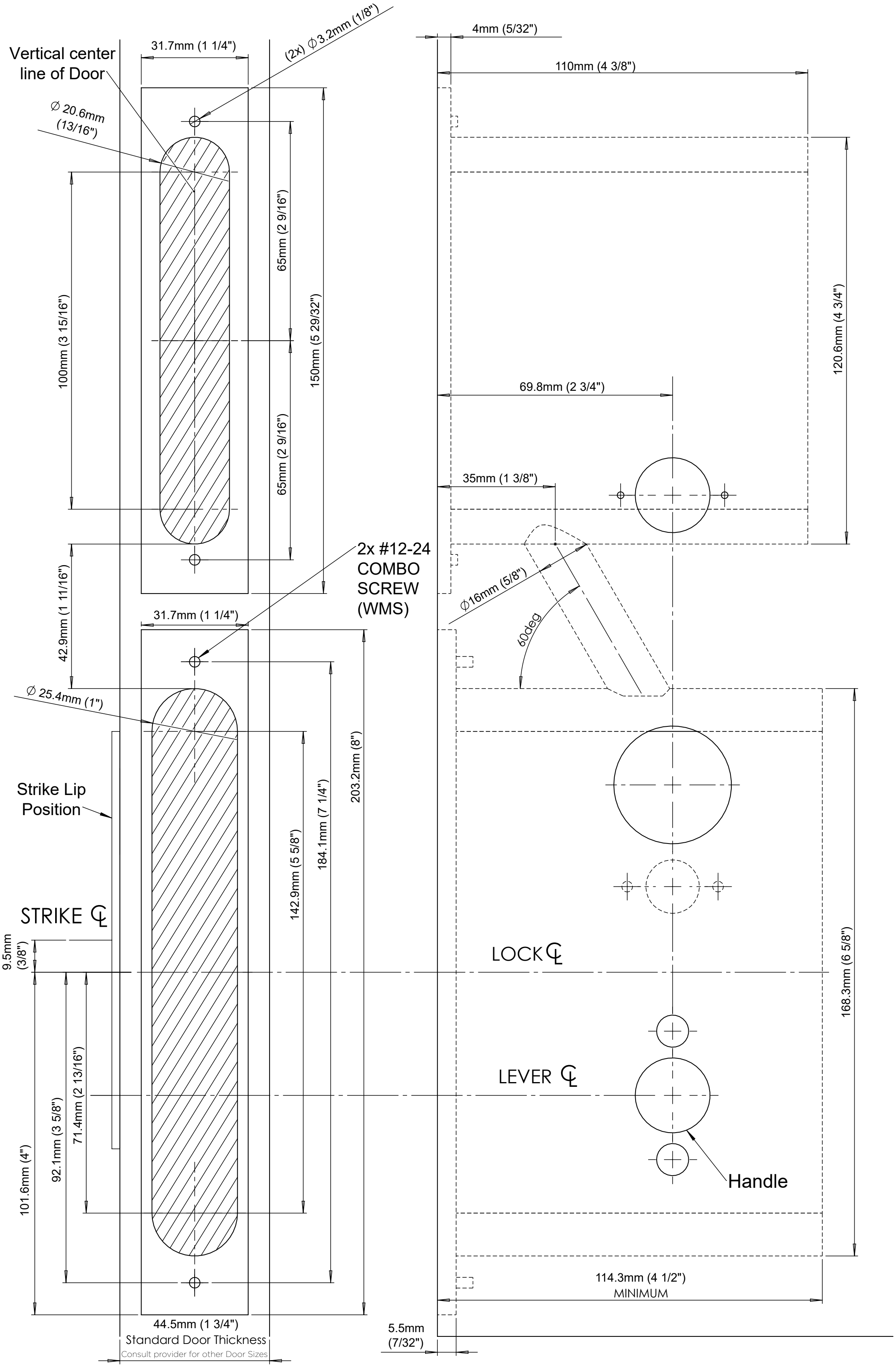


Door Template

May not be to scale.



Outside Section
Right Hand door
template


Vertical center line of Door
31.7mm (1 1/4")
(2x) ∅3.2mm (1/8")
4mm (5/32")
110mm (4 3/8")
∅ 20.6mm (13/16")
100mm (3 15/16")
65mm (2 9/16")
150mm (5 29/32")
65mm (2 9/16")
120.6mm (4 3/4")
69.8mm (2 3/4")
35mm (1 3/8")
42.9mm (1 11/16")
2x #12-24 COMBO SCREW (WMS)
∅16mm (5/8")
60deg
31.7mm (1 1/4")
∅ 25.4mm (1")
203.2mm (8")
184.1mm (7 1/4")
142.9mm (5 5/8")
Strike Lip Position
STRIKE ℄
9.5mm (3/8")
LOCK℄
168.3mm (6 5/8")
LEVER ℄
71.4mm (2 13/16")
92.1mm (3 5/8")
101.6mm (4")
Handle
114.3mm (4 1/2") MINIMUM
44.5mm (1 3/4")
Standard Door Thickness
Consult provider for other Door Sizes
5.5mm (7/32")

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 LR06 - AA 1.5V (x3)	
Expected Battery Life	2 years	40,000 activation cycles
	Maximum 140,000 activation cycles with MIFARE/DESFire	
	Maximum 180,000 activation cycles with Bluetooth® mobile	
Emergency Power Supply	USB-C connection allows power supply for emergency opening	
Operating Voltage	3.3 – 6V	
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	
Dimensions		
Reader Cover	Circular (OD x D)	Ø 45 x 12.5mm (Ø 1.77 x 0.49")
	Rectangular (H x W x D)	48 x 40 x 12.5mm (1.89 x 1.57 x 0.74")
Control Cartridge (H x W x D)	95 x 42.8 x 18.9mm (3.74 x 1.69 x 0.49")	
Armor Plate (H x W)	150 x 31.7mm (5.9 x 1.25”)	
Net Weight	310g (10.9oz)	
Gross Weight	TBC	
Operating Conditions		
Operating Temperature	UL/ULC 0° to 55°C (32° to 131°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)
Lock Specification	
Lock Type	Grade 1 mortise lock
Net Weight	TBC
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
Default Keyway	Schlage C Compatible (SCC). Other options available on request
Default Keying	Keyed Different (KD). Other options available on request
Handle Rotation	35 degrees
Door Thickness	44.45 to 50.8mm (1.75 to 2”) standard. Larger thickness by special order

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.

New Zealand and Australia

Intentional Transmitter Product Statement

The R-NZ compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

R-NZ

European Standards

CE Statement CE

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency magnetic field immunity tests (EN 61000-4-8)

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

UL and ULC Installation Requirements

Only UL / ULC listed compatible products are intended to be connected to a UL / ULC 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.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-60839-11-1 Listed portal locking device(s) for ULC installations.
- Input power must be supplied by a Class 2 or power limited device.

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.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 Listed electronic locks for UL installations.
- Input power must be supplied by a Class 2 or power limited device.
- 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.)

UL 10C

- This lock is rated in Positive Pressure Fire Tests of Door Assemblies for resistance endurance of 3 hours.

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.

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

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.