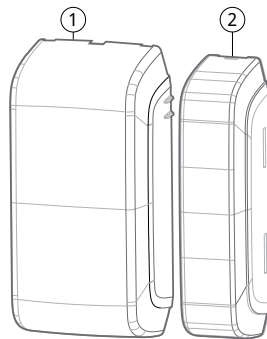


## Overview of the MC-312N NBIoT

The reference to MC-312N NBIoT throughout this manual includes the model MC-312N NBIoT.

**Figure 1: MC-312N NBIoT**



**Table 1: Device overview**

| Callout | Component |
|---------|-----------|
| 1       | Device    |
| 2       | Magnet    |

The MC-312 NBIoT is a wireless outdoor magnetic contact with an auxiliary input. This outdoor contact is an internet of things (IoT) device and works in narrowband (NB) IoT networks while connecting with data and device management (DM) servers.

The MC-312N NBIoT has a range of features, which include:

- Flat and curved surface installation
- Weatherproof and water-resistant IP66 outdoor transceiver
- Separate transmissions from sensor and auxiliary input that trigger the same cellular transmitter
- Battery life of up to 2 years with typical use
- Integrated magnetic sensor
- Anti-masking detection
- Auxiliary hardwired input, programmable as either normally open, normally closed, end of line or double end of line for use with an additional device
- Front and back tamper detection
- Paintable using non-metallic paint. Suggested paints include: DUPLI-COLOR Vinyl & Fabric Coating, RUST-OLEUM Plastic, KRYLON Fusion for Plastic
- Temperature level reports
- Bluetooth low energy (BLE) interface supporting the Installer and User Apps for local settings
- Over the air (OTA) and firmware over the air (FOTA) upgrade capability



- Power Save Mode (PSM)

## Getting Started

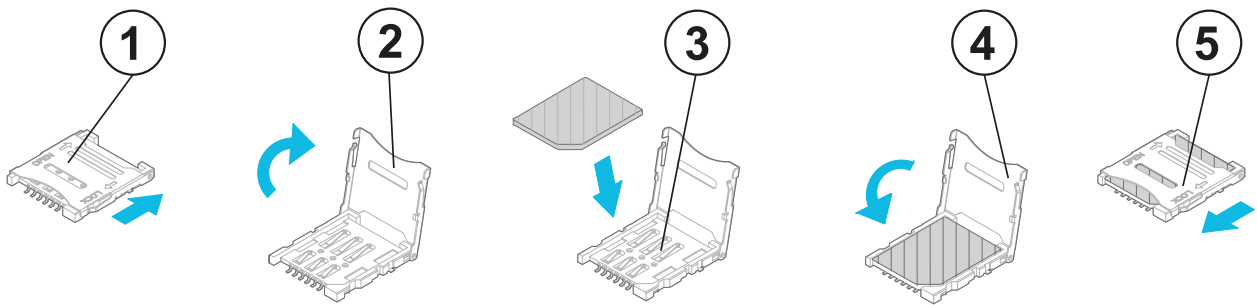
### Inserting the Micro SIM card

#### ► Important:

- In order to match the temperature range of the device, use an industrial grade IoT/ M2M Micro SIM card. For more information, see [Specifications](#).
- The Micro SIM card tray is located behind the batteries in the device. Before inserting the Micro SIM card you must remove the batteries. For more information, see [Inserting or replacing the batteries](#)

1. Slide up the metal cover to the **OPEN** position.
2. Open the cover.
3. Place the Micro SIM card in the tray with the chip face down.
4. Close the metal cover.
5. Slide the cover back to the **LOCK** position.

**Figure 2: Inserting the Micro SIM card**



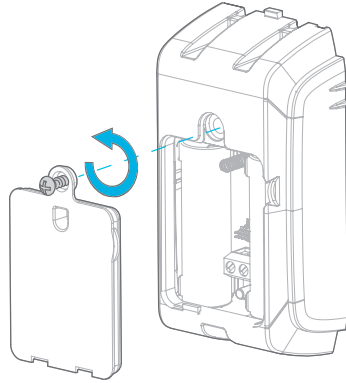
### Inserting or replacing the batteries

#### ⚠ WARNING:

- There is a risk of explosion if you replace the batteries with an incorrect type.
- Dispose of used batteries according to the battery manufacturer's instructions and according to local rules and regulations.

1. Insert a flat-head screwdriver into the slots provided and push upward to remove the decorative cover. See Figure 6
2. Unscrew the battery cover screw, then remove the battery cover. See Figure 3.

**Figure 3: Removing the battery cover**



3. To replace the batteries, remove the old batteries and wait one minute.
4. Insert the new batteries with the + and - symbols matching the illustration in the battery compartment.
5. Replace the battery cover and close the screw. Reattach the decorative cover. See Figure 4 .

**Figure 4: Replacing the battery cover**



## Enrolling the NB IoT device

- ❗ **Note:** Before enrolling the device you should perform a link quality test. For more information, see [Performing a link quality test](#)

For the device to operate as expected you must enroll or register the device at the device manager (DM) server. To do so, complete the following steps:

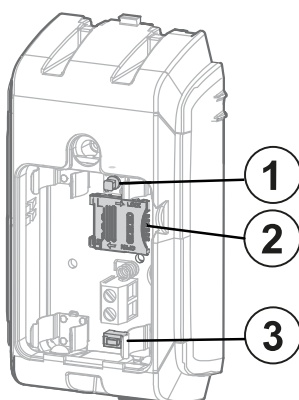
1. Insert the SIM card into the device. For more information, see Figure 2
2. Insert the batteries. For more information, see [Inserting or replacing the batteries](#)
3. Leave the battery cover open.
4. Follow the instruction on the application to enroll and register the device.

- ❗ **Note:** You can find your 15 digit IMEI number and PIN code printed on the box of the device when prompted by the application.

## Installation guidelines

- Only qualified service personnel can install the device.
- Place the device above the door or window on the fixed frame. Place the magnet on the movable part of the door or window. Do not place the magnet more than 44.5 mm or 1.75 in. from the marked side of the device.
- Mount the magnet either parallel or perpendicular to the device. For more information, see Figure 12 or Figure 13
- For devices with a back tamper, ensure the device is seated firmly within the bracket at all times and that the break-away bracket segment is fastened securely to the mounting surface. For more information, see callout 2 and callout 3 in Figure 7. For more information about tamper detection, see [Tamper detection](#)

**Figure 5: Device interior**



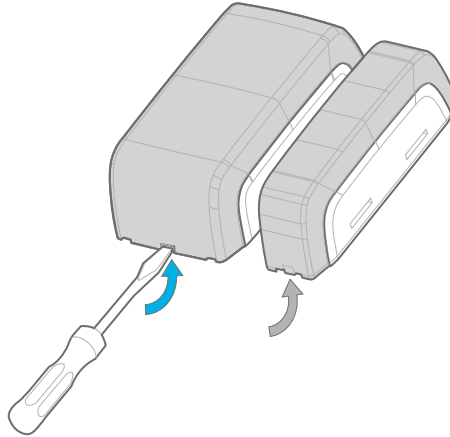
| Callout | Description                     |
|---------|---------------------------------|
| 1       | Front tamper switch             |
| 2       | Sim card holder                 |
| 3       | Anti-masking calibration button |

## Mounting the NBIoT device on a flat or curved surface

1. ⓘ **Note:** Align the device and magnet according to the specifications in [Range coverage directions](#).

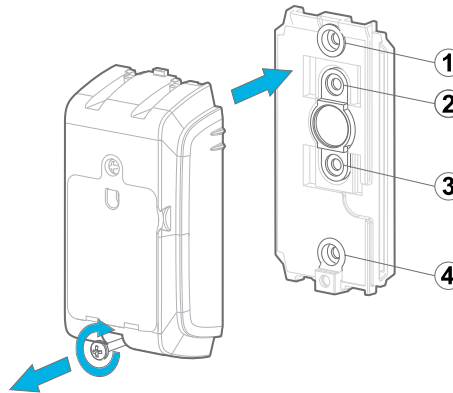
To remove the decorative cover, insert a flat-head screwdriver into the slot provided and push upward. See Figure 6

**Figure 6: Removing decorative cover**



2. Unscrew the lower screw from the device cover and separate the device from the bracket. See Figure 7

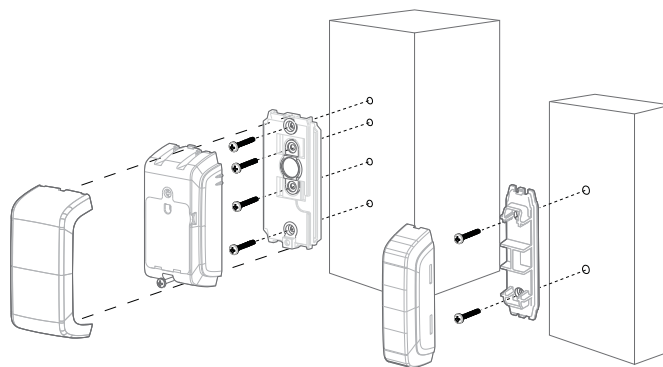
**Figure 7: Separating the device**



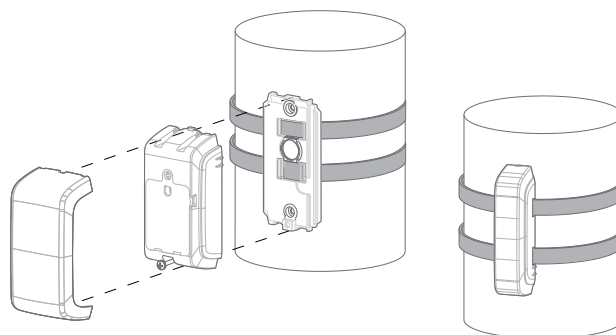
3. Mark, drill, and screw the required amount of holes in the mounting surface with one of the following options:
  - For tamper protection, use both middle holes. See Figure 8 and callout 2 and callout 3 in Figure 7.
  - For a standard mount, use the uppermost and lowermost hole in the device bracket only. See Figure 8 and callouts 1 and 4 in Figure 7.
  - To mount the device impermanently on a curved surface, insert the straps through the slots in the device and magnet brackets. Fasten both straps to the curved surfaces. See Figure 9

❗ **Note:** Straps are not included with the product.

**Figure 8: Flat surface mounting**



**Figure 9: Curved surface mounting**

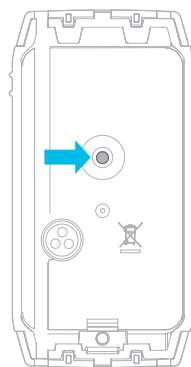


4. Reattach the device to the bracket and close the cover screw. Close the decorative cover. See Figure 8.
  5. Mount the magnet base to an adjacent surface with the two supplied screws and attach the magnet to the magnet bracket. See Figure 8.
- ❗ **Note:** The magnet can be mounted parallel or perpendicular to the device. Ensure that the magnet and device sensor markings align, depending on the magnet orientation. For more information, see Figure 12 or Figure 13.

## Tamper detection

The device is tamper protected front and back. The front tamper switch of the device activates when the cover is removed. The unit also has a back-tamper switch under the PCB. As long as the PCB is seated firmly within the base, the switch lever will be pressed against a special break-away base segment that is loosely connected to the base. Any unauthorized tampering with these items will result in an alarm.

**Figure 10: Back tamper**



Tamper detection includes the following features:

- Tamper alarm report when the cover is removed. For more information, see Figure 5
- Tamper alarm report when the back tamper is opened
- Tamper restore message when you close the front cover and back tamper

# Advanced settings

## Anti-Mask guidelines

- The anti-mask (AM) feature detects sabotage attempts, such as magnetic tampering.
- Complete the anti-mask learning process only after the enrollment process. Ensure that the device and the magnet are in the final installation position. This must be the shortest distance between the magnet and the device.
  - ❗ **Note:** For more information on the enrollment process, see [Enrolling the NBIoT device](#).
- To receive an alert when something interferes with the magnet, set the anti-mask configuration to **Enable**.
- Keep any additional magnets away from the device during the calibration process. A screw driver with a magnetic tip can also interfere.

For more information see [Calibrating the anti-mask](#)

## Calibrating the anti-mask

1. Position the device and magnet pointers to face each other, as shown in Figure 12 or Figure 13.
2. Ensure that the device and magnet are placed no more than 5 mm or 0.2 in. apart on the Z plane. See Figure 12 or Figure 13
3. Press and hold the anti-masking calibration button for 6 to 8 seconds to start the anti-mask learning process. Do not release the anti-masking calibration button while the yellow LED is lit. Release the button after the green LED lights at 6 seconds and before 8 seconds. If successful, the green LED flashes three times. If unsuccessful, the red LED flashes three times.
4. During the anti-mask learning process, the sensor and the magnet must be stable for 10 seconds. If the door is open while you press the anti-masking calibration button, the anti-mask learning process is ignored.

## Performing a link quality test

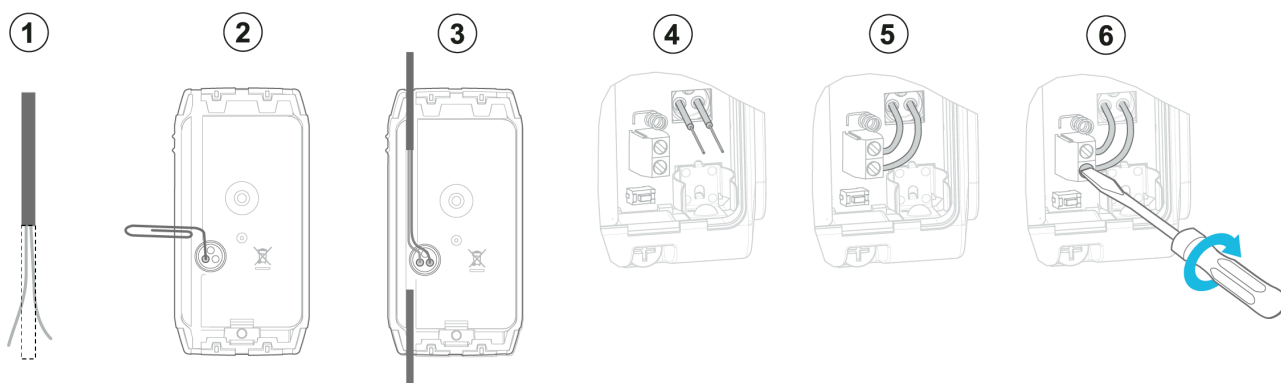
You should perform this test before enrolling to ensure the device is in an optimum position. To perform the link quality test, follow these steps:

1. Insert the SIM card. For more information, see [Inserting the Micro SIM card](#)
2. Insert the batteries. For more information, see [Inserting or replacing the batteries](#)
3. Leave the battery cover open.
4. Open the user application.
  - ❗ **Note:** You can find the 15-digit IMEI number and pin code on the box of the device when prompted by the application.
5. The application can report the link quality as **Strong, Good, Fair, or Poor**.
  - ❗ **Note:** A strong or good link quality is required for UL installations.

## Wiring the auxiliary input

① **Note:** To see more information about possible wiring options, see [Auxiliary wiring options](#)

1. Remove the jacket at the end of the cable to expose the wires within.
2. Perforate the silicon gasket at the back of the NBIoT device with a 0.8 mm. or 0.03 in. pin.
3. Pass each wire through an entry hole and out the opposite side.
4. Remove the insulation from the end of each wire.
5. Connect each wire to the relevant terminal, referencing Auxiliary wiring options.
6. Screw the terminal closed using a flat head screwdriver.

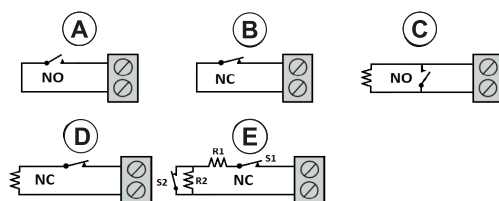


## Auxiliary wiring options

Add more devices to the circuit for normally closed (NC), normally open (NO), end of line (EOL), or double end of line (DEOL) applications. For more information regarding each application type, see the following definition list:

- **NC:** Use only series connected NC sensor contacts if the auxiliary input of the detector is defined as a normally closed type. An EOL resistor is not required. See callout B in Figure 11.
- **NO:** Use only parallel connected NO sensor contacts if the auxiliary input of the detector is defined as a normally open type. An EOL resistor is not required. See callout A in Figure 11.
- **EOL:** For EOL supervision, use NC or NO sensor contacts. A 5.6 k $\Omega$  EOL resistor must be wired at the far end of the zone loop. See callout C and callout D in Figure 11.
- **DEOL:** For DEOL supervision, use NC sensor contacts only. Two 5.6 k $\Omega$  EOL resistors must be wired at the far end of the zone loop. For more information, see callout E in Figure 11 .

**Figure 11: Alarm circuit options with E.O.L. resistors**



| Callout | Description                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------|
| A       | NO switch                                                                                              |
| B       | NC switch                                                                                              |
| C       | EOL: NO switch; 5.6 k $\Omega$ resistor                                                                |
| D       | EOL: NC switch; 5.6 k $\Omega$ resistor                                                                |
| E       | DEOL: NC switch only;<br>R1=5.6 k $\Omega$ resistor; S1=tamper<br>R2=5.6 k $\Omega$ resistor; S2=Alarm |

## Range coverage directions

Depending on what type of surface you mount the device and magnet, there are optimum ranges. When you mount the device and magnet on a slide door, refer to X. When you mount the device and magnet on a roller shutter, refer to Y. When you mount the device and magnet on a normal door, refer to Z. For more information, see Table 2 and Figure 12 or Figure 13.

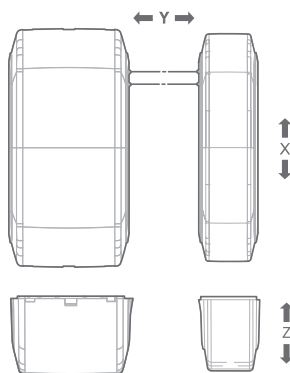
**Table 2: Range coverage directions**

| Axes   | Non-metallic surface |                   | Metallic surface  |                   |
|--------|----------------------|-------------------|-------------------|-------------------|
|        | Open                 | Close             | Open              | Close             |
| X up   | 40 mm or 1.6 in.     | 33 mm or 1.3 in.  | 32 mm or 1.26 in. | 25 mm or 0.98 in. |
| X down | 22 mm or 0.9 in.     | 17 mm or 0.67 in. | 17 mm or 0.67 in. | 8 mm or 0.3 in.   |
| Y      | 71 mm or 2.8 in.     | 52 mm or 2 in.    | 48 mm or 1.89 in. | 35 mm or 1.38 in. |
| Z      | 85 mm or 3.35 in.    | 55 mm or 2.17 in. | 55 mm or 2.17 in. | 30 mm or 1.2 in.  |

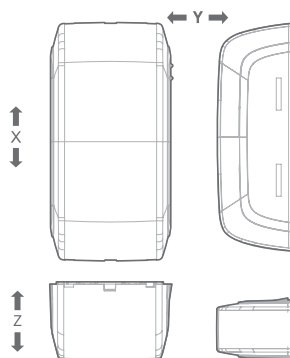
**Note:** The values stated may vary by up to 10%. For steel installations, the gaps cannot be less than 3.2 mm or 0.126 in.

**Note:** X up refers to the upper half of the X plane and X down refers to the bottom half of the device on the X plane. See Figure 12, and Figure 13.

**Figure 12: Parallel range coverage directions**



**Figure 13: Range coverage directions with perpendicular magnet**



## Configuring the NBIoT device

To configure the NBIoT device settings, open the AlarmInstall application and see the options in the following definition list:

- To set the auxiliary input, select one of the following options: **Normally open**, **Normally closed**, **End of line**, **Double end of line** or **Disabled**. The default setting is **Disabled**. For more information, see [Auxiliary wiring options](#)
- **Anti-mask:** To enable anti-mask protection, select **Enabled**. To disable anti-mask protection, select **Disabled**. The default setting is **Disabled**.

**Note:** The installer can configure locally through the BLE interface or remotely using the DM Server. Remote configuration is delivered to the NBIoT device when it is in wake up mode.

## Managing the Bluetooth low energy interface

1. To activate the Bluetooth low energy (BLE) interface insert the batteries. The BLE then activates for an initial 3 mins.
  2. Ensure the tamper is open. The BLE remains active while the tamper is open.
  3. The BLE interface disables when you close the tamper and there is no active BLE session.
- Note:** If the device does not appear in a scanner search, remove and reinsert the batteries and ensure the tamper is open to reactive the BLE.

## Specifications

|                                     |                                                                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Frequency Band (MHz)                | 4G Bands: B1, B2, B3, B4, B5, B8, B12, B13, B18, B19, B20, B25, B26, B27, B28, B66, B71, B85<br>BLE: 2.4 to 2.5 GHz |
| SIM card type                       | Industrial grade IoT/M2M Micro SIM (3FF)                                                                            |
| Maximum Tx Power                    | LTE: 21 dBm (Power Class 5)<br><br>BLE: 5dBm                                                                        |
| Alarm input                         | One internal and one auxiliary                                                                                      |
| Communication protocol              | LwM2M                                                                                                               |
| Battery type                        | 2 x AA Ultimate Lithium Energizer battery only                                                                      |
| Battery life expectancy             | Up to 2 years with typical use                                                                                      |
| Low battery threshold               | 3.0V *<br>* Dependant on temperature. From -10°C to 66°C the threshold is 3.05V                                     |
| Battery supervision                 | Every 24 hours                                                                                                      |
| Operating Temperature               | -40°C to 66°C or -40°F to 151°F                                                                                     |
| Color                               | Dark gray                                                                                                           |
| Relative Humidity (RH)              | Average relative humidity of approximately 75% non-condensing.                                                      |
| Dimensions (LxWxD)                  | 105 mm x 52 mm x 35 mm (4.1 in. x 2 in. x 1.4 in.)                                                                  |
| Device weight (including batteries) | 154 g or 5.4 oz                                                                                                     |

## Device limitations

DSC wireless systems are very reliable and are tested to high standards. However, the device can be installed in a place with bad LTE communication. Bad RSSI signal causes the network connection to become unstable which can cause significant delay in sending alarms or alerts.

- Receivers may be blocked by radio signals occurring on or near their operating frequencies, regardless of the digital code used.
- A receiver responds only to one transmitted signal at a time.
- Wireless devices should be tested regularly to determine if there are sources of interference and to protect against faults.

## Compliance with standards

MC-312N NB IoT complies with the following standards:

|                       |                                                                               |
|-----------------------|-------------------------------------------------------------------------------|
| <b>MC-312N NB IoT</b> | <b>USA: FCC (915 MHz):</b> CFR 47 part 15, 22/24<br><b>Canada:</b> IC-RSS-247 |
|-----------------------|-------------------------------------------------------------------------------|

① **Note:** 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.

Cet équipement a été testé et jugé conforme aux limites s'appliquant à un appareil numérique de classe B, conformément à la Partie 15 des réglementations de la FCC. Ces limites ont été élaborées pour offrir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle.

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

⚠ **WARNING:** Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules and with ISSED license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

To comply with FCC and IC RF exposure compliance requirements, the device should be located at a distance of at least 20 cm from all persons during normal operation. The antennas used for this product must not be co-located or operated in conjunction with any other antenna or transmitter.

Le dispositif doit être placé à une distance d'au moins 20 cm à partir de toutes les personnes au cours de son fonctionnement normal. Les antennes utilisées pour ce produit ne doivent pas être situées ou exploitées conjointement avec une autre antenne ou transmetteur.

## Limited Warranty

Digital Security Controls warrants that for a period of 12 months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use and that in fulfillment of any breach of such warranty, Digital Security Controls shall, at its option, repair or replace the defective equipment upon return of the equipment to its repair depot. This warranty applies only to defects in parts and workmanship and not to damage incurred in shipping or handling, or damage due to causes beyond the control of Digital Security Controls such as lightning, excessive voltage, mechanical shock, water damage, or damage arising out of abuse, alteration or improper application of the equipment.

The foregoing warranty shall apply only to the original buyer, and is and shall be in lieu of any and all other warranties, whether expressed or implied and of all other obligations or liabilities on the

part of Digital Security Controls. Digital Security Controls neither assumes responsibility for, nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

In no event shall Digital Security Controls be liable for any direct, indirect or consequential damages, loss of anticipated profits, loss of time or any other losses incurred by the buyer in connection with the purchase, installation or operation or failure of this product.

**Warning:** *Digital Security Controls recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.*

**Important Information:** *Changes or modifications not expressly approved by Digital Security Controls could void the user's authority to operate this equipment.*

EMAIL: [info@dsc.com](mailto:info@dsc.com)

INTERNET: [www.dsc.com](http://www.dsc.com)

©2022 Johnson Controls. All rights reserved. JOHNSON CONTROLS, TYCO and DSC are trademarks and/or registered trademarks. Unauthorized use is strictly prohibited.

D-308924 Rev.00 05/22

