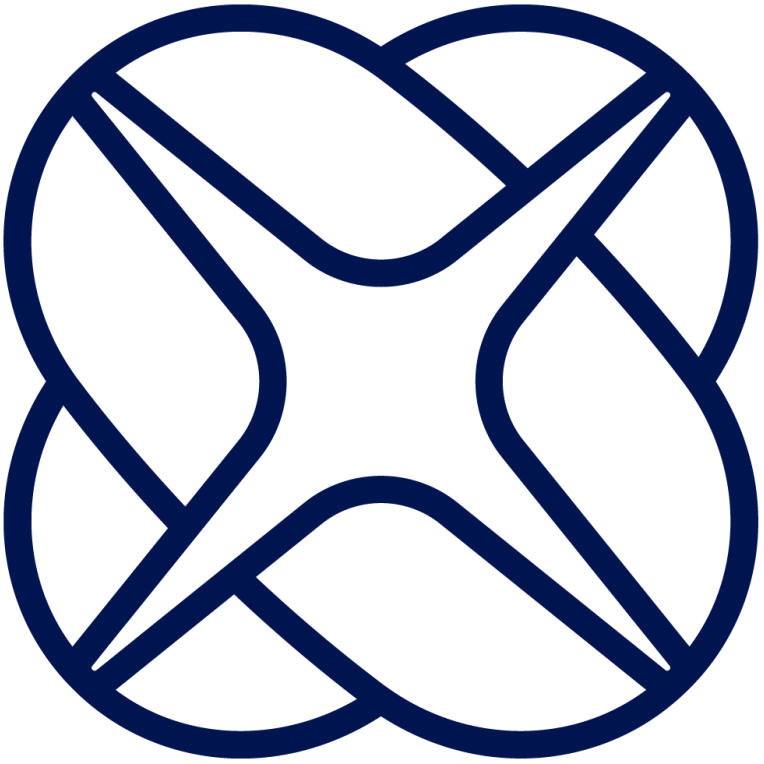


SecureEdge

Installation Manual

Version 1.3 April 2026

1. Contents

2. Introduction

This installation manual is for the SecureEdge family of products. The SecureEdge is available in multiple models which only differ in the available modes of communication:

Model	Description	Ethernet	4G/LTE	Wi-Fi	GNSS
IX5000	SecureEdge - Ethernet	✔			
IX5005	SecureEdge - 4G/LTE	✔	✔		✔
IX5010	SecureEdge - Wi-Fi	✔		✔	
IX5015	SecureEdge - 4G/LTE & Wi-Fi	✔	✔	✔	✔

The SecureEdge is delivered with the following accessories:

- Female 3-pin plug-in connector.
- SIM ejector pin tool only for IX5005 and IX5015

2.1. Help and support

For additional product support, installation tips and specifications go to https://support.ixon.cloud

For direct technical support and questions, get in touch with our Technical Support team.

E-mail support@ixon.cloud
Phone **+31 (0)85 744-1105**

⚠ Warning
Read this manual carefully before installing or operating the SecureEdge.

3. Safety instructions

Neglecting the essential safety precautions and safety guidelines outlined below could result in significant harm to individuals and property!

It is crucial to adhere to all the safety instructions and information provided in the relevant product documentation. Doing so is essential for ensuring safe and problem-free operation.

Please pay close attention to the specific safety instructions provided in the other sections of this manual.

3.1. Personnel

Only qualified and skilled personnel are allowed to work with the SecureEdge. They shall have the following qualifications:

- They are familiar with the installation, mounting, commissioning, and operation of the SecureEdge.
- They possess the appropriate qualifications for their tasks.
- They are familiar with all regulations for the prevention of accidents, directives, and laws applicable at the location and are able to apply them.

3.2. Device

The hardware and software of the SecureEdge must never be modified in a way that is not described in the installation manual. If you carry out any modifications that are not permitted, all your warranty claims will be null and void. This will result in exclusion of liability on the part of IXON.

3.3. Application

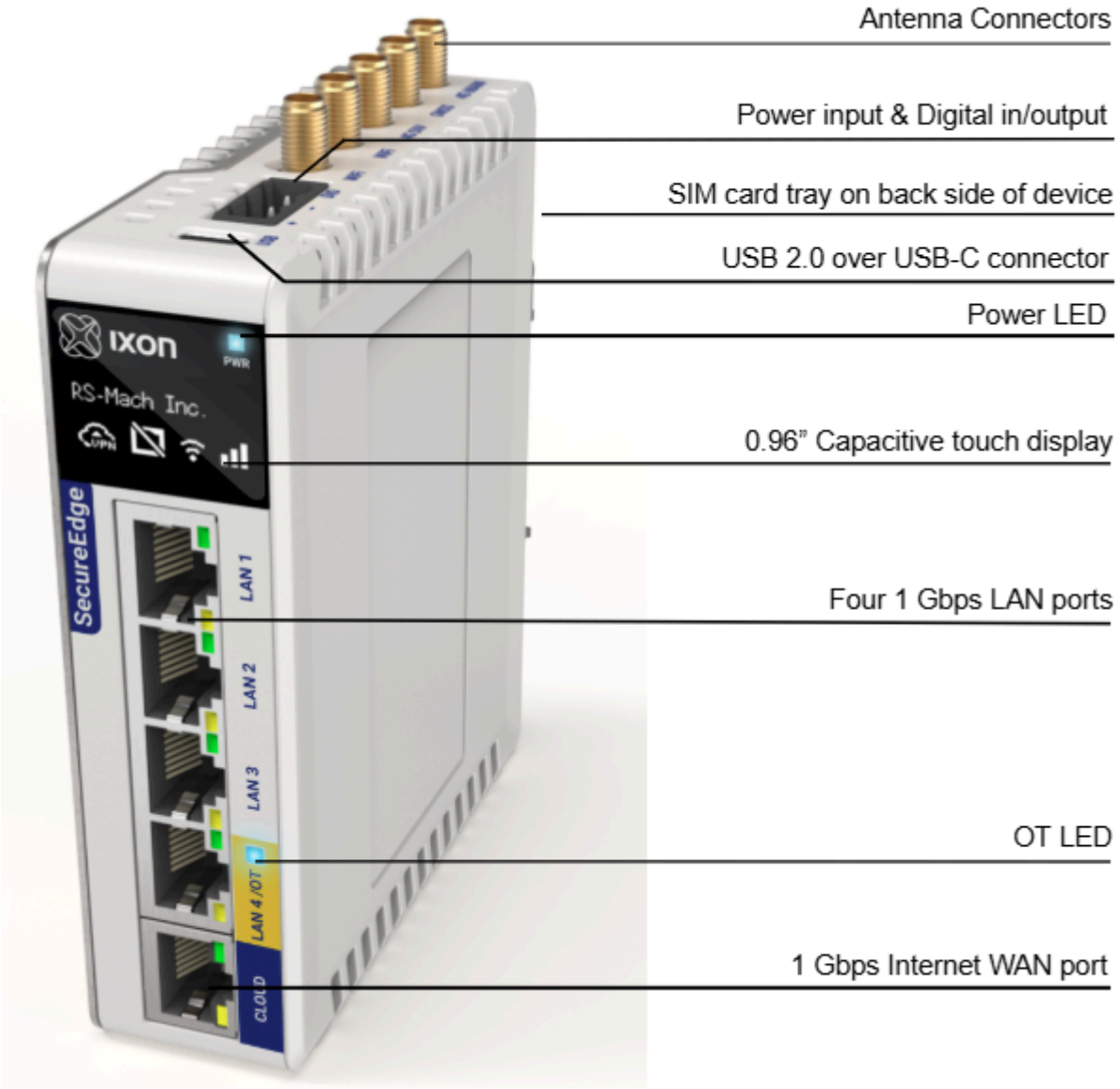
The SecureEdge is an electrical communication device. It is only suitable for installation in control cabinets or other similar closed operating environments. The environment should be protected from transient voltage and connected to the network without routing to outside plants.

3.4. Handling

The SecureEdge must be handled as follows:

- Connect or disconnect all pluggable terminals only when the SecureEdge is powered off.
- Only remove the SecureEdge from the installation when the SecureEdge is powered off.

4. Hardware features



i Notice
The availability of antenna connectors is dependent on the model.

4.1. Technical data

4.1.1. General specifications

	IX5000	IX5005	IX5010	IX5015
Power supply	12-24 VDC +/- 20% ES1, PS2			
Rated current	2A			
Rated power	2.5 W	3.5 W	3.2 W	4.5 W
Max. power	15 W			
Operating temperature	-25℃ to 60℃			
Operating humidity	10 to 95% non-condensing			
Operating altitude	Up to a maximum of 2000m			
Storage temperature	-25℃ to 60℃			
Storage humidity	10 to 95% non-condensing			
Storage altitude	Up to a maximum of 3000m			
Ethernet ports	4 LAN ports, 1 WAN port (all 1 Gbps) 1 LAN port can be configured as second WAN port			
USB version	USB 2.0 over USB-C connector			
Processor	Quad-Core ARM Cortex-A53, max 1.8GHz			
Digital Input	1 configurable Digital I/O			
Mounting type	DIN rail			
Size	112x101x31 mm (H x D x W)			
Weight	0.265 kg	0.301 kg	0.280 kg	0.315 kg
Display	0.96" monochrome OLED + CTP			

4.1.2. Wi-Fi specifications

Only applicable for models IX5010 and IX5015.

Wi-Fi version	IEEE 802.11 a/b/g/n/ac
Wi-Fi modes	Station (Client) Mode and Access Point
Frequency	2.4 GHz & 5 GHz
Speed	867 Mbps
Security protocol	WPA2-PSK
Contains FCC ID	2AATL-8274B-PR
Contains IC ID	24844-8274BPR

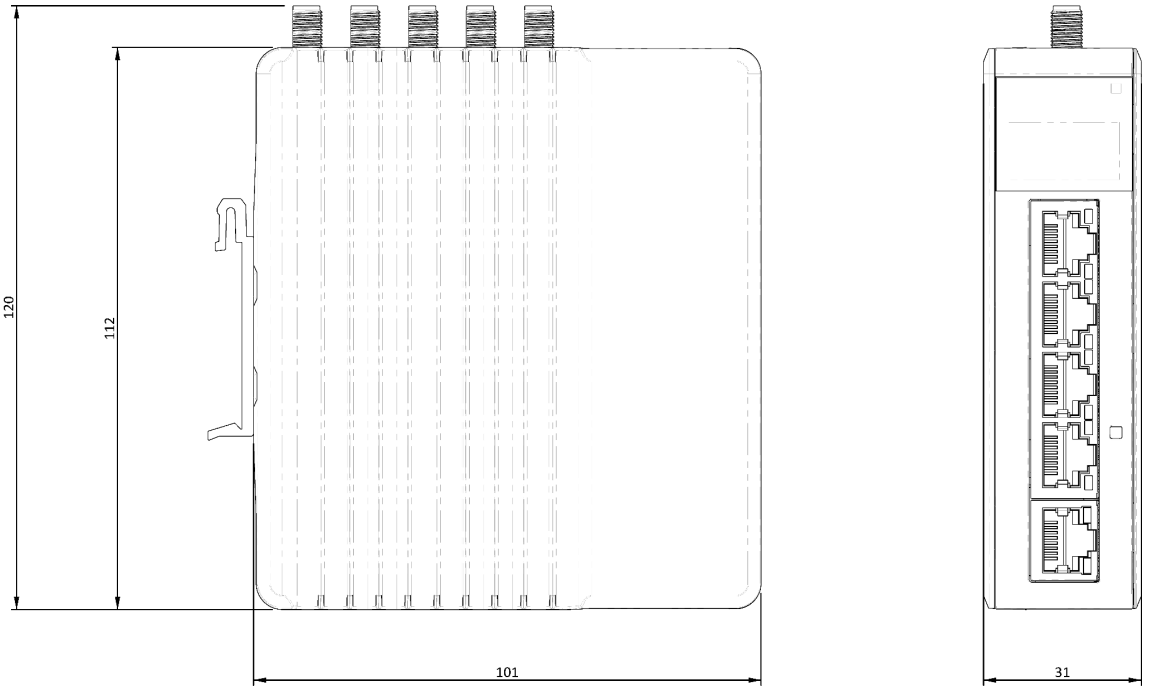
4.1.3. Cellular/GNSS specifications

Only applicable for models IX5005 and IX5015.

Frequency bands	LTE-FDD: B1, B2, B3, B4, B5, B7, B8, B12, B13, B18, B19, B20, B25, B26, B28 LTE-TDD: B38, B39, B40, B41 WCDMA: B1, B2, B4, B5, B6, B8, B19 GSM/GPRS/EDGE: B2, B3, B5, B8 GNSS: GPS, GLONASS, BeiDou, Galileo and QZSS
Data rates	LTE-FDD: Max. 150 Mbps (download) / Max. 50 Mbps (upload) LTE-TDD: Max. 130 Mbps (download) / Max. 30 Mbps (upload) DC-HSPA+: Max. 42 Mbps (download) / Max. 5.76 Mbps (upload) WCDMA: Max. 384 Kbps (download) / Max. 384 Kbps (upload) EDGE: Max. 296 Kbps (download) / Max. 236.8 Kbps (upload) GPRS: Max. 107 Kbps (download) / Max. 85.6 Kbps (upload)
SIM card	Nano SIM card (4FF)
Contains FCC ID	XMR201903EG25G
Contains IC ID	10224A-201903EG25G

5. Mechanical installation

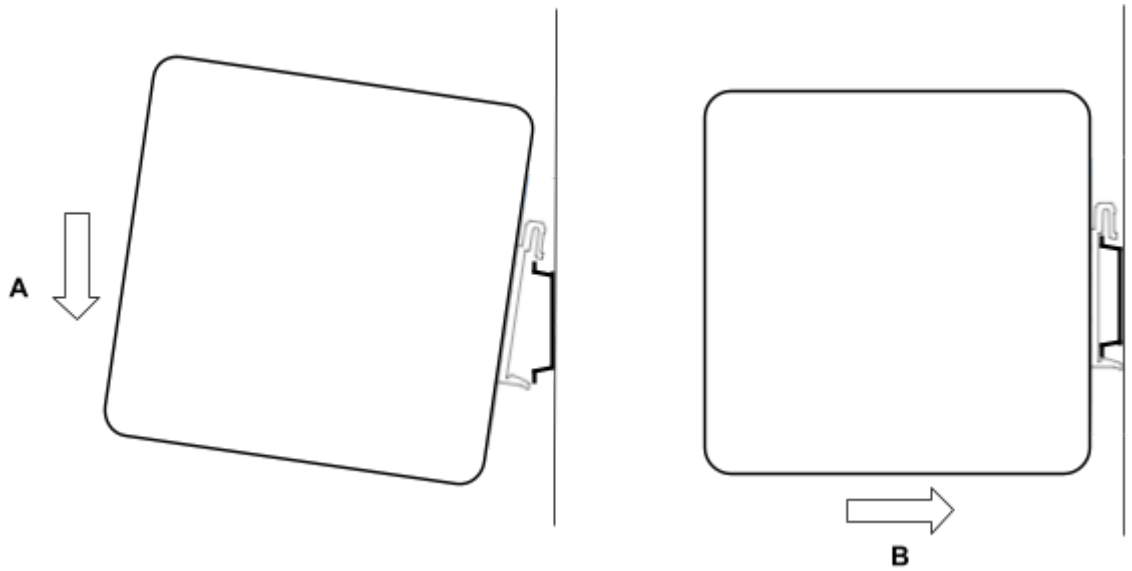
5.1. Dimensions



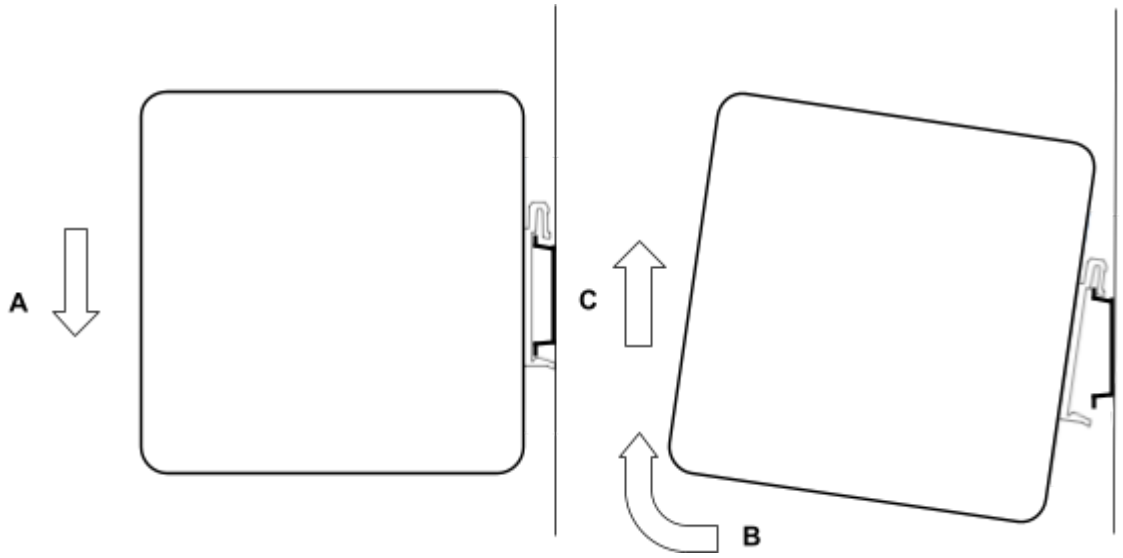
The SecureEdge is designed to be cooled using natural convection. For proper cooling, you must provide a clearance of at least 35 mm above and below the device. Also, allow at least 35 mm of depth between the front of the device and the inside of the control cabinet.

⚠ Warning
The provided installation clearances represent the minimum dimensions required to guarantee adequate air circulation for cooling purposes. However, these dimensions do not take into account the bend radius of the connecting cables and screw-on antennas for models equipped with Wi-Fi and/or 4G capabilities.

5.2. Mounting and dismounting



The SecureEdge is mounted on a standard DIN rail. Hang the device on the rail and (A) push the unit down and (B) towards the DIN rail until you feel a click.



To remove the unit, (A) push the device down, (B) pull and rotate the device up and (C) lift off the rail.

6. Electrical installation

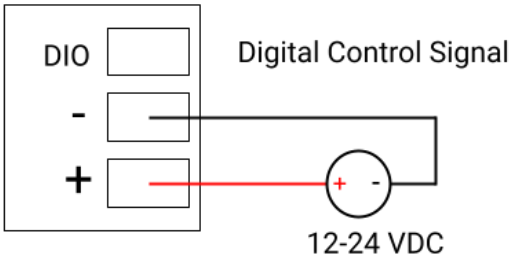
6.1. Instructions for installation

Consider the following instructions for installation:

- When installing devices in a control cabinet, always separate devices that generate high voltage and high electrical noise from low-voltage, logic-type devices such as the SecureEdge.
- Avoid placing low-voltage signal wires and communications cables in the same tray with AC power wiring and high-energy, rapidly-switched DC wiring.
- Always use an IEC/EN 62368 certified ES1, PS2 power supply for powering the SecureEdge. The output voltage of the power supply must not exceed 29 VDC.
- Always use the included female 3-pin plug-in connector when wiring the SecureEdge.
- Always use twisted pair power cables with a maximum length of 3 m.
- Always use CAT5-S/FTP or higher type shielded cables to ensure a stable LAN connection.
- Always use a shielded USB cable.

6.2. Mains connection

Mains connection	
Wire size range	18 - 12 AWG
Stripping length	7 mm
Max. cable length	3m
Ground	Attach to a proper shielded DIN rail



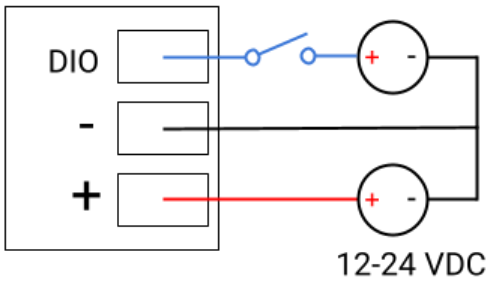
6.3. Digital Input/Output

By default, the Digital Input/Output (DIO) is not configured and doesn't need to be wired. It can be configured to work as Digital Input (DI) or Digital Output (DO).

⚠ Warning
Before configuring DIO to work as DI or DO, be sure that proper wiring connection is made.

6.3.1. Digital Input

Digital Input	
Type of digital input	Sinking
Voltage range	0-29 VDC
Voltage range (OFF)	0-3 VDC
Voltage range (ON)	7-29 VDC
Current range	2-5 mA

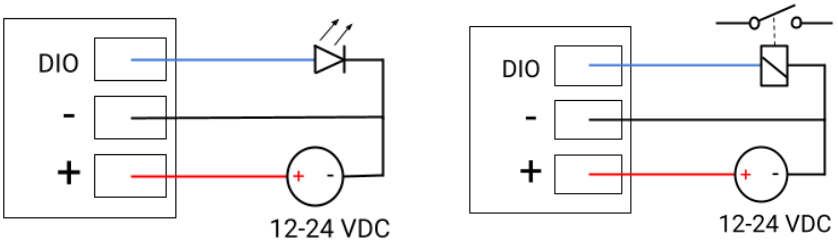


The Digital Input provides a way to locally manage SecureEdge's VPN connection (ON/OFF). The wiring for proper operation of Digital Input (DI) is depicted in the image above.

6.3.2. Digital Output

The Digital Output is for future use and has no functionality yet. The wiring for proper operation of Digital Output (DO) are depicted in the images below.

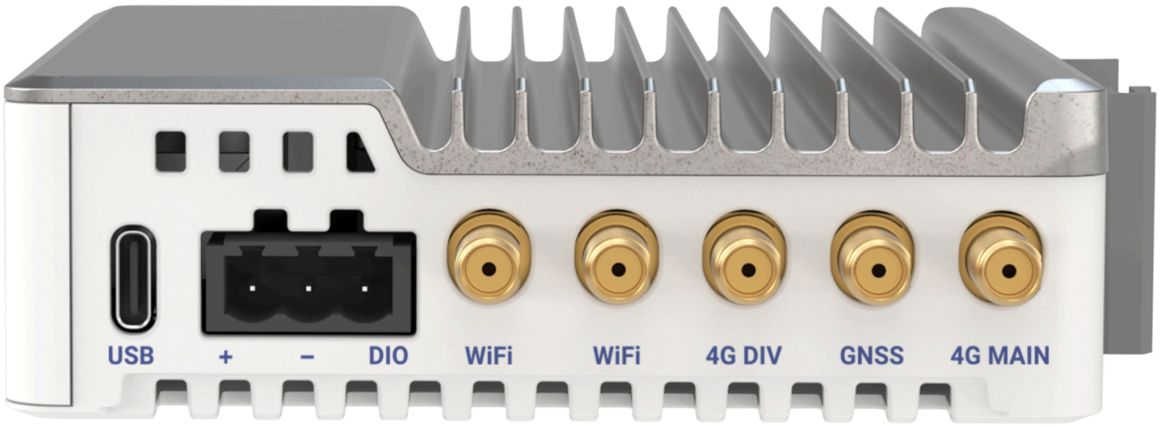
Digital Output	
Type of digital output	Sourcing
Maximum output current	100 mA



⚠ Warning
Use loads which have the same voltage rating as the input power supply.

6.4. Antennas

The SecureEdge has connectors for:



i Notice

Each SecureEdge model has different antenna ports as noted in the table.

⚠ Warning

Any antennas used with this transmitter must be installed with a separation distance of greater than 20 cm from all persons and must not be co-located or operated in conjunction with any other antennas or transmitters.

Port	Type	Description	IX5000	IX5005	IX5010	IX5015
WiFi	RP-SMA	WiFi connector.			✔	✔
WiFi	RP-SMA	WiFi connector.			✔	✔
4G DIV	SMA	Secondary 4G connector.		✔		✔
GNSS	SMA	GNSS connector.		✔		✔
4G MAIN	SMA	Primary 4G connector.		✔		✔

For optimal connection speed, connect both antenna connectors for Wi-Fi and Cellular.

⚠ Warning

Always connect the antenna to the primary connector first.

i Notice

Antennas are not included with the SecureEdge and can be purchased from IXON separately.

7. Secure installation

Please use the **Secure Baseline Guide** to configure your SecureEdge to its secure baseline, which delivers the device's most secure operational state and is certified under the IEC 62443-4-2 standard for industrial cybersecurity.

The Secure Baseline uses the principle of least functionality to minimize the device's attack surface and establish the strongest possible security by default. Completing this guide is the most direct way to effectively protect your connected machines.

Our **Advanced Hardening Guide** will further inform you about cybersecurity risks when using the SecureEdge under specific circumstances. It provides a reference for understanding and mitigating the risks associated with enabling features or modifying rules that are disabled in the Secure Baseline state. Both are available on trust.ixon.cloud.

7.1. Support period

IXON provides continuous technical security support for this product. This support includes active vulnerability monitoring, incident handling, and the provisioning of free firmware security updates which can be deployed directly via the IXON Cloud.

We guarantee this support period for at least 5 years after the product's purchase date. For the support period of your specific device model, visit https://support.ixon.cloud/s/article/Product-Lifecycle-Policy.

7.2. Vulnerabilities

To report and receive information about vulnerabilities in our products, and to access our coordinated vulnerability disclosure policy, please visit https://ixon.cloud/security.txt or contact us directly at security@ixon.cloud.

8. SIM card

i Notice

Only insert or remove the SIM card when the SecureEdge is powered off.

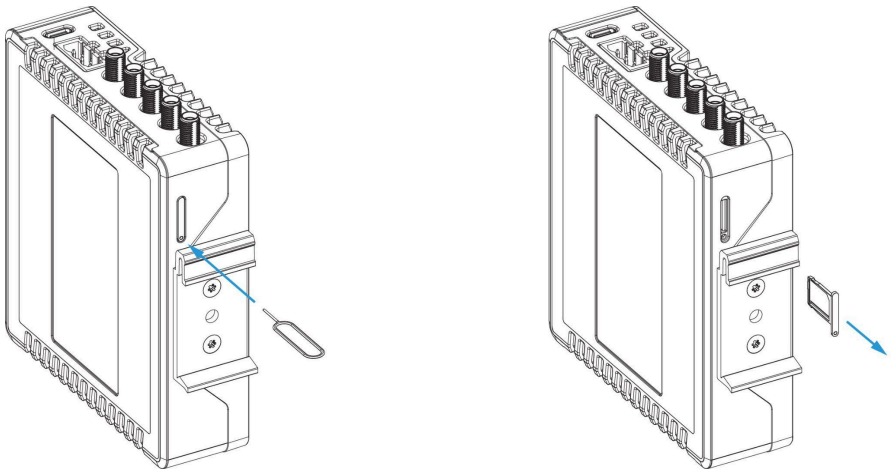
The SIM card is not included with the SecureEdge and can be purchased separately from external parties.

8.1. SIM card installation

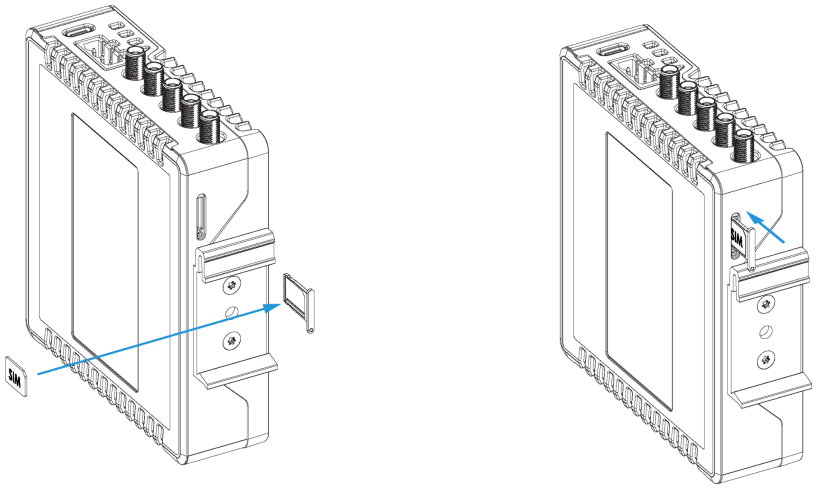
This information is only applicable for models IX5005 and IX5015.

The SIM card tray is positioned on the back side of the device and suits a Nano SIM card (4FF).

SIM card tray can be ejected using the SIM ejector pin tool provided with the device by following the process below.



The SIM card can be placed inside the SIM card tray and inserted back to SecureEdge by following the process below.



9. Display operation

The IXON SecureEdge can be easily set up and operated through the built-in display. This allows you to configure basic device settings, such as connectivity setup and registration in the IXON Cloud. The display is operated by the gestures: swipe horizontally, scroll vertically and tap (single). A complete overview of the SecureEdge display functionalities is found in this chapter.

9.1. Home Screen

The home screen displays the following information about the device:

- Name of the IXON Cloud company in which the device is registered;
- Cloud connection status (“Not connected”, “Connected VPN”, “Connected MQTT”, “Connected VPN&MQTT”, “Connected MQTT&Logging” or “Connected VPN&MQTT&Logging”)
- Ethernet connection status (“Unplugged” or “Connected”);
- Wi-Fi connection status (“Not connected” or signal strength);
- Cellular connection status (“Not connected” or signal strength).

i Notice
The display will turn-off after two minutes of inactivity.

Swiping left will show the settings menu of the SecureEdge which will allow you to configure basic device settings and view additional status information of the device:

Menu option	**Description**
Wi-Fi Client	Set up a Wi-Fi connection
Wi-Fi Hotspot	Set up a Wi-Fi hotspot
4G / LTE	Set up a cellular connection
Register	Register the device in the IXON Cloud
Network	View network information
Active errors	Show an overview of active device errors
Lock	Set up a screen lock for the device
Info	View device information
Factory reset	Reset the device back to factory default settings

9.2. Wi-Fi Client

To set up a Wi-Fi connection, navigate to the Wi-Fi client menu and turn on Wi-Fi. The device will automatically scan for available Wi-Fi networks. Select the SSID of the network you would like to connect to from the list and enter the password via the display.

9.3. Wi-Fi Hotspot

When you need an internet connection on your personal device, you can use the SecureEdge as a Wi-Fi hotspot. To set up a Wi-Fi hotspot, navigate to the Wi-Fi hotspot menu and turn on the hotspot. The device will automatically generate a network SSID and password. You can change the password by selecting the refresh button. Swiping down will show a QR code which you can scan with your smartphone to easily connect to the Wi-Fi hotspot.

9.4. 4G / LTE

To set up a cellular connection, you must first place a SIM card in the SecureEdge. See chapter 7.1. for SIM card placement instructions.

After placing the SIM card, navigate to the 4G/LTE menu item on the display, turn on 4G/LTE and enter the SIM card's APN and PIN.

The APN can be entered manually, or you can choose the default APN. Which method is most suitable, depends on the selected cellular provider:

- **Default**: Some cellular providers do not require an APN when connecting to their network. This is the case with most regular, but not all, providers. When configuring the APN, you can select the default APN option, which effectively leaves the APN empty and makes it easier to connect to these providers.
- **Manually**: If the provider requires a specific APN to connect, or if the default APN doesn't work, the APN will need to be set manually. If you are unsure about which APN to enter, you'll need to search online or contact the provider directly.

If there is no PIN code set on the SIM card, you can leave the "PIN code"-field empty.

9.5. Lock the SecureEdge

To restrict access to the SecureEdge's settings, you can configure a lock. Enabling the lock will prevent any unauthorized users from changing the SecureEdge's settings.

With lock enabled, users are only able to navigate to the following items on the display:

- Network information (read-only access)
- Active errors
- System information (firmware version, serial number, MAC addresses, hardware revision)

Navigating to other menu items will show a prompt requesting the lock code.

You can set up the lock by navigating to the Lock menu item and turning on the lock. Next, you can enter a 4-digit lock code to limit access to the SecureEdge display. You can disable the lock by navigating to the Lock menu item again and selecting “Turn off lock”.

i Notice

You can also enable or disable the lock in the fleet manager by navigating to the Info menu of your device. Here, you are also able to fill in the lock code to unlock the SecureEdge.

9.6. Network information

To obtain the network information from your device, you can navigate to the network information menu. Here, the WAN and LAN IP-addresses will be shown. If you are using a Wi-Fi connection, the IP-address of the Wi-Fi connection is visible as well.

This menu also allows you to configure your local VPN control. You can choose one of these settings:

- DI high: VPN on when digital input is high
- DI low: VPN on when digital input is low
- Disabled (default setting): VPN is always on and digital input is not used

9.7. IXON Cloud registration

You can register the SecureEdge in the IXON Cloud directly from the display. Navigate to the Register menu, scan the QR code with your smartphone and follow the instructions in the wizard. Ensure your smartphone has access to the internet. After registration, the SecureEdge is ready to use in the IXON Cloud.

For more information about the IXON Cloud, please visit https://support.ixon.cloud for extensive guides and help articles.

i Notice

Ensure that the mechanical and electrical installation have been completed and that the SecureEdge is supplied with voltage before commissioning.

10. Local web interface

The SecureEdge's local web interface can be used to view and change the WAN, LAN, and Firewall configurations locally.

The local web interface can be opened by connecting the SecureEdge to your computer using one of the edge gateway's LAN ports and entering the LAN IP address (by default http://192.168.140.1) into your browser. To change settings via the local web interface, enter the password which can be found on the product label on the side of the SecureEdge.

i Notice

The web interface is not accessible through the WAN port, or the LAN4/OT port when it's configured as a second WAN port.

11. Reset to factory default

⚠ Warning

A factory reset will delete all data, this cannot be undone! The current Firmware version will remain installed. After doing a factory reset, the SecureEdge needs to be re-registered to the IXON Cloud.

i Notice

If the edge gateway is still listed in the IXON Cloud and you want to re-use those settings, make sure to turn on **Recovery mode** before registering again.

Recovery mode is not compatible with registration via QR code. The device will need to be registered via USB stick or the local web interface.

To reset the SecureEdge, simply navigate to Factory Reset on the display and follow the on-screen steps. Your device will then be reset as stated above.

12. Connectivity requirements for local IT

The SecureEdge uses outgoing ports to establish a secure connection to the IXON Cloud. This means there is no need to open any incoming ports in your firewall. For a complete overview of ports, protocols, server allowlists, and more, please visit https://support.ixon.cloud/s/article/Connectivity-requirements.

13. Compliance

13.1. CE

Hereby, IXON B.V. declares that the radio equipment type SecureEdge is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.ixon.cloud/ce-declaration-of-conformity.

13.2. UL

This device is UL listed for USA and Canada under file number E492721.

13.3. FCC

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, and
- This device must accept any interference received, including interference that may cause undesired operation.

13.4. IC

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

Son utilisation est soumise aux deux conditions suivantes:

- Cet appareil ne doit pas causer d'interférences et
- Il doit accepter toutes interférences reçues, y compris celles susceptibles d'avoir des effets indésirables sur son fonctionnement.

Thanks for choosing us! We're dedicated to providing you with a reliable solution for seamless machine connectivity.

If you have any questions or concerns,
please don't hesitate to reach out to us.

IXON B.V.
Zuster Bloemstraat 20
5835 DW Beugen
The Netherlands