



IXON Security Guide



IXON Cloud | **Security Guide**
Last updated on: 26-01-2026

About this Guide

This IXON Security Guide is designed for everyone using IXON to connect their industrial machines – from machine builders integrating Edge Gateways to businesses using IXON Cloud.

While IXON provides secure-by-design tools and a secure cloud platform, the security of your specific connected systems requires configuring these tools correctly within your operational environment. Think of it as a shared effort to keep things safe.

This handbook serves as your practical guide. We'll walk you through:

- The basics of the secure machine-to-cloud connection.
- An inside look at the security architecture of the IXON Cloud.
- Our commitment to security via certifications and compliance.
- Recommendations to help you securely set up and manage your IXON Cloud accounts, users, and Edge Gateway devices.

Our aim is to help you with the knowledge and best practices needed to minimize risks and maintain strong security throughout the lifecycle of your connected machines.

We're here to support you. If anything is unclear, reach out to us at security@ixon.cloud.



Dylan Eikelenboom
Security Officer



Stan van Duijnhoven
Security Compliance

Table of contents

About this Guide	2
Table of contents	3
Cybercrime in manufacturing	4
Introduction to IXON	5
The machine-cloud connection explained	6
Inside the IXON Cloud platform	7
Security and IXON	9
Certifications and compliance	9
Cloud infrastructure	10
Technical and organizational measures	11
Additional resources	11
Implementation recommendations	12
IXON Cloud security	12
Edge gateway security	14
List of third parties	17
Summary	18

Cybercrime in manufacturing

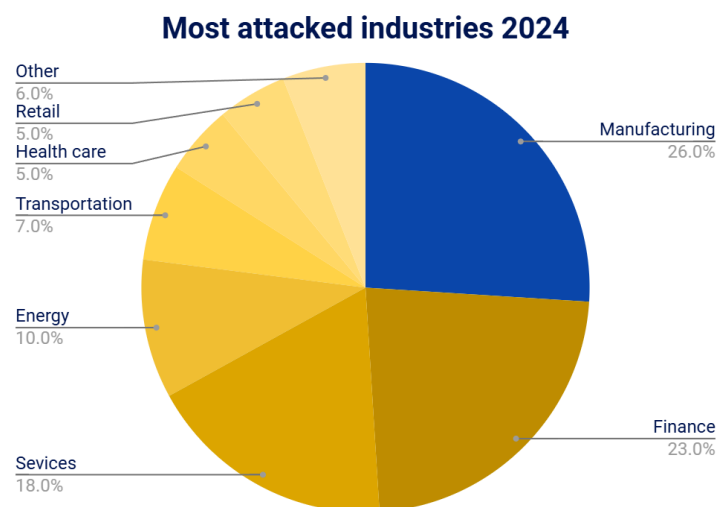
Cybercrime has emerged as one of the biggest threats to industries worldwide. Particularly vulnerable is the manufacturing sector, which has become a prime target for cybercriminals. As more technologies integrate into production lines and industrial processes, the attack surface also increases. Plant managers, now more than ever, must be vigilant when introducing new machinery into their environment.

Ransomware: A major risk for manufacturers

One of the security risks machines face is ransomware, which encrypts company data and demands a ransom for its release. This form of cybercrime can halt production, cause significant financial losses, and damage reputation. Given the nature of manufacturing regarding uptime requirements and intellectual property, ransomware can be especially devastating. Consider a scenario where machinery is attacked during peak hours; both the production halt and ransom fees can be financially crippling.

The business paradox: The necessity of cloud connectivity

In today's competitive landscape, manufacturing machines without cloud connectivity are virtually unthinkable. Cloud connectivity allows for real-time data analytics, predictive maintenance, and integration with other systems. The ability to remotely monitor performance metrics from anywhere in the world streamlines operations and drastically reduces machine downtime. Moreover, maintenance can take place exactly when needed, saving time and resources. This increased connectivity underscores the need for security. Security risks can be minimized by adopting the security measures detailed in this document.



Source: IBM X-Force Threat Intelligence Index 2025

Introduction to IXON

The machine builder of the future is a service provider. The very foundation is the physical connection with their customer's machines. Whether it's for remote access, or for developing new services based on machine data: without this connection, nothing is possible. IXON, the Industrial IoT platform tailored for machine builders, offers the most secure & reliable way to stay connected to machines & customers around the world.

Integrated remote access

Many remote access solutions are stand-alone tools, not connected to the bigger picture of your IoT strategy and IT infrastructure. This disconnection makes it hard for data and insights to flow smoothly. IXON is the only IoT platform with integrated remote access. This allows machine builders to manage machines and users in one single platform for both remote access and IoT services. As such, it stands as one of the most comprehensive and advanced solutions available in the market.

Full-fledged IoT platform

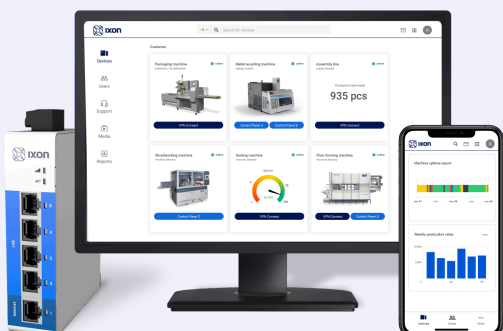
Your own IoT platform without the big upfront investment and a lengthy software development project. IXON is a full-fledged and low-code Industrial IoT platform with many functionalities included by default.

Open and expandable

Since every machine builder has its unique requirements, there are no limits to what's possible with our open and expandable IIoT platform. We integrate with your existing IT applications through APIs and provide the ability to develop custom web applications. Future-proof your service strategy with IXON.

Seamless integration from machine to the cloud

IXON edge gateways are supplied along with the IXON Cloud platform. These gateways are developed in-house by IXON and are a vital component of IXON's offering. Achieving the highest standards in reliable and secure connectivity between machines and the cloud demands seamless hardware and software integration.



Our mission

IXON's mission is to connect machine builders with their customers. We believe that close cooperation between machine owners and machine builders is the way to improve production and paves the way to a more sustainable world where machines never stop.

The machine–cloud connection explained

The machine connects to IXON Cloud via an IXON edge gateway. This gateway is mounted on a DIN rail in the machine’s electrical cabinet.

Firewall

The edge gateway is a firewall that separates the internal machine network from the OT- and IT-networks of the production plant. This separation is crucial because machine components are not designed for security, and are often not patched to adhere to the latest security standards. Therefore traffic between machine components and the plant’s IT network and internet should be minimized.

SCADA and MES systems

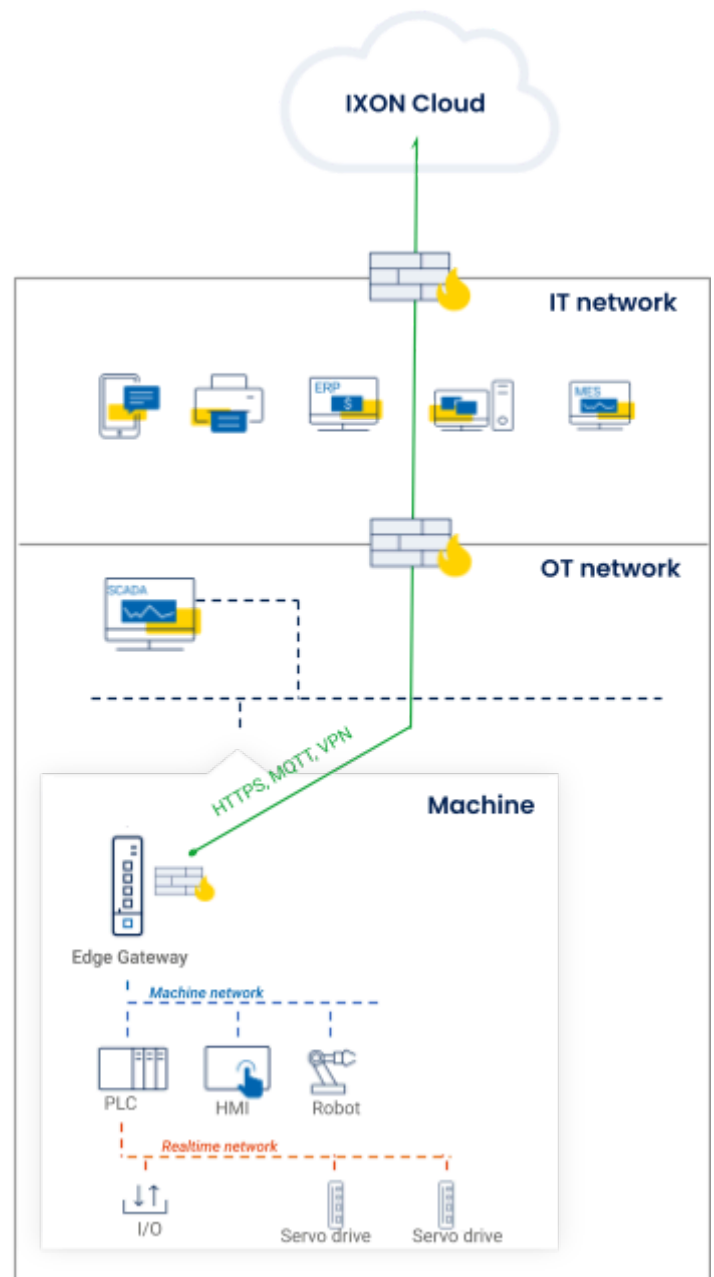
If necessary, firewall settings in the edge gateway can allow communication between the machine and SCADA/MES systems.

Outbound communication

The edge gateway communicates with the IXON Cloud platform using outbound connections only. This is designed to ensure that all inbound connections (ports) in the local firewall can remain closed. [More details on firewall ports.](#)

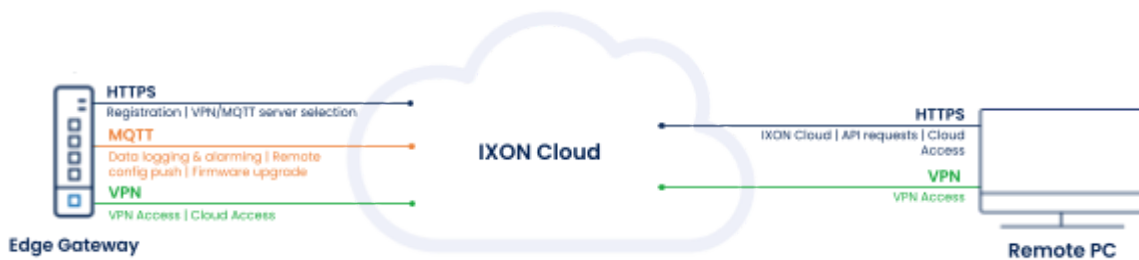
The edge gateway has 3 connections to IXON Cloud:

- An HTTPS connection for registering the device and selecting VPN/MQTT servers.
- An MQTT connection for remote configuration, firmware upgrades, and sending machine data and alerts.
- A VPN connection for remote access.



Inside the IXON Cloud platform

Transparency should be at the center when building trust. That is the reason we want to share information about the technology running the IXON Cloud platform. This section gives you high-level information that may be important when performing your own security assessment of IXON. Detailed information is available upon request.



API services

The API services are the heart of IXON Cloud and are located in data centers in Amsterdam. They handle key processes in IXON Cloud, including authorization, configuring VPN connections and retrieving data from our databases.

The API decides which VPN server is best for setting up a secure VPN tunnel, based on the physical location of the IXON edge gateway and its nearest VPN server. See status.ixon.cloud for a current overview of server locations.

MQTT broker services

IXON's MQTT broker services are used for pushing device configurations, sending commands to upgrade the firmware and for the transmission of data logging and alarm notifications. The MQTT broker services are located in data centers in Amsterdam.

On the other end of the tunnel, our VPN client is a lightweight application running in the background on your computer. This allows you to set up a secure VPN connection to your machine from within your browser.

VPN servers

IXON's VPN servers are located in data centers around the world to provide low-latency connections. The VPN server network has built-in redundancy, so if one VPN server goes down, the other servers take over automatically.



Even for computers without a VPN client connection, it's still possible to access the HMI or web-based controls of your machines. With EasyControl, the machine data is sent through the edge gateway to the VPN server using the already established VPN connection. That information is then streamed to your browser using HTTPS or a secure WebSocket connection.

Kubernetes cluster

The IXON Cloud platform contains multiple Kubernetes clusters for enabling and managing microservices. This architectural style ensures optimal scalability and availability of the IXON Cloud platform. Microservices allow large applications to be structured as a collection of loosely coupled, smaller applications (services) that can be managed and updated individually, without downtime. Each microservice is built as a Docker container.

Relational database cluster

The relational database stores information about IXON Cloud users, companies and devices. It's set up redundantly using a Primary-Secondary structure across multiple data centers in Amsterdam. The Primary receives and processes all requests to view or edit the database. The Secondary replicates all write/update events on the Primary and creates a backup every four hours.

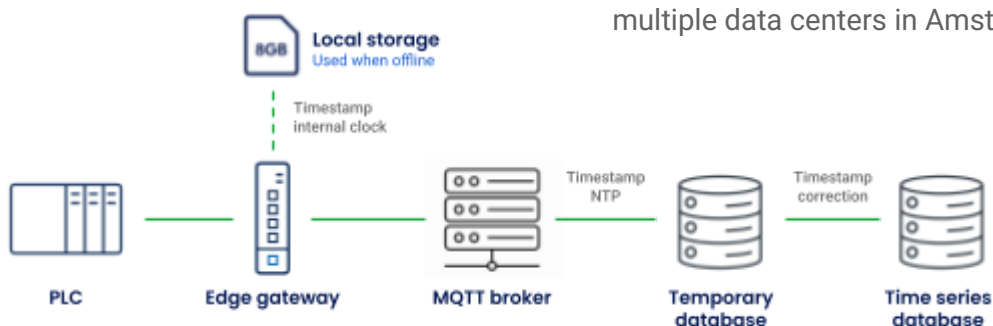
Time series database cluster

Machine data gathered with data logging is sent using the highly efficient MQTT protocol. After the edge gateway collects the data, it's first passed to our MQTT broker: a central station for receiving and sending data messages. There it's time-stamped and stored in a buffer database. Next, a time correction is applied to account for any possible discrepancies between the edge gateway's internal clock and the NTP time (actual time).

Finally, the data is stored in a time series database cluster, hosted in a data center in Frankfurt, Germany, which is optimized for handling time stamped data. The main advantage of a time series database is that it's. This allows users to request data over a large period of time in just a few milliseconds and perform operations, such as calculating the mean value, in a fast and highly efficient manner. Furthermore, time series databases allow for advanced data lifecycle management options, such as aggregation or downsampling of your machine data.

Non-relational database cluster

The non-relational database stores data on IXON Cloud platform events, generated alarms and audit trail events. This database is configured as a replica set in which the primary server receives and processes all requests, and the secondary servers replicate the primary server to ensure high availability and redundancy. The database servers are located in multiple data centers in Amsterdam.



Security and IXON

As a provider of OT cybersecurity products, IXON begins by securing its own organization. Cybersecurity is embedded into all internal processes and procedures with a comprehensive Information Security Management System (ISMS) and a Privacy Information Management System (PIMS).

Certifications and compliance

IXON's ISMS is certified in accordance with the **ISO 27001 standard**, the global benchmark for information security in organizations. This certification mandates compliance with diverse requirements, including access control, cybersecurity, training and awareness, compliance, risk management, and business continuity.

Besides this, IXON is also certified for other standards. Here is the complete overview:



IXON's management system is certified for:



✓ ISO 9001	Quality	Certificate
✓ ISO 27001	Information security	Certificate
✓ ISO 27017	Cloud security	Certificate
✓ ISO 27701	Privacy	Certificate
✓ IEC 62443-4-1	Secure software development	Certificate
✓ IEC 62443-4-2	Secure hardware components	Certificate

Scope of certification

The ISMS and PIMS encompass all of IXON's business activities, including developing cloud connectivity solutions, producing edge gateway devices, managing and maintaining the IXON Cloud platform, and handling personally identifiable information.

By choosing such a broad scope for the certification of our ISMS, we ensure the protection of data in IXON Cloud and in our internal systems.

Cloud infrastructure

IXON Cloud is an advanced network of over 150 servers distributed worldwide, optimized for peak performance, availability, and security. These servers are hosted by specialized providers, adhering to rigorous security standards and holding ISO 27001 certifications.

All servers handling data are located in the European Union, ensuring compliance with GDPR regulations.

Some key measures to maintain server security include:

- Automated installation of security updates and blocking unnecessary network traffic.
- 24/7 real-time server monitoring with immediate alerts for any anomalies.
- A Security Information and Event Management (SIEM) system examines server output for suspicious activity.
- Weekly third-party vulnerability scans and regular penetration tests on both the IXON Cloud platform and edge gateways.

On-premise solutions

IXON made a deliberate choice to not provide on-premise server solutions, due to the associated risks. These would require continuous monitoring and maintenance, as well as dedicated security specialists. Instead, IXON is committed to being a fully managed (SaaS) platform with strong security measures (see *Technical and organizational measures*).

Technical and organizational measures

For a complete list of technical and organization measures, see the [IXON Trust Center](#).

Additional resources

IXON Trust Center	Central hub for Security & Compliance information.
IXON Cloud terms of use	Details all legal clauses related to using IXON Cloud.
IXON Cloud privacy statement	This document explains in layman's terms how we handle your personal information and ensure it remains secure.
IXON status page	Shows the current IXON Cloud platform status and potential downtime occurrences.
IXON security advisories	This directory contains information about past security incidents, releases and updates for IXON products and services.

Security Desk and Legal Desk

We offer comprehensive documentation, training, and tools. For digital services, agreements regarding data privacy, data ownership, and liability are essential. IXON can assist you in understanding the arrangements between machine builders, machine owners and IXON. Access to IXON's Security Desk and Legal Desk is available free of charge.

Email: security@ixon.cloud
Phone: +31 (0)85 744 1105

Appendix A:

Implementation recommendations

IXON products require that a number of choices are made—regarding settings, features and connections—that directly impact security risks. The default settings of the IXON edge gateway are configured strictly, but are also compatible with an average machine. This chapter provides you with practical steps to safely use your IXON environment and ensure you can secure your machines.

To emphasize, the points below are intended as general best practices. You can have clear reasons to deviate from them: because of corporate policy, personal preference or a particular use case. Feel free to do so, but be aware of the potential security risks that it incurs.

IXON Cloud security

✓ Use strong account credentials

When creating your account, it's crucial to choose a strong password that is long, unique and hard to guess. Also, enable two-factor authentication to add an extra layer of security to your account by requiring a second form of verification in addition to your password. These two steps make it virtually impossible for unauthorized users to gain access to your account.

✓ Manage other users

The user who creates the IXON Cloud company will automatically be given administrator rights and can invite other users to the platform. Consider who to send an invite to. Below is a list of general good practices:

- Only invite people who need access to IXON Cloud.

- Give people a heads-up beforehand.
- Verify and double-check email addresses.
- Invite people using personal email accounts only (e.g. not info@company.com).
- Give users just the permissions they need (see next section).
- Add a message explaining the need for strong password credentials.
- If users only require temporary access, do not forget to set an expiration date.

To ensure that all users in your company employ strong credentials, we strongly recommend administrators enforce two-factor authentication for all users.

✓ Apply the principle of least privilege

Give users only the permissions they need to do their job, and nothing more. Also, restrict access to only edge gateways they need. As a rule of thumb, it is better to make an exception to temporarily give someone elevated permissions, than to give them permissions they will probably never need by default.

Be especially strict with 'Manage users' and 'Manage roles' permissions, since these allow you to invite other users and set permissions. For ease of use, create descriptive user roles and user groups to manage groups of users at once.

✓ Offboard leavers promptly

When a person leaves the company or changes job responsibilities, evaluate their IXON Cloud access as soon as possible. Update their permissions accordingly or remove them altogether.

✓ Only keep sessions open on devices you trust

During login, you can choose to "keep me logged in", which extends the session (the period during which you will not be asked for your credentials) from 24 hours to 30 days. This improves ease-of-use for protected devices where you are the sole user but is a risk for communal or borrowed devices. Similarly, on these types of devices, don't forget to log out once you have finished using IXON Cloud. You should regularly audit your active sessions and revoke those that should no longer be active.

✓ Review IXON Cloud activity

Regularly reviewing the audit log can help you identify any unusual or suspicious activity in your company. The audit log provides a record of all actions taken in your account, including logins, changes to user permissions, and more. Also, plan a moment to routinely review all security aspects of IXON Cloud; users, permissions, sessions, credentials, etc.

Edge gateway security

✓ Securely install new devices

New edge gateways need to be installed in a secure manner. Most importantly, physical access to the gateway and PLCs should be restricted by installing it in a locked cabinet or room. After all, having physical access to the gateway or machine allows you to directly connect to the machine, bypassing the firewall.

Registering the gateway to IXON Cloud is typically done with a configuration file (an *ixrouter.conf* file) on a USB drive. After registration, we recommend you remove the USB from the device. When inserted, the edge gateway will write logging information to the USB for debugging purposes, which may hold confidential information. We also recommend you delete the *ixrouter.conf* file from the USB. Generally speaking, there is no confidential information readily available in the configuration file, unless you configure the edge gateway to connect via an authenticated Wi-Fi connection. However, the configuration file may be used to register other edge gateways to your IXON Cloud environment.

Lastly, it's important to change the edge gateway's web interface password. The initial password is unique for each device, but is printed on the label and can be spotted by anyone with physical access. After using it for the initial login, change the password to something long, unique and hard to guess.

✓ Configure failover

If possible, you should configure edge gateways to employ Multi-WAN, which gives them failover capabilities in case their primary internet connection is disrupted.

✓ Enable local control over remote access

Connect a toggle switch to the edge gateway's digital input to choose when to allow VPN connections. In this way, operators have local control over remote access and EasyControl.

✓ Patch the firmware

We strongly advise updating devices when a security patch is available. However, it is generally good practice to update whenever a new version is available. While not every new firmware release contains security patches, they do contain stability improvements, new features and bug-fixes. The list of changes and improvements can be viewed in the IXON Cloud platform or in our release notes.

✓ **Whitelist necessary traffic**

To allow the IXON gateway to reach the IXON Cloud platform via the internet, you need to whitelist valid outbound network traffic in the local firewall. Use granular firewall rules to only allow necessary traffic. Edge gateway communication has the following characteristics:

- The IXON gateway communicates using TCP to destination port 443*
- IP-addresses listed in `whitelist.ixon.cloud` are valid destinations
- IXON domains end in `.ixon.net` or `.ayayot.com`

**Traffic may use port 8443 when using Stealth VPN mode or port 53 for DNS requests*

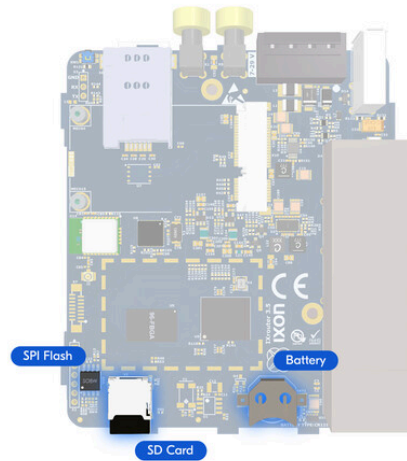
✓ **Restrict the firewall**

By default, the edge gateway firewall is configured as strictly as possible. Only change firewall rules when necessary to avoid allowing unwanted access. Changes like allowing LAN to WAN increase the likelihood of malicious traffic. Consult the image below to determine potential pitfalls:

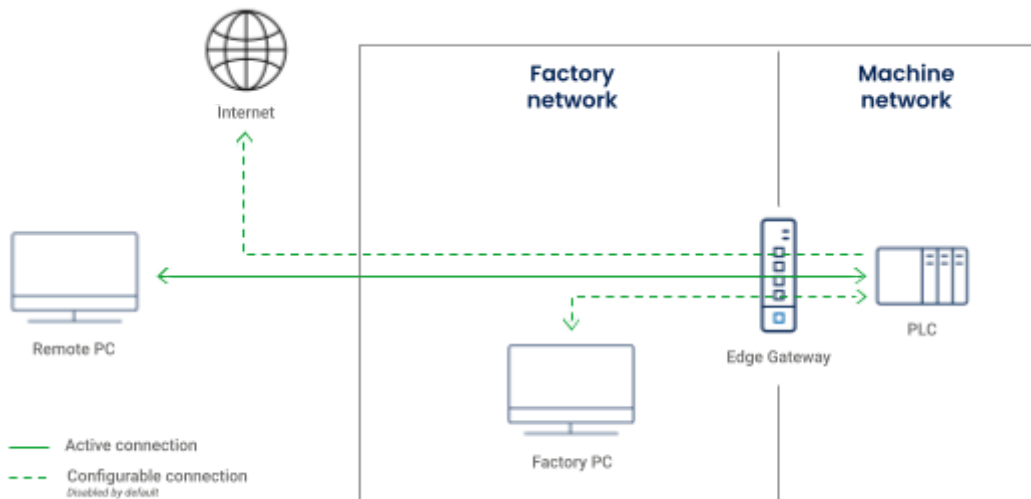
✓ **Dispose of decommissioned devices**

When a device is uninstalled and reused in a different environment, you may wish to factory reset the device and remove it from the IXON Cloud platform to ensure no old data remains. After this, you can treat it as a brand new device.

If a device is decommissioned, in some cases confidential data may be present on the device; The **SPI Flash** chip contains authentication keys used to identify itself as an IXON edge gateway and the **SD card** may hold machine logging data and core dumps after a crash. Please open the casing and remove or destroy these parts.



We also recommend you remove the coin cell battery and dispose of it in an environmentally friendly way.



Communication

✓ Keep informed about security events, updates and changes

To ensure you are kept informed about everything directly and indirectly related to security, please note the following sources:

- IXON status (status.ixon.cloud) - Shows the current status of the IXON Cloud platform and any potential downtime.
- IXON security advisories (support.ixon.cloud) - Contains the latest information about security incidents, releases and updates for all IXON products and services.
- IXON release notes (answers.ixon.cloud) - Lists all software updates to the IXON Cloud platform, edge gateways or VPN Client.

Appendix B:

List of third parties

For a complete list of third parties, see the [IXON Trust Center](#).

Summary

IXON is all about delivering an Industrial IoT platform that is not only secure but also improves collaboration between machine builders and production companies for optimal performance. With globally redundant servers and comprehensive security controls, we offer an agile and reliable solution that gives you peace of mind.

The trust of more than 2,500 companies worldwide—over 70,000 connected machines—is not won lightly. They have chosen IXON because they know that investing in our technology results in measurable benefits and growth. By continually innovating, we strive to help our users get the maximum potential from their investments.

At IXON, we proudly take on the responsibility of guarding your most valuable asset. Security is not just a promise; it's woven into the DNA of everything we do.

Trusted by Machine Builders worldwide



IXON Headquarters

Beugen, The Netherlands
t. +31 85 744 1105

www.ixon.cloud

support@ixon.cloud
sales@ixon.cloud
security@ixon.cloud

