# IXON Security Guide

IXON Cloud I **Security Guide**

Last updated on: 14-05-2024

# Preface

This guide is designed for machine builders who integrate IXON products into their machines and for businesses using these connected systems.

For IXON, cybersecurity is our top priority. We believe that the cornerstone of effective cybersecurity is transparency, rather than obscuring details or providing incomplete information. Our mission is to collaborate with you to ensure your machines remain safe. Therefore, it's crucial for you to have access to detailed information about the inner workings of IXON.

Cybersecurity is a very broad subject, making it challenging to address everything to a level of detail everyone is comfortable with. As a result, this handbook presents a thorough breakdown of our security approach at different levels, covering every aspect of IXON, our products, and guidelines on their safe deployment.

As always, we are here to help. If anything is unclear or missing, please let us know at security@ixon.cloud.

**Dylan Eikelenboom,**
**Security Officer at IXON**

# Table of contents

# Cybercrime in manufacturing

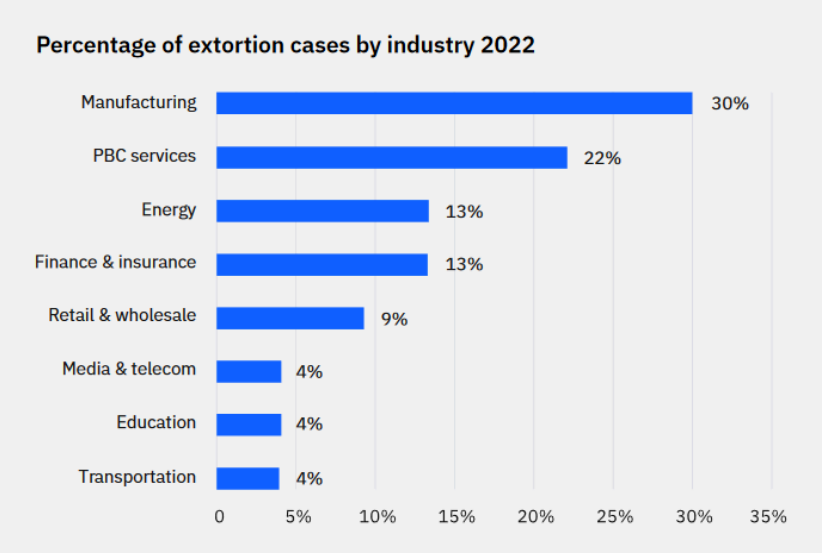
Cybercrime has emerged as one of the biggest threats to industries worldwide. Particularly vulnerable is the manufacturing sector, which has become a prime target for cybercriminals. As more technologies integrate into production lines and industrial processes, the attack surface also increases. Plant 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 seamless 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 both 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 2022

# 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

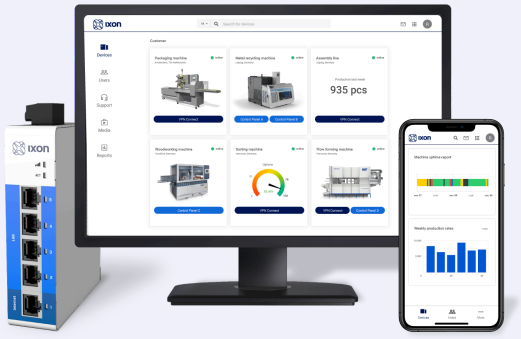
Your own IoT platform without the big upfront investment and a lengthy software development project. IXON is a full-fledged and low-code Industrial IoT platform with many functionalities included by default.

## 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

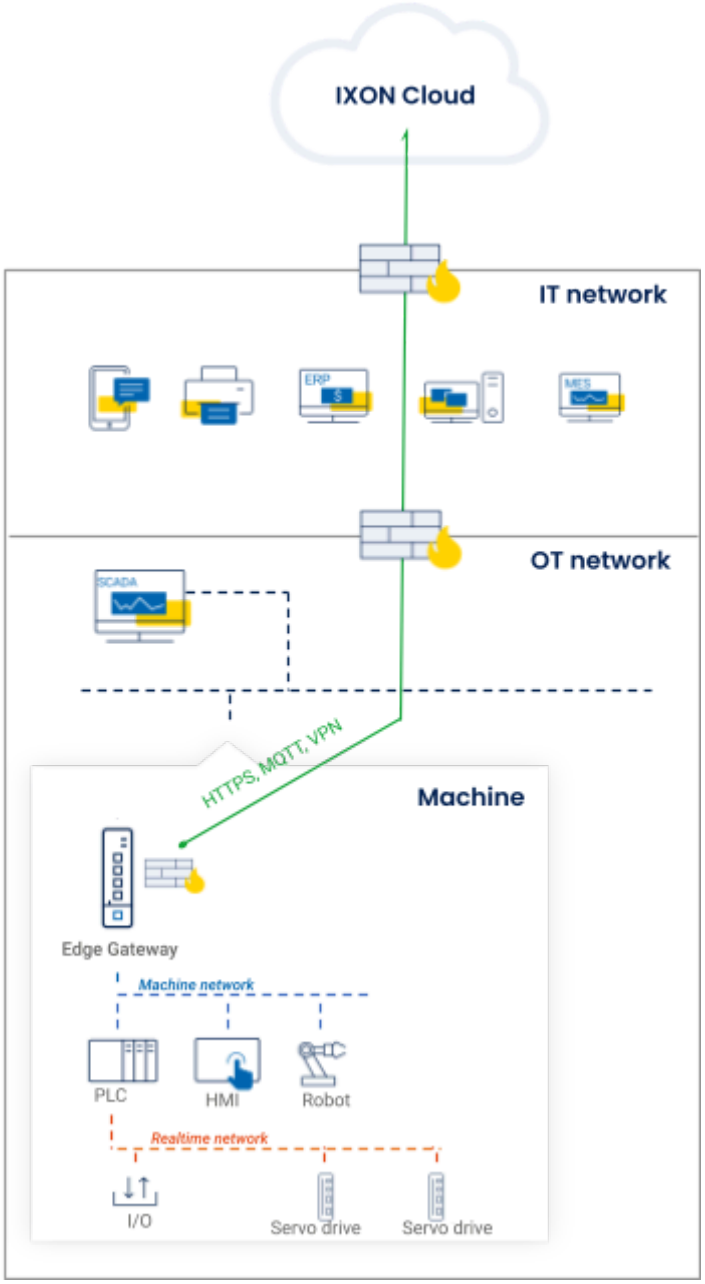
If necessary, firewall settings in the edge gateway can allow communication between the machine and SCADA/MES systems.

## 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.

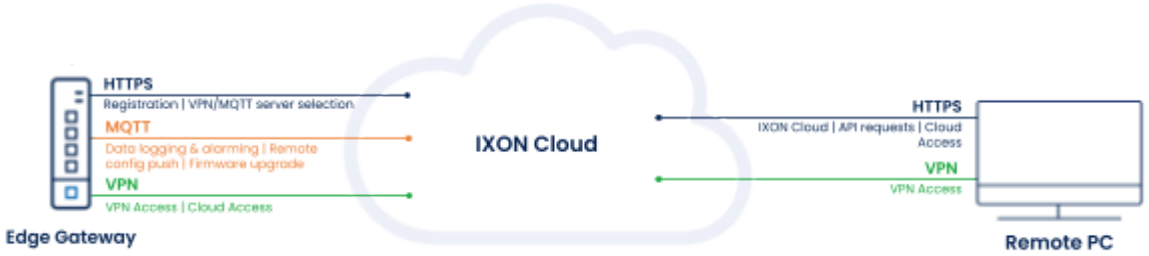
The edge gateway has 3 connections to IXON Cloud:

- 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

We believe 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.

### 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.

### 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.

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.

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.

Even for computers without a VPN client connection, it's still possible to access the HMI or web-based controls of your machines. With WebAccess, 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.

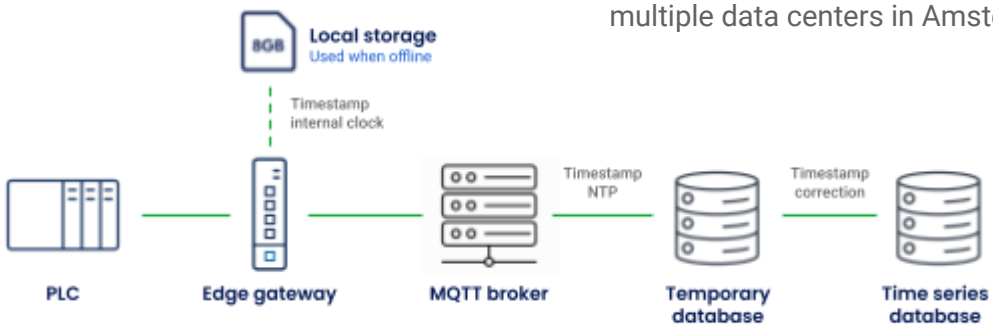
### Time series database cluster

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 and compliant with 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 |

| IXON devices are compliant with: | | |
|---|---|---|
| ✓ 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

Security is about more than just technology; it's also about the processes and standards we follow. In this chapter, we'll discuss the measures IXON takes, both technically and organizationally, to ensure your equipment stays secure.

## Infrastructure security

| | |
|---|---|
| **Server network** | IXON Cloud is a network of over 150 servers, distributed globally among various hosting providers. All are situated in data centers maintaining the highest security standards. |
| **High availability** | IXON servers are set up for high availability or have redundant deployments, ensuring that a single hardware or network failure won't compromise the availability of IXON Cloud. |
| **Backups** | Stateful servers are backed up weekly. Additionally, backups for essential customer and machine data are created every 4 hours. These backups are monitored in real-time for accuracy and undergo monthly validity tests. |
| **Server access** | Only authorized IXON personnel, including developers and administrators, can access servers. This is facilitated through unique usernames and private SSH keys. All server-related activities are logged and audited. |
| **Real-time monitoring** | Servers are constantly monitored using an array of both standard and custom checks analyzing internal metrics. Any deviations or anomalies are immediately alerted to relevant staff. |
| **Server configuration** | A master node manages server configuration, guaranteeing uniformity across servers. This system also enables effortless deployment of new servers. |
| **Server hardening** | Our servers undergo a hardening process, minimizing vulnerabilities by eliminating unused protocols, tightening file access permissions and mandating robust passwords. |
| **Patch management** | Critical patches are applied within a day. Weekly, non-critical software patches are assessed and those enhancing uptime, performance or security are deployed. |

| | |
|---|---|
| **Firewalls** | Each server contains a firewall, adopting a deny-all, permit-by-exception approach. Exceptions are rigorously evaluated to be as strict as possible, employing methods like source IP or protocol whitelisting. |
| **Inter-server exchange** | IXON Cloud servers operate within an internal mesh network, ensuring that communications between servers never traverse the public internet. |

## Data privacy and confidentiality

| | |
|---|---|
| **Privacy by design** | Every change in data handling, from software updates to subcontractor shifts or internal process modifications, undergoes a privacy impact analysis to ensure data privacy. |
| **GDPR compliance** | Personally identifiable information (PII) is processed and stored by EU-based third parties in line with GDPR legislation, as detailed in the 'List of 3rd parties'. IXON has designated a privacy officer to ensure compliance. |
| **Data ownership** | All personal and machine data stored or created in IXON Cloud remains your property. IXON may not, in any shape or form, misuse, distribute or sell this information. |
| **Data retention** | Data does not expire as long as you have an active user account. After deleting your account, data will be removed after 3 months. |
| **TLS encryption** | HTTPS and MQTT connections use TLS 1.2 or higher for encryption. We permit only strong encryption algorithms that support perfect forward secrecy, utilizing RSA keys of 4096 bytes. |
| **VPN encryption** | VPN connections utilize single-use TLS certificates for authentication. AES-256-CBC is used for encryption, using SHA512 as the authenticator. |
| **Password hashing** | IXON Cloud passwords are stored as hashes using Argon2id, configured with 3 iterations, 4 degrees of parallelism, 64 MiB memory, and a 16-byte salt. |

## Vulnerability management

| | |
|---|---|
| **Vulnerability scanning** | IXON Cloud servers are tested for vulnerabilities weekly using internal and external scans. |

| | |
|---|---|
| **Penetration testing** | Each year, the IXON Cloud platform and edge gateways have at least 2 third-party penetration tests. Tests range from black box evaluations of the entire IXON Cloud to white box analyses of significant architectural changes. |
| **Log analysis** | All server logs are gathered in a centralized log system and automatically analyzed according to community-maintained and custom security rules. |

## Incident handling

| | |
|---|---|
| **Security breach protocol** | A protocol is in place to address security incidents effectively and efficiently. Briefly, this protocol involves the following steps: 1) Incident verification, 2) Containment, 3) Evaluation and 4) Lessons learned. |
| **Incident notification** | Impacted parties and users are notified promptly about a security incident (usually via email). We strive to be as transparent as possible in our communication. |
| **Incident training** | Annually, using a tabletop setting or a simulated environment, we replicate a major security breach to ensure IXON personnel are familiar with their role in the security breach protocol. |
| **Business continuity plan** | A plan is in place to ensure business operations continue uninterrupted during various man-made or natural events. |

## Application security

| | |
|---|---|
| **Authentication** | The initial login to IXON Cloud uses Basic Authentication. After successful login, users receive a Bearer token valid for their session duration. |
| **Password strength** | We mandate passwords be deemed ‘unguessable’ (no. guesses > $10^8$) by our strength estimator. We don't enforce complexity requirements for passwords. This system also blocks commonly used passwords. |
| **Brute force protection** | Repeated failed login attempts (>10 tries) result in a temporary block. This time increases with subsequent failed attempts, up to a maximum of 1 hour. |
| **Multi-factor authentication** | Time-based one-time passwords (TOTPs) can be employed as an additional authentication factor. They can be activated for individual users or mandated for all users within your IXON Cloud environment. |

| | |
|---|---|
| **Granular permissions** | Administrators can fine-tune permissions using user groups and roles, adjusting access for multiple users simultaneously. These permissions can provide access to all devices, target specific ones (Limited LAN access) or restrict certain device services, such as VPN or WebAccess (WebVNC or WebHTTP). |
| **Logical separation of data** | Although customer data resides in multi-tenant environments, we implement multiple layers to safeguard data confidentiality. Initially, requests validate your Bearer token. Subsequently, data filtering occurs based on your domain, company ID, and permission role—returning only the information you're authorized to view. |
| **Session control** | Active IXON Cloud sessions are accessible within your account details. Implementing a security change, like updating your password, auto-revokes all ongoing sessions. |
| **Audit trails** | IXON Cloud provides device-specific and company-wide audit trails, offering users a comprehensive record of historical events. |

## Software development

| | |
|---|---|
| **Security by design** | Security requirements are created before development which must be met before changes may be deployed. |
| **Peer reviews** | Any code modifications undergo a review by at least one senior, unbiased developer. This ensures readability, clarity, and completeness. All identified issues must be resolved before approval. |
| **Automated testing** | Upon committing changes to our software versioning system, the code undergoes comprehensive automated tests. This encompasses unit tests, scenario tests, and security evaluations. |
| **Staged deployment** | We employ distinct environments to segregate (potentially) insecure code before it reaches production:<br>• Development: runs locally on developers' systems, facilitating code modifications and automated testing.<br>• Testing: holds finished features and serves as a platform for manual tests.<br>• Staging: contains code ready for production, and is utilized for integration and stress testing. |

## Organizational security

| | |
|---|---|
| **Vendor reviews** | Suppliers and third parties undergo an initial security review and subsequent annual checks. Essential suppliers, like hosting providers, must possess an ISO 27001 certificate or equivalent. |
| **Training and awareness** | All security personnel must meet a set training quota each quarter. New hires are trained on IXON's security policies during onboarding, and the entire staff regularly undergoes updates on pertinent security topics. |
| **Policy management** | Our security policies are accessible via an internal webpage. Policy alterations are documented, requiring approval before being published. Policies undergo a biannual review. |
| **Risk management** | Quarterly risk assessments categorize threats by likelihood and impact. Risks exceeding acceptable thresholds are documented in a treatment plan, outlining specific corrective actions and their respective deadlines. |
| **Endpoint protection** | All company hardware features hard-disk encryption and endpoint protection software. In-depth antivirus scans run weekly, with any anomalies instantly reported to our security team. |
| **Certifications** | IXON's management system holds certifications in:<br>● ISO 9001: Quality Management<br>● ISO 27001: Information Security Management<br>● ISO 27017: Cloud System Information Security<br>● ISO 27701: Privacy Management<br>Accredited third-party NCI conducts yearly external audits.<br><br>IXON is also compliant with:<br>● IEC 62443-4-1: Secure Software Development<br>● IEC 62443-4-2: Secure Hardware Components |
| **Internal audits** | Every quarter, internal audits are undertaken by independent IXON employees. |

# Additional resources

| | |
|---|---|
| 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.

For more information, please contact our Security Officer, Dylan Eikelenboom:

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 in a strict way, 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 WebAccess.

### ✔ 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 on outgoing 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*

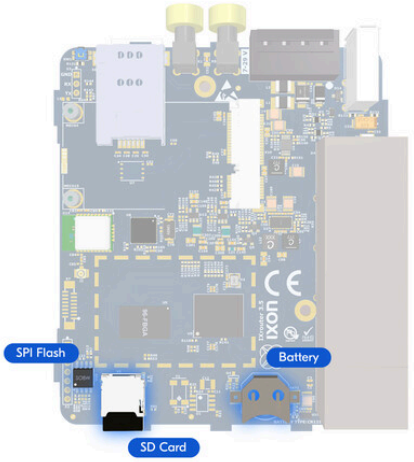
### ✔ Restrict the firewall

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:

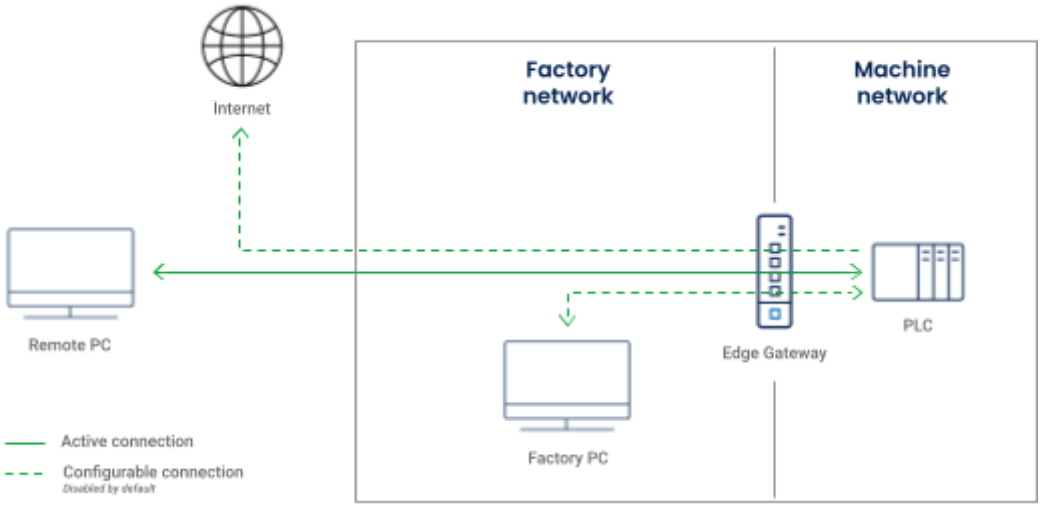
### ✔ Dispose of decommissioned devices

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

IXON uses certain platform subcontractors, as well as infrastructure suppliers and other third-party business partners, to provide its services to its customers.

**What is a subcontractor?**
A subcontractor is a third party engaged by IXON to perform part of its service, who may have access to production infrastructure with customer data or process customer data. The icon GDPR indicates the party handles or may handle your personally identifiable information, depending on how you are using our services.

**Due diligence**
IXON undertakes due diligence to evaluate the data privacy and security posture of (potential) subcontractors both prior to engagement and yearly. Our activities are designed to ensure that processing is only performed by entities with sufficient ability to meet our data protection standards.

**Contact information**
If you have any questions regarding IXON's use of subcontractors, or wish to express concerns, please contact us at privacy@ixon.cloud.

## IXON Cloud infrastructure

IXON Cloud consists of ~150 Linux-based servers, located primarily in the EU. These servers are provided by hosting providers, after which proprietary IXON software is installed. At a minimum, each provider used to host IXON Cloud servers is ISO 27001-certified and GDPR-compliant.

### Databases

| Company | Server location(s) | Type of data stored |
|---|---|---|
| Aiven<br>aiven.io | Germany | Machine data (for Enterprise customers) |
| GDPR Digital Ocean LLC<br>digitalocean.com | The Netherlands | Audit trail data |
| | | Customer data |
| | | Machine data (backup) |
| InfluxData<br>influxdata.com | Germany | Machine data |
| GDPR UpCloud Ltd.<br>upcloud.com | The Netherlands | Audit trail data |
| | | Customer data |

## VPN servers

*Note: data transmitted over VPN is encrypted and only readable by the intended recipient (i.e. client). VPN traffic is not stored in any form.*

| Company | Server location(s) |
|---|---|
| Digital Ocean LLC<br>digitalocean.com | Singapore, the Netherlands and the United States |
| Exoscale<br>exoscale.com | Austria and Germany |
| Alibaba Cloud<br>alibabacloud.com | China |
| Linode LLC<br>linode.com | The United States |
| UpCloud Ltd.<br>upcloud.com | Germany and the Netherlands |
| Vultr Holdings Corp.<br>vultr.com | Australia, Germany and the United States |

## Ancillary infrastructure

| Company | Purpose | Server location(s) |
|---|---|---|
| Upcloud<br>upcloud.com | Internal networking, CDN and server monitoring | The Netherlands |
| Digital Ocean LLC<br>digitalocean.com | API, internal networking, load balancer, server monitor, MQTT broker | The Netherlands |
| | (Internal) API | Singapore and the United States |
| Vultr Holdings Corp.<br>vultr.com | Domain hosting and server monitoring | The Netherlands |
| TransIP<br>transip.eu | Server monitoring and automated server provisioning | The Netherlands |

## IXON Cloud platform

| Company | Purpose | Server location |
|---|---|---|
| Akamai<br>akamai.com | CDN services | |
| Apple<br>apple.com | App store | |
| ClouDNS<br>cloudns.net | DNS services | |
| Firebase<br>firebase.google.com | Pushover messages | |
| Google LLC<br>play.google.com | App store | |
| GDPR ElasticCloud<br>elastic.co/cloud | Centralized logging | The Netherlands |
| GDPR Mailchimp<br>mailchimp.com | Email services | United States |
| Realtime Register<br>realtimeregister.com | DNS services | |
| Segment<br>segment.com | User identification | |
| Sentry<br>sentry.io | Error tracking | |
| Tenable<br>tenable.com | Security vulnerability scanning | |
| GDPR TransIP<br>transip.eu | Customer data backup | The Netherlands |
| Userpilot<br>userpilot.com | User onboarding | |

## Ancillary services

| Company | Purpose | Server location(s) |
|---|---|---|
| Discourse<br>discourse.org | Public forum (answers.ixon.cloud) | |
| GitLab<br>about.gitlab.com | Software versioning | |
| Google LLC<br>datastudio.google.com | Business analytics | |
| GDPR Hubspot<br>hubspot.com | Corporate website (www.ixon.cloud) and integration with CRM | Germany |
| Microsoft Corp.<br>powerbi.microsoft.com | Business analytics | |
| Readme<br>readme.com | Support page (developer.ixon.cloud) | |
| GDPR Salesforce.com Inc.<br>salesforce.com | CRM | France and Germany |
| Status.io<br>status.io | Status page (status.ixon.cloud) | |
| Zendesk<br>zendesk.com | Support page (support.ixon.cloud) | |

# 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