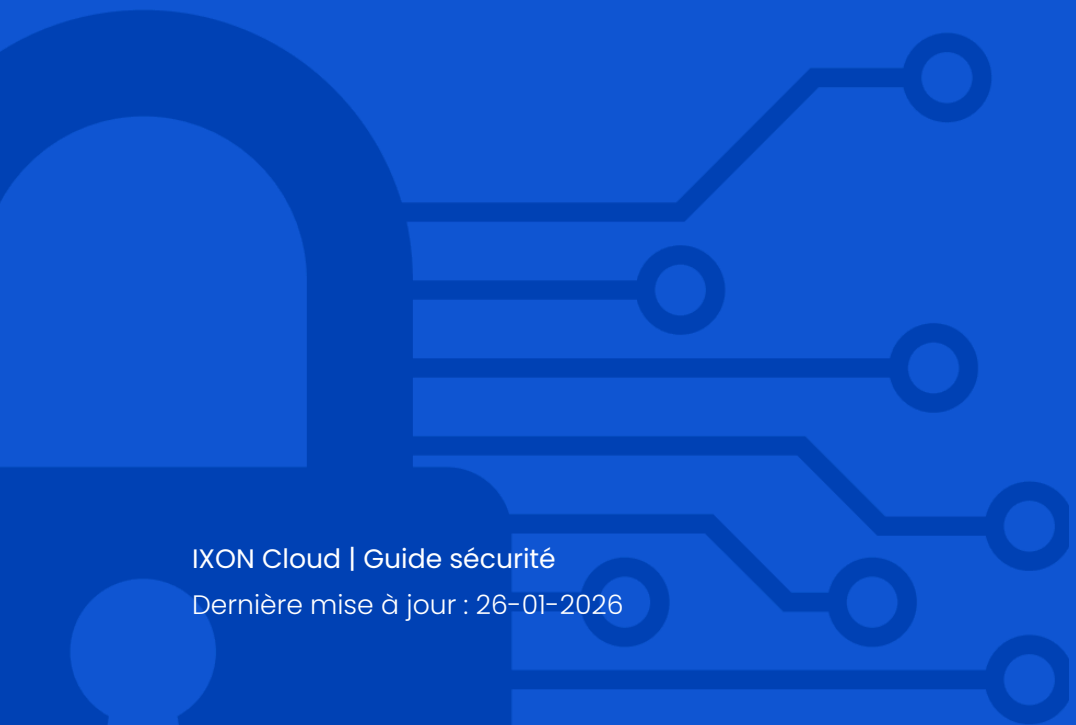
Guide de sécurité IXON



Dernière mise à jour : 26-01-2026

À propos de ce guide

Ce guide de sécurité IXON est conçu pour tous ceux qui utilisent IXON pour connecter leurs machines industrielles, des constructeurs de machines intégrant des passerelles Edge aux entreprises utilisant IXON Cloud.

Bien qu'IXON fournisse des outils de sécurité intégrés et une plateforme cloud sécurisée, la sécurité de vos systèmes connectés dépend de la configuration adéquate de ces outils au sein de votre environnement opérationnel. Il s'agit d'un effort collectif pour garantir la sécurité de vos systèmes.

Ce manuel vous servira de guide pratique. Nous vous expliquerons en détail :

- Les principes de base d'une connexion sécurisée machine-cloud.
- Un aperçu de l'architecture de sécurité du cloud IXON.
- Notre engagement en matière de sécurité passe par les certifications et la conformité.
- Recommandations pour vous aider à configurer et à gérer en toute sécurité vos comptes IXON Cloud, vos utilisateurs et vos périphériques Edge Gateway.

Notre objectif est de vous fournir les connaissances et les meilleures pratiques nécessaires pour minimiser les risques et maintenir une sécurité optimale tout au long du cycle de vie de vos machines connectées.

Nous sommes là pour vous aider. Si quelque chose n'est pas clair, n'hésitez pas à nous contacter à l'adresse suivante : security@ixon.cloud.



Dylan Eikelenboom
Responsable sécurité



Stan van Duijnhoven
Responsable conformité sécurité

Table des matières

À propos de ce guide 2
Table des matières 3
La cybercriminalité dans le secteur manufacturier 4
Introduction à IXON 5
Explication de la connexion machine-cloud 6
Au sein de la plateforme IXON Cloud 7
Sécurité et IXON 9
Certifications et conformité 9
Infrastructure cloud 10
Mesures techniques et organisationnelles 11
Ressources supplémentaires 11
Recommandations de mise en œuvre 12
Sécurité du cloud IXON 12
Sécurité de la passerelle Edge 14
Liste des tiers 17
Résumé 18

La cybercriminalité dans le secteur industriel

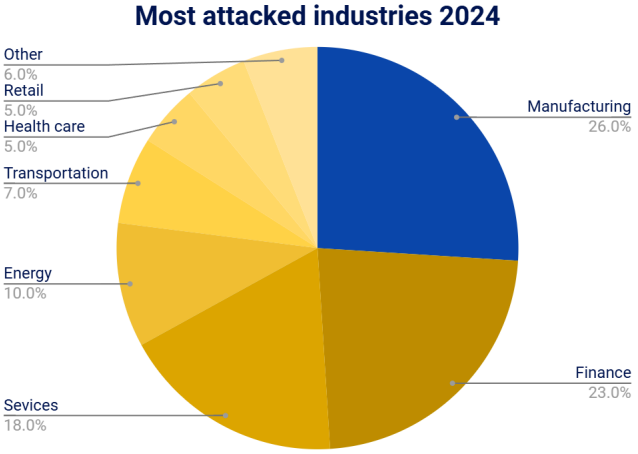
La cybercriminalité est devenue l'une des plus grandes menaces pour les industries du monde entier. Le secteur manufacturier est devenu une cible privilégiée des cybercriminels. Avec l'intégration croissante des technologies dans les chaînes de production et les processus industriels, la surface d'attaque s'accroît également. Les responsables d'usine doivent, plus que jamais, faire preuve de vigilance lors de l'introduction de nouvelles machines dans leur environnement.

Ransomware : un risque majeur pour les fabricants

L'un des risques de sécurité auxquels sont confrontées les machines est le ransomware, qui chiffre les données de l'entreprise et exige une rançon pour leur déchiffrement. Cette forme de cybercriminalité peut interrompre la production, engendrer des pertes financières considérables et nuire à la réputation. Compte tenu des impératifs de disponibilité des équipements et de la protection de la propriété intellectuelle dans le secteur manufacturier, un ransomware peut s'avérer particulièrement dévastateur. Imaginons une attaque sur une machine en pleine période de pointe : l'arrêt de la production et le montant de la rançon peuvent avoir des conséquences financières désastreuses.

Le paradoxe des entreprises : la nécessité de la connectivité au cloud

Dans le contexte concurrentiel actuel, il est pratiquement impensable de concevoir des machines de production sans connexion au cloud. Cette connectivité permet l'analyse des données en temps réel, la maintenance prédictive et l'intégration avec d'autres systèmes. La surveillance à distance des indicateurs de performance, où que l'on soit, rationalise les opérations et réduit considérablement les temps d'arrêt machine. De plus, la maintenance peut être effectuée précisément au moment opportun, ce qui représente un gain de temps et de ressources. Cette connectivité souligne l'importance de la sécurité. Les risques peuvent être minimisés en adoptant les mesures détaillées dans ce document.



Source: IBM X-Force Threat Intelligence Index 2025

Introduction à IXON

Le constructeur de machines de demain est un prestataire de services. Son fondement même repose sur la connexion physique avec les machines de ses clients. Qu'il s'agisse d'accès à distance ou de développement de nouveaux services basés sur les données machines, sans cette connexion, rien n'est possible. IXON, la plateforme IoT industrielle conçue pour les constructeurs de machines, offre la solution la plus sûre et la plus fiable pour rester connecté aux machines et aux clients du monde entier.

Accès à distance intégré

De nombreuses solutions d'accès à distance sont des outils autonomes, déconnectés de votre stratégie IoT globale et de votre infrastructure informatique. Cette déconnexion entrave la circulation fluide des données et des informations. IXON est la seule plateforme IoT intégrant l'accès à distance. Elle permet aux constructeurs de machines de gérer leurs machines et leurs utilisateurs depuis une plateforme unique, pour l'accès à distance et les services IoT. De ce fait, elle se positionne comme l'une des solutions les plus complètes et performantes du marché.

Plateforme IoT complète

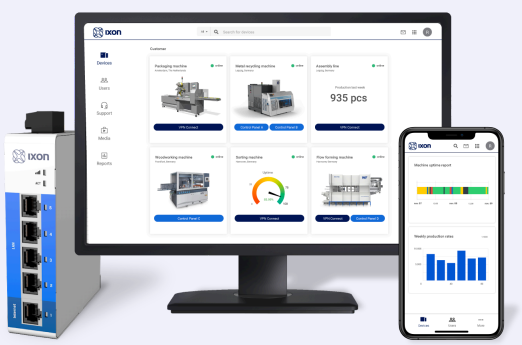
Créez votre propre plateforme IoT sans investissement initial important ni long projet de développement logiciel. IXON est une plateforme IoT industrielle complète et facile à mettre en œuvre, dotée de nombreuses fonctionnalités intégrées.

Ouvert et extensible

Chaque constructeur de machines ayant des exigences spécifiques, notre plateforme IIoT ouverte et évolutive offre des possibilités illimitées. Nous nous intégrons à vos applications informatiques existantes via des API et vous permettons de développer des applications web personnalisées. Pérennisez votre stratégie de services avec IXON.

Intégration transparente de la machine au cloud

Les passerelles Edge d'IXON sont fournies avec la plateforme IXON Cloud. Développées en interne par IXON, elles constituent un élément essentiel de son offre. Garantir une connectivité fiable et sécurisée optimale entre les machines et le cloud exige une intégration matérielle et logicielle parfaite.



Notre mission

La mission d'IXON est de mettre en relation les constructeurs de machines et leurs clients. Nous croyons qu'une étroite collaboration entre les industriels et les constructeurs est la clé pour améliorer la production et construire un monde plus durable où les machines fonctionnent en continu.

Explication de la connexion machine-cloud

La machine se connecte au cloud IXON via une passerelle IXON Edge. Cette passerelle est montée sur un rail DIN dans l'armoire électrique de la machine.

Pare-feu

La passerelle edge est un pare-feu qui sépare le réseau interne des machines des réseaux OT et IT de l'usine de production. Cette séparation est essentielle car les composants des machines ne sont pas conçus pour la sécurité et ne sont souvent pas mis à jour pour respecter les dernières normes de sécurité. Ainsi, le trafic entre les composants des machines et le réseau informatique de l'usine ainsi qu'Internet doit être réduit au minimum.

Systèmes SCADA et MES

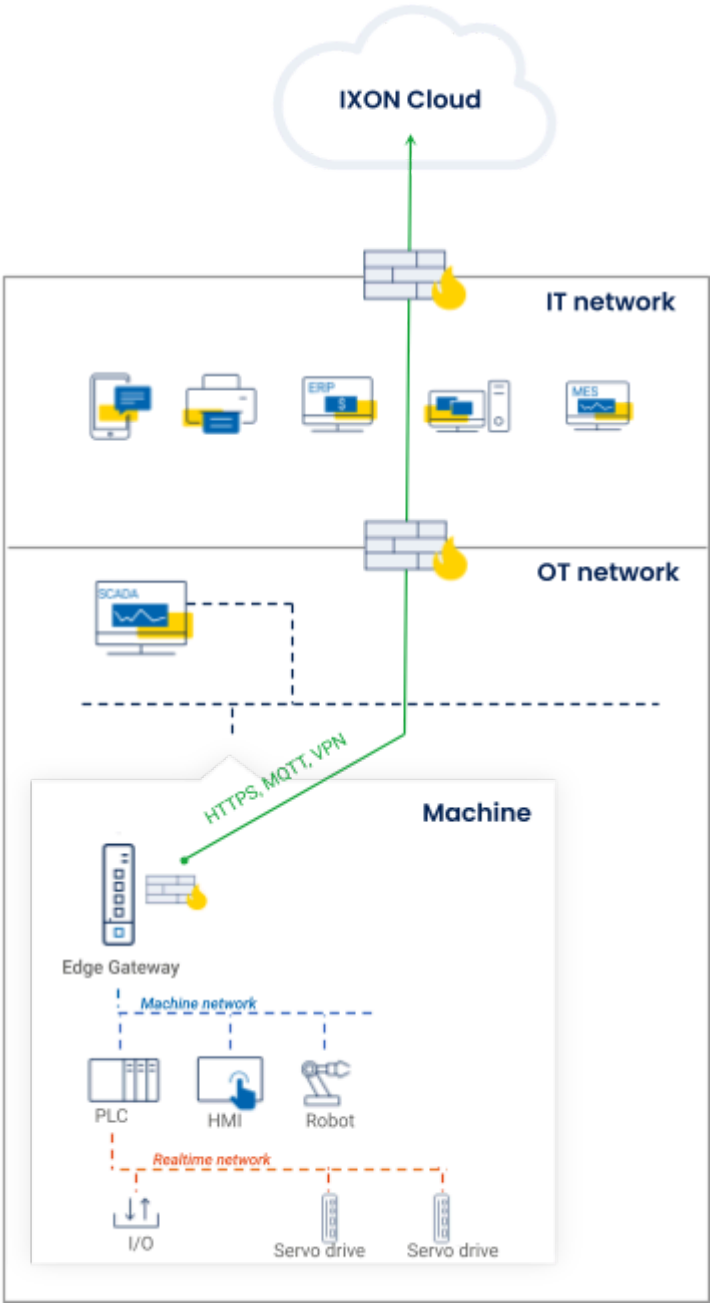
Les paramètres du pare-feu de la passerelle edge peuvent autoriser la communication entre la machine et les systèmes SCADA/MES.

Communication sortante

La passerelle edge communique avec IXON Cloud uniquement via des connexions sortantes. Ceci garantit que toutes les connexions entrantes du pare-feu local restent fermées.
Plus de détails sur les ports du pare-feu.

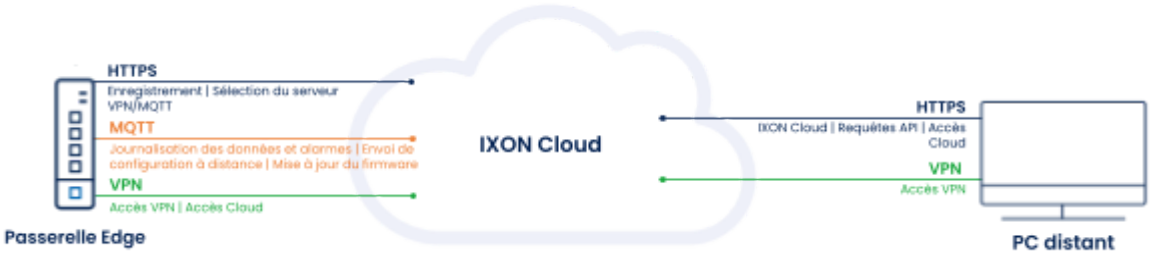
La passerelle edge possède 3 connexions au cloud IXON :

- HTTPS pour enregistrer l'appareil et sélectionner les serveurs VPN/MQTT.
- MQTT pour la configuration à distance, les mises à jour du firmware, l'envoi de données et d'alertes machine.
- VPN pour l'accès à distance.



Au sein de la plateforme IXON Cloud

La transparence est essentielle pour instaurer la confiance. C'est pourquoi nous souhaitons partager des informations sur la technologie qui sous-tend la plateforme IXON Cloud. Cette section vous fournit des informations générales qui peuvent s'avérer utiles pour votre propre évaluation de la sécurité d'IXON. Des informations détaillées sont disponibles sur demande.



Services API

Les services API sont au cœur d'IXON Cloud et sont hébergés dans des datas centers à Amsterdam. Ils gèrent des processus clés d'IXON Cloud, notamment l'autorisation, la configuration des connexions VPN et la récupération des données de nos bases de données.

Services broker MQTT

Les services de broker MQTT d'IXON sont utilisés pour la diffusion des configurations des appareils, l'envoi de commandes de mise à jour du firmware et la transmission des données d'enregistrement ainsi que des notifications d'alarme. Les services de broker MQTT sont hébergés dans des data centers situés à Amsterdam.

Serveurs VPN

Les serveurs VPN d'IXON sont répartis dans des data centers à travers le monde afin de garantir des connexions à faible latence. Le réseau de serveurs VPN intègre une redondance : si un serveur tombe en panne, les autres prennent automatiquement le relais.

L'API détermine le serveur VPN le plus adapté à l'établissement d'un tunnel VPN sécurisé, en fonction de l'emplacement physique de la passerelle IXON et du serveur VPN le plus proche. Voir statut.ixon.cloud pour obtenir un aperçu actuel de l'emplacement des serveurs.

De l'autre côté du tunnel, notre client VPN est une application légère qui s'exécute en arrière-plan sur votre ordinateur. Vous pouvez configurer une connexion VPN sécurisée à votre machine directement depuis votre navigateur.



Même pour les ordinateurs sans connexion VPN, il est possible d'accéder à l'IHM ou aux commandes web de vos machines. Avec EasyControl, les données machine sont transmises via la passerelle Edge au serveur VPN grâce à la connexion VPN déjà établie. Ces informations sont ensuite diffusées en continu vers votre navigateur via HTTPS ou une connexion WebSocket sécurisée.

Cluster Kubernetes

La plateforme IXON Cloud comprend plusieurs clusters Kubernetes pour l'exécution et la gestion de microservices. Cette architecture garantit une évolutivité et une disponibilité optimales. Les microservices permettent de structurer les applications de grande envergure comme un ensemble d'applications plus petites et faiblement couplées, pouvant être gérées et mises à jour individuellement, sans interruption de service. Chaque microservice est conçu comme un conteneur Docker.

Cluster de base de données relationnelle

La base de données relationnelle stocke les informations relatives aux utilisateurs, aux entreprises et aux appareils d'IXON Cloud. Elle est configurée de manière redondante selon une architecture primaire-secondaire répartie sur plusieurs data centers à Amsterdam. Le serveur primaire reçoit et traite toutes les requêtes de consultation ou de modification de la base de données. Le serveur secondaire réplique toutes les opérations d'écriture et de mise à jour effectuées sur le serveur primaire et crée une sauvegarde toutes les quatre heures.

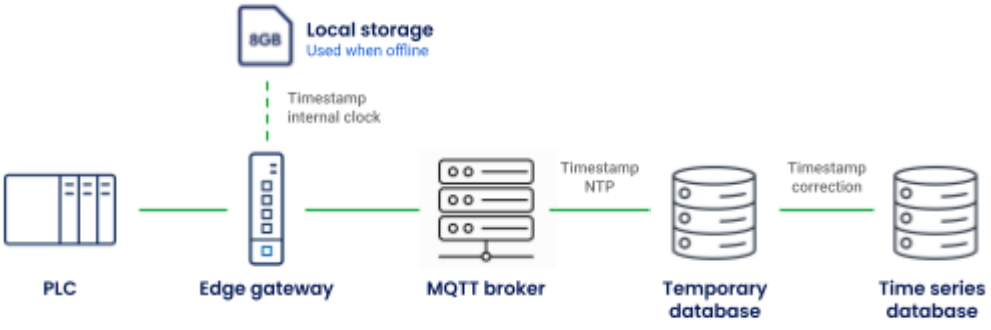
Cluster de base de données de séries temporelles

Les données machine collectées par l'enregistreur sont transmises par la passerelle edge via le protocole MQTT jusqu'à notre broker MQTT. Elles y sont horodatées et stockées dans une base tampon. Une correction temporelle compense tout décalage entre l'horloge interne de la passerelle et l'heure NTP (heure réelle).

Les données sont ensuite stockées dans un cluster de bases de données de séries temporelles hébergé à Francfort, en Allemagne. Ce type de base de données est conçu pour les données horodatées et se distingue par sa rapidité : il permet d'interroger de longues périodes en quelques millisecondes et de réaliser efficacement des opérations comme le calcul de moyennes. Il offre aussi des options avancées de gestion du cycle de vie des données, comme l'agrégation ou le sous-échantillonnage.

Cluster de bases de données non relationnelles

La base de données non relationnelle stocke les données relatives aux événements d'IXON Cloud, aux alarmes générées et aux journaux d'audit. Cette base de données est configurée en tant que jeu de réplicas : le serveur principal reçoit et traite toutes les requêtes, tandis que les serveurs secondaires répliquent le serveur principal afin de garantir une haute disponibilité et une redondance optimale. Les serveurs de la base de données sont répartis dans plusieurs data centers à Amsterdam.



Sécurité et IXON

En tant que fournisseur de solutions de cybersécurité OT, IXON commence par sécuriser sa propre organisation. La cybersécurité est intégrée à tous les processus et procédures internes grâce à un système de gestion de la sécurité de l'information (SMSI) et un système de gestion des informations relatives à la protection de la vie privée (PIMS) complets.

Certifications et conformité

Le système de gestion de la sécurité de l'information (SMSI) d'IXON est certifié conforme à la **norme ISO 27001.** Cette certification constitue la référence mondiale en matière de sécurité de l'information au sein des organisations. Elle impose la conformité à diverses exigences, notamment le contrôle d'accès, la cybersécurité, la formation et la sensibilisation, la conformité, la gestion des risques et la continuité des activités.

Par ailleurs, IXON est également certifié pour d'autres normes. Voici un aperçu complet :

Le système de gestion d'IXON est certifié pour :		
✓ ISO 9001	Qualité	Certificat
✓ ISO 27001	sécurité de l'information	Certificat
✓ ISO 27017	Sécurité du cloud	Certificat
✓ ISO 27701	Confidentialité	Certificat
✓ IEC 62443-4-1	Développement logiciel sécurisé	Certificat
✓ IEC62443-4-2	Composants matériels sécurisés	Certificat

Étendue de la certification

Le système SMSI et le système PIMS englobent toutes les activités commerciales d'IXON, y compris le développement de solutions de connectivité cloud, la production de passerelles edge, la gestion et la maintenance de la plateforme IXON Cloud et le traitement des informations personnelles identifiables.

En choisissant un périmètre aussi large pour la certification de notre SMSI, nous assurons la protection des données dans IXON Cloud et dans nos systèmes internes.

Infrastructure cloud

IXON Cloud est un réseau avancé de plus de 150 serveurs répartis dans le monde entier, optimisé pour des performances, une disponibilité et une sécurité maximales. Ces serveurs sont hébergés par des fournisseurs spécialisés, respectant des normes de sécurité rigoureuses et certifiés ISO 27001.

Tous les serveurs traitant les données sont situés dans l'Union européenne, garantissant ainsi la conformité au RGPD.

Voici quelques mesures clés pour maintenir la sécurité des serveurs :

- Installation automatisée des mises à jour de sécurité et blocage du trafic réseau inutile.
- Surveillance serveur en temps réel 24h/24 et 7j/7 avec alertes immédiates en cas d'anomalie.
- Un système de gestion des informations et des événements de sécurité (SIEM) examine les données de sortie du serveur à la recherche d'activités suspectes.
- Analyses hebdomadaires des vulnérabilités par des tiers et tests d'intrusion réguliers sur la plateforme IXON Cloud et les passerelles edge.

Solutions sur site

IXON a fait le choix délibéré de ne pas proposer de solutions serveur sur site, en raison des risques associés. Celles-ci nécessiteraient une surveillance et une maintenance continues, ainsi que des spécialistes de la sécurité dédiés. IXON privilégie une plateforme entièrement gérée (SaaS) dotée de mesures de sécurité robustes (voir la section Mesures techniques et organisationnelles).

Mesures techniques et organisationnelles

Pour une liste complète des mesures techniques et organisationnelles, voir le Trust Center d'IXON.

Ressources supplémentaires

Trust Center IXON	Plateforme centrale pour les informations relatives à la sécurité et à la conformité.
Conditions d'utilisation d'IXON Cloud	Détails de toutes les clauses juridiques relatives à l'utilisation d'IXON Cloud.
Déclaration de confidentialité d'IXON Cloud	Ce document explique en termes simples comment nous traitons vos informations personnelles et comment nous assurons leur sécurité.
Page d'état IXON	Affiche l'état actuel de la plateforme IXON Cloud et les éventuelles interruptions de service.
Avis de sécurité IXON	Ce répertoire contient des informations sur les incidents de sécurité passés, les versions et les mises à jour des produits et services IXON.

Bureau de sécurité et bureau juridique
Nous proposons une documentation complète, des formations et des outils. Pour les services numériques, les accords relatifs à la confidentialité, à la propriété et à la responsabilité des données sont essentiels. IXON peut vous aider à comprendre les accords conclus entre les constructeurs et les propriétaires de machines, ainsi qu'avec IXON. L'accès aux services de sécurité et juridiques d'IXON est gratuit.

E-mail : security@ixon.cloud
Téléphone : +31 (0)85 744 1105

Annexe A :

Recommandations de mise en œuvre

Les produits IXON nécessitent plusieurs choix concernant les paramètres, les fonctionnalités et les connexions, ce qui a un impact direct sur les risques de sécurité. Les paramètres par défaut de la passerelle IXON Edge sont configurés de manière stricte, tout en restant compatibles avec une machine standard. Ce chapitre vous propose des étapes pratiques pour utiliser votre environnement IXON en toute sécurité et garantir la protection de vos machines.

Il est important de préciser que les points ci-dessous constituent des bonnes pratiques générales. Vous pouvez légitimement vous en écarter : par exemple, en raison de la politique de l'entreprise, de vos préférences personnelles ou d'un cas d'usage particulier. N'hésitez pas à le faire, mais soyez conscient des risques de sécurité potentiels que cela peut engendrer.

Sécurité du cloud IXON

✔ Utilisez des identifiants de compte robustes
Lors de la création de votre compte, choisissez un mot de passe robuste : long, unique et difficile à deviner. Activez l'authentification à deux facteurs pour renforcer la sécurité de votre compte en exigeant une deuxième méthode de vérification. Ces deux étapes rendent l'accès à votre compte pratiquement impossible pour les personnes non autorisées.

✔ Gérer les autres utilisateurs
L'utilisateur qui crée la société IXON Cloud aura automatiquement des droits d'administrateur et pourra inviter d'autres utilisateurs sur la plateforme. Réfléchissez bien aux personnes à inviter. Voici quelques bonnes pratiques :

- N'invitez que les personnes qui ont besoin d'accéder à IXON Cloud.
- Prévenez ces personnes en amont.
- Vérifiez et revérifiez les adresses e-mail.
- Invitez les personnes uniquement via des adresses e-mail nominatives (par exemple, pas info@company.com).
- Accordez aux utilisateurs uniquement ce dont ils ont besoin (voir la section suivante).
- Ajoutez un message expliquant la nécessité d'utiliser des mots de passe robustes.
- Si les utilisateurs n'ont besoin que d'un accès temporaire, n'oubliez pas de définir une date d'expiration.

Pour garantir que tous les utilisateurs de votre entreprise utilisent des identifiants robustes, nous recommandons vivement aux administrateurs d'imposer l'authentification à deux facteurs pour tous les utilisateurs.

✔ Appliquer le principe du moindre privilège
N'accordez aux utilisateurs que les autorisations nécessaires à l'exercice de leurs fonctions, et rien de plus. Limitez également leur accès aux seules passerelles edge dont ils ont besoin. En règle générale, il est préférable d'accorder temporairement des privilèges élevés à un utilisateur plutôt que de lui octroyer par défaut des autorisations dont il n'aura probablement jamais besoin.

Soyez particulièrement vigilant avec les autorisations « Gérer les utilisateurs » et « Gérer les rôles », car elles vous permettent d'inviter d'autres utilisateurs et de définir des permissions. Pour plus de simplicité, créez des rôles et des groupes d'utilisateurs descriptifs afin de gérer plusieurs utilisateurs simultanément.

✔ Enregistrer rapidement les départs
Lorsqu'une personne quitte l'entreprise ou change de poste, évaluez son accès à IXON Cloud dès que possible. Mettez à jour ses autorisations en conséquence ou supprimez-les.

✔ Ne laissez les sessions ouvertes que sur les appareils de confiance.
Lors de la connexion, vous pouvez choisir de « rester connecté », ce qui prolonge la session (la période pendant laquelle vos identifiants ne vous seront pas demandés) de 24 heures à 30 jours. Cette option facilite l'utilisation sur les appareils protégés dont vous êtes le seul utilisateur, mais représente un risque pour les appareils partagés ou empruntés. De même, sur ces appareils, n'oubliez pas de vous déconnecter une fois que vous avez terminé d'utiliser IXON Cloud. Il est recommandé de vérifier régulièrement vos sessions actives et de révoquer celles qui ne devraient plus l'être.

✔ Examiner l'activité IXON Cloud
La consultation régulière du journal d'audit vous permet d'identifier toute activité inhabituelle ou suspecte au sein de votre entreprise. Ce journal enregistre toutes les actions effectuées sur votre compte, notamment les connexions, les modifications des autorisations utilisateur, etc. Pensez également à prendre le temps de vérifier régulièrement tous les aspects de sécurité d'IXON Cloud : utilisateurs, autorisations, sessions, identifiants, etc.

Sécurité de la passerelle edge

✔ Installez de nouveaux appareils en toute sécurité

Les nouvelles passerelles edge doivent être installées de manière sécurisée. Il est primordial de limiter l'accès physique à la passerelle et aux automates programmables en les installant dans une armoire ou une pièce verrouillée. En effet, un accès physique à la passerelle ou à la machine permet de s'y connecter directement, en contournant le pare-feu.

L'enregistrement de la passerelle auprès d'IXON Cloud s'effectue généralement à l'aide d'un fichier de configuration (*ixrouter.conf)* sur une clé USB. Après l'enregistrement, nous vous recommandons de retirer la clé USB de l'appareil. Lorsqu'elle est insérée, la passerelle Edge y enregistre des informations de journalisation à des fins de débogage, lesquelles peuvent contenir des informations confidentielles. Nous vous recommandons également de supprimer le fichier *ixrouter.conf* qui se trouve sur la clé USB. En règle générale, il ne contient aucune information confidentielle, sauf si vous configurez la passerelle Edge pour une connexion Wi-Fi authentifiée. Ce fichier peut toutefois servir à enregistrer d'autres passerelles Edge dans votre plateforme IXON Cloud.

Enfin, il est important de modifier le mot de passe de l'interface web de la passerelle. Le mot de passe initial est unique pour chaque appareil, mais il est imprimé sur l'étiquette et peut être repéré par toute personne ayant un accès physique. Après l'avoir utilisé pour la première connexion, choisissez un mot de passe long, unique et difficile à deviner.

✔ Configurer le basculement

Si possible, configurez les passerelles périphériques pour utiliser le Multi-WAN, ce qui leur confère des capacités de basculement en cas d'interruption de leur connexion Internet principale.

✔ Activer le contrôle local de l'accès à distance

Connectez un interrupteur à bascule à l'entrée numérique de la passerelle Edge pour choisir quand autoriser les connexions VPN. Ainsi, les opérateurs contrôlent localement l'accès distant et EasyControl.

✔ Mettre à jour le firmware

Nous vous recommandons vivement de mettre à jour vos appareils dès qu'un correctif de sécurité est disponible. Toutefois, il est généralement conseillé de procéder à la mise à jour à chaque nouvelle version. Bien que toutes les nouvelles versions de firmware ne contiennent pas de correctifs de sécurité, elles apportent des améliorations de stabilité, de nouvelles fonctionnalités et des corrections de bugs. La liste des modifications et améliorations est consultable sur la plateforme IXON Cloud ou dans nos notes de version.

✔ Autoriser le trafic nécessaire

Pour permettre à la passerelle IXON d'accéder à la plateforme IXON Cloud via Internet, vous devez autoriser le trafic réseau sortant valide dans le pare-feu local. Utilisez des règles de pare-feu précises pour n'autoriser que le trafic nécessaire. La communication de la passerelle Edge présente les caractéristiques suivantes :

- La passerelle IXON communique via TCP avec le port de destination 443*
- Les adresses IP répertoriées sur whitelist.ixon.cloud sont des destinations valides
- Les domaines IXON se terminent par .ixon.net ou .ayayot.com

Le trafic peut utiliser le port 8443 en mode VPN furtif ou le port 53 pour les requêtes DNS.

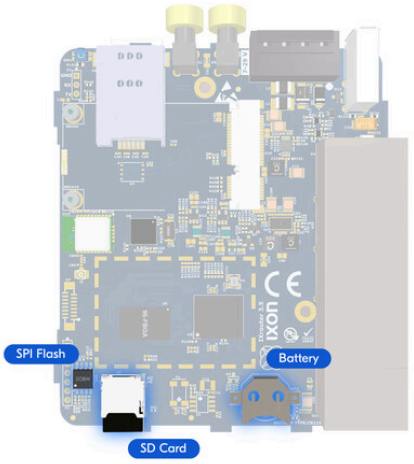
✔ Restreindre le pare-feu

Par défaut, le pare-feu de la passerelle Edge est configuré de la manière la plus restrictive possible. Ne modifiez les règles de pare-feu qu'en cas de nécessité afin d'éviter tout accès non autorisé. Des modifications telles que l'autorisation du trafic LAN vers WAN augmentent le risque de trafic malveillant. Consultez l'image ci-dessous pour identifier les pièges potentiels :

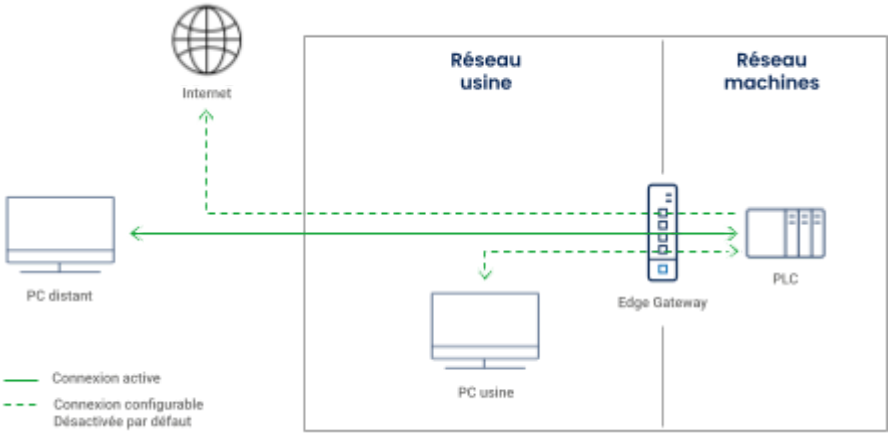
✔ Éliminer les appareils mis hors service

Lorsqu'un appareil est désinstallé puis réutilisé dans un autre environnement, il est conseillé de le réinitialiser aux paramètres d'usine et de le supprimer de la plateforme IXON Cloud. Il pourra ensuite être utilisé comme un appareil neuf.

Si un appareil est mis hors service, il peut, dans certains cas, contenir des données confidentielles ; la puce **SPI Flash** contient des clés d'authentification utilisées pour s'identifier en tant que passerelle périphérique IXON, et la **carte SD** peut contenir des données de journalisation du système ainsi que des vidages de mémoire suite à un plantage. Veuillez ouvrir le boîtier et retirer ou détruire ces composants.



Nous vous recommandons également de retirer la pile bouton et de vous en débarrasser de manière écologique.



Communication

✔ Restez informé(e) des événements, mises à jour et modifications liés à la sécurité

Pour vous tenir informé(e) de tout ce qui concerne directement et indirectement la sécurité, veuillez consulter les sources suivantes :

- statut IXON (statut.ixon.cloud) - Affiche l'état actuel de la plateforme IXON Cloud et toute interruption de service potentielle.
- Avis de sécurité IXON (support.ixon.cloud) - Contient les dernières informations concernant les incidents de sécurité, les versions et les mises à jour pour tous les produits et services IXON.
- notes de version d'IXON (answers.ixon.cloud) - Liste toutes les mises à jour logicielles de la plateforme IXON Cloud, des passerelles périphériques ou du client VPN.

Annexe B :

Liste des tiers

Pour une liste complète des tiers, consultez le Trust Center d'IXON.

Résumé

IXON se consacre à la fourniture d'une plateforme IoT industrielle sécurisée qui améliore la collaboration entre les constructeurs de machines et les entreprises de production pour une performance optimale. Grâce à des serveurs redondants à l'échelle mondiale et à des contrôles de sécurité complets, nous offrons une solution agile et fiable qui vous assure une totale tranquillité d'esprit.

La confiance de plus de 2 500 entreprises à travers le monde, soit plus de 70 000 machines connectées, ne se gagne pas facilement. Elles ont choisi IXON car elles savent qu'investir dans notre technologie se traduit par des avantages concrets et une croissance tangible. Grâce à une innovation constante, nous nous efforçons d'aider nos utilisateurs à tirer le meilleur parti de leurs investissements.

Chez IXON, nous assumons avec fierté la responsabilité de protéger votre bien le plus précieux. La sécurité n'est pas qu'une promesse ; elle est inscrite dans l'ADN de tout ce que nous faisons.

Approuvé par des constructeurs de machines du monde entier

Siège social d'IXON
Beugen, Pays-Bas
tél. +31 85 744 1105

www.ixon.cloud

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

