

Sirix

Protection de sites grâce à la vidéosurveillance alimentée par l'IA Sirix

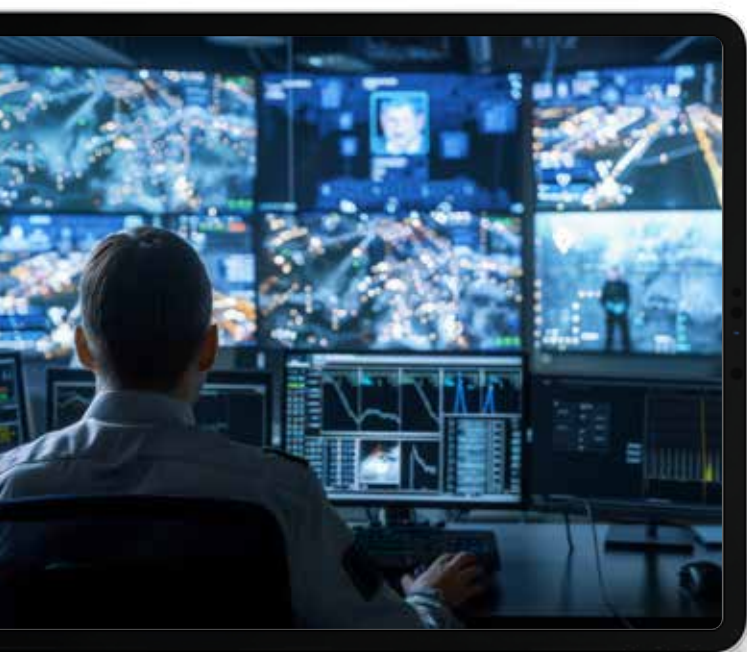
Votre guide d'installation et de performance



Propriété intellectuelle, politique d'utilisation et mises à jour

Quatrième édition.

Publiée: Février 2026



Ce guide fournit des informations complètes sur l'installation des caméras de sécurité, les meilleures pratiques en matière de vidéosurveillance à distance et les directives pour une détection efficace afin de garantir une protection optimale du périmètre. Il comprend également des informations détaillées sur toutes les solutions Sirix, des instructions étape par étape pour les techniciens sur site, des conseils pour établir des connexions, utiliser divers outils en ligne et contacter notre Support.

Toute utilisation, reproduction ou distribution non autorisée de ce guide, en tout ou en partie, sans l'autorisation écrite préalable de Sirix, est strictement interdite.

Copyright © 2025 par Sirix. Tous droits réservés. Produit au Canada.

Veuillez noter que les informations contenues dans ce guide peuvent devenir obsolètes à mesure que la technologie évolue. Pour vous assurer de disposer des informations les plus récentes, veuillez contacter Sirix afin d'obtenir la dernière version de ce guide.

Table des matières

Introduction	05
1. Canaux de communication	06
2. Installation des caméras de sécurité	07
2.1 Points clés à considérer	07
• Emplacement de la prise électrique	
• Installation le long du périmètre ou sur la structure du bâtiment	
• Transmission du signal IA	
2.2 Résolution des problèmes d'alimentation et de signal	08
• Fonctionnement sans électricité	
• Fonctionnement sans connexion Internet ou Wi-Fi	
• Fonctionnement sans couverture réseau LTE	
2.3 Résumé	09
3. Optimisation de la couverture et de la détection des caméras	10
3.1 Chevauchement des caméras	10
3.2 Détection des objets	10
3.3 Comprendre la couverture des caméras et les valeurs PPM recommandées	11
3.4 Hauteur et angle optimaux pour la détection	12
3.5 Optimisation de la précision et de la performance de détection	13
• Temps de détection	
• Contraintes liées à la détection et à la vitesse	
• Restrictions pour les caméras fisheye	
3.6 Points clés à considérer	14
3.7 Résumé	15
4. Connexion au centre de commandement de Sirix	16
4.1 Comment connecter un nouveau site	16
4.2 Comment connecter des haut-parleurs	18
4.3 Tests sur site	19
• Autotests	
• Test de marche sur site avec Sirix	
• Test des haut-parleurs réalisé par Sirix	
• Pourquoi les tests sont-ils importants ?	
4.4 Connexion VPN	20
4.5 Liste de contrôle pour les techniciens sur site	21
4.6 Problèmes de connexion et vérification de l'état des appareils de sécurité	22
• Comment Sirix gère les problèmes de connexion	
• Vérification de l'état de la caméra, du NVR et du VMS	
• Vérification de l'état des haut-parleurs	
• Surveillance des coupures de courant	
4.7 Comment relier les appareils de sécurité pour déclencher des événements	25
• Boutons d'urgence, contacts de porte et détecteurs de mouvement	
• Panneaux d'alarme	
4.8 Application mobile Sirix	26
• Installation et identifiants d'accès	
• Gérer la sécurité du site, visionner les images et suivre les performances	
4.9 Stratégies efficaces d'armement et de désarmement	27
4.10 Conditions requises pour un accès administrateur complet	28

4.11	Durée de conservation des vidéos d'incidents	28
4.12	Processus complet d'activation du compte Sirix	29
5.	Réponse aux alarmes et protocole d'intrusion	31
5.1	Processus de gestion des alarmes	31
5.2	Protocoles de sécurité	32
	- Script et processus des interventions vocales - Interventions vocales personnalisées - Autres procédures de sécurité - Actions entreprises pour compléter les procédures de sécurité - Étapes d'une intervention vocale - Installation optimale des haut-parleurs	36
5.3	Équipe d'audit Sirix	36
6.	Rapports	37
6.1	Rapports d'incidents	37
6.2	Rapports de problèmes	37
6.3	Destinataires des rapports	38
6.4	Masquage, sites et changements de configuration de l'IA	39
7.	Détection de fumée et de feu par l'IA Sirix	40
7.1	Définition du modèle	40
7.2	Fonctionnement	40
7.3	Fonctions supplémentaires du modèle	40
7.4	Attentes en matière de faux positifs	41
7.5	Exigences techniques	41
7.6	FAQs	41
8.	Conditions particulières	42
8.1	Politiques de surveillance et de facturation	42
8.2	Politique pour les sites délinquants	43
8.3	Ressources supplémentaires	43
8.4	Procédures de déconnexion (surveillance en direct)	44
9.	Maintenance proactive des systèmes de sécurité	45
10.	Au-delà de la vidéosurveillance – Moyens de dissuasion essentiels	46
10.1	Clôtures	46
10.2	Bornes de sécurité	46
10.3	Barrières	46
10.4	Serrures	47
10.5	Renforts de serrures	47
10.6	Panneaux d'avertissement	47
10.7	Éclairage	48
11.	Liens utiles	49
11.1	Liste des prix	49
11.2	Partenaires d'intégration	49
11.3	Support à l'intégration	49
11.4	Formulaires	49
11.5	Portail des événements	49
11.6	Calculateur FFP	49
11.7	Helpdesk	49



Maîtriser la protection périmétrique avec Sirix

La sécurité périmétrique représente la première ligne de défense d'un site. Elle joue un rôle essentiel en permettant de détecter et de dissuader les menaces avant qu'elles n'atteignent les zones sensibles. Un système bien conçu assure la protection des personnes et des biens, limite les risques et prévient toute escalade d'incident.

Ce guide d'installation et de performance propose des instructions claires et structurées, étape par étape, pour l'installation, la configuration et l'intégration des appareils de sécurité avec le centre de commandement intelligent de Sirix, propulsé par l'intelligence artificielle. Il couvre notamment :

- La configuration des appareils : caméras, enregistreurs NVR, alarmes et haut-parleurs;
- Le paramétrage des alarmes, des zones de détection et du masquage;
- L'exploitation des fonctions avancées telles qu'AktivSense, permettant la surveillance en temps réel de l'état des dispositifs ainsi que l'analyse intelligente des données via l'IA.
- La réalisation de tests de validation sur site et la mise en place d'interventions vocales.

Conçu pour assurer une installation optimale et une intégration harmonieuse, ce guide vous accompagne dans l'exploitation complète des solutions Sirix, afin de déployer une protection périmétrique fiable, cohérente et hautement performante.

Canaux de communication

Pour toute assistance, veuillez contacter l'équipe concernée en utilisant les coordonnées ci-dessous.



Opérations

Pour toute demande liée à l'intégration, au site client ou à la surveillance :

- Téléphone : 1-855-788-1919
- Courriel : operation@sirixmonitoring.com



Support

Pour toute question technique ou pour obtenir de l'aide concernant la connexion des sites :

- Téléphone : 1-866-765-6667
- Courriel : support@sirixmonitoring.com



Facturation

Pour toute question relative à la facturation :

- Courriel : billing@sirixmonitoring.com

Installation efficace des caméras de sécurité

Une installation optimale des caméras est essentielle pour garantir une sécurité périmétrique efficace. Les caméras doivent être installées de façon à offrir un champ de vision dégagé, sans obstruction, afin de permettre aux outils d'analyse de détecter avec précision les mouvements et de classer correctement les objets. Un mauvais positionnement peut générer des angles morts, facilitant ainsi le contournement du système par des intrus, qui pourraient accéder aux lieux sans être détectés.

Emplacement des prises de courant

Pour assurer le bon fonctionnement de vos appareils de sécurité, commencez par repérer l'emplacement des prises électriques sur votre site. Cette étape facilitera la conception d'un plan d'installation des caméras à la fois efficace et adapté à l'infrastructure existante.

Installation sur le périmètre ou sur le bâtiment

Assurer un champ de vision dégagé en limitant les obstacles

Installer les caméras uniquement sur le bâtiment peut créer des angles morts, les voitures stationnées ou d'autres objets pouvant bloquer la vue. L'installation des caméras le long du périmètre de la propriété permet une couverture claire des zones de stationnement et des points d'entrée, rendant plus difficile l'intrusion discrète.

Optimisation des performances de l'IA

Pour que l'intelligence artificielle des caméras puisse classer efficacement les objets, elle doit bénéficier d'une vue dégagée d'au moins une grande partie du corps d'une personne. Les caméras doivent être installées avec un angle horizontal ne dépassant pas 45 degrés. Les caméras montées sur les bâtiments ne répondent souvent pas à ces exigences, ce qui rend les caméras périmétriques cruciales pour une détection fiable.

Transmission du signal IA

Lorsque les caméras sont installées à plus de 90 mètres du bâtiment principal, leur signal IA doit être retransmis pour l'enregistrement et l'analyse. Il existe deux méthodes principales pour transmettre ce signal :

- **Antennes unidirectionnelles (solution sans fil)**

Utilisez des antennes, telles que celles proposées par [Ubiquiti](#), pour transmettre le signal sans fil vers le bâtiment principal.

- **Répéteurs PoE (solution filaire)**

Les appareils PoE (Alimentation par Ethernet) transmettent à la fois l'alimentation et les données via un seul câble Ethernet. [Veracity](#) propose des solutions PoE fiables pour connecter directement des caméras éloignées.

Résoudre les problèmes d'alimentation et de signal.

Sur de nombreux sites, tels que les chantiers de construction, l'alimentation électrique, Internet ou la couverture réseau peuvent être indisponibles. Nous fournissons des solutions pour surmonter ces défis et garantir une sécurité sans faille et fiable sur les sites.

Fonctionnement sans électricité

En cas d'absence d'électricité, un système de vidéosurveillance 4G LTE 5MP HD tout-en-un alimenté par batterie peut être rapidement déployé dans des zones reculées et est disponible à la location chez Sirix. Il offre une vue en direct et une détection à longue distance jusqu'à 45 mètres à un angle de 60°, garantissant une surveillance fiable sans source d'alimentation.

Fonctionnement sans connexion Internet ou Wi-Fi

Si vous ne disposez pas d'une connexion Internet ou Wi-Fi, deux options fiables s'offrent à vous : configurez votre propre réseau LTE à l'aide d'un routeur LTE, d'un commutateur PoE et d'une antenne externe en option pour améliorer la puissance du signal, ou utilisez le réseau existant de votre client en connectant votre système de sécurité à son infrastructure Internet sur site. Pour garantir une connectivité optimale, vous pouvez tester la vitesse du réseau sur speedtest.net.

Fonctionnement sans couverture réseau LTE

Si la couverture réseau LTE n'est pas disponible, deux solutions fiables garantissent une connectivité continue : les systèmes satellitaires ou fixes sans fil impliquent l'installation d'équipements tels que des antennes paraboliques ou des récepteurs, avec des forfaits adaptés à l'emplacement du site et à l'infrastructure disponible. Sinon, les satellites LEO (Low-Earth Orbit) + antennes offrent un accès Internet rapide et à faible latence grâce à une communication par constellation de satellites, garantissant une connectivité fiable même dans les zones reculées. Des fournisseurs tels que Starlink, HughesNet et Xplore proposent des solutions adaptées à divers environnements.

Résumé

Installation efficace des caméras de sécurité

Repérez les prises électriques

Commencez par localiser les prises électriques afin d'élaborer un plan d'installation des caméras qui soit en adéquation avec l'infrastructure de votre site.

Installez les caméras sur le long du périmètre

Évitez les obstructions. Placer les caméras le long du périmètre permet d'éviter que des éléments comme des véhicules ne bloquent la vue, assurant ainsi une couverture complète des zones de stationnement et des points d'entrée.

Optimisez la détection par intelligence artificielle. Pour que l'IA identifie correctement les objets, les caméras doivent offrir une vue claire avec un angle de prise de vue ne dépassant pas 45°. Les installations murales ne respectent souvent pas ces critères, ce qui peut nuire à la précision des analyses.

Transmettez efficacement le signal IA

Si les caméras se trouvent à plus de 90 mètres du bâtiment principal, le signal IA doit être relayé :

Solution sans fil. Utilisez des antennes unidirectionnelles, telles que celles proposées par Ubiquiti.

Solution câblée. Utilisez des prolongateurs POE, tels que Veracity ou Enable-it.

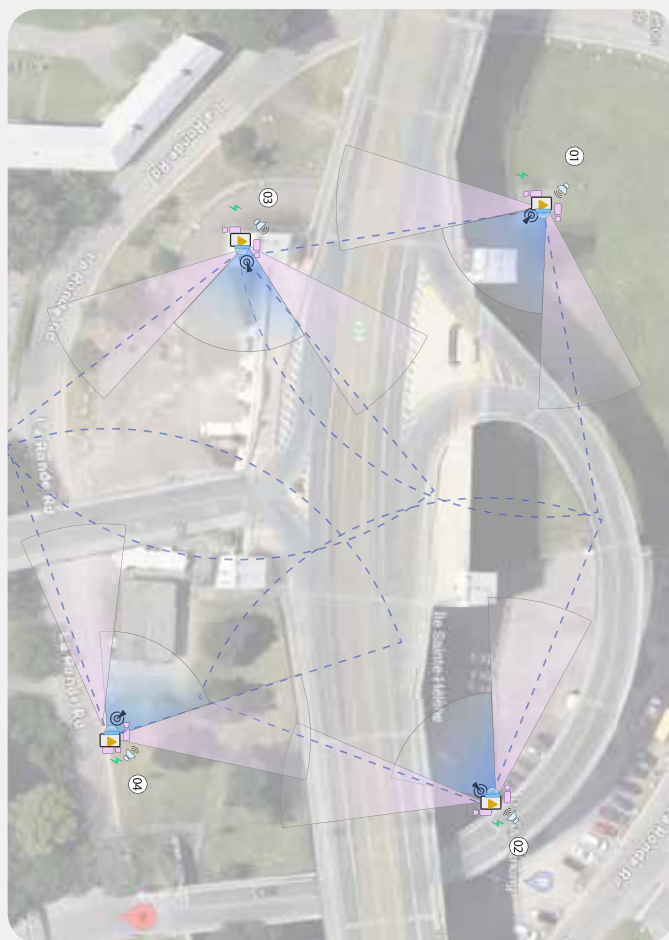
Relevez les défis liés à l'alimentation et à la connectivité

Pas d'électricité. Louez le système de sécurité vidéo HD 5MP tout-en-un 4G LTE alimenté par batterie de Sirix pour une surveillance fiable sans source d'alimentation.

Absence de connexion internet et de Wi-Fi. Configurez votre propre réseau LTE ou utilisez celui de votre client. Testez la vitesse du réseau sur : <https://www.speedtest.net>

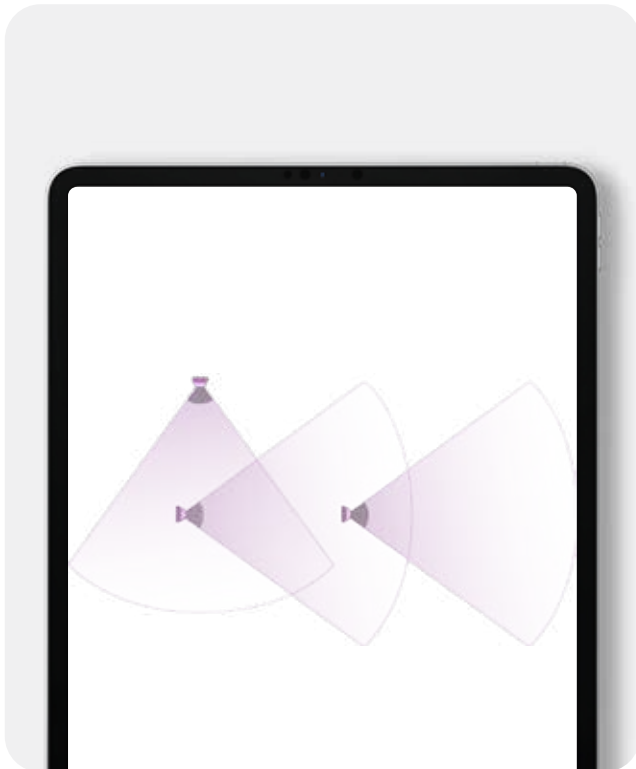
Absence de couverture réseau LTE. Utilisez des systèmes satellites ou sans fil longue portée, ou optez pour des solutions satellites en orbite basse (LEO) à faible latence pour les zones reculées (ex. : Starlink, HughesNet, Xplore).

Cette approche structurée garantit que le bon positionnement des caméras, dès la première étape, constitue la base d'une sécurité efficace.



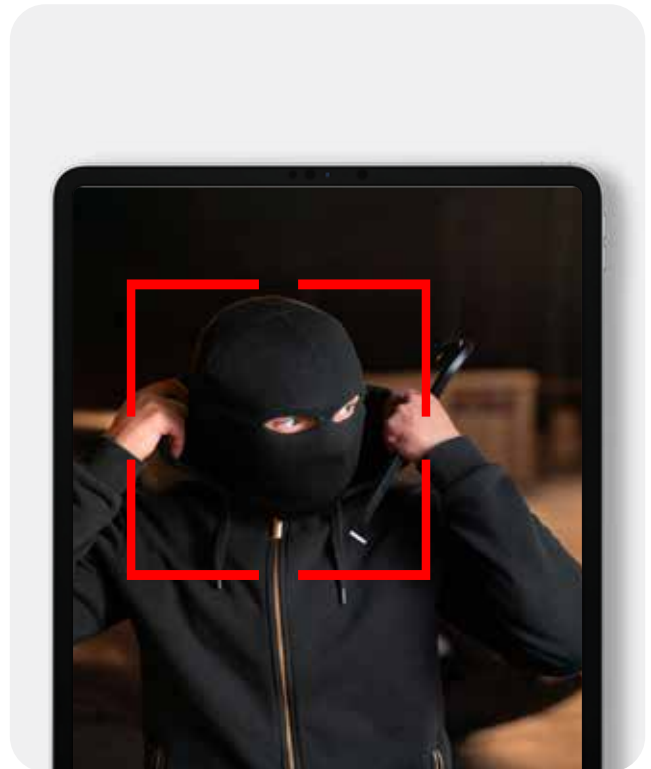
Sirix propose à ses partenaires des plans de sécurité complets, alliant efficacité, fiabilité et couverture intégrale.

Couverture et détection vidéo. Parfaitement optimisées.



Chevauchement des caméras. Le chevauchement se produit lorsque deux caméras surveillent une même zone sous des angles différents. Cette approche augmente considérablement les chances de détection. Si une caméra ne parvient pas à repérer un intrus en raison d'un angle trop prononcé ou d'une visibilité partielle du corps, l'autre caméra, placée sous un angle différent, pourra capter l'événement.

Pour une sécurité optimale, concevez votre plan de déploiement de caméras de manière à ce que toutes les zones sensibles soient couvertes par plusieurs angles de vue. Cela permet de réduire les angles morts et d'améliorer la capacité de détection.



Détection d'objets. La détection d'objets est une fonctionnalité essentielle de l'analyse vidéo, permettant aux caméras d'identifier et de suivre des éléments tels que des personnes, des véhicules ou d'autres objets dans leur champ de vision. Grâce à des algorithmes avancés, la caméra analyse le flux vidéo afin de reconnaître les objets d'intérêt et de déclencher des alertes.

Cette fonction agit comme le cerveau de la caméra, en interprétant ce qu'elle capte. Lorsqu'une personne ou un véhicule est détecté, le système envoie une alerte à l'équipe de sécurité et continue à suivre l'objet dans la zone couverte par la caméra, garantissant ainsi une réaction rapide et une surveillance efficace.

Comprendre la couverture d'une caméra

La portée et la précision de détection d'une caméra dépendent de trois paramètres essentiels.

- **Pixels per feet (PPF)**

Le PPF correspond à la densité minimale de pixels nécessaire pour qu'une caméra puisse correctement identifier des objets tels que des personnes ou des véhicules. Si la densité de pixels est trop faible, la caméra risque de ne pas reconnaître les objets avec précision, ce qui peut empêcher le déclenchement d'alertes.

- **Valeur mégapixel du moteur d'IA**

Les caméras n'utilisent pas toujours leur pleine résolution pour l'analyse. Le moteur d'intelligence artificielle traite la vidéo à une densité de pixels réduite afin d'optimiser les performances du processeur de la caméra. Il est donc essentiel de connaître la véritable résolution utilisée par l'IA lors de l'analyse pour garantir une détection fiable.

- **Champ de vision horizontal (HFOV)**

Le HFOV détermine la largeur du champ visuel de la caméra. Un champ de vision plus étroit augmente la portée de détection, tandis qu'un champ plus large réduit la distance de détection mais couvre une zone plus vaste.

Valeurs PPF recommandées – Références générales

Systèmes Sirix avec Cloud IA :

**5 PPF en
résolution 720p**

Systèmes Avigilon :

**9 PPF en
résolution 1080p**

Caméras de sécurité standards :

**9 PPF en résolution
480p**

Caméras de détection d'incendie :

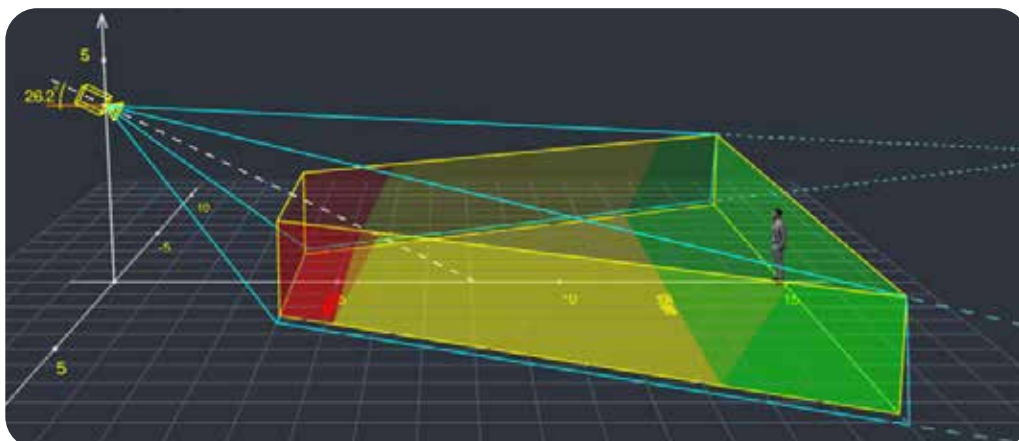
**3 PPF en résolution
640x480**

Consultez la notice pour vérifier les valeurs spécifiques de PPF, de mégapixels et de champ de vision horizontal (HFOV) propres à vos caméras; Pour effectuer des calculs complémentaires liés à la longueur focale de la lentille, à la densité de pixels et aux zones de couverture, utilisez un [calculateur de lentille CCTV](#).

La portée de détection dépend de l'angle et de la distance focale de la caméra.

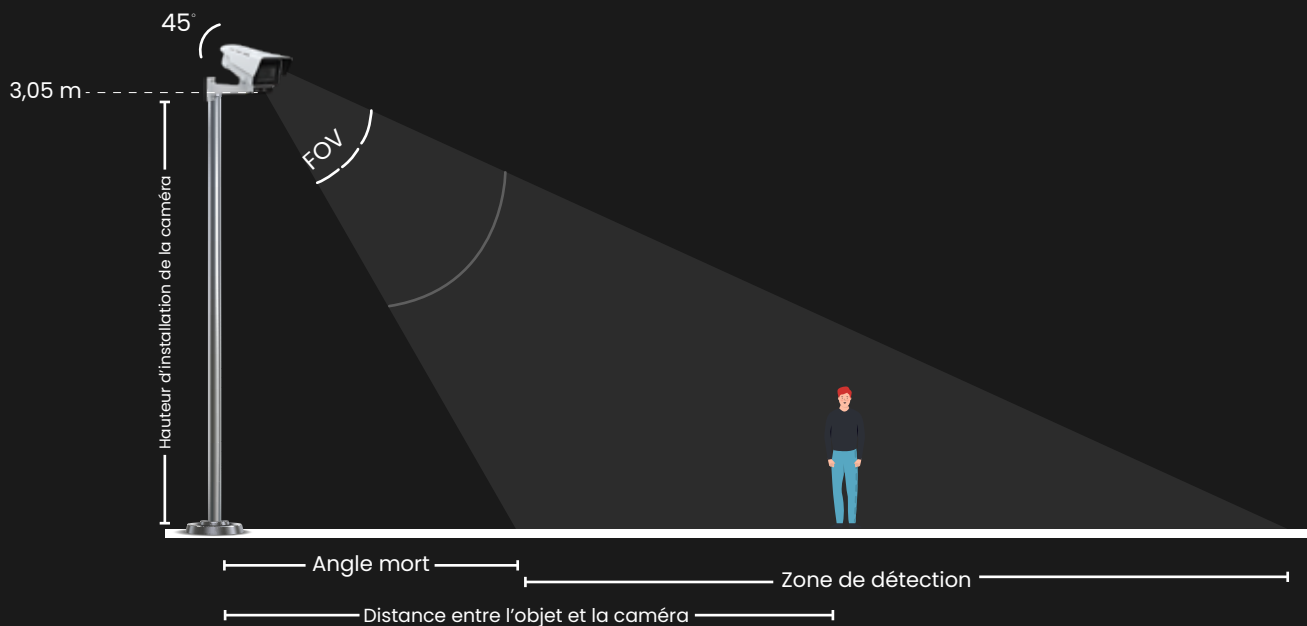
Angle large (~90° ou distance focale de 2,8 mm). Détection d'objets à une distance de **50 à 95 pieds**.

Angle étroit (30° ou focale de 10 mm). Détection d'objets à une distance de **160 à 295 pieds**.



Hauteur et angle optimaux pour l'installation des caméras

Il est essentiel d'installer les caméras à la bonne hauteur et au bon angle pour garantir une détection précise. À l'extérieur ou dans de grands espaces intérieurs, les caméras doivent être installées à une hauteur minimale de 2,8 m (9 pieds) et positionnées à l'horizontale par rapport à l'horizon et au sol. Les caméras peuvent être inclinées de 30° par rapport à l'horizontale pour une classification optimale des objets, avec une inclinaison maximale de 45° par rapport à l'horizontale. Augmenter l'angle d'inclinaison peut aider à détecter les cibles qui s'approchent directement de la caméra. Toute vibration de la surface de montage peut nuire à la précision de la détection des objets. Il est donc essentiel de fixer la caméra sur une surface stable.



Optimisation de la précision et de la performance de détection



Temps nécessaire à la détection

Contrairement aux détecteurs de mouvement traditionnels, les caméras de sécurité intelligentes nécessitent entre 1 et 4 secondes pour analyser et classer un objet de manière fiable. Durant ce court délai, la caméra affiche généralement un cadre de détection autour de l'objet pendant que l'intelligence artificielle confirme s'il s'agit d'une personne, d'un véhicule ou d'une autre cible. La majorité des systèmes d'IA requièrent au moins 2 secondes de visibilité continue pour pouvoir déclencher une alerte.



Détection et limitations de vitesse

Tous les systèmes d'intelligence artificielle ne réagissent pas de la même manière face à des objets en mouvement rapide. Certains sont capables de détecter une personne qui court, tandis que d'autres peuvent avoir du mal à générer une alerte dans ce type de situation. C'est pourquoi il est essentiel de prendre en compte ces limitations dès la phase de conception du système de sécurité. La mise en œuvre de mesures complémentaires comme des clôtures physiques ou des barrières virtuelles permet de renforcer la protection et de compenser les éventuelles zones à risque.



Caméras fisheye : efficacité réduite en extérieur

Les caméras fisheye ne conviennent pas à la surveillance vidéo à distance en extérieur. Leur lentille grand angle répartit la densité de pixels sur un champ de vision très large. La perte en clarté et en détail de l'image complique la détection et le suivi des activités surtout dans les grands espaces extérieurs.

Pour de meilleures performances, il est préférable d'utiliser un autre type de caméra plus adapté à la surveillance extérieure. En cas de besoin spécifique, veuillez contacter le **Support** pour des recommandations.

Détection : points clés à considérer



Même si les véhicules à l'arrière-plan sont visibles à la caméra, ils peuvent se trouver au-delà de la portée de détection de la caméra, ce qui rend les intrusions potentielles indétectables. Pour remédier à cela, des caméras de sécurité supplémentaires doivent être placées stratégiquement afin d'assurer une couverture complète du site.



Même si un objet se trouve dans la zone de détection de la caméra, la détection peut être compromise si l'angle de la caméra ne permet pas une visibilité complète. Par exemple, une personne qui marche entre des voitures dans une zone ombragée peut ne pas être entièrement visible. Pour éviter cela, il est recommandé d'installer des caméras supplémentaires à des emplacements stratégiques afin d'assurer une couverture complète du site.

Résumé

Couverture et détection de la caméra. Optimisées.



Chevauchement des caméras

Le chevauchement consiste à positionner deux caméras ou plus pour surveiller une même zone sous des angles différents. Cela permet d'augmenter les chances de détection en couvrant les angles morts d'une caméra avec le champ de vision d'une autre.

Détection d'objets

La détection d'objets utilise des algorithmes avancés pour identifier et suivre des objets tels que des personnes ou des véhicules. Lorsqu'un objet est détecté, le système envoie des alertes et poursuit le suivi dans le champ de vision de la caméra afin d'assurer une réponse rapide.

Comprendre la couverture des caméras

Pixels Par Mètre (PPF). Densité minimale de pixels requise pour classer avec précision les objets détectés.

Valeur mégapixel utilisée par l'IA. L'intelligence artificielle traite la vidéo à une résolution réduite afin d'optimiser les performances de la caméra.

Champ de vision horizontal (HFOV). Un champ large couvre une plus grande surface, mais réduit la portée de détection. Par contre, un champ plus étroit permet de détecter à plus longue distance, mais avec une couverture latérale plus limitée.

Portée de détection selon la focale

- **2,8 mm (~90°)** : permet une détection entre 50 et 95 pieds.
- **10 mm (30°)** : permet une détection entre 160 et 295 pieds.

Hauteur et angle optimaux pour l'installation

Installez les caméras à une hauteur comprise entre 9 à 12 pieds et inclinez-les entre 30° et 45° par rapport à l'horizontale. Veillez à les fixer sur une surface stable car les vibrations peuvent nuire à la précision de détection.

Optimisez la précision et la performance de détection

Temps de détection. Les caméras nécessitent entre 1 et 4 secondes de visibilité continue sur un objet pour pouvoir le classer correctement.

Limitation de vitesse. Certaines IA ont des difficultés à détecter des objets en mouvement rapide. Pour y remédier, il est recommandé d'ajouter des mesures de sécurité complémentaires comme des clôtures.

Restrictions concernant les caméras fisheye. Les caméras fisheye sont peu adaptées à la surveillance extérieure car leur champ de vision très large réduit la clarté de l'image sur de grandes zones. Pour de meilleurs résultats, envisagez d'autres types de caméras ou contactez notre équipe pour obtenir des recommandations adaptées.

Détection – Points clés à considérer

Au-delà de la portée de détection. Des objets visibles en arrière-plan peuvent se trouver hors de la portée effective de détection nécessitant l'ajout de caméras supplémentaires pour une couverture complète.

Limite liée à l'angle. Même dans la zone de détection, un angle mal ajusté peut compromettre la visibilité ; il est donc important de positionner les caméras de façon stratégique afin d'éviter les angles morts.

Connexion au centre de commandement de Sirix

Configuration d'un nouveau site

Après avoir installé tous les appareils de sécurité sur le site, suivez les étapes ci-dessous pour établir une connexion avec le centre de commandement de Sirix :

Fournissez l'adresse IP ou le nom DNS

- Indiquez l'adresse IP publique ou le nom DNS, et assurez-vous que la redirection de ports recommandée par le fabricant est correctement configurée pour un accès à distance.
- Ports courants requis (tous en TCP) pour les systèmes pris en charge :
 - **Hikvision.** HTTP 80 ou HTTPS 443, Serveur 8000, RTSP 554
 - **Dahua.** HTTP 80 ou HTTPS 443, Serveur 37777, RTSP 554
 - **Avigilon.** Serveur 38880–38882
 - **AXIS Cameras/Speakers.** HTTP uniquement
 - **Uniview.** HTTP 80, RTSP 554
 - **Any RTSP Camera.** HTTP 80, RTSP 554
 - **AXIS Camera Station.** Serveur 55756
 - **AXIS Camera Station Pro.** Serveur 29204
 - **Digital Watchdog/Hanwha Wave.** Serveur 7001
 - **ExacqVision OEM.** Serveur 22609, HTTP 80
- Pour d'autres systèmes, contactez le Support afin de confirmer les ports et procédures requis.

Vérifiez l'accessibilité Internet

- Assurez-vous que tous les appareils et ports sont accessibles depuis Internet.
- Utilisez [YouGetSignal Port Checker](#) pour vérifier les ports ouverts.

Filtrage d'adresses IP (si applicable)

- Ajoutez la plage d'adresses IP de la station de surveillance Sirix :
 - 216.113.34.128/28
 - 52.26.85.174
 - 54.187.110.2
 - 72.193.100.108 (Aktivsense)
 - 15.204.236.130 (Aktivsense)
- Une fois configuré, demandez au Support de tester les ports.

Connexion au centre de commandement de Sirix (Suite)

Soumettez les informations requises

- Remplissez le [formulaire technique](#) fourni avec les informations suivantes :
 - Nom de l'entreprise de sécurité et nom du site surveillé
 - Services demandés
 - Technologie, informations de connexion et plan du site
 - Adresse IP publique (WAN) ou nom DNS de l'appareil
 - Ports HTTP et RTSP de l'appareil redirigés
 - Identifiants de connexion à l'appareil (NVR/DVR/VMS)
 - Caméras surveillées et identifiées
 - Détails du haut-parleur IP utilisé pour les interventions vocales (modèle, adresse IP, port, identifiants de connexion)
 - Date de début de la surveillance

Testez les paramètres de la caméra

- Assurez-vous que le flux secondaire en direct est configuré avec :
 - **Résolution.** 720p ou moins
 - **Codec.** H.264
 - **Fréquence d'image.** 4 FPS, 8 i-Frame

Tests sur site (optionnels, mais recommandés)

- Les tests sur site sont fortement recommandés pour vérifier le bon fonctionnement des systèmes d'analyse, d'alarme et des haut-parleurs. Pour obtenir des instructions détaillées sur la planification et la réalisation de ces tests, veuillez consulter :
 - **Section 4.2 :** Tests de marche
 - **Section 4.3 :** Tests des haut-parleurs

Site en mode test

Après avoir terminé les tests sur site, Sirix placera le site en mode test pendant 24 à 48 heures. Cette période de surveillance permet à Sirix de s'assurer qu'aucune fausse alarme excessive n'est déclenchée.

Début de la surveillance

La surveillance démarre une fois la période de test terminée sauf si une autre date de début a été spécifiée dans les formulaires d'intégration.

Connexion des haut-parleurs au centre de commandement de Sirix

Veuillez suivre les étapes ci-dessous pour établir la connexion entre vos haut-parleurs et le centre de commandement de Sirix

Haut-parleurs analogiques

- Contactez le **Support** pour déterminer la meilleure méthode de connexion.

Haut-parleurs IP

- Assurez-vous que les haut-parleurs sont installés sur un réseau avec accès à Internet.
- Obtenez les **informations de compte SIP** (identifiant, mot de passe et nom du serveur) pour chaque haut-parleur en contactant le Support.
- **Configuration du haut-parleur :**
 - Redirigez le port HTTP du haut-parleur si vous souhaitez que Sirix effectue la configuration à distance.
- **Planifiez un test des haut-parleurs :**
 - Réservez une session avec Sirix pour tester le volume sonore des haut-parleurs dans toutes les zones du site.

Haut-parleurs GSD

- Redirigez les ports HTTP et RTSP pour garantir le bon fonctionnement.
- Contactez le **Support** pour toute assistance ou clarification supplémentaire si nécessaire.

Phase de test. Sécurité maximale.

Les tests de marche et de haut-parleurs sont essentiels, autant lors de l'installation d'un nouveau site que dans le cadre d'un entretien régulier. Ils servent à confirmer le bon fonctionnement des alarmes, caméras et haut-parleurs, assurant ainsi une sécurité optimale et minimisant les risques de défaillance.

Auto-vérification pour garantir la sécurité. Après l'installation de vos caméras, il est important de tester tout l'équipement avec des tests de marche afin de s'assurer que les déclencheurs réagissent correctement.

- **Tester dans différentes conditions.** Effectuez des tests de marche de nuit afin de repérer d'éventuels problèmes d'éclairage pouvant nuire à la performance de l'intelligence artificielle.
- **Tests réguliers.** Planifiez des tests de marche périodiques pour vous assurer que tous les équipements fonctionnent normalement et que la couverture de sécurité reste optimale.

Test de marche avec le centre de commandement de Sirix. Pour confirmer que le centre de commandement de Sirix reçoit bien toutes les alarmes, suivez les étapes suivantes :

1. Planifier une rencontre

- Prenez rendez-vous pour une séance de 15 minutes avec l'équipe Sirix en appelant le 1-855-788-1919.
- Vous pouvez également communiquer avec le soutien technique par courriel ou par téléphone.
- Lors de la réservation, veuillez indiquer clairement :
 - la date et l'heure souhaitées pour la rencontre;
 - le nom du technicien qui sera sur place;
 - le nom du site où le test de marche sera effectué.

2. Présence sur le site

- Assurez-vous d'être présent sur le site pour effectuer le test de marche.

3. Avisez l'opérateur

- Au début de la rencontre :
 - confirmez votre nom à l'opérateur. Assurez-vous qu'il correspond à celui indiqué lors de la prise de rendez-vous pour la vérification de sécurité;
 - mentionnez le nom du site à tester afin que l'opérateur puisse facilement l'identifier dans le système.

4. Effectuez le test de marche

- Parcourez le site en passant devant chaque caméra de sécurité afin de tester leur réactivité.

5. Vérifiez le déclenchement des alarmes.

- L'opérateur de Sirix confirmera que chaque fois que vous apparaissez dans le champ de vision d'une caméra, une alarme est bien enregistrée, afin de valider la détection adéquate.

Test des haut-parleurs pour assurer l'audibilité. Au cours de la même rencontre, les opérateurs de Sirix effectueront des interventions vocales via les haut-parleurs du site. Assurez-vous que les messages d'avertissement sont audibles et clairs dans toutes les zones du site afin de garantir une dissuasion efficace.



Importance des tests de marche périodiques. Les tests de marche réguliers jouent un rôle crucial dans le maintien de la sécurité de votre site. Ils permettent de s'assurer que tous les éléments du système à savoir caméras, alarmes et haut-parleurs fonctionnent normalement. En validant le bon déclenchement des alarmes, ces tests garantissent que toute intrusion sera détectée, permettant aux opérateurs d'agir rapidement pour prévenir le vol, le vandalisme ou toute autre activité criminelle.

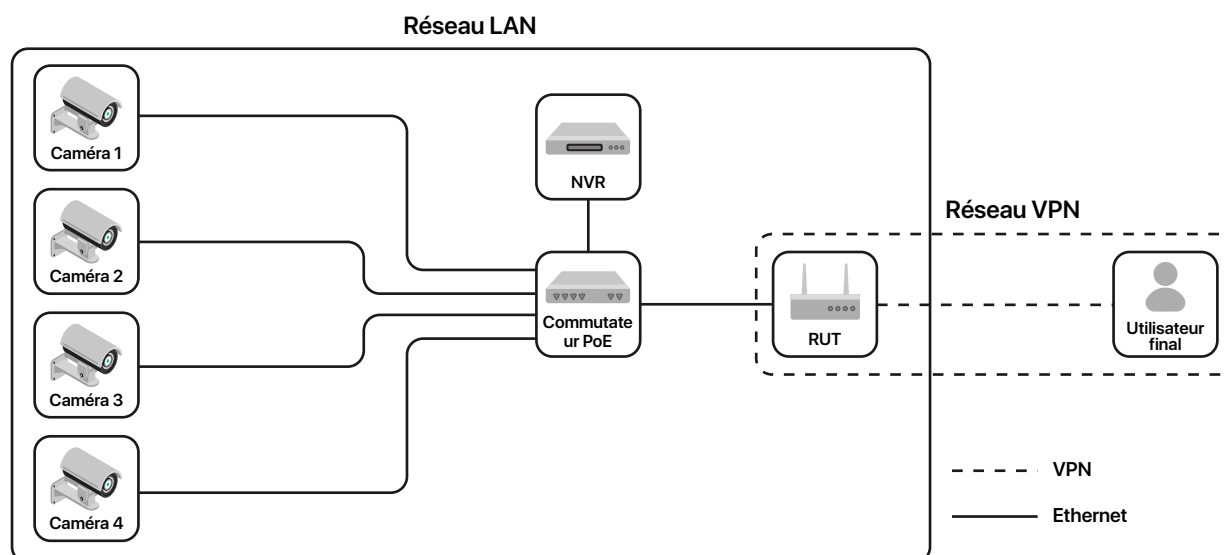
Connexion VPN

Le choix de la solution VPN idéale dépend de plusieurs facteurs, tels que la vitesse requise et l'environnement d'utilisation, qu'il soit intérieur ou extérieur.

Pour choisir la méthode la plus appropriée et procéder à la configuration de la connexion :

- Veuillez contacter le **Support**.

Notre équipe vous aidera à choisir la solution la plus adaptée à vos besoins et vous accompagnera tout au long de la configuration.



Grille de vérification post-installation pour les techniciens sur le site

Cette grille de vérification permet de s'assurer que les appareils de sécurité sont installés correctement afin de garantir une protection complète du site.

Grille de vérification

Assurez-vous que toutes les étapes ci-dessous sont réalisées:

1- Le transfert de port est effectué.	
2- Le sous-flux en direct est configuré.	
3- Les alarmes et les zones de masquage sont configurées.	
4- Les haut-parleurs sont configurés.	
5- <u>Le formulaire technique est rempli, y compris :</u>	a. Le nom d'utilisateur et le mot de passe administrateur pour le NVR/DVR/VMS b. L'horaire de surveillance pour les alertes et alarmes via Cloud IA c. Les détails de configuration des haut-parleurs SIP (numéro et modèle, s'il y a lieu)
6- Un rendez-vous a été pris avec l'équipe Sirix pour des tests de marche en appelant le 1-855-788-1919.	
7- Attendre le courriel de confirmation de Sirix :	a. Une fois les tests de marche complétés, Sirix procédera à la vérification de la configuration du site. b. Vous recevrez un courriel dans un délai de 2 à 5 jours ouvrables confirmant que le site est actif et sous surveillance.

Remarque importante : Cette grille de vérification s'applique uniquement aux sites standards.



Sites standards

- Sites avec un NVR connecté à un réseau de caméras utilisant le transfert de port
- Sites avec des caméras individuelles configurées avec le transfert de port



Sites hors norme

- Sites nécessitant des configurations spécialisées, telles qu'un VPN, une infrastructure réseau MPLS, des systèmes radar, etc.
- Pour les projets hors norme, veuillez contacter le **Support** pour obtenir de l'assistance.



Partenaires SIRIX PRO

- Les étapes 2, 3 et 4 ne sont pas obligatoires.

Problèmes de connexion. Réglés.

La gestion des problèmes de connexion dépend de l'abonnement du client à AktivSense.

Voici comment cela fonctionne :

Lorsque le partenaire n'est pas abonné à AktivSense.

- Le partenaire est responsable de surveiller la connectivité des appareils et de résoudre les déconnexions avec l'utilisateur final.
- Si l'ensemble du site perd la connexion, Sirix recevra une alarme et appliquera la Procédure Opérationnelle Standard (POS) du client jusqu'à ce que le problème soit résolu.

Lorsque le partenaire est abonné à AktivSense.

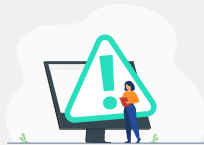
- Sirix assume l'entière responsabilité de la gestion de tous les problèmes de déconnexion des appareils.
- Sirix appliquera la procédure opérationnelle standard (POS) du client jusqu'à ce que le problème soit résolu.

Qu'est-ce qu'AktivSense ?

AktivSense est un système intelligent développé par Sirix, conçu pour surveiller en temps réel l'état des caméras de sécurité. Propulsé par l'intelligence artificielle, il détecte les problèmes techniques et envoie des alertes en cas d'anomalies, telles que :



Problèmes d'affichage de la caméra



Problèmes de connexion au NVR/VMS



Défaillances de la caméra



Défaillances du disque dur



Problèmes d'enregistrement



Inexactitudes de l'heure et de la date

Pour en savoir davantage sur AktivSense, cliquez ici [Détails sur AktivSense](#)

Maintenir sous contrôle les caméras, les enregistreurs NVR et les plateformes VMS.

Grâce à des vérifications intelligentes des caméras et systèmes VMS/NVR, Sirix assure une performance optimale, avec des niveaux d'accompagnement personnalisés selon le forfait du partenaire.



Pour les partenaires SIRIX PRO

Intervention à distance. Lorsque le problème peut être résolu à distance, Sirix passe rapidement à l'action et fournit un rapport détaillé au partenaire et/ou à l'utilisateur final à la fin de l'intervention.

Intervention sur site. Lorsque la résolution à distance n'est pas possible, Sirix accompagne le partenaire avec des directives précises et structurées pour assurer une résolution rapide et efficace sur le terrain.



Pour les partenaires non-SIRIX PRO.

Sirix envoie un rapport détaillé présentant les problèmes identifiés, accompagné d'instructions claires pour les résoudre.

Vérifications de l'état des disques durs.

Sirix prend en charge les vérifications de rétention des données et de corruption pour les supports suivants : cartes SD, enregistreurs NVR et disques durs VMS.

Cartes SD ou disques durs NVR



Marques compatibles.

- Axis
- Uniview
- Hanwha Wisenet
- LTS
- GSD
- TVT
- Avycon
- Alibi Witness
- Alibi Vigilant
- Luma
- Turing
- Reolink
- Camect
- Dahua
- Hikvision

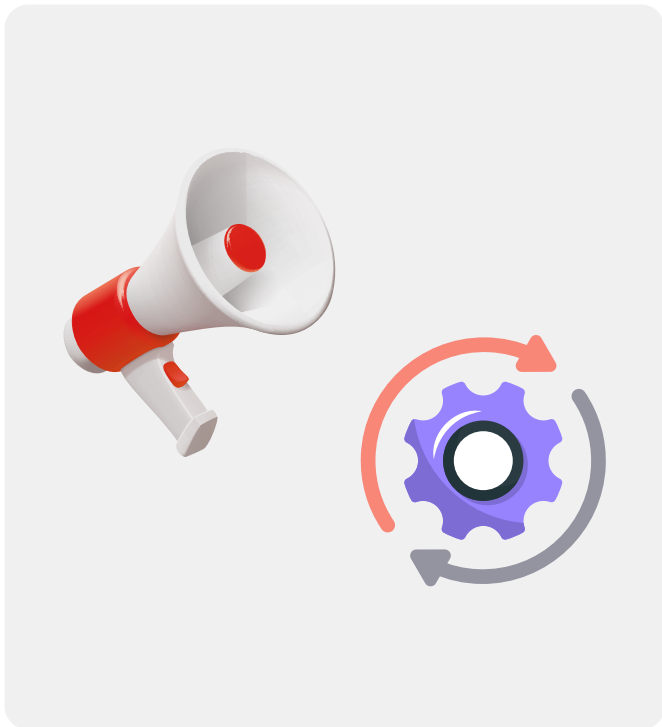


Disques durs pour systèmes VMS

Marques compatibles.

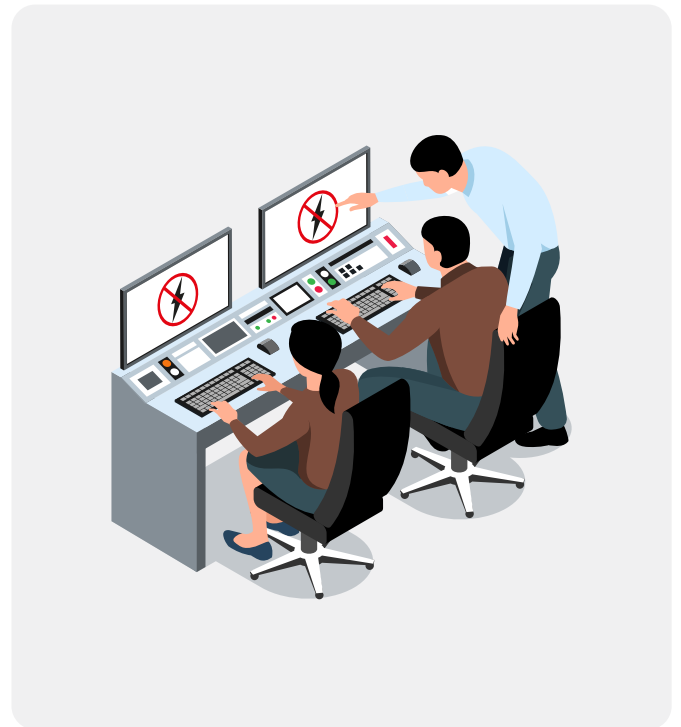
- Milestone
- Genetec
- Cognyte
- Avigilon
- ExacqVision
- Alta Aware
- Rhombus
- Digital Watchdog
- Network Optix
- Hanwha Wave
- i-Pro VMS
- Openeye

Des voix qui portent. De l'énergie qui passe.



Vérifications de l'état des haut-parleurs.

Pour les partenaires utilisant la boîte de sécurité autonome de Sirix ou abonnés à AktivSense, Sirix propose une surveillance en temps réel des haut-parleurs sur site afin de détecter toute déconnexion. Pour plus d'information, veuillez contacter votre représentant aux ventes.



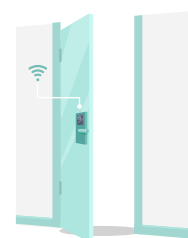
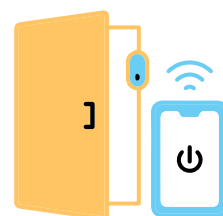
Surveillance des pannes de courant. Sirix peut détecter les pannes de courant sur un site lorsque l'UPS (alimentation sans coupure) est connecté au NVR via une sortie numérique (I/O output). Cette configuration permet à Sirix de recevoir des alertes en temps réel en cas d'interruption de courant. Une fois l'alerte reçue, nous appliquons rapidement les procédures spécifiques du client pour gérer la déconnexion du site, assurant ainsi une réponse rapide et appropriée.

Comment relier des appareils de sécurité pour déclencher des événements

Vous pouvez connecter des boutons de panique, des contacts de porte, des détecteurs de mouvement ou des panneaux d'alarme afin de déclencher des événements vidéo ou d'armer/désarmer un site, en suivant les étapes ci-dessous :

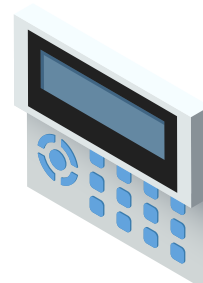
Boutons de panique, contacts de porte et détecteurs de mouvement

1. **Connexion** : branchez les câbles de l'appareil (par exemple : bouton de panique, détecteur de mouvement ou contact de porte) à l'entrée d'alarme d'une caméra, d'un encodeur ou d'un NVR compatible.
2. **Supported devices**. Consultez notre liste de compatibilité sur la page [Intégration des Partenaires](#). Vérifiez la colonne « Relais » pour confirmer si l'appareil est compatible (case à cocher).
3. **Classification des alarmes**. Sirix classera les alarmes déclenchées par ces appareils sous la catégorie ALARMES. Elles seront transmises aux opérateurs de Sirix pour une intervention immédiate.



Panneau d'alarme

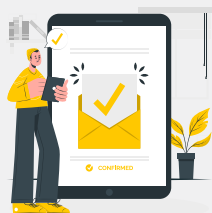
1. **Connexion**. Connectez la sortie PGM du panneau d'alarme à l'entrée d'alarme d'un encodeur, NVR ou caméra compatible à l'aide du câble approprié.
2. **Appareils compatibles**. Consultez notre liste de compatibilité sur la page [Intégration des partenaires](#). Vérifiez la colonne « Relais » pour confirmer la compatibilité (case à cocher).
3. **Classification des déclenchements**. Les alarmes déclenchées entraîneront l'armement ou le désarmement du site, selon la configuration faite.



Application mobile Sirix

Installez-la. Obtenez vos identifiants.

Pour installer l'application mobile Sirix et obtenir vos identifiants d'accès à vos données de site, veuillez suivre l'une des méthodes ci-dessous :



OPTION 1.

Soumettre le formulaire de procédure

Remplissez le formulaire de procédure avec toutes les informations requises.



OPTION 2.

Envoyer un courriel au Support de Sirix.

Envoyez un courriel avec les renseignements suivants :

- Le nom de la personne qui utilisera l'application mobile
- Son adresse courriel pour recevoir les identifiants d'accès ainsi que les instructions d'installation de l'application

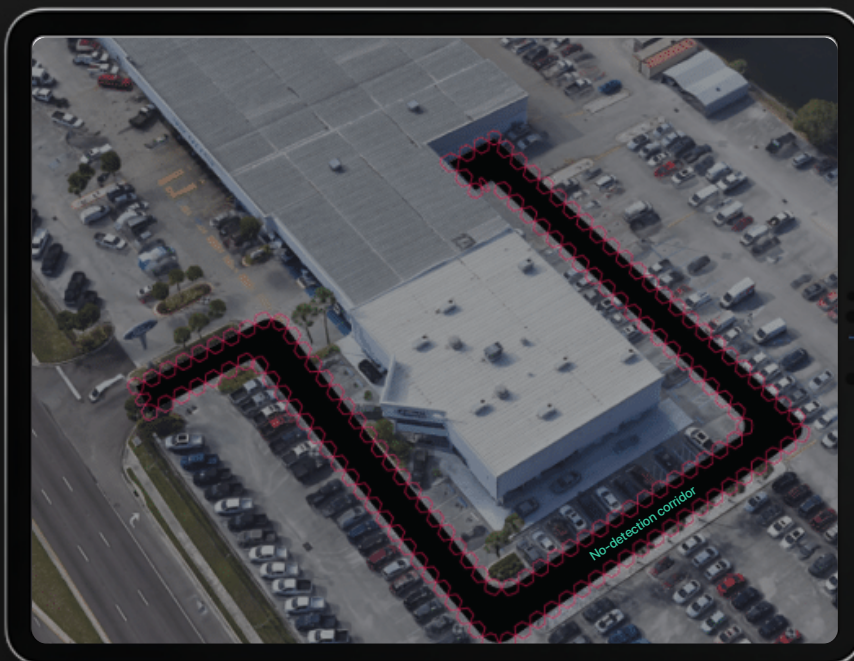
Prenez le contrôle de votre site.

A screenshot of the Sirix mobile application interface, showing a dashboard with various charts and data. The interface is displayed on a tablet and two smartphones. Various features are highlighted with callouts:

- Indicateurs de rendement des opérateurs Sirix par site surveillé**: Points to a line chart on the tablet dashboard.
- Nombres d'alarmes et rapports de "outcomes" spécifiques au site**: Points to a bar chart on the tablet dashboard.
- Nom du site**: Points to a text field on the smartphone screen.
- Cause de l'alarme**: Points to a text field on the smartphone screen.
- Date et heure de détection de l'événement**: Points to a timestamp on the smartphone screen.
- Temps requis pour l'exécution de la SOP après déclenchement d'alarme**: Points to a text field on the smartphone screen.
- Simplifiez la protection de votre site**: Points to a green 'Armer' button on the smartphone screen.
- Armez ou désarmez votre système à distance, d'un simple toucher, avec l'application mobile de Sirix.**: Points to a red 'Désarmer' button on the smartphone screen.
- Délai d'intervention des opérateurs Sirix en cas d'alarme**: Points to a text field on the smartphone screen.
- Actions et horodatages des opérateurs de Sirix en réponse à l'alarme**: Points to a list of actions on the smartphone screen.

Choisissez la meilleure stratégie d'armement et de désarmement

Un plan d'armement et de désarmement efficace est essentiel pour maintenir la sécurité en dehors des heures d'ouverture et pour réduire les fausses alarmes. Voici trois éléments clés à prendre en compte pour élaborer la stratégie la mieux adaptée à votre site :



Établissez un horaire de surveillance

Idéalement, la dernière personne à quitter les lieux arme le système, et la première personne à arriver le désarme. Cependant, pour tenir compte des erreurs humaines, il est recommandé de définir un horaire de surveillance par défaut. Un horaire forcé peut être configuré pour s'activer 30 minutes après la fermeture et se désactiver 30 minutes avant l'ouverture, afin d'assurer une couverture constante.

Choisissez une méthode d'armement et de désarmement

Les employés ou sous-traitants, tels que les équipes de nettoyage ou les livreurs, doivent disposer d'un moyen fiable de désarmer le système pendant les heures de surveillance afin d'éviter les fausses alarmes. Les options disponibles comprennent des applications mobiles, des télécommandes et des claviers d'alarme, offrant une flexibilité adaptée aux besoins et aux activités du site.

Créez des corridors sans détection

Les corridors sans détection sont des zones désignées où les mouvements effectués durant les heures de surveillance ne déclenchent pas d'alarme. Ces zones permettent aux personnes arrivant tôt d'accéder aux claviers ou lecteurs pour désarmer le système, et peuvent aussi servir de zones fonctionnelles, comme les points de dépôt ou les aires de livraison.

Accès administrateur. Ce dont nous avons besoin.

Sirix n'exige pas un accès administrateur complet pendant toute la durée de votre contrat. Pour assurer la sécurité de votre système tout en permettant des mises à jour techniques fluides, la résolution de problèmes ou des modifications de configuration, Sirix ne nécessite qu'un accès restreint, selon les considérations suivantes :

L'accès est limité aux fonctions nécessaires selon :



Les fonctionnalités incluses dans votre forfait.



Le type de système utilisé.



Si c'est un partenaire SIRIX PRO.



Cette approche minimise les risques d'atteinte à la sécurité tout en assurant une gestion efficace du système.



Durée de conservation des vidéos d'incident

Sirix conserve l'ensemble des enregistrements vidéo liés aux incidents pendant une période de 90 jours sur le [Portail des événements](#).

Processus d'activation du compte Sirix

Pour établir une connexion avec Sirix, vous devez remplir les deux formulaires suivants

Formulaire de procédure

Adresse du site des partenaires Sirix : www.portal.sirixmonitoring.com

Lien vers le formulaire de procédure : [Formulaire de procédure](#)

Informations requises pour compléter le formulaire :

1- Informations sur le site

- Nom du site
- Nom du contact principal, numéro de téléphone et adresse courriel

2- Adresse du site

- Adresse physique et/ou emplacement du terrain
- Instructions ou directives particulières (si nécessaire)

3- Fuseau horaire du site

- Remarque : Pour les sites situés en Saskatchewan, s'assurer qu'il n'y a pas d'heure avancée (heure d'été)

4- Numéro de téléphone de la police locale

- Service de répartition de la GRC pour les emplacements ruraux ou éloignés

5- Description du site

- Type de périmètre
- Informations importantes ou particulières concernant le site
- Carte de la zone surveillée, incluant les limites du périmètre et le plan des caméras

6- Réponse aux alarmes

(Pour les services de vérification d'alarme seulement)

- Nom de la centrale de surveillance
- Numéro de compte et mot de passe du site

7- Inclusions de services spéciaux

- Sirix Pro ?
- Boîte autonome (si applicable), numéro de boîte autonome et numéro de carte SIM

8- Procédure en cas d'intrusion

- Intervention vocale, liste d'appel d'urgence, service de gardes, lumière stroboscopique/sirène, intervention vocale personnalisée, IncidentCode

9- Armez / Désarmez

(Horaire de surveillance)

- Entièrement personnalisable

10- Liste des contacts d'urgence

- Service de répartition de la police locale
- Nom, numéro de téléphone, adresse courriel et mot de passe (jusqu'à 3 contacts)

11- Liste des contacts autorisés

- Nom et mot de passe (nombre illimité de contacts)

12- Utilisateurs de l'application mobile

(si applicable)

- Nom complet et adresse courriel (jusqu'à 5 utilisateurs)

13- Utilisateurs de IncidentCODE (si applicable)

- Nom, numéro de téléphone mobile (SMS) et adresse courriel (jusqu'à 3 utilisateurs)

14- Contact IT ou de soutien du site

- Type de contact et titre du poste
- Nom complet
- Nom de l'entreprise (si applicable)
- Adresse courriel
- Numéro de téléphone

15- Préférences de rapports

- Rapports de problèmes : Oui ou Non (adresse courriel requise)
- Rapports d'événements : Oui ou Non (adresse courriel requise)

Formulaire technique

Adresse Web de Sirix : www.portal.sirixmonitoring.com

Lien vers le formulaire technique : [Formulaire technique](#)

Informations requises pour compléter le formulaire technique

- 1- Nom du site
- 2- Services à acquérir
- 3- Sirix Pro : Oui ou Non
- 4- Types de détection présents sur le site
- 5- Types d'analytique Cloud (type de caméra)
- 6- Connexion LTE : Oui ou Non
- 7- Informations réseau
 - Adresse IP externe / DNS pour le serveur
 - Ports HTTP/HTTPS et port RTSP
 - Nom du VMS, nom d'utilisateur et mot de passe
- 8- Tunnel VPN : Oui ou Non
- 9- Caméras en cours de surveillance et autres caméras connectées
- 10- Marque / modèle du haut-parleur IP

Confirmation et réponse

Une fois les deux formulaires soumis, vous pouvez vous attendre à une réponse dans un délai de 3 à 5 jours ouvrables (à l'exception des vendredis).

Ce délai permet de procéder à :

- la connexion aux appareils;
- la mise à l'essai de l'équipement;
- les ajustements nécessaires des paramètres.

Des informations exactes dans les deux formulaires assurent un processus d'activation fluide et une connexion réussie avec Sirix.

De l'alerte à la résolution

Ce processus décrit étape par étape comment les opérateurs de Sirix gèrent les alarmes déclenchées afin d'assurer une résolution rapide et efficace.

Processus de gestion des alarmes

Déclenchement de l'alarme



Lorsqu'une alarme est déclenchée, elle apparaît sur le poste de travail de l'opérateur, comme illustré sur l'image à gauche.

Examen de l'incident



L'opérateur clique sur l'alarme, ce qui affiche les éléments suivants :

- **Fenêtre de gauche.** Image montrant ce qui a déclenché l'alarme
- **Fenêtre de droite.** Flux vidéo en direct provenant de la caméra qui a déclenché l'alarme

Évaluation de l'alarme

L'opérateur examine d'abord la fenêtre de gauche pour comprendre la cause de l'alarme. Il analyse ensuite le flux vidéo en direct dans la fenêtre de droite pour évaluer la situation.

Si l'alarme indique une menace réelle, l'opérateur :

- Ouvre toutes les caméras du site pour obtenir une vue d'ensemble complète
- Consulte les procédures spécifiques au site ainsi que les notes pertinentes

Action.

L'opérateur suit la procédure d'exploitation normalisée (PON) du partenaire afin de gérer la situation efficacement.

Le crime s'arrête ici.

Interventions vocales

Première intervention vocale

« ATTENTION ! ATTENTION ! ICI LA SÉCURITÉ. VEUILLEZ QUITTER IMMÉDIATEMENT LES LIEUX OU COMPOSER LE 1-855-788-1919 POUR VOUS IDENTIFIER. »

Ce message est diffusé deux fois.



Deuxième intervention vocale (15 à 30 secondes plus tard – si nécessaire)

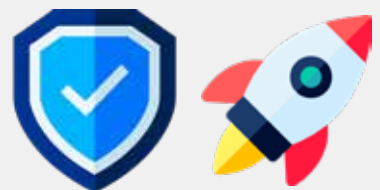
« ATTENTION ! ATTENTION ! ICI LA SÉCURITÉ. VEUILLEZ QUITTER IMMÉDIATEMENT LES LIEUX OU COMPOSER LE 1-855-788-1919 POUR VOUS IDENTIFIER, SANS QUOI LA POLICE SERA DÉPÊCHÉE SUR PLACE. »

Ce message est diffusé deux fois.



Escalade

Si l'intrus demeure sur les lieux après la deuxième intervention vocale, l'opérateur passe à l'étape suivante, conformément à la procédure de sécurité en vigueur.



Allons droit au but. Commandes vocales personnalisées. Réponses rapides.

Interventions vocales personnalisées.

- Les messages vocaux peuvent être personnalisés selon les préférences de votre client.
- Cette option est disponible uniquement avec les haut-parleurs Axis ou GSD.
- Des frais supplémentaires peuvent s'appliquer pour ce service.



Autres procédures de sécurité.

Les opérateurs de Sirix suivent des procédures de sécurité spécifiques selon la situation. Voici les actions les plus courantes effectuées en complément des interventions vocales :

- Appeler la liste de contacts d'urgence
- Aviser les services policiers
- Envoyer un rapport d'incident via IncidentCode
- Activer la sirène / la lumière stroboscopique



Des gardiens à l'œuvre. Des actions qui protègent.

Pour assurer la protection du site, les opérateurs peuvent entreprendre les actions suivantes. Chaque intervention est consignée dans un rapport d'incident, transmis en temps réel par courriel. (Consultez la Section 6 : Rapports, pour plus de détails.)

- Un représentant de votre personnel ou de l'équipe d'entretien a appelé et son identité a été vérifiée à l'aide d'un mot de passe valide. Un véhicule de livraison a été détecté; la caméra X a été désarmée temporairement pendant 30 minutes.
- Une première intervention vocale a été effectuée.
- Une deuxième intervention vocale a été effectuée.
- L'accès a été accordé au personnel autorisé.
- Un employé a authentifié son identité avec un mot de passe valide.
- Un événement IncidentCode a été lancé.
- La caméra X a été désarmée pour 30 minutes.
- Le personnel d'entretien est entré dans les lieux.
- La liste de contacts d'urgence était injoignable; un message vocal a été laissé.
- Un ou plusieurs individus ont quitté les lieux.
- Un ou plusieurs individus sont demeurés sur place.
- Les services policiers ont été dépêchés sur les lieux.
- Le déploiement des policiers a été annulé.
- Le déneigement ou l'entretien du site a été constaté; le site a été désarmé pendant 30 minutes.
- Des membres du personnel ont accédé au site.
- Les droits d'accès ont été vérifiés et confirmés.
- Le contact d'urgence a été rejoint.
- Le rapport IncidentCode a été envoyé.
- La sirène et la lumière stroboscopique ont été activées.
- Le site a été désarmé jusqu'à une heure précisée.
- L'intrus a été observé en train de quitter les lieux.
- Un acte de vandalisme ou un vol a été observé.
- Un ou plusieurs véhicules ont quitté les lieux.
- Un ou plusieurs véhicules sont restés sur place.

Cette approche structurée assure une couverture de sécurité complète et une transparence totale des actions effectuées.

Une sécurité qui s'impose

Les interventions vocales diffusées par haut-parleurs sur le site sont l'un des moyens les plus efficaces pour interrompre une intrusion et dissuader toute activité criminelle. Grâce à des avertissements audio en temps réel, elles permettent de perturber les comportements illégaux et de prévenir toute escalade de la situation.



Où faut-il installer les haut-parleurs ?

Pour une couverture optimale, installez les haut-parleurs à chaque coin du bâtiment ou à des points stratégiques du périmètre. Cela garantit que les avertissements sonores soient audibles dans toutes les zones de la propriété, augmentant ainsi la probabilité que les intrus entendent le message et quittent immédiatement les lieux. Un placement stratégique maximise la dissuasion et renforce la sécurité sur l'ensemble du site.

Équipe d'audit Sirix

Les professionnels de la performance des sites.

Les tests de marche et de haut-parleur sont essentiels à la fois lors de la connexion d'un nouveau site et régulièrement afin de garantir le bon fonctionnement de votre système de sécurité. Ces tests permettent de vérifier que les alarmes, caméras et haut-parleurs fonctionnent comme prévu, assurant ainsi une protection optimale et évitant les failles de sécurité.

Causes des fausses alarmes

Les fausses alarmes peuvent résulter de :

Problèmes d'analyse vidéo. Défaillances ou configuration incorrecte des analyses.

Zones de détection mal configurées. Les zones de détection sont mal définies, comme les rues ou trottoirs très fréquentés. Cela se produit lorsque les caméras détectent des mouvements dans des zones inappropriées. Ces zones doivent être définies comme zones de non-détection pour éviter les fausses alarmes causées par une activité constante.

Facteurs externes

- Éclairage inadéquat.
- Lentilles sales (ex. : toiles d'araignée, gouttes d'eau).
- Interférences environnementales.

Erreurs de procédure. Les employés ou sous-traitants n'appliquent pas correctement les procédures d'armement/désarmement du système.

Comment Sirix réduit les fausses alarmes

Pour les partenaires SIRIX PRO

Si le problème peut être résolu à distance. Sirix travaille avec diligence pour résoudre le problème et fournit un rapport au partenaire et/ou à l'utilisateur final une fois le problème résolu.

Si le problème ne peut pas être résolu à distance. Sirix fournit des instructions claires et détaillées pour permettre au partenaire de le résoudre sur place.

Pour les partenaires non-SIRIX PRO

Sirix envoie un rapport détaillé identifiant les problèmes et fournit des instructions pour les résoudre.



En répondant à ces défis, l'équipe d'audit Sirix contribue à maintenir une surveillance des sites fiable et efficace.

Rapports

La transparence assurée.

Sirix fournit trois types de rapports afin de garantir la transparence, des mises à jour rapides et une communication claire.

Qui reçoit les rapports ?

- **Rapports d'incident.** Envoyés instantanément aux destinataires spécifiés (partenaire de sécurité et/ou utilisateur final).
- **Rapports de problèmes.** Envoyés quotidiennement, exclusivement aux partenaires.
- **Rapports d'incident escaladé.** Envoyés sous 48 heures aux partenaires.

Rapports d'incident

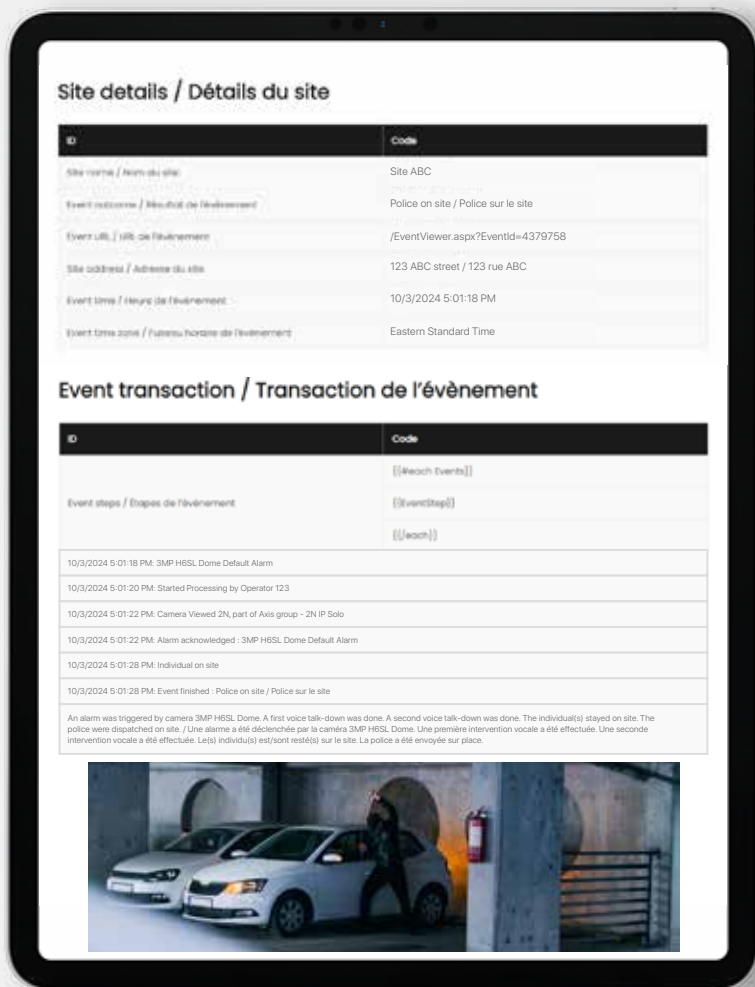
But. Les rapports d'incident sont envoyés instantanément par courriel aux destinataires désignés (partenaire de sécurité et/ou utilisateur final) lorsqu'un opérateur sélectionne un "outcome" spécifique.

Preuve visuelle. Chaque rapport comprend une image claire de ce qui a déclenché l'événement, offrant une transparence et une compréhension totales.

Accès. Tous les détails des incidents sont stockés en toute sécurité dans le Portail des Événements Sirix (live.sirix.ca).

Déclencheurs. Des rapports d'incident sont générés pour les outcomes suivants :

- Garde envoyé / Garde dépêché
- Garde sur le site / Garde sur place
- Police envoyée / Police dépêchée
- Police sur le site / Police sur place
- Alarme feu-eau / Alerte feu-eau
- Porte-barrière ouverte / Accès ouvert
- Intrus expulsé / Individu évacué
- Connexion rétablie / Lien restauré
- Patrouille effectuée / Ronde complétée
- Appel central alarme / Appel au centre d'alarme
- Personnel sur place / Équipe sur site
- Script effectué / Procédure suivie
- Patrouille effectuée – Problème constaté / Ronde complétée – Anomalie détectée
- Protection VIP / Sécurité VIP



Rapports de problème

But. Envoyés une fois par jour aux partenaires, les rapports de problème incluent à la fois des rapports d'incident et des détails sur les problèmes techniques affectant le site.

Contenu.

- **Problèmes techniques.** Les rapports couvrent :
 - Aucun enregistrement / No footage available
 - Problème d'horaire / Schedule problem
 - Perte de connexion / Connection loss
 - Intervention-strobe non fonctionnelle / Voice-strobe not working
 - Intervention-strobe non configurée / Voice-strobe not configured
 - Alarmes excessives / Excessive alarms

Rapports d'incident escaladé

- **Les rapports d'incident escaladé** sont des résumés détaillés envoyés au partenaire de sécurité dans un délai de 48 heures. Ils détaillent tout événement grave nécessitant l'intervention de la police, comme un vol, un incendie ou une intrusion confirmée.

Modifications du masquage, du site et de la configuration de l'IA. On vous tient informé des mises à jour sur le site

Lorsque des modifications sont apportées au masquage, à la configuration du site ou à celle de l'intelligence artificielle, Sirix garantit une communication claire et une documentation rigoureuse grâce au processus suivant :



Notification au partenaire

Nous informons le partenaire via l'adresse courriel indiquée dans le [formulaire de procédure](#) sauf si une autre méthode de communication a été spécifiée par le partenaire.

Confirmation de la modification

Pour confirmer la modification, nous envoyons :



Une image montrant la configuration d'origine.



Une image reflétant la configuration mise à jour.

Ce processus garantit la transparence et permet au partenaire d'examiner et d'approuver les modifications.

Détection de fumée et d'incendie par IA

Une technologie allumée.

Définition du modèle. Le modèle de détection d'incendie de Sirix reconnaît la présence de fumée ou de feu dans le champ de vision de la caméra lorsque celle-ci est armée, et distingue les deux types de détection lors de l'envoi des alertes.

Comment fonctionne cette technologie ? Nos algorithmes de vision par ordinateur sont entraînés à partir de jeux de données publics sous licence et de données propriétaires contenant des milliers d'images. Ils détectent la présence de fumée ou de feu localisée ou dans l'ensemble du champ de la caméra. Après quelques secondes de détection continue, une alerte est envoyée.

Fonctionnalités supplémentaires du modèle

1. Délais configurables pour générer une alerte.
2. Paramètres d'alerte configurables pour chaque caméra et chaque analyse : niveau de confiance, zones ignorées, seuil de cadrage, zones de recadrage.
3. Spécificité par type : feu, fumée ou les deux.
4. Période de refroidissement entièrement configurable pour chaque caméra.
5. Multiples modes de réception des alertes : texte, courriel, VMS, interface de surveillance, IMMIX. Toutes les alertes sont envoyées simultanément de notre côté.



Attentes concernant les faux positifs

1. Davantage de faux positifs (FP) lors des tests initiaux, fortement réduits une fois le modèle optimisé pour chaque cas d'usage.
2. Conditions météo sévères (ex. : fortes pluies) pouvant altérer la visibilité des caméras et augmenter le nombre de FP.
3. Le brouillard peut ressembler à de la fumée et provoquer des FP.
4. Des paramètres comme les zones ignorées et le niveau de confiance sont configurables pour limiter les FP.

IA de détection du feu et de la fumée

Exigences techniques

Min. FPS	Résolution min.	Portée de détection	Plage de bande passante (50–100 % de mouvement)	Compatible SMTP ?	Compatible thermique ?	Compatible fisheye ?
1	480p	3 PPF	~43 kbit/s	Non	Non	Non

Par caméra, en utilisant un filtre de mouvement à la résolution et au taux d'images minimum



Assurez une connexion internet stable. Les connexions instables ou les pannes fréquentes entraînent une perte d'images et de détections.



Des résolutions et des taux d'images plus élevés n'entraînent pas nécessairement de meilleures détections, mais augmentent l'utilisation de la bande passante. Cependant, une haute résolution peut être utile dans certains cas, comme lorsque la caméra couvre une grande zone.



Le modèle d'incendie est compatible avec toutes les intégrations en disponibilité générale, mais non compatible avec les intégrations de type clips.



Une large plage de FPS (images par seconde) est acceptable selon le cas d'usage. Les situations explosives nécessitent un FPS plus élevé pour générer une alerte immédiate. Les incendies à progression lente peuvent être surveillés sur une plus longue période avec un FPS plus faible.

FAQs

Quels types d'incendies ce modèle a-t-il été entraîné à détecter ?



Il a été entraîné à détecter : fumées/incendies de chantier, fumées/incendies de voiture, fumées/incendies en intérieur.



Il n'a pas été entraîné à détecter : incendies chimiques, feux d'artifice, fumée « non naturelle » (vapotage, bombes fumigènes, fusées éclairantes).

Quand le modèle décide-t-il d'envoyer une alerte ?

Par défaut, si la majorité des images capturées pendant une période de 10 secondes contiennent des détections de fumée ou de feu, Sirix enverra une alerte. Dans les cas où l'on s'attend à une progression lente du feu (par exemple sur un chantier), cette durée peut être étendue à 30 ou 60 secondes avant de déclencher l'alerte. Pour les sites à risque d'explosion, il est recommandé d'utiliser un taux d'images plus élevé et un intervalle de temps plus court que 10 secondes.

Pourquoi des fausses alertes apparaissent-elles avec des lumières fortes ou du brouillard ?

Les caméras vidéo utilisent des lentilles pour capter la lumière et créer une image. Comme les flammes et les fortes lumières produisent toutes deux une lumière vive, leur similitude peut tromper les capteurs de lumière de la caméra et générer des représentations visuellement similaires. Le brouillard ressemble fortement à de la fumée, notamment lorsqu'il est soufflé devant la lentille par le vent. Filtrer une vraie fumée serait dangereux, donc une alerte est toujours envoyée à l'utilisateur pour la confirmer ou non.

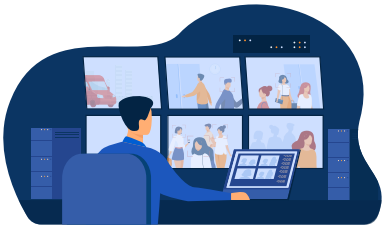
Politiques, protocoles et bien plus encore

Politiques de surveillance et de facturation.

Heures de surveillance

Un contrat de surveillance standard inclut jusqu'à 108 heures par semaine. Tout dépassement de cette limite peut entraîner des frais supplémentaires.

Dans le cas d'une surveillance temporaire 24 /7, un tarif de 55,00 \$ par bloc de 10 heures s'applique, au-delà des 108 heures hebdomadaires incluses.



Période d'engagement

La tarification est basée sur un engagement minimal de 3 mois.

Des frais d'activation de 200,00 \$ s'appliquent pour toute connexion de site inférieure à trois mois.



Jours fériés au Canada et aux États-Unis

La surveillance est assurée pendant les jours fériés canadiens et américains, sans frais supplémentaires. Cette couverture est incluse dans le forfait standard.



Frais liés à l'intervention policière

Si une facture est émise par les services policiers, les frais facturés comprendront le montant exigé par la police, auquel s'ajoutent des frais administratifs de 15 %.



Procédures « script » dynamiques

Pour les services nécessitant une procédure dynamique de type « script », veuillez communiquer avec votre représentant des ventes pour obtenir plus de détails.



Politique pour les sites délinquants

Un site est considéré comme délinquant lorsqu'un armement/désarmement inadéquat ou des défaillances techniques entraînent un excès de fausses alarmes. Sirix ne tient pas les partenaires responsables des incidents échappant à leur contrôle (par exemple, déclenchements causés par des passants inoffensifs).

Étapes suivies pour régler le problème des sites délinquants

(0 heure)

Courriel de notification.
Un courriel est envoyé au partenaire.



(72 heures)

Deuxième avis. Si le problème n'est pas résolu après 3 jours, un second courriel de suivi est envoyé.



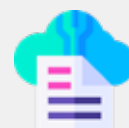
(96 heures)

Suivi téléphonique. Un appel est effectué auprès du partenaire. Si personne ne répond, un message vocal est laissé.



(144 heures)

Implantation de Cloud IA. Le Cloud IA est intégrée à la caméra problématique. Si un mauvais usage est constaté et que le problème persiste, Sirix se réserve le droit d'imposer des frais de 1\$ pour chaque fausse alerte.



Ressources supplémentaires.

Sirix Pro

Évitez les frais supplémentaires liés aux fausses alarmes en vous inscrivant à ce service. L'entretien des appareils et une ligne d'assistance d'urgence sont inclus.



Cloud IA

Cloud IA corrige les fausses alarmes causées par une IA inefficace sans modifier votre infrastructure physique.

Les solutions basées sur l'infonuagique sont simples à mettre en œuvre et réduisent la pression sur les ressources TI (Technologie de l'Information).



Procédures de déconnexion (surveillance en direct)

Toute personne entrant dans le périmètre surveillé doit désarmer la zone ou aviser le centre de commandement de Sirix. Dans certains cas précis, les alarmes sont gérées de la manière suivante :



Véhicules de remorquage ou de livraison

Les caméras déclenchant une alarme sont mises en pause pendant 30 minutes si un véhicule est identifié comme étant en remorquage ou en livraison.



Agent de sécurité

Tous les appareils sont mis en pause pendant 30 minutes si un agent de sécurité non annoncé est reconnu.



Services de déneigement

Tous les appareils sont mis en pause pendant 30 minutes si un service de déneigement non annoncé est reconnu.



Services d'aménagement paysager

Ils doivent téléphoner au centre de commandement. Une fois leur présence confirmée, le site sera désarmé pendant 30 minutes.



Agents d'entretien et employés

Ils doivent s'identifier auprès de l'opérateur. Celui-ci désarmera alors les caméras concernées pendant 15 minutes afin de permettre l'entrée.



Alarmes excessives

Si un appareil commence à déclencher des fausses alarmes :

Première fois : la caméra ou le site est désarmé pendant 60 minutes.

Deuxième fois : il est désarmé jusqu'au prochain moment de réarmement prévu.

Si le site est désarmé en raison d'un excès de fausses alarmes, la procédure de perte de communication enregistrée sera appliquée. Un rapport de problème détaillé sera envoyé le matin ouvrable suivant.

Maintenance proactive



Nettoyez régulièrement les lentilles des caméras. Nettoyez les lentilles au moins deux fois par an pour garantir une image claire. Dans des environnements difficiles comme ceux exposés à des températures élevées, des vents forts, de la poussière, ou situés près d'autoroutes ou de chantiers, un nettoyage plus fréquent est recommandé pour maintenir la performance.



Inspectez pour détection de bris ou de sabotage. Vérifiez régulièrement les caméras et équipements pour repérer toute pièce brisée, trafiquée ou mal alignée pouvant nuire au bon fonctionnement du système.



Surveillez la rouille et la corrosion. Soyez attentif aux signes de corrosion sur l'équipement extérieur. Appliquez des revêtements de protection ou remplacez les pièces rouillées pour éviter des dommages à long terme.



Testez les systèmes d'alimentation de secours. Vérifiez périodiquement les batteries UPS et les sources d'alimentation de secours afin d'assurer le maintien des opérations en cas de panne.



Mettez à jour les micrologiciels et logiciels. Assurez-vous que les caméras, moteurs IA et logiciels de surveillance sont à jour avec les derniers correctifs de sécurité et de performance. Même si Sirix gère généralement ces mises à jour, il est recommandé de vérifier que le système fonctionne avec la version la plus récente.



Vérifiez la stabilité des supports de montage. Inspectez les supports et fixations pour garantir que les caméras sont **solidement installées**. Toute vibration ou mouvement peut perturber la détection d'objets et nuire à la performance du système.



Effectuez des diagnostics réguliers du système. Réalisez des diagnostics périodiques pour vous assurer que les caméras, capteurs et alarmes fonctionnent correctement. Ce processus comprend des tests de marche (comme indiqué dans la section précédente - tests de marche et haut-parleur) afin d'identifier et de résoudre les problèmes avant qu'ils ne compromettent la sécurité.

Au-delà de la vidéosurveillance

Pour assurer une sécurité optimale sur un site, il est essentiel de compléter la vidéosurveillance par des dispositifs de dissuasion physique. Des mesures comme des clôtures, bornes, éclairages et panneaux d'avertissement ajoutent des couches de protection supplémentaires, réduisant les risques d'intrusion. Ces éléments agissent en synergie avec la vidéosurveillance pour renforcer votre stratégie de sécurité et protéger efficacement vos installations.



Clôtures

Les clôtures créent une **barrière physique robuste**, rendant l'accès plus difficile pour les intrus.

- **Installation.** Installez des clôtures tout autour du périmètre de la propriété. Utilisez des blocs de ciment dans les zones isolées pour empêcher les véhicules ou les biens de valeur d'être emportés.
- **Choix.** Les clôtures en treillis d'acier sont une excellente option en raison de leur résistance et durabilité.



Bornes de protection

Les bornes assurent une protection physique tout en préservant l'esthétique, empêchant les véhicules d'accéder à des zones non autorisées.

- **Disposition.** Disposez les bornes suffisamment rapprochées pour bloquer même les véhicules les plus étroits.
- **Choix.** Choisissez des bornes adaptées aux besoins du site, en conciliant sécurité et attrait visuel.

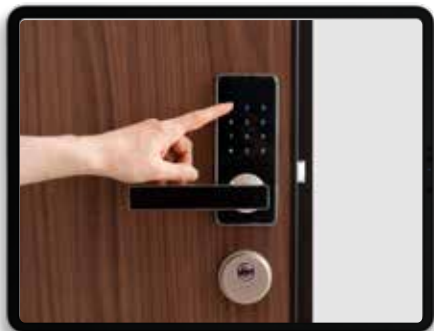


Barrières

Une barrière sécurisée est essentielle pour prévenir les intrusions. Des charnières faibles ou une barrière mal ajustée peuvent facilement être forcés.

- **Choix.** Adaptez les charnières du portail à son poids et à sa largeur. Choisissez des serrures, loquets et roulettes appropriés afin d'éviter les points de faiblesse.

Au-delà de la vidéosurveillance



Serrures

Les serrures sont des moyens de dissuasion essentiels, montrant que la sécurité est prise au sérieux.

- **Types.** Les verrous à pêne dormant, les cadenas, les serrures électroniques, les serrures intelligentes et les serrures biométriques offrent différents niveaux de sécurité.
- **Sélection.** Utilisez des serrures robustes pour retarder les intrus, rendant les effractions plus difficiles.



Renforcements des serrures

Renforcer les serrures ajoute une couche de protection supplémentaire, rendant plus difficile le contournement de la sécurité par les intrus.

- **Exemples :**
 - **Fermeurs en acier massif.** Offrent une résistance contre les tentatives de levier et de coupe.
 - **Serrures à anse dissimulée.** Protègent les remorques ou véhicules avec des barrières supplémentaires.
 - **Coffrets antivols.** Protègent les serrures de conteneurs avec des couvercles inviolables

Ajouter des renforcements augmente le temps nécessaire pour forcer l'entrée, décourageant ainsi les intrus de persister.



Panneaux d'avertissement

Les panneaux d'avertissement informent les intrus potentiels que le site est surveillé, dissuadant ainsi les accès non autorisés.

- **Positionnement.** Affichez les panneaux de manière visible aux entrées, autour du périmètre, près des caméras de sécurité et à l'intérieur du site.
- **Visibilité.** Choisissez des polices et des couleurs visibles dans toutes les conditions d'éclairage, et évitez les obstructions comme les arbres ou les drapeaux.

Au-delà de la vidéosurveillance



Lumière

Un bon éclairage est essentiel à la fois pour dissuader les intrus et pour améliorer les performances des caméras. Voici comment garantir l'efficacité de votre installation lumineuse :

Emplacement des sources de lumière :

- **Entrées et sorties.** Empêchez les accès non autorisés et facilitez l'identification des allées et venues.
- **Périmètre.** Éclairez toutes les limites pour dissuader les intrus de s'approcher.
- **Près des caméras de surveillance.** Améliorez la visibilité des caméras et assurez une qualité d'image optimale.
- **Panneaux d'avertissement.** Mettez en valeur les panneaux pour renforcer leur visibilité la nuit.

Comment évaluer votre installation lumineuse

- **Visitez la nuit.** Promenez-vous sur le site la nuit pour vérifier si chaque zone est bien éclairée. Portez une attention particulière aux entrées, aux stationnements et aux zones de stockage.
- **Assurez une lumière uniforme.** Évitez les zones avec de forts contrastes lumineux, qui peuvent créer des ombres et des angles morts.

Bonnes pratiques pour le positionnement de l'éclairage

- **Évitez la lumière directe sur les caméras.** Les sources lumineuses intenses, comme le soleil ou les phares de voiture, peuvent temporairement éblouir les caméras.
- **Éloignez-vous des surfaces réfléchissantes.** Les miroirs, sols brillants ou plafonds peuvent provoquer de fausses alarmes en raison des reflets.
- **Évitez les caméras avec infrarouge intégré.** Ces caméras peuvent avoir des difficultés avec la pluie, le brouillard ou les toiles d'araignées, qui reflètent la lumière et déforment les images. Utilisez plutôt des caméras standards avec un éclairage à proximité ou des caméras thermiques pour de meilleures performances.

Un site bien éclairé ne dissuade pas seulement les intrus, il garantit également une visibilité claire pour l'analyse vidéo, permettant une détection et une réponse rapides.

Pour en savoir plus sur les mesures de sécurité physique qui complètent la vidéosurveillance à distance, [visitez notre blog](#).

Liens utiles.

Liste de prix

Pour connaître en détail les tarifs de tous les services et produits Sirix, veuillez contacter votre représentant local pour obtenir la liste complète des prix.

Remarque importante. 1 lentille = 1 caméra. Chaque lentille de caméra est considérée comme une caméra distincte lors de la tarification.

Formulaires fréquemment utilisés

Lien vers le [formulaire de procédure](#)

Lien vers le [formulaire technique](#)

Lien vers le [formulaire de modification de fiche client](#)

Calculateur FFP

Pour des calculs supplémentaires sur la longueur focale des lentilles, la densité de pixels et les zones de couverture, utilisez le [calculateur de lentille CCTV](#)

Partenaires d'intégration et support

Pour consulter la liste des partenaires d'intégration et du support, veuillez visiter notre [page d'intégration des partenaires](#)

Portail des événements

Accédez aux vidéos en direct et enregistrées ainsi qu'aux informations importantes sur le site via le portail des événements à l'adresse suivante : <https://live.sirix.ca/>

Helpdesk

Pour soumettre un ticket, télécharger des formulaires ou trouver des réponses sur des sujets comme l'onboarding, l'intégration, la configuration, AktivSense et plus encore, consultez le [Helpdesk](#) de Sirix.

Sirix

Pour toute question ou demande d'assistance, veuillez contacter notre équipe **Support**. Nous nous engageons à résoudre rapidement les problèmes et à assurer un succès mutuel.

info@sirixmonitoring.com | 1-855-788-1919 (24/7 SOC)

