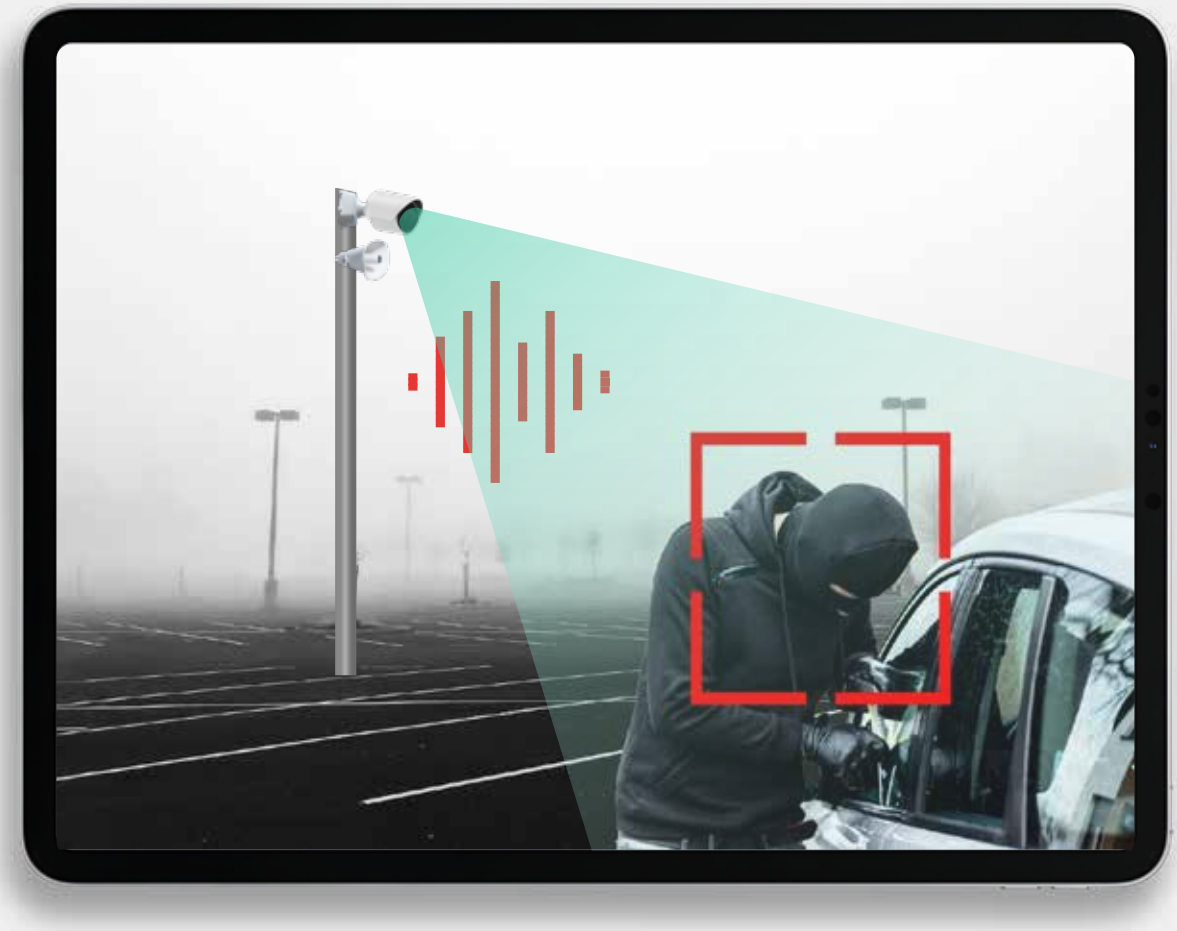
Sirix

Securing sites with Sirix AI-powered video monitoring

Your installation & performance guide



2525 Bd Daniel-Johnson Suite #405
Laval, QC. H7T 1S9
1-855-788-1919 (24/7 SOC)

Release Date:
February 2026

Total Pages:
50 Pages

Revision 4.0

Copyright, usage policy, and updates

Fourth edition.
Published: February 2026

This guide offers comprehensive information on security camera installation, best practices for remote video monitoring, and guidelines for effective detection to ensure optimal perimeter protection. It also includes detailed insights into all Sirix solutions, step-by-step instructions for on-site technicians, guidance on establishing connections, using various online tools, and contacting our support team.

Unauthorized use, reproduction, or distribution of this guide, in whole or in part, without the express written consent of Sirix, is strictly prohibited.

Please note that the information contained in this guide may become outdated as technology evolves. To ensure you have the most current information, please contact Sirix for the latest version of this guide.

Table of contents

Mastering perimeter protection with Sirix

Perimeter security is the first line of defense, ensuring threats are detected and deterred before reaching critical areas. A well-designed system safeguards people and property, reduces risks, and prevents incidents from escalating.

This **installation & performance guide** provides clear, step-by-step instructions for installing, configuring, and integrating security devices with Sirix's AI-powered command center. It covers:

- Device setup, including cameras, NVRs, alarms, and speakers.
- Configuring alarms, masking, and detection zones.
- Using advanced features like **AktivSense** for health monitoring and AI analytics.
- Conducting walk tests and setting up voice interventions.

Designed to ensure efficient installation and seamless integration, this guide helps you fully leverage Sirix's solutions and achieve reliable, comprehensive perimeter protection.

Communication channels

For any assistance, please reach out using the appropriate contact information below:

Operations

For help with onboarding, client site details, or monitoring-related questions:

- **Phone:** 1-855-788-1919
- **Email:** operation@sirixmonitoring.com

Support

For technical issues or assistance with site connections:

- **Phone:** 1-866-765-6667
- **Email:** support@sirixmonitoring.com

Billing

For inquiries related to billing:

- **Email:** billing@sirixmonitoring.com

Security camera placement. Done right.

Proper camera placement is essential for effective perimeter security. Cameras must be positioned to provide clear, unobstructed views, enabling analytics to accurately detect movement and classify objects. Incorrect placement can leave blind spots, allowing intruders to bypass detection and access the premises unnoticed.

Power outlet location

To ensure your security devices function properly, start by identifying where power outlets are located on your property. This will help you design an effective camera placement plan that aligns with your infrastructure.

Perimeter vs. building installation

Preventing obstacles from blocking views.

Mounting cameras only on the building can create blind spots, as parked cars or other objects may obstruct the view. Installing cameras along the property's perimeter ensures clear coverage of parking areas and entry points, making it harder for intruders to slip by unnoticed.

Optimizing AI performance.

For cameras' AI to classify objects effectively, it needs a clear view of at least a large portion of a person's body. Cameras should be installed at a horizontal angle no greater than 45 degrees. Building-mounted cameras often fail to meet these requirements, making perimeter cameras critical for reliable detection.

AI signal transmission

When cameras are installed more than 300 feet from the main building, their AI signal must be relayed back for recording and analysis. There are two primary methods for transmitting this signal:

- **Unidirectional antennas (Wireless solution).**
  Use antennas, such as those from Ubiquiti, to wirelessly transmit the signal to the main building.
- **PoE extenders (Hardwired solution).**
  Power over Ethernet (PoE) devices transmit both power and data through a single ethernet cable. Veracity provides dependable PoE solutions to connect distant cameras directly.

Solving power and signal gaps.

On many sites, such as construction sites, power, internet, or network coverage may be unavailable. We provide solutions to overcome these challenges and ensure seamless, reliable site security.

No electricity

If electricity is unavailable, a battery-powered all-in-one 4G LTE 5MP HD video security system can be rapidly deployed in remote areas and is available for rent from Sirix. It offers live view and long-distance detection up to 147 feet at a 60º angle, ensuring reliable monitoring without a power source.

No Internet connection or Wi-Fi

If there is no internet connection or Wi-Fi, you have two reliable options: **set up your own LTE network** using an LTE router, PoE switch, and optional external antenna for enhanced signal strength, or **utilize your client's existing network** by connecting your security system to their on-site internet infrastructure. To ensure optimal connectivity, you can test the network speed at speedtest.net.

No LTE network coverage

If LTE network coverage is unavailable, two reliable solutions ensure continuous connectivity: **Satellite or Fixed Wireless Systems** involve installing equipment like dishes or receivers, with service packages tailored to the site's location and available infrastructure. Alternatively, **LEO (Low-Earth Orbit) Satellites + Antennas** offer fast, low-latency internet by communicating through satellite constellations, providing reliable connectivity even in remote areas. Providers such as Starlink, HughesNet, and Xplore offer solutions for diverse environments.

Summary

Security camera placement. Done right.

Identify power outlets

Start by locating power outlets to design a camera placement plan that aligns with your site's infrastructure.

Install cameras on the perimeter

Avoid obstructions. Perimeter installation prevents objects like cars from blocking views, ensuring full coverage of parking areas and entry points.

Enhance AI detection. For accurate object classification, cameras must capture a clear view at an angle no greater than 45 degrees. Building-mounted cameras often fail to meet these criteria.

Transmit AI signal effectively

If cameras are over 300 feet from the main building, the AI signal must be relayed:

Wireless solution. Use unidirectional antennas, such has Ubiquiti.

Hardwired solution. Use POE extenders, such as Veracity or Enable-it.

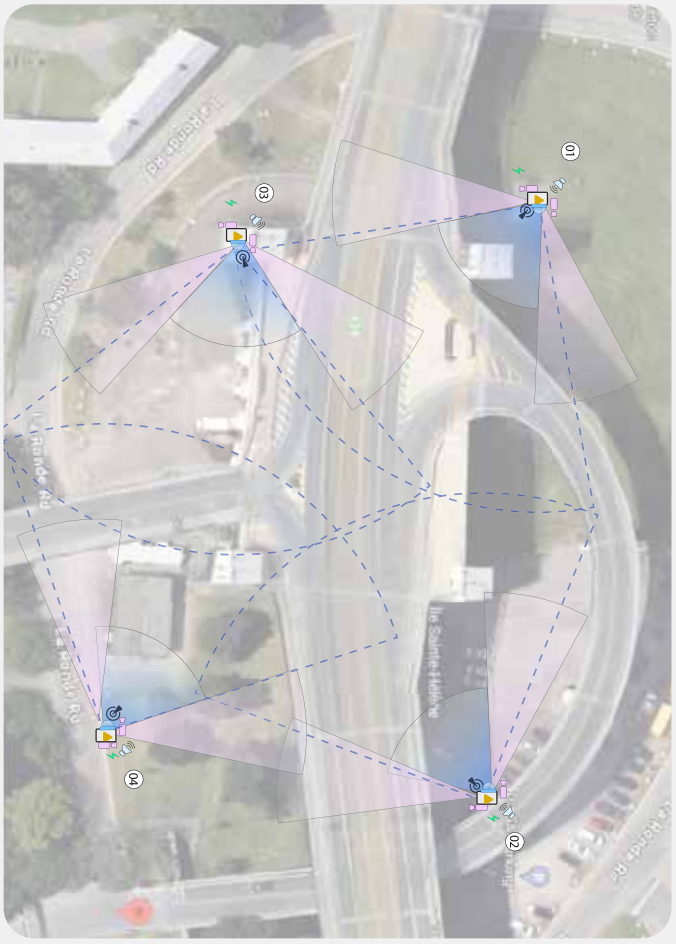
Overcome power & connectivity challenges

No electricity. Rent Sirix's battery-powered all-in-one 4G LTE 5MP HD video security system for reliable monitoring without a power source.

No Internet or Wi-Fi. No Internet or Wi-Fi. Set up your own LTE network or connect to your client's existing network. Test network speed at https://www.speedtest.net/

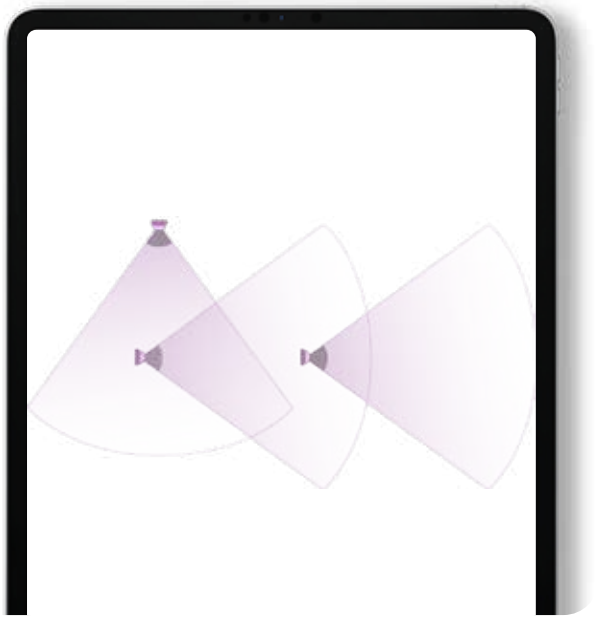
No LTE network coverage. Use satellite or fixed wireless systems for long-range connectivity, or leverage LEO satellite solutions for fast, low-latency internet in remote areas (e.g., Starlink, HughesNet, Xplore).

This structured approach ensures that proper camera placement, as the first step, lays the foundation for effective security.



Sirix offers complete security design plans for its partners, ensuring optimal protection and seamless coverage.

Camera coverage & detection. Optimized.



Overlapping of cameras. Overlapping occurs when two cameras monitor the same area from different angles. This approach significantly increases the chances of detection. If one camera fails to identify an intruder due to a steep angle or limited body visibility, the other camera from a different angle can capture the event.

For optimal security, design your camera layout to ensure all vulnerable areas are covered by multiple fields of view, minimizing blind spots and enhancing detection.

Object detection. Object detection is a key feature of camera analytics, enabling cameras to identify and track objects such as people, vehicles, or other items within their field of view. Using advanced algorithms, the camera analyzes the video feed to recognize objects of interest and trigger alerts.

This function serves as the "brain" of the camera, interpreting what it captures. When a person or vehicle is detected, the system sends an alert to the security team and continues tracking the object within the camera's coverage area, ensuring rapid response and effective monitoring.

Understanding camera coverage.

How far a camera can detect and classify objects depends on three key values.

- **Pixels per foot (PPF)**

  PPF refers to the minimum pixel density required for a camera to correctly classify objects such as humans or vehicles. If the pixel density is too low, the camera may fail to recognize objects accurately, preventing alarms from being triggered.

- **AI engine's megapixel value**

  Cameras do not always use their full resolution for analytics. The AI engine processes video at a reduced pixel density to optimize the camera's CPU performance. Knowing the true megapixel value used during analysis is essential for reliable detection.

- **Horizontal Field of View (HFoV)**

  HFoV determines the width of the camera's view. A narrower field of view extends the detection range, while a wider field of view reduces the detection distance but covers more area.

Recommended general PPF values.

Sirix's Cloud AI systems:

5 PPF at 720p

Standard security cameras:

9 PPF at 480p

Avigilon systems:

9 PPF at 1080p

Fire detection cameras:

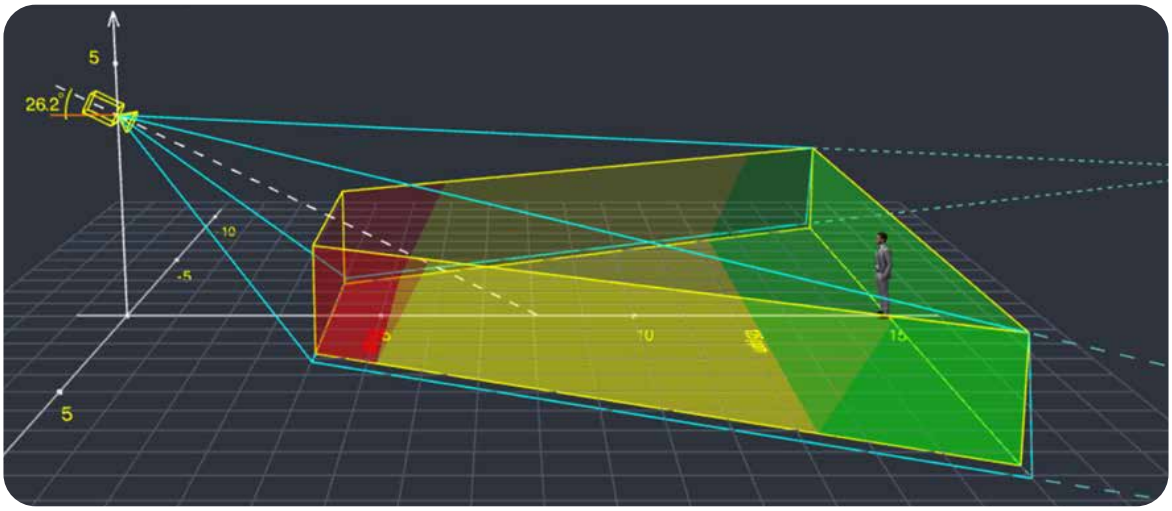
3 PPF at 640x480

Refer to the manufacturer's documentation to confirm the specific PPF, megapixel, and HFoV values for your cameras. For further calculations on lens focal length, pixel density, and coverage zones, use the CCTV lens calculator.

Detection range depends on the camera's **angle & focal length.**

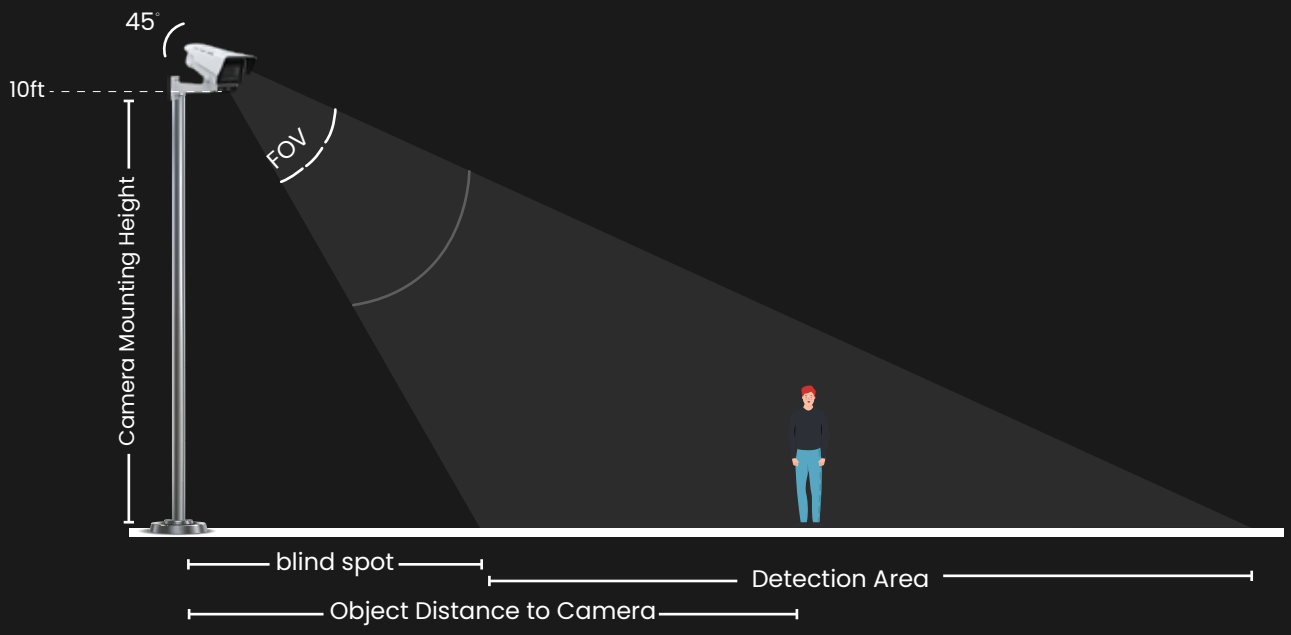
Wide angle (~90º or 2.8mm focal length). Detects objects from **50 to 95 feet.**

Narrow angle (30º or 10mm focal length). Detects objects from **160 to 295 feet.**



Optimal height & angle. For camera placement.

Mounting cameras at the correct height and angle is critical for accurate detection. For outdoor or large indoor areas, cameras should be mounted at a minimum height of 2.8 m (9 ft) and positioned level to the horizon and ground plane. Cameras can be tilted within 30° from the horizontal for optimal object classification, with a maximum tilt of 45° from the horizontal. Increasing the tilt angle can help detect targets that are directly approaching the camera. Any vibration in the mounting surface can hinder the accuracy of object detection, so securing the camera on a stable surface is essential.



Maximizing detection accuracy and performance.

Time to detect

Unlike regular motion detectors, security cameras require 1 to 4 seconds to analyze and classify objects accurately. During this time, the camera often displays a bounding box around the object while the AI confirms whether it is a person, vehicle, or another target. Most AI systems need at least 2 seconds of continuous visibility to trigger an alarm.

Detection & speed limitations

Some AI systems can detect fast-moving objects, like people running, while others may struggle to trigger alarms in such cases. Understanding these limitations is crucial during the design phase, as additional measures—like fence lines—can help enhance security and compensate for potential gaps.

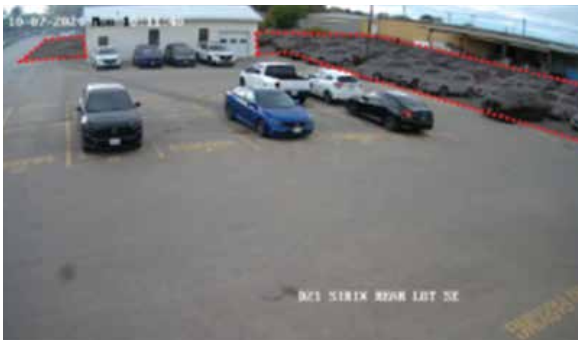
Restrictions on fisheye cameras

Fisheye cameras are not suitable for outdoor remote video monitoring because their wide-angle design spreads pixel density across a large field of view. This reduces image clarity and detail, making it difficult to accurately detect or monitor activities, especially in large outdoor spaces.

For optimal performance, consider using other camera types, which are better suited for detailed monitoring in outdoor environments. If you have specific requirements, contact **Support** for recommendations.

Detection. Things to consider.

Even if vehicles in the background are visible on camera, they may be positioned beyond the camera's detection range, leaving potential intrusions unnoticed. To address this, additional security cameras should be strategically placed to ensure full site coverage.



Even if within the camera's detection range, detection can be compromised if the camera angle limits full visibility of an object (e.g., an individual walking between cars in the shaded area shown above). To mitigate this, additional cameras should be strategically placed to ensure comprehensive site coverage.

Summary

Camera coverage & detection. Optimized.

Overlapping cameras

Place two or more cameras to monitor the same area from different angles. Increases detection chances by covering blind spots from one camera with another.

Object detection

Uses advanced algorithms to identify and track objects like people or vehicles. Sends alerts and continues tracking within the camera's field of view to ensure fast response.

Understanding camera coverage

Pixels per foot (PPF). Minimum pixel density needed for accurate classification.

AI megapixel value. AI processes video at reduced resolution to optimize performance.

Horizontal Field of View (HFoV). Wider views cover more area but shorten detection range; narrower views detect farther but with limited width.

Detection range by focal length

- **2.8mm (~90º):** Detects 50–95 feet.
- **10mm (30º):** Detects 160–295 feet.

Optimal height & angle for placement

Install cameras 2.8–3.7m (9–12ft) high and tilt them 30° to 45° from horizontal. Use stable surfaces to prevent vibration, which can affect detection accuracy.

Maximizing detection accuracy & performance

Time to detect. Cameras need 1–4 seconds of continuous visibility to classify objects.

Speed limitations. Some AI struggles with fast-moving objects; complement with fence lines or other measures to reduce gaps.

Restrictions on fisheye cameras. Fisheye cameras are unsuitable for outdoor monitoring due to reduced image clarity over wide areas; for better results, consider other camera types or contact us for recommendations.

Detection. Things to consider

Beyond detection range. Objects visible in the background may be outside the detection range, requiring additional cameras for full coverage.

Limited by angle. Even within detection range, improper angles can compromise visibility; place cameras strategically to avoid blind spots.

Connecting to the Sirix command center.

Setting up a new site

After installing all security devices on the site, follow these steps to establish a connection with Sirix's command center:

Provide IP address or DNS

- Share the public IP address or DNS, and ensure the recommended manufacturer port forwarding is configured for remote access.
- Common port requirements (all TCP) for supported systems:
  - **Hikvision.** HTTP 80 or HTTPS 443, Server 8000, RTSP 554
  - **Dahua.** HTTP 80 or HTTPS 443, Server 37777, RTSP 554
  - **Avigilon.** Server 38880-38882
  - **AXIS Cameras/Speakers.** HTTP only
  - **Uniview.** HTTP 80, RTSP 554
  - **Any RTSP Camera.** HTTP 80, RTSP 554
  - **AXIS Camera Station.** Server 55756
  - **AXIS Camera Station Pro.** Server 29204
  - **Digital Watchdog/Hanwha Wave.** Server 7001
  - **ExacqVision OEM.** Server 22609, HTTP 80
- For other systems, contact **Support** to confirm required ports and procedures.

Verify internet accessibility

- Ensure all devices and ports are accessible from the internet.
- Use YouGetSignal Port Checker to verify open ports.

IP address filtering (if applicable)

- Add the Sirix monitoring station IP address range:
  - **216.113.34.128/28**
  - **52.26.85.174**
  - **54.187.110.2**
  - **72.193.100.108 (Aktivsense)**
  - **15.204.236.130 (Aktivsense)**
- Once set, request support to test the ports by contacting **Support.**

Connecting to the Sirix command center. (Continued)

Submit required information

- Fill out the provided Technical Form with the following details:
  - Security company name and monitored site name
  - Services required
  - Technology, connection information, and site plan
  - Public IP address (WAN) or DNS name of the device
  - Device HTTP and RTSP ports forwarded
  - Login credentials to the device (NVR/DVR/VMS)
  - Monitored labeled cameras
  - Details of IP speaker used for voice intervention (Speaker model, IP address, port, and login credentials)
  - Date of monitoring start

Test camera settings

- Ensure the live substream is configured with:
  - **Resolution.** 720p or lower
  - **Codec.** H.264
  - **Frame rate.** 4 FPS, 8 i-Frame

On-site testing (optional, but recommended)

- On-site testing is highly recommended to verify the functionality of analytics, alarms, and speaker systems. For detailed instructions on booking and conducting these tests, refer to:
  - **Section 4.2:** Walk Tests
  - **Section 4.3:** Speaker Tests

Site test mode

After completing the on-site tests, Sirix will place the site in test mode for 24-48 hours. This monitoring period allows Sirix to ensure that no excessive false alarms are triggered.

Monitoring start

Monitoring begins after the testing period is complete, unless a different start date is specified in the onboarding forms.

Connecting speakers to Sirix command center

Follow these steps to connect your speakers to the Sirix command center:

Analog speakers

- Contact **Support** to determine the best method for establishing the connection.

IP speakers

- Ensure the speakers are installed within an internet-enabled network.
- Obtain the **SIP account details** (User ID, password, and server name) for each speaker by contacting **Support.**
- **Speaker configuration:**
  - Redirect the speaker's **HTTP port** if you require Sirix to configure it remotely.
- **Schedule a speaker test:**
  - Book a session with Sirix to test the speaker volume across all areas of the site.

GSD speakers

- Redirect both the **HTTP** and **RTSP** ports for proper functionality.
- Contact **Support** for further assistance or clarification if required.

Testing. For total protection.

Walk and speaker tests are crucial both when connecting a new site and on a regular basis to ensure your security system functions properly. These tests verify that alarms, cameras, and loudspeakers operate as intended, maintaining optimal protection and preventing security lapses.

Self-testing for security assurance. After setting up your cameras, it's essential to walk test all equipment to confirm that triggers are functioning correctly.

- **Test in different conditions.** Conduct walk tests at night to identify lighting issues that could affect AI performance.
- **Regular testing.** Schedule regular walk tests to ensure all equipment remains fully operational and security coverage is optimal.

Walk test with Sirix command center. To confirm that Sirix's command center receives all alarms, follow these steps:

1. **Book a meeting**
   - Schedule a 15-minute session with the Sirix team by calling at 1-855-788-1919.
   - Alternatively, email or call **Support**.
   - When booking, clearly provide:
     - The preferred date and time for the meeting.
     - The name of the technician who will be on-site.
     - The name of the site where the walk test will be conducted.
2. **Be on site**
   - Ensure you are physically present at the location to conduct the walk test.
3. **Inform the operator**
   - At the beginning of the meeting:
     - Confirm your name with the operator. Ensure it matches the name provided during booking for security verification.
     - Share the name of the site being tested to help the operator identify the correct location in the system.
4. **Perform the walk test**
   - Walk through the site, passing in front of each security camera to test their responsiveness.
5. **Verify alarm triggers**
   - The Sirix operator will confirm that alarms are logged each time you appear in the camera's view to ensure proper detection.

Speaker test. Ensuring audibility. During the same session, Sirix operators will perform voice interventions through the site's loudspeakers. Verify that the warnings are loud and clear across all areas of the site to ensure effective deterrence.

Why periodic walk tests matter. Periodic walk tests are essential for maintaining your site's security by ensuring all components—cameras, alarms, and loudspeakers—are functioning properly. These tests guarantee that intruders will trigger alarms, allowing operators to respond promptly to prevent theft, vandalism, or other criminal activities.

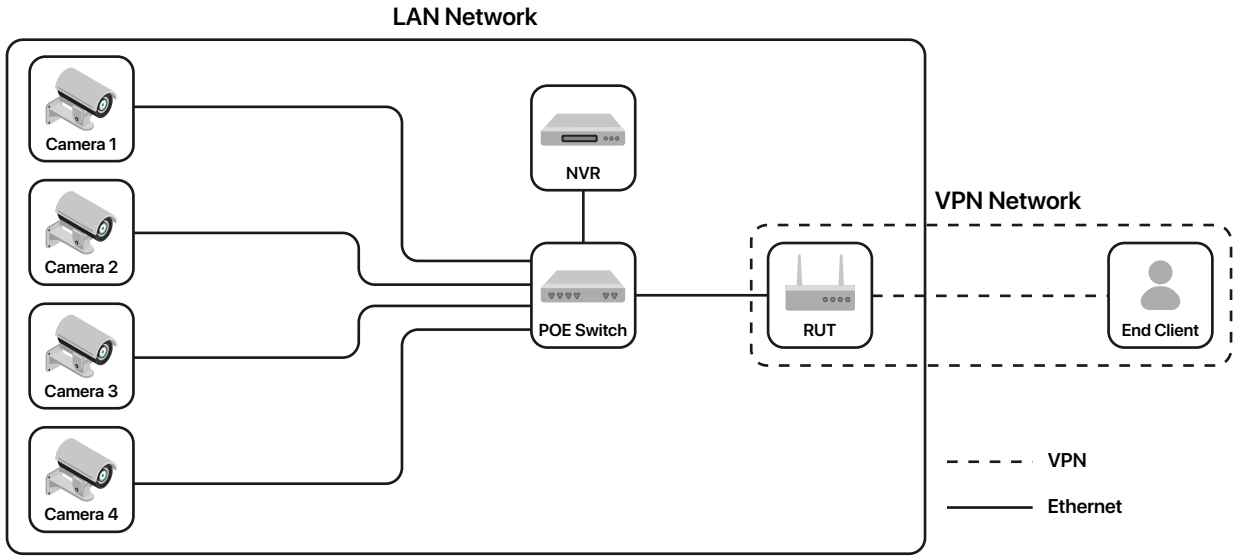
VPN connection

The ideal VPN solution depends on specific requirements, such as speed and whether the connection will be used indoors or outdoors.

To determine the best method and set up the connection:

- Contact **Support** for guidance.

Our team will help you choose the most suitable solution and assist with the setup.



Post-installation checklist for on-site technicians

This checklist ensures that security devices are installed correctly to guarantee total site protection.

Checklist

Please ensure the following steps are completed:

1- Port forwarding is done		
2- Live substream is configured		
3- Alarms/masking are configured		
4- Speakers are configured		
5- Technical Form is completed, including:	a. Admin username and password for NVR/DVR/VMS.	
	b. Surveillance schedule for alerts/alarms using Cloud AI.	
	c. Details for SIP speaker configuration (number and model, if applicable).	
6- A meeting has been booked with the Sirix team for walk tests by calling 1-855-788-1919.		
7- Await confirmation email from Sirix:	a. After completing the walk tests, Sirix will review the site configuration.	
	b. You will receive an email within 2-5 business days confirming the site is live and under monitoring.	

Important notes: This checklist applies to "in-scope" sites only.

In-scope sites

- Sites with an **NVR connected to a camera network with port forwarding.**
- Sites with **individual cameras using port forwarding.**

Out-of-scope sites

- Sites requiring specialized setups such as **VPN, MPLS network infrastructure, radar systems,** etc.
- For **out-of-scope** projects, contact **Support** for assistance.

Partners with SIRIX PRO.

- May skip steps 2, 3, and 4.

Connection issues. Sorted.

Proper handling of connection issues depends on the client dealer's subscription to AktivSense. Here's how it works:

When the client dealer is not subscribed to AktivSense.

- The client dealer is responsible for monitoring device connectivity and resolving disconnections with the end-user.
- If the entire site disconnects, Sirix will receive an alarm and follow the client's Standard Operating Procedure (SOP) until the issue is resolved.

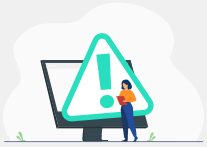
When the client dealer is subscribed to AktivSense.

- Sirix takes full responsibility for managing all device disconnection issues.
- Sirix will follow the client's SOP until the problem is resolved.

What is AktivSense?

AktivSense is Sirix's advanced AI-driven system that monitors the health of security cameras and alerts to issues such as:

Camera view problems



NVR/VMS connection issues

Camera failures

Hard disk failures

Recording issues

Time and date inaccuracies

Learn more about AktivSense here: AktivSense details.

Keeping cameras, NVRs, and VMS systems in check.

Sirix conducts health checks for cameras and VMS/NVR systems to ensure optimal performance, with different levels of support based on the partner's package:

For SIRIX PRO partners.

Remote resolution. If the issue can be fixed remotely, Sirix resolves it promptly and provides a detailed report to the partner and/or end-user once completed.

On-site resolution. If the issue cannot be resolved remotely, Sirix provides clear, step-by-step instructions to help the partner address the problem efficiently.

For non-SIRIX PRO partners.

Sirix sends a detailed report outlining the identified issues and includes instructions for resolving them.

Hard-drive health checks

Sirix supports data retention and corruption checks for the following SD cards, NVRs, and VMS hard drives:

Camera SD cards or NVR hard drives

Supported brands.

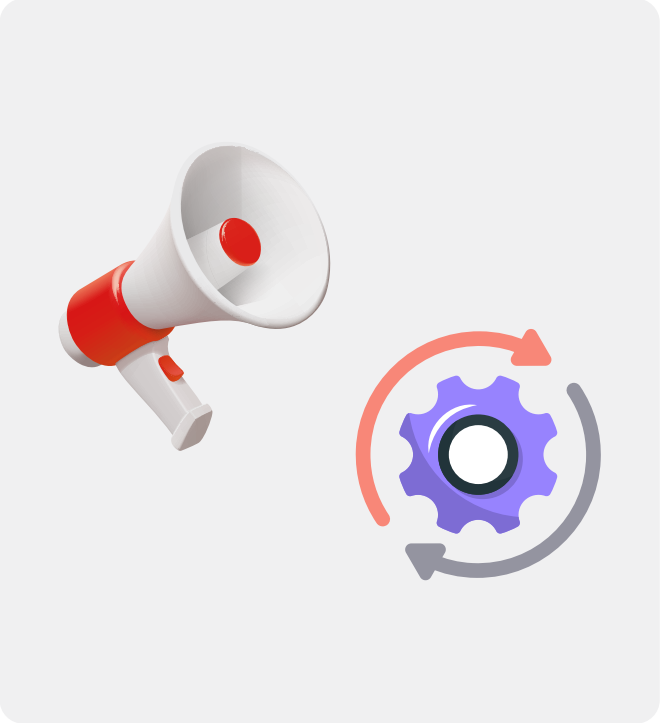
- Axis
- Uniview
- Hanwha Wisenet
- LTS
- GSD
- TVT
- Avycon
- Alibi Witness
- Alibi Vigilant
- Luma
- Turing
- Reolink
- Camect
- Dahua
- Hikvision

Hard drives for VMS systems

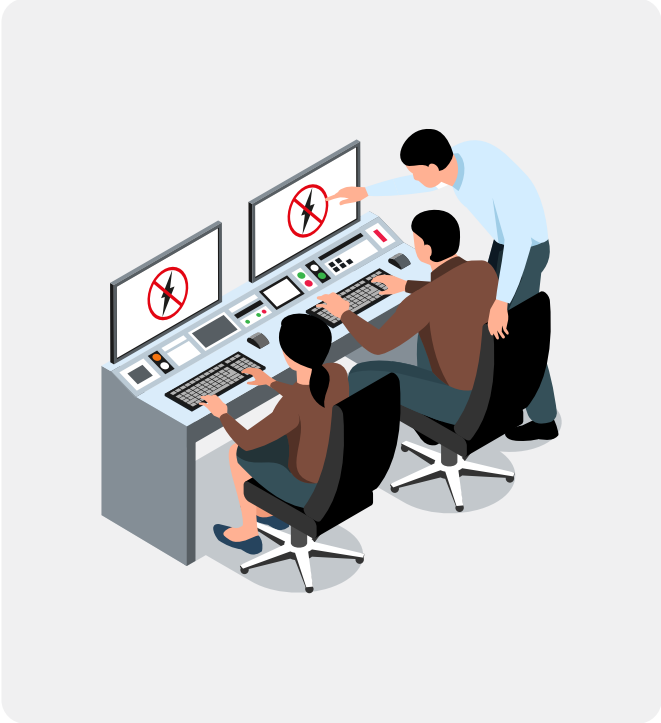
Supported brands.

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

Speakers speaking. Power flowing.



Speaker health checks. For partners using Sirix's Autonomous Security Box or subscribed to AktivSense, Sirix offers real-time monitoring of on-site speakers to detect disconnections. Contact your sales representative for more information.

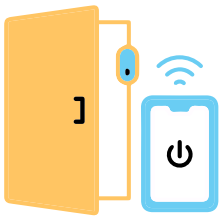


Power outage monitoring. Sirix can detect power outages on a site when the UPS (Uninterruptible Power Supply) is linked to the NVR through a digital output (I/O output). This setup allows Sirix to receive real-time alerts about power disruptions. Once notified, we quickly follow the client's specific procedures for managing site disconnection, ensuring a swift and appropriate response.

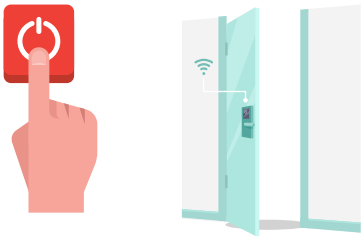
How to link security devices to trigger events

You can link panic buttons, door contacts, motion detectors, or alarm panels to trigger video events or arm/disarm a site by following these steps:

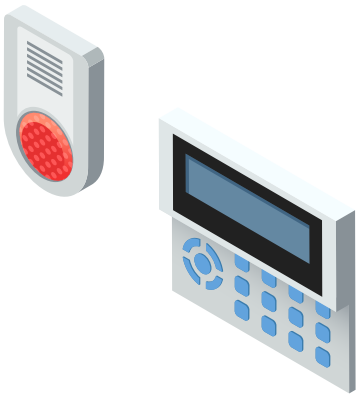
Panic buttons, door contacts, and motion detectors



1. **Connection.** Connect the cables from the device (e.g., panic button, motion detector, or door contact) to the **alarm input** of a supported camera, encoder, or NVR.
2. **Supported devices.** Refer to our **Integration Support list** on the Partner Integration page. Check the "Relays" column to verify if the device is supported (indicated by a checkmark).
3. **Alarm classification.** Sirix will classify alarms triggered by these devices as **ALARMS.** These alarms will be sent to Sirix operators for immediate response.



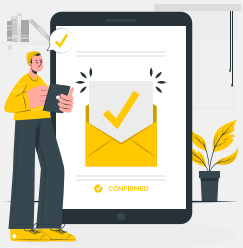
Alarm panel



1. **Connection.** Connect the **PGM output** of the alarm panel to the **alarm input** of a supported encoder, NVR, or camera using the appropriate cable.
2. **Supported devices.** Refer to our **Integration Support list** on the Partner Integration page. Check the "Relays" column to confirm compatibility (indicated by a checkmark).
3. **Trigger classification.** Alarms triggered will result in the site being **armed or disarmed** accordingly.

Sirix mobile app
Install it. Get credentials.

To install the Sirix mobile app and obtain credentials for accessing your site data, please follow one of the methods below:



OPTION 1.

Submit the procedure form.

Complete the Procedure Form with all the required information.

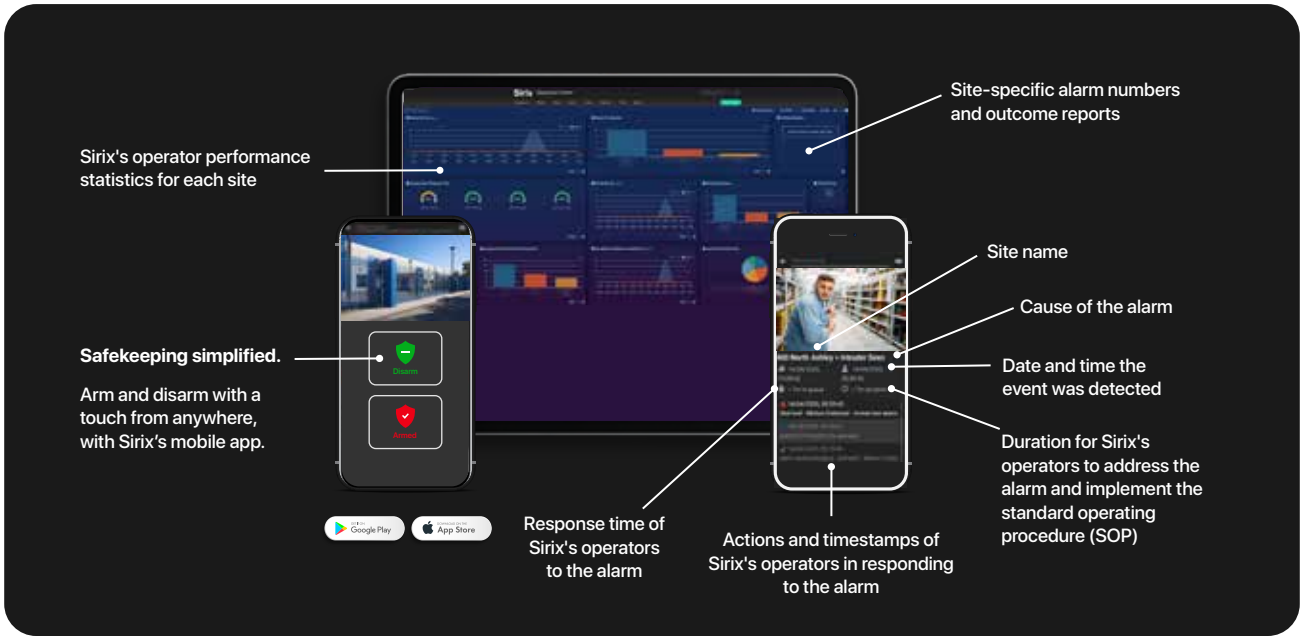
OPTION 2.

Email Sirix support.

Send an email to Support with the following details:

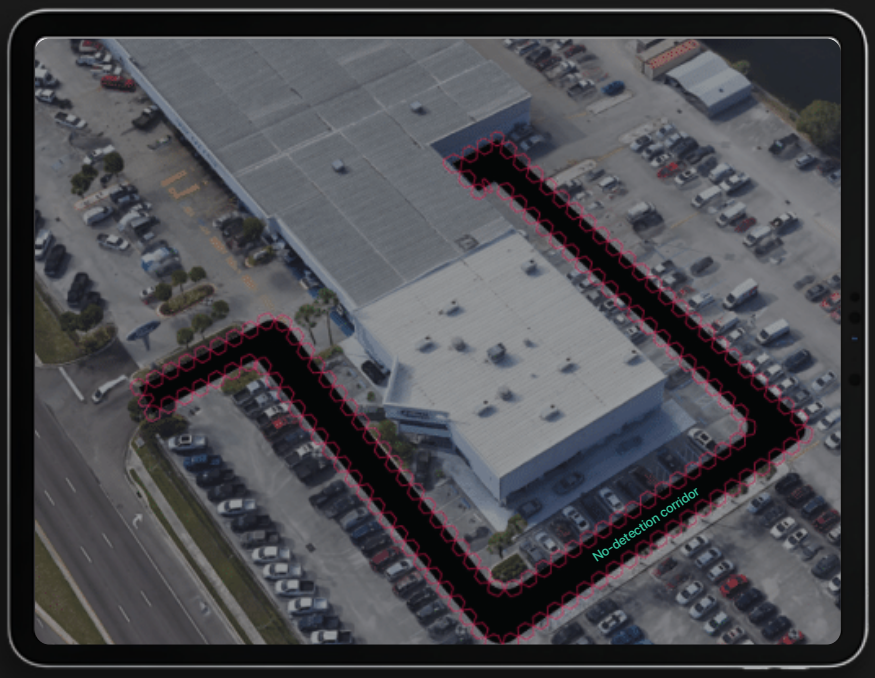
- Name of the person who will use the mobile app.
- Their email address for receiving the app credentials and installation instructions.

Your site in your hands.



Choosing the best arming and disarming strategy

An effective arming and disarming plan is essential for maintaining security during off-hours and minimizing false alarms. Here are three key elements to consider when developing the right strategy for your site:



Establish a surveillance schedule

Ideally, the last person to leave arms the system, and the first person to arrive disarms it. However, to account for human error, it's recommended to set up a default surveillance schedule. A forced schedule can activate 30 minutes after closing and deactivate 30 minutes before opening to ensure consistent coverage.

Select an arming & disarming method

Employees or subcontractors, such as cleaning crews or delivery personnel, must have a reliable way to disarm the system during surveillance hours to avoid false alarms. Options include mobile apps, remote controls, and keypads, allowing flexibility based on the site's needs and operations.

Create no-detection corridors

No-detection corridors are designated zones where movement during surveillance hours does not trigger an alarm. These zones allow early arrivals to access keypads or readers for disarming and can serve functional areas, such as drop-off points or delivery zones.

Admin access. What we need.

Sirix does not require full admin access for the entire duration of your contract. To ensure the security of your system while allowing for smooth technical updates, issue resolution, or configuration changes, Sirix only needs restricted access with the following considerations:

Access is limited to the functions necessary based on:

The features included in your package.

The type of system in use.

Whether the partner is subscribed to **SIRIX PRO.**

This approach minimizes the risk of security breaches while maintaining efficient system management.

Incident video retention time

Sirix stores all incident videos for **90 days** in the Event Portal.

Sirix account activation process.

Establishing a connection with Sirix requires the completion of two forms:

Procedure form

Sirix dealer portal site address: www.portal.sirixmonitoring.com

Procedure form link: Procedure form

Information required to complete the form:

1- Site information	• Site name • Main contact name, number, and email address
2- Site address	• Physical address and/or land location • Special directions or instructions (if necessary)
3- Time zone of the site	• Note. For sites in Saskatchewan, ensure **NO Daylight Savings**
4- Phone number of local police	• RCMP dispatch for rural/remote locations
5- Site description	• Type of perimeter • Important/unique site information • Monitoring area map including perimeter limits and camera layout
6- Alarm response (For Alarm Verification services only)	• Central station name • Account number and site password
7- Special service inclusions	• Sirix Pro? • Autonomous Box (if applicable), Autonomous Box number, and SIM card number
8- Procedure in case of intrusion	• Voice Down, Emergency Call List, Guard Service, Strobe/Siren, Custom Voice Down, IncidentCODE
9- Arm/disarm (monitoring schedule)	• Fully customizable
10- Emergency contact list	• Local police dispatch • Name, phone, email, and password (up to 3 contacts)
11- Authorized contact list	• Name and password (unlimited number of contacts)
12- Mobile app users (if applicable)	• Full name and email (up to 5 users)

13- IncidentCode Users (if applicable)	• Name, SMS, and email (up to 3 users)
14- Site IT or support contact	• Contact type & title • Full name • Company name (if applicable) • Email • Phone
15- Reporting preferences	• Problem reports. Yes or No (Email address required) • Event reports. Yes or No (Email address required)

Technical form

Sirix dealer portal site address: www.portal.sirixmonitoring.com

Technical form link: Technical form

Information required to complete the form:

1- **Site name**

2- **Services being acquired**

3- **Sirix Pro.** Yes or No

4- **Types of detection on-site**

5- **Cloud analytics and type** (camera type)

6- **LTE connection.** Yes or No

7- **Network information**
   - External IP/DNS for server
   - HTTP/HTTPS port and RTSP port
   - VMS name, username, and password

8- **VPN tunnel.** Yes or No

9- **Cameras being monitored and other connected cameras**

10- **IP speaker make/model**

Confirmation and response

Upon submitting both forms, expect a response within 3-5 business days (excluding Fridays).

This allows time for:

- Establishing connections to devices
- Testing equipment
- Making necessary parameter adjustments

Accurate information in both forms ensures a smooth activation process and successful connection with Sirix.

From alert to resolution.

This step-by-step process outlines how Sirix operators handle triggered alarms to ensure rapid and effective resolution.

Alarm handling process

Alarm trigger.

When an alarm is triggered, it appears on the operator's workstation, as illustrated in the image on the left.

Incident review.

The operator clicks on the alarm, displaying:

Left window. Image showing what triggered the alarm.

Right window. Live video feed from the camera that triggered the alarm.

Alarm assessment.

The operator reviews the left window first to understand the cause of the alarm.
They then analyze the live camera footage in the right window to assess the situation.
If the alarm indicates a genuine threat, the operator:

- Opens all site cameras for a comprehensive view.
- Consults the site's specific procedures and notes.

Action.

The operator follows the client's Standard Operating Procedure (SOP) to handle the situation effectively.

Crime stops here.

Voice interventions

First voice intervention

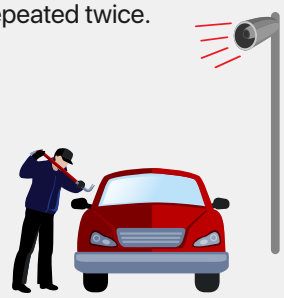
"ATTENTION! ATTENTION! THIS IS SECURITY. PLEASE LEAVE THE SITE IMMEDIATELY OR CALL 1-855-788-1919 TO IDENTIFY YOURSELF."

Repeated twice.

Second voice intervention (15-30 seconds later) - when needed

"ATTENTION! ATTENTION! THIS IS SECURITY. PLEASE LEAVE THE SITE IMMEDIATELY OR CALL 1-855-788-1919 TO IDENTIFY YOURSELF, OR THE POLICE WILL BE DISPATCHED."

Repeated twice.



Escalation

If the intruder remains on-site after the second intervention, the operator escalates to the next step as per the security procedure.

Talking about...
Customized commands. Swift responses.

Personalized voice interventions.

- Voice messages can be customized to align with your client's preferences.
- This option is available only with Axis or GSD speakers.
- Additional fees may apply for this service.

Other security procedures.

Sirix operators follow specific security procedures depending on the situation. Below are the most common procedures in addition to voice interventions:

- Call emergency contact list
- Police dispatch
- Send incident report via IncidentCode
- Activate siren/strobe

Guardians at work.
Actions that protect.

To ensure the site is safeguarded, operators may perform the following actions. Each action is documented in the **Incident Report** that is sent by email in real time. (Refer to **Section 6: Reports** for more details).

- A representative of your staff or cleaning team called in, and their identity was verified using a valid password.
- A delivery vehicle was detected; **Camera X** was temporarily disarmed for 30 minutes.
- A first voice intervention was conducted.
- A second voice intervention was conducted.
- Access was granted to authorized personnel.
- An employee authenticated their identity with a valid password.
- An **IncidentCode** event was initiated.
- Camera X was deactivated for 30 minutes.
- Cleaners entered the premises.
- Emergency contact list was unreachable; voicemail left.
- Individual(s) left the site.
- Individual(s) remained on-site.
- Police were dispatched to the site.
- Police dispatch was canceled.
- Snow removal or site maintenance was identified; the site was disarmed for 30 minutes.
- Staff entered the premises.
- Access rights were verified and confirmed.
- The emergency contact was reached.
- The IncidentCode report was sent.
- The siren and strobe were activated.
- The site was disarmed until a specified time.
- The trespasser was observed leaving the site.
- Vandalism or theft was observed.
- Vehicle(s) left the site.
- Vehicle(s) remained on-site.

This structured approach ensures comprehensive security coverage and transparency in the actions taken.

Security that speaks up.

Voice interventions through on-site loudspeakers are one of the most effective ways to halt intruders and deter criminal activity, using real-time audio warnings to disrupt unlawful behavior and prevent escalation.

Threat detection

When a device detects activity, Sirix operators receive a video alarm.

Footage analysis

Operators review the footage to verify the situation.

Voice intervention

Operators use voice intervention to deter intruders.

Operation success

The intruder leaves the site.

Event recorded

A report is saved in your Sirix portal account.

Ultimate deterrence

Intruders avoid your site as word spreads.

Security procedure alternatives

If the intruder stays, operators follow your SOP, such as contacting authorities or dispatching security.

Where should you place the speakers?

For optimal coverage, install speakers at each corner of the building or along key perimeter points. This ensures that audio warnings are audible from all areas of the property, increasing the likelihood that intruders will hear the message and leave the premises immediately. Strategic placement maximizes deterrence and reinforces security across the entire site.

Sirix audit team
Site performance pros.

Walk and speaker tests are crucial both when connecting a new site and on a regular basis to ensure your security system functions properly. These tests verify that alarms, cameras, and loudspeakers operate as intended, maintaining optimal protection and preventing security lapses.

Causes of false alarms

False alarms can result from:

Video analytics issues. Malfunctions or incorrect configuration of analytics.

Misconfigured detection zones. Detection areas improperly set, such as busy streets or sidewalks.This occurs when cameras are set to detect movement in areas they shouldn't, such as busy streets or sidewalks. These zones should be configured as non-detection zones to avoid false alarms caused by constant activity in these areas.

External factors.

- Inadequate lighting.
- Dirty lenses (e.g., spider webs, water drops).
- Environmental interference.

Protocol errors. Employees or subcontractors failing to follow proper arming/disarming procedures.

How Sirix reduces false alarms

For SIRIX PRO partners.

If the issue can be resolved remotely. Sirix works diligently to fix the problem and provides a report to the partner and/or end-user once resolved.

If the issue cannot be resolved remotely. Sirix provides clear, step-by-step instructions for the partner to address the issue.

For non-SIRIX PRO partners.

Sirix sends a detailed report outlining the issues and provides instructions on how to resolve them.

By addressing these challenges, the Sirix Audit Team helps maintain reliable and efficient site monitoring.

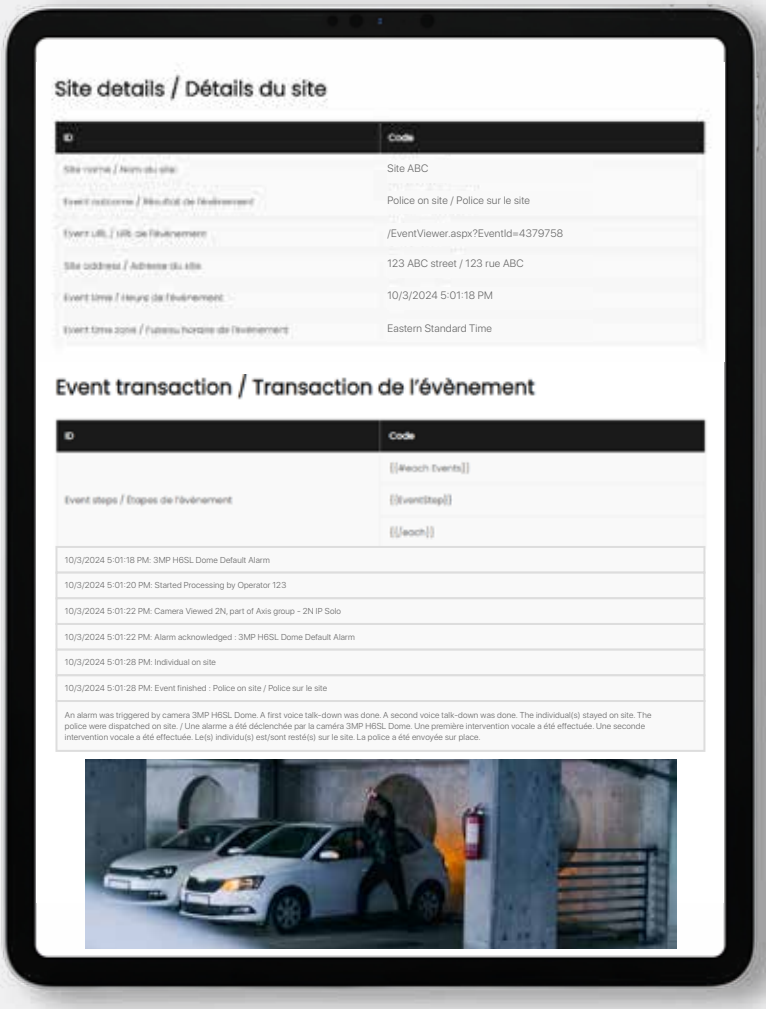
Reports

Transparency delivered.

Sirix provides three types of reports to ensure transparency, quick updates, and clear communication.

Who receives the reports?

- **Incident reports.** Sent instantly to the specified recipients (security partner and/or end-user).
- **Problem reports.** Sent daily, exclusively to partners.
- **Escalated incident reports.** Sent within 48 hours to partners.



Incident reports

Purpose. Incident reports are sent instantly via email to designated recipients (security partner and/or end-user) whenever an operator selects a specific outcome.

Visual evidence. Each report includes a clear image of what triggered the event, providing full transparency and insights.

Access. All incident details are securely stored in the **Sirix Event Portal** (live.sirix.ca).

Triggers. Incident reports are generated for the following outcomes:

- Guard dispatched / Garde envoyé
- Guard on site / Garde sur le site
- Police dispatched / Police envoyée
- Police on site / Police sur le site
- Fire-Water alarm / Alarm feu-eau
- Door-Gate open / Porte-barrière ouverte
- Intruder expelled / Intrus expulsé
- Connection restored / Connexion rétablie
- Patrol completed / Patrouille effectuée
- Alarm central call-in / Appel centrale intrusion
- Staff on site / Personnel sur place
- Script completed / Script effectué
- Patrol completed - Problem observed / Patrouille effectuée - Problème constaté
- VIP protection / Protection VIP

Problem reports

Purpose. Sent once a day to partners, problem reports include both incident reports and details about technical issues affecting the site.

Content.

- **Technical issues.** Reports cover:
    - No footage available / Aucun enregistrement
    - Schedule problem / Problème d'horaire
    - Connection loss / Perte de connexion
    - Voice-strobe not working / Intervention-strobe non fonctionnelle
    - Voice-strobe not configured / Intervention-strobe non configurée
    - Excessive alarms / Alarmes excessives

Escalated incident reports

- **Escalated incident reports** are detailed summaries sent to the security partner within 48 hours when serious events occur—such as theft, vandalism, fire, or confirmed intrusions that required police intervention.

Masking, site, & AI configuration changes

Keeping you informed on site updates

When changes are made to masking, site configuration, or AI configuration, Sirix ensures clear communication and documentation with the following process:

Partner notification

We notify the partner via the email address provided on the Procedure Form, unless another communication method is specified by the partner.

Change confirmation

To confirm the modification, we send:

A **before image** showing the original configuration.

An **after image** reflecting the updated configuration.

This process ensures transparency and allows the partner to review and approve the changes.

AI-powered smoke and fire detection
Lighting the way to safety.

Model definition. Sirix's fire detection model recognizes when a smoke or fire appears into the camera's view when the camera is armed, and differentiates between the two when sending alerts.

How does it work? Our computer vision algorithms are trained on publicly-licensed and proprietary data sets of thousands of images and searches for localized or camera-wide smoke or fire. After detecting smoke or fire for a few seconds, an alert is sent.

Additional model features.

1. Configurable timeframes to generate alert.
2. Configurable alert settings for individual cameras + analytics. Confidence level, ignore zones, frame thresh, crops.
3. Class-specific. Fire, smoke, or both.
4. Cool-down period fully configurable for each camera.
5. Multiple ways to receive alerts. Text, email, VMS, monitoring UI, IMMIX. All alerts are sent simultaneously from our end.

False positive expectations.

1. More FPs during initial testing, greatly reduced when we have optimized the model for each use case.
2. Severe weather (ex. heavy rain) that distorts camera visibility can increase the number of FPs.
3. Fog resembles smoke and has the potential to cause FPs.
4. Features such as ignore zones and confidence level are configurable to limit FPs.

Smoke and fire detection AI
Technical requirements.

Min. FPS	Min. resolution	Detection range	Bandwidth range (50-100% motion)*	SMTP compatible?	Thermal compatible?	Fisheye compatible?
1	480p	3 PPF	~43 kbit/s	No	No	No

*Per camera using motion filter at min resolution and frame rate

Ensure stable internet connection. Unstable connections or frequent outages result in lost frames and detections.

Higher resolutions and frame rates will not necessarily lead to better detections but will increase bandwidth usage. However, high resolution may be helpful in certain cases, such as when the camera is covering a large area.

Fire model is compatible with all general availability integrations, but not available for clips integrations.

Wide ranges of FPS are acceptable, depending on use case. Explosive situations need higher FPS to alert right away. Slower-growing fires can be checked over time at lower FPS.

FAQs

What kinds of fires was this model trained to detect?

It was trained to detect: construction smoke/fires, car smoke/fires, indoor smoke/fires,

It was not trained to detect: chemical fires, fireworks, "unnatural smoke" (vapes, smoke bombs, flares)

When does the model decide to alert? By default, if the majority of frames have smoke or fire detections in a period of 10 seconds, Sirix will alert. In a case where we expect fires to grow slowly such as on a construction site, this can be extended to 30 or 60 seconds before alerting. For sites where explosions are a risk, we recommend using a higher frame rate and a timeframe shorter than 10 seconds.

Why am I seeing false alarms on bright lights or on fog? Video cameras use lenses to capture light and create an image. As lights and fires both generate bright light, the similarity between bright fires and bright lights can cause the light sensors in the camera to create nearly-similar representations. Fog strongly resembles smoke, especially as smoke off-camera blows past the camera lens. Filtering out real smoke is dangerous, so the alert will be sent to the customer to discern.

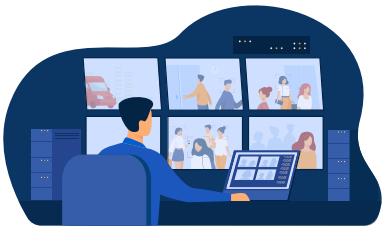
Policies, protocols, and beyond.

Monitoring and billing policies.

Monitoring hours.

A standard monitoring contract includes up to **108 hours per week.** Exceeding this limit may result in additional charges.

For temporary **24/7 monitoring,** the rate is **$55.00 per 10-hour block** beyond the included 108 hours per week.



Engagement period.

Pricing is based on a **minimum 3-month commitment.**

A **$200 activation surcharge** applies for sites connected for less than 3 months.

Canadian & American holidays.

Monitoring services include coverage on Canadian and American holidays as part of the package.

Police-related fees.

If an invoice is issued by the police, the charge will include the police fee plus an additional **15% administration fee.**

Dynamic "script" procedures

For services that require a dynamic "script" procedure, please contact your sales representatives for more details.

Delinquent site policy.

A site is considered **delinquent** when improper arming/disarming or device malfunctions cause excessive false alarms. Sirix does not hold partners responsible for issues outside of their control (e.g., harmless passerby triggers).

Steps to address delinquent sites.

(0 hours)

Notification email. A notification is sent to the partner.

(72 hours)

Second notice. If unresolved after 3 days, a follow-up email is sent.

(96 hours)

Phone follow-up. A call is made to the partner. If unanswered, a voicemail is left.

(144 hours)

Cloud AI implementation. Cloud AI is integrated with the problematic camera.

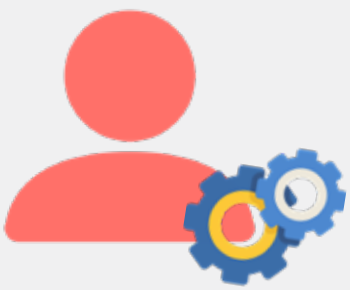
If misuse is identified and the issue persists, Sirix reserves the right to impose a **$1 surcharge** for each false alarm.

Additional resources.

Sirix Pro

Avoid false alarm surcharges by enrolling in this service.

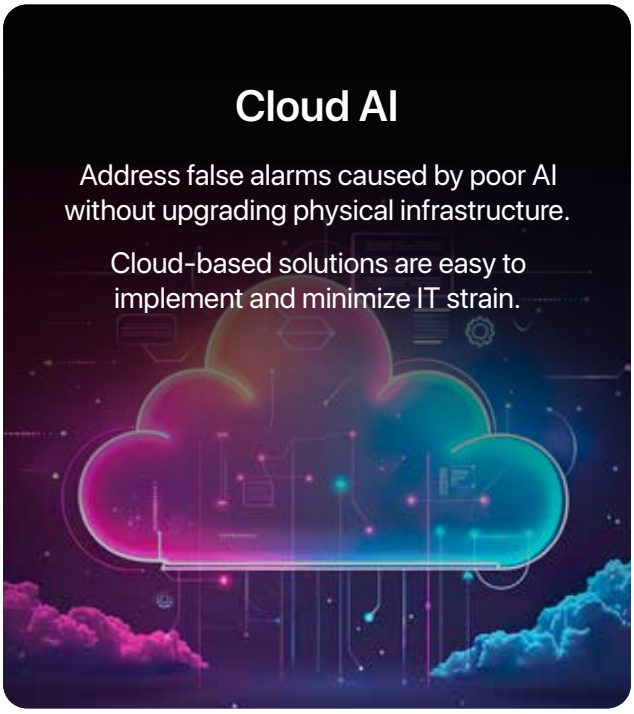
Includes device maintenance and an emergency support line.



Cloud AI

Address false alarms caused by poor AI without upgrading physical infrastructure.

Cloud-based solutions are easy to implement and minimize IT strain.



Disconnection procedures (live monitoring)

Every individual entering the monitored perimeter must disarm the area or notify the Sirix command center. In specific scenarios, alarms are managed as follows:

Towing/delivery vehicles.

Cameras triggering alarms are placed on hold for 30 minutes if a vehicle is identified as towing or delivery.

Security guard.

All devices are placed on hold for 30 minutes if an unannounced security guard is recognized.

Snow removal services.

All devices are placed on hold for 30 minutes if an unannounced snow removal service is recognized.

Landscaping services.

They must call in. Once confirmed, the site will be disarmed for 30 minutes.

Cleaners and employees.

They must identify themselves. The operator will then disarm the affected cameras for 15 minutes to allow entry.

Excessive alarms.

If a device starts triggering false alarms:

First time, the camera or site is disarmed for 60 minutes.

Second time, it is disarmed until the next scheduled rearming.

If the site is disarmed due to excessive false alarms, the loss of communication procedure on file will be followed. A detailed problem report will be sent the following business day morning.

Proactive maintenance.

Clean camera lenses regularly. Clean lenses at least twice a year for clear images. In challenging environments—such as areas with high temperatures, strong winds, dust, or near motorways or construction sites—cleaning should be done more frequently to maintain performance.

Inspect for damage or tampering. Check cameras and equipment regularly for broken, tampered, or misaligned components that could affect system functionality.

Monitor for rust and corrosion. Look for signs of rust on outdoor equipment. Apply protective coatings or replace rusted parts to avoid long-term damage.

Test backup power systems. Check UPS batteries and backup power sources periodically to ensure systems remain operational during outages.

Update firmware and software. Keep cameras, AI engines, and monitoring software up to date with the latest patches to maintain security and performance. Although Sirix typically manages these updates, it's good practice to confirm the system is running on the latest version.

Confirm proper mounting stability. Inspect mounting brackets and fixtures to ensure cameras are stable. Vibration or movement can disrupt object detection and impair system performance.

Run routine system diagnostics. Conduct regular diagnostics to ensure cameras, sensors, and alarms function correctly. This process includes walk tests (as outlined in the previous section - Walk & speaker tests) to identify and resolve issues before they compromise security.

Beyond video monitoring.

To achieve optimal site security, it's crucial to complement video surveillance with additional physical deterrents. Measures like fences, bollards, lights, and warning signs create extra layers of protection, reducing the chances of intrusions. These elements work together with video monitoring to strengthen your security strategy and keep your property safe.

Fences

Fences create a strong physical barrier, making it more difficult for intruders to enter.

- **Placement.** Install fences around the entire perimeter of the property. Use cement blocks in secluded areas to prevent vehicles or other valuable assets from being driven away.
- **Selection.** Steel mesh fences are an excellent option due to their strength and durability.

Bollards

Bollards provide physical protection while maintaining aesthetics, preventing vehicles from unauthorized access.

- **Arrangement.** Space bollards close enough to block even the narrowest vehicle.
- **Selection.** Choose bollards that suit the site's needs, balancing security with visual appeal.

Gates

A secure gate is crucial to preventing intrusions. Weak hinges or poorly fitted gates can easily be breached.

- **Selection.** Match gate hinges with the weight and width of the gate. Choose appropriate locks, latches, and wheels to avoid weak points.

Beyond video monitoring.

Locks

Locks are essential deterrents, showing that security is taken seriously.

- **Types.** Deadbolts, padlocks, electronic locks, smart locks, and biometric locks offer different levels of security.
- **Selection.** Use robust locks to delay intruders, making break-ins more difficult.

Reinforcements for locks

Reinforcing locks adds an extra layer of protection, making it harder for intruders to bypass security.

- **Examples:**
  - **Solid steel hasps.** Provide resistance to prying and cutting attempts.
  - **Hidden shackle locks.** Secure trailers or vehicles with additional barriers.
  - **Anti-theft cases.** Protect container locks with tamper-proof covers.

Adding reinforcements increases the time it takes to break in, discouraging intruders from persisting.

Warning signs

Warning signs alert potential intruders that the site is monitored, deterring unauthorized access.

- **Placement.** Display signs prominently at entrances, around the perimeter, near security cameras, and inside the site.
- **Visibility.** Choose fonts and colors that are legible in all lighting conditions, and avoid obstructions like trees or flags.

Beyond video monitoring.

Lights

Proper lighting is essential for both deterring intruders and enhancing camera performance. Here's how to ensure your lighting setup is effective:

Where to place lights

- **Entrances and exits.** Prevent unauthorized access and make it clear who is coming and going.
- **Perimeter.** Illuminate all boundaries to deter intruders from approaching.
- **Near surveillance cameras.** Improve the camera's visibility and ensure high-quality footage.
- **Warning signs.** Highlight signs to enhance visibility at night.

How to assess your lighting setup

- **Visit at night.** Walk around the site at night to check if every area is well-lit. Pay special attention to entrances, parking lots, and storage areas.
- **Ensure uniform lighting.** Avoid areas with extreme light contrast, which can create shadows and blind spots.

Lighting placement best practices

- **Avoid direct light at cameras.** Bright light sources, such as the sun or headlights, can temporarily blind cameras.
- **Steer clear of reflective surfaces.** Mirrors, shiny floors, or ceilings can cause false alarms due to reflections.
- **Avoid cameras with built-in infrared.** These cameras may struggle with rain, fog, or spider webs, which reflect light and distort images. Instead, use standard cameras with nearby lighting or thermal cameras for better performance.

A well-lit site not only deters intruders but also ensures clear visibility for camera analytics, enabling rapid detection and response.

For more information on physical security measures that complement remote video monitoring, visit our blog.

Useful links.

Price list

For detailed pricing on all Sirix services and products, please **contact your local rep** for the full price list.

Important note. 1 lens = 1 camera. Each camera lens is treated as a separate camera when determining pricing.

Integration partners & support

To view all integration partners and support, please visit our Partner integration page.

Frequently used forms

Link to procedure form.

Link to technical form.

Link to client sheet modification form.

Event Portal

Access live and recorded video footage and view important site details through the Event Portal using this link: https://live.sirix.ca/

FFP calculator

For further calculations on lens focal length, pixel density, and coverage zones, use the CCTV lens calculator.

Helpdesk

To submit a ticket, download forms, or find answers to questions on topics like onboarding, technical support, integration, setup, AktivSense, and more, visit the Sirix Helpdesk.

Sirix

For any questions or assistance, please contact our support team. We are dedicated to prompt problem resolution and mutual success.

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