Verkada

User Guide for Professional Monitoring

Table of Contents

Overview

Verkada offers event-based professional monitoring to help organizations detect, verify and respond to threats as they happen, rather than after the fact once damage is already done.

A Verkada Alarms License is required to use the Verkada Alarms platform, and each license tier includes a different level of professional monitoring.

Using advanced AI person and vehicle detection, Verkada cameras paired with professional monitoring can act as a standalone alarm system. Other Verkada devices, including intrusion sensors, access control, and environmental sensors, can also be configured as monitored alarm triggers for additional site coverage.

If your Alarm License includes video verification (see pg. 4), monitoring agents will review footage of the alarm trigger event to determine if there is a threat to people or property, and will only escalate verified threats.

Customers will be notified of a raised alarm via email, SMS and phone call. Monitoring agents can also request emergency dispatch and talk down to intruders through a powerful on-site speaker.

Monitoring is provided by fully redundant, U.S.-based, UL-listed central stations with Five Diamond Certification from the Monitoring Association. Additional certified monitoring centers are available in the UK, Canada, and Australia.

Alarm License Tiers

A Verkada Alarm License lets you use Verkada devices as alarm triggers and configure custom alarm responses. It also lets you view and manage all alarm events, devices, users, and settings in the Verkada Command dashboard.

Customers can choose from three tiers of the Verkada Alarm License. Each tier includes a different level of professional monitoring.

One Alarm License is required per location (physical address).

LIC-BB Basic Alarm License	**LIC-BA** Standard Alarm License	**LIC-BV** Premium Alarm License	Custom Video Monitoring
Video verification • No video verification	**Video verification** • Up to 100 events/month (~3 events/day) • Up to 50 cameras reviewed	**Video verification** • Up to 1,000 events/month (~33 events/day) • Up to 50 cameras reviewed	**Video verification** • More than 1,000 events/month • More than 50 cameras reviewed
Example use cases • Organizations that have very few alarm events or do not expect false alarms • Organizations that have live guards, an in-house monitoring team, or SOC	**Example use cases** • Buildings that are closed at night and expect no human activity • Restricted access areas, such as storerooms or safes	**Example use cases** • Buildings that expect limited human activity at certain hours • Parking garages that are open at night • Parks or other public spaces at night • ATMs at night	**Example use cases** • Monitor all cash register transactions • Monitor all entrances and exits

How Professional Monitoring Works

Cameras, intrusion sensors, access control, environmental sensors

A site moves into an armed state through an automated schedule, key code entry, badge swipe, Command, or the Alarms mobile app. If an exit delay is set up, the site will wait that amount of time after a key code is entered before arming the system.

A camera, intrusion sensor, access control device, or environmental sensor detects activity when the site is armed. (NOTE: environmental sensor events are never video-verified.)

Video verification enabled

The trigger event and footage from nearby cameras (if applicable) are sent to a professional monitoring agent on the "verify team." The agent will verify the event according to the customer's chosen Verification Rules. There are three options:

Normal security

If the verify agent sees a visible threat to people or property, they will raise an alarm.

If the verify agent does not see a threat to people or property, they will dismiss the event. The event is logged in Command and the agent loses access to the customer's cameras.

END

Max security

If the verify agent sees any person present (regardless of behavior or appearance), they will raise an alarm.

If the verify agent does not see anyone present, they will dismiss the event. The event is logged in Command and the agent loses access to the customer's cameras.

END

Custom rules

If the activity observed on camera matches the rules set by customer (see pg. 11), the agent will follow the designated instructions for that rule:

Raise alarm: The verify agent will raise an alarm.

Notify only: The verify agent will notify the customer and then dismiss the event. The event is logged in Command and the agent loses access to the customer's cameras.

END

Do nothing: The verify agent will dismiss the event. The event is logged in Command and the agent loses access to the customer's cameras.

END

Video verification not enabled

An alarm is automatically raised.

Alarm Raised

Emergency dispatch enabled

Camera footage[1] is sent to a professional monitoring agent on the "dispatch team" for response. If the dispatch agent sees an emergency in progress, they will immediately notify law enforcement. If there is suspicious activity but not an active emergency, the agent will first talk down to the intruder (if enabled). In parallel, SMS/email notifications (including a link to view the trigger and/or context camera footage) will automatically be sent to the contact list. If configured, any automated alarm actions (e.g. alarm outputs, lockdown) will also take effect.

The dispatch agent will call down the contact list and explain what actions they have taken so far. If the police have not already been notified, the agent will ask the customer if they would like dispatch. The agent will attempt to call each person on the contact list two times. If no contact responds, the agent will proceed to call dispatch.[2] While an alarm is active, any contact may call back the agent at any time and request action be taken. If dispatch was already contacted and the customer requests it to be canceled, best efforts will be made to call off emergency services.

When the alarm event has concluded, the customer can resolve the alarm. The customer can also ask the agent (via phone or SMS) to resolve the alarm, while keeping the site armed or temporarily disarming the site (for up to 12 hours). If the alarm has not been resolved after one hour, the agent will resolve the alarm event. An alarm report is logged in Command and both the verify and dispatch agents lose access to the customer's camera(s).
NOTE: If dispatch was going to be contacted but the alarm was resolved first, the dispatch request will not proceed. If the alarm is resolved after the police have already been contacted, best efforts will be made to call off the police.

If the site remained armed at the conclusion of the alarm event, the site can later be disarmed through automated schedule, key code entry, badge swipe, Command, or the Alarms mobile app. If an entry delay is set up, the system will wait that amount of time after a trigger event is detected before raising an alarm.

END

Emergency dispatch not enabled

SMS/email notifications (including a link to view the trigger and/or context camera footage) will automatically be sent to the contact list.

If configured, any automated alarm actions (e.g. alarm outputs, lockdown) will also take effect.

When the alarm event has concluded, the customer can resolve the alarm.

An alarm report is logged in Command and, if applicable, the verify agent loses access to the customer's cameras.

The site will remain armed at the conclusion of the alarm event, until it is disarmed through automated schedule, key code entry, badge swipe, Command, or the Alarms mobile app.

If an entry delay is set up, the system will wait that amount of time after a trigger event is detected before raising an alarm.

END

[1] This includes (if applicable) live video of the camera that triggered the alarm, live video of emergency dispatch context cameras, and/or historical video clips that have been video-verified by the Verify team.

[2] If the alarm site is in Test Mode, the agent will raise an alarm but will not request police dispatch if no contact can be reached. However, if the site is in Test Mode and the agent sees an active emergency in progress, they will still request police dispatch.

Panic buttons, duress code

A wireless or digital panic button is pressed, or a duress code is entered. Panic and duress are never video-verified, and will always raise an alarm, whether or not the site is armed.

Emergency dispatch enabled

The trigger event and footage from emergency dispatch context cameras (if applicable) will be sent to a professional monitoring agent on the "dispatch team".

SMS/email notifications (including a link to view the trigger and/or context camera footage) will automatically be sent to the contact list.

If configured, any automated alarm actions (e.g. alarm outputs, lockdown) will also take effect.[1]

Immediate dispatch on panic enabled

The dispatch agent will bypass calling the contact list for confirmation, and will proceed immediately to request emergency dispatch.[2]

Immediate dispatch on panic not enabled

The dispatch agent will call down the contact list to confirm if there is a legitimate emergency and ask the customer how they would like to proceed.

The agent will attempt to call each person on the contact list two times. If no contact responds, the agent will proceed to call dispatch.[2]

If the agents sees an active emergency in progress via context cameras, they will bypass the contact list and request dispatch first.

When the alarm event has concluded, the customer can resolve the alarm. The customer can also ask the agent (via phone or SMS) to resolve the alarm. If the alarm has not been resolved after one hour, the agent will resolve the alarm event.

An alarm report is logged in Command and the dispatch agent loses access to the customer's context cameras.

NOTE: If dispatch was going to be contacted but the alarm was resolved first, the dispatch request will not proceed. If the alarm is resolved after the police have already been contacted, best efforts will be made to call off the police.

END

Emergency dispatch not enabled

SMS/email notifications (including a link to view the trigger and/or context camera footage) will automatically be sent to the contact list.

If configured, any automated alarm actions (e.g. alarm outputs, lockdown) will also take effect.

When the alarm event has concluded, the customer can resolve the alarm.

An alarm report is logged in Command.

END

[1] Panic button only. For safety reasons, no automated alarm actions will take effect if a duress code is entered.
[2] If the alarm site is in Test Mode, the agent will raise an alarm but will not request police dispatch if no contact can be reached. However, if the site is in Test Mode and the agent sees an active emergency in progress, they will still request police dispatch.

Use and limitations

Professional monitoring with video verification is designed for event-based monitoring. Monitoring agents will only review short video clips from events designated as alarm triggers by customers in Command. Customers should not use professional monitoring to monitor spaces where continuous video monitoring is required, or for any situation where a threat to people or property would not be self-evident from the video footage. Accurate person detection requires a minimum level of detail, expressed quantitatively as pixels per foot (PPF), which varies by camera model (see pg. 17).

Professional monitoring with video verification is provided by fully redundant U.S.–based, UL–listed, TMA Five Diamond certified central stations. For local emergency dispatch, additional certified monitoring centers are available in Canada, the UK, and Australia. Visit verkada.com/alarms-availability for a complete list of countries where Verkada Professional Monitoring is available, as well as to see monitoring center certifications by region. Verkada will disclose monitoring provider information to prospects, customers, or partners that request the information under NDA.

Setting Up Alarm Triggers

Once a site is set up as an alarm site, events from any device in the organization can become alarm triggers that monitoring agents will review and escalate as needed.

Each site is capable of having its own alarm triggers, customized responses, arm/disarm schedule, etc. Make sure to configure your desired settings for each alarm site separately.

Start by specifying the physical location of your site. Verkada will use this address in the event emergency services need to be dispatched.

Setting up cameras to be monitored

When you designate a camera as an alarm trigger, you will be asked to select which type(s) of behavior should raise an alarm. You may configure more than one option:

Person detection

If a person is detected in the camera's field of view, it will trigger an event. You can also get more granular by specifying a "region of interest" (Image 1). This is the only area where person detection will trigger an alarm event; people detected outside that region will be ignored.

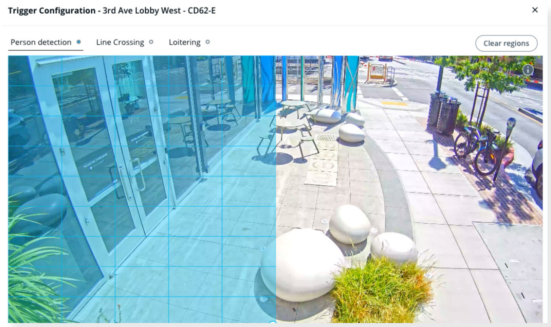


Image 1: Region of interest

Line crossing[1]

Allows you to set a line and specify the direction(s) of travel (person or vehicle[2]) you care about. The trigger is tripped if there is detection on the line crossing you set. In (Image 2), for example, the trigger would trip only if a person went in or out of the door, and would omit pedestrian traffic on the sidewalk.

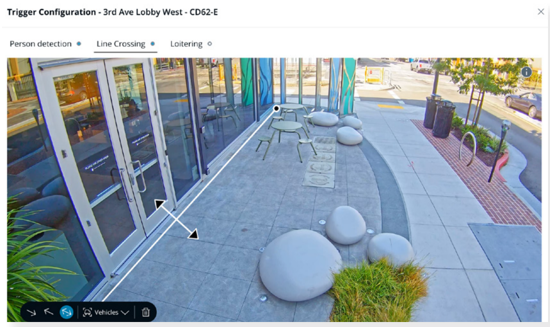


Image 2: Line crossing

Loitering[1]

Allows you to define a region and how long a person or vehicle[2] has to stay in that region before an alarm event occurs (Image 3). This helps to detect a person or vehicle that is loitering near a building, rather just passing by. This trigger type is intended for any area with expected public activity, such as outdoor cameras facing a public space or where people may be loitering near shop premises.

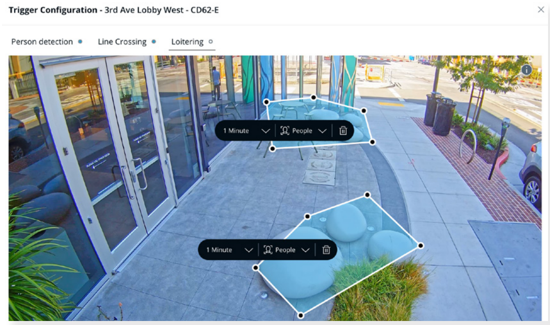


Image 3: Loitering

We strongly recommend configuring line crossing or loitering as both features provide more granularity than person detection and can help avoid unnecessary verification events.

[1] These features are only available on camera models that end in "2" or higher (for example, CD42, CD52, CD62, etc.) and CF81 in Panoramic mode only.
[2] Vehicle detection events are not video-verified and will automatically raise an alarm.

Additional alarm triggers

In addition to or instead of cameras, organizations can configure events from any of the following devices as alarm triggers that can be monitored:

Wired sensors

Third-party wired sensors (motion, panic, glass break, etc.) Nearby cameras can be associated with these sensors for video verification.

Wireless sensors

Verkada's wireless motion, door contact, panic button, glass break, or water leak sensors. Nearby cameras can be associated with these sensors for video verification.

Access control

A Verkada access controller can trigger an alarm based on a door open, door held open, or door forced open event. Nearby cameras configured in Access Control will automatically be used for video verification.

Air Quality Sensors

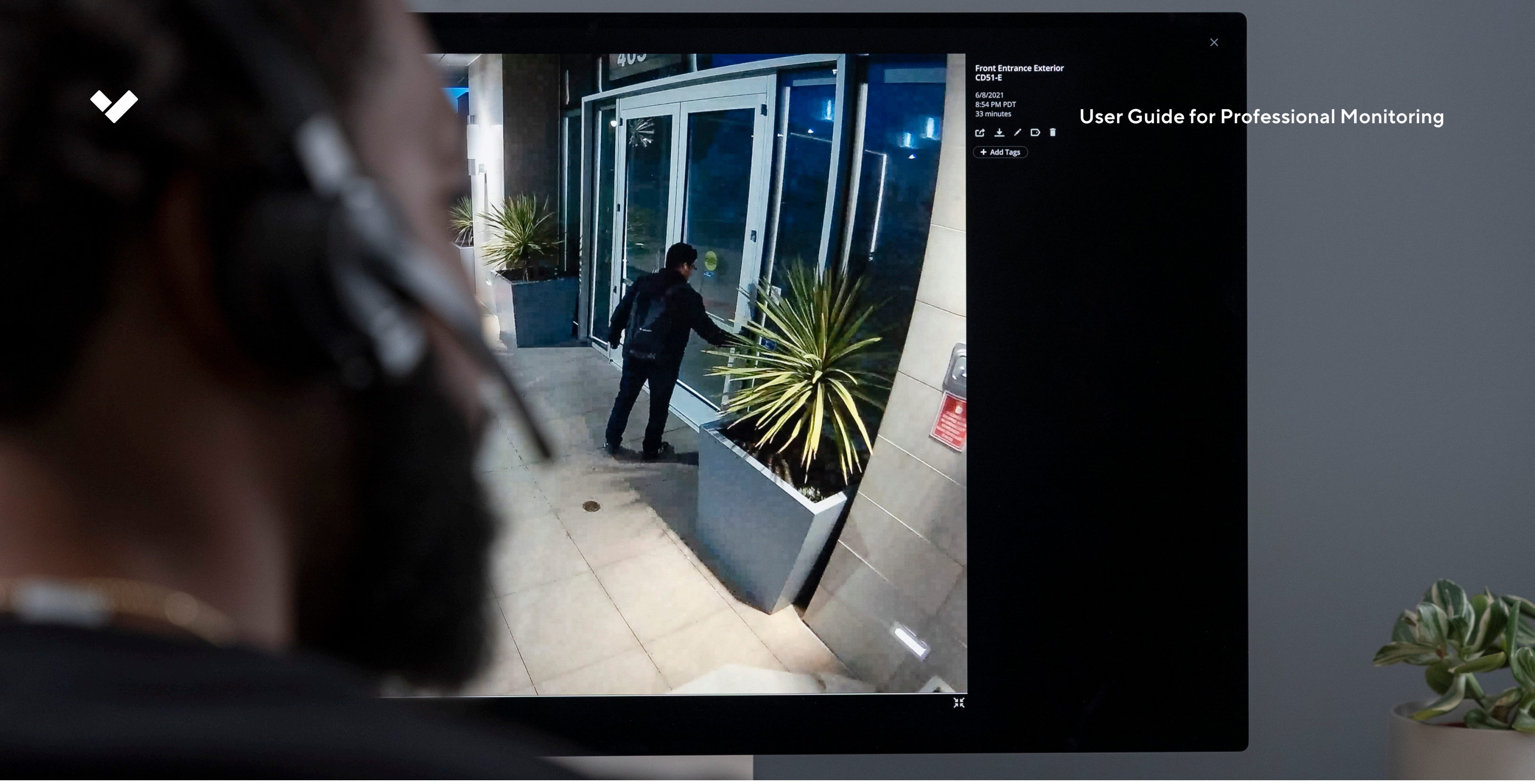
Verkada Air Quality Sensors detect motion, changes in temperature, humidity, noise, etc. Air Quality triggers are not video verified.

Intercom

A Verkada Intercom can trigger an alarm based on a door open, door held open, door forced open or as a camera trigger.

Offline events

An alarm device going offline can trigger an alarm.



Video Verification

What is video verification?

Verkada offers alarm monitoring with the LIC-BB Basic Alarm License and video verification with the LIC-BA Standard Alarm License or the LIC-BV Premium Alarm License.

Verkada's video verification allows monitoring agents to review video when an alarm event is triggered to determine if there is a legitimate threat. If the organization uses cameras as alarm triggers, agents will review the footage in which a person detected on camera triggered the alarm. For non-camera alarm triggers, agents will review footage from the specified nearby camera(s).

Customers must opt-in to video verification; it is turned off by default. Customers can check the number of events that have been video-verified that month through the "Location" section in the Settings page of the alarm site. They can see a summary of verifications for all sites in the Reports section of Alarms in Command.

Traditional alarm monitoring versus video-verified alarms

Alarm monitoring is a common service for alarm systems. If an intrusion sensor (e.g. motion detector) is tripped, that alarm signal will go to a professional monitoring agent. The agent will notify the customer and ask for instructions, such as requesting police dispatch or canceling the alarm without taking further action. With traditional alarm monitoring, the agent is usually not able to provide additional information about why the alarm was triggered.

With extremely high rates of false alarms, many police departments will no longer respond to non-verified alarms, or they will de-prioritize the dispatch request. Many municipalities also impose fines for organizations that report more than a certain number of false alarms in a given time period.

Video verification is hugely beneficial because it gives monitoring agents access to live and historical camera footage to help determine why an alarm was triggered and screen out false alarms. Moreover, many police departments consider a video-verified alarm to be an "eyewitness crime" and will prioritize responding to that event quickly.

Setting up video verification

1. **Normal security:** Monitoring agents will only raise an alarm if there is a visible threat to people or property. If there is no visible threat, or if the situation is ambiguous, the agent will dismiss the alarm. This is recommended for most installs.

2. **Max security:** Agents will raise an alarm if a person is detected on camera, regardless of what they are doing. This setting is intended for high-security areas in which no one should be present while the site is armed.

3. **Custom rules:** Customers have the ability to specify whether the agent should raise an alarm, notify the customer, or do nothing in response to different scenarios. Scenarios include:

   Threat to person or property:

   An agent witnesses a visible threat to people or property. The agent response for this category is always fixed to raise an alarm and cannot be customized.

   Agent cannot determine threat:

   The agent sees a person but is undecided if they are a threat.

   Unknown person INSIDE business:

   There is no visible threat, but the agent sees a person inside a business who does not appear to be an employee or emergency service personnel.

   Unknown person OUTSIDE business:

   There is no visible threat, but the agent sees a person outside a business who does not appear to be an employee or emergency service personnel.

   Emergency service personnel on site:

   There is no visible threat, but the agent sees one or more people that appear to be emergency service personnel.

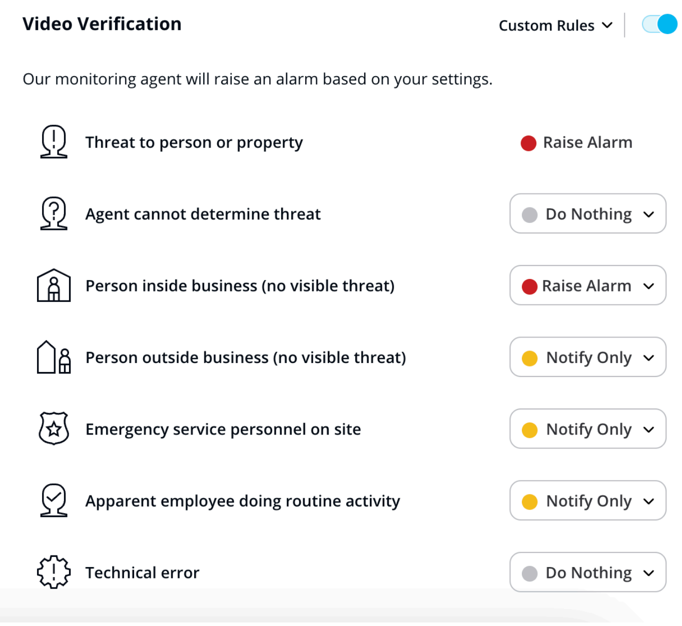
   Apparent employee doing routine activity:

   There is no visible threat, but the agent sees a person who appears to be an employee doing routine activity. The person may be wearing a uniform and/or clearly performing work-related tasks.

   Technical error:

   The video could not be viewed due to technical issues.

Verkada's 24/7 professional monitoring service can verify all alarm triggers with video from Verkada cameras.



Video Verification — Custom Rules

Our monitoring agent will raise an alarm based on your settings.

Threat to person or property	● Raise Alarm
Agent cannot determine threat	● Do Nothing
Person inside business (no visible threat)	● Raise Alarm
Person outside business (no visible threat)	● Notify Only
Emergency service personnel on site	● Notify Only
Apparent employee doing routine activity	● Notify Only
Technical error	● Do Nothing

Available agent responses include:

Raise alarm

Monitoring agent follows normal alarm procedures, as specified in your site settings.

Notify only

Verkada only sends automated SMS and email notifications to your contact list. The event does not raise an alarm. Note: You will not be able to contact the agent by responding to the text since it is an automated message.

Do nothing

The event is dismissed. No notifications are sent and the event does not raise an alarm.

Monitoring Agent Responses

Organizations can choose one or more alarm responses per site. If configured, some of these responses will take effect automatically when an alarm is raised, including:

- Contact list notifications via SMS and/or email, including a link to view the alarm event in Command
- Turning on a deterrence device (siren, strobe, etc.)
- Playing a pre-recorded alert message or siren sound via the BZ11 Horn Speaker or BC82 Alarm Console (Note: if automatic speaker alerts are configured, an alert message will play via the BZ11 Horn Speaker immediately after an alarm event is detected, prior to an actual alarm being raised)
- Locking doors via Verkada Access Control

Other response actions - including requesting emergency dispatch and talking down to intruders - are taken by monitoring agents.

Emergency dispatch

Organizations can choose to allow monitoring agents to request emergency dispatch on their behalf.

If a monitoring agent observes a visible emergency or crime in progress, they will skip the normal alarm handling procedure and immediately notify emergency services before taking any other action.

If a monitoring agent observes suspicious activity, but not an emergency, they will first call down the customer's contact list in the specified order. The agent will explain the alarm event to the customer and ask them what action they would like to take. If no customer contact can be reached, the agent will proceed to notifying law enforcement.

Options for configuring emergency dispatch:

- **Emergency dispatch context cameras:** Monitoring agents by default do not have live access to your cameras. This setting allows you to grant the monitoring agents a live stream of up to a maximum of 10 cameras alongside any footage that has been video-verified to gather additional context during an active alarm. Due to typical site bandwidth constraints, we recommend choosing no more than 5 cameras to share.

- **Immediate dispatch on panic:** When enabled, monitoring agents will dispatch emergency services immediately without verifying the event or contacting the customer. This only applies to duress and panic alarms.

  Monitoring test mode (see pg. 16): If enabled, the monitoring agent will still reach out in the order of your contact list, but will not dispatch emergency services if they are unable to reach you.

- **Permit number or URN:** You can add an optional permit number or URN to be shared with emergency services when dispatch is requested. This may be a requirement in certain regions.

Talk down

Verkada's professional monitoring agents have the ability to remotely talk down to an intruder to try to scare them off.

Agents talk down via Verkada's BZ11 Horn Speaker, which is paired with one or more cameras in an alarm site. Note that agents can only talk down through cameras that triggered an alarm, are specified as nearby cameras, or were sent as emergency dispatch context cameras. Make sure, therefore, that at least one of the cameras received by the agent has a speaker associated with it.

Normal event flow

If the agent sees something suspicious on camera, they can initiate talk down directly from the camera feed. If enabled, the agent will request emergency dispatch regardless of the outcome of talk down. The agent will then call down the customer's contact list, describe the result of talk down, and request next steps from the customer. At this point, you may choose to have the agent contact dispatch, if they have not already, or resolve the alarm and either leave the site armed or temporarily disarm the site.

Exceptions

There are two exceptions to this flow:

1. If your site panics (from a panic button, duress code entry, and/or web panic), and agent talk down is enabled along with "Immediate Dispatch on Panic", the agent will call dispatch directly before initiating talk down, and the rest of the flow will proceed normally.
2. If your site panics (from a panic button, duress code entry, and/or web panic), and agent talk down is enabled along with "Immediate Dispatch on Panic", and silent panic is enabled for your device, the agent will not perform talk down. A silent panic overrides all settings for agent talk down. The agent will directly call dispatch and no alarm output will trigger at your site.

What will the agent say?

The talk down script will contain:

- Description of person (within reason)
- Description of activity (within reason)
- Description of agent action if person does not cease described activity

Furthermore, agents will give a reasonable amount of time for intruders to cease activity before calling through the contact list. A sample script may look like this:

"Person with dark clothing and covering face with a mask attempting to peek inside building, you are on monitored private property. Cease all activity immediately, otherwise police will be dispatched."

The agent may repeat the script until it is reasonably clear that the person has either left the property entirely or refuses to leave the property.

Schedule overrides

Certain use cases may require that your verification settings or alarm responses change during different time periods. The system will follow the default rules for a given alarm site unless an override is configured.

How does schedule override work?

This feature allows you to specify a timeframe where the system can override the default configuration to follow a different set of rules.

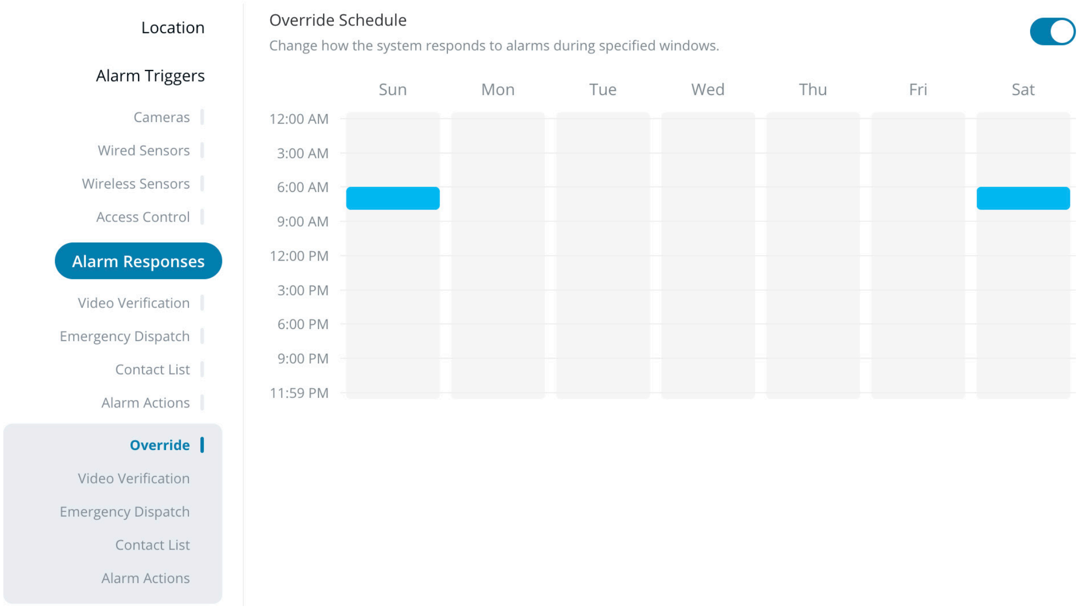
For example, your site is armed between 10 PM and 8 AM, 7 days a week to follow the rules as follows:

- Video verification set to Max Security
- Contact the night shift security guard
- Enable a siren when an alarm is raised

However, starting at 6 AM on weekends, maintenance sometimes comes around and has been known to trigger cameras, and there is a shift change from the night guard to the day guard. You want your system to follow these set of rules:

- Video verification set to Normal Security
- Contact the day guard following the shift change
- Disable any siren to avoid disruptions

Using the schedule override feature, you can configure the system to follow a different set of rules from 6–8AM on weekends.



Override Schedule

Change how the system responds to alarms during specified windows.

Setting up a schedule override

1. In site settings, scroll down to "Override" under Alarm Responses (highlighted in blue)
2. Start by selecting the timeframe in which your override rules should take effect
3. Below you can configure an override for video verification, emergency dispatch, contact list, and/or alarm actions

Arm / Disarm Settings

Alarm triggers and responses will only take effect when a site is armed. Verkada offers multiple means of arming and disarming your site, as well as additional settings to customize your site.

Arm/disarm options

Schedule: Automatically arm the site during specified days/times.

Key Codes: Users can enter a key code via the BK11/BK21 Alarm Keypad or the BC82 Alarm Console to arm or disarm the system. You can add multiple general key codes and/or individual user key codes that will work across every site that user has access to.

Badge Swipe / Door Unlock: Select which doors automatically arm or disarm the site when the door is unlocked via a badge swipe. This option is only available if a Verkada access controlled-door exists in the site. Note the exit delay is 20 seconds.

Web: Arm or disarm a site in Command by using the toggle in an alarm site's Activity page.

Alarms App or Command App: Arm/disarm by selecting the shield icon next to the Alarms site.

Additional settings

Entry Delay: Number of seconds to wait after a trigger event occurs before raising an alarm or verification.

Exit Delay: Number of seconds to wait after entering the code entry before arming site.

Geofence Arm/Disarm: Restricts Verkada Alarms mobile app arm/disarm when the user is within 200 meters of the alarm site.

Auto Re-Arm: If disarmed during the arm period, automatically re-arms the site after a set period of time.

Auto Disarm: Automatically disarms the site at the end of the schedule.

Arm/Disarm Notification Window: Receive a notification whenever an arm/disarm occurs within a specific time range.

Output on Arm: A wired output is enabled when the site is armed and disabled when it is disarmed.

Toggle via Doors: Toggle between armed/disarmed for this site when one of these doors grant access.

Duress Key Code: You can enter this code to trigger a panic alarm on the BC82 Alarm Console or BK11/21 Alarm Keypad in case of an emergency. When a duress code is entered, the system disarms the site, but still triggers alarm notifications and emergency dispatch (if enabled).

Testing Your Alarm System

After you have configured your desired alarm triggers, video verification settings, and response(s), you should validate system operations by raising a test alarm.

When the system is placed in test mode, the system and monitoring agents will still go through your custom Alarms flow, but will NOT dispatch emergency services unless you explicitly request it.

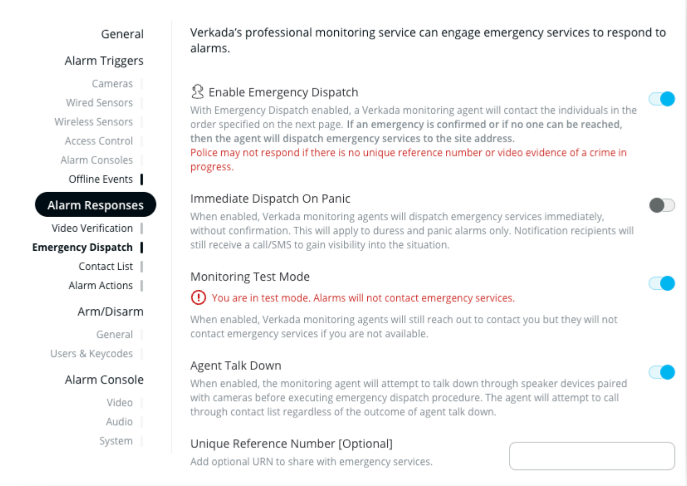
How to set up a test alarm

1. In site settings, click on "Emergency Dispatch" under Alarm Responses
2. Enable Emergency Dispatch
3. Enable Monitoring Test Mode
4. For testing purposes, we suggest setting Video Verification to Max Security so that agents will raise an alarm when an alarm event is detected.

Arm your site and trip one of your alarm triggers. You should receive a call from a monitoring agent, per your response flow. Users on the contact list can resolve an alarm by spelling out their last name and phone number associated with their account to the monitoring agent. Command users can also manually resolve the alarm banner or by disarming their system.

In Command, you can then expand the alarm-raised event by clicking the red See Details button. In this view, you will see details on the flow of events for the raised alarm event, including the list of device events and context camera footage for said events, if configured.

As a final check, under the Alarm site devices tab, ensure that all expected alarm triggers (cameras, sensors, etc.) have populated at least one event.



Verkada's professional monitoring service can engage emergency services to respond to alarms.

Enable Emergency Dispatch

With Emergency Dispatch enabled, a Verkada monitoring agent will contact the individuals in the order specified on the next page. **If an emergency is confirmed or if no one can be reached, then the agent will dispatch emergency services to the site address.**
Police may not respond if there is no unique reference number or video evidence of a crime in progress.

Immediate Dispatch On Panic

When enabled, Verkada monitoring agents will dispatch emergency services immediately, without confirmation. This will apply to duress and panic alarms only. Notification recipients will still receive a call/SMS to gain visibility into the situation.

Monitoring Test Mode

You are in test mode. Alarms will not contact emergency services.

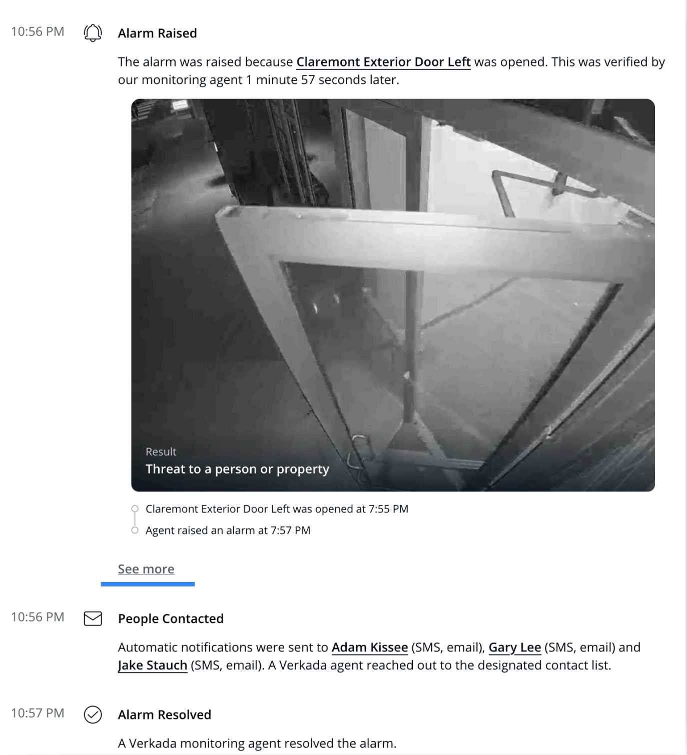
When enabled, Verkada monitoring agents will still reach out to contact you but they will not contact emergency services if you are not available.

Agent Talk Down

When enabled, the monitoring agent will attempt to talk down through speaker devices paired with cameras before executing emergency dispatch procedure. The agent will attempt to call through contact list regardless of the outcome of agent talk down.

Unique Reference Number [Optional]

Add optional URN to share with emergency services.



10:56 PM **Alarm Raised**

The alarm was raised because Claremont Exterior Door Left was opened. This was verified by our monitoring agent 1 minute 57 seconds later.

Result
Threat to a person or property

Claremont Exterior Door Left was opened at 7:55 PM
Agent raised an alarm at 7:57 PM

See more

10:56 PM **People Contacted**

Automatic notifications were sent to Adam Kissee (SMS, email), Gary Lee (SMS, email) and Jake Stauch (SMS, email). A Verkada agent reached out to the designated contact list.

10:57 PM **Alarm Resolved**

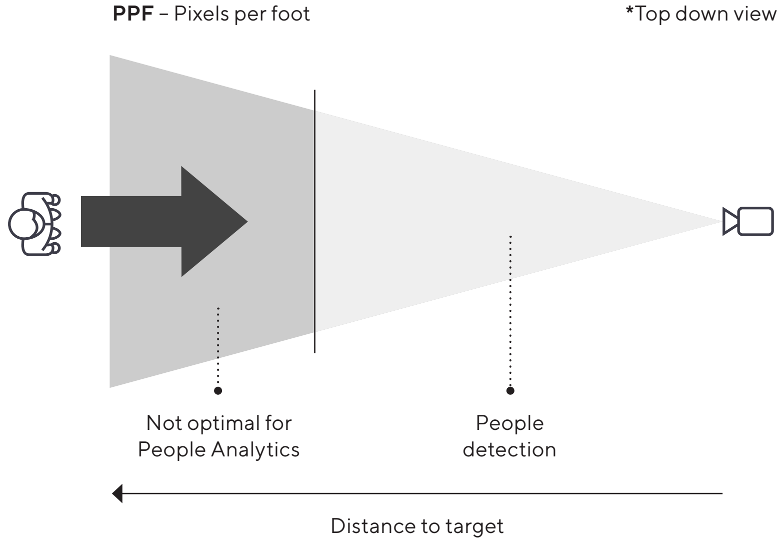
A Verkada monitoring agent resolved the alarm.

Appendix

Optimizing person detection performance

Person detection requires a minimum level of detail, expressed quantitatively as pixels per foot (PPF). PPF decreases with distance from the camera. The PPF at any given distance varies with the camera's field of view and the image resolution.

To calculate the PPF value at the distance you wish to detect people, divide the camera's horizontal pixel count (available in the camera's datasheet under "Tech Specs" → "Sensor Resolution") by the width in feet of the camera's horizontal field of view (HFoV) at that distance.



$$\frac{\text{Horizontal Pixels}}{\text{HFoV Width}} = \textbf{PPF}$$

example:

$$\frac{\text{3840 p}}{\text{12 ft}} = 320\ \textbf{PPF}$$

This image was taken from a CD62 with a resolution of 3840 x 2160 and the width of the horizontal field of view at the target distance is 12 feet. Using the PPF formula we find that we have a PPF value of 320 at the doorway, which is sufficient for all People Analytics features.

The maximum target distances we recommend for our camera models are listed below. (These distances are recommendations only and can vary based on conditions of a particular camera deployment.) Note that the PPF required to detect people depends on the camera model. Our latest generation camera models run on more powerful hardware and are therefore able to run larger, more powerful computer vision models. This allows them to detect people with fewer pixels per foot.

The table below shows the maximum recommended distances for person detection on our camera models:

Person detection

(Person history, Person attributes)

Camera Series	Model Number	0% zoom	100% zoom	PPF
Dome				
	CD22/E	84.3ft / 25.7m		15
	CD32/E	84.3ft / 25.7m		15
	CD42/E	110.6ft / 33.7m		15
	CD52/E	100.0ft / 30.5m	269.1ft / 82.0m	15
	CD62/E	125.0ft / 38.1m	409.3ft / 124.8m	13
	CD31/E	11.3ft / 3.4m		75
	CD41/E	15.8ft / 4.8m		75
	CD51/E	19.9ft / 6.0m	50.0ft / 15.3m	75
	CD61/E	21.5ft / 6.5m	75.0ft / 22.9m	75
	D40	16.0ft / 4.9m		75
Mini Dome				
	CM42	108.7ft / 33.1m		15
	CM41/E/S	22.1ft / 6.7m		75
	CM61	31.6ft / 9.6m		75
Bullet				
	CB52-E	82.1ft / 25.0m	253.0ft / 77.1m	15
	CB52-TE	267.8ft / 81.6m	637.5ft / 194.3m	15
	CB62-E	111.3ft / 33.9m	395.0ft / 120.4m	13
	CB62-TE	395.0ft / 120.4m	988.2ft / 301.2m	13
	CB51-E	20.6ft / 6.3m	50.0ft / 15.3m	75
	CB51-TE	50.6ft / 15.4m	125.0ft / 38.1m	75
	CB61-E	23.5ft / 7.2m	75.0ft / 22.9m	75
	CB61-TE	66.7ft / 20.3m	175.0ft / 53.3m	75
Fisheye				
	CF81-E (pano)	40.0ft / 12.2m		40
	CF81-E (4-way)	18.0ft / 5.5m		75
	CF81-E (ePTZ)	–		75
Multisensor				
	CH52-E	103.1ft / 31.4m	284.2ft / 86.6m	15
PTZ				
	CP52-E	173.0ft / 52.7m	4800.0ft / 1463.0m	15

Verkada's CD22 and CD22-E do not support facial recognition.

When does detection occur?

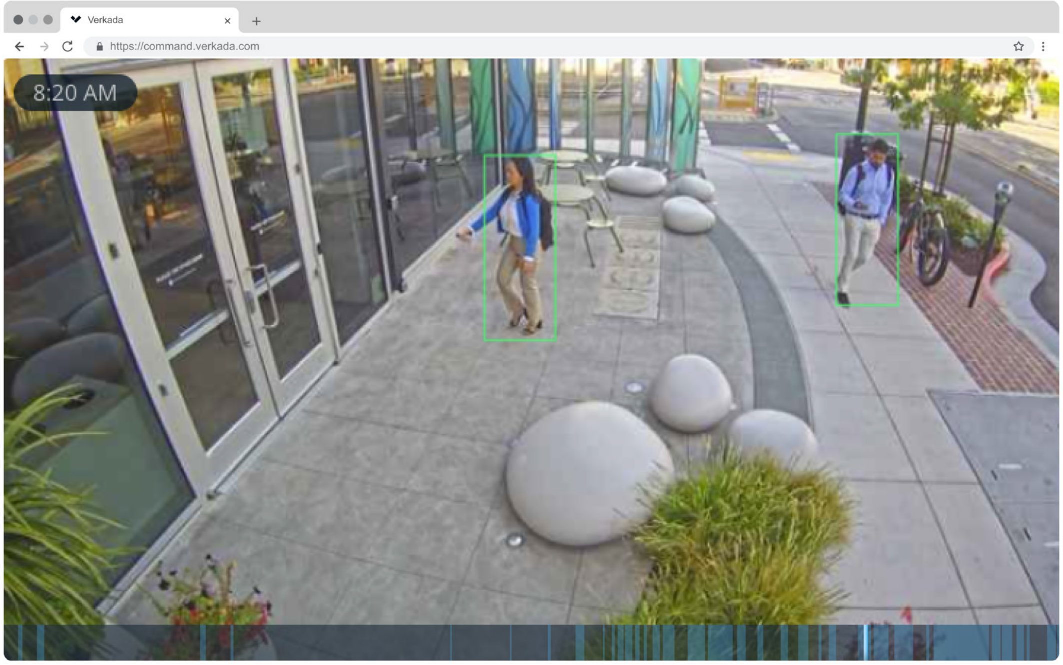
When a Verkada camera detects an object, green bounding boxes appear over the detected object(s). (You can see examples of these bounding boxes when scrubbing through a camera's motion search or historical video.)

Person detection

Detection is determined whenever any part of a person's bounding box intersects with the configured region of interest.

Line crossing and loitering detection

Detection is determined when the center bottom of a person's or vehicle's bounding box crosses a line or sits inside a loitering region. The image below illustrates where that point would exist.



For loitering, once the person's trigger point intersects the loitering region, the timer begins. If the trigger point remains in this region for the configured time, a detection event occurs. If the person trigger point briefly exits and re-enters the loitering region within 4 seconds, the counter continues. If the camera loses track of an individual (for example, walking out of frame or behind a car) or the trigger point is outside the loitering region for more than 4 seconds, the counter resets.

Tips to reduce missed person detection

Ensure camera lenses and covers remain clean

There will be times when the lens or dome cover of your camera will be dirty because of dust, debris, fingerprints, smoke, condensation, etc. In addition to potentially blocking the camera's view, this can cause the IR illuminators to reflect light to the lenses and give you an unfavorable view in night mode. This may result in a missed person detection.

Rain or snow may cause missed person detection

Heavy rain or snow may reduce a camera's visibility, causing the camera to miss detecting a person or vehicle.

Ensure cameras are optimized for Night Mode

Each camera has night vision capabilities, using a sensor to detect low light situations. It is particularly important that customers using person detection as an alarm trigger have their cameras optimized for Night Mode, given that many alarm incidents happen after dark.

When external lighting is low, the camera will switch to Night Mode and record in black and white using infrared LEDs (IR) to illuminate the environment. If the IR is emitted improperly through the dome or reflected back into the lens it will negatively impact image quality and person detection. It is imperative that the dome remain free of debris and the camera is installed properly to achieve the best image quality. Learn more about resolving issues with Night Mode.

Ensure cameras are secured installed

Regions of interest, line crossing, and loitering are set based on the camera's current field of view. If a camera is moved or shifts for any reason (tampering, strong wind, etc.), those boundaries may no longer be accurate. Therefore we recommend making sure that all cameras are securely installed and periodically checking that any detection triggers are still accurate.

Tips to reduce false person detection

Ensure that camera lenses and covers remain clean

There will be times when the lens or dome cover of your camera will be dirty because of dust, debris, fingerprints, smoke, condensation, etc. In addition to potentially blocking the camera's view, this can cause the IR illuminators to reflect light to the lenses and give you an unfavorable view in night mode. This may result in a false person detection.

Ensure cameras are optimized for Night Mode

Each camera has night vision capabilities, using a sensor to detect low light situations. It is particularly important that customers using person detection as an alarm trigger have their cameras optimized for Night Mode, given that many alarm incidents happen after dark.

When external lighting is low, the camera will switch to Night Mode and record in black and white using infrared LEDs (IR) to illuminate the environment. If the IR is emitted improperly through the dome or reflected back into the lens it will negatively impact image quality and person detection. It is imperative that the dome remain free of debris and the camera is installed properly to achieve the best image quality. Learn more about resolving issues with Night Mode.

Rain or snow may cause false person detection

Heavy rain or snow may cause a camera to falsely detect a person or register duplicate person detection events.

Check for moving objects in the camera's field of view

Frequently moving objects (e.g. balloons, flags, digital signage) may cause the camera to falsely detect a person. We recommend removing these types of objects from the field of view of any camera being used as an alarm trigger.

Check for nearby reflections

Cameras that are facing windows or other reflective surfaces may falsely detect people in areas where they are not. This can often be resolved by setting up line crossing as an alarm trigger, rather than detecting a person anywhere in the camera's field of view. You may also set up a region of interest that does not include the reflective surface.

High volume verification events

A high volume event is a verification event that raises an alarm because there are more than 15 verifications triggered within an hour.

On the 16th verification within an hour, the monitoring agent will follow normal alarm procedure irrespective of the security prompt selected by the customer, content of the provided video, or whether test mode is enabled:

1. If there are contacts in the contact list, the agent will attempt to reach them and will say that this is a courtesy call due to a high volume event.
2. The customer may choose to resolve the alarm or dispatch emergency services if necessary. They can also ask the agent to disarm the site for up to 12 hours.
3. If the agent cannot reach any listed contacts, the site will remain in a courtesy alarm state until action is taken. Emergency services are not dispatched for high volume events.

Situations when a high volume event is initiated could include a cleaning crew that forgets to disarm the alarm system and triggers multiple events as they move through the building, or a camera trigger that points to a sidewalk with heavy late-night foot traffic.

How can a high volume event be avoided?

1. Check your camera configuration, in particular:
    - Make sure the camera is not pointing to an area where there can be heavy foot traffic while your site is armed.
    - Make sure to set up regions of interest or line crossing on the camera(s) that you'd like to use as alarm triggers to specify parts of the video on which it should detect movement/people.
    - Make sure that you are deliberate about selecting which cameras to set up as alarm triggers. Remove cameras that may be sending redundant or unhelpful video verification events.
2. Check your site configuration, in particular:
    - Ensure that your arming schedule is appropriate for your business so that the system only arms when necessary.
    - Consider breaking up your site into multiple sites if the cameras need to follow a different arming schedule to minimize unnecessary verification events that may be triggered.

Exceeding your verification event limit

One LIC-BA Standard Alarm License includes up to 100 verified events per month; the LIC-BV Premium Alarm includes up to 1,000 verified events per month.

Customers can check the number of video verifications they have used so far through the "Location" section in the Activity page of the alarm site.

Customers get a 2-month grace period, during which they will receive warning emails if they exceed their monthly limit. Customers are expected to adjust their site or alarm trigger configurations to reduce the number of verification events. In the third consecutive month, agents will verify events up to the customer's normal limit. After that point, events will not be verified and will be automatically escalated to an alarm.

Frequently Asked Questions

How long does video verification take?

While the length of time can vary, video verification of an alarm event typically takes less than two minutes. The average time to verify is approximately 35 seconds.

How long does police dispatch take?

If emergency dispatch is enabled, monitoring agents will contact police dispatchers immediately once an alarm is raised. Customers can see when dispatch was requested in the Alarm Summary page in Command. Verkada does not know or have control over when the police actually dispatch or arrive on scene.

Can I provide monitoring agents with additional context to help them determine if there's a real threat?

Customers can use the Custom Rules video verification option to specify how agents should response to specific scenarios, such as an apparent employee doing routine activity. However, customers cannot provide agents with additional context, such as what color an employee is likely wearing.

Can I provide monitoring agents with feedback about whether they classified an event correctly?

After an alarm is resolved, customers can note in Command whether it was a real alarm, false alarm, or test alarm. This information may be used by Verkada to better train our monitoring agents. Customers can not provide feedback directly to agents.

Can agents share live camera feeds with first responders?

Yes. If you have emergency dispatch enabled, monitoring agents can share 1) historical camera footage from camera(s) that triggered the alarm, 2) live footage from nearby cameras that are paired with the device that triggered the alarm, and/or 3) live footage from emergency dispatch context cameras (see pg. 12).

What phone number will monitoring agents call from?

If emergency dispatch is enabled, an agent on the "dispatch team" will call from +1 (619) 304-4016. We suggest users add this phone number to their contact list as "Verkada Monitoring Agent," or something similarly descriptive.

Can people on the contact list reply to monitoring agents via SMS, rather than waiting for a call?

Yes, an agent on the "dispatch team" will send SMS's from one of three numbers, all of which users can reply to:

+1 (619) 329-8928
+1 (619) 329-8846
+1 (619) 329-8736

Users cannot reply to the automated text messages that Verkada sends to notify them of a raised alarm.

What happens if the monitoring agent cannot reach anyone on the contact list?

Agents will call down the entire contact list twice. If they still unable to reach anyone, and if emergency dispatch is enabled, they will proceed to requesting dispatch. If Test Mode is enabled, the agent will not request dispatch if no contact can be reached.

Ordering Information

LIC-BB Basic Alarm License pricing*

Includes alarm monitoring with no video verification

Model Number	Description	Cost (MSRP) USD
LIC-BB-1Y	1-Year Basic Alarm License	$600
LIC-BB-3Y	3-Year Basic Alarm License	$1,800
LIC-BB-5Y	5-Year Basic Alarm License	$3,000
LIC-BB-10Y	10-Year Basic Alarm License	$6,000

LIC-BA Standard Alarm License pricing*

Includes professional monitoring with video verification, up to 100 events/month

LIC-BA-1Y	1-Year Standard Alarm License	$1,500
LIC-BA-3Y	3-Year Standard Alarm License	$4,500
LIC-BA-5Y	5-Year Standard Alarm License	$7,500
LIC-BA-10Y	10-Year Standard Alarm License	$15,000

LIC-BV Premium Alarm License pricing*

Includes professional monitoring with video verification, up to 1,000 events/month

LIC-BV-1Y	1-Year Premium Alarm License	$12,000
LIC-BV-3Y	3-Year Premium Alarm License	$36,000
LIC-BV-5Y	5-Year Premium Alarm License	$60,000
LIC-BV-10Y	10-Year Premium Alarm License	$120,000

For custom video monitoring pricing, please contact your Verkada sales representative or email sales@verkada.com.

*One Alarm License needed per physical address; required to operate all Verkada Alarms hardware.

Additional Resources

Help Center

Click here for detailed Help Center articles.

Verkada Support

support@verkada.com

North America +1 (650) 514-2500
Latin America +52 (55) 9990 8275
Europe +44 (0)20 3048 6050
Asia / Pacific +61 (2725) 99300

Live chat available in Verkada Command