SECURITHINGS

Minimizing IP Cameras' Downtime

The 5 Main Reasons IoT Security Cameras Go Offline—and How to Resolve Them

For today's organizations, downtime of IoT devices including security cameras is a serious issue.

Whenever any type of IoT device goes offline or stops functioning properly, its organization risks having its regular operations disrupted. In addition to damaging the organization's productivity, this can hurt its revenue and reputation. And the stakes are particularly high in the realm of physical security.

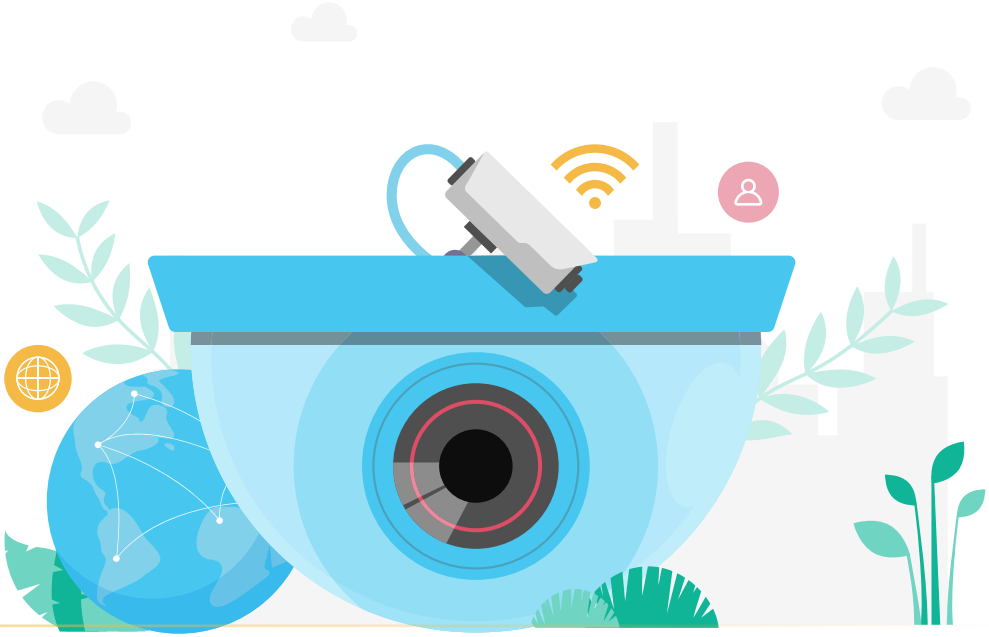
Because connected security devices (including cameras, as well as a variety of other device types) are tasked with protecting both people and property, any downtime of these devices temporarily removes an effective safety measure designed to protect those people and that property.

Of course, the longer a security camera stays offline or nonfunctional, the greater the risk that a security incident will occur while the device is not working properly. That makes it crucial to minimize each of three metrics when an IoT camera's functioning is interrupted:

- **Time to identification**—the amount of time between a device's initial failure and when the team identifies there is an issue.
- **Time to diagnose**—the amount of time between when a team identifies an issue and when the cause of the issue is determined.
- **Time to resolution**—the amount of time between when a team is notified of an issue and when the issue is fixed.

By understanding the main issues affecting IP cameras, a team can keep these metrics to a bare minimum. Fortunately, there are several common causes for camera downtime, and learning to address these issues can empower organizations to reduce the risk of downtime. In addition, technologies such as SecuriThings' Horizon solution can help organizations to take preventive and proactive measures more efficiently, to get notified of camera issues more promptly, to diagnose issues more quickly based on camera data, and to resolve issues more efficiently (and often remotely).

Given the importance of accelerating each of the processes involved in getting a security camera back to proper functioning, this guide will provide an overview of the **five most common reasons for IP camera downtime** and how you can address them. In addition to explaining how each of these causes can prevent a camera from functioning properly, the following pages will provide some practical solutions for addressing each one of them. With this information, you can help your organization to maximize the uptime of its IP cameras.



1. Power Supply Issues

A variety of problems can knock an IP camera offline by preventing it from getting adequate, consistent power. While diagnosing some of these issues requires a certain degree of investigative work, others are visible with little effort.

In some cases, a device goes offline because its equipment is not providing enough power. Batteries are sometimes the source of this type of issue, either because a battery is faulty or because it simply has a low charge. Cables can also cause this kind of problem for any of several reasons, including:

- A loose cable connection, such as to the power supply
- A cable that is too long, or that supplies power for too many devices at once.
- A faulty power cable—often because the cable is old, damaged, degraded, or cut.

Because some IP cameras rely on power over ethernet (PoE) technology rather than conventional power cables, problems with a PoE switch or a PoE injector can also cause downtime.

On the other extreme, cameras can go offline due to excessive power. For example, a power surge—such as those caused by lightning—can prevent a camera from functioning. Interference from nearby electrical equipment can also cause power issues, as can mounting a security camera on a conductive metal surface.

The Solution

The first step to resolve a power supply issue is identifying the source of the problem. Since many of these issues stem from faulty equipment or a problematic setup, these issues require physical fixes. Afterwards, some issues will resolve themselves, some should be resolved by remotely restarting the camera, or PoE switch port and some require a manual fix.

Root cause analysis is a critical step here, it pinpoints the faulty element looking at both the device and network and provides visibility into both taking all dependencies into account. It also can help you identify the right steps to take to address the cause of the camera downtime your organization faces. SecuriThings Horizon streamlines this process by using machine learning to analyze metrics from IP cameras (metrics such as stream status, network status, SD card performance, CPU usage, RAM usage, and camera temperature). With this type of automated technology, you can identify the source of the downtime quickly, reliably, and efficiently—empowering you to get your cameras back online as rapidly as possible

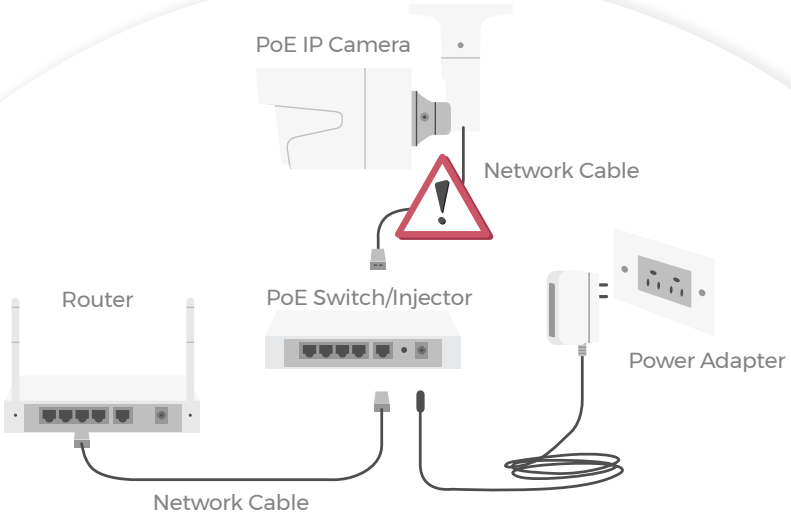
2. Network Connection Issues

Like power issues, problems with a network connection can prevent a camera from staying online—even though the camera itself may be functioning properly.

There are several common reasons that an IP camera may not be able to communicate properly with the router or switch to which it is (or is supposed to be) connected. In some cases, a camera is simply too far from the router or switch. In other cases, there are too many barriers between the camera and the network dependency, causing interference and interrupting the signal.

A poor network connection can also result from insufficient bandwidth. The number of devices on a network affects the speed with which those devices can access the network, and having too many devices connected at once can impede the functioning of those devices.

In addition, software issues can cause Wi-Fi connection problems that force a camera offline. Incompatibilities between IP cameras and their routers—for example, different settings regarding the type of signal transmitted—can prevent the device from communicating properly with its network. Changes in a network's SSID can also result in downtime.



The Solution

Most network problems responsible for IP cameras' downtime need to be resolved manually. For example, manual fixes are necessary if a camera is too far from its router or switch, if there are too many barriers, or if there is insufficient bandwidth for the number of devices on a network.

Still, the intelligent analysis of metrics from the IoT ecosystem can help you identify the source of the problem quickly, so that you can minimize downtime. For example, Horizon can store IoT and physical security devices' metrics going back up to two years. By examining the timeline of when devices have gone offline in the past, you can zero in on the cause (or causes) of that downtime efficiently.

3. Streaming Issues

The category of streaming issues that can cause downtime for an IP camera is particularly broad and varied, which can make the diagnosis and resolution of these issues relatively complex.

In some cases, the source of a problem with a camera's streaming reliability lies within the camera itself. A camera may be unreachable, its connectivity may be unstable, it may restart repeatedly and unexpectedly, or it may simply stop recording. Additionally, the camera's streaming may be disrupted because its password has changed or SSL certificate expired. It may also stop streaming because its SD card or recording server disk is full.

In other cases, an IP camera may go offline due to either issues facing its server or issues regarding the connection between the camera and its server. A server's connectivity may be unstable as a result of too many devices connected to it. Or, even if a camera stays connected to its network, that camera may become disconnected from its recording server—a problem that can cause the camera's NVR device to stop recording.

Streaming problems can also be caused by a variety of other types of issues, some of which stem from incompatible settings between different elements of the IoT ecosystem. Sometimes equipment within the ecosystem becomes overloaded with more unique streams than it can handle. Similarly, a camera's latency may be too high for that equipment, likely due to factors such as the camera's resolution, image settings, audio settings, compression settings, capture frequency, and image processing.

Other factors that can cause a video surveillance ecosystem to become overloaded include:

- The network infrastructure's data capacity and its transmission protocol (UDP or TCP).
- The setup, including its CPU, GPU, memory cards, and other elements that can affect image fluency.
- The framerate, bitrate, and shutter speed of a security camera.

The Solution

Typically, IP cameras' streaming issues can be resolved by restarting these devices. Rather than spend the time and money required for a truck roll, you can use Horizon to restart one or hundreds of cameras remotely and to verify that they are properly configured. And should you need to diagnose a streaming-related issue, you can use the timeline of IoT device metrics that Horizon automatically stores, letting you see when in the past two years your IP cameras have had downtime.

Additionally, you can use Horizon to ensure that your entire fleet of IP cameras is running the latest VMS compatible firmware versions. This way, by optimizing the stream's performance, you can minimize the chances that a streaming issue will cause downtime. If no new firmware updates are available because a camera has passed its official end of life, Horizon also lets you know that it is time to replace the camera.

Just as importantly, Horizon lets you automatically rotate SSL certificates in bulk, both on physical security devices such as cameras (even across different locations, groups, and models) in line with your organization's requirements—helping ensure that SSL-related issues don't result in downtime.

4. Device Overload

Just as the video surveillance ecosystem can get overloaded and cause its devices to go offline, an individual video device can get overloaded, resulting in downtime.

How often this happens to an IP camera depends largely on the camera's chipset and on the demands put on it. How high those demands are can be affected by the total data throughput (bandwidth) that the camera's hardware must handle. Factors such as the complexity of an image and its lighting conditions can affect this data throughput.

The frequency of camera downtime can also be affected by how many applications run simultaneously. For multi-sensor or multi-channel cameras, using motion detection on several channels simultaneously can increase the likelihood of issues that will result in downtime. High-frequency HTTPs (or HTTP) requests can also raise the chances of an issue that will force a camera offline.

In some cases, unexpected restarts can be a sign that a camera has started to become overloaded. Temperature issues can also affect camera performance, with cameras that are either too hot or too cold at risk of downtime.

The Solution

Keeping all security cameras running the latest compatible firmware can minimize the likelihood of device overload.

When a camera does face this type of issue, the first step in getting it back online is to restart the camera. If this does not resolve the issue, your next step is to determine whether the issue is actually caused by device overload. By intelligently analyzing metrics gathered from the camera, automated root cause analysis can help you distinguish between device issues and network issues, as well as between issues facing a single device and global issues (such as a problem with a switch). This approach can also help you determine whether a camera is disconnected from the management system despite being available on the network.

With Horizon, you can perform both the camera restart and the root cause analysis automatically and remotely, helping you get your camera back online quickly and efficiently.

5. Certificate Issues

One relatively straightforward reason for camera downtime is the presence of issues with certificates. These issues can occur either because of a conflict or because a certificate has expired.

There are two main types of certificates that IoT ecosystems rely on: SSL certificates and 802.1x certificates. When either type of certificate expires (or preferably beforehand), it must be promptly replaced. Should a certificate expire without being replaced, it can knock physical security devices offline or fail to record video, resulting in downtime and missed recordings until the issue is resolved.

The Solution

Should there be an unexpected issue with a certificate, Horizon also alerts you in real time, so that you can take action to resolve the issue promptly.

The most effective way to avoid camera downtime stemming from expired certificates is to set up mass certificate rotation. Horizon makes it easy to automate this process, preventing expired certificates from causing downtime.

Conclusion

There are various reasons physical security devices such as IP cameras can go offline. By grouping these issues into five main categories, we can simplify them in order to understand how to address them in general. These five categories can also be useful in terms of recommendations for proactive and preventive steps to avoid unnecessary downtime.

By automating routine maintenance steps—such as rotating passwords and certificates and updating firmware—you can minimize the chances of unnecessary downtime. This step can go a long way toward keeping your IP cameras (as well as other IoT devices) operating smoothly. But it cannot prevent all unexpected downtime.

When a camera does go offline, sometimes a simple restart is all it takes to resolve the issue. In this case, the capability to resolve the issue remotely can offer you significant savings of time and money, as well as the ability to get the camera back online rapidly.

But when the steps required to get an IP camera back online are more complicated, the key is rapid, remote root cause analysis. By using an automated, intelligent solution to quickly understand what the source of the issue causing the downtime is, you can take action to resolve it promptly (and, in many cases, remotely).

Not only does this streamlined approach enable you to efficiently diagnose the issue, but—more importantly—it enables you to minimize camera downtime. In other words, it empowers your organization to maximize the return on your investment in IP cameras by reducing truck rollouts, tech support hours and cuts downtime.

ABOUT SECURITHINGS

Founded by leading security and IoT experts, SecuriThings empowers Operations & IT professionals to automate the operational management of IoT devices at scale, while also ensuring full compliance and security within their organization. The solution is trusted by Fortune 100 companies and has been deployed by numerous large enterprises such as major airports, universities, hospitals and more. SecuriThings partners with key system integrators as well as device manufacturers to provide unprecedented insights, coverage, and reliability.

For more information, please contact us at **info@securithings.com.**

www.securithings.com