



Pelco Calipsa Integration Manual

for Immix

Document number: C6787M

Publication date: 2026-02-23

Pelco Calipsa Integration Manual for Immix

© 2026, Pelco Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Pelco Corporation or its licensors.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Pelco Corporation reserves the right to make any such changes without notice. Neither Pelco Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Pelco Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Pelco Corporation
pelco.com

HTML-PROJECT-A
Revision: 1 - EN
20260223

Contents

Calipsa Integration with Immix	4
Integration Checklist for Immix	5
Integration Requirements	6
Pelco Calipsa Requirements	6
Immix Requirements	6
Integration Overview	7
Prerequisite Steps	8
Adding SMTP Server Addresses	8
Whitelisting Calipsa IP Addresses	8
Integration	9
Adding the Calipsa System to Immix	9
Configuring Email Notifications for True Alarms	10
Addressing Failed or Faulted Alarms	11
Retraining the AI on False Positives	11
Enabling AI Verification for an Alarm	12
Configuring Alarm Recording Durations (Post-Alarm)	12
Enabling Pre-Alarm Context	13
Detecting Scene Changes and Tampering	14
Merging Duplicate "Attached Footage" Cameras	14
Troubleshooting "NULL" Cameras	15
Troubleshooting Unprocessed Alarms	15
Improving Accuracy via False Alarm Reporting	16
Troubleshooting Failed Alarm Verification	17
More Information & Support	18

Calipsa Integration with Immix

Integrating Pelco Calipsa with Immix simplifies event processing by synchronizing the two systems. The integration procedure involves setting up a secure connection between Immix and Pelco Calipsa. You must also configure Immix for integration before finally validating that true alarms are being received from Pelco Calipsa.



NOTE

Refer to manufacturer's documentation for more information on Immix products.

Integration Checklist for Immix

Use this checklist to ensure that the Immix system is configured properly for integration with Pelco Calipsa.

1. **System Version** – See [Integration Requirements on the next page](#) for more information.
2. **Product License** – The correct product licenses has been applied.
3. **Recording Cameras** – All cameras that will be used with Calipsa are recording.
4. **Motion Detection** – All cameras that will be used with Calipsa are configured for motion detection.
5. **Time Synced** – All devices (Core, cameras, recorders) must be time synced.
6. **Admin Privileges** – You need administrative privileges to your Calipsa account.
7. **Secure Communication** – All communication between the application and Product_Type, and between the application and the Calipsa cloud service is encrypted via HTTPS (TSL/SSL) over port 443.
8. **CA Certificates** – install and load SSL CA Certificates on the server for system security.
9. **Firewall Rules** – the Firewalls must allow outbound and inbound communication between the servers and Pelco Calipsa.
10. **Public IP** – the Immix System must have a public IP in order to work with the Calipsa connector. The system can have more than one server but there must be one Public IP per system.
11. **Port Numbers** – the standard port is typically 8401 for HTTPs. Check if the customer has changed the port and use the new port number if required.
12. **Authentication** – each Immix system needs a username and password for the Calipsa connector to access the server information.
13. **Event Names** – the event names should be as descriptive as possible. Choose a descriptive name so you can recognize it when Calipsa beings processing alarms and sending notifications, e.g., Calipsa-CameraName-Description.

Integration Requirements

Check the requirements for Pelco Calipsa and Immix before beginning the integration.

Pelco Calipsa Requirements

- Calipsa subscription (Basic/Detect or higher)

Immix Requirements

- Ensure all camera devices in Immix are configured to use HTML5. Devices using Proxy (Flash) are not supported and will fail to send footage for verification.
- AI Verification is enabled via the Immix AI-Link

Integration Overview

Integrate Pelco Calipsa with Immix systems for AI-powered event verification. When a camera detects certain activities, the Immix server will send event data to Calipsa cloud to verify the event details. Calipsa will send the event verification information back to the Immix server and you will see the result in the VMS along with the event information.

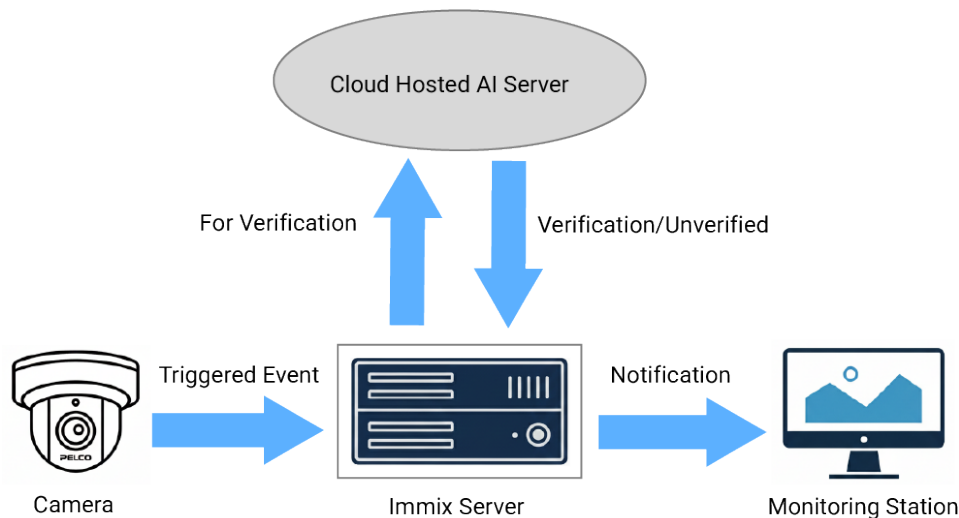


Figure 1: Overview of the integration between Pelco Calipsa and Immix.

AI Verification is designed to reduce the number of false or nuisance alarms/events that a central station operator must handle. This allows the station to increase the overall number of sites and/or customers supported without increasing staff, thus improving margin and efficiency.

The Immix AI-Link solution does not provide recording or live view functionality. Instead, it takes video footage from any Immix integration that provides video or alarm detection, receives that clip(s) as normal, and uploads the clip(s) to the AI solution provider (Calipsa) selected in the Immix AI-Link window.

Once received, Immix will analyze and classify the detected threat based on the threshold and rules set for the camera. This entire process takes seconds, with Calipsa processing an alarm typically within 0.8-1.2 seconds.

- If the clip is verified as having a true threat, the clip is delivered into the Immix alarm queue on the main Alarms page identified as "Verified".
- If the clip is not verified, it is auto handled and will not be presented to the main alarm queue.



NOTE

"Unverified" events still appear in the Alarms tab in the Site Monitor page if an operator or supervisor wishes to review them, but they do not appear in the main Alarm queue, meaning no processing is required for these events.

Suggested Next Topic: [Prerequisite Steps on the next page](#)

Prerequisite Steps

You must configure the network settings on your servers to allow communication between Immix and Pelco Calipsa.

Adding SMTP Server Addresses

You must add the SMTP server addresses for integration with Immix. This is required so your security platform can receive notifications from Calipsa. See the Immix product documentation for instructions on how to add server addresses.

SMTP Server Address for United States (US) Deployments:

- smtp.us-01.calipsa.io

SMTP Server Address for European Union (EU) Deployments:

- smtp.calipsa.io

Whitelisting Calipsa IP Addresses

Whitelisting Calipsa's specific IP addresses ensures that your server does not block incoming verified alarms, guaranteeing that critical events reach the monitoring station.

Considerations:

- You must configure your firewall rules to allow both outbound and inbound communication between your servers and Pelco Calipsa via HTTPS (port 443).
- The specific IP addresses to whitelist depend on your geographic deployment (US vs. EU).

Steps (Server/Firewall Configuration):

1. Access your server or firewall network configuration settings.
2. Locate the Allow List (Whitelist) for inbound traffic.
3. Add the following IP addresses based on your region:
4. United States (US): 18.232.251.52 and 35.153.146.21.
5. European Union (EU): 34.240.200.29 and 54.247.163.162.
6. Ensure port 443 is open for these addresses.
7. Save the network configuration.

Successfully whitelisting these addresses prevents communication blocks, allowing true alarms to appear in the Immix alarm queue.

Suggested Next Topic: [Adding the Calipsa System to Immix on the next page](#)

Integration

Integrating Pelco Calipsa with Immix establishes a secure, two-way synchronization between the monitoring platform and the Calipsa Cloud to significantly simplify event processing. The core function of this integration is AI Verification, a process designed to filter out nuisance alarms (such as those caused by weather or foliage) so operators can focus solely on genuine security threats.

Adding the Calipsa System to Immix

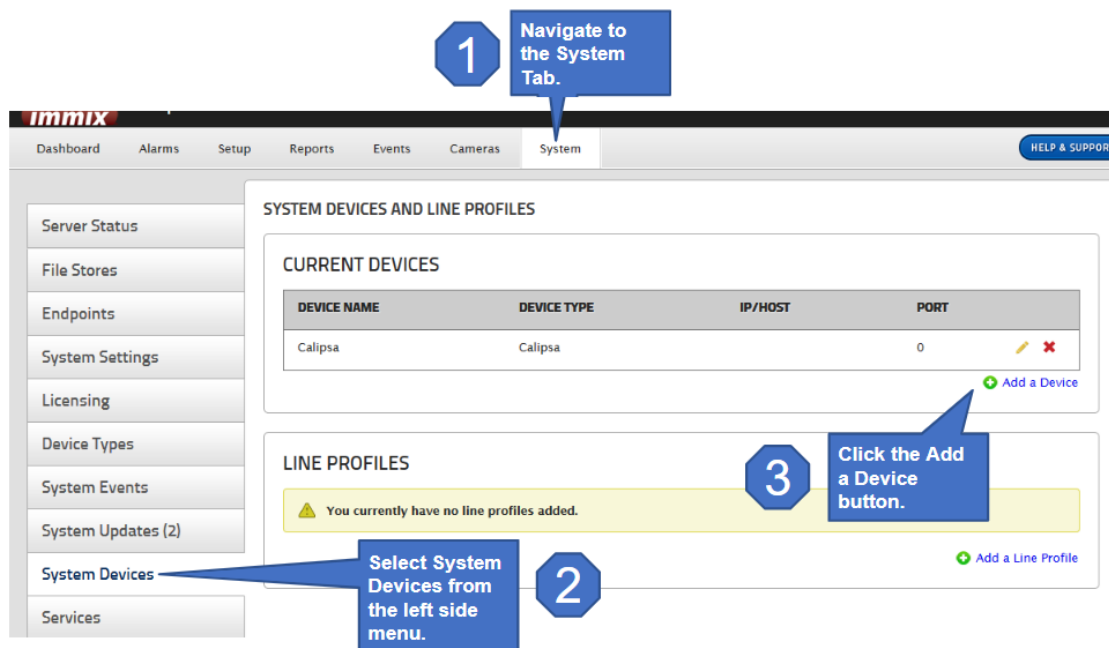
Adding Pelco Calipsa as a system device within the Immix Monitoring Station is the foundational step required before you can link any specific cameras or alarms for verification.

Considerations:

- You will need the AI Link credentials provided by Immix before starting this task.
- Crucial: Do not enter an IP address or Port number during this setup; these fields must be left blank.

Steps:

1. Open Immix and navigate to the **System** tab.
2. Select **Devices** from the left-side menu.
3. Click the **Add a device** button.



4. In the Device Details name your device. This will auto populate but you can customize.

5. Add the AI Link credentials provided by Immix.



NOTE

Leave the IP and Port fields blank.

6. Click **Update**.

Successfully adding the device creates the connection between Immix and the Calipsa cloud, enabling you to select "Calipsa" when configuring individual alarm verifications.

Suggested Next Topic: [Configuring Email Notifications for True Alarms below](#)

Configuring Email Notifications for True Alarms

Configuring the global SMTP settings ensures that verified "True" alarms are automatically forwarded to your monitoring station software via email for immediate operator awareness.

Considerations:

- These settings apply globally to all new sites added. To direct a specific site to a different location, you must change the SMTP details at the site level.
- Ensure Calipsa IP addresses are whitelisted on your monitoring station software first, or the emails may be blocked.

Steps:

1. Log into your Calipsa account.
2. Select Settings in the bottom left-side panel.
3. Navigate to Global configuration and click Edit.
4. Under Host/IP Address, enter the IP address or DNS of your server.
5. Under HTTP port, enter your port number (try 25 if unsure).
6. Leave the Username and Password sections blank if you are using Immix.
7. Enter a Test Email address belonging to that server (e.g., S123@immixalarms.com) and click Test.
8. If the connection succeeds, click Save.

Successfully configuring these settings results in Calipsa forwarding true alarm details to your monitoring station's email gateway.

Suggested Next Topic: [Addressing Failed or Faulted Alarms on the next page](#)

Addressing Failed or Faulted Alarms

Identifying the specific error code associated with a "Faulted" alarm allows you to quickly resolve configuration issues preventing video verification.

Considerations:

- Common errors include [NoVideoFile] (missing clip) or [ConnectionFailed] (network issues).
- Devices using Flash (Proxy) are not supported and will fail verification.

Steps:

1. Open the Immix Monitoring Platform and locate the failed alarm.
2. Check the Device Type: Ensure it is set to use HTML5. If it is using Proxy, it will not send for verification.
3. Check the Recording Action: Ensure the alarm has a "Record Camera" action set to a value greater than 0 seconds (e.g., 10 seconds).
4. Check System Devices: Verify that the username and password in the Calipsa device setup match the credentials you were given.
5. If the error is [AllinkDown], check that the AI Link Forwarder service is running in Windows Services on the server.

Correcting these settings resolves [Faulted] statuses, allowing the system to resume sending video clips to Calipsa for analysis.

Suggested Next Topic: [Retraining the AI on False Positives below](#)

Retraining the AI on False Positives

Marking incorrect verifications as "False" provides feedback to the Calipsa algorithm, which retrains the system to ignore specific environmental triggers (like spider webs or trees) on that camera view.

Considerations:

- This process improves results over time, typically showing noticeable improvement within 2-3 months.

Steps:

1. Log into the Calipsa portal.
2. Navigate to the Alarms tab.
3. Locate the alarm that was incorrectly identified as a person or vehicle.
4. Mark the alarm as False.

Successfully marking alarms as false submits the footage for algorithm retraining, reducing similar false alarms from that camera in the future.

Suggested Next Topic: [Enabling AI Verification for an Alarm on the next page](#)

Enabling AI Verification for an Alarm

Enabling AI verification allows the system to filter up to 95% of nuisance alarms, ensuring operators only respond to genuine threats involving people or vehicles.

Prerequisites:

- Before enabling verification, ensure the camera device type in Immix is set to use HTML5, as devices using Proxy (Flash) will not be sent for verification.
- Additionally, you must have the Calipsa AI Link device added to your Immix system configuration before you can link it to specific alarms.

Steps:

1. Navigate to the Setup tab in the Immix Monitoring Station.
2. Select the specific Site you wish to configure.
3. Click Manage Devices and Alarms.
4. Select the Alarms tab from the top menu.
5. Click the pencil icon (edit) next to the specific alarm you want to verify.
6. Check the box labeled Enable AI Verification to reveal the settings menu.
7. In the dropdown menu, select the Calipsa device you previously added.
8. Check the boxes for Person and/or Vehicle and set the confidence threshold (default is usually 75%).
9. Click Save.

Successfully enabling verification results in alarms from this camera being routed to Calipsa for analysis; only confirmed threats will appear as "Verified" (Red) in the operator queue.

Suggested Next Topic: [*Configuring Alarm Recording Durations \(Post-Alarm\) below*](#)

Configuring Alarm Recording Durations (Post-Alarm)

Configuring a specific recording duration is critical because Calipsa requires a video clip to analyze movement; without this clip, the alarm will fail to verify.

Prerequisites:

- You must set the "Record Camera" action to a value greater than 0 seconds. If this is set to 0 or left blank, the alarm will fail and appear as "Faulted" with the error [NoVideoFile] or [NoVideoDataInFile]. A duration of 10 seconds is recommended (or 5 seconds if you are also using Pre-Alarm).
- Disable "Attached Footage" for Single Images. If your NVR/DVR sends only a single image or a clip shorter than 3 seconds (common with Videcon or Adpro units), you should disable the alarm attachment setting on the NVR itself. Calipsa requires a minimum of 3 unique images (ideally 1 second apart) to accurately detect motion. Relying on Immix "Post-Alarm" recording actions is preferred for these devices.
- If you are using Adpro FastTrace 2 devices, reconfigure the "Quad image interval" to 1 second to ensure valid clips are sent to Calipsa.

Steps:

1. Navigate to the Setup tab and select Manage Devices and Alarms for your site.
2. Click the Alarms tab and locate the alarm you configured in the previous topic.
3. Click the Actions link next to the alarm.
4. Click Add an Alarm Action.
5. Set Action to "Record Camera."
6. Select the correct Camera from the dropdown.
7. In the Number of seconds field, enter 10 (or 5 if using pre-alarm).
8. Click Done.

Successfully configuring the recording duration ensures that when an alarm triggers, Immix generates a valid MP4 clip that Calipsa can analyze for threats.

Suggested Next Topic: [Enabling Pre-Alarm Context below](#)

Enabling Pre-Alarm Context

Capturing footage from before the alarm triggers provides operators with vital context, such as seeing how a subject entered the frame, which helps verify the legitimacy of the threat.

Prerequisites:

- Enable "Post-Alarm" recording: Pre-alarm settings are located in a different area than the standard alarm actions. This feature relies on the camera system's ability to buffer video; some older systems may not support this. You must have "Post-Alarm" recording (see previous topic) enabled for this to work.

Steps:

1. Navigate to the System tab in the main toolbar.
2. Select System Settings.
3. Click the Alarms dropdown menu to expand the options.
4. Locate the field "Number of seconds to go back for pre-alarm."
5. Enter the desired duration (e.g., 5 seconds).
6. Save your changes.

Successfully enabling pre-alarm context results in the video clip sent to Calipsa (and the operator) starting 5 seconds prior to the actual motion trigger.

Suggested Next Topic: [Detecting Scene Changes and Tampering on the next page](#)

Detecting Scene Changes and Tampering

Enabling Scene Change detection allows the system to alert you if a camera has been moved, covered, or tampered with, ensuring the integrity of your security perimeter.

Considerations:

- This is part of the Immix AI Link V2 feature set (Detect Pro). It functions alongside Person and Vehicle detection. If you do not see this option, ensure your system integration is updated to support V2 features.

Steps:

1. Navigate to Setup > Manage Devices and Alarms.
2. Select the Alarms tab and click the pencil icon (edit) for the target camera.
3. Ensure Enable AI Verification is checked.
4. In the AI Verification menu on the right, locate the checkbox for Scene Change.
5. Check the box to enable it.
6. Click Save.

Successfully enabling this feature results in specific alarms being generated if the camera view is significantly altered or obstructed.

Suggested Next Topic: [Merging Duplicate "Attached Footage" Cameras below](#)

Merging Duplicate "Attached Footage" Cameras

Merging duplicate cameras prevents you from being billed for two streams for a single device and ensures your dashboard analytics are accurate.

Considerations:

- **Attached Footage:** If your NVR sends "Attached Footage" (clips sent via SMTP), Calipsa creates a second camera instance labeled "Attached Footage" in the dashboard. While the system attempts to auto-merge these, it may fail if the parent camera has a privacy mask or if unique identifiers don't match. These must be merged manually.
- **Auto-Merge Limitations:** The system attempts to auto-merge "Attached Footage" cameras with their parent cameras. However, this will not occur automatically if the parent camera has a privacy mask applied, or if the unique `response\_id` between the two cameras does not match.
- **Visual Alert for Mask Conflicts:** If you perform a manual merge and privacy masks exist on both cameras, a red alert notification will appear against the camera in the client tree. You must click the camera and select which mask to apply (Parent vs. Attached) to resolve the conflict.

Steps:

1. Log in to the Calipsa Dashboard.
2. Locate the camera entry labeled "Attached footage" in the site tree.
3. Open the camera settings.
4. Find the "This camera is currently merged with" dropdown menu.
5. Select the matching Parent Camera (the live stream camera) from the list.
6. Click Save.
7. Optional: If prompted regarding privacy masks, select which camera's mask settings should take precedence.

Successfully merging cameras results in a single camera entry in the Calipsa dashboard that processes both live streams and attached SMTP clips, ensuring correct billing.

Troubleshooting "NULL" Cameras

If a camera appears as "NULL" in the Calipsa tree structure, it indicates the "Input number of the NVR" is missing from the data sent by Immix. Ensuring this value is included resolves the tree structure issue.

Suggested Next Topic: [Troubleshooting Unprocessed Alarms below](#)

Troubleshooting Unprocessed Alarms

Enabling the "Raise Unprocessed Alarms" feature allows you to view clips that Calipsa rejected (such as corrupted files or single images), providing transparency into why certain events were not verified.

Considerations:

- By default, Calipsa may reject clips that are too short or consist of only a single image (common with Videcon or Adpro units) to prevent false positives. These rejected clips are hidden unless this setting is enabled.
- Intentional Rejection: In Immix AI Link V2, Calipsa is configured to reject single-image clips to prevent false positives. These rejected clips will appear in the Immix Site Monitor as "Unprocessed" only if the "Raise Unprocessed Alarms" setting is enabled. This allows operators to audit why a clip was not verified without clogging the main alarm queue.

Steps:

1. Navigate to the System tab.
2. Select System Settings.
3. Expand the AI Analytics section.
4. Check the box labeled "Raise Unprocessed Alarms".
5. Save the settings.

Successfully enabling this feature results in rejected clips appearing in the Immix Site Monitor queue with the status "Unprocessed", allowing operators or technicians to audit the footage.

Suggested Next Topic: [Improving Accuracy via False Alarm Reporting on the next page](#)

Improving Accuracy via False Alarm Reporting

Reporting false positives provides critical feedback that retrains the Calipsa algorithm, specifically teaching the system to ignore persistent environmental triggers (like spider webs, moving foliage, or shadows) for that specific camera view.

Considerations:

- This process is performed within the Calipsa Portal, not the Immix application.
- Improvements are not instantaneous; this feedback trains the algorithm over time, with improved results typically expected within 2-3 months.
- Note on False Negatives: If a genuine threat (person/vehicle) was missed and marked as "False" by the system, you cannot correct this in the portal. Instead, you must email the clip to support@calipsa.io for investigation.

Steps:

1. Log into the Calipsa portal.
2. Navigate to the Alarms tab.
3. Locate the specific alarm event that was incorrectly identified as a Person or Vehicle (False Positive).
4. Mark the alarm as False.

Successfully marking alarms as false submits the footage for algorithm retraining, reducing the frequency of similar false alarms from that camera in the future.

Suggested Next Topic: [Troubleshooting Failed Alarm Verification on the next page](#)

Troubleshooting Failed Alarm Verification

Identifying the specific error code associated with a "Faulted" alarm allows you to quickly resolve configuration, network, or file issues preventing Calipsa from analyzing your video footage.

Considerations:

- **HTML5 Requirement:** Devices using Proxy (Flash) are not supported. If a device is not set to use HTML5, it will fail to send footage for verification.
- **Faulted vs. False:** This topic addresses alarms that fail to complete the process (Status: [Faulted]). These appear in the main operator queue and must be acknowledged manually.
- **Stuck in "Processing":** If alarms remain stuck in the Yellow [Processing] state in the Site Monitor, check the Windows Services on the server. The AI Link Forwarder service may have stopped; ensure it is running and set to "Automatic".
- **Common Error Codes:**
 - [NoVideoFile]: No MP4 clip exists (often due to 0-second recording duration or non-HTML5 device).
 - [ConnectionFailed]: Credential mismatch or blocked firewall ports.
 - [AILinkDown]: The Windows Service on the server is not running.
 - [NoVideoDataInFile]: The video file is corrupted (0KB).

Steps:

1. Open the Immix Monitoring Platform and locate the failed alarm in the queue.
2. Check Device Type: Ensure the camera is set to use HTML5. If it uses Proxy/Flash, the verification will fail.
3. Check Recording Duration: Verify the alarm has a "Record Camera" action set to a value greater than 0 seconds. If set to 0 or missing, the system cannot generate the clip required for analysis.
4. Verify Credentials: Navigate to the System Devices page and confirm that the username and password match the AI Link credentials provided to you.
5. Check Windows Services: If the error is [AILinkDown] or alarms are stuck in [Processing], access the server and ensure the AI Link Forwarder service is running and set to "Automatic".
6. Check File Path: If the error is [NoFileStorePath], ensure the event record folder exists and the path is reachable.

Correcting these configuration settings resolves the [Faulted] status, allowing the system to successfully generate and transmit video clips to Calipsa for verification.

Suggested Next Topic: [More Information & Support on the next page](#) if you need to contact Technical Support.

More Information & Support

For additional product documentation and software and firmware upgrades, visit support.pelco.com.

Technical Support

Contact Calipsa Technical Support at support@calipsa.io or Pelco support.pelco.com/s/contactsupport.