LUMINYS

LumiCloud Cameras

User Manual

Rev. 1

Foreword

General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the LumiCloud camera. Please read it carefully before using the platform and store it safely for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	February 2026

Privacy Protection Notice

As a device user or data controller, you may collect personal data such as facial images, fingerprints, and license plate numbers. It's essential to comply with local privacy laws to safeguard individuals' rights. This includes providing clear identification of surveillance areas and necessary contact information.

Disclaimer

While we strive to ensure the accuracy and completeness of this document, we do not provide any formal guarantees. The use and results derived from this document are the sole responsibility of the user. We also reserve the right to modify its contents without prior notice.

About the Manual

- This manual is for reference only and may have minor discrepancies with the actual product.
- We are not liable for damages resulting from improper operation contrary to this manual.
- The manual will be updated to align with the latest laws and regulations. For more information, refer to the paper manual, scan the QR code, use our CD-ROM, or visit our official website. Minor differences may exist between electronic and paper versions.
- All designs and specifications are subject to change without notice. Product updates may lead to discrepancies between the manual and the actual product. Contact customer service for the latest information and documentation.
- There may be errors or inaccuracies in the descriptions of functions, operations, and technical data. We reserve the right of final interpretation in case of questions or disputes.
- If the manual cannot be opened, please update your reader software or try another compatible reader.
- All trademarks and company names mentioned are the properties of their respective owners.
- For assistance, visit our website or contact your supplier or customer service.
- We reserve the right of final interpretation in case of questions or disputes.

Safety Instructions

The following symbols might appear in the manual.

Symbol	Definition
⚠	Indicates a risk hazard that, if not avoided, may result in death, injury, property damage, data loss, decreased performance, or unpredictable outcomes.

Symbol	Definition
	Offers methods to help you troubleshoot issues or save time.
	Provides more context and information.

Important Safeguards and Warnings

Transportation and Storage Requirements

- Only transport and store the device under the allowed humidity and temperature conditions.
- Use the original manufacturer-provided packaging or equivalent high-quality packaging for safe transportation.
- Avoid applying excessive pressure, exposing the device to strong vibrations, or immersing it in liquid during transit.
- Keep the device away from humid, dusty, extremely hot or cold environments, as well as areas with strong electromagnetic radiation or unstable lighting conditions.
- Avoid placing heavy pressure on the device, exposing it to strong vibrations, or immersing it in liquid during storage.

Installation Requirements

- Adhere to local electrical safety codes and standards, verifying the correct power supply before operating the device.
- Ensure the power supply meets **ES1 in IEC 62368-1** standards and does not exceed PS2. Verify power requirements on the device label.
- It is recommended to use the power adapter provided with the device.
- Do not connect the device to multiple power sources unless explicitly stated, as this may cause damage.
- Install the device in a location accessible only to trained professionals to prevent potential injury to unauthorized individuals. Professionals must be fully aware of all safety precautions and warnings associated with the device.
- Avoid applying excessive pressure, exposing the device to strong vibrations, or submerging it in liquid during installation.
- Ensure an emergency disconnect device is installed in an easily accessible location to allow for immediate power shutoff when necessary
- For enhanced lightning protection, use the device with a lightning protection device. In outdoor environments, strictly follow lightning protection regulations.
- Ground the functional earthing section of the device to enhance reliability. As a Class I electrical appliance, ensure the device is connected to a power socket with protective grounding.

  ⓘ Some models may not have designated earthing holes
- The dome cover is an optical component; avoid direct contact or wiping the surface during installation to prevent damage.

Operation Requirements

- Never open the device cover while the device is powered on.
- Avoid touching the heat dissipation components to prevent the risk of burns.
- Use the device within the specified humidity and temperature ranges.
- Do not aim the device at strong light sources (e.g., lamps, sunlight) when focusing, as this may shorten the lifespan of the CMOS sensor and cause overbrightness or flickering.
- Do not expose the device to laser radiation.
- Do not allow liquid to enter the device.
- Protect indoor devices from rain and moisture to reduce the risk of electric shock or fire.
- Do not obstruct the ventilation openings near the device to prevent heat buildup.

- Ensure that the power cord and wires are not subject to pressure or walking on, especially at plugs, power sockets, and exit points from the device.
- Avoid direct contact with the photosensitive CMOS sensor. Use an air blower to clean the lens from dust or dirt.
- The dome cover is an optical component; avoid direct contact or wiping its surface.
- There may be a risk of electrostatic discharge on the dome cover. Always power off the device when installing the cover after adjusting the camera. Avoid touching the cover and ensure that it is not exposed to other equipment or individuals.
- Enhance the protection of the network, device data, and personal information. Implement necessary security measures such as using strong passwords, regularly updating passwords, keeping firmware updated, and isolating computer networks. For some older IP Camera firmware versions, the ONVIF password may not synchronize automatically after the main system password is changed; you will need to update the firmware or manually change the password.

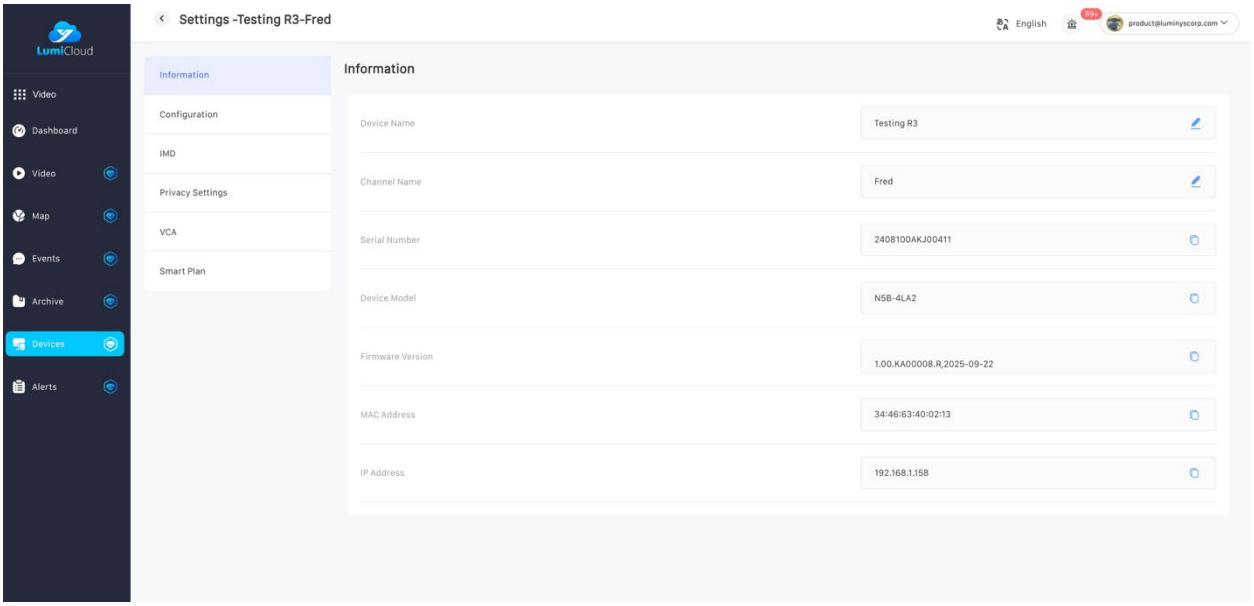
Maintenance Requirements

- Always follow the provided instructions when disassembling the device. Non-professionals attempting to dismantle the device may cause water leakage or poor image quality. If the device requires disassembly before use, ensure that the seal ring is properly seated in the seal groove when reassembling the cover. If condensation appears on the lens or the desiccant turns green after disassembly, contact after-sales service for desiccant replacement. (Desiccants may not be provided for certain models.)
- Only use manufacturer-approved accessories.
- Only allowed qualified personnel to install, maintain, and operate the device.
- Never touch the photosensitive CMOS directly. Use an air blower to remove dust or dirt from the lens. If cleaning is necessary, slightly moisten a soft cloth with alcohol and gently wipe away dirt.
- Clean the device body with a soft, dry cloth. For stubborn stains, use a cloth lightly dampened with neutral detergent and wipe the surface dry. Avoid using volatile solvents (e.g., ethyl alcohol, benzene, or diluent) or abrasive detergents, as these may damage the coating and degrade the device's performance.
- The dome cover is an optical component. If it becomes dirty with dust, grease, or fingerprints, use degreasing cotton lightly moistened with ether or a clean, soft cloth dipped in water to gently clean it. An air blower is also effective for removing dust.
- Cameras made from stainless steel may develop rust when exposed to corrosive environments (e.g., near the seaside or in chemical plants). To remove rust, use an abrasive soft cloth moistened with a mild acid solution (vinegar is recommended) and gently wipe the rust away. Then, wipe the surface dry.

Table of Contents

Device Configuration

There are two ways to navigate to the device config section: through the sidebar or through channel settings. You can view basic camera information and configure the camera mode and resolution, intelligent motion detection (iMD), privacy settings, Video Content Analytics (VCA), and Smart Plan.

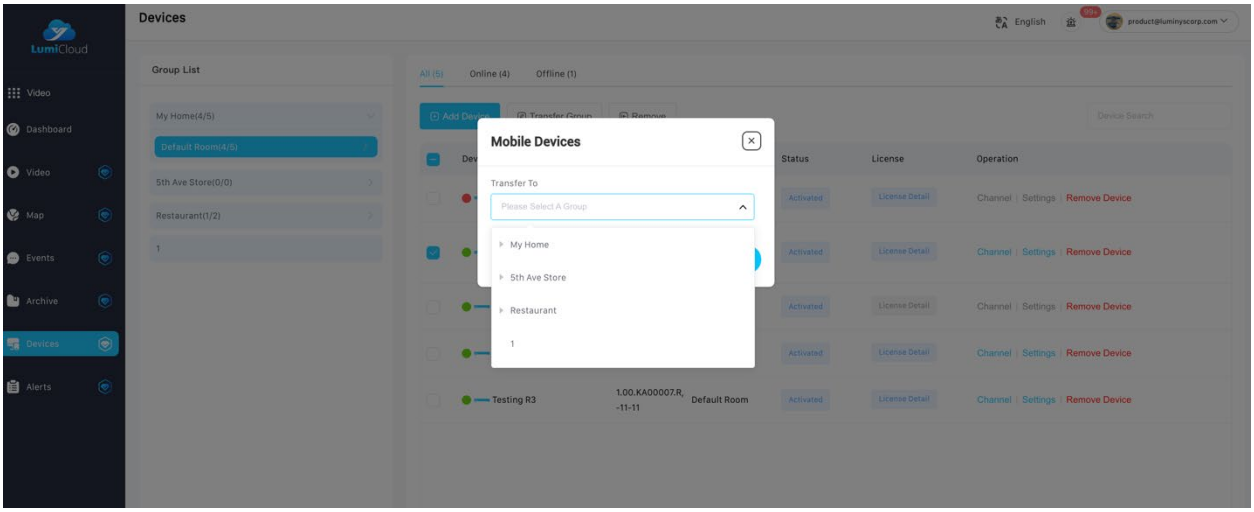


Device Configuration Menu

Transfer a Device to a Different Group

Follow the steps below to add a device to LumiCloud.

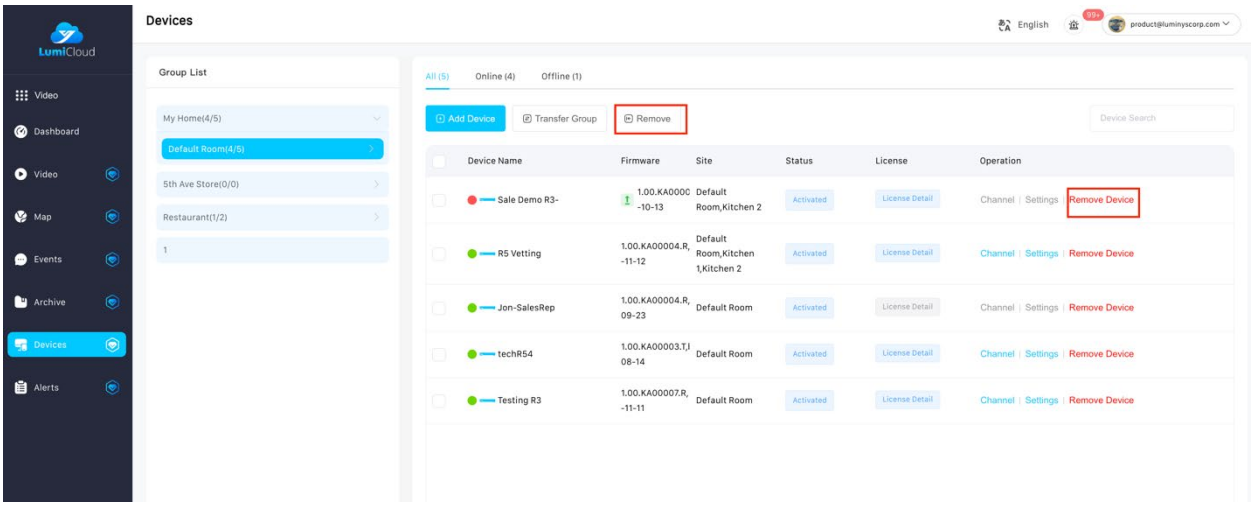
1. Navigate to **Devices**.
2. Find the device in the group list.
3. Click **Transfer Group**.
4. Choose a new group to transfer the device.
5. Click **Save** when done.



Transfer Device to Different Group

Remove a Device

To remove a device, navigate to **Devices** and select the device from the group list. Click **Remove** at the top of the screen or next to the right side of the screen.



Remove a Device

Add a Device License

To add a device license, refer to the LumiCloud camera quick start guide.

All LumiCloud cameras include a complimentary one-year trial subscription license of LumiCloud HD Unity (LVL-HDV-UC). After the trial subscription expires, licenses must be purchased and added to a device by the user.

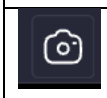
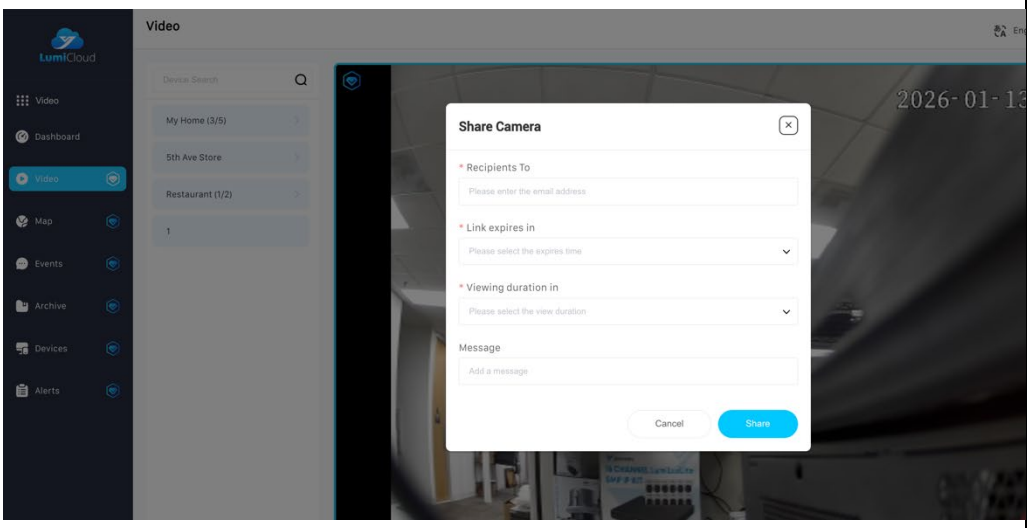
View the Dashboard

The LumiCloud camera dashboard allows users to view the following information: the number of sites associated with an account, device numbers, device licenses and their status, event summaries for humans and vehicles, and system alert summaries from the 60 minutes, seven days, 24 hours, or 30 days.

Live View and Playback

Live View

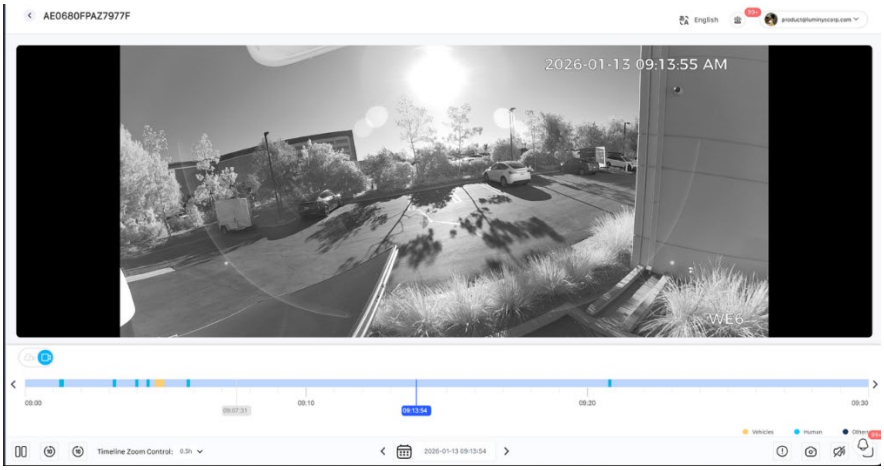
Refer to this section to learn about the live view playback functions of the LumiCloud platform.

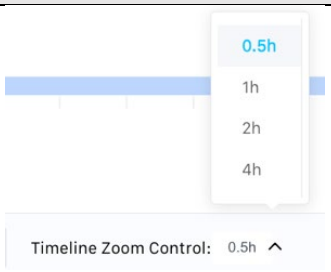
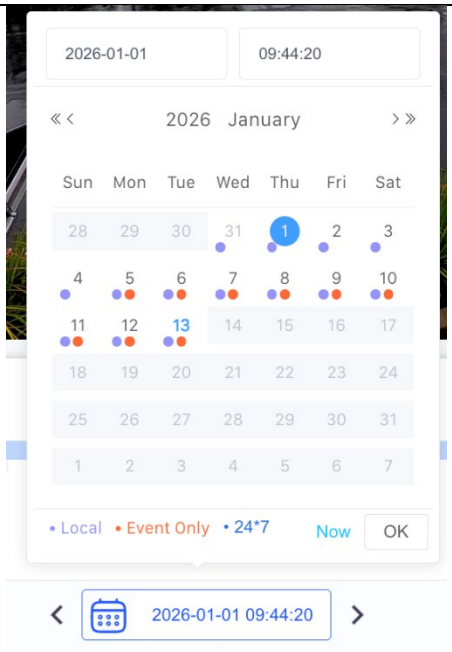
Icon	Description and Function
	Creates a new live-view grid of an area.
	Configures the number of spaces and layout of the live-view grid.
	Takes a snapshot of the live view.
	Zooms in and out of the live-screen view. Only available singular view layouts.
	Allows users to share up to two (2) minutes of video with a specific recipient. 
	Controls PTZ functions. These settings are not applicable to LumiCloud cameras.
	Allows users to play back video.

Video Playback

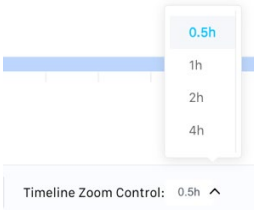
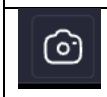
LumiCloud supports local storage and cloud storage playback. Refer to this section to learn about the functions available on the playback section of LumiCloud.

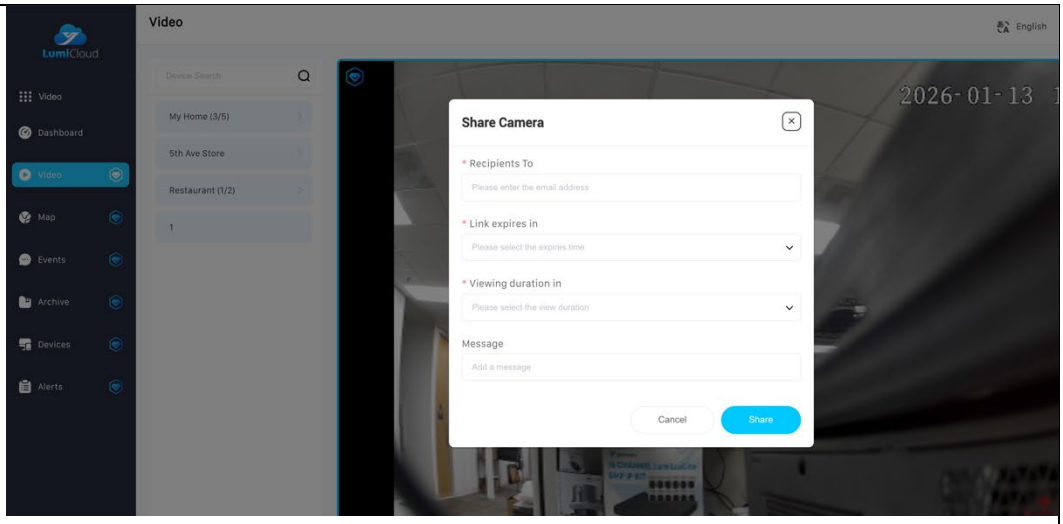
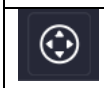
ⓘ A LumiCloud 24/7 storage subscription must be purchased for cloud storage playback. See the LumiCloud data storage subscription license datasheet on the official Luminys website for more information.



Function	Description	Image
Time Zoom Control	Adjusts the timeline interval.	
Calendar	Find and view videos from a specific day. The type of video available for playback is visually indicated. Days that are greyed out have no recordings available for view.	

	Only shows video clips with events.	
		
		
		

Function	Description
Time Zoom Control	Adjusts the timeline interval. 
	Configures the number of spaces and layout of the live-view grid.
	Takes a snapshot of the live view.
	Zooms in and out of the live-screen view. Only available singular view layouts.
	Allows users to share up to two (2) minutes of video with a specific recipient.

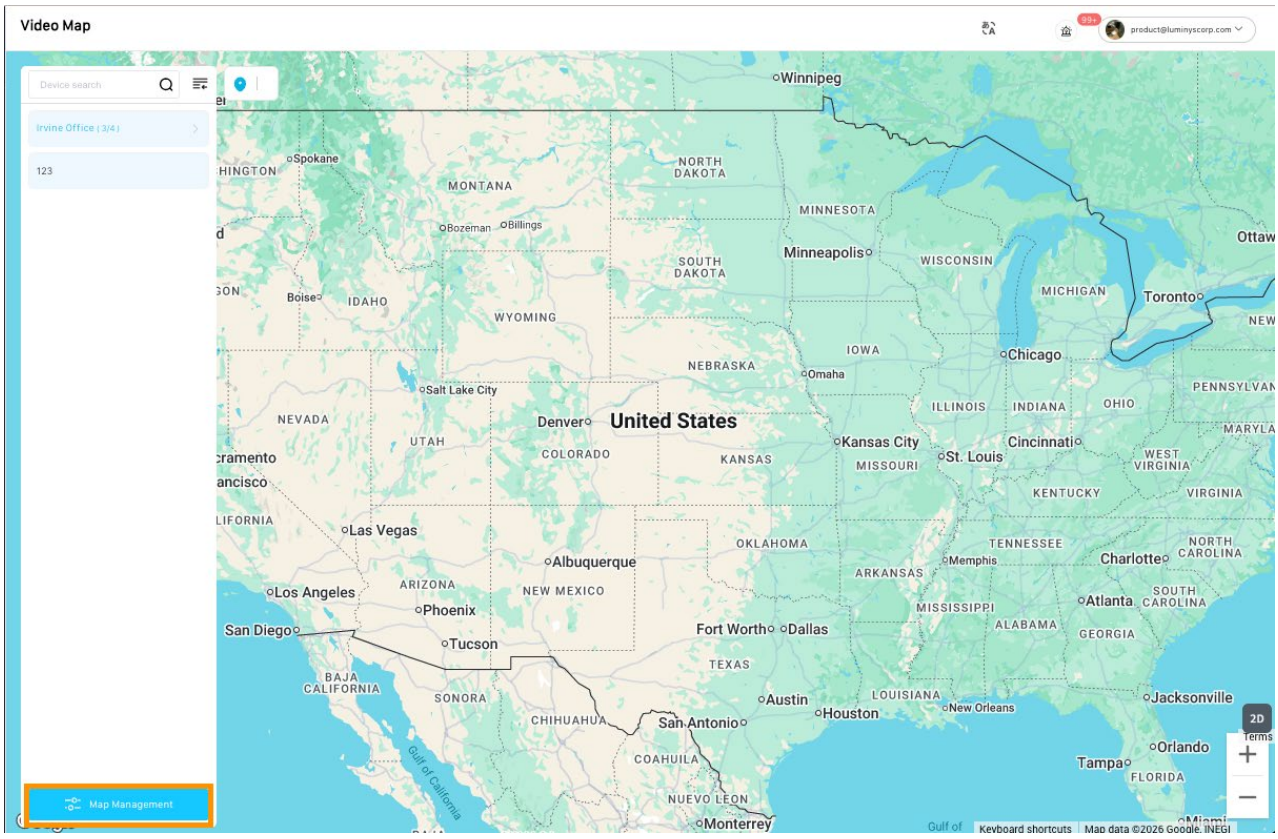
	
	Controls PTZ functions. These settings are not applicable to LumiCloud cameras.
	Allows users to play back video.

Device Location

Users can assign LumiCloud cameras to a specific location. Cameras assigned to a location will appear on the same map for streamlined device management.

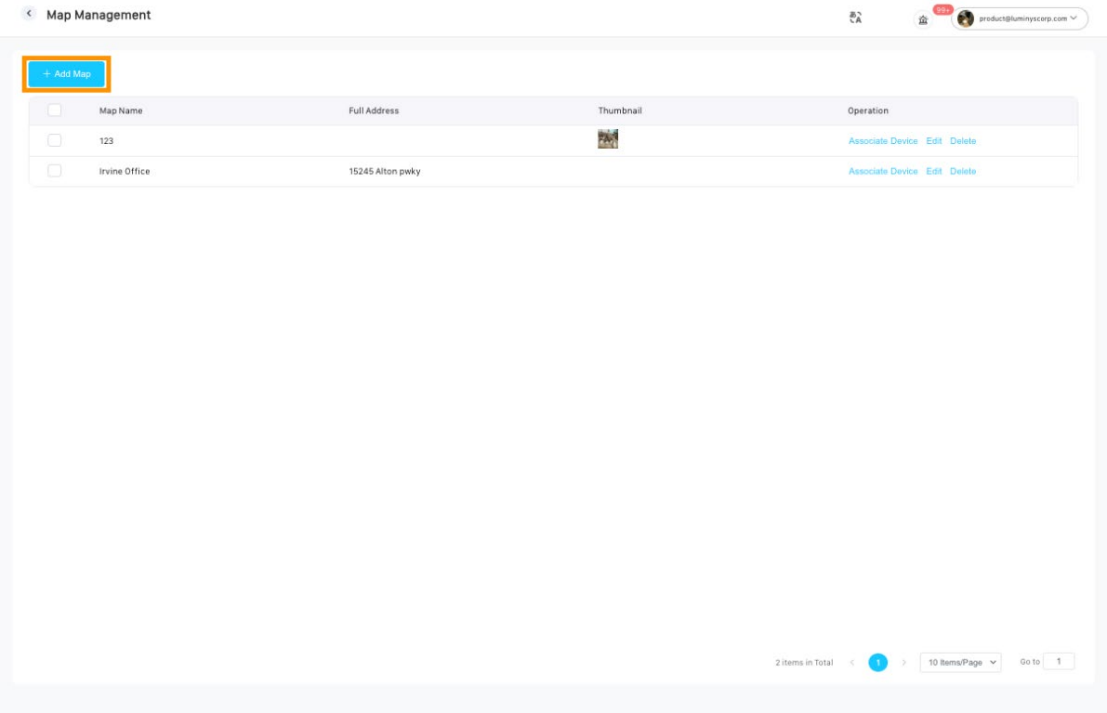
Follow the steps below to generate a map location and assign a device to it.

1. Navigate to the map in LumiCloud. Click **Map Management.**



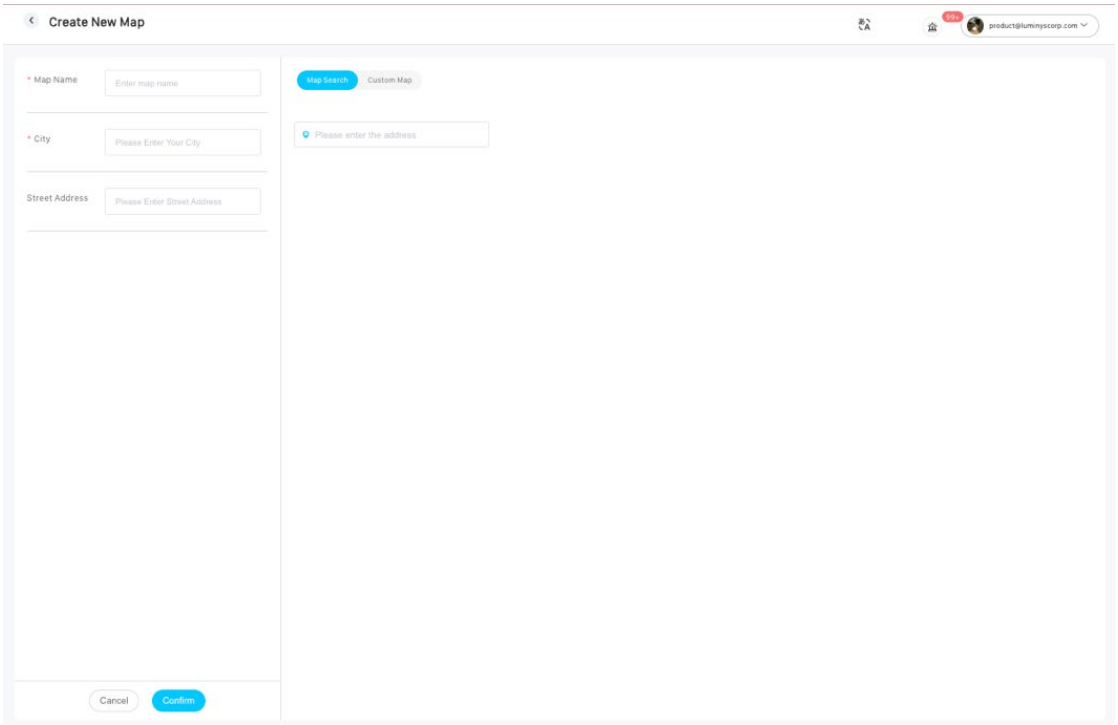
Map Management

2. Click **Add Map**.



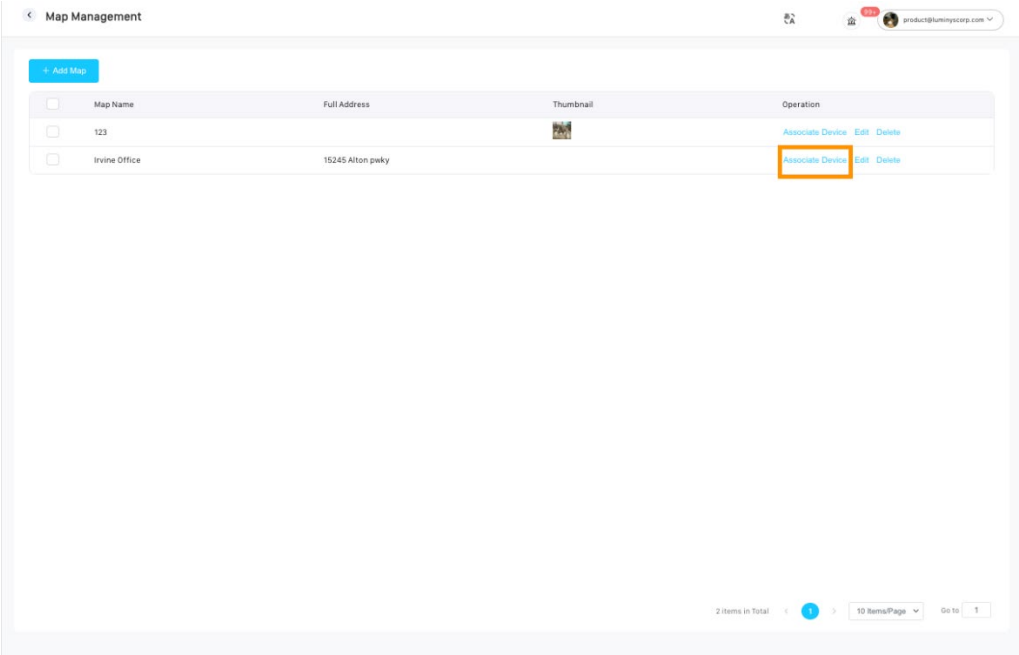
Add Map

3. Enter the map name and the device location. You may enter the name of the city the device is in or the full device address. Click **Confirm** when done.



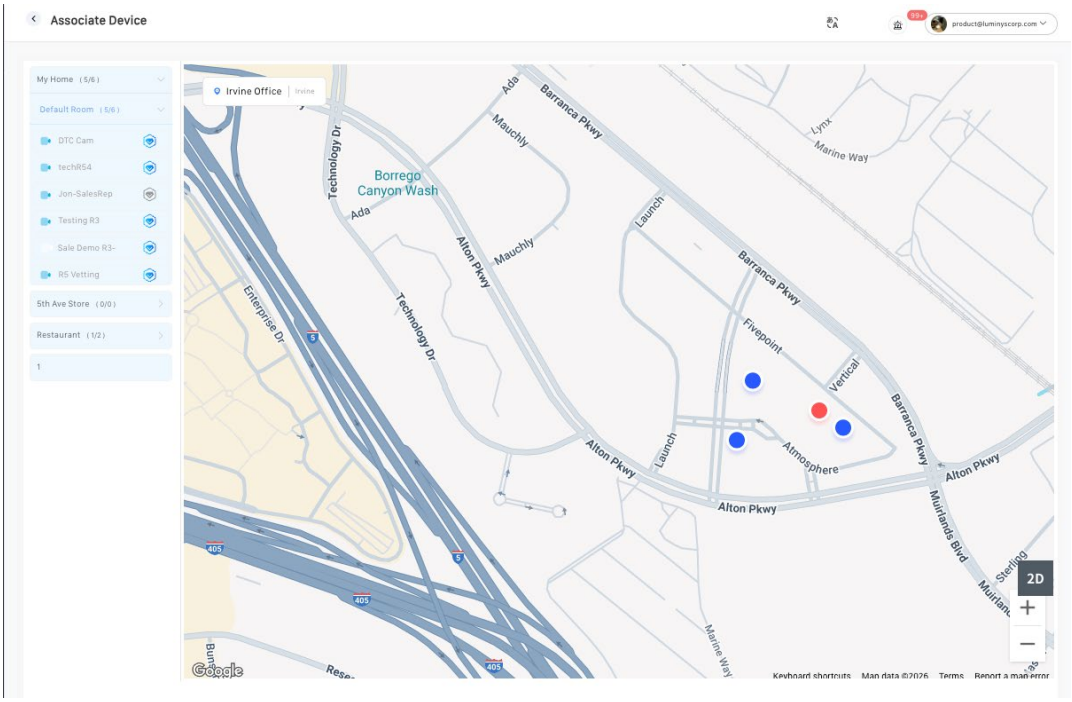
Create New Map

4. Click **Associate Device** for the desired address on the Map Management page.



Associate Device

5. Click and drag the desired devices onto the map to assign them to the selected location.



Add Devices to Location

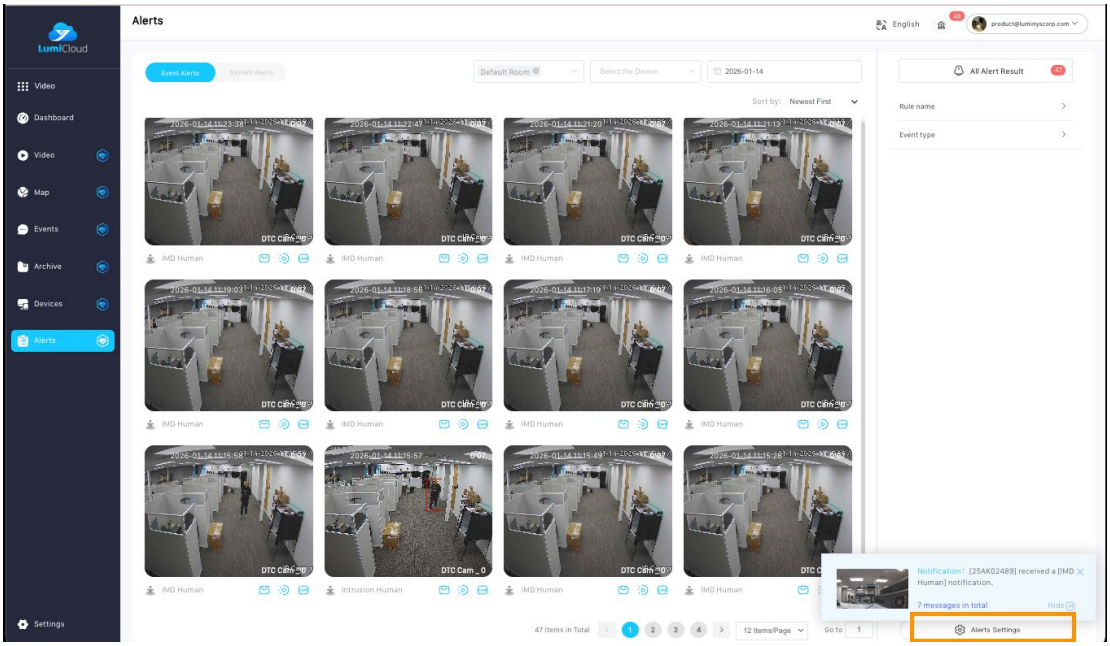
Users may edit a location and the devices assigned to it by clicking **Edit** for the address on the Map Management page.

Event and System Alerts

Create or Edit an Event Alert Rule

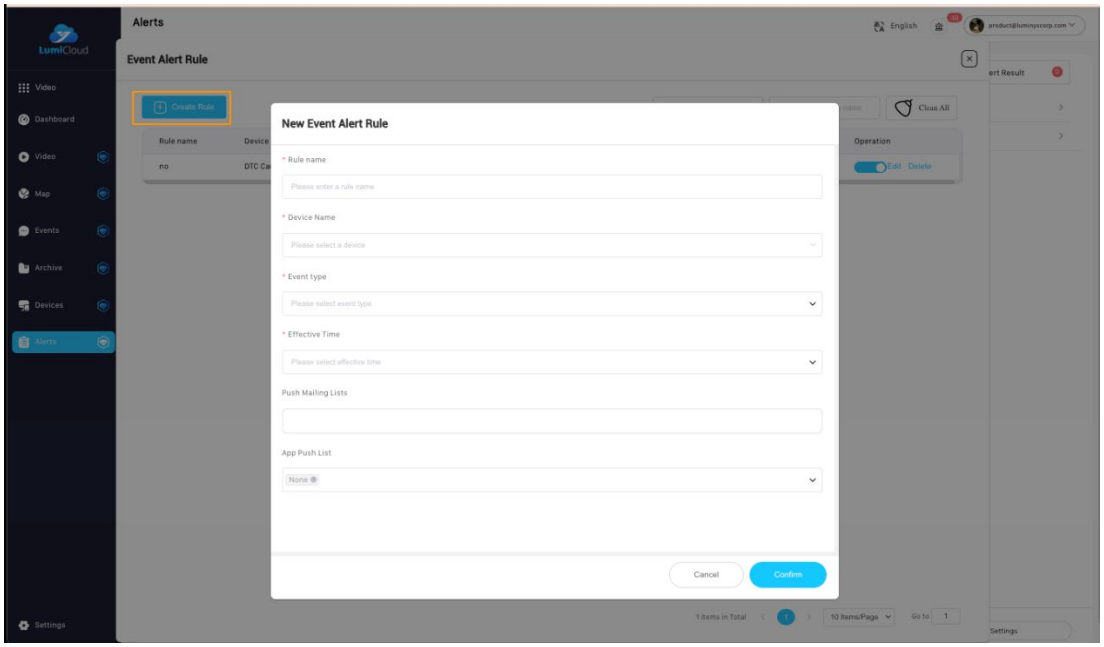
Follow the steps below to create or edit an alarm rule for an event.

1. Navigate to **Alerts → Event Alerts → Alerts Setting**.



Event Alerts Setting

2. Click **Create Rule**. Enter the name of the rule, device, rule effective date, and one of the nine event alert types supported by LumiCloud.
3. If desired, enable email alerts by entering the recipients for email notifications and LumiCloud mobile app alerts.
4. Click **Confirm** when done.



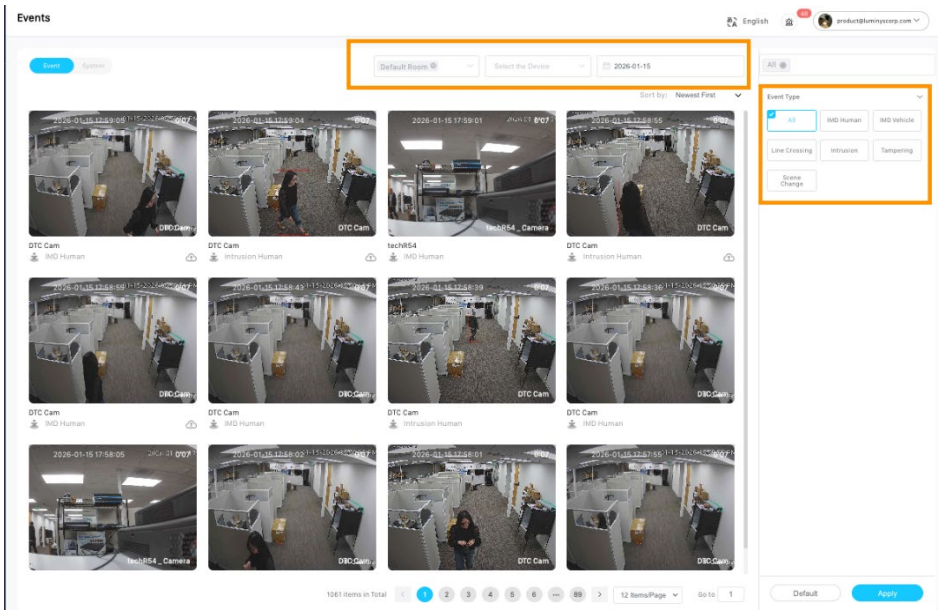
New Event Alert Rule

ⓘ

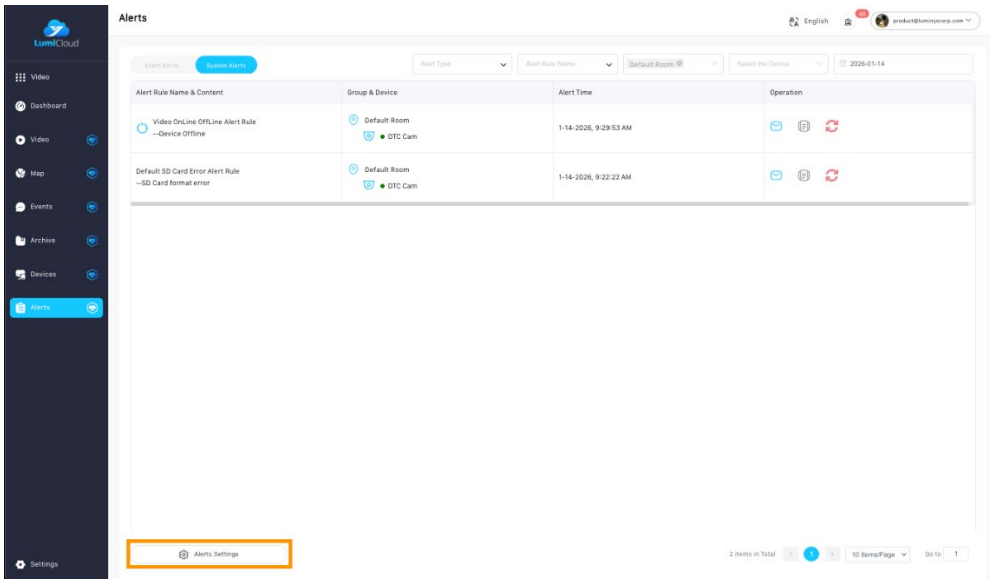
- The type of system alerts may vary depending on the device.
- Only an admin account can set the rule effective date and enable email and app alerts. Regular user accounts are only able to create and edit alert rules associated with devices assigned to them and enable email and app alerts for themselves only.

Create or Edit an System Alert Rule

Follow the steps below to create or edit an alert rule for your system. There are three system alerts supported by LumiCloud: device offline, no SD card, or SD card error.



1. Navigate to **Alerts → System Alerts → Alerts Setting**.



Alerts Setting

2. Toggle the button under operation to enable system notifications.

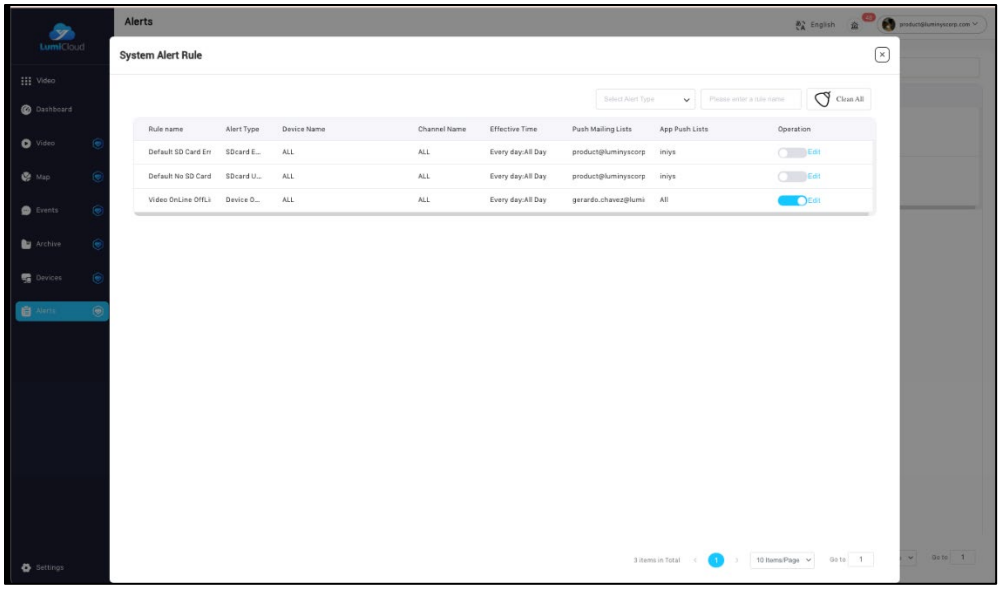


Figure 1

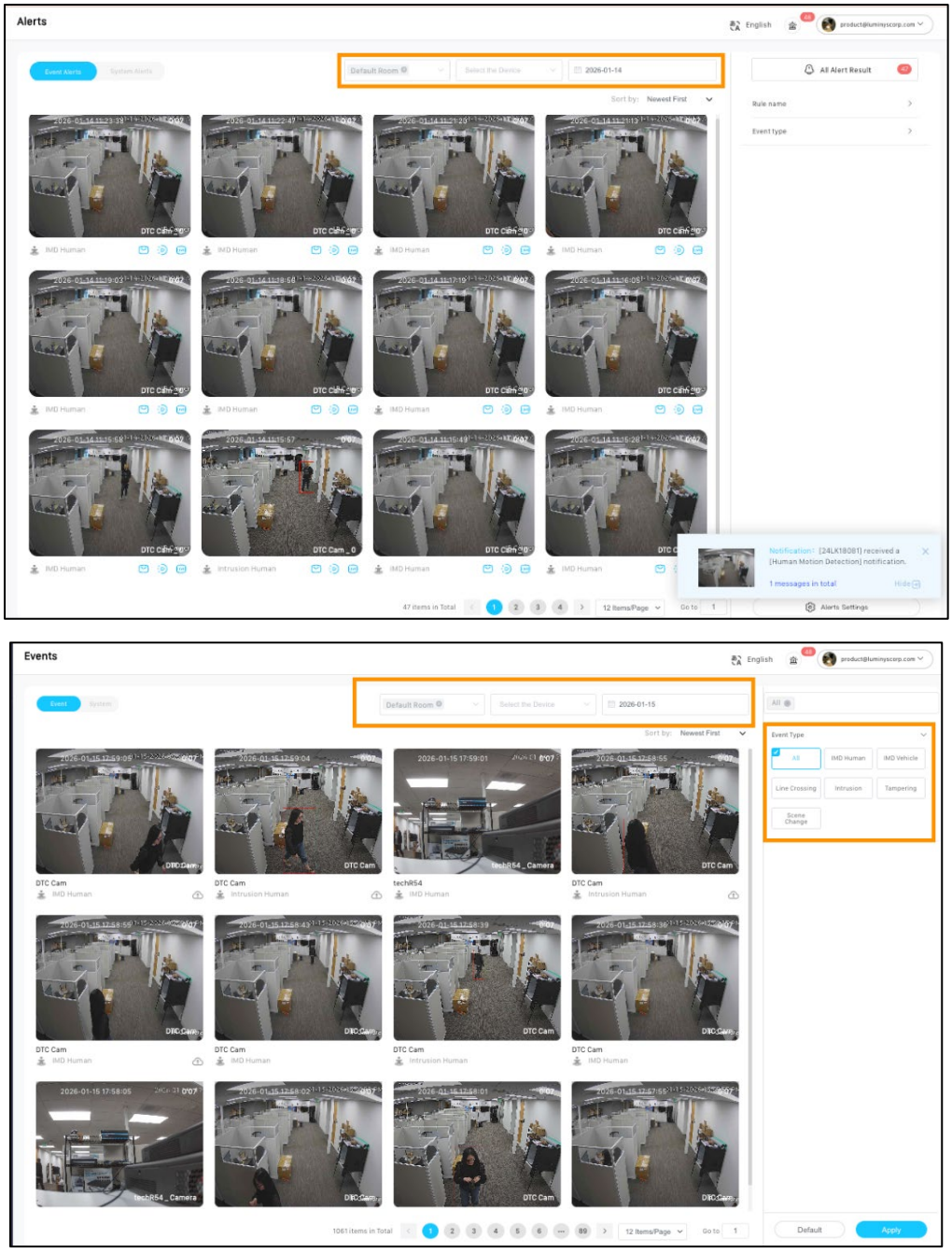
ⓘ

- The type of system alerts may vary depending on the device.
- Only an admin account can enable and edit system alerts. Regular user accounts are only edit system alerts for devices assigned to them.

View Event and System Alerts

View Event Alerts

Users can view event alerts from the Alert section and filter the event alerts based on dates, device, location, rule name, or event type.

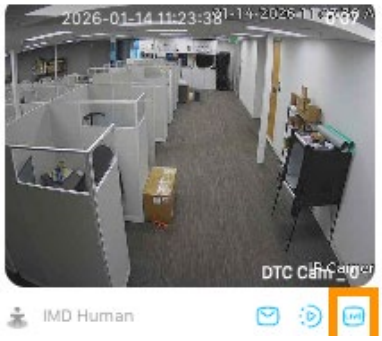


View Event Alerts

Users can also go to the playback section and view the video that triggered the alert by clicking the playback button.

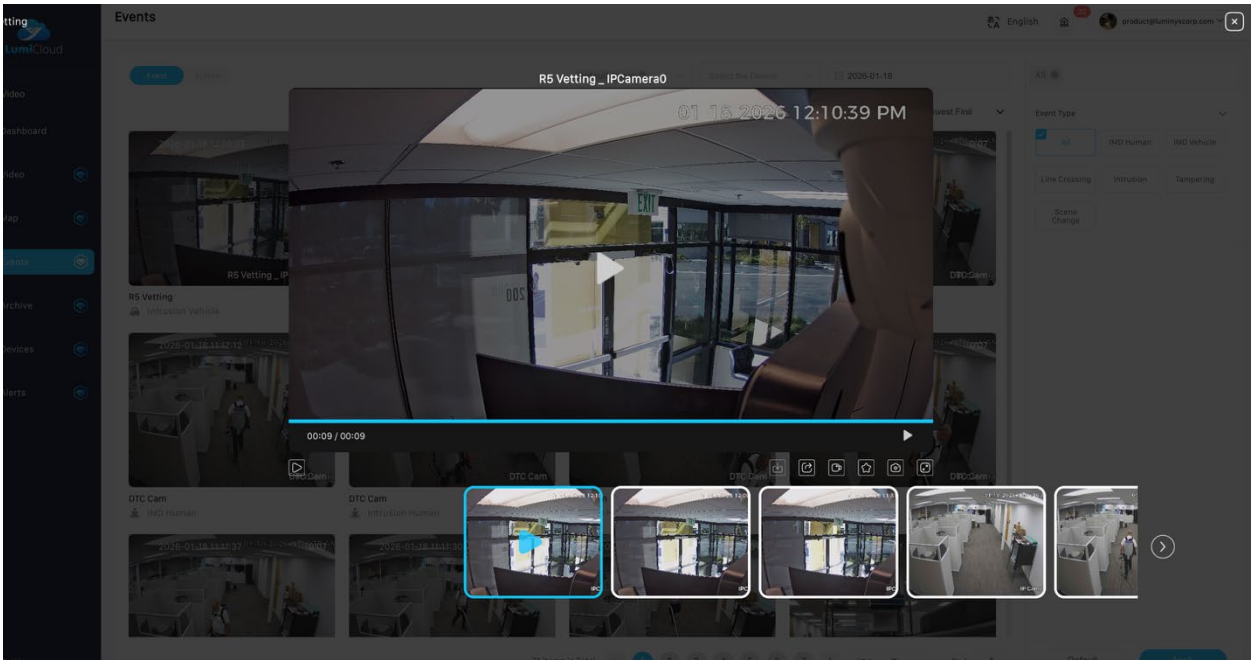
Playback

Users can also go to live view from the alerts page by clicking on the icon in the bottom right corner.



Live View

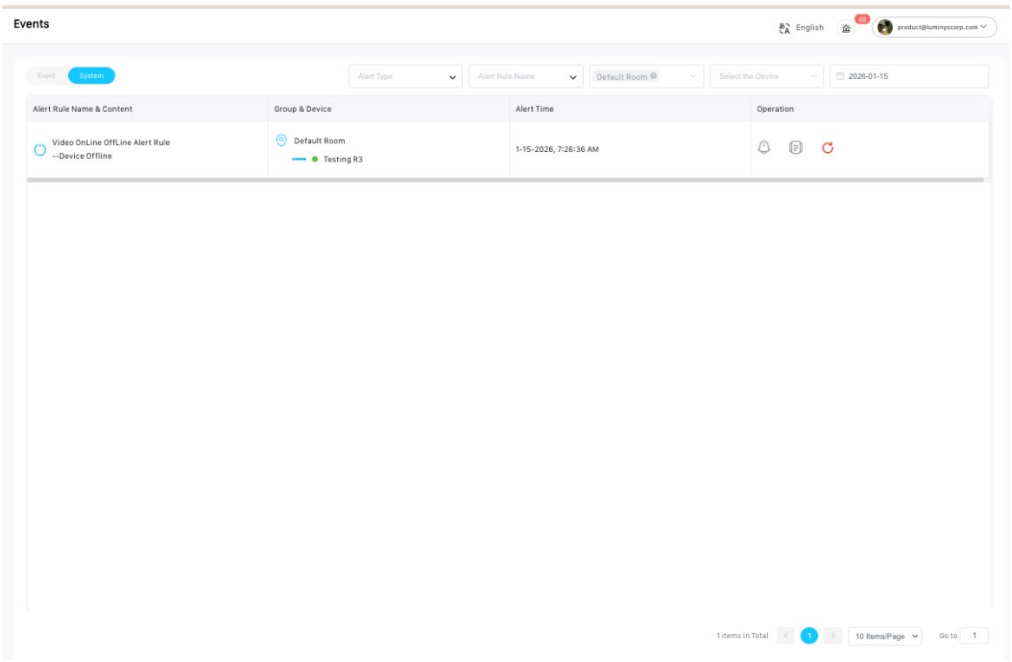
Users can click on a specific event to share the event via email, view related events, play back video from the time the event began, take a snapshot of the event, or archive the event.



Event

View the System Alerts

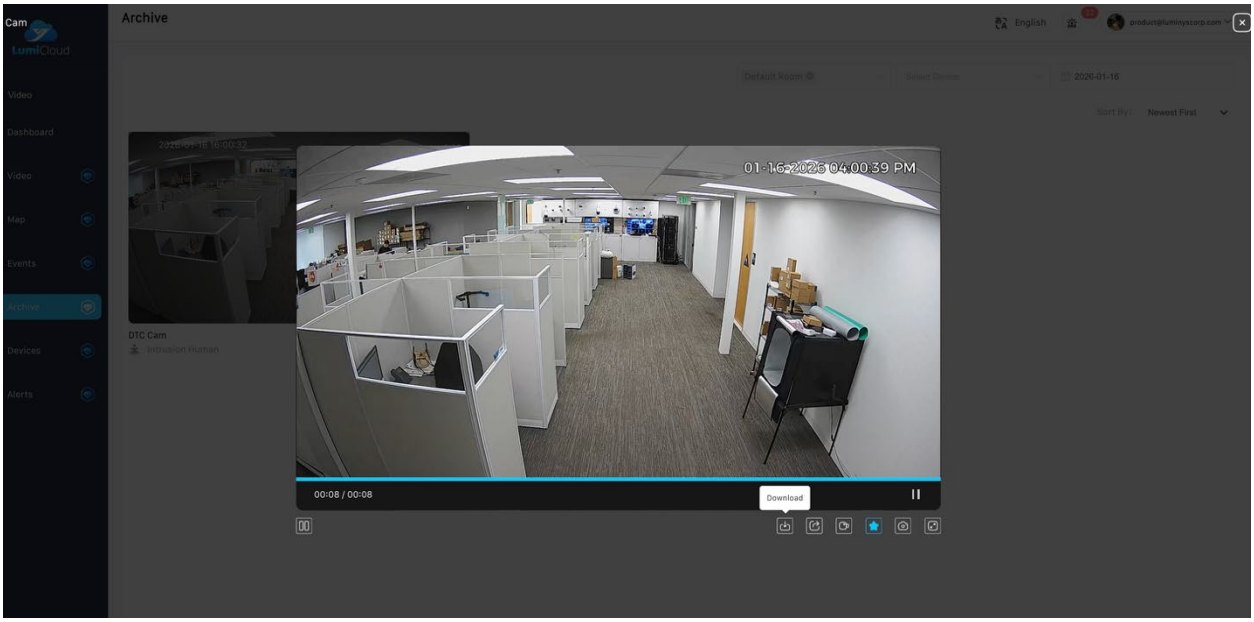
Users can view system alerts from the system alert section and reboot the device from the cloud if the device has offline alerts enabled. Alerts can also be filtered based on type, rule, and location.



View System Alerts

Archive

Up to 30 GB of video can be archived in LumiCloud. Administrators and regular users share the 30 GB and do not have their own individual archive. Event clips may be downloaded from the archive after archiving them from the event section. Archived events can be filtered by group, date, or device for fast location.



Download Archive Clip

Appendix: Cybersecurity Recommendations

Account Management

1. **Use complex passwords.**

Follow the guidelines below to create a strong password:

- The password should be at least 8 characters long.
- Include at least two types of characters: uppercase letters, lowercase letters, numbers, and symbols.
- Avoid using the account name or its reverse.
- Do not use consecutive characters (e.g., 123, abc).
- Do not use repeating characters (e.g., 111, aaa).

2. **Change passwords periodically.**

It's advisable to regularly change the device password to minimize the risk of it being guessed or cracked.

3. **Allocate accounts and permission appropriately.**

Add users based on service and management needs, assigning the minimum necessary permissions

4. **Enable account lockout function.**

The account lockout function is enabled by default. Keep it enabled to enhance account security; after multiple failed login attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner.**

The device supports a password reset function. To reduce the risk of unauthorized access, update this information promptly if there are any changes. When setting security questions, avoid using easily guessed answers

Service Configuration

1. **Enable HTTPS.**

It’s recommended to enable HTTPS for secure access to web services

2. **Change passwords periodically.**

If your audio and video data contents are important or sensitive, use encrypted transmission function to reduce the risk of your audio and video data being eavesdropped on during transmission.

3. **Allocate accounts and permission appropriately.**

It's advisable to disable services such as SSH, SNMP, SMTP, UPnP, and AP hotspot when not in use or required to reduce attack surfaces. If these services are necessary, consider the following safe modes:

- **SNMP**: Use SNMP v3 with strong encryption and authentication passwords.
- **SMTP**: Use TLS for accessing the mailbox server.
- **FTP**: Use SFTP with complex passwords.
- **AP Hotspot**: Use WPA2-PSK encryption with complex passwords.

4. **Enable account lockout function.**

It is advisable to change the default ports for HTTP and other services to any port between 1024 and 65535 to reduce the risk of being targeted by threat actors.

Network Configuration

1. **Enable Allowlist.**

It is recommended to enable the allow list function and only permit IP addresses on the allow list to access the device. Be sure to add your computer's IP address and any supporting device IP addresses to the allow list

2. **MAC address binding.**

It is advisable to bind the gateway's IP address to the device's MAC address to mitigate the risk of ARP spoofing.

3. **Build a secure network environment.**

To enhance device security and reduce potential cyber risks, the following measures are recommended:

- **Disable Port Mapping**: Turn off the port mapping function on the router to prevent direct access to internal devices from the external network.
- **Network Partitioning**: Based on actual network needs, partition the network. If there is no communication requirement between two subnets, consider using VLANs and gateways to achieve network isolation.
- **Implement 802.1x Access Authentication:** Establish an 802.1x access authentication system to minimize the risk of unauthorized terminal access to the private network.

Security Auditing

1. **Check online users.**

Check online users regularly to identify illegal users

2. **Check device logs.**

Review logs to learn about the IP addresses attempting to log in and track key operations performed by authorized users

3. **Configure network logs.**

The device can only retain a limited number of logs. To save logs for an extended period, it's recommended to enable the network log function to synchronize critical logs to a network log server for future reference

Software Security

1. **Update firmware on time.**

It is important to update device firmware to the latest version to ensure access to the latest features and security enhancements. If the device is connected to the public network, enable the automatic detection function for online upgrades to receive timely firmware update notifications from the manufacturer

2. **Update client software on time.**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended to implement physical protection for devices, especially storage devices. Consider placing them in a dedicated machine room or cabinet and establish access control and key management to prevent unauthorized personnel from damaging hardware and peripheral equipment (e.g., USB flash drives, serial ports).