

User Manual



Overview

Thank you for selecting VORTEX as your AI-enhanced and cloud-empowered surveillance system. Please refer to this user manual whenever you have questions using VORTEX. In addition, you can check VORTEX FAQ on the web for more information.

Revision History

Document Version	Release Date	Product Version	Comment
1.0	N/A	N/A	Initial release.
1.1	2026-07-31	3.12.5	Added new features. Improved instructions and explanations. Corrected typos and grammatical errors.

Table of Contents

1 Introduction	P8
2 Legal Information & Terms of Service	P9
3 System Requirements	P10
4 Establishing a VORTEX Service	P11
Creating a VORTEX Account & Adding Devices (Web Portal)	
Creating a VORTEX Account & Adding Devices (Mobile App)	
Adding a VIVOTEK NVR Device	
Adding a VIVOTEK VSS	
5 Joining a VORTEX Service	P19
Adding a VORTEX Account via the Web Portal	
Adding a VORTEX Account by Invitation	
6 Managing Your Account	P23
My Account	
Profile	
Preferred Language	
Multi-Factor Authentication (MFA)	
Notification Center	
API Key Management	
About VORTEX	
Sign Out	
7 View	P28
Sharing Device Live View and Playback	
Frame by Frame Playback	
Synchronized playback	
8 Customized View	P36

Create a Customized View
 Setup Carousel View
 Copy and Send Customized View

9 Devices P39

Device Settings

System > Device Information
 System > Firmware update for both VORTEX camera & VIVOTEK NVR
 System > Remote support
 System > Installation
 System > Network Speaker
 System > NVR Settings
 Media > Image Settings
 Media > Image Focus Adjustment
 Media > Audio Settings
 Detection > Audio Detection
 Detection > Tampering Detection
 Detection > Video Content Analysis
 VORTEX VCA Set Up
 DI/DO > Digital Input
 DI/DO > Digital Output
 Recording & Storages > Cloud Backup

10 User Management P55

Role Settings

Invite Users

11 AI Hub P58

Deep Search

Deep Search Interfaces
 Deep Search (New Interface)
 Original Deep Search
 Using Deep Search to Search for People
 Using Deep Search to Search for Vehicles
 Using Re-Search

Think Search

Think Search

Event Insight

Case Vault

12 Profile Search P72

Creating a Profile

Records

13 Message Center P79

Event Type

Search Filter

Snooze Single Rule

14 Archive P83

Create Archived Video Clips

Search Archived Video Clips

Sharing Archived Files

15 System P89

Organization Details

Alarm Management

Snooze the Alarm

Global Device Settings > Auto Firmware Update

Global Device Settings > Event Delay

Global Device Settings > Smart Privacy Switch

Reseller Management

Single Sign-on Configuration

Audit Log

Organization-Level Multi-Factor Authentication (MFA)

16 License P99

License Plan

Pre-bundle kit

License Types for the Organization on xStd/xPro Plan

Camera Licenses

Network Speaker Licenses

Cloud Backup Licenses

Advanced AI Bundle Licenses

License Information

License Control Overview

Organization Status and Phases

Add-On License Rules

Downgrade from xStd/xPro to xLite

17 License-Required Features

P103

Network Speaker

Bridge Set-up

Full Feature Unlock

Why It Matters

VORTEX Set-up Guide

Set Up Talk Down Feature

Operate Talk Down

Manage Audio Files

Set Up Alarm Management for Audio Deterrent

Introduction

VORTEX is an AI-powered, cloud-native video surveillance-as-a-service (VSaaS) platform designed to transform how businesses approach security. By combining powerful edge computing with the flexibility of the cloud, VORTEX moves beyond traditional recording to provide a proactive, data-driven security ecosystem. It empowers users to monitor complex environments—from single locations to large-scale multi-site operations—through a single, intuitive interface, ensuring that comprehensive protection is always within reach.

Legal Information & Terms of Service

2

Thank you for choosing **VORTEX Cloud Video Surveillance**. To ensure that you understand your legal rights and how we safeguard your personal information and video data, please carefully review the following policies and agreements.

By continuing to use VORTEX services, you acknowledge that you have read and agreed to the terms outlined below. The most up-to-date versions of these documents are always available on our official website.

1. Privacy Policy

This policy explains how VORTEX collects, processes, uses, and protects your personal information and video data. It also outlines our commitment to data encryption and security measures.

- View Full Document: <https://www.vortexcloud.com/tc/privacy-policy>

2. End User License Agreement (EULA)

The EULA defines the scope of software authorization, your rights as a user, and the restrictions governing the use of VORTEX software and platform features.

- View Full Document: <https://www.vortexcloud.com/tc/agreement-user>

3. Terms and Conditions

These terms govern the general use of the VORTEX cloud platform, including account registration requirements, subscription and payment terms, and the scope of liability of both parties.

- View Full Document: <https://www.vortexcloud.com/tc/terms-and-conditions>

System Requirements

Before using VORTEX, have the following items ready:

- A PC or laptop running Chrome or Edge
- A router
- VORTEX cameras or VORTEX app (from App Store or Google Play)
- VORTEX cameras

NOTE

An internet connection is also a must. Otherwise, VORTEX cameras and the VORTEX service cannot communicate with the VORTEX servers, so you will not be able to use important features such as video storage, live view for real-time monitoring, or any of the other functionalities offered by the service.

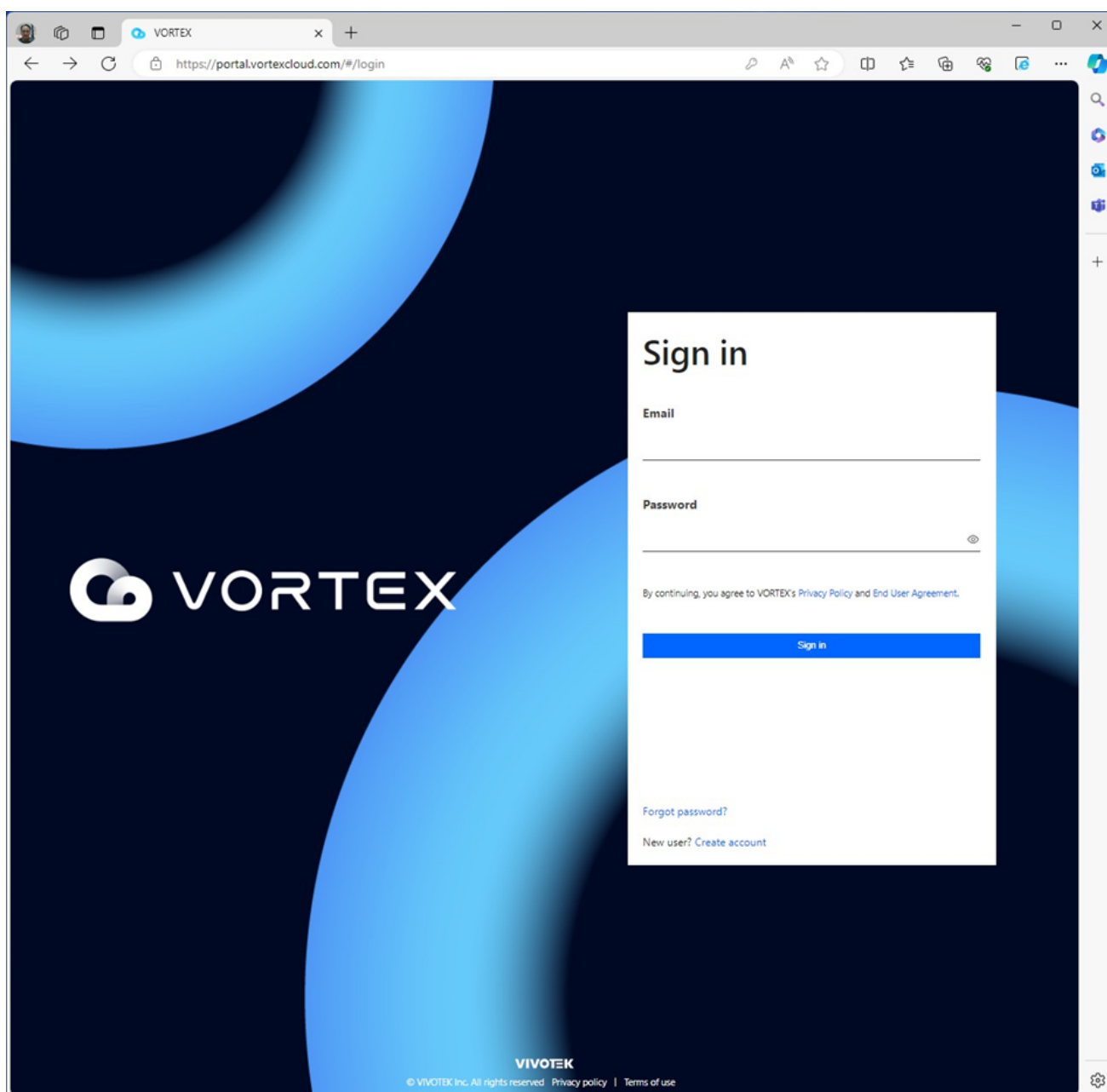


Establishing a VORTEX Service

The first time you use VORTEX, you, as a VORTEX service owner, must establish a VORTEX service. To do so, you can use one of the following two methods:

Creating a VORTEX Account & Adding Devices (Web Portal)

1. Visit <https://portal.vortexcloud.com/#/login> and click **Create account**.



2. Enter an email address and set up your password according to the requirements. Then, click **Create account**. The VORTEX system will send an activation email. In the email inbox, click **Verify Email**. The browser will display a confirmation message.

Welcome to VIVOTEK Vortex Inbox x

no-reply@vortexcloud.com

to ▼

Please activate your VORTEX account by clicking on [Verify Email](#) within 24 hours after signing up. Once your account is activated, you'll be able to start enjoying VORTEX service. If you did not create a VORTEX account, please ignore this email.

Regards,
VIVOTEK VORTEX Team



3. Return to the VORTEX sign-in page, enter your email address and password and then click **Sign in**.
4. Because you are new to VORTEX and you do not belong to any organization, a message will appear asking you to **create an organization** (service).
5. Enter your organization name, select a region, select an organization type (paid or free), and then click **Next**.

Create your organization in VORTEX

Enter your organization name

Select type of organization

Paid

Advanced video surveillance solution supporting all VORTEX cameras and VORTEX Connect Pro. Comprehensive features for AI applications and management functions.

Free

Basic video surveillance solution for VORTEX Connect. Limited to essential features and excludes VORTEX camera support.

Select your data storage location

Choose where videos and images will be stored. This setting cannot be changed after the organization is created.

Next

6. Review the information you entered. Note that once you select a region and click **Create**, you cannot change the region later.
7. Start adding devices to your organization by entering the Device ID (MAC address) and other required information.

Add a device

✕

1. Enter the device ID

Enter the device ID to add the device to your organization. You can find a 12-digit code right below the QR Code on the device ID label on your device.



Device ID

2. Edit your device

Assign your device to a device group, name your device, and set up a time zone for your device based on its location. These configurations can also be made later in the device settings.

☐ Retain the original settings on the device

Device group

📁 Ungrouped Cameras

Device name

Device 1

Time zone

America/Los_Angeles (PST, GMT-8:00) ▼

Add

Creating a VORTEX Account & Adding Devices (Mobile App)

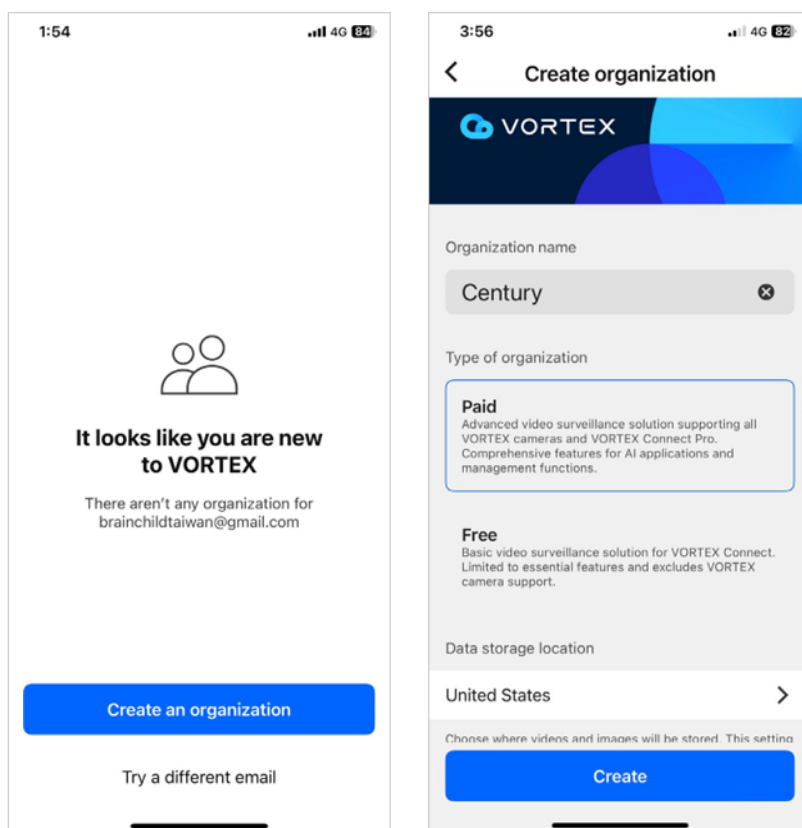
1. Install VORTEX from App Store or Google Play by scanning one of the following QR codes via your mobile device.



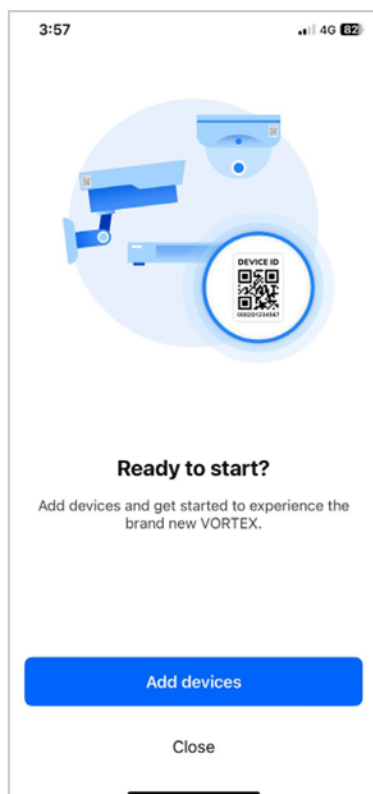
2. Tap **Create account**, enter the email address and password of the organization owner, and then tap **Create account**.

The image displays two screenshots of the VORTEX mobile application. The left screenshot shows the main login screen with the VORTEX logo at the top. Below the logo are input fields for 'Email address' and 'Password', a 'Forgot password?' link, a 'Sign in' button, and a 'Create account' link at the bottom. The right screenshot shows the 'Create account' screen. It features the VORTEX logo and the title 'Create account'. There are input fields for 'Email' (containing 'an@gmail.com') and 'Password' (masked with dots). Below the password field is a list of password requirements: 8-64 characters with no space, at least one uppercase alphabetic character, at least one lowercase alphabetic character, and one numeric character. There is also a 'Confirm password' field. At the bottom, there is a 'Create account' button and a link to the Privacy Policy and End User Agreement.

3. The VORTEX system will send an activation email. In the email inbox, click **Verify Email**. A confirmation message will appear in the browser.
4. Return to the VORTEX app, enter the email address and password, and then sign in. Because you are new to VORTEX and do not belong to any organization, a message will appear asking you to create an organization (service).
5. Tap **Create** an organization and enter the organization details.



6. Note that once you select a region and tap **OK**, you cannot change the region later.
7. Tap **Add devices** as needed.



8. Once devices are added to your organization, you can view cameras on your mobile device.

NOTE

1. When using a mobile device to add devices to your organization, you can scan a device QR code instead of entering its device ID.
2. A device ID can also be found on a VIVOTEK NVR. See the next section for details.
3. In addition to scanning a QR code, you can manually enter a MAC address to add a device.
4. You can add devices at any time by tapping the organization icon > **+ Add Devices** in the upper-left corner of the mobile app.
5. If you press the reset button on a camera in an organization, the camera will be removed from the organization. All camera data (SD card / cloud videos) will also be removed.



Example of a device ID on a VIVOTEK packaging box



Example of a device ID on a VIVOTEK camera

Adding a VIVOTEK NVR Device

Before adding an NVR to your VORTEX account, ensure that the VORTEX Connect service is enabled on the NVR. You can enable it from the Cloud Service page on either the NVR web interface or local interface. Follow the steps below:

1. Log in to the NVR web interface or local interface.
2. Go to **System > Cloud Service**, and locate the **VORTEX Connect** service.
3. Enable the **VORTEX Connect** service. The information required for adding the device will then be displayed below.
4. Add the NVR through the VORTEX portal or VORTEX app:
 - **Portal:** Follow the steps in [Creating a VORTEX Account and Adding Devices \(Web Portal\)](#).
 - **App:** Follow the steps in [Creating a VORTEX Account and Adding Devices \(Mobile App\)](#).
5. On the device setup page, there is an option to use the same settings as the NVR. When this option is **enabled** (recommended if the basic settings have already been configured on the NVR):
 - **Device Name:** No field is displayed. The NVR name is used directly.
 - **Device Group:** Ungrouped Cameras is used as the default device group. You can also assign the device to an existing group or create a new group.
 - **Time Zone:** No field is displayed. The NVR time zone is used directly.

When this option is disabled:

- **Device Name:** The NVR name is editable. The default name is "NVR + number" (from 1 to 99).
 - **Device Group:** Ungrouped Cameras is used as the default device group. You can select an existing group or create a new one.
 - **Time Zone:** Uses the time zone configured in VORTEX.
6. Once you finish the initial configuration, click **Add** to add the NVR to your account. All devices connected to the NVR will then be displayed.

Adding a VIVOTEK VSS

[**xLite** only]

Before adding a VSS to your VORTEX account, ensure that the VORTEX Connect service is enabled in the VSS client. Follow the steps below:

1. Go to the **Settings > VORTEX Connect**, and enable VORTEX Connect in your VSS.
2. Confirm that the **Cloud connection status** shows **Connected**. A unique **Device ID** will be generated when your VSS is successfully linked to the VORTEX platform.
3. If the **Cloud connection status** shows **Disconnected**, check your network connection. An active internet connection is required to use this feature.

You can add your VSS to a VORTEX Organization using either of the following methods:

From the VORTEX Portal

1. Go to the **Devices** page and select **Add Device**.
2. Enter the **Device ID** shown on the VSS VORTEX Connect page

From the VORTEX Mobile App

1. Select **Add Device**.
2. Use the QR code scanner to scan the QR code displayed on the VSS VORTEX Connect page.

After adding your VSS to a VORTEX Organization:

1. In the VORTEX Portal or App, check that your VSS appears in the **Devices** Tab.
2. In your VSS VORTEX Connect screen, confirm that the **Organization binding status** shows **Bound**.

NOTE

1. Currently, only standalone VSS servers are supported by VORTEX Connect. If the VSS is configured as a CMS with substations, the substations will not be displayed in VORTEX.
2. Currently, VSS can only be added to a free organization (xLite).

Joining a VORTEX Service

You can join a VORTEX service by directly creating an account via the web portal or the app. Also, a VORTEX organization owner can invite you as a VORTEX service user.

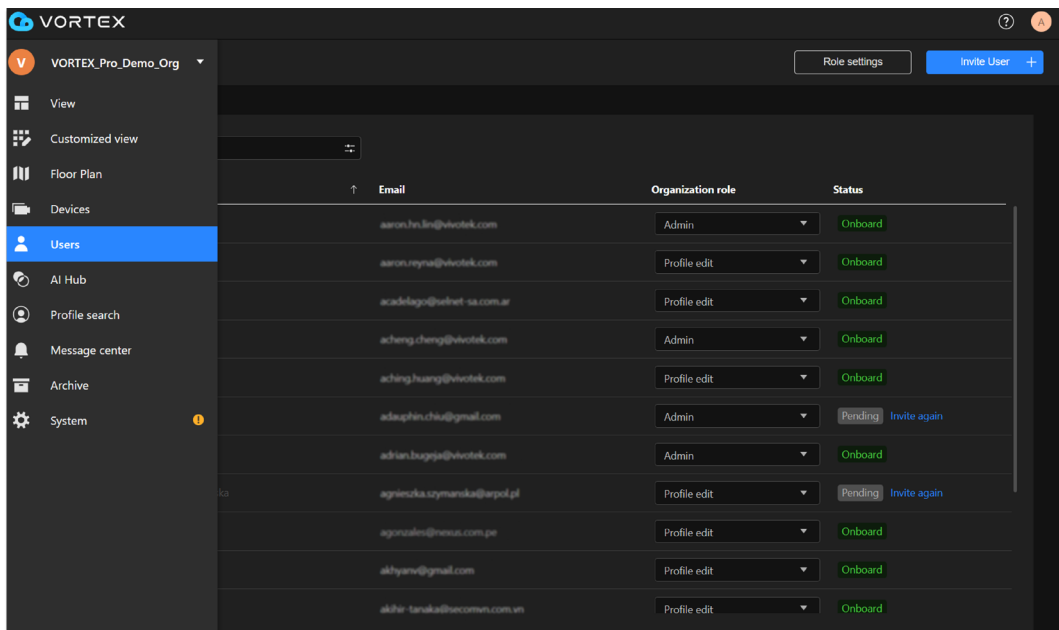
Adding a VORTEX Account via the Web Portal

1. Visit <https://portal.vortexcloud.com/#/login> and click **Create account**.
2. Follow the remaining steps as described previously for the web portal.

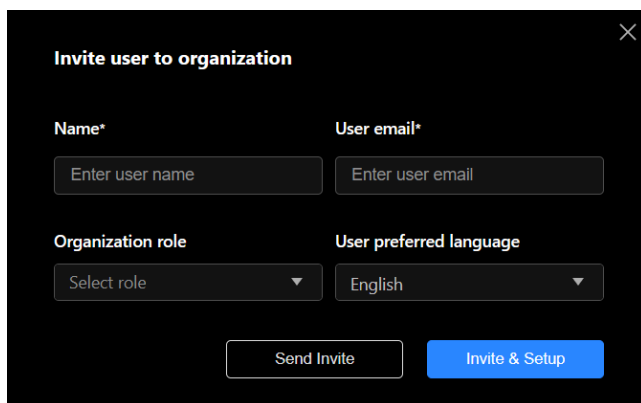
Adding a VORTEX Account by Invitation

If you are the owner of a VORTEX organization, you can invite users to join your organization with the user privileges you specify. Note that user management is not available in the mobile app; therefore, users cannot be invited through the mobile app.

1. Go to **Users** and click **Invite User**.



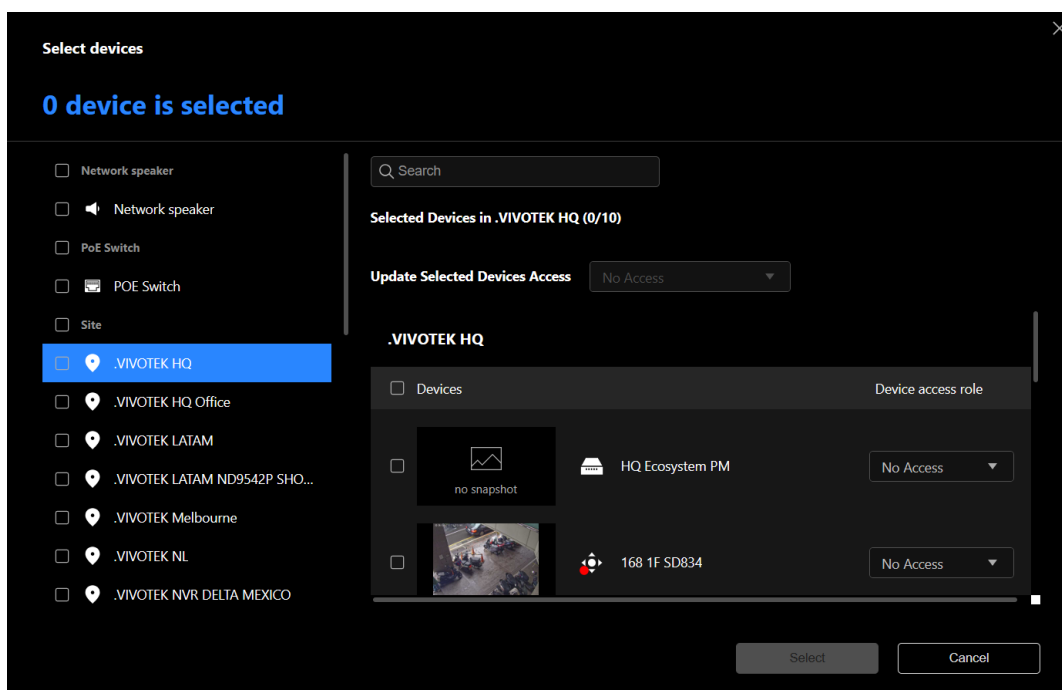
2. Enter the user's name and email address, choose the organization role and preferred language, and then click **Invite & Setup**.



The dialog box titled "Invite user to organization" contains the following fields and buttons:

- Name***: Input field with placeholder "Enter user name".
- User email***: Input field with placeholder "Enter user email".
- Organization role**: Dropdown menu with "Select role" as the current selection.
- User preferred language**: Dropdown menu with "English" as the current selection.
- Buttons**: "Send Invite" and "Invite & Setup".

3. Select the devices to which the user should have access, assign the appropriate device access role for each device, and then click **Select**.



The "Select devices" dialog box shows the following components:

- Header**: "Select devices" and "0 device is selected".
- Left Panel**: A list of categories and sites with checkboxes:
 - Network speaker
 - Network speaker
 - PoE Switch
 - POE Switch
 - Site
 - .VIVOTEK HQ** (highlighted)
 - .VIVOTEK HQ Office
 - .VIVOTEK LATAM
 - .VIVOTEK LATAM ND9542P SHO...
 - .VIVOTEK Melbourne
 - .VIVOTEK NL
 - .VIVOTEK NVR DELTA MEXICO
- Search**: A search bar with the placeholder "Search".
- Selected Devices in .VIVOTEK HQ (0/10)**: A section with an "Update Selected Devices Access" dropdown set to "No Access".
- .VIVOTEK HQ**: A table of devices with checkboxes and access roles.

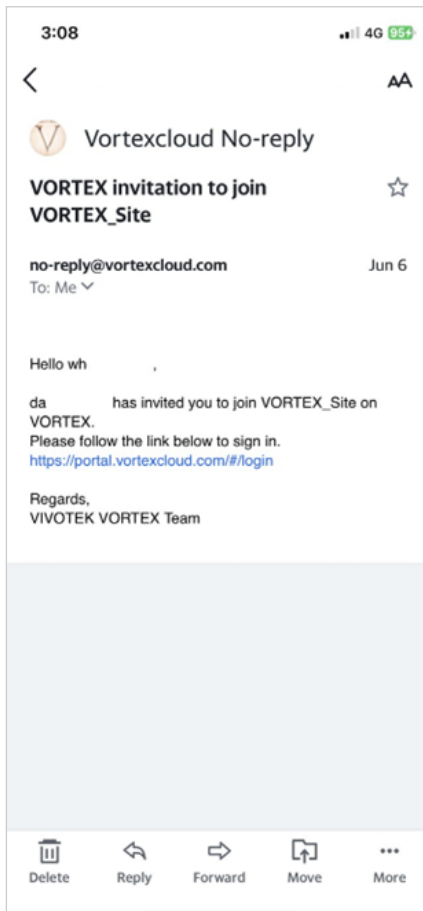
Devices	Device access role
☐  no snapshot	☐ HQ Ecosystem PM No Access
☐  168 1F SD834	☐ 168 1F SD834 No Access
- Buttons**: "Select" and "Cancel".

The table below shows the user type and their access level in VORTEX. You can refer to this table to set up user type and user access right.

Role	Management Access Level	Device Group Access Level	Feature Access Level
Owner 	Organizational group / device / user	Full access	SI Management transfer/delete organization Full access
Admin 	group / device / user	Full access	Full access
Supervisor 	device	Assigned only	Limited access
Viewer 	X	Assigned only	View only

- **Owner:** This role has full access to all settings, including all organization and user creation, management, and overall system configuration.
- **Admin:** While this role also has full access to settings, user management, and system configuration, Admin cannot delete an entire organization.
- **Supervisor:** This role has limited access to device configuration, as set by higher roles. It does not have control over groups or users.
- **Viewer:** This role can only view devices that have been granted access by higher roles, such as the Admin and Owner.

4. Meanwhile, the recipient of the email should receive an invitation email like below. Simply click the link and sign in VORTEX.

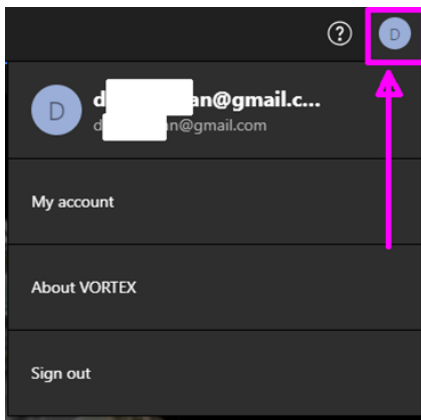


Managing Your Account

Click the personal icon in the upper-right corner of the VORTEX portal to open the account menu. The menu displays the account name, email address, and the following options:

- My Account
- About VORTEX
- Sign Out

The profile icon displays the first letter of the account name.



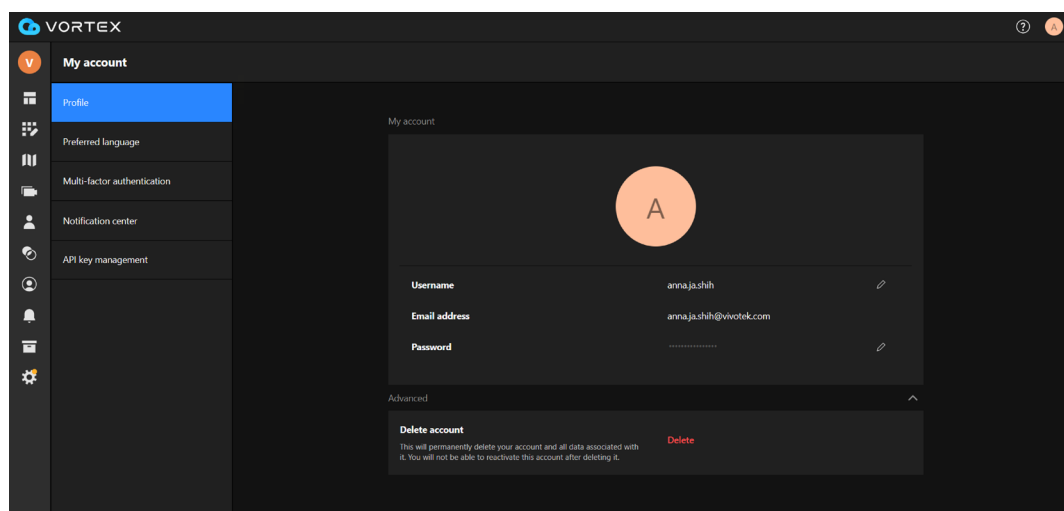
My Account

Select **My Account** to manage account-related settings.

Profile

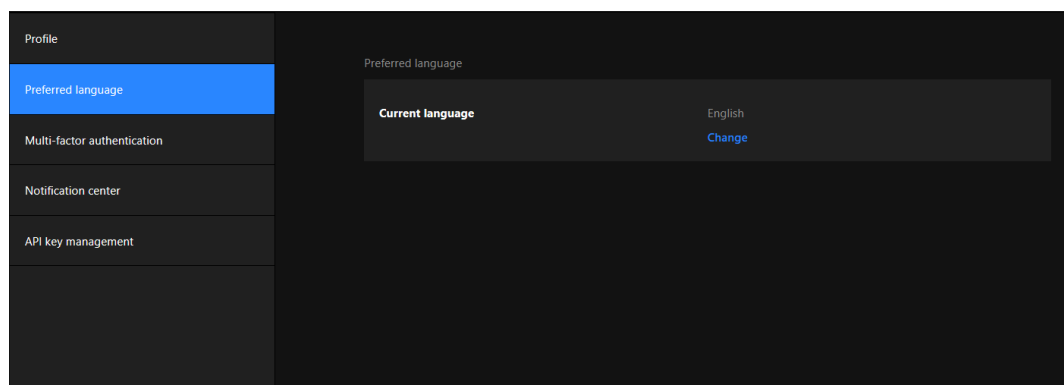
The **Profile** page displays the account information, including the username, email address, and password. Users can:

- Edit the username.
- Change the account password.
- View the registered email address.



Preferred Language

The Preferred Language page allows users to change the display language of the VORTEX portal.



Multi-Factor Authentication (MFA)

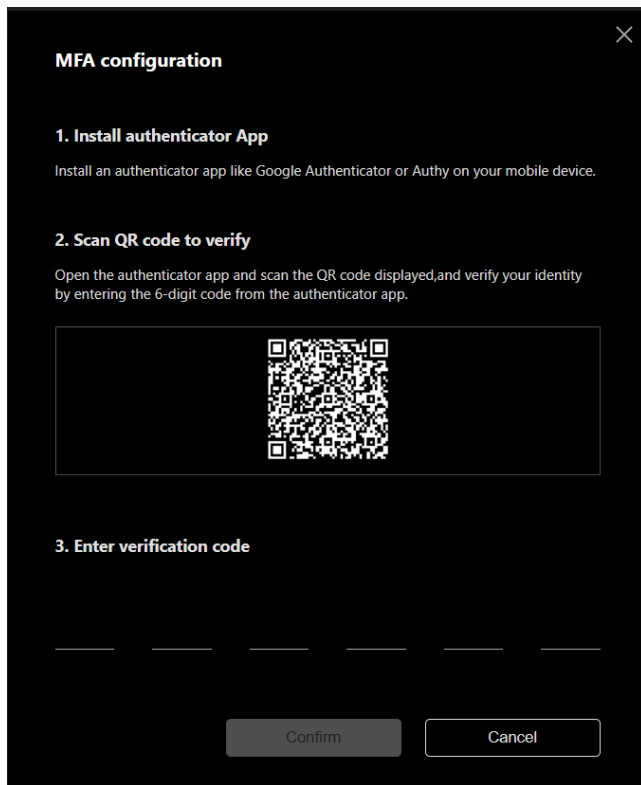
The Multi-factor Authentication page allows users to configure MFA for enhanced account security.

[xStd and xPro only]

VORTEX supports MFA through authenticator applications such as Google Authenticator and Microsoft Authenticator. These applications generate time-based one-time passwords (TOTP). After MFA is enabled, users must enter both their VORTEX account credentials and a one-time verification code when signing in.

Configuring MFA on the VORTEX Portal

1. Install an authenticator application, such as Google Authenticator or Microsoft Authenticator, on a mobile device.
2. Enter the VORTEX account password.
3. An MFA configuration dialog box containing a QR code is displayed.



MFA configuration [Close icon]

1. Install authenticator App
Install an authenticator app like Google Authenticator or Authy on your mobile device.

2. Scan QR code to verify
Open the authenticator app and scan the QR code displayed, and verify your identity by entering the 6-digit code from the authenticator app.



3. Enter verification code

Confirm

Cancel

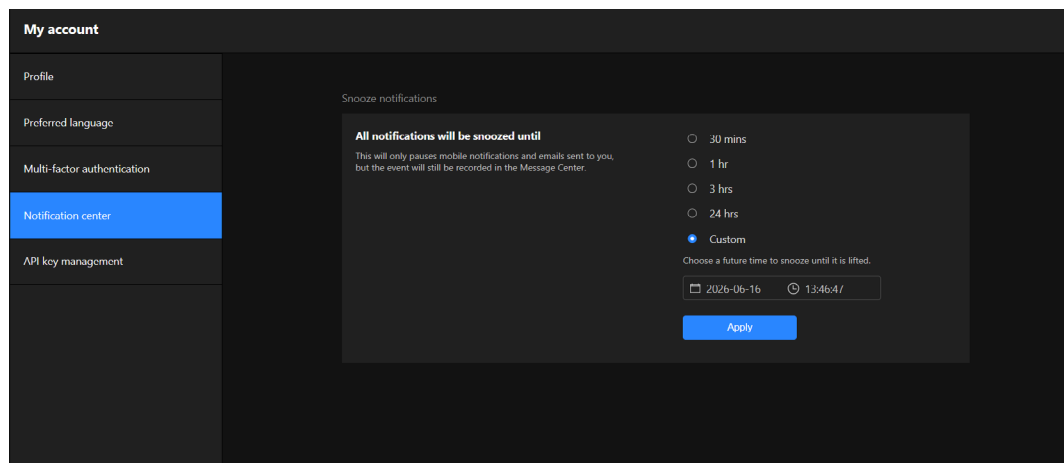
4. Use the authenticator application on the mobile device to scan the QR code.
5. A 6-digit verification code is generated.
6. Enter the verification code in the MFA configuration dialog box and click Confirm.

Configuring MFA on the VORTEX App

1. Open the side menu and select **My Account**.
2. Enable **Set Up MFA**.
3. Enter the VORTEX account password.
4. The MFA configuration dialog box displays the account name and setup key. Enter the account name and setup key into the authenticator application on the mobile device.
5. A 6-digit verification code is generated.
6. Enter the verification code in the MFA configuration dialog box and tap **Confirm**.

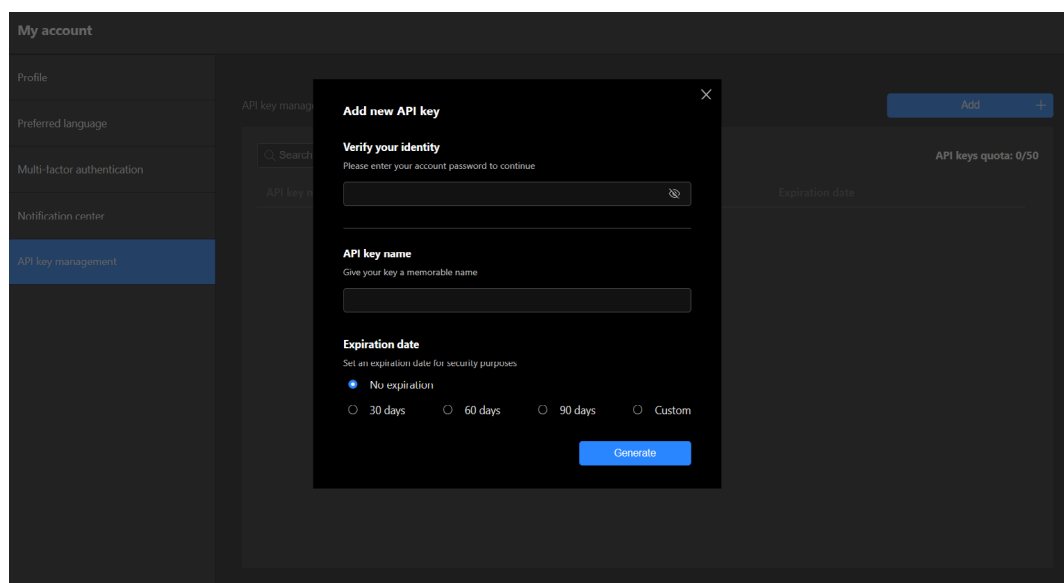
Notification Center

The Notification Center page allows users to manage notification-related settings.



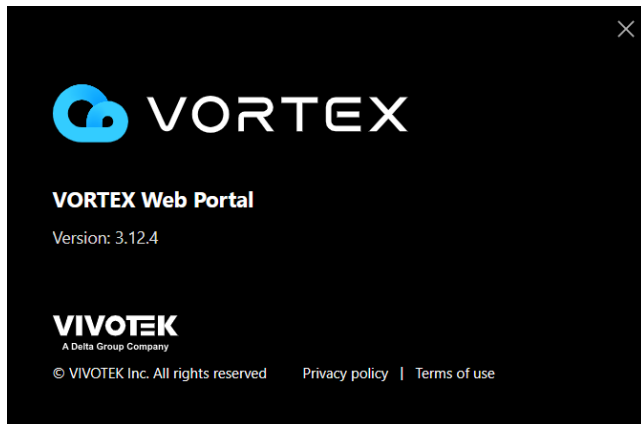
API Key Management

The API Key Management page allows users to create and manage API keys for API access and third-party integrations.



About VORTEX

Select **About VORTEX** to view legal information and software details, including the Privacy Policy, Terms of Use, and software version information.



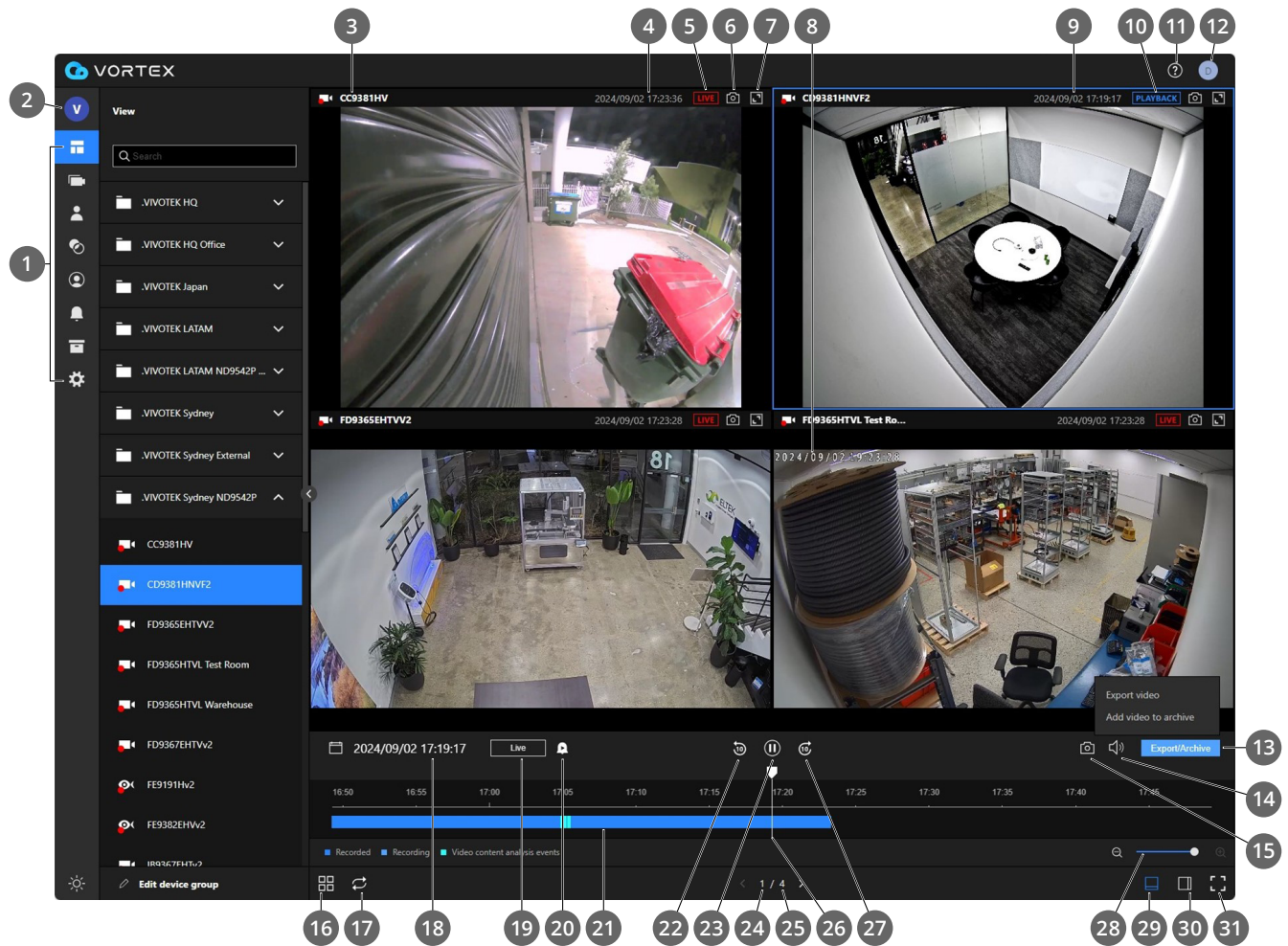
Sign Out

Select **Sign Out** to log out of the VORTEX portal.

View

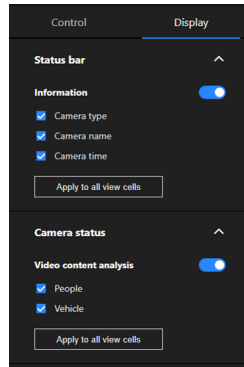
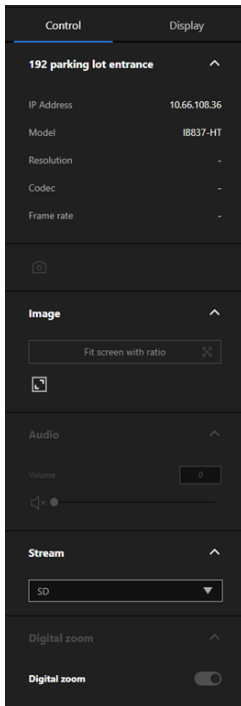
7

The VORTEX live view feature provides real-time access to all connected cameras. Simply click a designated group to view live footage from your cameras.



- 1 **Side menu:** Provides various tool options.
- 2 **Organization name:** Shows the current organization in use.
- 3 **Video title:** Shows the video title name.
- 4 **Timestamp:** Shows the current local time based on your system.
- 5 **LIVE:** Shows the current real-time footage streaming from the camera.
- 6 **Snapshot:** Captures a still image of the current video frame and saves as a photo.
- 7 **Toggle view:** Toggles between a single cell view and a full cell view.
- 8 **Date & time overlay:** Shows the current date and time based on the camera.
- 9 **Show the timestamp.**

- 10 **Video status:** Shows the status of video stream, such as Live View or Playback.
- 11 **Help:** Connects to online tutorials and FAQs or sends feedback/comments to the VORTEX development team.
- 12 **Account settings:** Change password, delete account, or display privacy policy and terms of use.
- 13 **Export / Archive:** The “Archive” feature is handy for important events. You can save a specific video duration directly to the cloud archive with a simple click. Note that the Export function is available only when using an NVR.
- 14 **Volume control:** Adjust the audio volume. Note that this feature requires the audio input for camera.
- 15 **Take a snapshot.**
- 16 **View cell layout:** Changes how video cells are arranged on a screen.
- 17 **Toggle carousel view:** Turns on/off showing video cell views in turn.
- 18 **Time picker:** Shows the timestamp of a recorded video segment.
- 19 **Live (in white):** Returns to the current live view.
- 20 **Show event only:** Shows events only on the timeline.
- 21 **Playback timeline:** Displays the timeline of recorded video segments. Drag the timeline to navigate to a specific playback time.
NOTE: For xLite, timeline thumbnails are updated every 5 minutes. For xStd and xPro, timeline thumbnails are updated every 30 seconds.
- 22 **Fast rewind:** Jumps back 10 seconds.
- 23 **Play/Pause:** Plays or Pauses a video playback.
- 24 **Move to the previous page under the current layout.**
- 25 **Move to the next page under the current layout.**
- 26 **Play:** Indicates the current playback position on the timeline.
- 27 **Fast forward:** Jumps back 10 seconds.
- 28 **Timeline zoom-in/out.**
- 29 **Show/Hide timeline panel.**
- 30 **Show/Hide control panel** (Control panel and display panel are shown below).
- 31 **Fullscreen** (press Esc to exit).

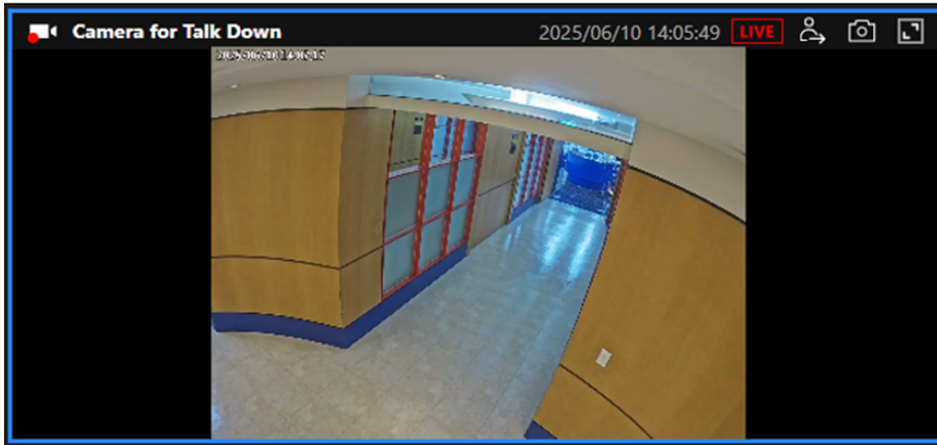


- **Control panel:** shows network connection info and model name. You can also control image ratio, audio volume, stream quality and digital zoom (if available).
- **Display panel:** lets you decide how you want to display the information on camera type, name, and time. You can also decide if to turn on video content analysis.

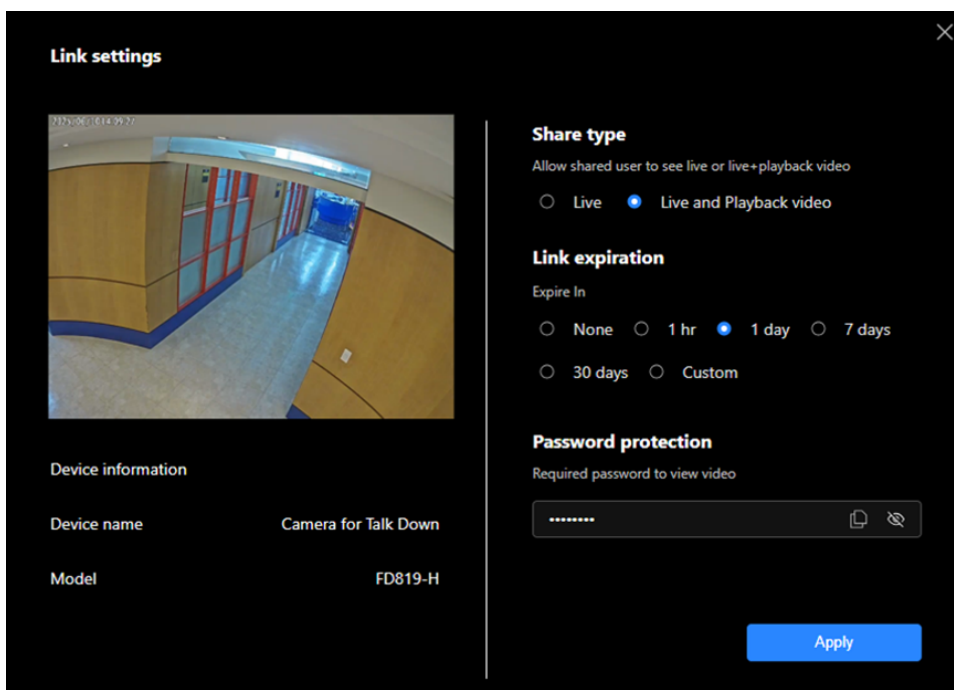
Sharing Device Live View and Playback

You can create a share link to allow external parties (e.g., police) to access live streams or playback footage from selected cameras. This is useful for sharing key areas or critical moments without requiring login access. Follow the steps below to share a device.

1. Click the device sharing icon  on the view cell of the camera you want to share. This will open the link settings page.

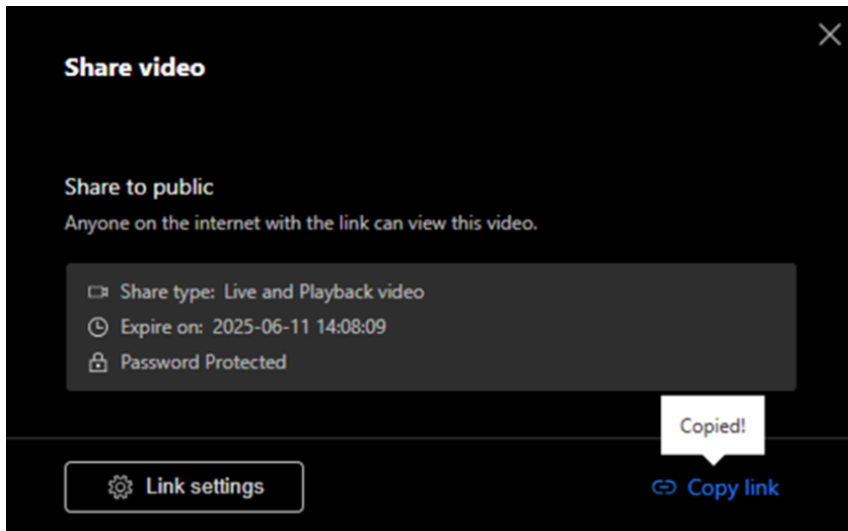


2. Set up the share link settings and click apply to generate the link.



- **Share Type**
Live: Share only the live stream of the camera.
Live and Playback: Share both the live stream and past video footage.
- **Link Expiration:** Sets the expiration period for the shared link.
- **Password Protection (mandatory):** Sets password for the shared link to control access.

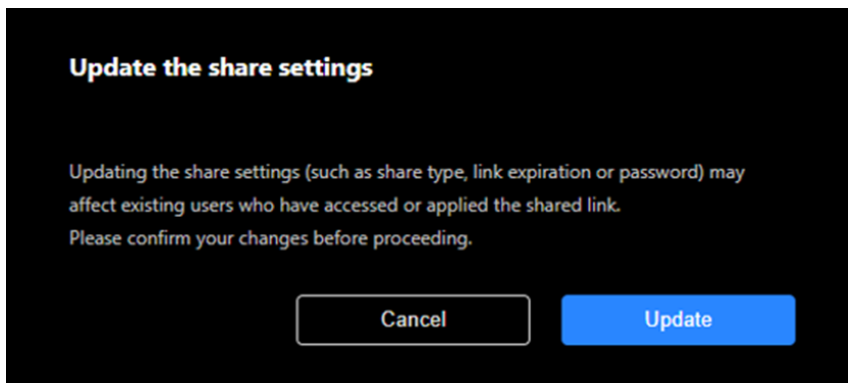
3. The shared link information will be displayed. Click Copy link to copy the URL and share with the external parties.



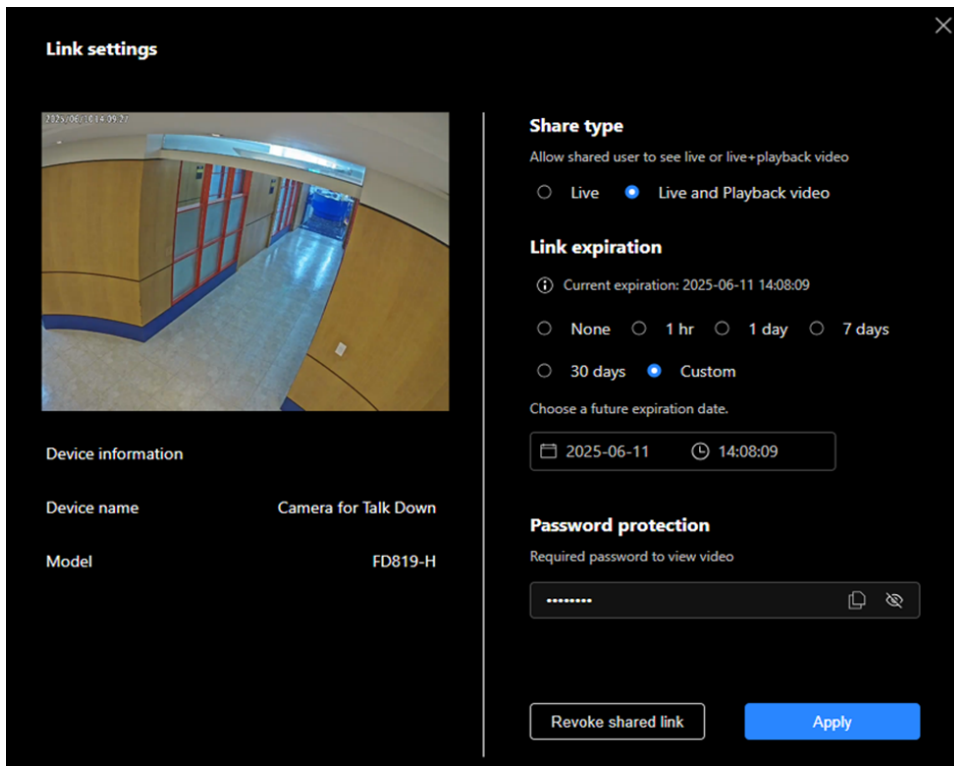
4. External users can open the link in a web browser such as Chrome or Edge. Mobile users can also access it using browsers like Safari on iOS or Chrome on Android.

5. A camera with an active shared link will display a blue mark on its view cell.

6. You can click **device sharing icon**  to view current sharing details or update the link settings. Please note updating the link settings will affect current viewers, so please confirm any changes before proceeding.



7. You can revoke the shared link at any time, even before it expires. To do so, go to the link settings and click **Revoke shared link** to disable it.

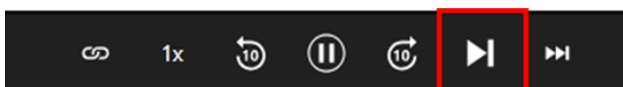


Frame by Frame Playback

This feature helps users review footage frame by frame (in forward direction only), enabling precise inspection of visual details and event timing to improve video analysis efficiency.

Below shows the steps to use it:

1. When a scene of interest is found during playback, pause the video first and then click Frame by Frame button to enter Frame by Frame mode. (You can also directly click the Frame by Frame button without pausing first)



2. Click the Frame by Frame button repeatedly to move forward one frame at a time.
3. Alternatively, you can use the hotkeys to move to the next frame.

Action	Windows	mac OS
Move to the next frame	Ctrl + →	Cmd + →

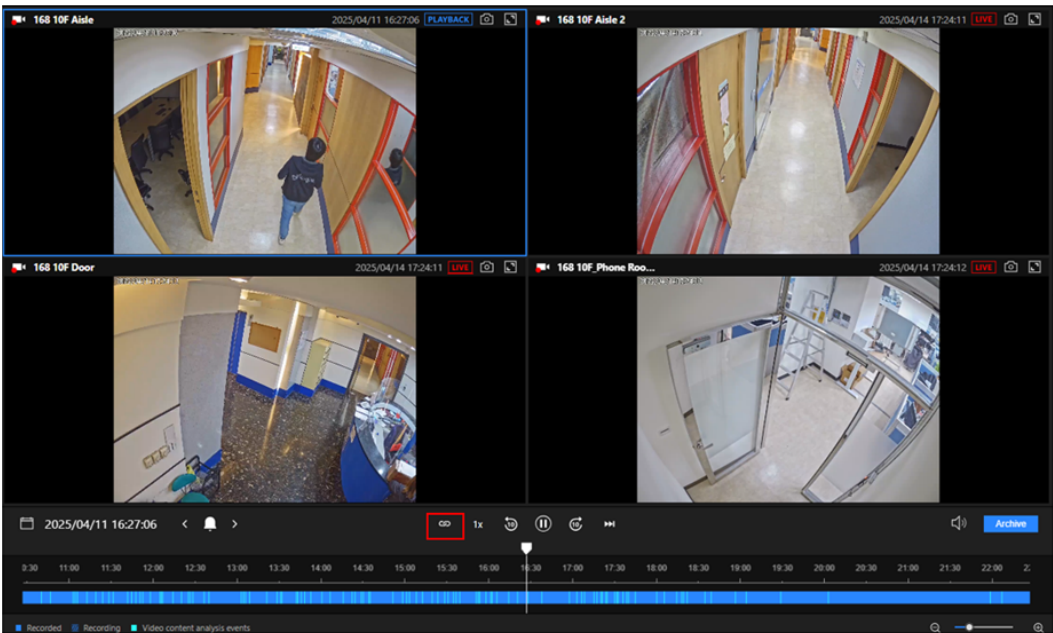
Notes

1. The frame by frame feature is only available for the camera in the focused view cell.
2. This feature is not supported in Event Only mode.

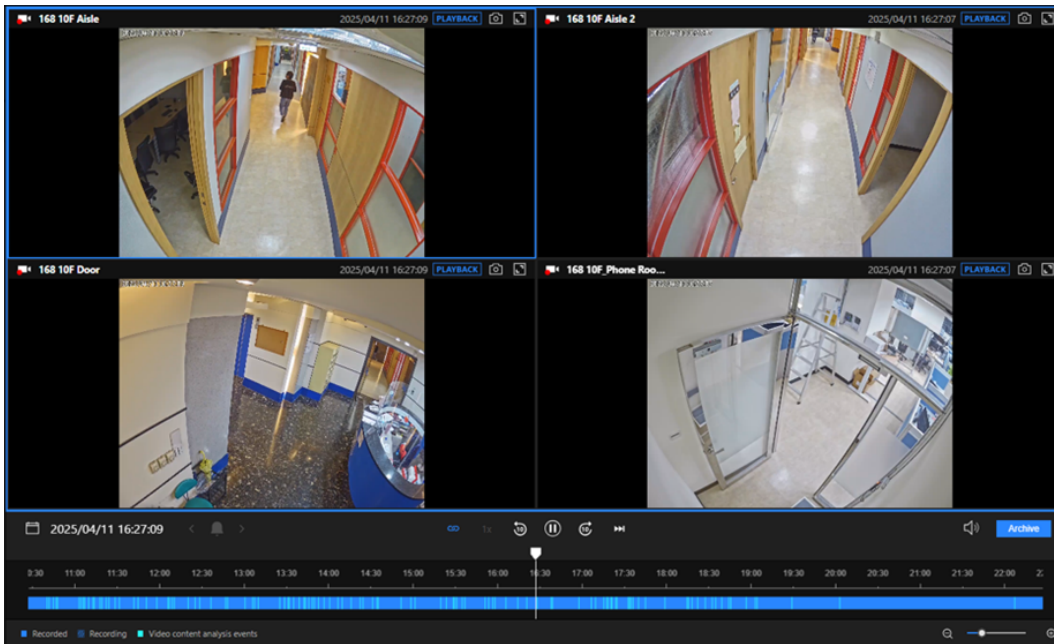
Synchronized playback

Synchronized playback supports up to four cameras playing recordings simultaneously in the same view, helping users quickly grasp the full view of an event.

1. Focus on a single camera view cell in the playback mode, you can then enable synchronized playback.
2. Click the Synchronized Playback icon (🔗)



3. All cameras in the view(up to 4) will begin playback from the same point in time.



4. Drag the timeline or adjust the date time picker to navigate to a different time in the recordings.
5. To exit synchronized playback, click the **Synchronized Playback** icon again or **Jump to live** icon (⏮)

NOTE

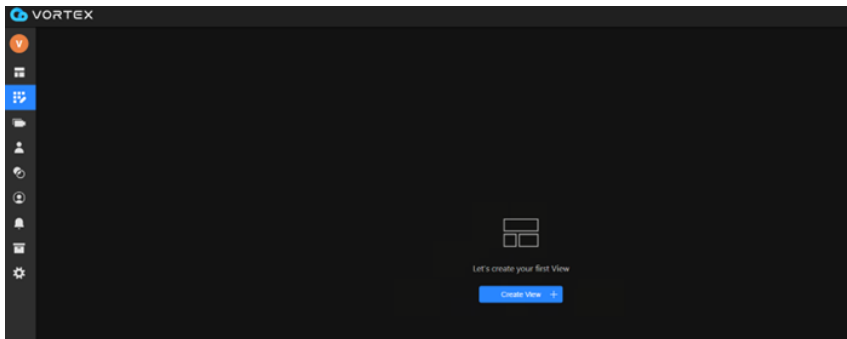
1. Synchronized playback supports only the following view layouts: 2x2, 1P+3, and 3V.
2. If a camera experiences a delay, the other ready cameras will still start synchronized playback. Once the delayed camera is ready, it will begin playing from the original start time rather than catching up to the current time of the others. You can adjust the timeline to restart synchronized playback if needed.

Customized View

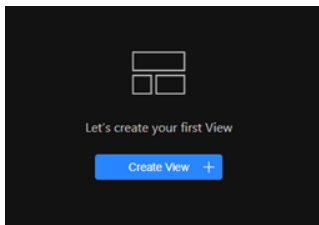
Customized view is a feature for users to create personalized views by grouping cameras from different sites into a single view page. Therefore, users can conveniently monitor live or playback footage from multiple camera groups on one unified page.

Create a Customized View

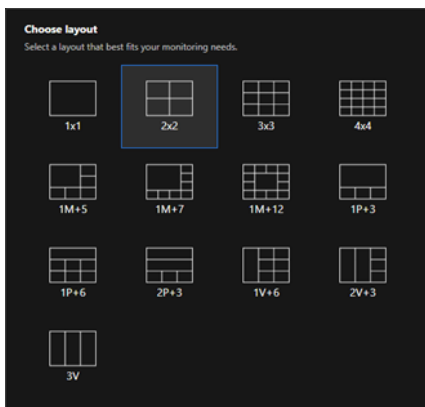
1. Click the Customized View icon,  on the side menu.



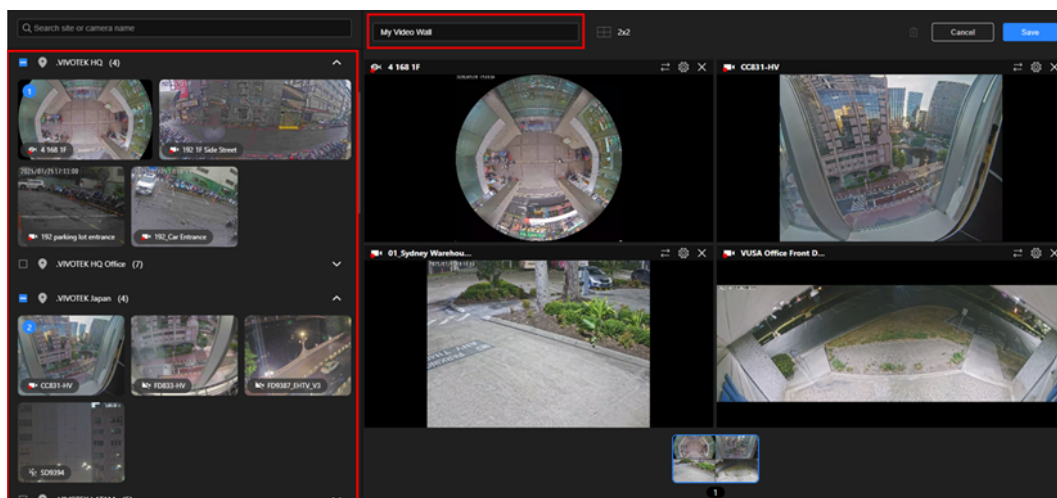
2. Click Create View to start creating a new customized view.



3. Name your customized view and select view layout icon  to choose your preferred layout.

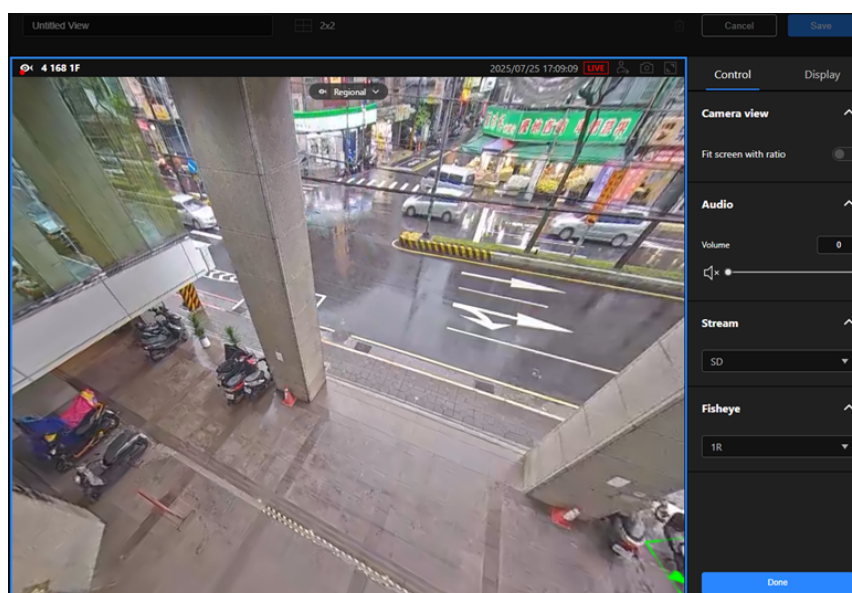


4. Select cameras from the left panel. Once selected, the cameras will be added to your customized view shown on the right panel immediately. You can also move the positions of the cameras on your customized view by clicking .

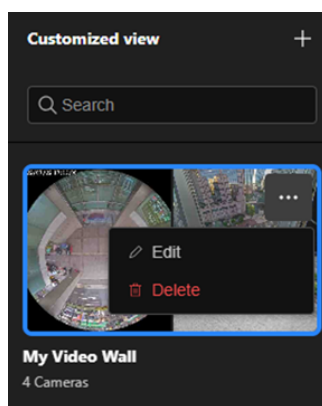


5. You can configure the preference of control and display by click setting icon  on each view cell. The available options include:

- Fit screen with ratio
- Audio volume
- Stream (SD, HD)
- Fisheye dewarp (for fisheye camera only)
- Zoom in/ out



6. Once you finish the configuration, click **Save**. The customized view is created and reflects the selected layout and camera positions. In addition, the preferences configured for each view cell are displayed when the view cell is selected.
7. To edit a customized view, click the **More** icon of the selected view in the view list.



8. Note that configuration changes are saved only when they are made in **Edit Mode**. In addition, the saved fisheye dewarping mode and zoom level are applied only to the selected view cell in the user portal.

Setup Carousel View

Customized views support selectable time intervals for carousel view, allowing you to control how long each page remains visible during rotation. In addition, you can pause the carousel at any time during monitoring.

1. Click **Play**  on the toolbar to start the carousel view for each page within the current customized view.
2. Expand the time options to choose how long each page stays visible. Available options: 15 seconds, 30 seconds, 1 minute, and 3 minutes.
3. Click Pause to stop the carousel view. You can resume it by clicking **Play**.

Copy and Send Customized View

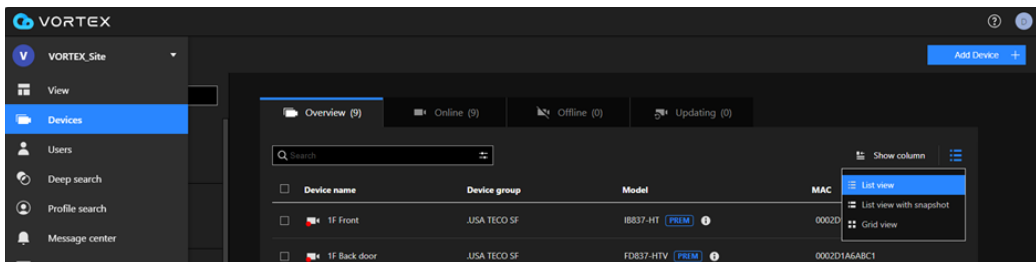
You can copy your customized view and share it with others in the same organization. The recipients can further personalize the received views to suit their individual preferences without affecting the original view created by you. This streamlines the setup process by eliminating the need for each user to manually recreate identical camera combinations.

To send a copy:

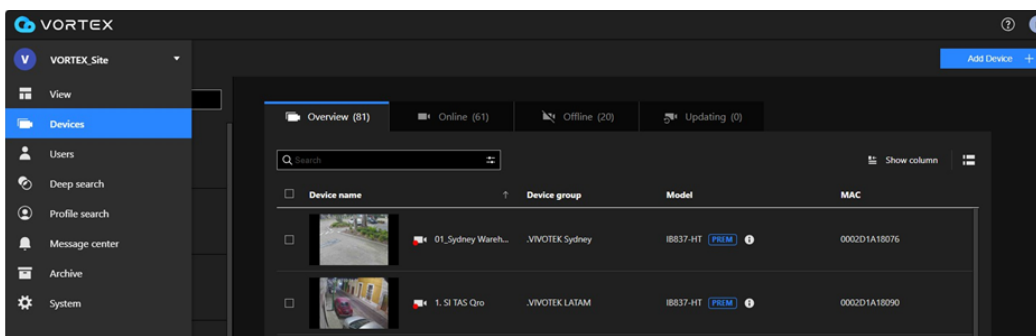
1. In the Customized View list, locate the view you want to share.
2. open the **More menu** and select **Send Copy**.
3. Select the users you want to share your customized view with.
4. The copied view will appear in the recipients' Customized View list. (Customized views shared via the portal will appear in the recipient's portal views, while views shared via the app will appear only in the recipient's app views.)
5. Recipients can then further adjust the view as needed, independently of your original settings.

Devices

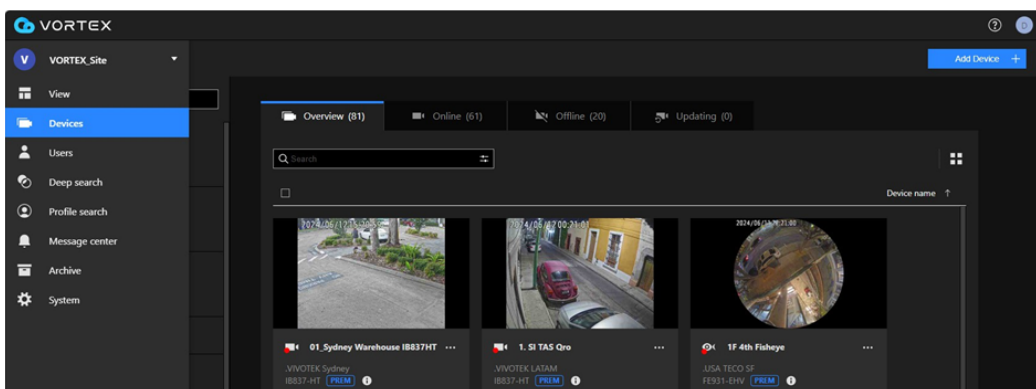
The VORTEX Devices pages show all available cameras, NVRs, and other devices used by an organization in List view, List view with snapshot, and Grid view. For each device, the device name, device group, model name, MAC address, and other settings can be found on this page.



List view



List view with snapshot



Grid view

When your mouse cursor is over the MAC address (or "... in the Grid view), you can find the following four options:

- Settings: Check settings like device name, group, time zone, reboot, or reset to default.
- Move to: Select to move to another group.
- Video content analysis: Shows video detection type results.
- Delete: removes the camera from the organization. This deletion will also remove all data / SD card / cloud videos associated with the deleted camera from the organization.

Device Settings

Click **Settings** to access device-specific configuration options.

Device Settings for VORTEX Cameras

- System: Device information, firmware update, remote support, and installation.
- Media: Image settings, image focus adjustment, privacy mask, audio settings and RTSP.
- Detection: Audio detection, tampering detection, video content analysis, license plate recognition and facial recognition.
- DI/DO: Digital input and output.
- Recording & Storage: Recording retention and cloud backup.

Device Settings for NVR Devices

- System: Device information, firmware update, remote support, and NVR settings.

Device Settings for Cameras Connected by NVR Devices

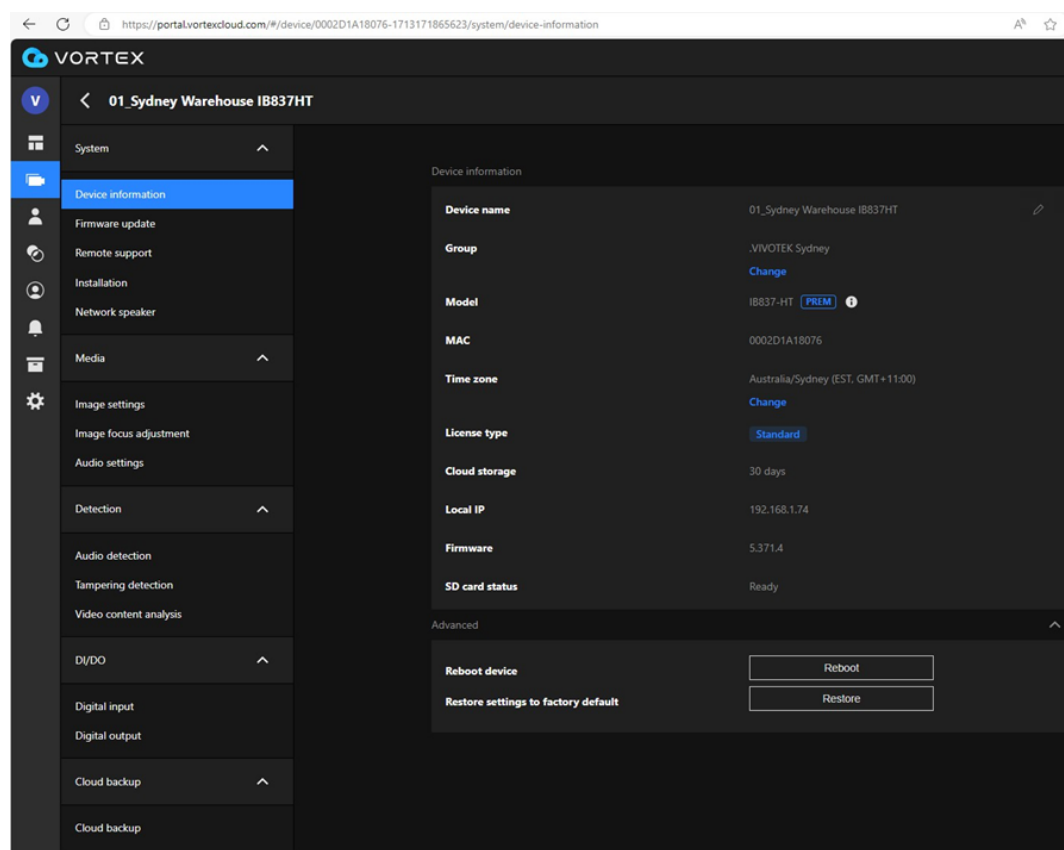
- System: Device information, firmware update, camera settings webpage.

System > Device Information

For Cameras

Displays basic camera information, including the device name, group, model, MAC address, time zone, license type, cloud storage status, local IP address, firmware version, and SD card status.

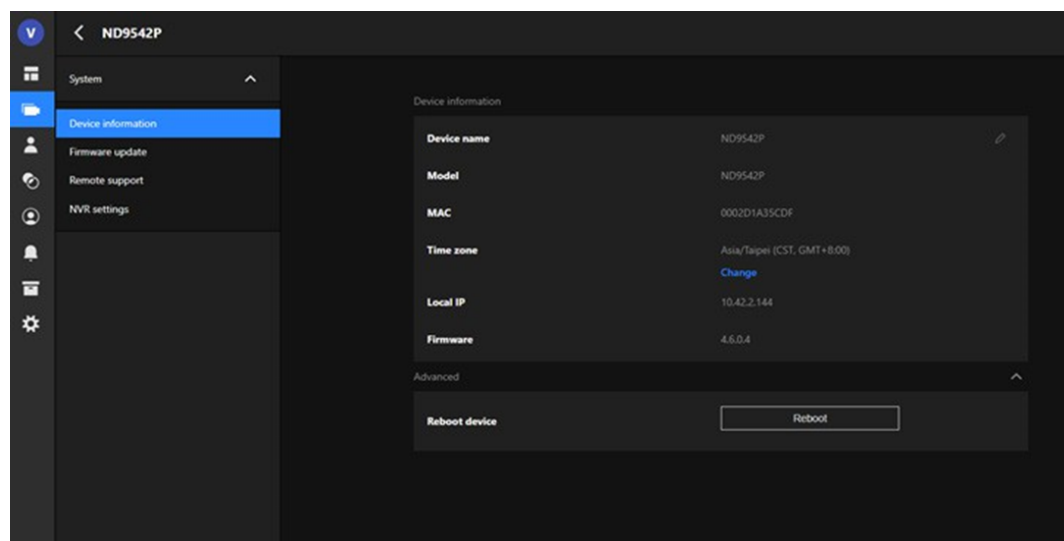
Users can also reboot the camera or restore it to factory default settings.



Device information

For NVR Devices and Bridges

Displays basic device information, including the device name, model, device ID, time zone, local IP address, and firmware version.



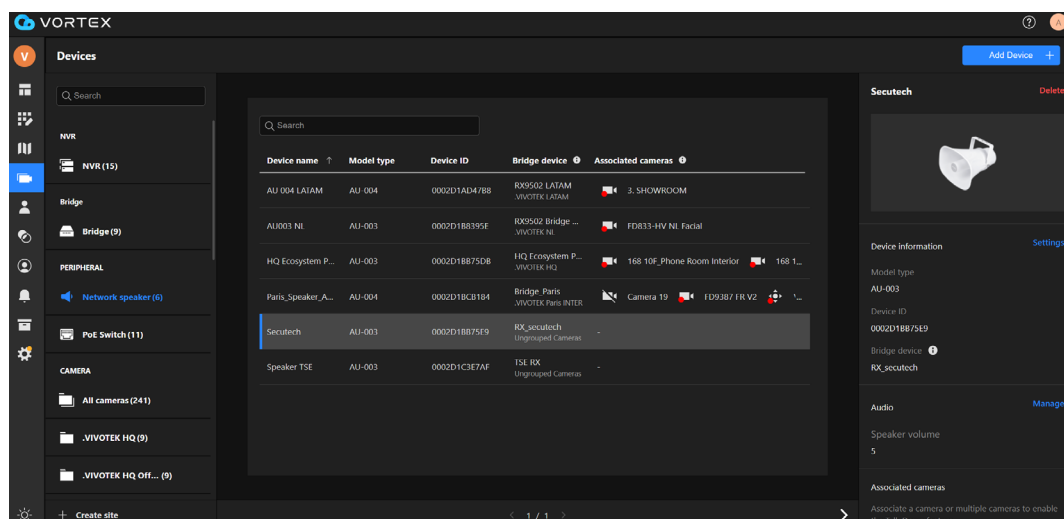
For VSS

Displays basic VSS information, including the device name, model, device ID, time zone, local IP address, and firmware version.

Users can also restart the VSS service.

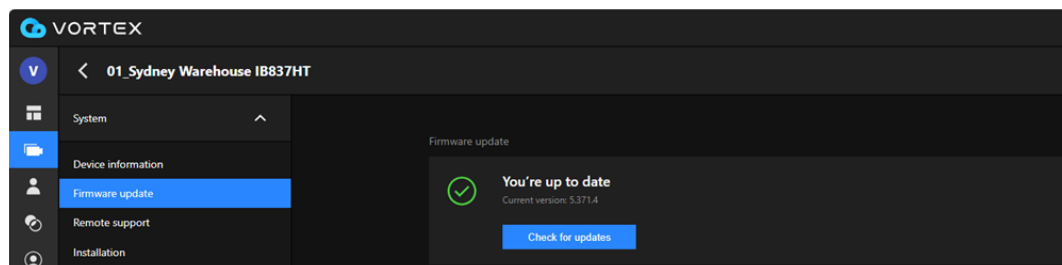
For Peripherals

Displays basic peripheral device information, including the device name, model type, device ID, bridge device, and associated cameras.



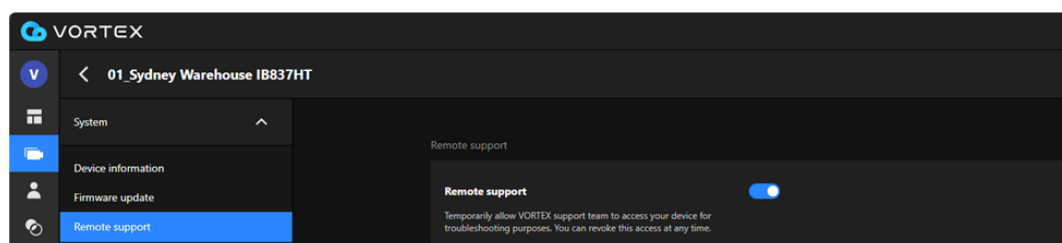
System > Firmware update for both VORTEX camera & VIVOTEK NVR

Shows the current firmware version. You can also check if there is firmware update here.



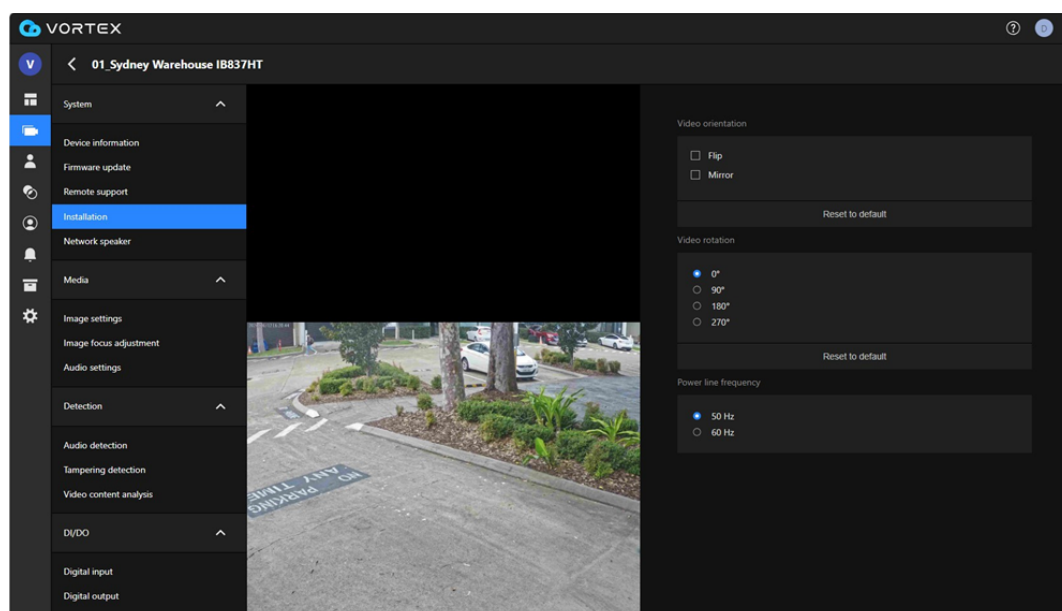
System > Remote support

Temporarily allows the VORTEX customer service to access your device for troubleshooting.



System > Installation

Depending on how your camera is installed, you can change the video orientation, rotation, and power line frequency here.



System > Network Speaker

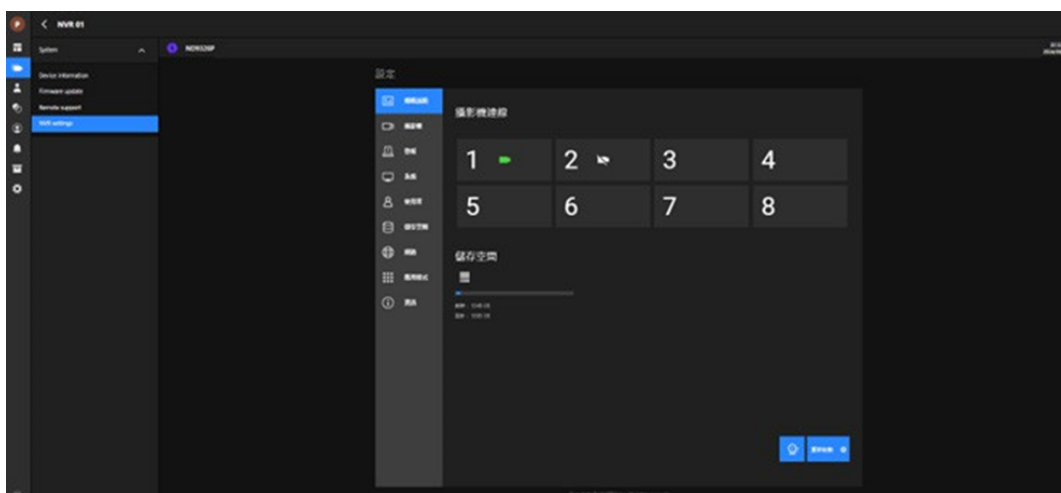
For Network Speakers Only

If your system comes with network speakers (with a pre-recorded audio track to warn intruders if a specific event happens), you can install them here.

System > NVR Settings

For NVR Only

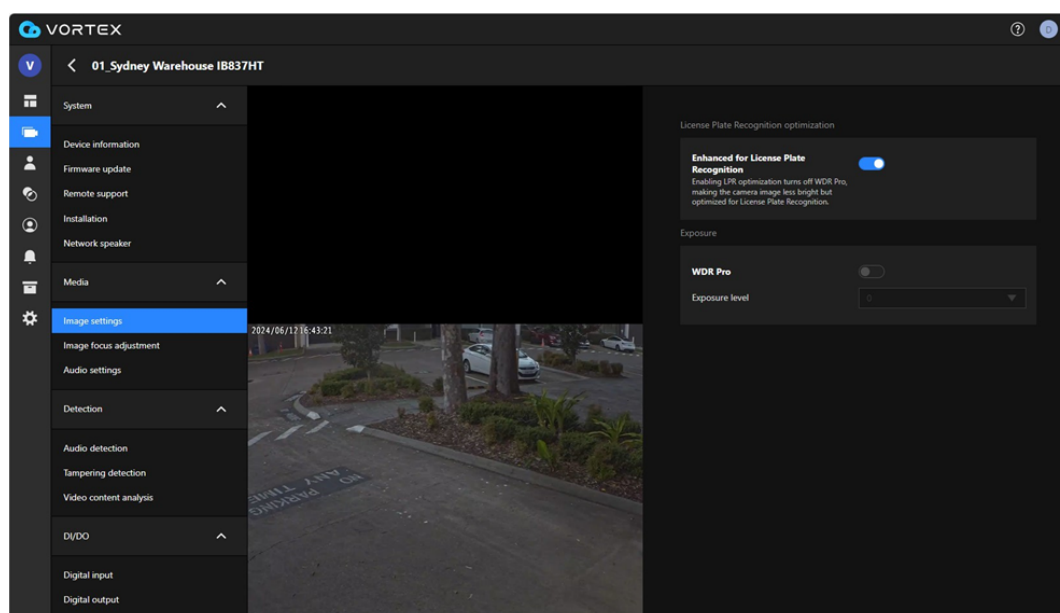
Allow the user to open an embedded page to configure NVR settings.



Media > Image Settings

For VORTEX Cameras Only

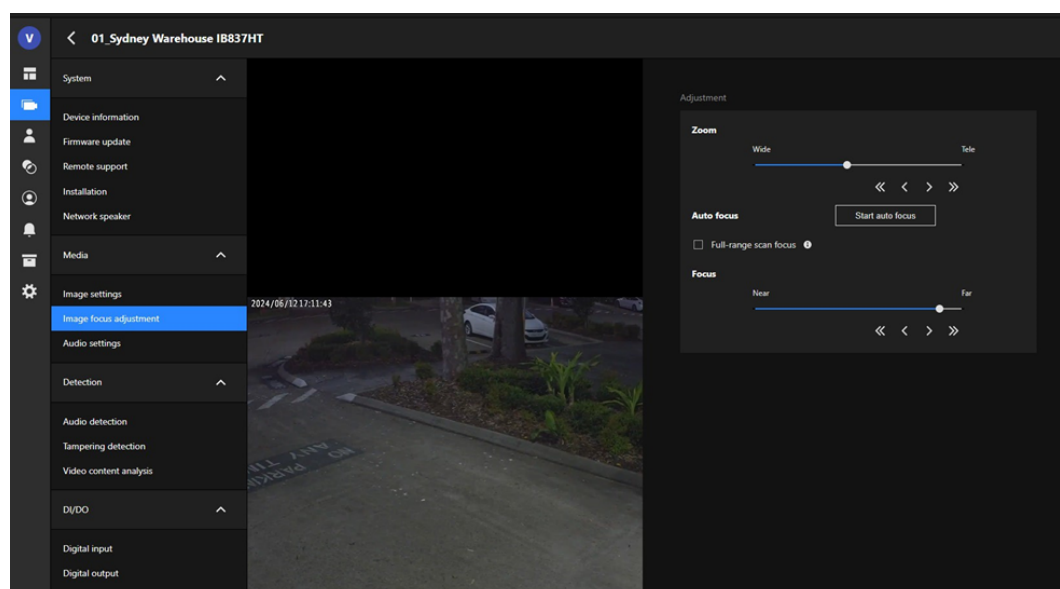
If your camera comes with the remote lens, turning on the enhancement option helps better recognize the plate (though the image would be less bright).



Media > Image Focus Adjustment

For VORTEX Cameras Only

If your system comes with the image focus adjustment feature, you can manually adjust the focus or use the auto focus feature to make sure the subject in your image is clear enough.



Media > Audio Settings

For VORTEX Cameras Only

This is where you decide if you want to record audio while recording the video (when your camera has the audio feature).

Detection > Audio Detection

For VORTEX Cameras Only

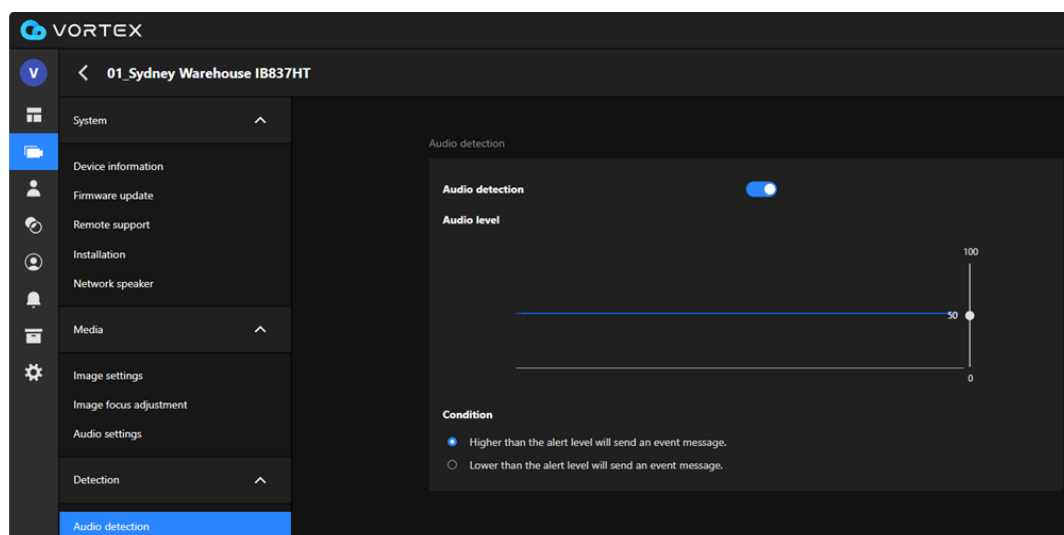
Audio Detection allows events to be triggered based on the detected audio level. Adjust the audio threshold and select the audio detection condition to define when an event is triggered.

Manage Audio Files

For VORTEX cameras that support two-way audio, audio files can be uploaded and used as an audio source for alarm events.

Each camera supports up to two audio files in WAV format (PCM S16LE, 8 kHz, mono), with a maximum file size of 2 MB per file.

This feature is available only for cameras with an xPro license.



Detection > Tampering Detection

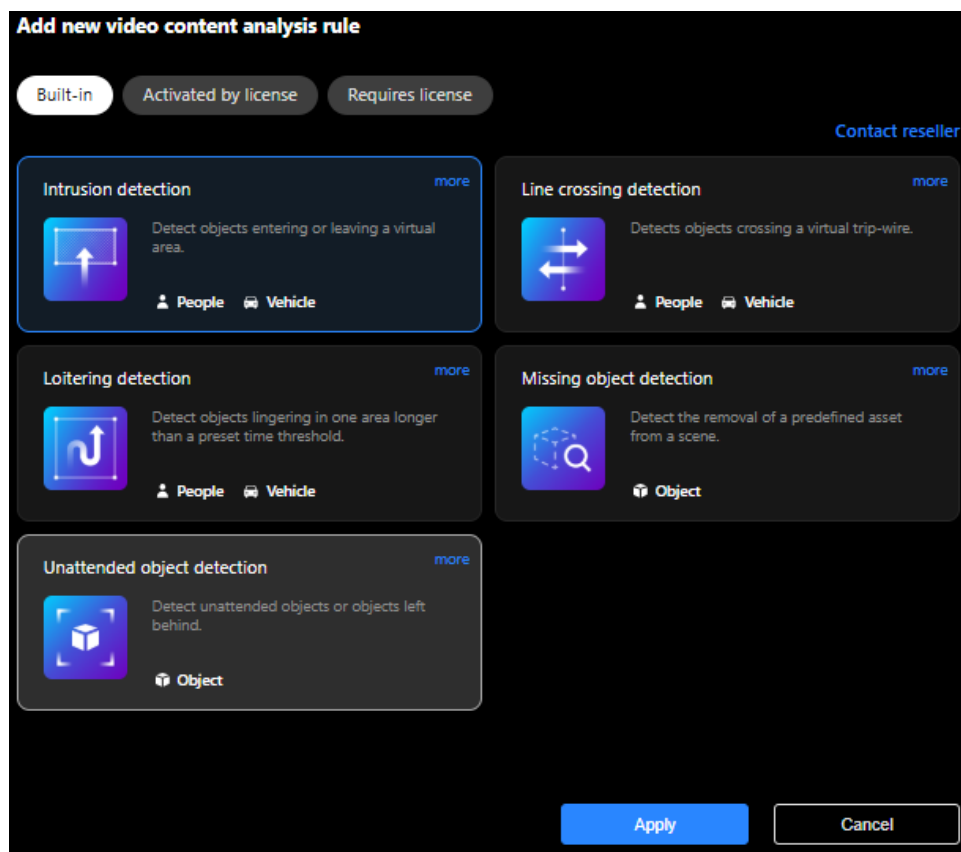
For VORTEX Camera Only

This is when the camera is being meddled with during normal operation, a tampering detection event should occur.

Detection > Video Content Analysis

For VORTEX Cameras Only

The Video Content Analysis (VCA) page provides a clear overview of available detection features based on their license status. Features are organized into the following categories:



1. Built-in

- VCA rules that are included by default and do not require any additional license.
- Available features:
 - Intrusion Detection
 - Line Crossing Detection
 - Loitering Detection
 - Missing Object Detection
 - Unattended Object Detection

2. Activated by License

- Displays Add-on AI detection types that have been activated with a purchased license.
- Once licensed, these features can be configured directly from this page.

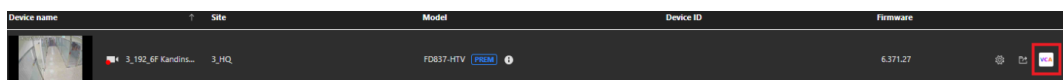
3. Requires License

- Displays all currently supported Add-on AI detection types that require an additional license for activation.
- Helps users easily identify available options and decide whether to enable them.

VORTEX VCA Set Up

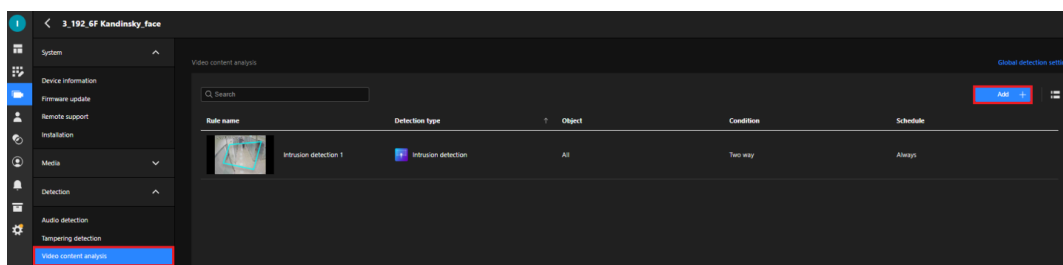
Where to Set Up

- VORTEX VCA is configured individually for each VORTEX camera.
- Go to **Devices** and select the **VCA** icon from the device list.

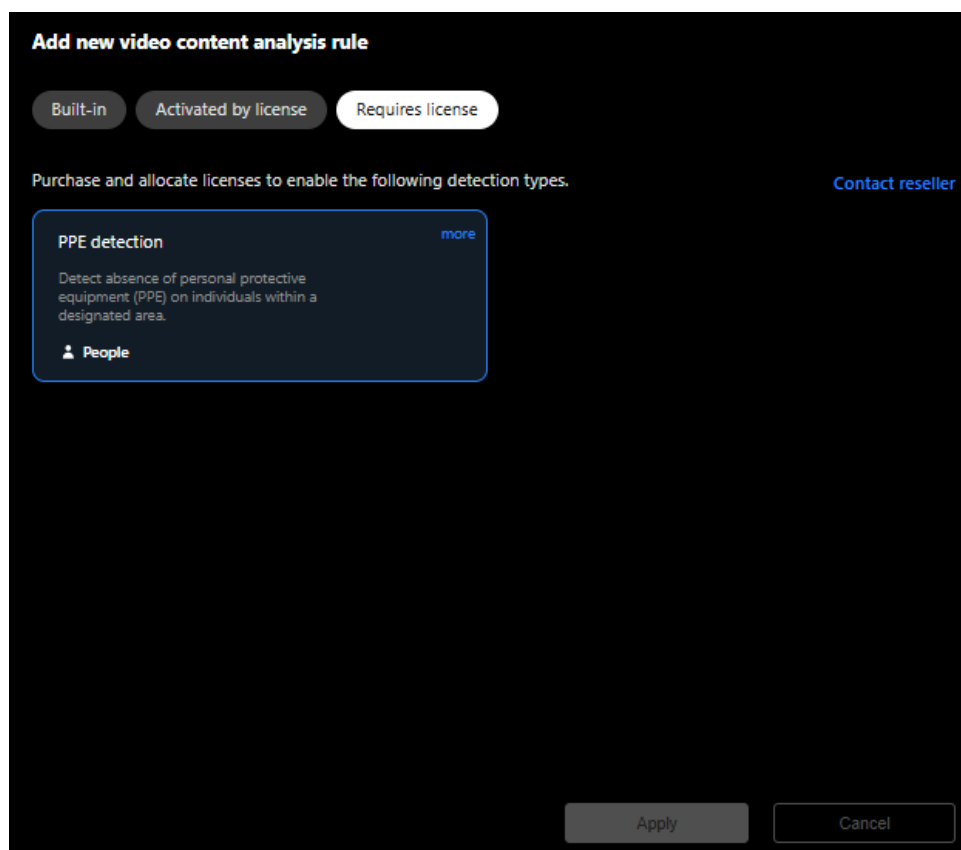


or

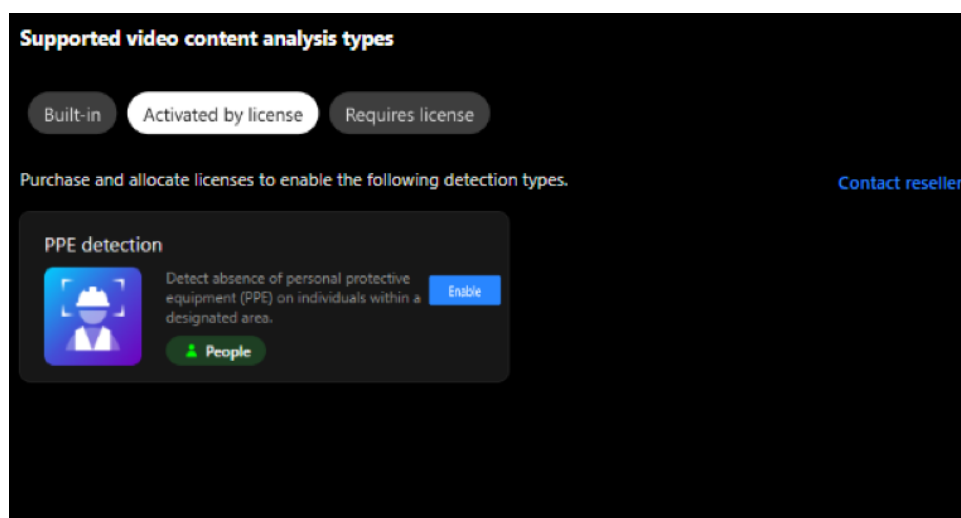
- Go to **Devices > select a camera > Detection > Video Content Analysis > Add**.



- Users can configure different detection rules for each camera based on specific monitoring requirements. Each camera supports multiple VCA rules simultaneously, providing flexibility for various surveillance scenarios. **The maximum number of rules supported is 5 for the Essential type and 10 for the Premium type.**
- Built-in detection types can be configured at any time. However, Add-on AI detection types require an AI license before they can be used. To obtain a license, contact the assigned reseller. Click **Contact Reseller** to view the reseller's contact information. If no reseller has been assigned to the organization, follow the on-screen instructions to locate a suitable reseller.



- Once you have a license for the Add-on AI detection type, you can enable and use it.

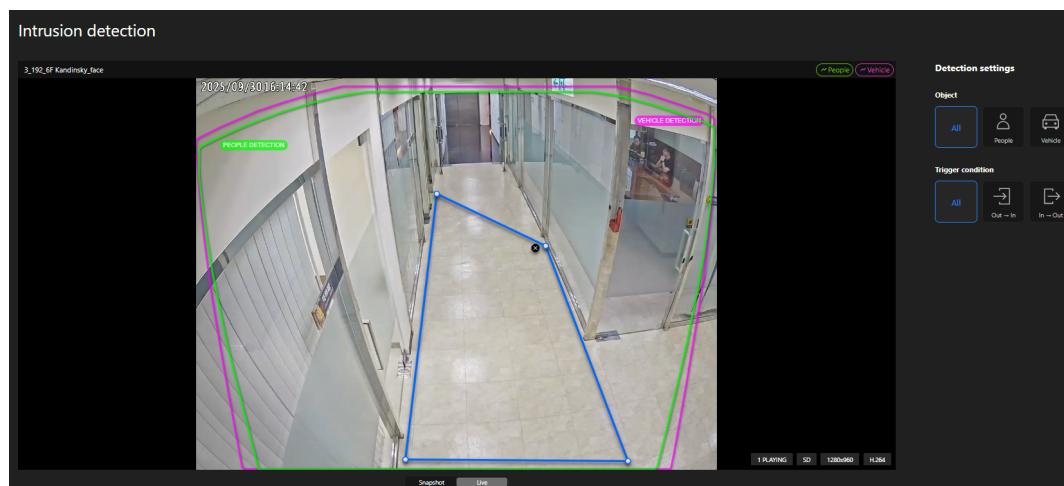


Detection Rule Introduction

Built-in Detection Types

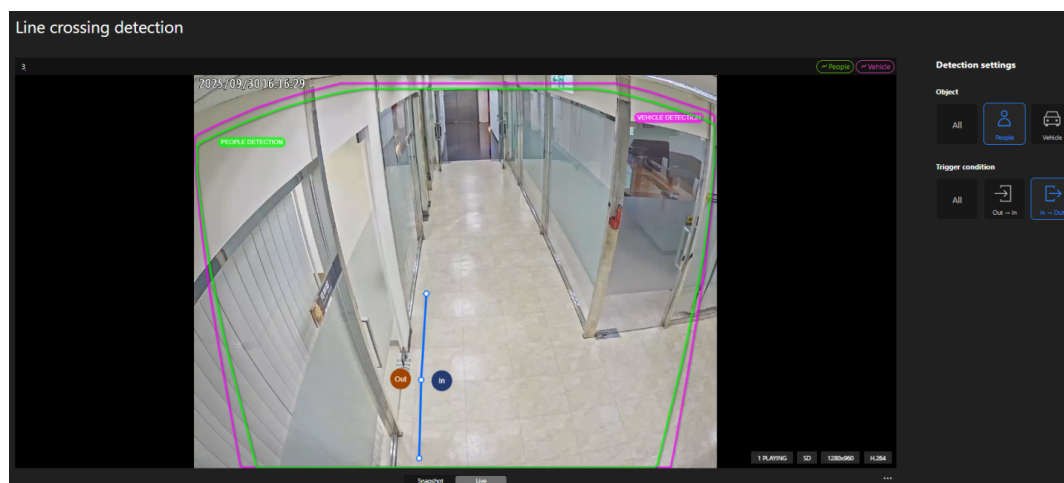
Intrusion Detection

Monitors objects (people or vehicles) entering or leaving a designated area. This feature is commonly used to detect unauthorized access to restricted zones.



Line Crossing Detection

Detects objects crossing a predefined line (virtual tripwire). This feature is ideal for monitoring entrances, boundaries, or exits.



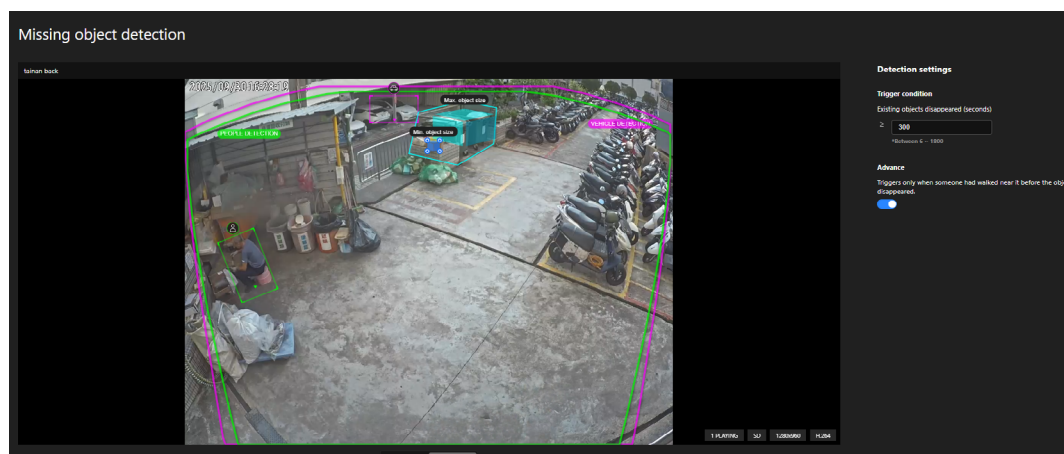
Loitering Detection

Monitors whether an object (person or vehicle) remains within a defined area for an extended period. This feature is useful for detecting suspicious behavior, such as loitering, or monitoring illegal parking.



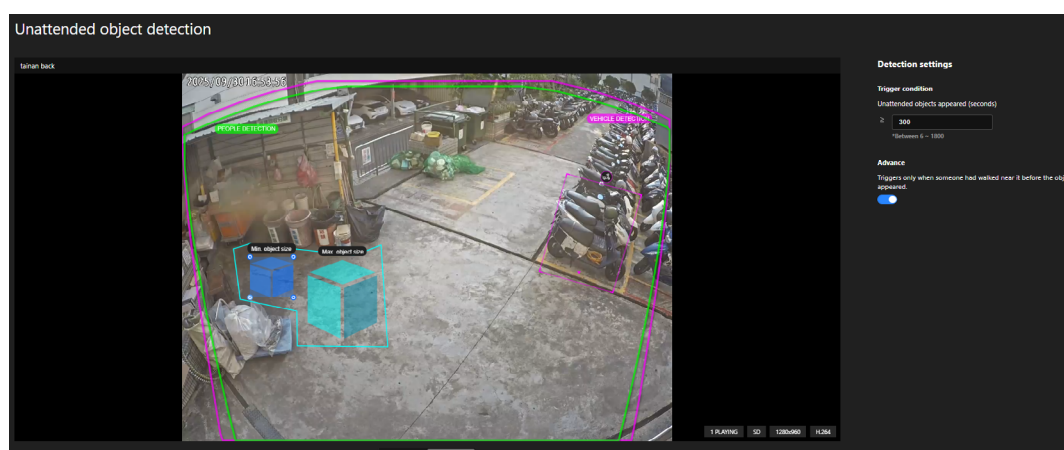
Missing Object Detection

Detects when an object is removed from a defined area. This feature is particularly useful for protecting valuable items or ensuring that important objects remain in place.



Unattended Object Detection

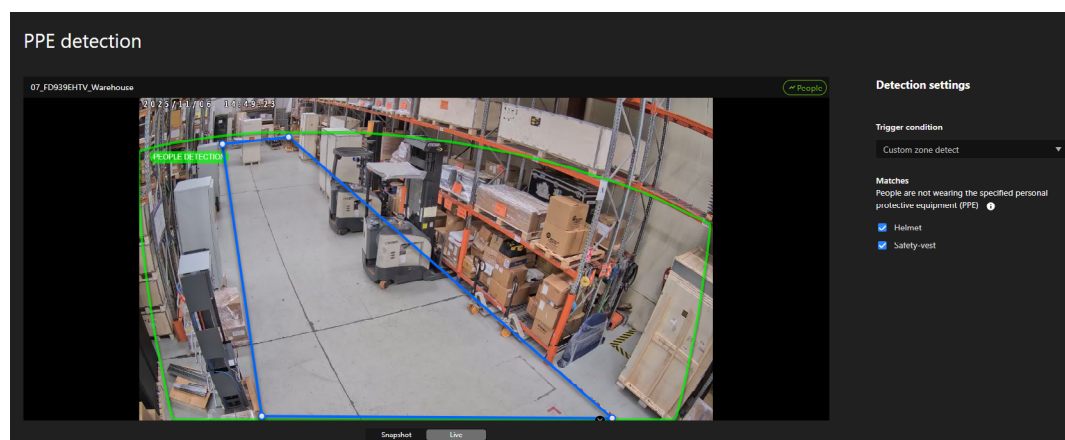
Triggers when an object is left in an area where objects should not be placed. This feature is commonly used in retail stores, logistics facilities, data centers, building entrances, garage entrances, and warehouse environments.



Add-On Detection Types

PPE Detection

Automatically detects whether personnel are wearing required safety equipment, including hard hats and reflective vests. This feature helps improve workplace safety and compliance in real time.

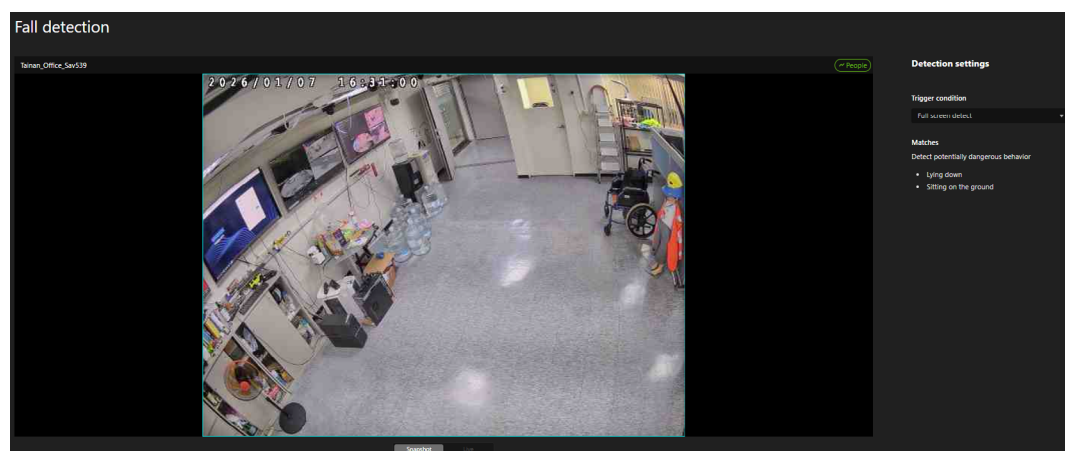


Fall Detection

Detects people who are lying or sitting on the floor. An alert is triggered only after the person remains motionless for several seconds.

Note

To ensure dedicated processing resources and maximum accuracy, Fall Detection and PPE Detection cannot be enabled simultaneously. Select the mode that best fits the current monitoring scenario.



Think Alert

Think Alert allows users to define custom alert triggers using natural language input.

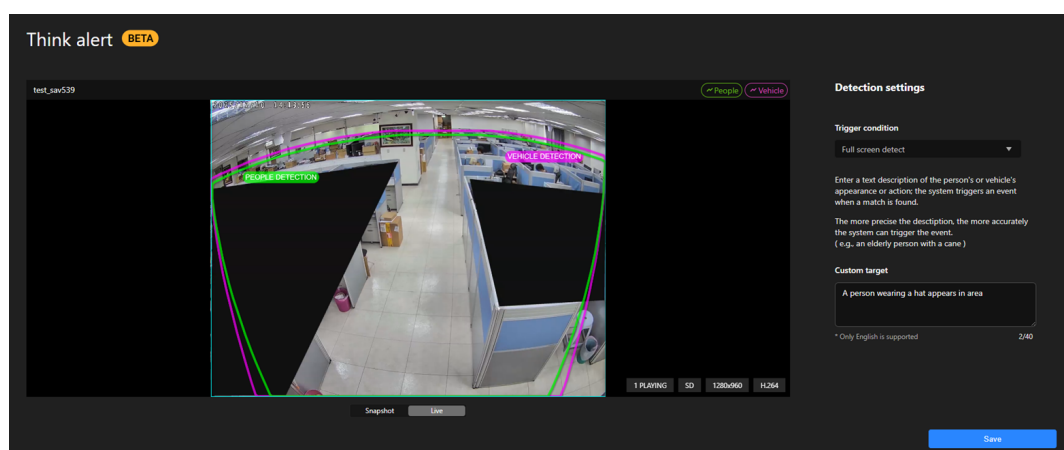
Supported Languages

Refer to the system for the latest list of supported languages.

English (en), Simplified Chinese (zh), Spanish (es), Hindi (hi), Arabic (ar), Bengali (bn), Portuguese (pt), Russian (ru), Japanese (ja), Punjabi (pa), Malay (ms), Tamil (ta), French (fr), German (de), Turkish (tr), Korean (ko), Urdu (ur), Hausa (ha), Greek (el), Dutch (nl), Hebrew (he), Italian (it), Indonesian (id), Serbian (sr), Swahili (sw), Marathi (mr), Belarusian (be), Slovak (sk), Thai (th), Finnish (fi), Ukrainian (uk), Swedish (sv), Malayalam (ml), Punjabi (pa), Czech (cs), Bulgarian (bg), Irish (ga), Georgian (ka), Lithuanian (lt), Amharic (am), Albanian (sq), Armenian (hy), Azerbaijani (az), Catalan (ca), Macedonian (mk), Maltese (mt), Malayalam (ml), Slovenian (sl), Serbian (sr), Kazakh (kk), Mongolian (mn), Latvian (lv), Estonian (et), Lithuanian (lt), Georgian (ka), Kikuyu (ki), Sorani Kurdish (ckb), Hakka Chinese (hak), Ossetian (os), Cherokee (chr), Kurdish (ku), Greek (el), Polish (pl), Latin (la), Greek (el), Sinhalese (si), Hebrew (iw), Belarusian (be), Hakka Chinese (hak), Spanish (es), Chinese (ch), Spanish (es).

NOTE

1. The search primarily targets objects. Currently, VORTEX supports two object categories: **People** and **Vehicles**.
2. Detection focuses on identifying a single person or a single vehicle.

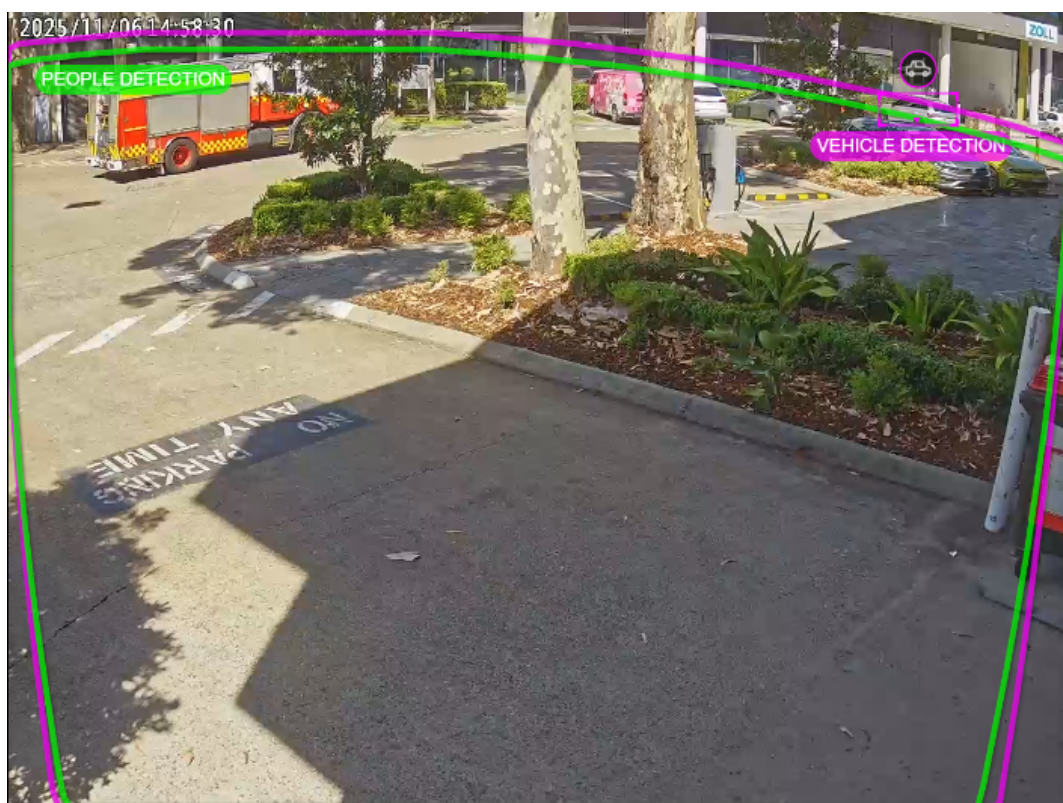


TIPS

Effective Detection Area

The green frame indicates the effective detection area for people. Use this area as a reference when defining detection zones.

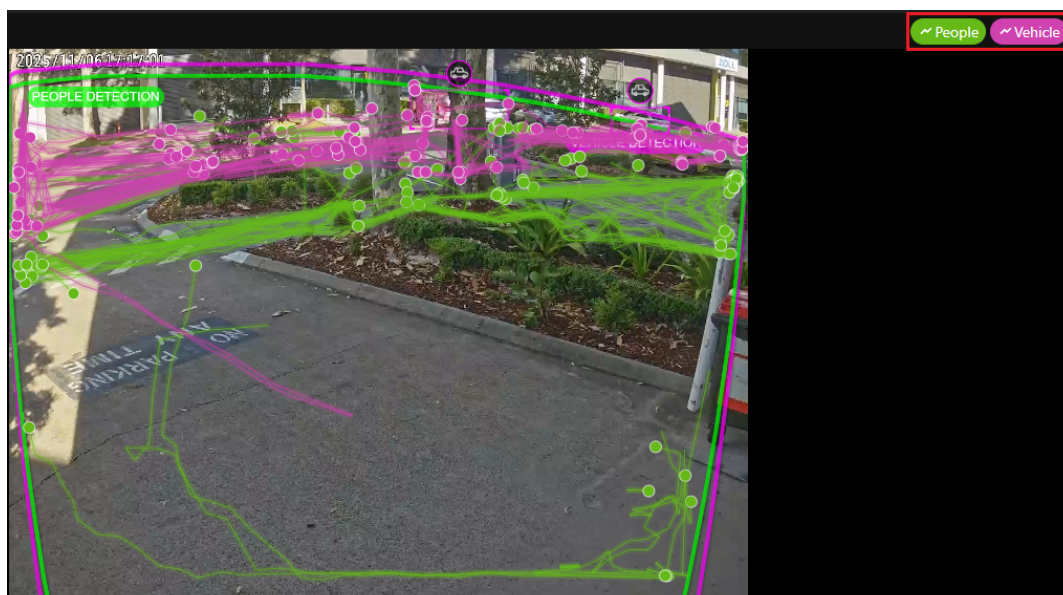
Similarly, the purple frame indicates the effective detection area for vehicles and can be used as a reference when configuring vehicle detection zones.



Last 100 Trajectories for Reference

Click **People** or **Vehicle** in the upper-right corner of the screen to display the most recent 100 trajectories for the selected object type.

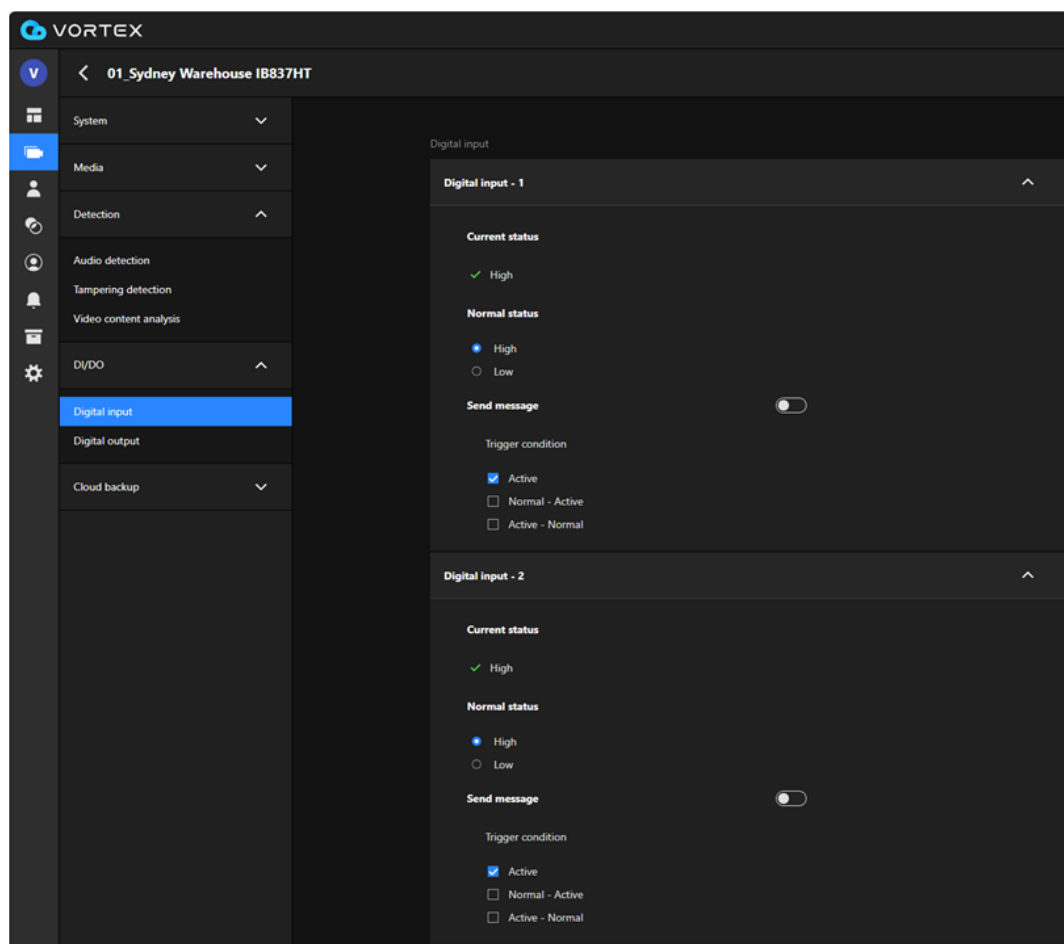
These trajectories help determine which areas should be included or excluded when configuring detection zones.



DI/DO > Digital Input

For VORTEX Cameras Only

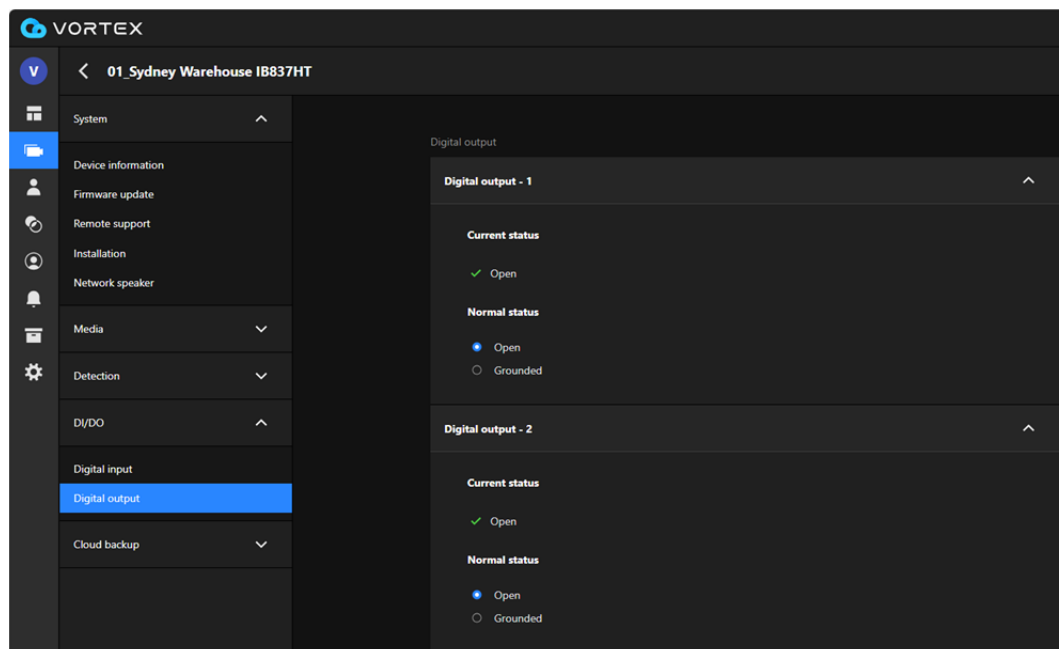
Select High or Low as the Normal status for the digital input. Connect the digital input pin of the Network Camera to an external device to detect the current input connection status.



DI/DO > Digital Output

For VORTEX Cameras Only

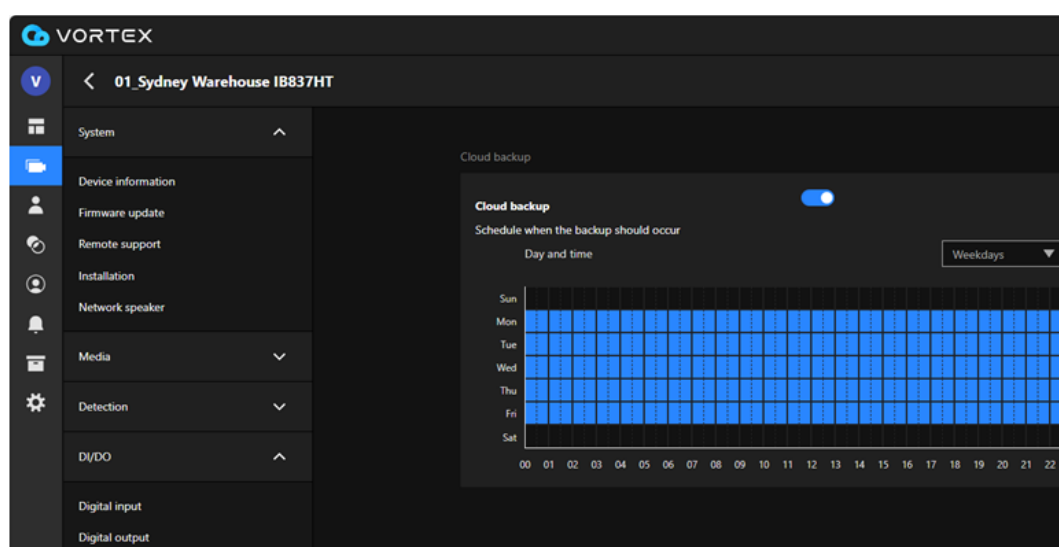
Select Grounded or Open to define the normal status for the digital output. Connect the digital output pin of the Network Camera to an external device to detect the current output connection status.



Recording & Storages > Cloud Backup

For VORTEX Cameras Only

Enable Cloud backup by sliding the toggle button. When enabled, videos will be stored in the cloud storage. Set your desired schedule to back up your video footage to the cloud by selecting an option from the drop-down list or dragging the mouse across the screen.



User Management

User management offers a safe and efficient way to manage user access with flexible role customization and device accessibility, preventing unauthorized access and privilege for your security system.

Name	Email	Organization role	Status
aaron.reyna	aaron.reyna@vivotek.com	Profile edit	Onboard
acadelago	acadelago@selnet-sa.com.ar	Profile edit	Onboard
acheng.cheng	acheng.cheng@vivotek.com	Admin	Onboard
aching.huang	aching.huang@vivotek.com	Profile edit	Onboard
adauphin.chiu	adauphin.chiu@gmail.com	Admin	Pending Invite again
agnieszka.szymanska	agnieszka.szymanska@arpol.pl	Profile edit	Pending Invite again

Role Settings

[xStd and xPro only]

Users can set up the privilege by two roles including organization role and device access role. The combination of permission for organization role and devices access role defines what the user can do in the organization.

Go to “Users” in side menu, you will find a button called role setting on the upper right corner. In there, you will see role settings for you to pick features you would like for customized role to have.

Role name	Permission summary
Owner	All admin permissions and has the right to transfer org or delete org
Admin	Grant admin permissions and all devices access
Member	No system setting permission

Role name	Permission summary	Role created on
Kisi	Access for Kisi Demo	2026/06/13 00:31:51
TEST	Sky_Test	2026/06/02 11:16:41
Alarmonly		2026/05/08 08:55:29
Temporary Demo		2026/04/21 23:57:42
security guard		2026/03/26 02:45:24

Organization role

- Default roles include owner, admin and member.
- Users can create a custom role with the permission at systematic level, such as user management.

Device access role

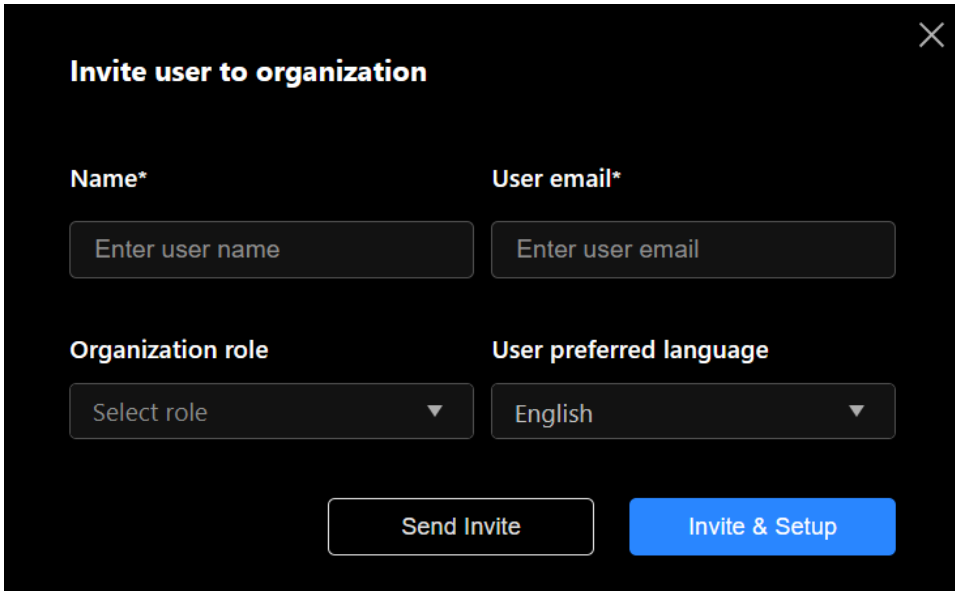
- Default roles include supervisor and viewer.
- Users can create a custom role for what you can do operating each camera, such as live view and playback.

NOTE

- **You cannot create roles with permissions** you don't already have yourself. For example, to grant someone the ability to manage access control or alarm management, you must have those permissions yourself.
- There's a built-in **Admin** role that inherently has the highest privileges in the org (cannot be removed).
- In practice, each role assigned is limited to what the creator has access to — following the **principle of least privilege**.
- You can't grant user access permission on devices that you don't have access to yourself.
- **Bottom line:** You can't escalate privileges beyond your own when assigning roles and granting access to devices you don't have access to. The system respects your current permission set as an upper bound. For example: John Doe has Role/Users/Profile/integration, he can only assign org role with users/profile/integration or fewer to another user.

Invite Users

1. Select users by inviting them. To do so, click the "Invite User" button on the upper-right corner.
2. Enter the name and email address for the user.
3. Select the organization role for the user and preferred language for the portal.
4. Click on invite and setup to further configure the device access permission.
5. Select the device that the user can access and assign the device access role for selected device.



Invite user to organization ✕

Name* **User email***

Enter user name Enter user email

Organization role **User preferred language**

Select role English

Send Invite Invite & Setup

NOTE

- Users can assign different device access roles to different devices within a user account.
- User access permission and organization role can be set or edited by clicking on the user.

[**xLite** only]

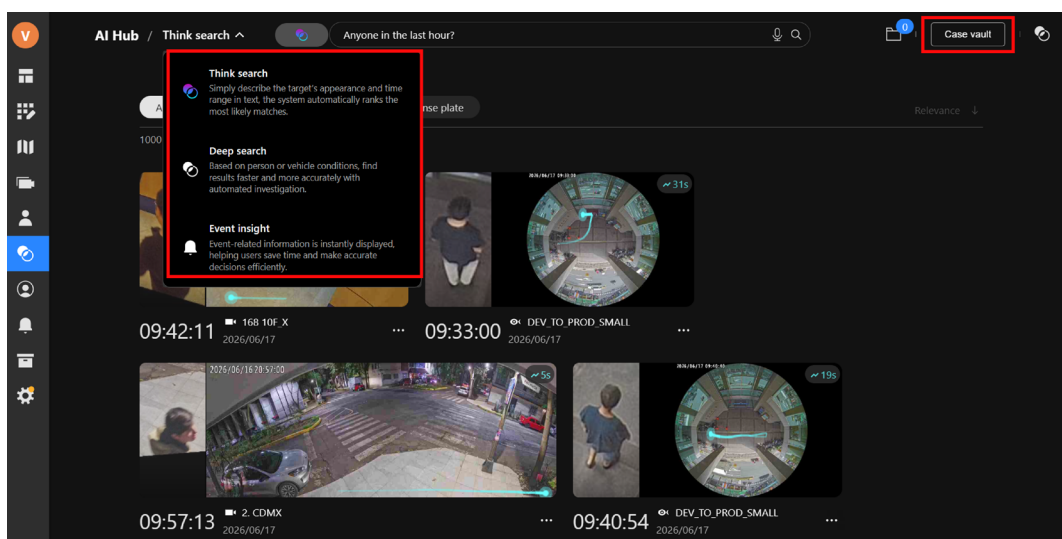
User can only invite user with admin permission without custom role. and there is a user account limitation up to 10 accounts.

[xPro only]

AI Hub is a centralized platform within VORTEX that unifies and streamlines AI-powered surveillance features. It provides a single interface for accessing Think Search, Deep Search, Event Insight, and Case Vault, helping users perform surveillance investigations more efficiently and intuitively.

NOTE

AI Hub is initially released as a beta feature.



Deep Search

Deep Search is a post-event search function that enables users to efficiently search for objects (people or vehicles) in recorded video. Typical application scenarios include locating a thief in a department store, finding a lost child in a station, or identifying a suspect vehicle.

Using AI-powered video analytics, video content is analyzed in real time, and objects along with their attributes are extracted and stored as metadata. With Deep Search, users no longer need to manually review recorded videos from multiple cameras frame by frame to locate a specific person or vehicle. For example, users can quickly search for a person wearing a red T-shirt and blue jeans. This can reduce investigation time from days to minutes.

A key advantage of VORTEX Deep Search is that video analytics are performed at the edge rather than on cloud servers. Edge AI processing detects and tracks objects (supported on both Essential and Premium cameras) and extracts object attributes (supported on Premium cameras only). Deep Search then uses this metadata to locate matching objects, providing significantly faster search performance than traditional server-based solutions.

NOTE

VORTEX Connect PRO does not currently support Deep Search.

Deep Search Interfaces

VORTEX provides two Deep Search interfaces:

- Deep Search
- Original Deep Search

The new Deep Search interface is displayed by default. Users can switch to the legacy interface at any time by clicking Back to Original Deep Search in the upper-right corner of the page.

Deep Search (New Interface)

The new Deep Search interface provides a streamlined workflow for locating people and vehicles in recorded video. Search results are displayed as visual cards, allowing users to quickly review snapshots, trajectories, timestamps, and camera locations.

By default, Deep Search searches for People across all devices during the last hour.

Search Criteria

Use the search bar at the top of the page to define the search criteria.

The following filters are available:

Object Type

- People
- Vehicles

Time Range

- Select the time interval for the search.

Devices

- Select one or more cameras to search.

Advanced Filters

- Scene Search
- Attribute Search

Search Results

Search results are displayed as visual cards.

Each card contains:

- Object snapshot
- Scene snapshot
- Camera name
- Detection timestamp
- Object trajectory
- Tracking duration

For People Search, users can switch between **All** and **Face** views to filter search results.

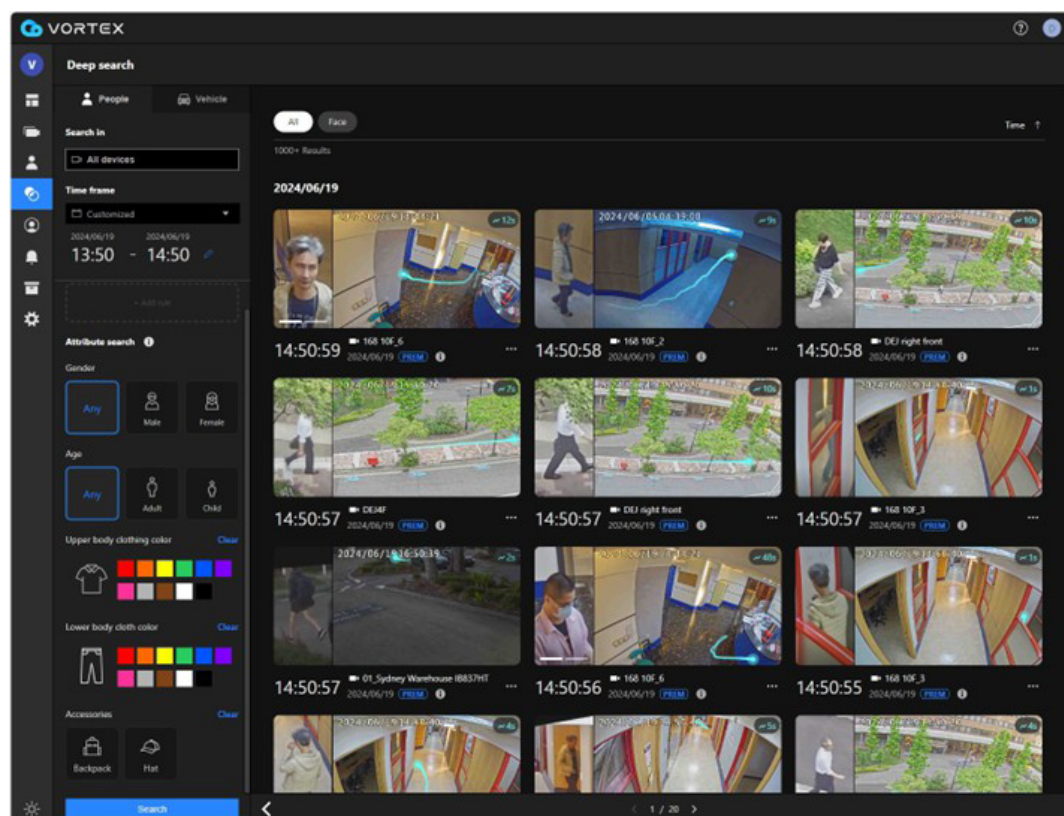
Click a search result card to open the playback page. The corresponding recorded video is displayed for further investigation.

Selected search results can also be added to **Case Vault** for investigation management.

Original Deep Search

Go to **AI Hub**, select **Deep Search** from the drop-down menu, and click **Back to Original Deep Search** in the upper-right corner of the page. The default search results are displayed.

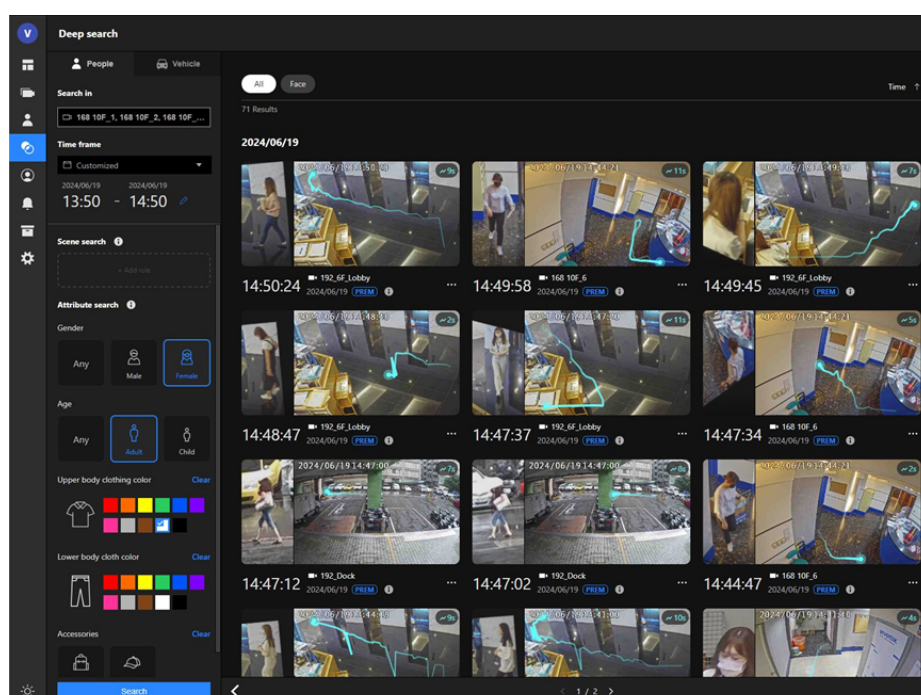
By default, Deep Search searches for **People** across all cameras within the VORTEX organization during the previous hour. Therefore, the initial search results display people detected by all cameras during the last hour.



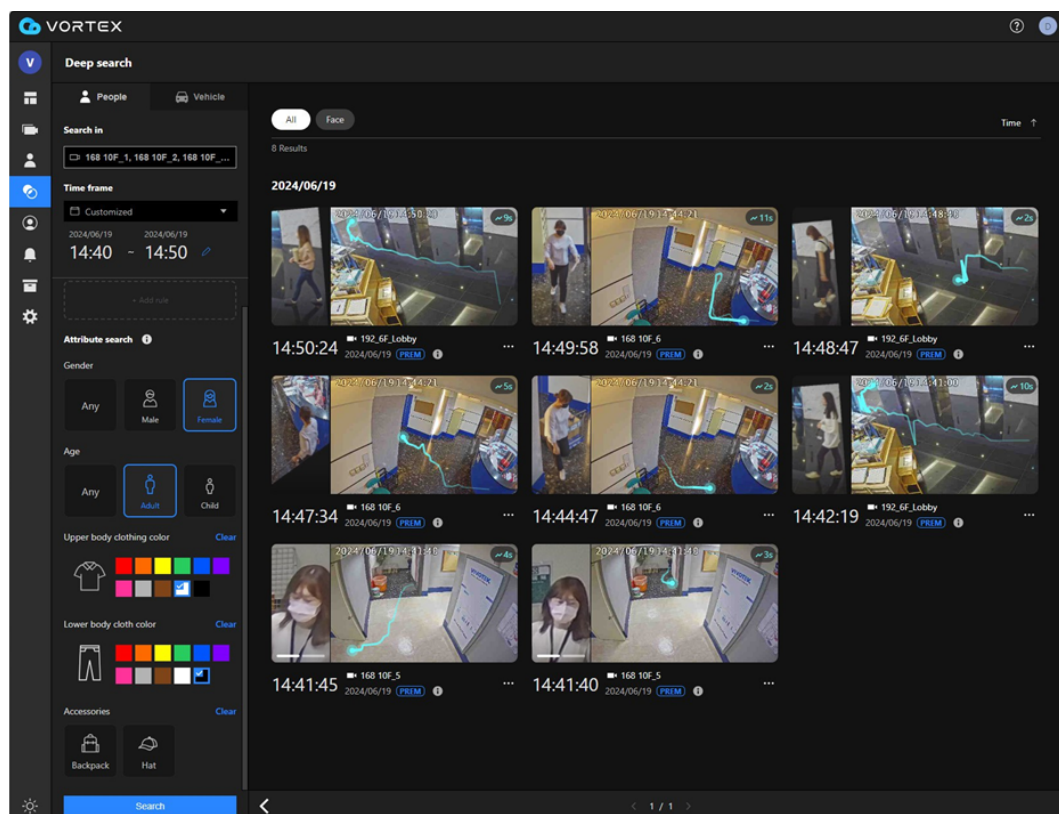
Example of the default Deep Search results

Using Deep Search to Search for People

1. Configure the search criteria using the options in the left panel:
 - Which camera(s) to search for
 - Search time interval (time frame)
 - Filter by rule (a.k.a. Scene Search)
 - Line Crossing Detection rule
 - Loitering Detection rule
 - Intrusion Detection rule
 - Filter by appearances (a.k.a. Attribute Search)
 - Gender
 - Age
 - Upper body cloth color
 - Lower body cloth color
 - Accessories - Backpack
 - Accessories - Hat
2. Click **Search**.
3. The search results appear. Note the following:
 - Each search result consists of two parts. The left image is a representative snapshot of the detected person during the tracked time interval, while the right image is a snapshot of the camera view.
 - The person's trajectory is overlaid on the right image, allowing users to easily understand the person's movement during the captured time interval.
4. Click the scene snapshot of a search result to open the playback page. The recorded video containing the detected person is played. Click **Archive** to save the video if needed.



5. To further narrow the search results, add additional search criteria, such as a shorter time frame.



Using Deep Search to Search for Vehicles

1. Configure the search criteria using the options in the left panel:

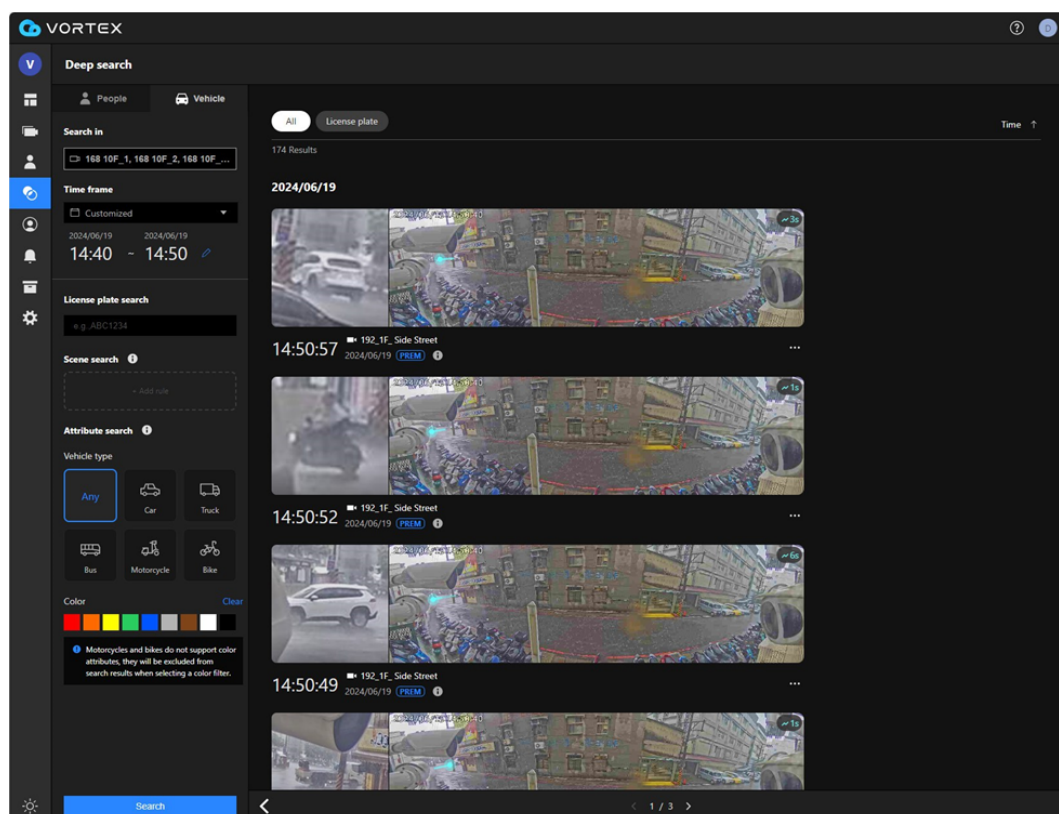
- Which camera(s) to search for
- Search time interval (time frame)
- Filter by rule (a.k.a. Scene Search)
 - Line Crossing Detection rule
 - Loitering Detection rule
 - Intrusion Detection rule
- Filter by appearances (a.k.a. Attribute Search)
 - Vehicle type
 - Color (do not support motorcycles and bikes)

2. Click **Search**.

3. The search results are displayed. License plate information is also available when License Plate is enabled. Note the following:

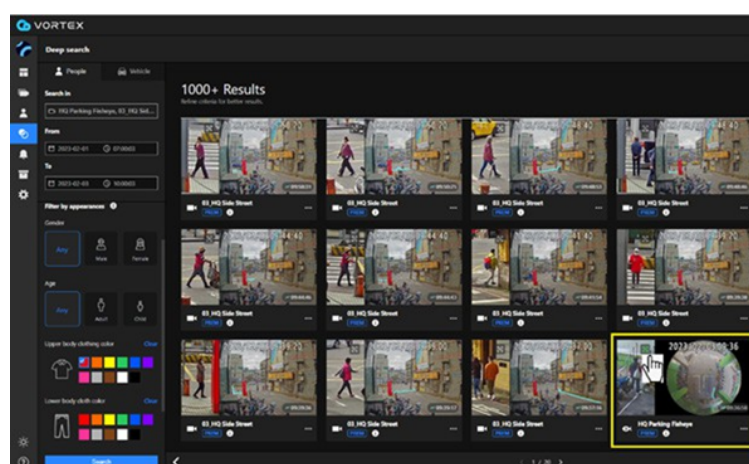
- Each search result consists of two parts. The left image is a representative snapshot of the detected vehicle during the tracked time interval, while the right image is a snapshot of the camera view.
- The vehicle's trajectory is overlaid on the right image, allowing users to easily understand the vehicle's movement during the captured time interval.

- Click the scene snapshot of a search result to open the playback page. The recorded video containing the detected vehicle is played.

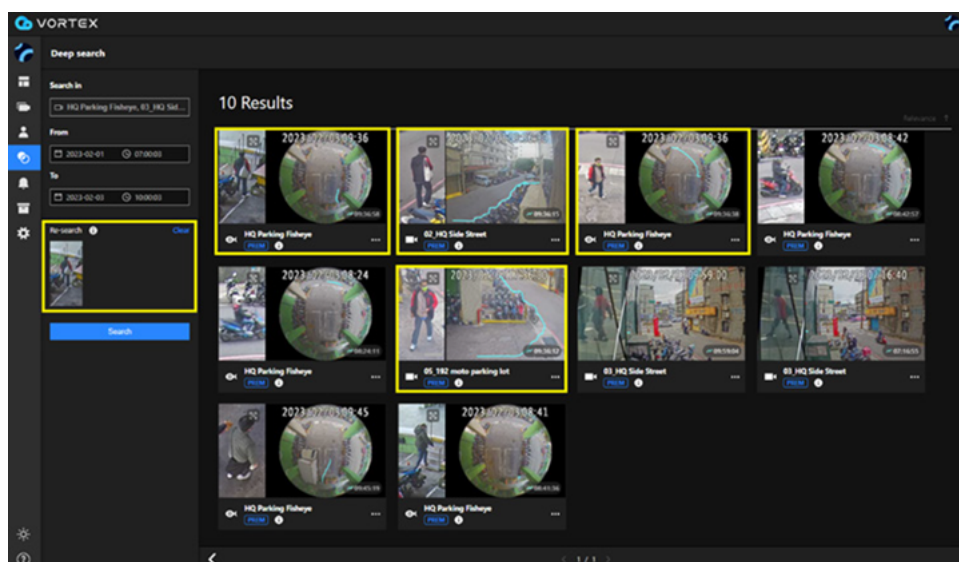


Using Re-Search

Re-Search is based on Person Re-Identification (Re-ID) technology. When a person of interest is found in the search results, Re-Search can be used to locate the same person across all selected cameras using the selected snapshot as a reference image.



Click a person snapshot of interest to do Re-Search.



Person re-identification (Re-ID)

The example above uses the selected snapshot to perform a Re-Search. Among the ten search results, the first three video clips and the sixth video clip are confirmed to contain the same person captured by different cameras. This demonstrates how Re-Search helps users efficiently perform cross-camera investigations.

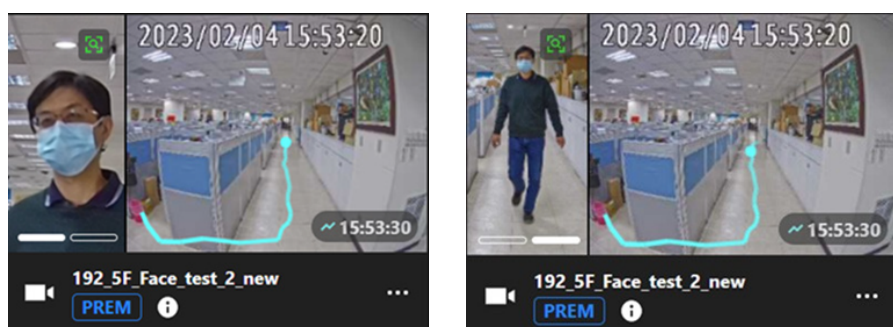
Person Re-Identification (Re-ID)

When a person's face is captured with sufficient resolution, two snapshots are available on the left side of the search result.

- Face snapshot
- Full-body snapshot

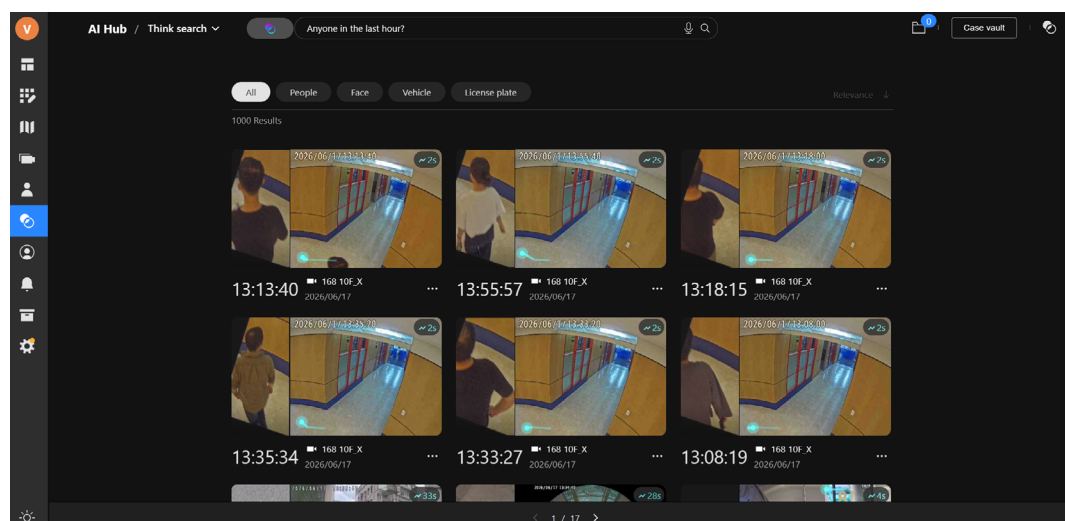
Click the white bar below the snapshot to switch between the two images.

When available, facial features are also incorporated into the search process to improve search accuracy.



Think Search

Think Search allows users to quickly locate relevant video footage based on specific objects or contextual information.



Think Search

Powered by VLM (Vision-Language Model), this feature enables users to enter natural language queries (e.g., "man with a red shirt" or "white SUV at the entrance") to locate matching events or best-shot images. This makes video search more flexible and intuitive.

Best Practice

For optimal search results, structure queries using the following format:

[Person or Vehicle] + [Action/Descriptor] + [Optional Connector] + [Optional Second Descriptor] + [Optional Location]

Examples:

- Person wearing a black jacket with sunglasses on the street at 7 a.m.
- Person carrying a large backpack with headphones in the library.
- White SUV parked at the entrance.
- Person crossing the lobby carrying a suitcase.

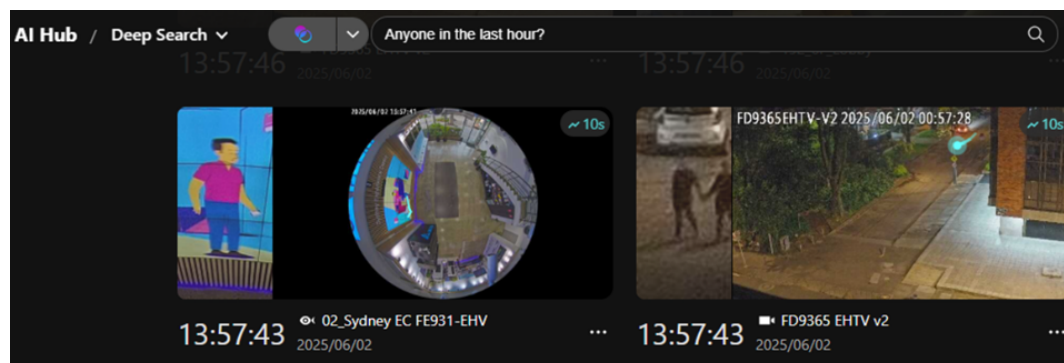
Supported Languages

Think Search supports the following languages:

English (en), Simplified Chinese (zh), Spanish (es), Hindi (hi), Arabic (ar), Bengali (bn), Portuguese (pt), Russian (ru), Japanese (ja), Punjabi (pa), Malay (ms), Tamil (ta), French (fr), German (de), Turkish (tr), Korean (ko), Urdu (ur), Hausa (ha), Greek (el), Dutch (nl), Hebrew (he), Italian (it), Indonesian (id), Serbian (sr), Swahili (sw), Marathi (mr), Belarusian (be), Slovak (sk), Thai (th), Finnish (fi), Ukrainian (uk), Swedish (sv), Malayalam (ml), Czech (cs), Bulgarian (bg), Irish (ga), Georgian (ka), Lithuanian (lt), Amharic (am), Albanian (sq), Armenian (hy), Azerbaijani (az), Catalan (ca), Macedonian (mk), Maltese (mt), Slovenian (sl), Kazakh (kk), Mongolian (mn), Latvian (lv), Estonian (et), Kikuyu (ki), Sorani Kurdish (ckb), Hakka Chinese (hak), Ossetian (os), Cherokee (chr), Kurdish (ku), Polish (pl), Latin (la), Sinhalese (si), and Chinese (ch).

Known Limitations

- Accuracy may decrease when searching for multiple people simultaneously.
- Small objects (for example, phones, wallets, and earbuds) may be difficult to identify.
- Action-based scenes (for example, running or waving) may produce less precise results.

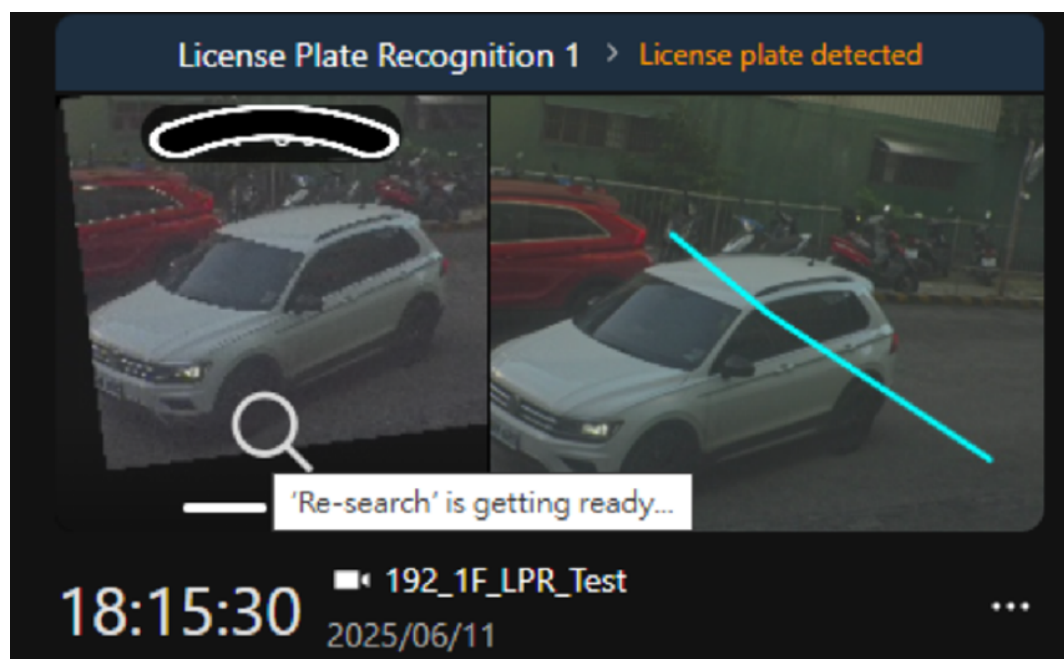


Event Insight

Event Insight provides users with a visual summary and detailed breakdown of key events detected by AI. It helps identify the person or object responsible for specific incidents, understand behavior patterns, and spot anomalies.

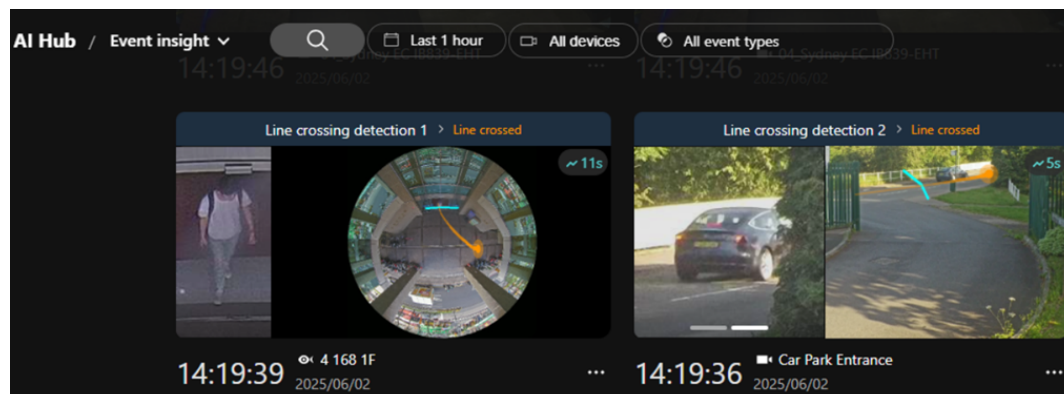
Known Limitations:

- Event source from NVR does not support the "Add to case" feature
- When data is not ready, a tip appear to notify you that the data is not ready for further operation.



The difference in data information between VORTEX camera and VORTEX Connect

- No best shot displayed on the event from VORTEX Connect.
- No detection area/line displayed on the event from VORTEX Connect.
- No path displayed on the event from VORTEX Connect.
- Only archive and send feedback are supported for events from VORTEX Connect.



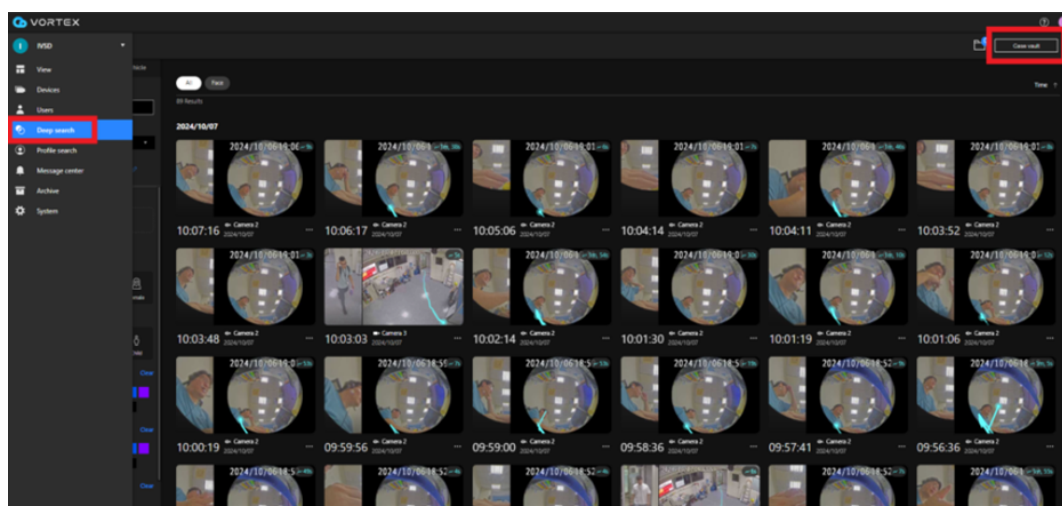
Case Vault

Case Vault is designed for securely storing and organizing critical footage related to investigations. Users can group video clips, add notes, and collaborate with team members — all within a dedicated case management space. This improves workflow for incident review, evidence sharing, and long-term retention.

How to Create a Case Report:

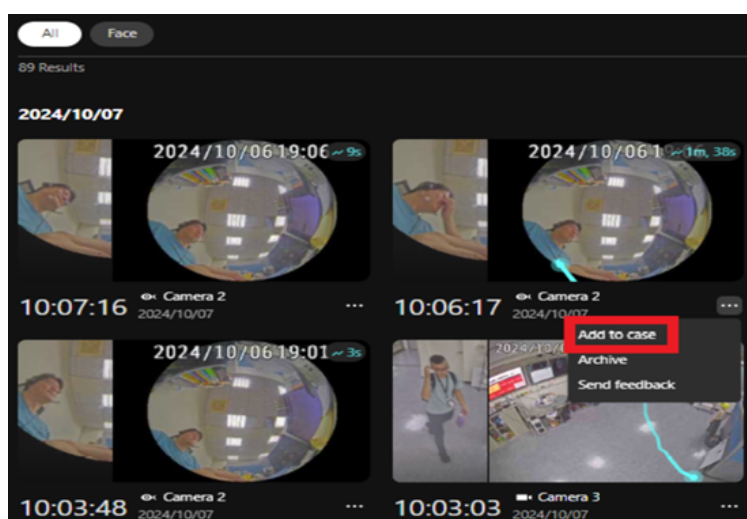
1. Access Case Vault:

Navigate to the Deep Search section, you can find Case Vault on the upper-right of the Deep Search page. This section allows you to manage video clips, snapshots, and other relevant data associated with specific incidents.

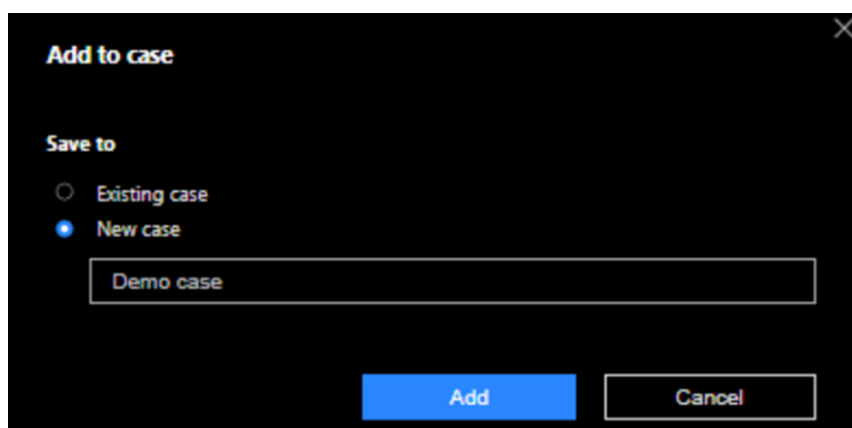


2. Create a New Case:

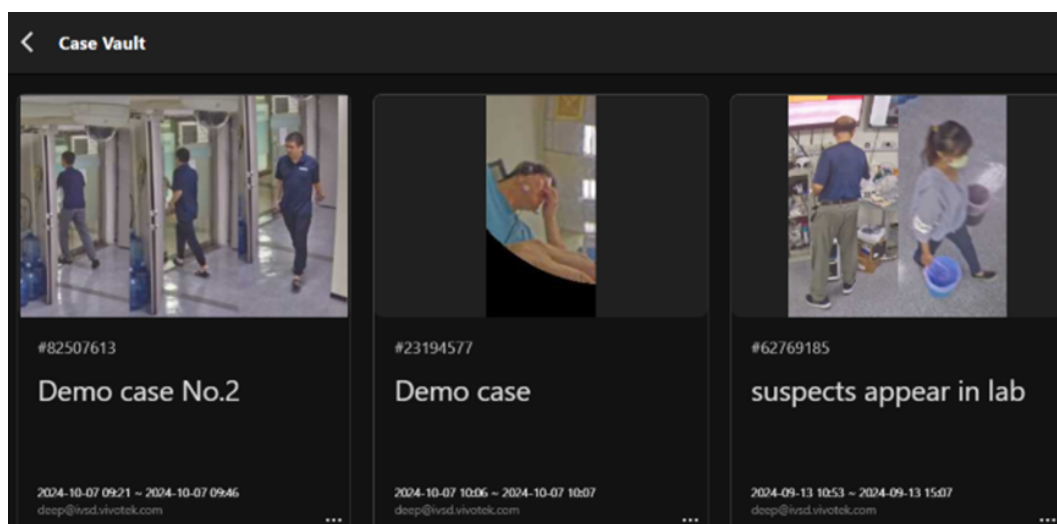
1. Two ways to create a new case:
2. Add one specific event to a case:
3. Click more button of the specific event you need, and click "Add to case"



4. Add this event either to "New case" or the "Existing case", and click "Add" to next step

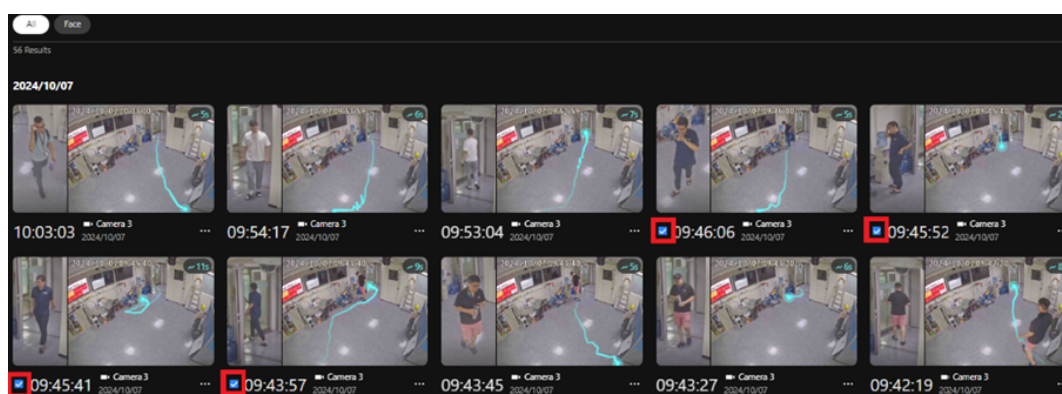


5. A new case has been added to the Case Vault

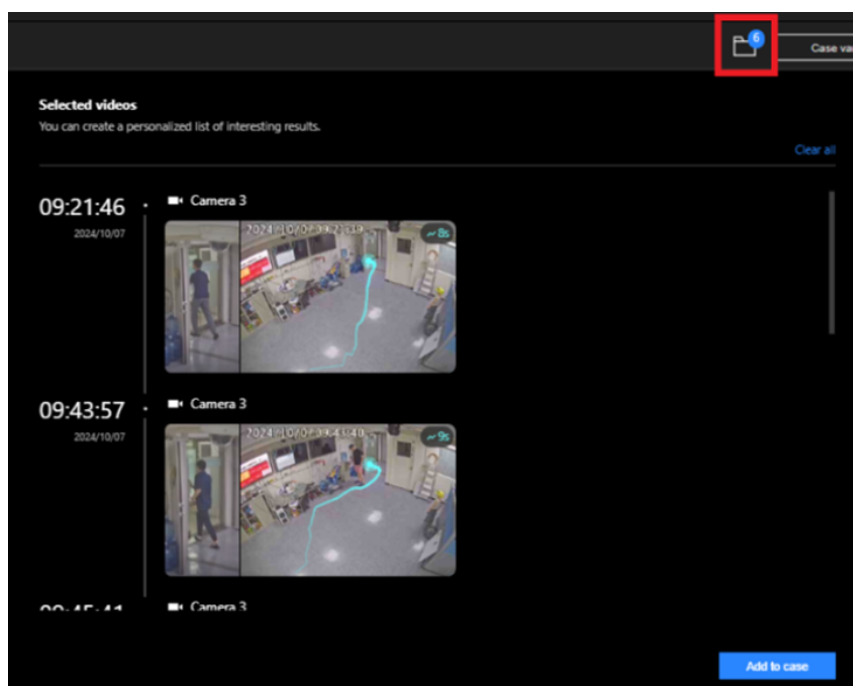


3. Add a series of events to a new case

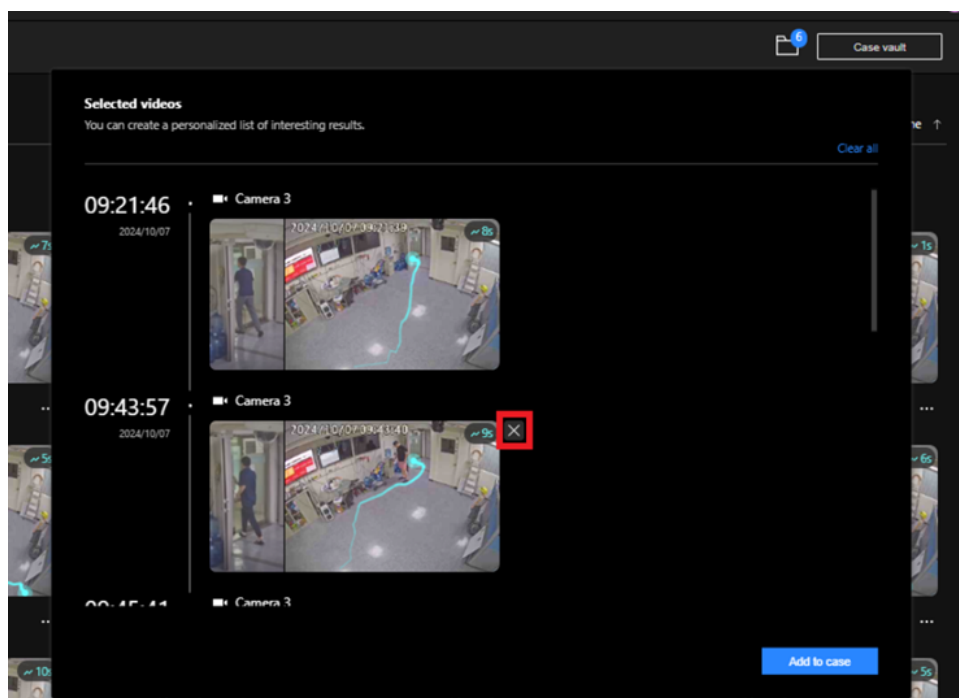
1. Select events by click checkbox to this new case.



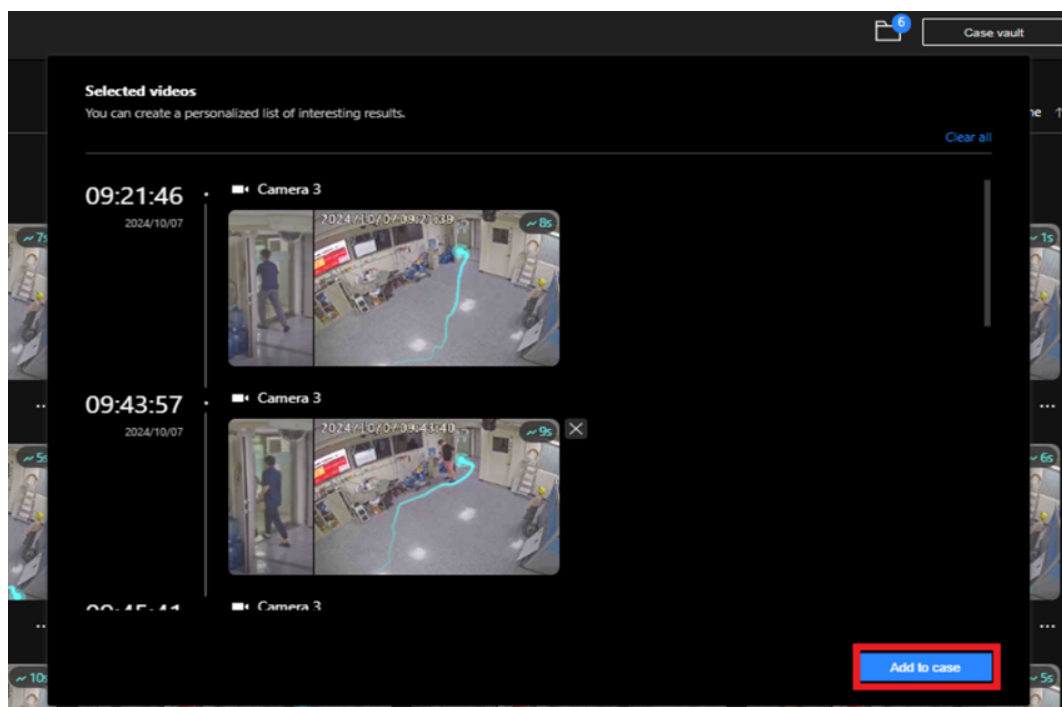
2. The selected videos are added to the folder in the upper-right corner of the panel.



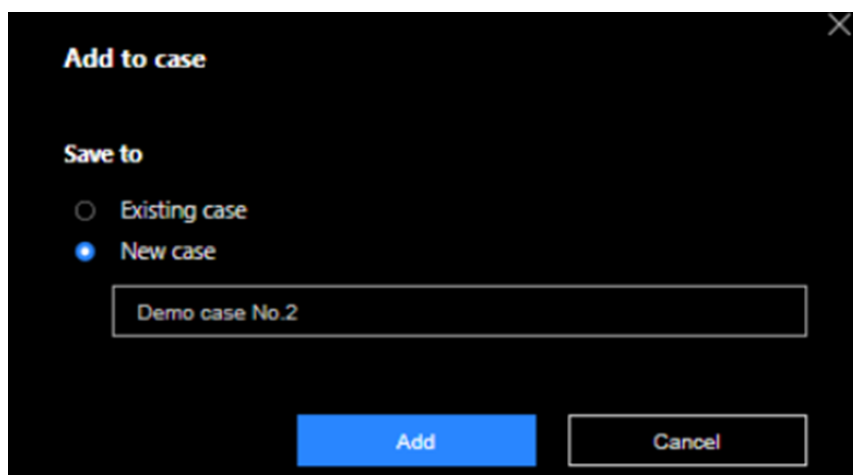
3. If there's any video you don't need, you can delete it by clicking "Delete" button next to the video thumbnail



4. Click "Add to case" to the next step



5. Add those series of event either to "New case" or the "Existing case", and click "Add" to next step



Add to case

Save to

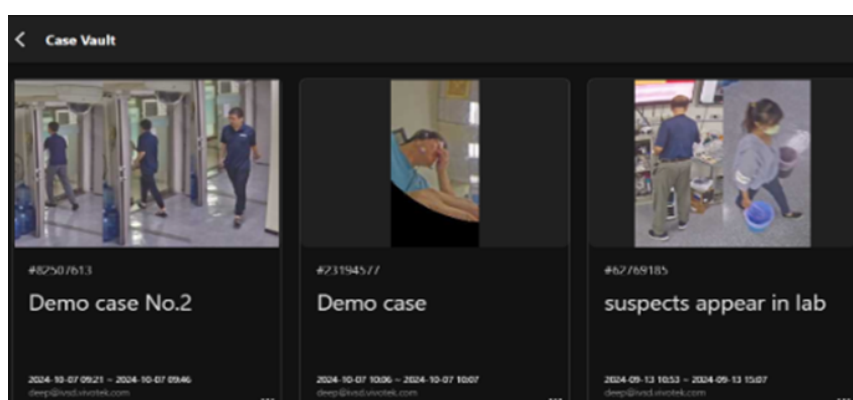
☐ Existing case

☒ New case

Demo case No.2

Add Cancel

6. A new case has been added to the Case Vault



4. Export the information you need:

Once the case has been created and relevant video clips are attached, you can export it as a:

- Case report in PDF format (including the following information: case name, case ID, Reporter, Activity duration, description)
- Best shots
- Videos

5. Download and share the report:

After exporting the report, you can download it from the browser and securely share it with others via cloud sharing or email.

This workflow ensures that incidents are documented, archived, and easily retrievable for later analysis or legal purposes.

Profile Search

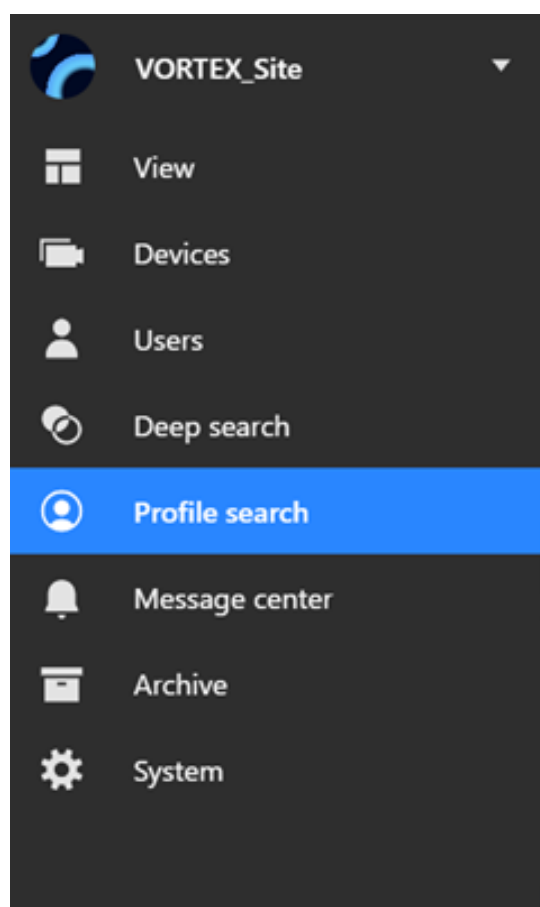
[ only]

Profile Search allows users to create profiles with a person's facial image(s) and search for that person by those facial image(s) in the profile. A user can upload a profile's facial images from a computer or save them from a Deep Search result. Users can search for the person in the recorded videos immediately when the profile is created or later.

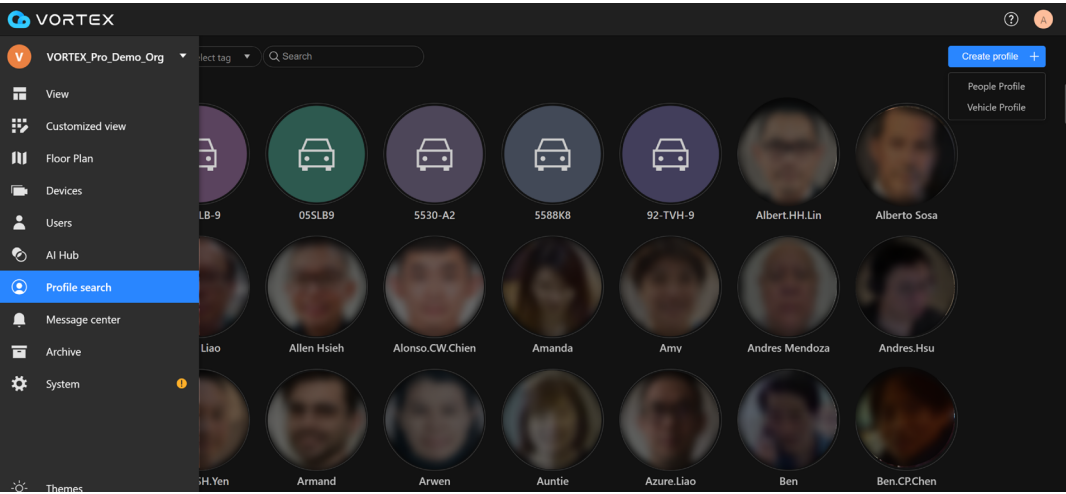
The key feature of VORTEX AI is that the core of video analytics is done at the edge, not on the cloud server side. The onboard video analytics detect faces and extract face features. Those metadata are saved in the cloud for post search.

Creating a Profile

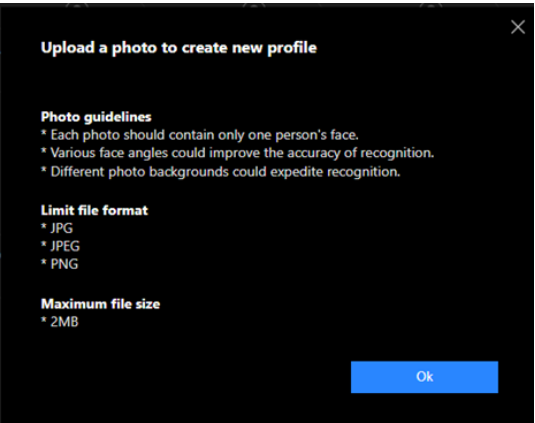
Open the VORTEX User Portal and click on the 'Profile Search' option in the left-hand menu.



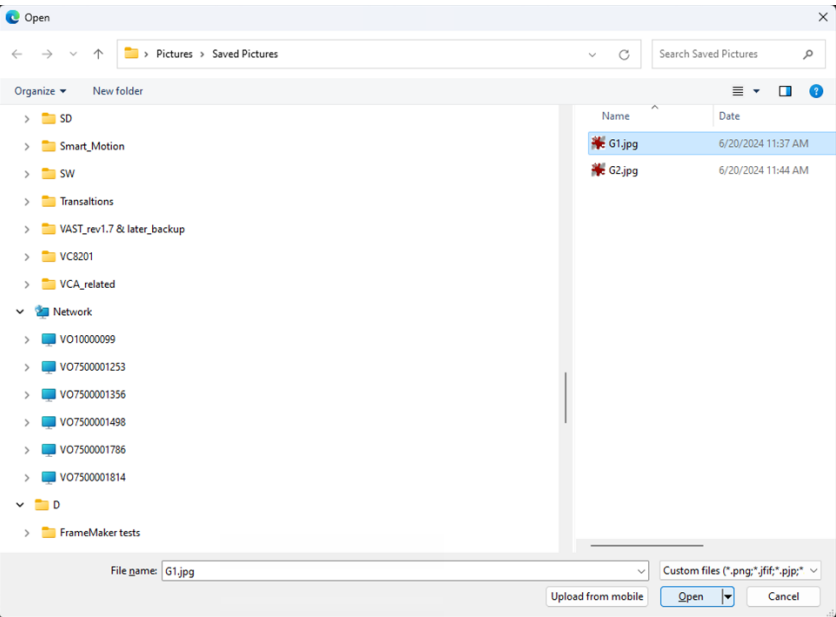
Once you're on the Profile Search page, you can create a new profile for people or vehicles by clicking on the 'Create Profile' button.

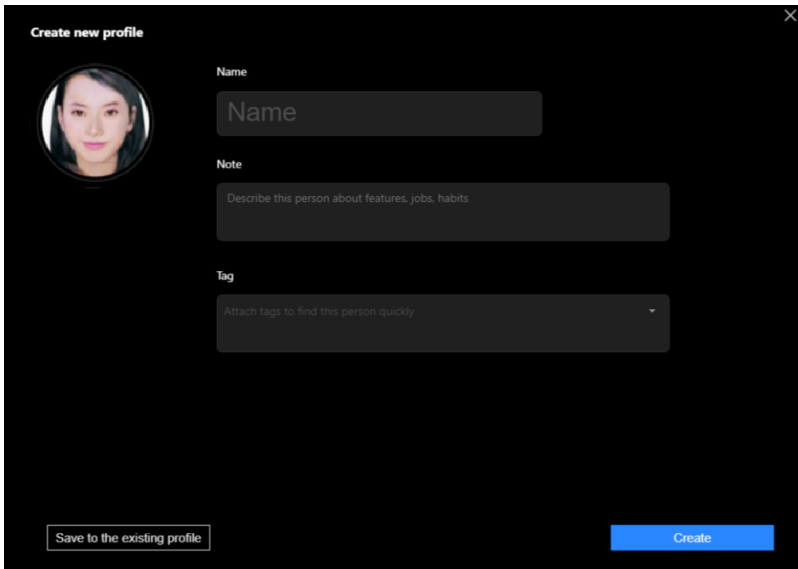


Create a People Profile



Choose a face image to upload and then fill in the Name, Note, and Tag information for the new profile.





Create new profile

Name
Name

Note
Describe this person about features, jobs, habits

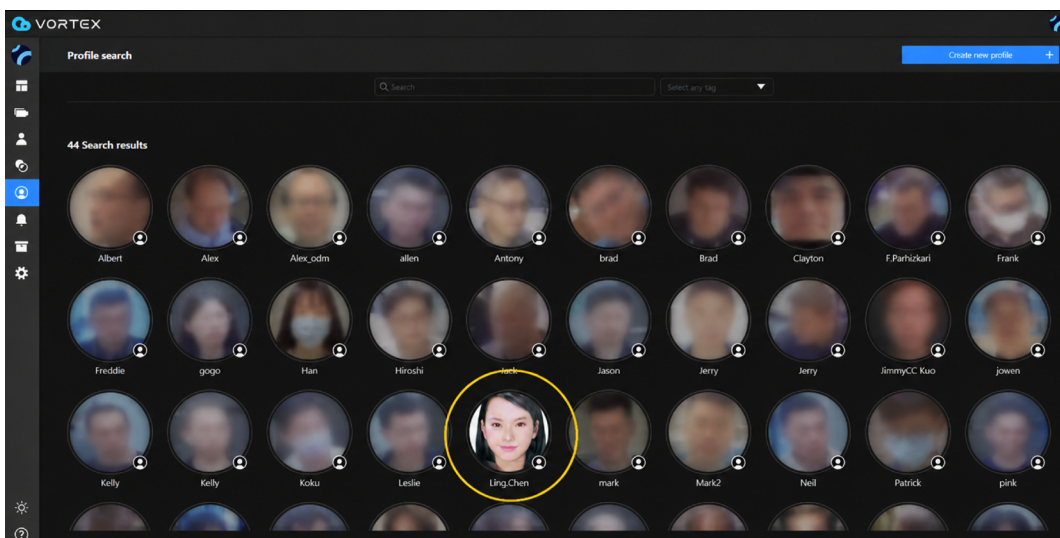
Tag
Attach tags to find this person quickly

Save to the existing profile Create

NOTE

If the uploaded image should be added to an existing profile, click 'Save to Existing Profile' instead.

Click the 'Create' button to finalize the profile. You should be able to see the new image listed in the profile search lists.



Create a Vehicle Profile

After clicking 'Create Vehicle Profile,' a window will pop up, and then fill in the Name, Note, and Tag information for the new profile.

Create new profile



License plate number

ABC1234

Note

Describe this vehicle's features, owners, and users.

Tag

Add or assign tags to find quickly

Create multiple profiles

Create

If you have more than one vehicle profile to create, please click 'Create multiple profiles' in the lower-left corner. Fill in the tags, license plate, and notes, then click 'Create' to save your changes.

Create multiple profiles

Multiple profiles

Add or assign tags to find quickly

Profile list

#01	License Plate	Note
#02	License Plate	Note
#03	License Plate	Note
#04	License Plate	Note
#05	License Plate	Note
#06	License Plate	Note
#07	License Plate	Note

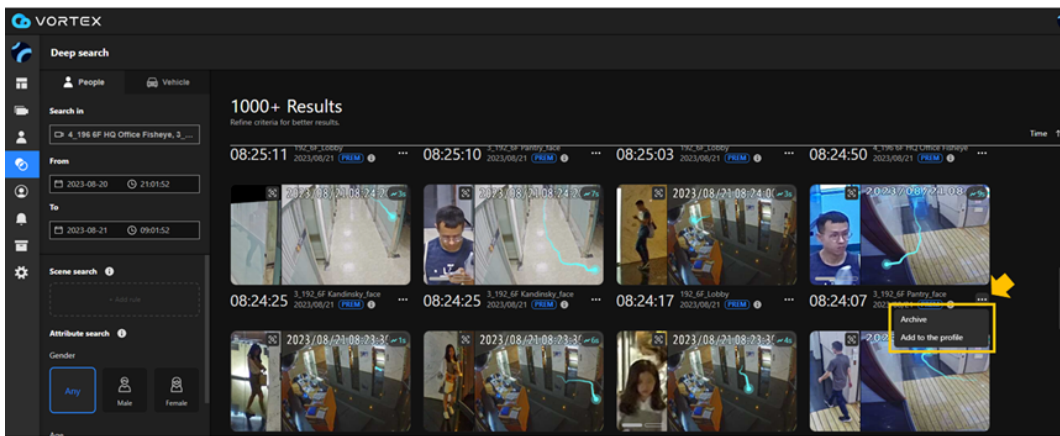
Create single profile

Create

Please note that the license plate is a unique identifier; only one profile can be created per plate number.

Create a New Profile or Add to an Existing Profile Through Deep Search

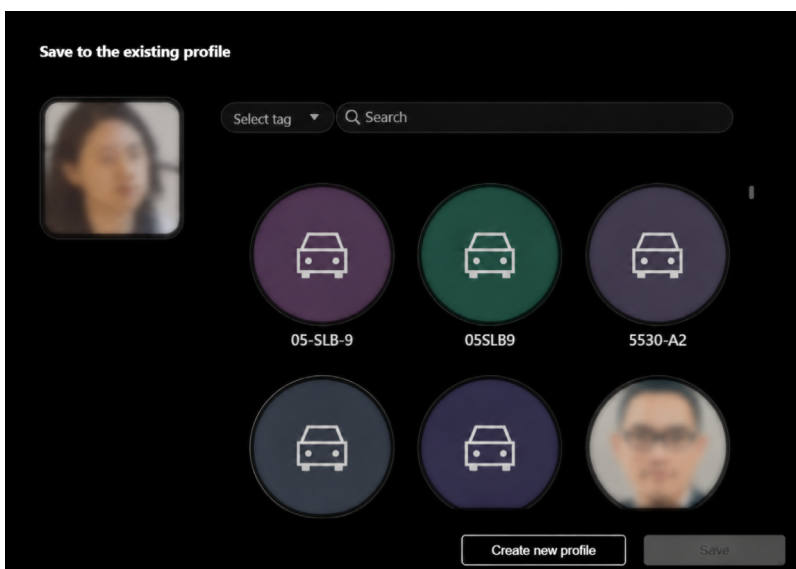
Another way to create a profile is through Deep Search results. When a person or vehicle of interest is found, click the ... icon on the search result card and select **Add to Profile**.



How to Search

You can then:

- **Create a New Profile** using the selected face image or license plate.
- **Add to an Existing Profile** by selecting a previously created profile from the list.

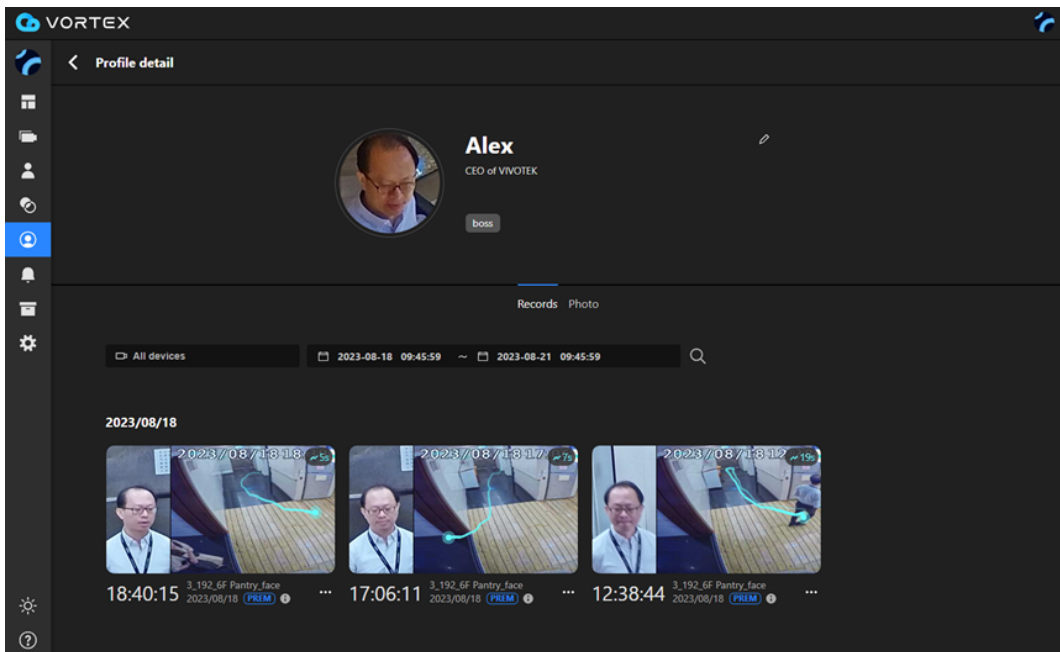


After creating a profile, users can search for a person using the face images stored in that profile in the recorded videos.

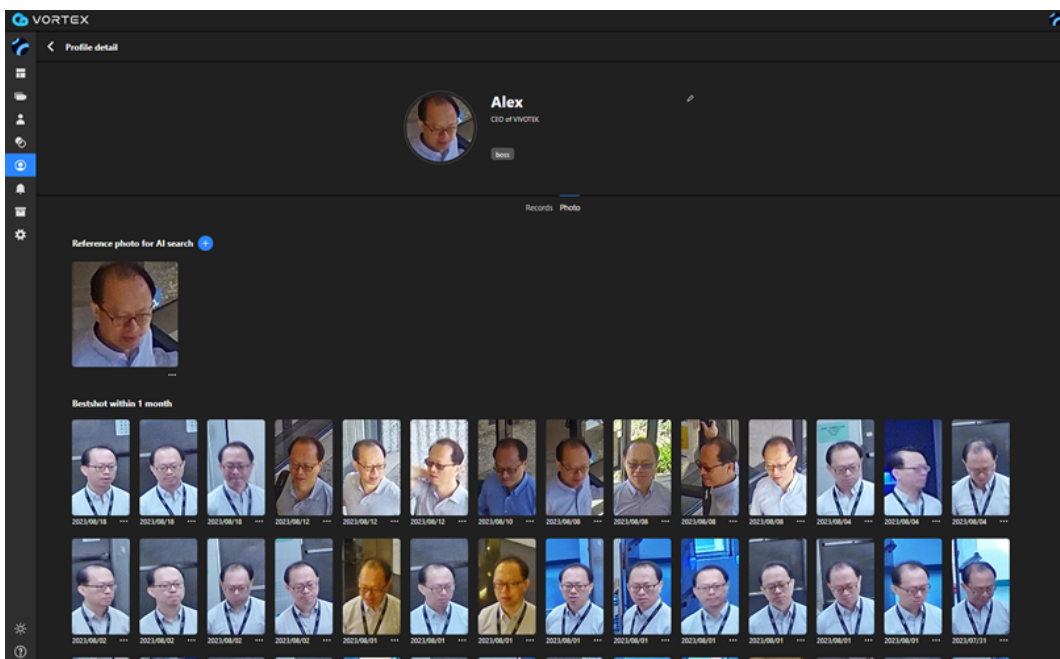
Records

If you go to Profile Search > Profile detail and click on the "Records" tab, you will be able to perform a search based on specified conditions such as which cameras to use and what time period to search.

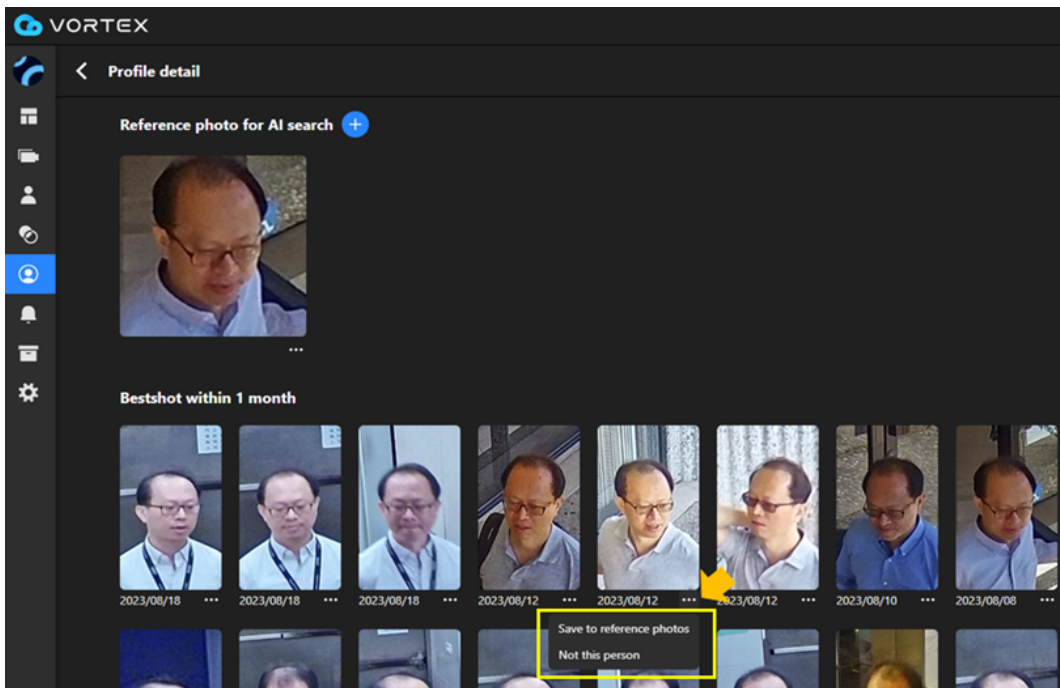
It is similar to the Re-Search function (search by an image) in Deep Search, while in Profile Search, multiple face images in a profile can be used together for the search, and the face image can be a photo uploaded by a user from a computer.



When users click the 'Photo' tab within a profile, the best facial shots of a person or license plate of transportation within a month are searched and displayed.



When clicking on the '...' icon under any of the photos displayed, you will see two options: 'Save to reference photos' and 'Not this person.' Please note, **these two functions are only supported for people profiles.**



Save to reference photos: Use the 'Save to reference photos' option when you see a photo that accurately represents the person in the profile. By doing so, this image will be added to a set of reference photos within that profile. You can save up to 6 different reference photos in a single profile to improve the accuracy of future searches.

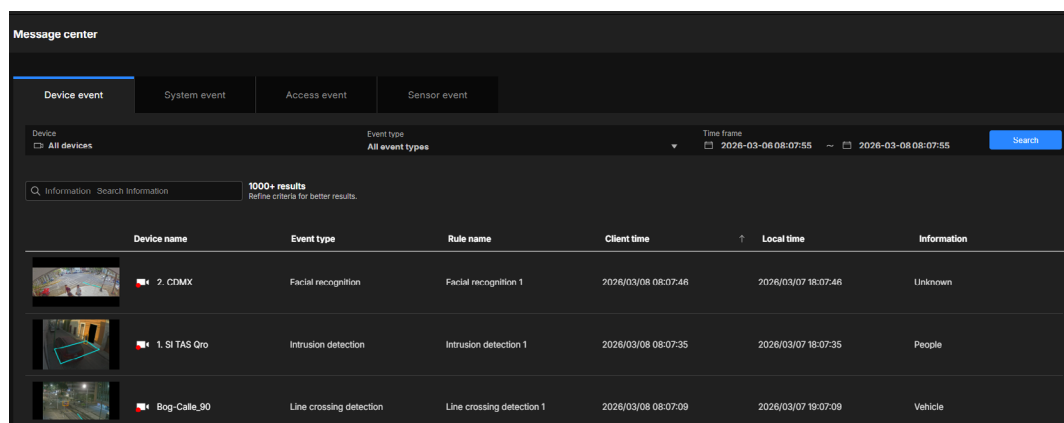
Not this person: If you notice that one of the 'best shots' does not actually match the person in the profile, you can select the option 'Not This Person'. When you do this, the system recognizes the mistake and initiates a new search, using your feedback to refine its search algorithms.

By managing your reference photos and providing corrective feedback, you contribute to the system's learning and help improve the accuracy of future searches.

On the Records tab, use the device and time frame column to start your search for this person based on the profile photos. On the Photos tab, you can add maximum 6 reference photos to help make profile searches.

Message Center

The message center serves as a hub for viewing past events. The message list will only include events associated with pre-configured triggers: Device, System, and Access Control. Once you set the search criteria based on triggers, click the blue Search button to get the search results.



Event Type

The following four event types can be used as search conditions:

- Device event: general event of camera and NVR as well as VCA event.
- System event: general system event of camera and NVR regarding to the online status, recording error, etc.
- Access event: integration event of access control devices.
- Sensor event: integration event of smart sensor.

Event List

Type	xLite	xStd	xPro
Device	AI: intrusion, loitering, line crossing, missing object, unattended object General: audio detection, camera DI/ DO, tampering detection, PIR	AI: intrusion, loitering, line crossing, missing object, unattended object, PPE detection, fall detection, face detection, crowd detection, running detection, restricted zone detection, parking violation, smart tracking an object, motion detection, license plate recognition, facial recognition General: audio detection, camera DI/DO, tampering detection, PIR	
System	Device online/offline, firmware update failed, recording error, SD card error, SD card life expectancy, disk failure, disk full, system DI/DO, PoE error		
Access	N/A	Access denied, access granted, door held open, door forced open, REX unlock, remote unlock, force open/close, door/ elevator/ place lockdown, schedule started/ended, scheduled override, reader/ controller tempered	
Sensor	N/A	Vaping: vape detection, THC detection, smoking detection, air masking detection Safety and security: help sounds, aggression sounds, gunshot detection, loud sound, motion detection, high occupancy count, light level, panic button, device tamper Health: temperature, humidity, health index, air quality index, CO/CO2, TVOC, PM1/PM2.5/ PM10, NO2/NH3, pressure	

Search Filter

1. Device: Select which device group(s) you want to filter events for
2. Event type: Select the event types (generated from cameras or NVRs) you want to see when reviewing the filtered videos.
3. Associate group (for access and sensor event only): Select the group to which the access control device belongs.
4. Time frame: Set a specific time range to narrow down or widen your search results.

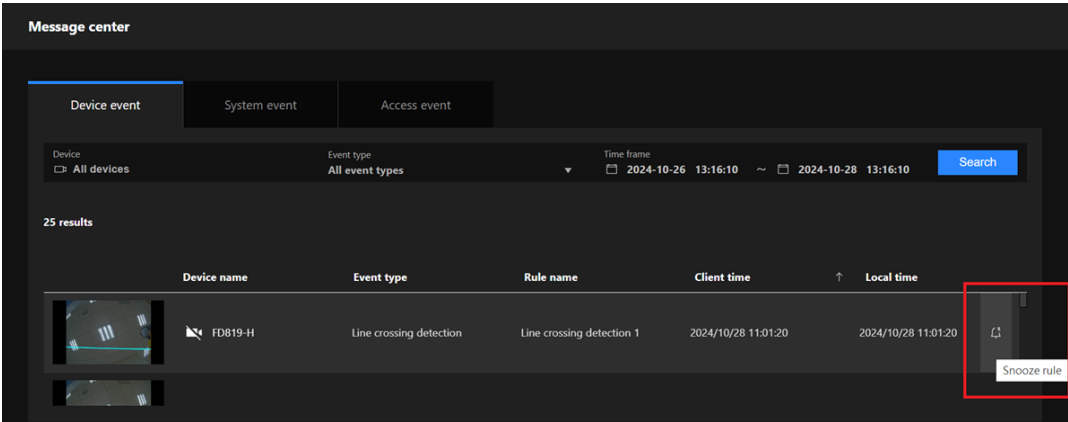
NOTE

- In the search results, you can click any item to view the associated video and other details (as shown on the right). Also, you can click the Archive button to save the video. So, later you can go to the Archive tab to see all archived video in a more organized way.
- Client time means the system time when the event happened. Note that the client time, though equal to local time, may have time difference.
- Local time means the local system time when the event happened. There is only one local time, but it may be equal to many client time (depending on the region where you access the VORTEX system.)

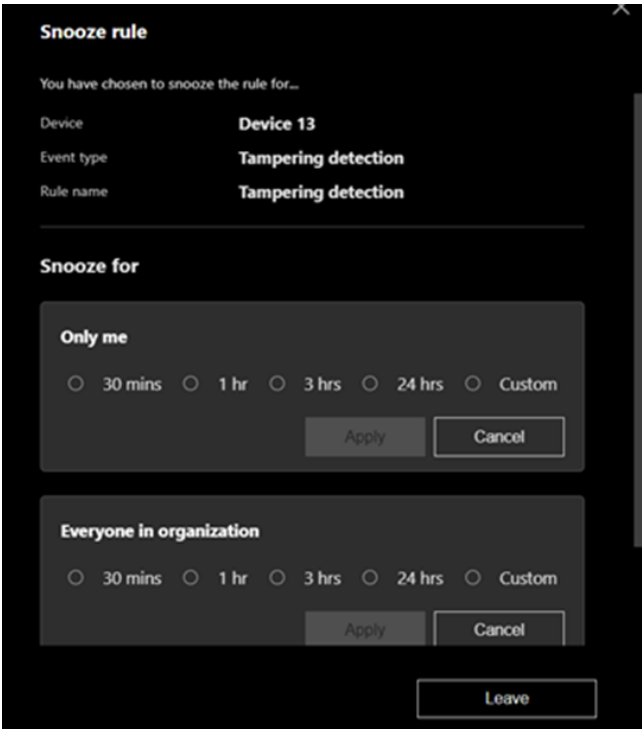
Snooze Single Rule

[Web Portal]

Simply navigate to the rule you wish to snooze, a snooze button will be there for you.



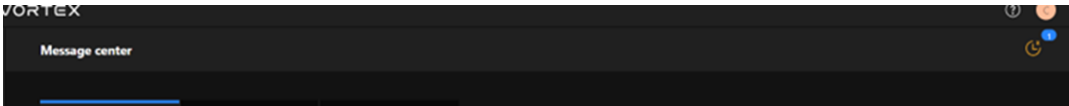
Once you go into snooze rule setting, you will have the option to set schedule, to choose whether to snooze the alarm just for yourself or the entire organization.



Once a rule is snoozed, the notification will be suspended. You still can see the logs in message center, what is snoozed is “alarm notification itself”.

Role “supervisor” and up have the authority to snooze a rule for the entire organization.

On the upper right corner of message center, you can find all the rules that have been snoozed that affected you, including the rules that set snooze for entire organization by other users.



[App]

Same as web portal, it is located within the message tab. Here you can manage the rule you wish to snooze, and view the list of rules snoozed by you and by others in the organization.

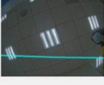
Message

Device

System

Access

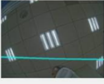
Filter



Line crossing detection
FD819-H

2024/10/28 11:01:20





Line crossing detection
FD819-H

2024/10/28 10:28:45





Line crossing detection
FD819-H

2024/10/28 10:09:52

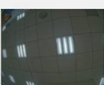




Line crossing detection
FD819-H

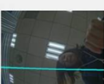
2024/10/28 10:02:46





Tampering detection
FD819-H

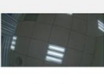
2024/10/28 10:00:46



Line crossing detection
FD819-H

2024/10/28 09:59:37





Line crossing detection
FD819-H



View

Deep search

Message

Archive

×

Snooze rule

You have chosen to snooze the rule for...

Device

FD819-H

Event type

Line crossing detection

Rule name

Line crossing detection 1

Snooze for

Only me

+

Everyone in organization

Snoozed until 2024/10/28 16:27:32

Edited by: Sasha.wu

This will only snooze the notifications (App and emails) for this rule, but the event will still be recorded in the Message Center.

Archive

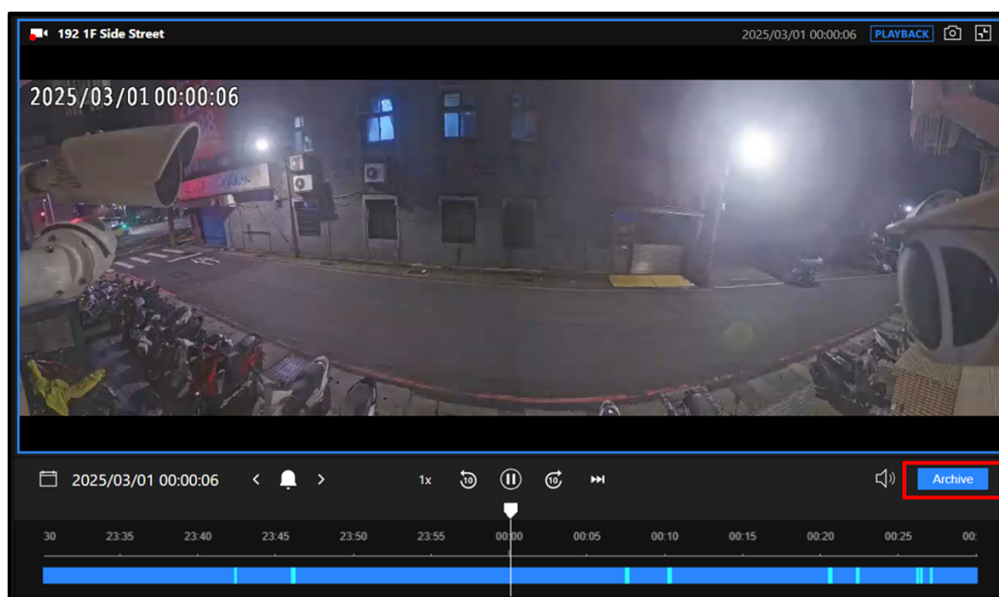
[xStd and xPro only]

You can create an archive file to store key moments in the VORTEX cloud for easy access in the future. This allows for quick review or reducing the time spent searching again later.

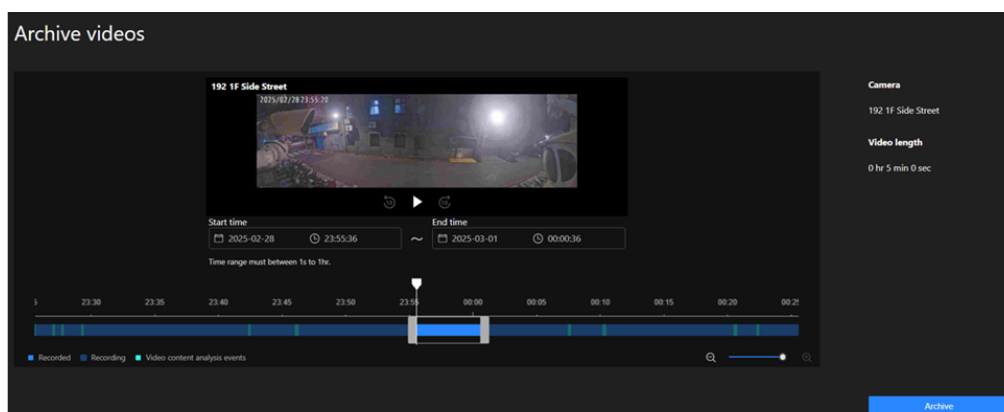
Create Archived Video Clips

The archive feature is available on different pages on the portal, including View, Message Center, and Deep Search. The creation process is the same across these pages. Below is an example of how to archive a file in View.

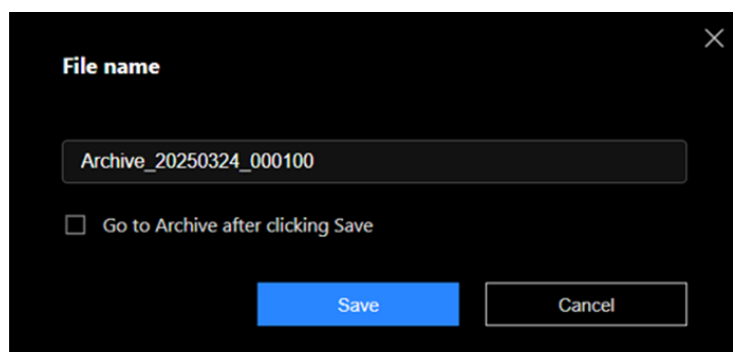
1. Click "Archive"



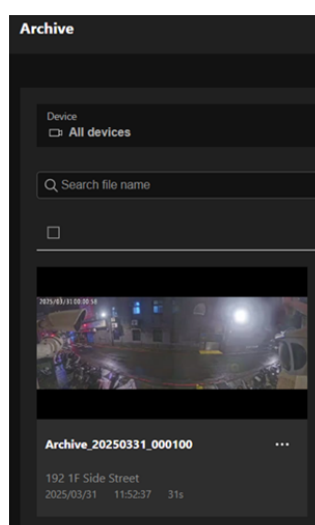
2. Set the start and end time for the key moment to create the archived file. The duration can range from 1 second to 1 hour. Beside using the date time picker, you can also adjust the interval in the timeline to select the time range. After selecting the time range, click "Archive".



3. Edit the file name (optional). If you want to be directed to the Archive page automatically after saving, check "Go to Archive after clicking Save".

A dark-themed dialog box titled "File name" with a close button (X) in the top right corner. It contains a text input field with the value "Archive_20250324_000100". Below the input field is a checkbox labeled "Go to Archive after clicking Save", which is currently unchecked. At the bottom are two buttons: "Save" (highlighted in blue) and "Cancel".

4. Go to the "Archive" in navigation menu and you will find the file.



NOTE

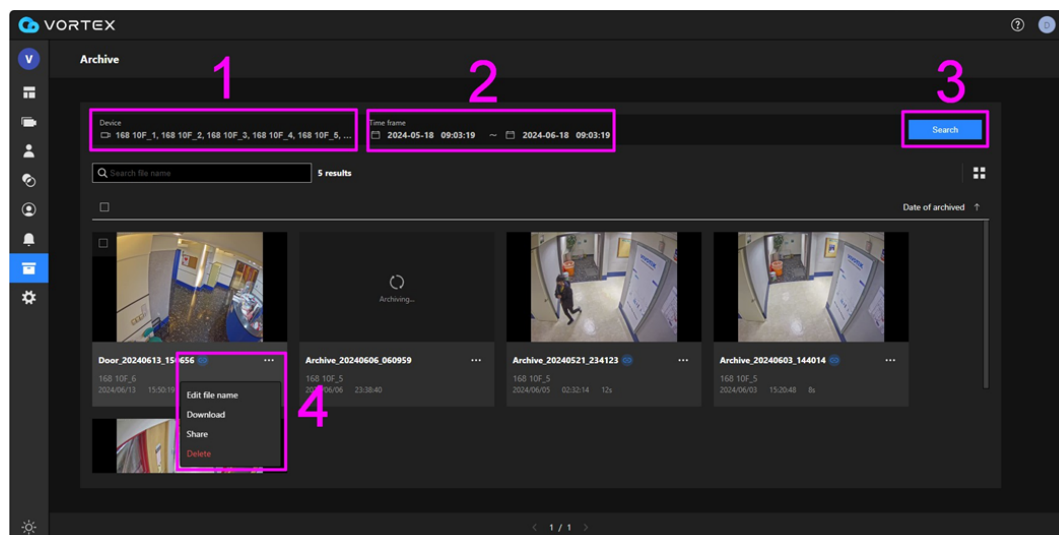
VORTEX Apps also support create archive file. Click the **Archive** icon (📁) to start the creation process on View, Deep Search and Message page.

Search Archived Video Clips

The Archive page is your gateway to accessing and managing the video clips saved from your VORTEX cloud. There are three ways to search for archive video clips:

1. Search by cameras and time:

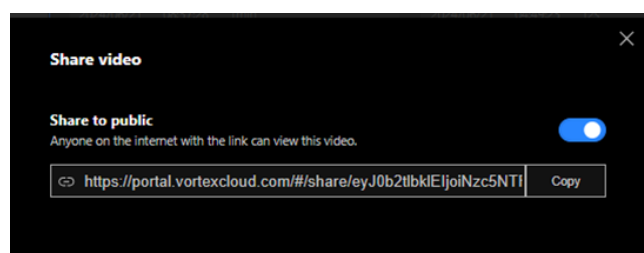
Click the "All devices" button to select cameras, and set the time frame. Then, click the "Search" button.



Example of search results

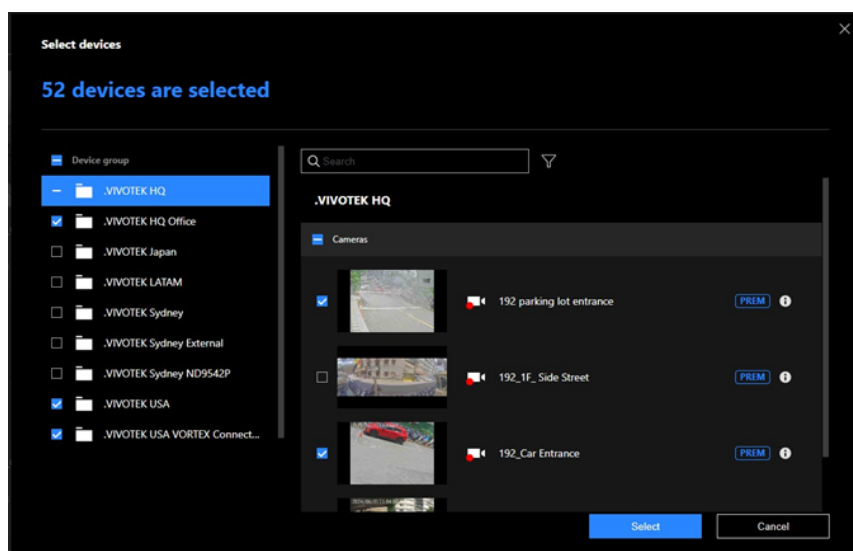
Once you have found the archived video you're looking for, you can click the "..." icon in the video cell. This will pop up a window that allows you to edit the file name of the archived video, download the video directly to your computer, share the video, and delete it.

For example, if you want to share a video, click the "..." icon > Share in the selected video cell. This will pop up a window that allows you to turn on the sharing option and let you copy the link to share with others.



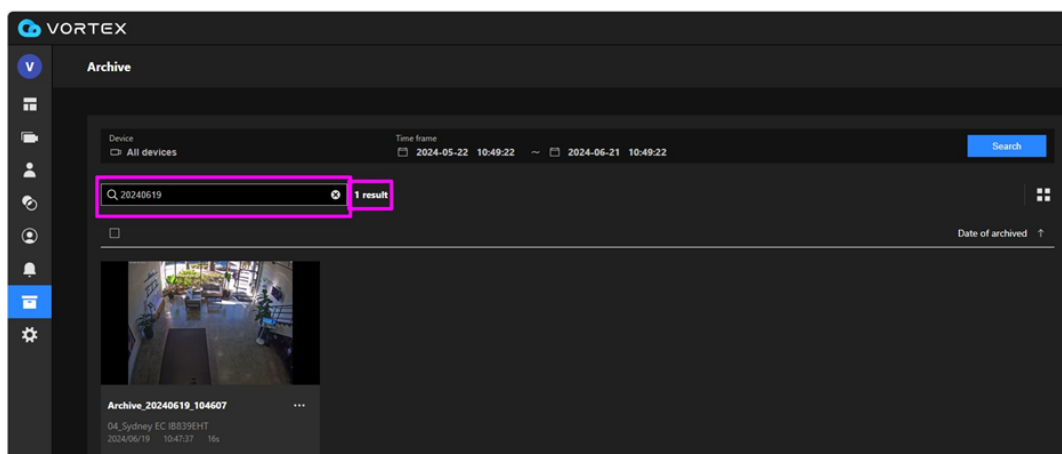
2. Search by camera(s) in group(s):

If you're looking for archives from specific cameras, start by clicking the camera box in the upper-left corner. This brings up the camera selector. Click "Groups" from here to see a list of your camera groups. Simply select the cameras from which you wish to view archives.

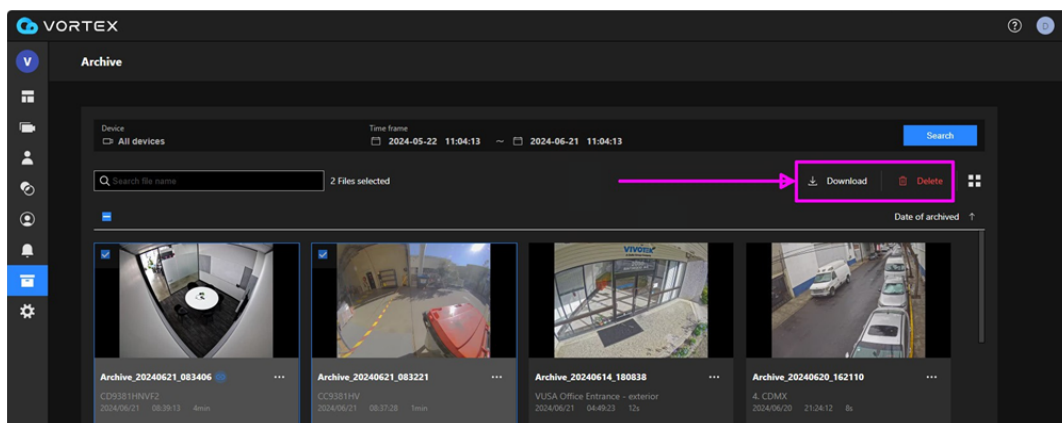


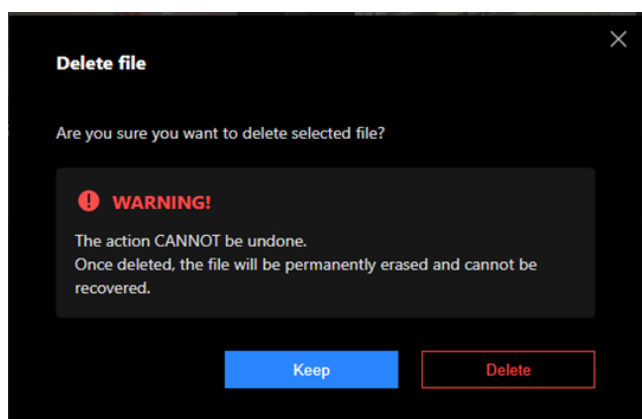
3. Search by video file name:

In the Search box, enter a keyword of the file name you are looking for to narrow down the search results.



In addition, in the search results, if you click one or more video cells. Another two options "Download" and "Delete" will appear. You can download videos as needed and/or delete video(s) with caution.

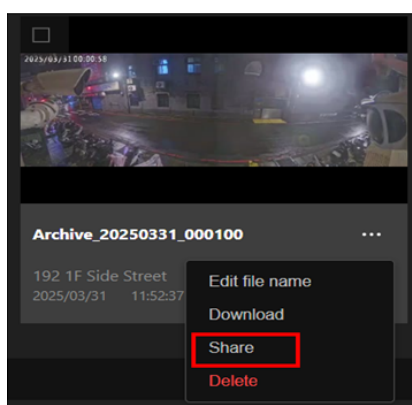




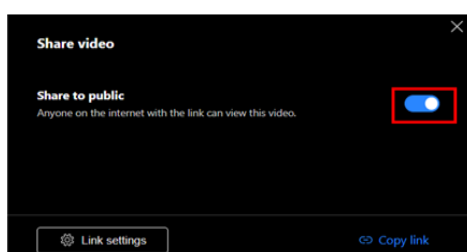
Sharing Archived Files

You can share an archive file with someone outside your organization to help them review important moments. Please follow the steps below:

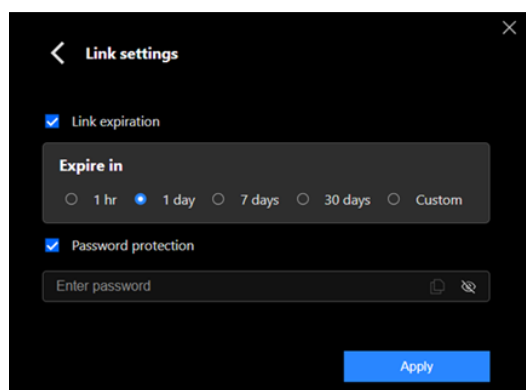
1. Go to the **Archive** page
2. Locate the archive file you want to share and click the **More** icon (...).
3. Select **Share**.



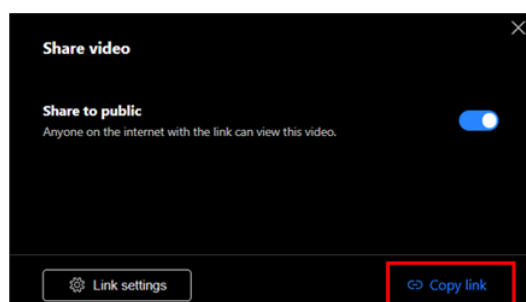
4. A configuration window will appear.
5. Toggle the **Share to public** switch to enable sharing. A shareable link will be generated.



6. Click **Link Settings** to set a **password** and **expiration date** for the link. You can also enable the permission to allow viewers to download the file to their local system.



7. **Copy link** and send it to the external party.



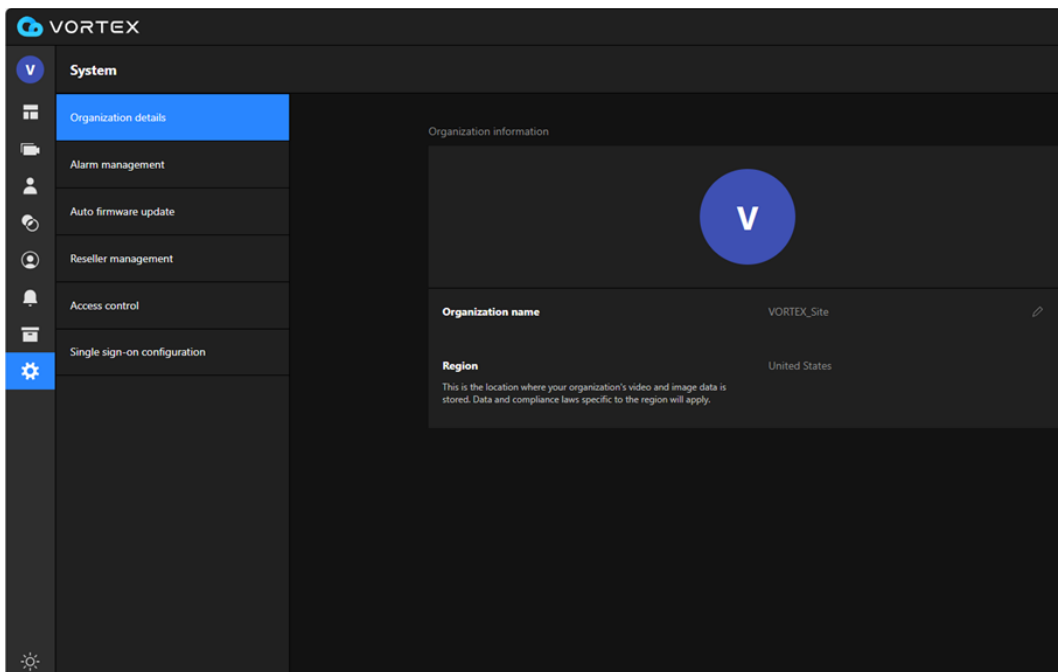
NOTE

The share link for the same archive file is **shared across your organization**. If someone else updates the link settings, it will affect all users accessing that link.

This section lets you manage system-related settings such as organization information.

Organization Details

You can change your organization name here if you are an organization owner, administrator, or supervisor. In addition, only the VORTEX organization owner can transfer ownership to another user and can delete the organization when all devices are deleted.



Alarm Management

If you are the owner or an administrator and you need to be notified of certain activities such as VCA events and device status, please click the "Add alarm" button and set up the following five steps:

1. Select the event(s) and issue(s) you want to be notified of, and then click NEXT.

Events

Select which event types that will trigger an alarm

Device events

> ☐ Video Content Analysis event

▼ ☒ General event

- ☒ Audio detection
- ☒ Camera DI
- ☒ Tampering detection
- ☒ Camera DO (NVR)
- ☒ PIR (NVR)

For device events to be in effect, you will have to configure them within each camera's settings.

System events

> ☐ General system issues

▼ ☒ Camera system issues

- ☒ Recording error
- ☒ SD card error
- ☒ SD card life expectancy

Next

2. Select the source(s) to trigger the alarm, and then click NEXT.

Sources

Select which sources will trigger an alarm

Choose sources that initiate Device & System events

NVR & Camera [Select sources](#)

.VIVOTEK HQ Office

- 168 10F_1
- 168 10F_2

Choose sources that initiate Access events

Door [Select sources](#)

Next

3. Select the actions(s) the alarm will trigger, and then click NEXT.

4. Select the time frame the alarm is on.

5. Check if all the items you select are correct. If yes, click Add.

EventsSourcesActionsScheduleSummary

Summary

This is a brief summary of your alarm, you can also give your alarm a desirable name.

Alarm name

Alarm 68

Events

Audio detection

Camera DI

Tampering detection

Camera DO

PIR

Recording error

SD card error

SD card life expectancy

Sources

.VIVOTEK HQ Office

Actions

Send email

Audio deterrent

Schedule

Day and time

Sun

Mon

Tue

Wed

Add

Now, you can move the slider (ON/OFF) to decide whether to enable the alarm you just created.

VORTEX

System

Organization details

Alarm management

Auto firmware update

Reseller management

Access control

Single sign-on configuration

Alarm management

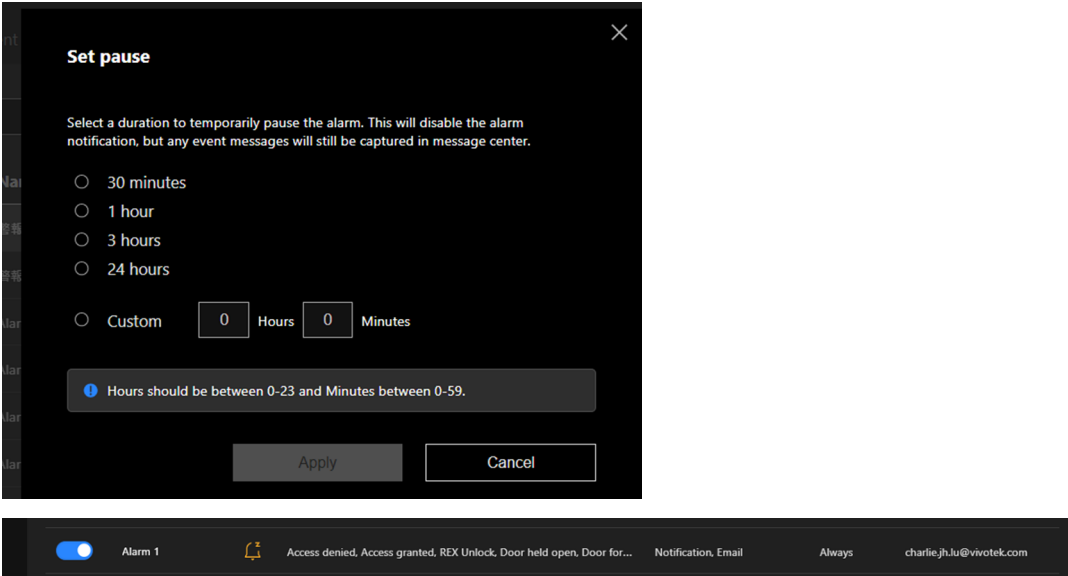
Add alarm +

Search

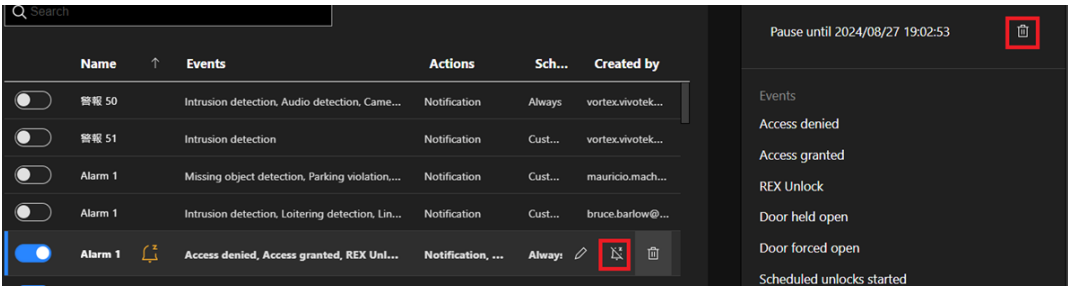
	Name	Events	Actions	Schedule	Created by
☒	Alarm 57	Intrusion detection, Loitering detection, Line crossing detec...	Notification	Custom	vivotek.com
☐	Alarm 59	Intrusion detection	Notification	Custom	@vivotek.c...
☐	Alarm 60	Intrusion detection, Line crossing detection	Notification	Custom	@vivotek.c...
☐	Alarm 61	Line crossing detection	Notification	Custom	@vivotek.c...
☐	Alarm 62	Intrusion detection	Notification	Custom	@vivotek.c...
☒	Alarm 63	Intrusion detection, Loitering detection, Line crossing detec...	Notification, Webhook	Always	otek.com
☒	Alarm 66	Intrusion detection, Loitering detection, Line crossing detec...	Notification, Email	Always	@vivot...
☒	Alarm 67	Audio detection, Tampering detection, Camera DO, PIR, Ca...	Email	Custom	@gmail.com
☒	Alarm 68	Audio detection, Camera DI, Tampering detection, Camera ...	Email, Audio deterrent	Custom	@gmail.com
☐	Alarma Demo Rosarito	Camera DI, Device offline, Loitering detection	Notification, Email	Always	@vivi...

Snooze the Alarm

You can snooze an alarm for a specified period, during which notifications for that alarm are disabled. By clicking the icon , you can set the snooze duration. An indicator shows which alarms are currently snoozed.

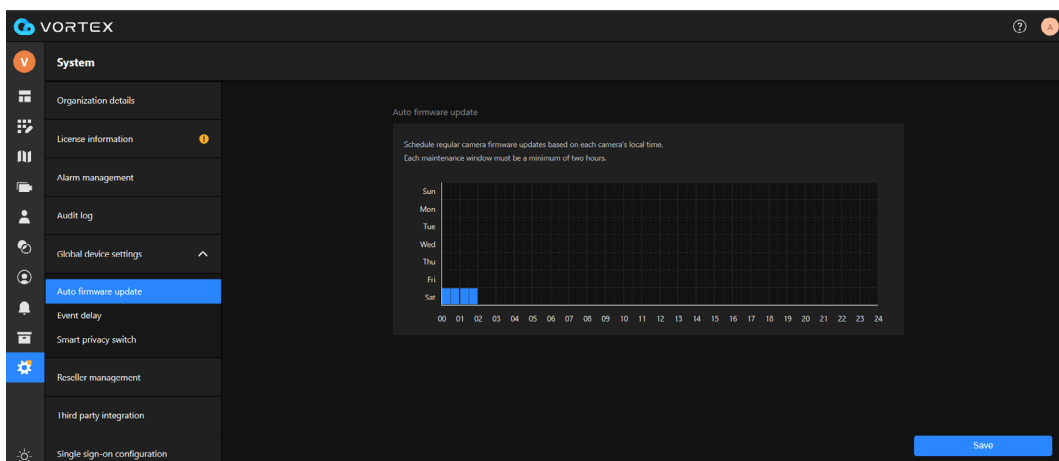


If you would like to resume the alarm before the schedule up, you can manually stop the pause using the same snooze icon or from the right panel.



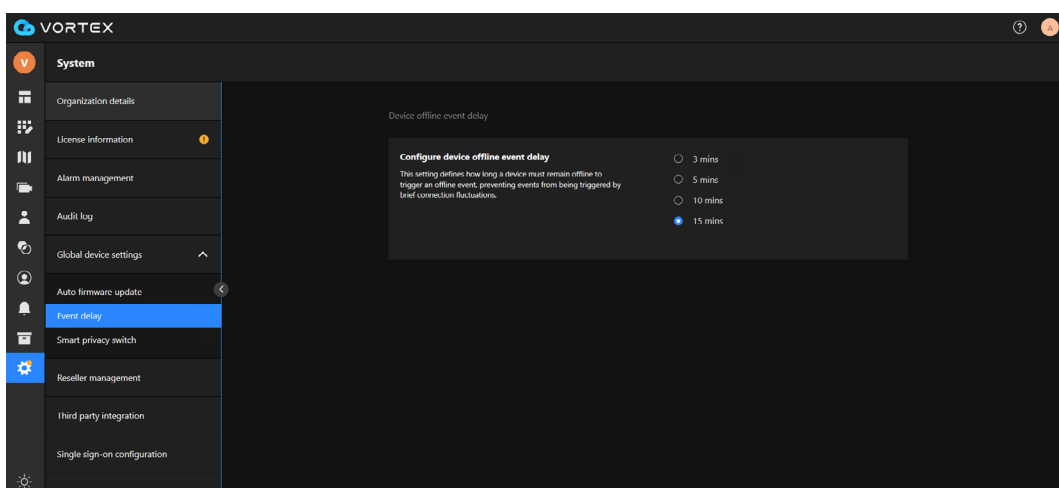
Global Device Settings > Auto Firmware Update

VORTEX can automatically push firmware updates to your devices on a regular basis based on the schedule you set (minimum two hours per update session). Note that only direct to cloud camera and NVR can have the auto firmware update.



Global Device Settings > Event Delay

The **Event delay** setting controls how long a device must remain offline before VORTEX generates a **Device Offline** event. This delay helps prevent unnecessary alarms caused by brief network interruptions or temporary connectivity fluctuations.



By increasing the delay, short disconnections are ignored, reducing false offline notifications. Conversely, selecting a shorter delay allows administrators to be notified more quickly when a device becomes unavailable.

Available options:

- 3 mins – Fastest detection of offline devices.
- 5 mins – Suitable for environments with stable network connections.
- 10 mins – Provides a balance between responsiveness and false alarm prevention.
- 15 mins – Recommended for networks where occasional short disconnections are expected, minimizing unnecessary offline events.

Global Device Settings > Smart Privacy Switch

The Smart Privacy Switch feature enables users to activate AI-based surveillance features such as Facial Recognition (FR), ensuring compliance with local regulations regarding data privacy.

How it works:

When the feature goes live, the Owner or Admin of the organization will be prompted to sign an agreement upon their first login to the VORTEX portal or app. This ensures that the user is informed about the AI functionalities and their compliance with privacy regulations in their jurisdiction.

Usage:

Once the agreement is signed, users can enable or disable these AI features based on local legal requirements and their specific needs. This will help ensure that the use of AI-driven surveillance is carried out within the legal framework for their region.

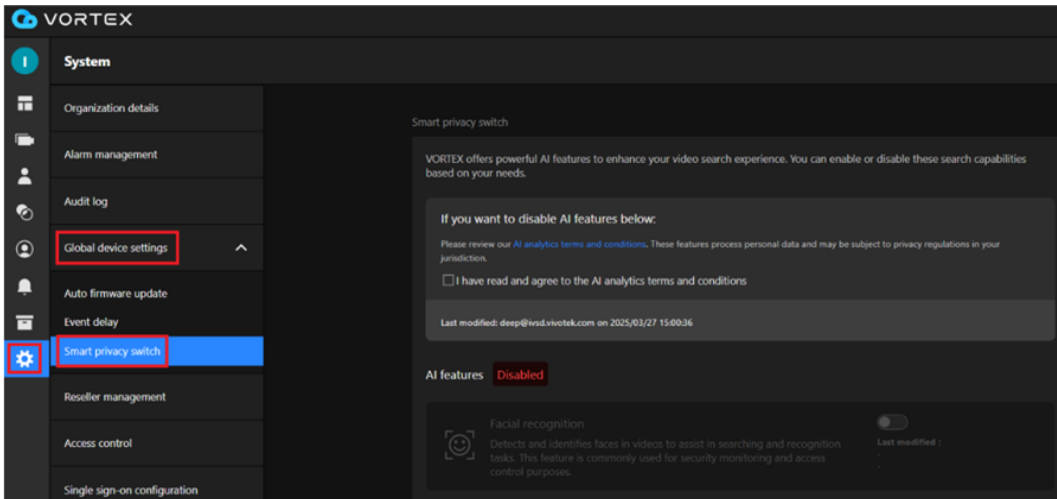
NOTE:

- Upon first login, the Owner or Admin will see a **pop-up** notification asking them to review the **AI Analytics Terms and Conditions**.
- After reviewing the terms, the user must check the box confirming they have read and agree to these terms.
- Users can then toggle the **AI features** ON or OFF according to their needs and legal requirements.

Feature location and its functionality

• Location in Portal:

The Smart Privacy Switch feature can be found under the **System/Global device settings/Smart Privacy Switch** section in the portal. This section allows the user to review and activate the AI functionalities related to Facial Recognition and License Plate Recognition.



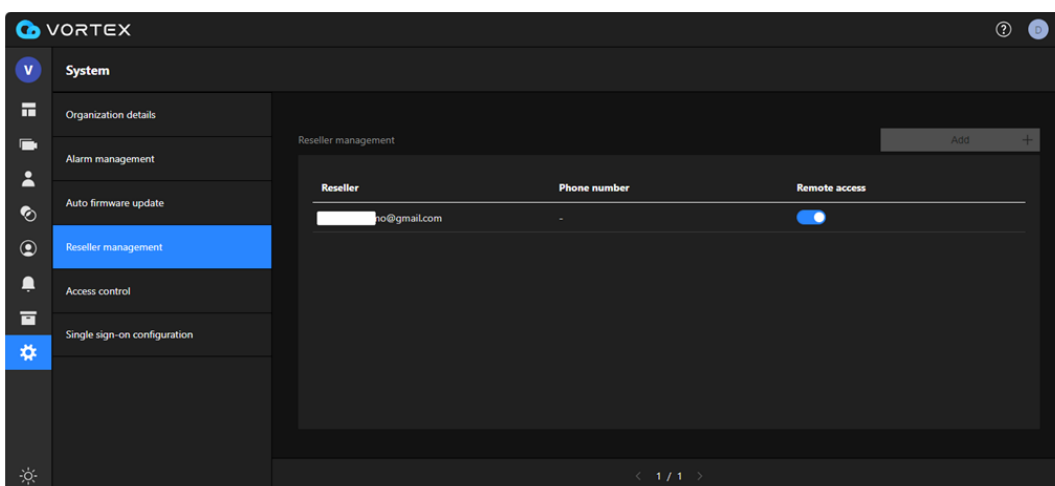
Impact of Disabling Facial Recognition

When **Facial Recognition** is disabled, the organization will no longer receive facial-related data. The affected areas are as follows:

- **Live View:** Facial recognition will not be performed to distinguish between known and unknown users.
- **Device:** Premium devices will not be able to set up facial recognition rules, and this feature will be hidden.
- **Profile Search:** Any existing profiles will be deleted, and the Profile Search functionality will no longer be available.
- **Message Center:** No facial recognition-related event logs will be generated.
- **Alarm Management:** Since facial recognition is disabled, the configured alarm rules will have no effect.

Reseller Management

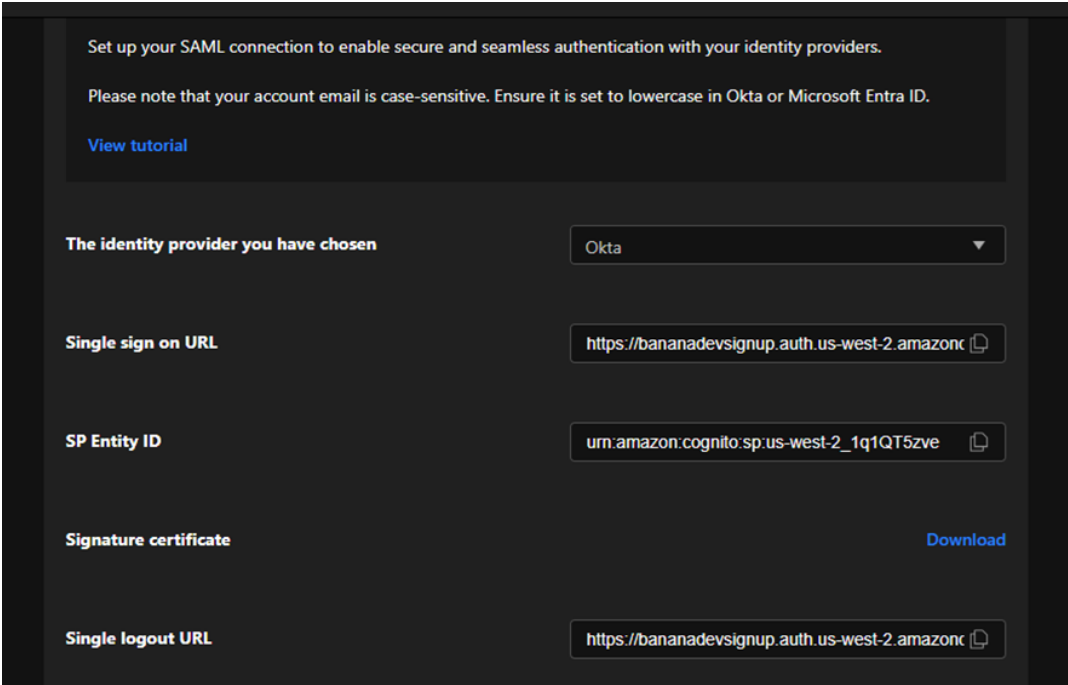
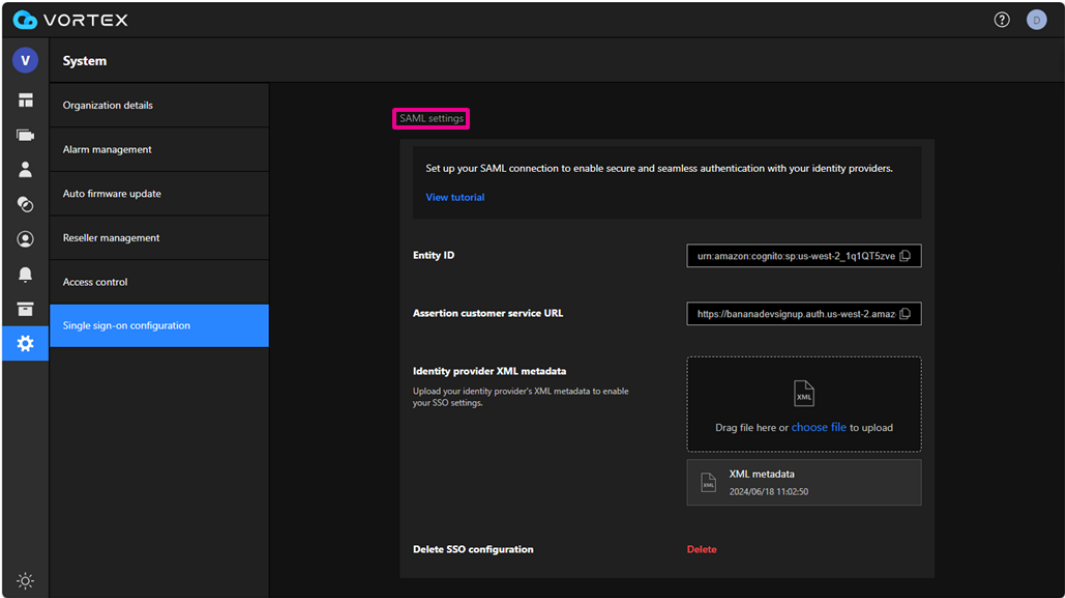
Here, you can add your service provider and decide whether to grant them remote access.



Single Sign-on Configuration

Microsoft Entra and Okta

Single Sign-On (SSO) is a solution for verifying user identity and increasing the user convenience by not having to remember lots of different user IDs and passwords for various websites or locations with security control. Also, the owner, administrator, or reseller should perform this function to ease their burden on access control. For details on how to set up, click View tutorial.

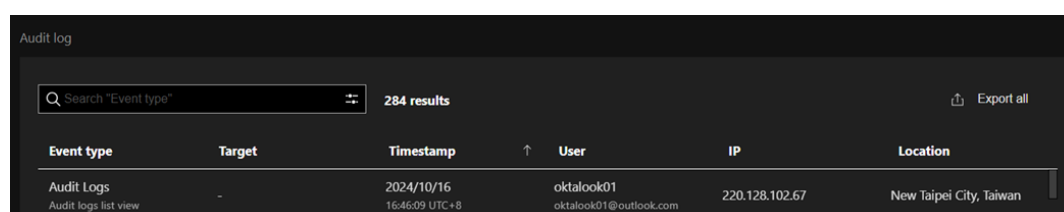


Audit Log

Audit log tracks the activities within the organization, for example, access to the organization, viewing logs and user setting management. The log will be accessible to users for up to one year.

Logs will include specific information, such as: timestamp of when the action took place, IP address and location of the user who performed the action and username/e-mail of the user who performed the action.

Only owner and administrator role can access audit logs.



Event type	Target	Timestamp	User	IP	Location
Audit Logs Audit logs list view	-	2024/10/16 16:46:09 UTC+8	oktalook01 oktalook01@outlook.com	220.128.102.67	New Taipei City, Taiwan

Organization-Level Multi-Factor Authentication (MFA)

As an owner or administrator in your organization, you can enable organization-level MFA to require all users in your organization to use MFA.

Here are the configuration steps on VORTEX portal:

1. Navigate to **System > Organization security**.
2. Turn on Require MFA for all users in organization and click Confirm.

NOTE

- Users who haven't set up MFA will be directed to MFA setup process on the next time they log in.
- Users won't be able to skip MFA until the organization-level MFA requirement is disabled.
- The MFA setup in VORTEX is configured solely for VORTEX account logins. If you are using SSO login and require MFA, please reach out to your SSO service provider to enable MFA for your account.

Reset MFA for a user

If a user loses their MFA access by some cases, for example, they change or lose their mobile phone, an owner or administrator can reset their MFA settings. The user will then need to set up MFA again.

Here are the configuration steps on VORTEX portal:

1. Navigate to Users and select the user needs their MFA reset
2. Click the more menu icon
3. Select Reset MFA and click confirm

License Plan

A newly created organization is automatically set to the **xLite plan** by default. It supports basic features but comes with certain limitations.

The upgrade from xLite to the **xStd or xPro plan** happens automatically in either of the following cases:

1. When an xStd or xPro camera license is activated for a channel in the organization.
2. When a bundle camera is added to the organization.

Organizations on the **xStd or xPro plans** unlock advanced features such as AI Hub, Archive, and Cloud Backup. The transition is fully automatic and happens within the same organization, so there's no need to recreate or move devices manually.

Likewise, VORTEX also provides an option for users to switch back to the **xLite plan** if preferred.

Pre-bundle kit

To simplify onboarding and ensure a seamless out-of-the-box experience, we introduced the VORTEX Pre-Bundle Kit. Under the current flow, manually allocating licenses can be time-consuming and requires familiarity with the Reseller Portal. The Pre-Bundle Kit eliminates this extra step by:

- Eliminate the need for initial license setup
- Speed up deployment and reduce IT workload
- Giving customers immediate access to VORTEX AI features, including Deep Search
- Auto-activating a 1-year xPro license when a VORTEX Camera is added to an account

After the First Year

- Customers may renew with xPro, or choose to switch to xStd starting in the second year.
- xPro is the only option available during the first year for Pre-Bundled units.

License Types for the Organization on xStd/xPro Plan

VORTEX provides a flexible licensing framework for managing devices and cloud services. Organizations can scale their deployments as needed while benefiting from cloud management, advanced AI features, and flexible storage options.

Camera Licenses

To enable and manage your VORTEX cameras and NVR channels, a valid camera license is required. Each camera license determines the range of cloud services and features available through the VORTEX platform.

- **xStd**

xStd provides unlimited scalability, including unlimited users, channels, and sites. It also provides Cloud Archive with 5GB of storage per camera.

- **xPro**

xPro includes everything in xStd, plus an expanded Cloud Archive capacity of 30GB per camera and access to advanced AI features such as AI Hub, Deep Search, Event Insight, and Case Vault.

Network Speaker Licenses

The network speaker license enables management and speaker-specific features such as talk-down communication and audio deterrent actions for your VORTEX network speaker.

Cloud Backup Licenses

For users requiring additional data protection and extended storage retention, **Cloud Backup** is available as an add-on license for both xStd and xPro.

Cloud Backup continuously records and stores video securely in the VORTEX cloud, ensuring redundancy and quick access for event review or incident recovery.

Backup storage is available for retention periods of 30, 60, 90, 120, 180, or 365 days.

NOTE

An xStd or xPro camera license must be activated before Cloud Backup can be used.

Advanced AI Bundle Licenses

A specialized suite of analytics designed to transform your surveillance system into an automated safety supervisor. The suite includes Think Alert, PPE, Fall Detection and upcoming features with latest AI technology.

NOTE

An xPro camera license must be activated before the Advanced AI Bundle can be used.

License Information

[ and  only]

The **License Information** page provides an overview of all licenses within the organization. It allows users to quickly review license usage, including license types, quantities, and current status.

Navigate to **System > License** Information to view the page.

License Control Overview

Organization Status and Phases

License status is managed at the organization level. This means that the condition of a single camera license can impact the entire organization. If any camera is unlicensed or its camera license expires, the organization progresses through defined phases.

The first phase is the Grace Period, which lasts for 30 days. During the Grace Period, the system continues to allow access to all functions, ensuring that normal operations are not immediately disrupted. Add-on services will also remain available during this period, provided that their respective licenses are still valid. If the expired issue is not resolved within this timeframe, the organization transitions into the Renewal Overdue Period.

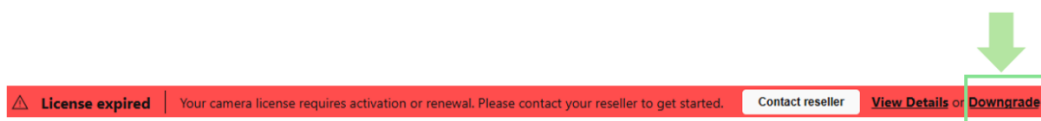
When the organization reaches the Renewal Overdue Period, main service restrictions are applied. Core functions such as Live View, Playback, AI hub, Alarms capabilities are no longer available. Cloud-based operations, including cloud upload and event processing, are also disabled. All add-on services are stopped regardless of their license status.

Add-On License Rules

Add-on licenses such as cloud backup license or Advanced AI license are managed independently from the main service timeline and do not include a Grace Period. Once an add-on license expires, the corresponding service stops immediately without any extension window.

Downgrade from xStd/xPro to xLite

The downgrade option appears once the organization enters grace period or renewal overdue phase. You can access it via the banners displayed during either phase.



When you choose to downgrade, the system will first check whether all licenses in your organization have expired. If any active licenses remain, you will not be able to proceed with the downgrade.

If all licenses are expired, a checklist will be displayed. This checklist helps you review whether your organization meets the xLite plan requirements (for example, user account limit) and guides you to make the necessary adjustments before completing the downgrade.

Please note that the actual checklist items are subject to what is shown in the system interface at the time, as the content may be updated and is not exhaustively listed in this manual.

Once all requirements are met, the downgrade process can be proceeded.

License-Required Features

This section introduces the accessory requiring the license information while using VORTEX.

Network Speaker

VORTEX supports seamless integration with VIVOTEK network speakers, currently AU-003 and AU-004. To connect these speakers to the VORTEX cloud, a VIVOTEK RX9502 is required as a bridge device, enabling cloud-based audio management.

Bridge Set-up

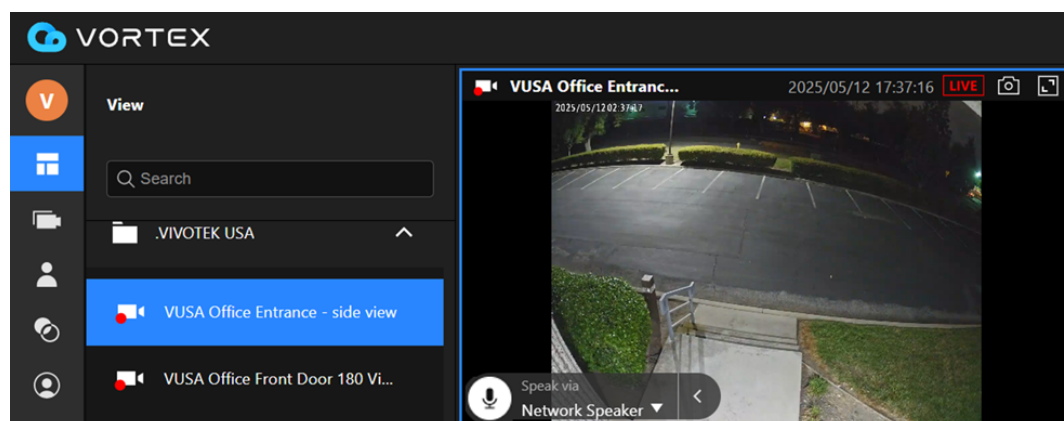
System Integrators can follow the RX9502 setup guide to update the device's firmware, converting it into a dedicated VORTEX Cloud Bridge. Once added to your VORTEX organization, the RX9502 is able to detect and bring in LAN-connected VIVOTEK speakers into the VORTEX portal.

Full Feature Unlock

With speakers paired, end users gain access to:

- Event-triggered broadcasting — play pre-loaded warning audio when VORTEX VCA detects events or other regular events
- Talk-down function — live voice communication via VIVOTEK network speakers

This integration supports typical surveillance use cases such as alerting intruders, directing crowd flow, and assisting emergency response. VIVOTEK speaks to VORTEX's intelligence-led approach to proactive deterrence.



Why It Matters

1. Automated Deterrence

Speakers react immediately to VCA events —like intrusion or loitering—without manual intervention.

2. Operational Efficiency

Automated messaging cuts reliance on onsite staff and standardizes responses .

3. Emergency Management

During crises, such as evacuations or security breaches, speakers can deliver timely instructions—vital for crowd control and safety

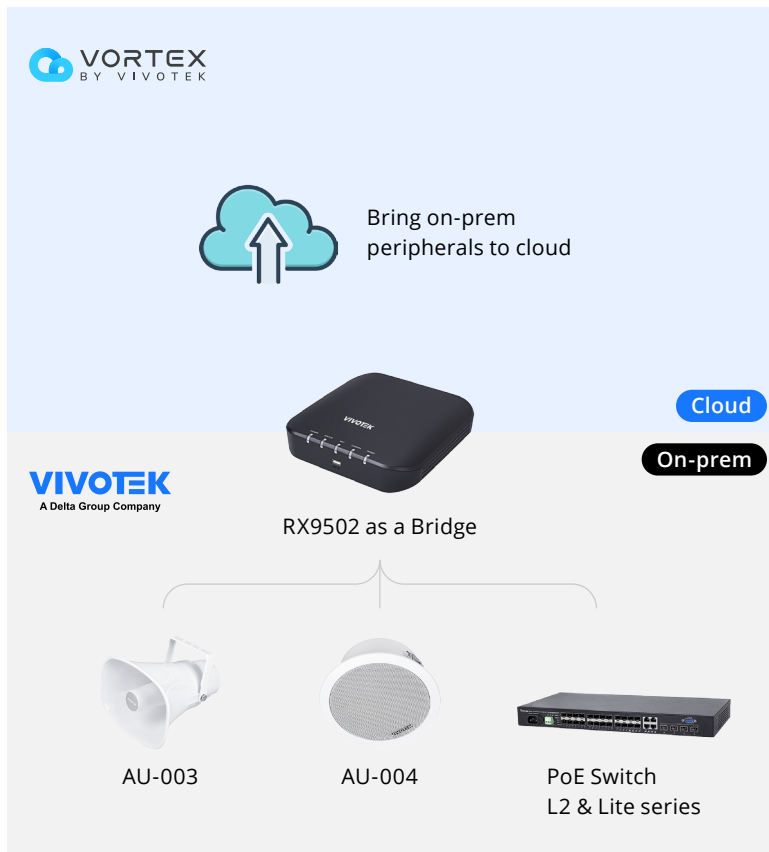
Resources & Further Reading

- **Notification:** Once the RX9502 is converted to a VORTEX Bridge via firmware update, its original video receiver functionality will be disabled. Please take this into consideration before purchase and deployment.
- **Setup Guide:** Refer to the official VORTEX Network Speaker Setup Guide on [VORTEX reseller portal](#) for the firmware upgrade SOP and the bridge setup. Or check the [set-up document](#).
- **Feature Insights:** See our feature article [Top 5 Reasons to Install Network Speakers with VORTEX](#)
- **Real-world case:** [Smart Surveillance: VORTEX's AI Detection and IP Speaker Deter Suspicious Activity](#)

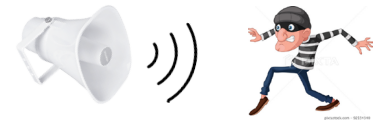
Device Models

- **AU-003:**
https://www.vivotek.com/products/accessories/network_audio_devices/au-003
- **AU-004:**
https://www.vivotek.com/products/accessories/network_audio_devices/au-004
- **RX9502:**
https://www.vivotek.com/products/network_video_recorder_and_appliance/video_decoder/rx9502

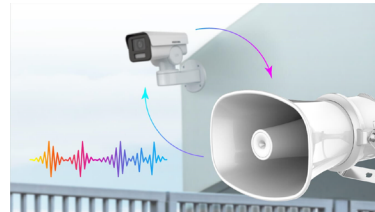
Integration Overview



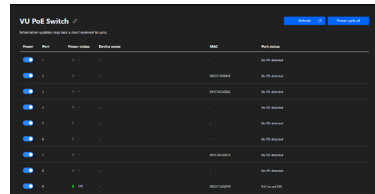
• Talk Down



• Auto-play Pre-recorded Messages



• PoE Switch Remote Power Cycle



Device Overview

Bridge Device	Peripherals	Hardware Charge	Software License Charge	Feature Support	Firmware Support From
RX9502	-	Δ (Buy first, convert to peripheral license later)	X	- Device management - OTA (Video Receiver features are removed)	TBD (PM will inform marcomm before announcement)
	AU-003	V	V MSRP \$99 /year Golden Disty. \$50	- Pre-recorded message - Talk down (currently web portal only, considering support mobile app)	1.0.7
	AU-004	V	V MSRP \$99 /year Golden Disty. \$50		1.0.7
	PoE Switch (L2 & Lite)	V	X	Remote power cycle	L2: 002, Lite:001

NVR	-	V	Δ VORTEX Connect	-	Deprecated – NVR and camera's ability to serve as a bridge will be phased out in the end of 2025. AU-001 is EOL.
	PoE Switch (L2 & Lite)	V	X	• Remote power cycle	
VORTEX Camera	-	V	V	-	
	AU-001	V	X	• Pre-recorded message (only 1 audio file can be uploaded)	

Note

After updating the VIVOTEK RX9502 to the VORTEX Firmware, the RX9502 will function as a Bridge device and will no longer support the original Video Receiver functionality.

VORTEX Set-up Guide

Using RX9502 to Bridge VIVOTEK Network Speaker

This quick guide explains how to connect a VIVOTEK Network Speaker to the VORTEX cloud using the RX9502 as a network bridge.

Included in this guide:

- Supported models of RX9502 and Network Speakers
- How to update RX9502 firmware
- Steps to add speakers into the VORTEX portal

Supported models and the information are as below:

Network Speakers

- VIVOTEK AU-003, AU-004
<https://www.vortexcloud.com/product/network-speaker>

Bridge

- RX9502
https://www.vivotek.com/products/network_video_recorder_and_appliance/video_decoder/rx9502

RX9502 Firmware Requirement

Before using the RX9502 to bridge a VIVOTEK Network Speaker to the VORTEX cloud, please make sure the RX9502 is updated to the following firmware version:

- Required Firmware Version: 4.6.101.2.v08050800
- Download Link: <https://downloadvivoteknew.blob.core.windows.net/downloadfile/vortex/RX9502-VVTK-4.6.101.2.v08050800.img>
- Firmware update SOP: Please refer to next slides

Important Note

The RX9502 will function only as a VORTEX Bridge with this firmware version. Its on-premise video receiver and decoder functions will not be available while using this firmware.

RX9502 Firmware Update

- Using Shepherd to scan & access RX9502 within LAN

Shepherd download:

<https://www.vivotek.com/en-US/products/software/shepherd>

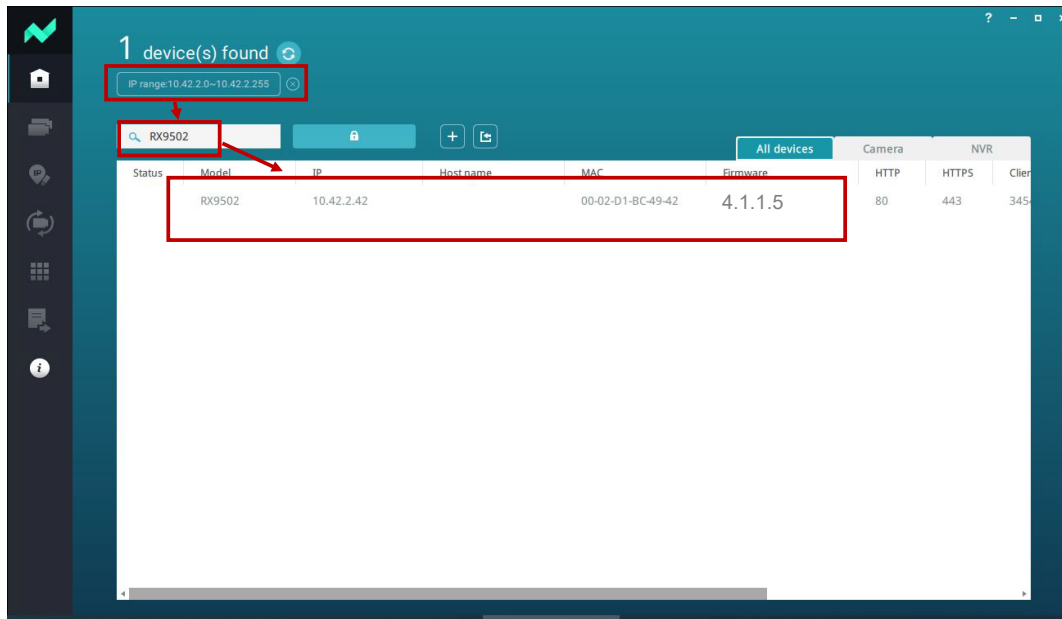
- Firmware update

Double click on RX9502 via Shepherd

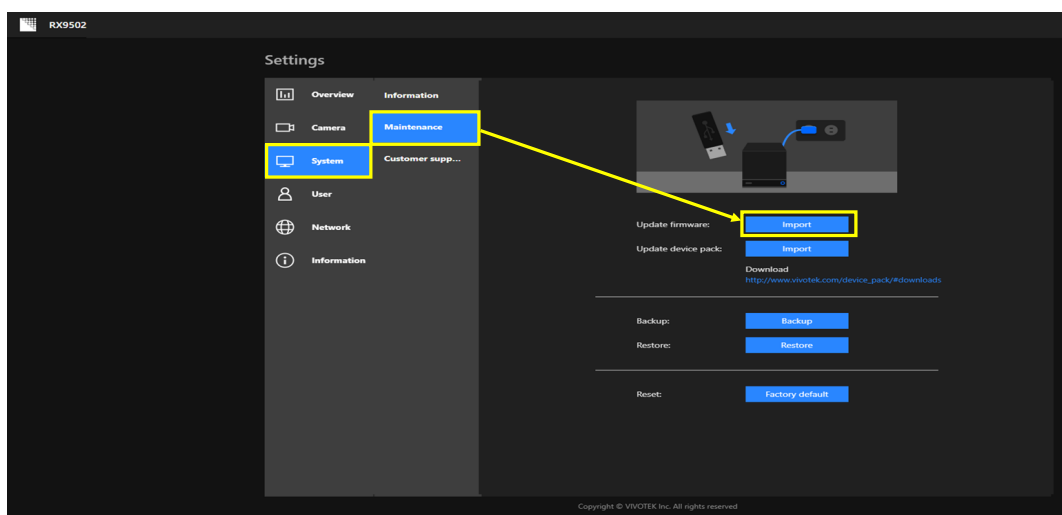
Log-in RX9502 webUI > “System” > “Maintenance” > “Import” to “update firmware”

Important Note

The RX9502 will function only as a VORTEX Bridge with this firmware version. Its on-premise video receiver and decoder functions will not be available while using this firmware.



Scan RX9502 with Shepherd and access to RX9502 WebUI by double clicking it.



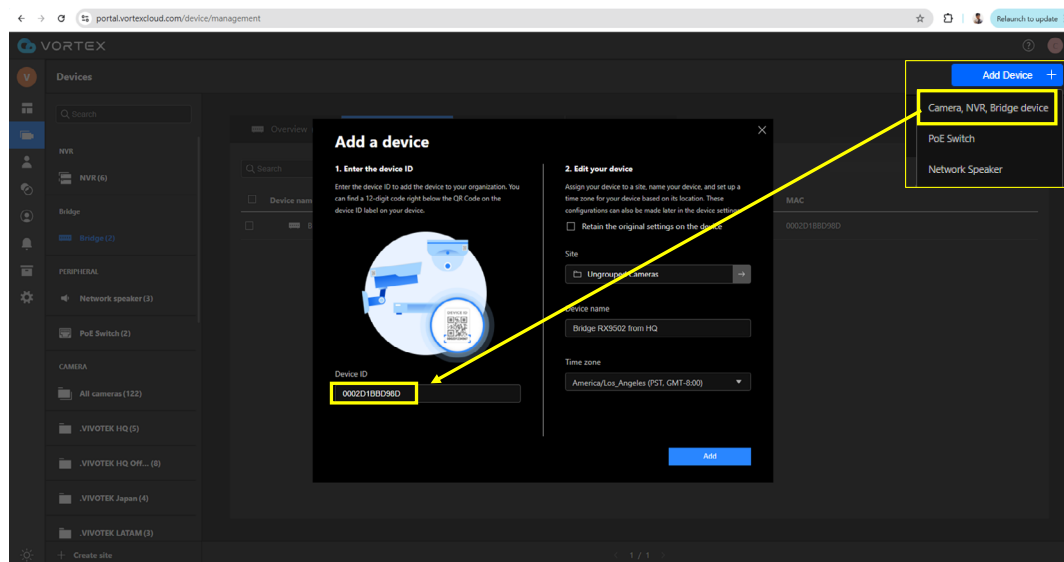
Upgrade RX9502 firmware with version 4.6.101.2.v08050800

Add RX9502 in VORTEX as a bridge

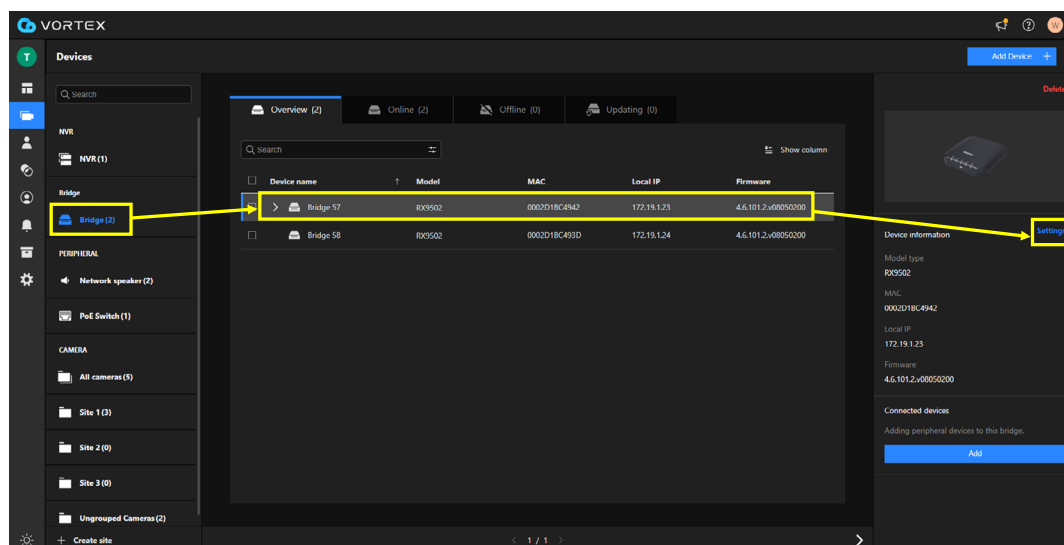
- Log-in VORTEX > “Add devices” > “Bridge device”
 - Key in RX9502 MAC

• Set up

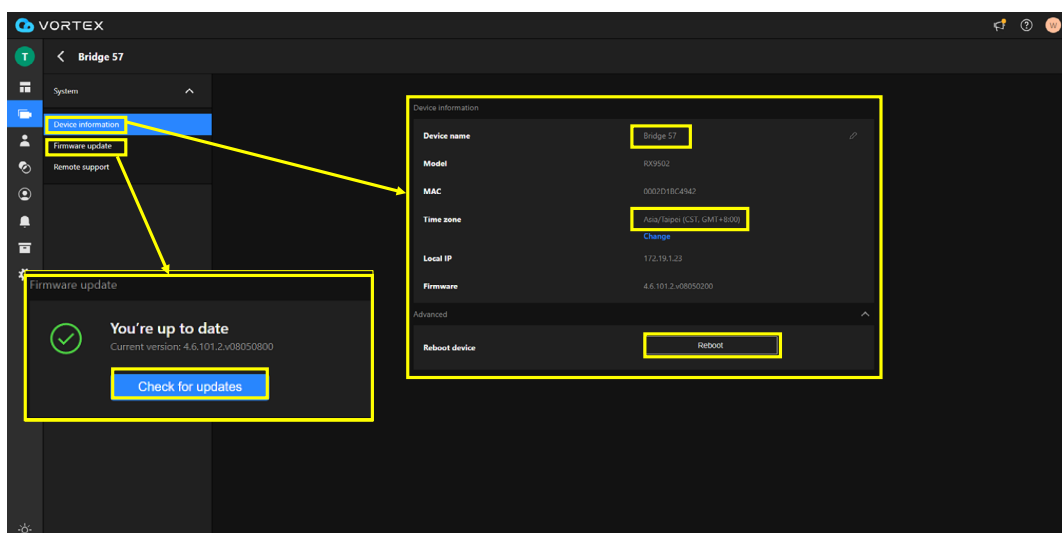
- "Device" > "Bridge" > "Setting"
- Device Information:
 - Edit for Device name/Timezone and reboot
- Firmware update:
 - Latest firmware update check



Add RX9502 by key-in the MAC address.



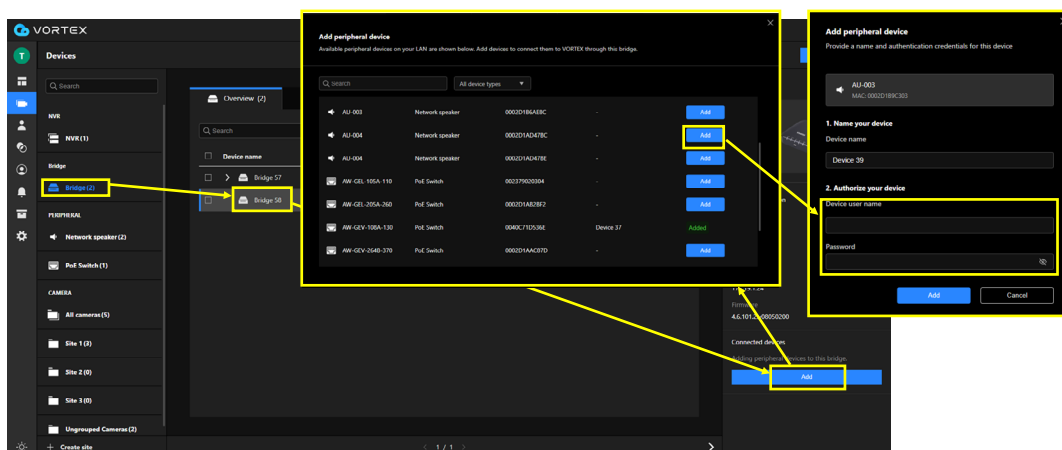
Verify and set-up the name/firmware/timezone if needed.



Verify and set-up the name/firmware/timezone if needed.

Search VIVOTEK Network Speaker and add it into VORTEX portal

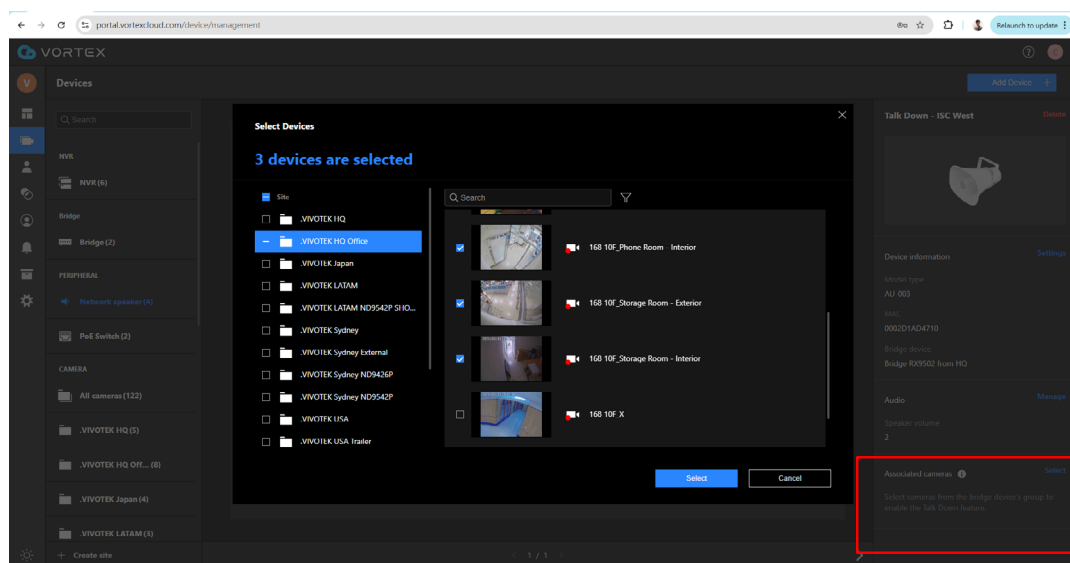
- Log-in VORTEX > “Device” > “Bridge”
 - Click on RX9502
- Search for VIVOTEK Network Speaker and add it in VORTEX
 - Click on “Add” (Under “bridge” > “connected devices”)
 - Select the Network Speaker > “Add” > Authorize the device > “Add”
 - Default credential:
Name: 1234
Password: 1234



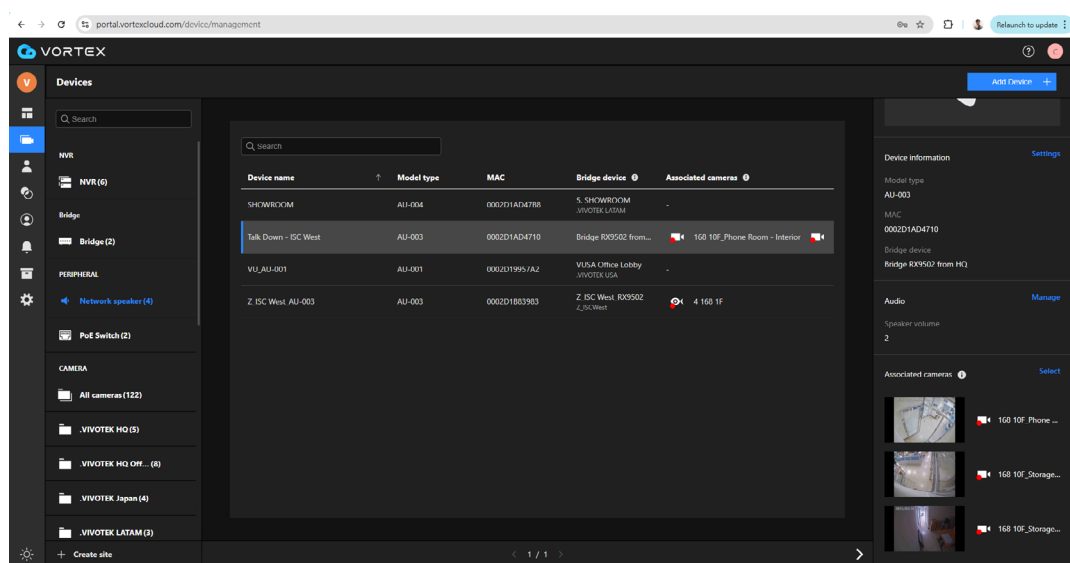
Bridge Network Speaker on VORTEX with RX9502.

Set Up Talk Down Feature

1. Click the device to display the right sidebar for device settings and select “Associated cameras in the right-bottom. Select the cameras you want to associate with the network speaker.

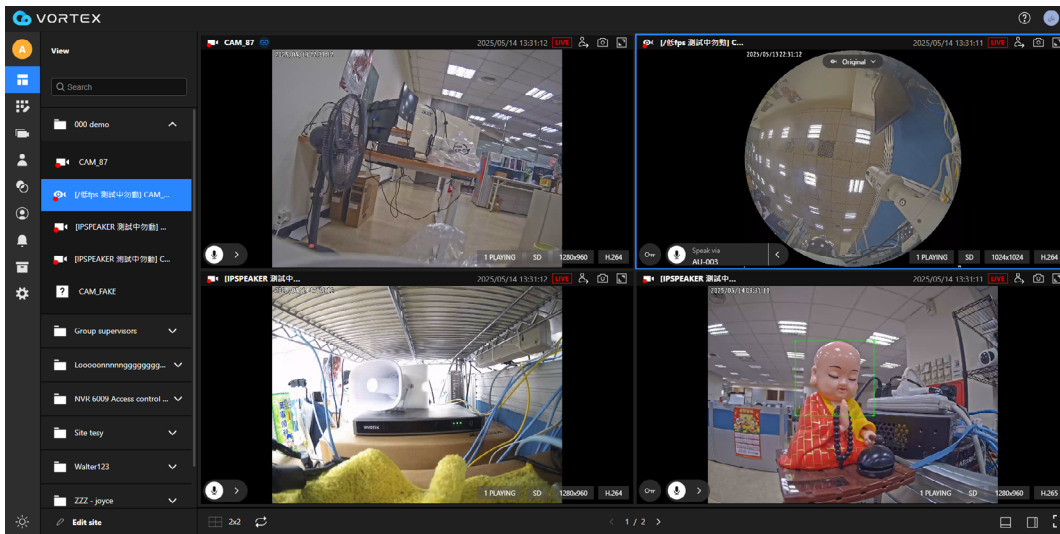


2. The association is completed and the result is displayed.

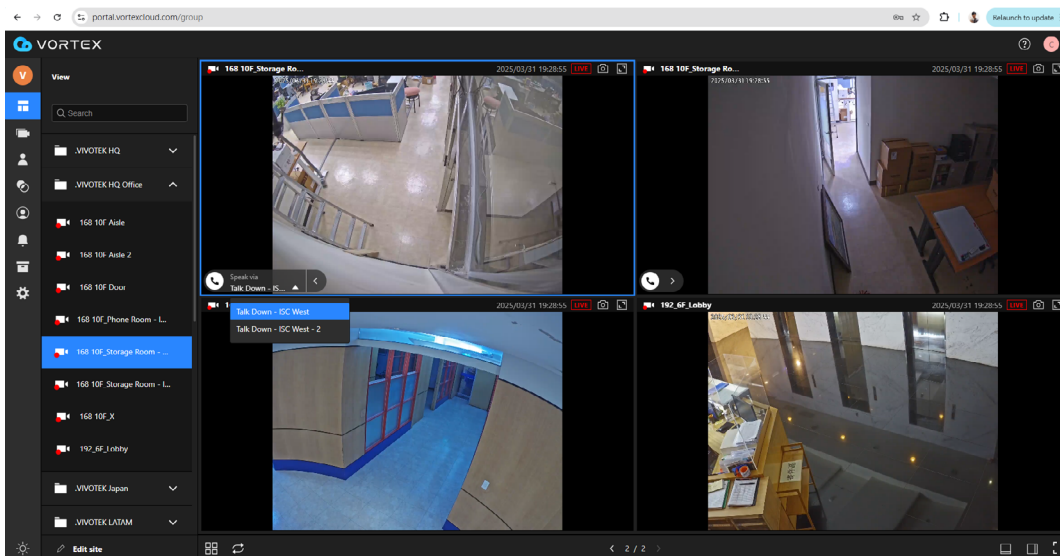


Operate Talk Down

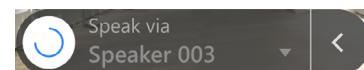
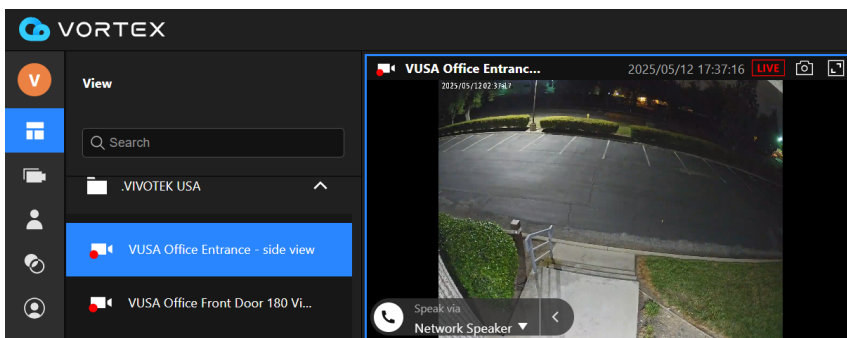
1. Go to Live page and you will see a Microphone icon displayed in the camera you associated with network speakers.



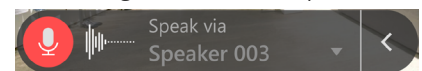
2. Click the arrow icon for dropdown list and choose the Network speaker you want to initiate talk down.



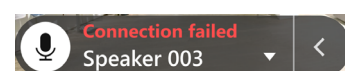
3. Click the microphone icon to start talk down. There are four possible states when you initiate the call.



Connecting to the Network speaker



Talk-down in progress; the sound wave icon will fluctuate when speaking

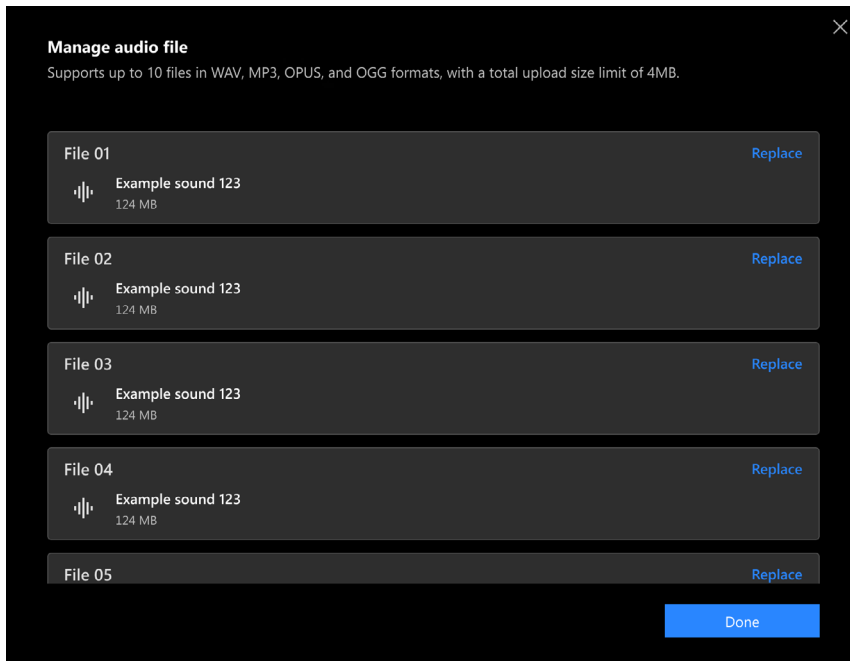


Unable to connect to the Network speaker

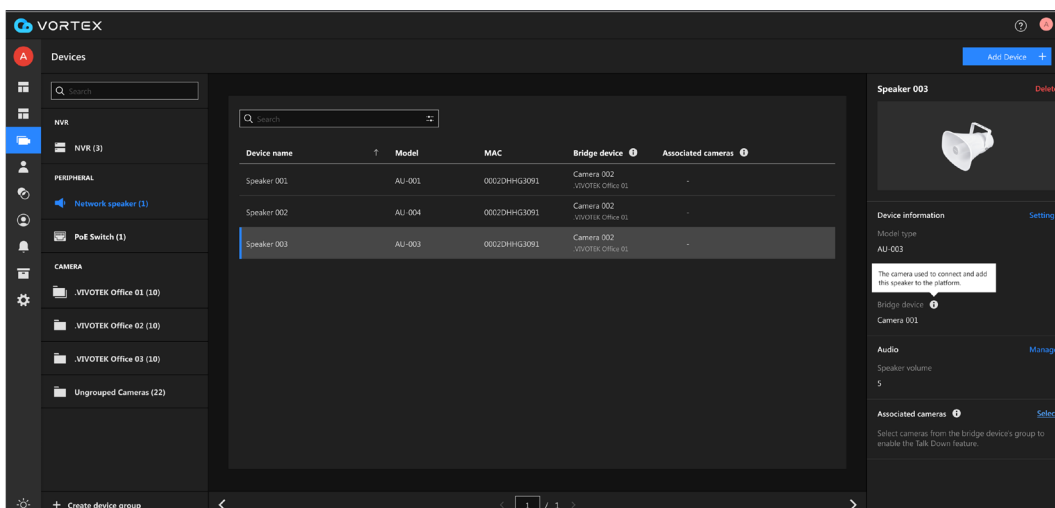
Manage Audio Files

Goal

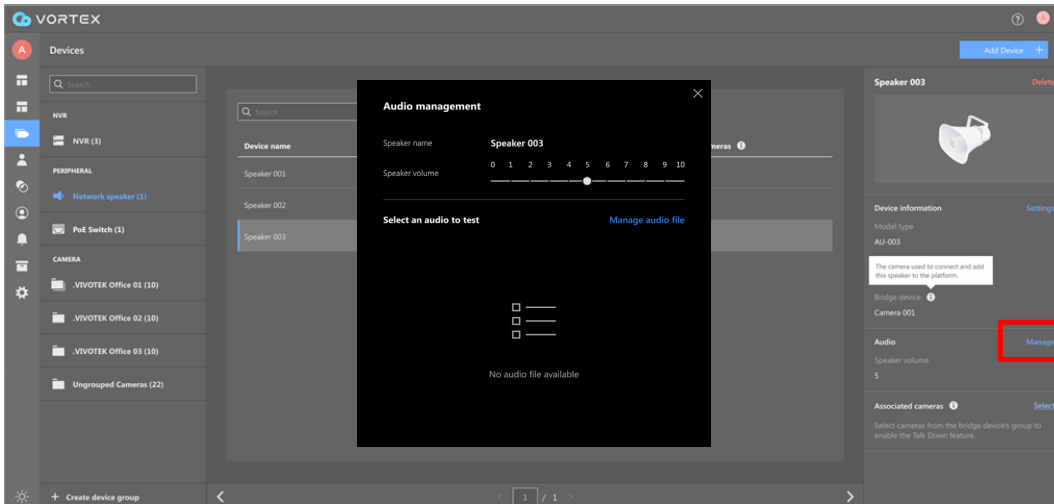
- Upload audio files to the network speaker to allow auto-play of specific files for different alarms to deter intruders.



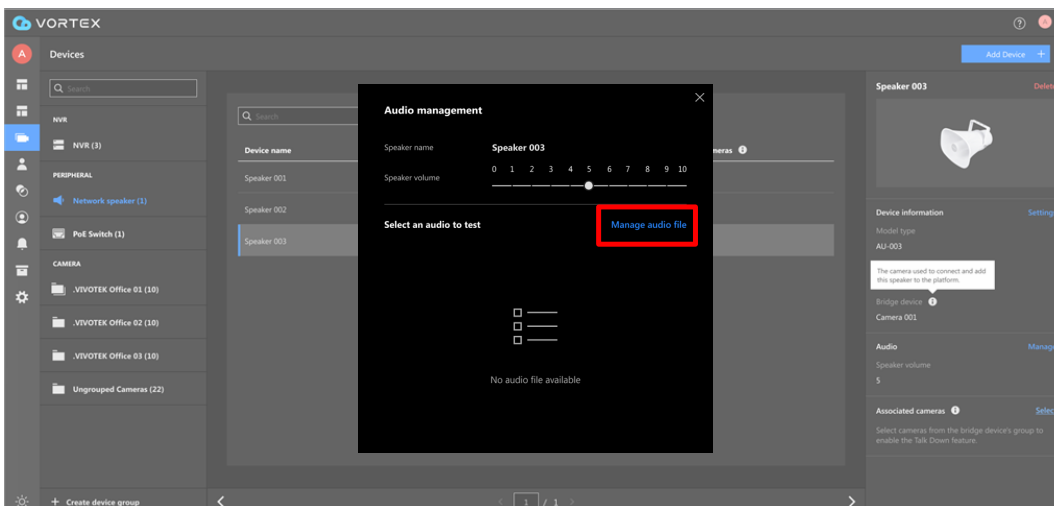
1. Select the network speaker to display the right panel for device management.



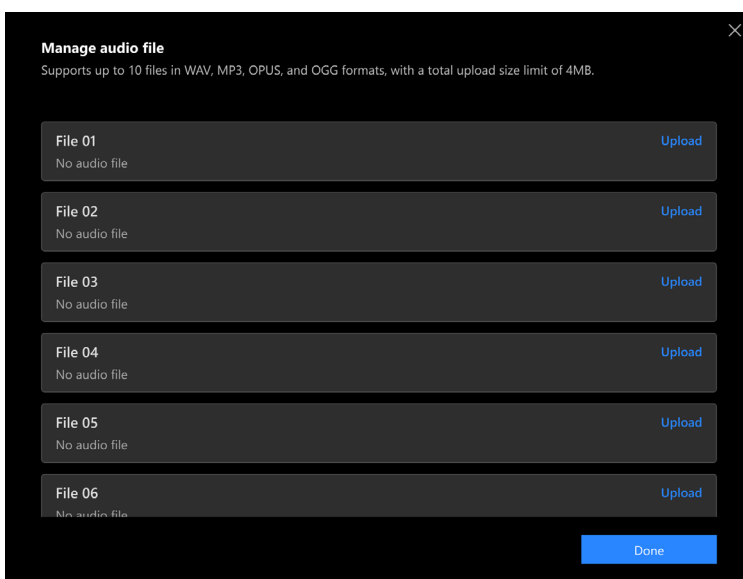
2. Select 'Manage' in the Audio section to open the Audio management window.



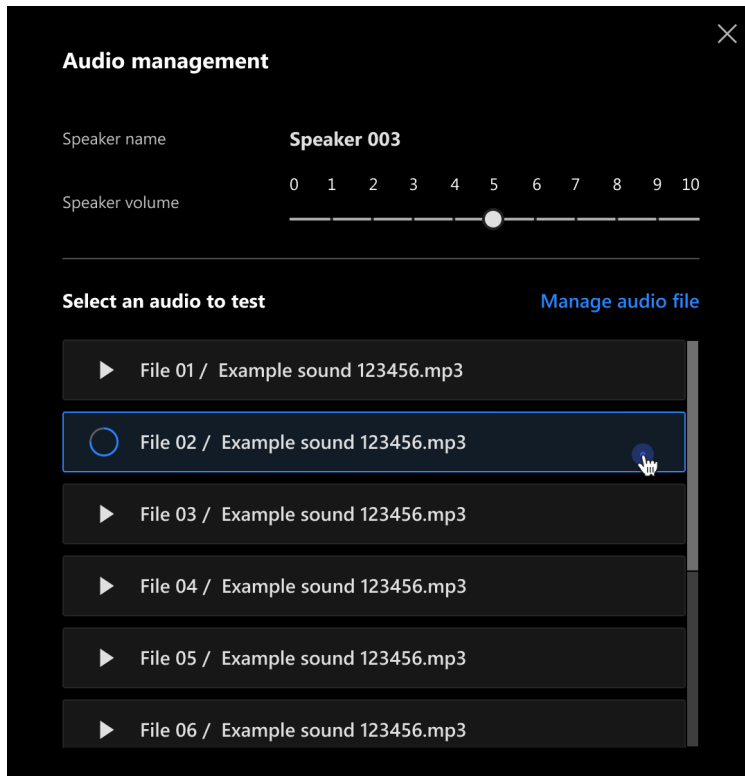
3. Select 'Manage audio file'.



4. Upload your audio files for auto-play messages. Up to 10 files in WAV and MP3 formats, with a total upload size limit of 4MB.



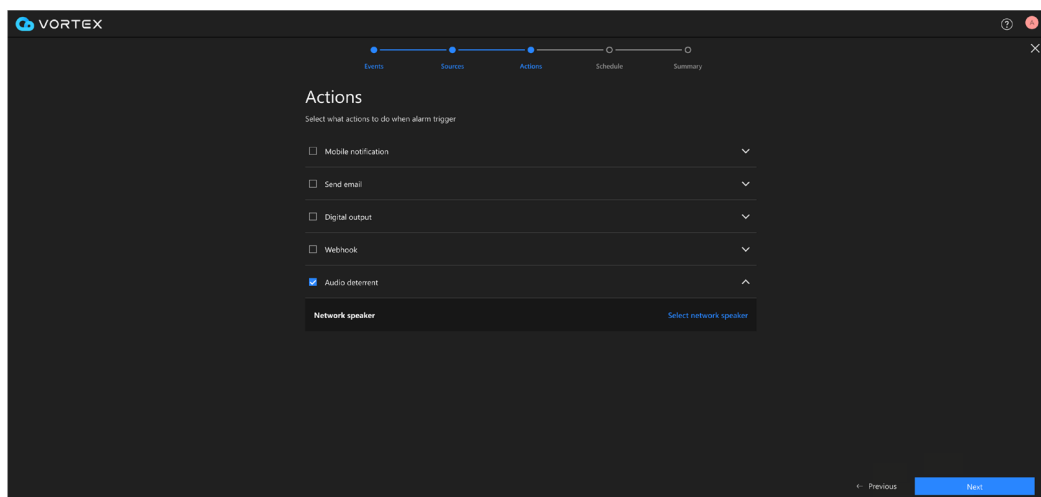
5. To test your audio files, click play icon.



Set Up Alarm Management for Audio Deterrent

Goal

Configure network speaker as audio deterrent in Alarm Management, using the audio files uploaded to auto-play and deter intruders.



The configuration of alarm management is the same as the current VORTEX functionality. This guide skips other basic steps and focuses solely on the 'Actions - Audio Deterrent' step.

In 'Actions', select Audio deterrent. Choose the network speaker and select the audio file for this alarm.

VORTEX

Events

Sources

Actions

Schedule

Summary

?

✕

Actions

Select what actions to do when alarm trigger

☐ Mobile notification

▼

☐ Send email

▼

☐ Digital output

▼

☐ Webhook

▼

☒ Audio deterrent

▲

Network speaker

Select network speaker

Speaker 001

Selected audio

File 01 / Example sound 1234567...

Speaker 002

Selected audio

File 01 / Example sound 12345678912...

Speaker 003

Selected audio

File 04 / Example sound 123.mp3

Speaker 004

Selected audio

File 08 / Example sound 123.mp3

Speaker 005

Selected audio

File 09 / Example sound 123.mp3

Unable to access audio files from this speaker. Please check the speaker's status or select another file.

← Previous

Next →

VIVOTEK

A Delta Group Company

www.vivotek.com

DESIGN AND SPECIFICATIONS ARE SUBJECT TO CHANGE WITHOUT NOTICE
Copyright © 2025 VIVOTEK INC. All rights reserved.