VIVOTEK
A Delta Group Company

User Manual

VORTEX

Document Version: 1.0

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

Doc. Ver.	Comment
Rev.1.0	Initial release.

Table of Contents

System requirements

1

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

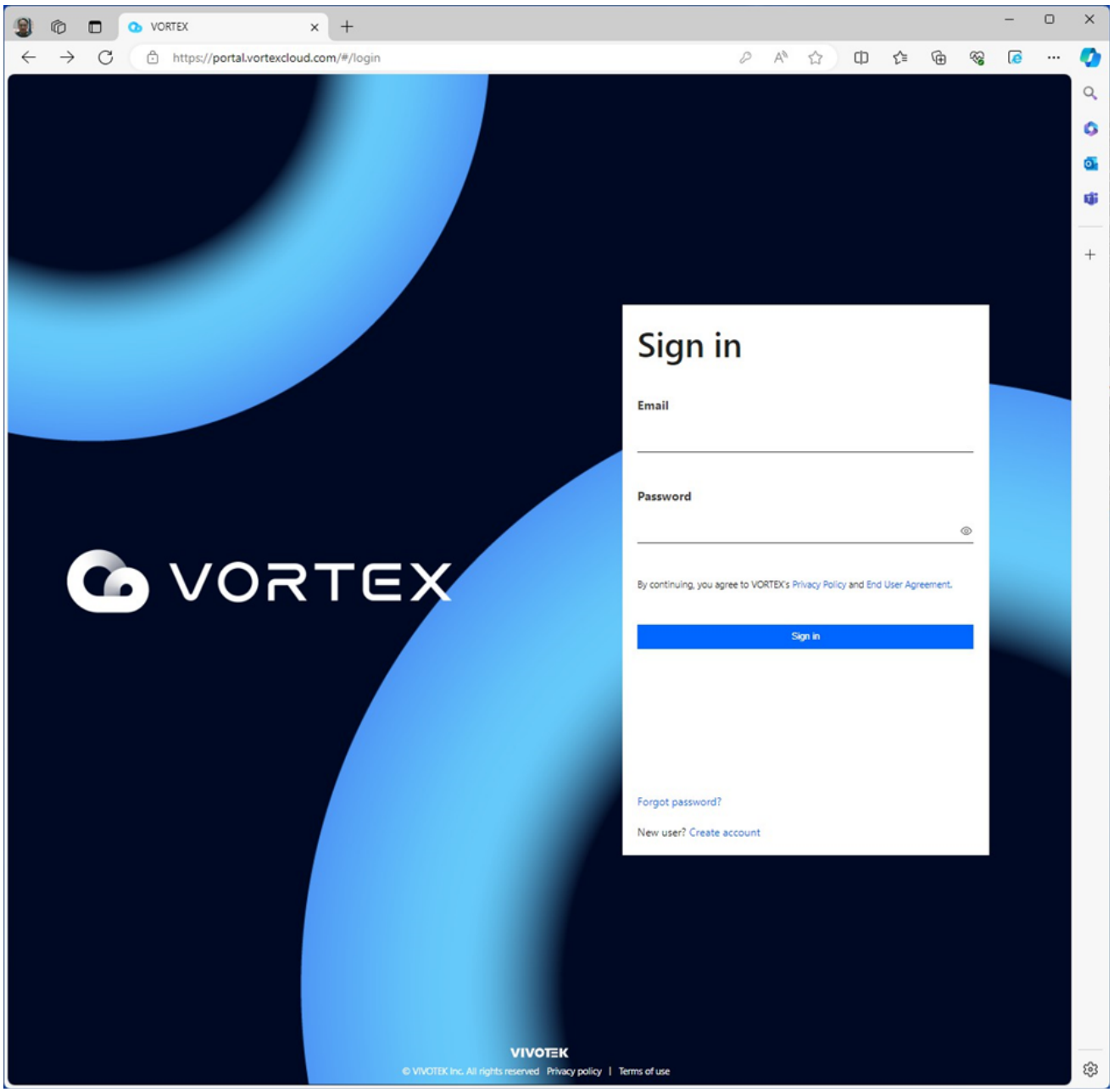
An internet connection is also a must. Otherwise, VORTEX cameras and the VORTEX service cannot communicate with the VORTEX servers, so you will not be able to use important features such as video storage, live view for real-time monitoring, or any of the other functionalities offered by the service.

Establishing a VORTEX service 2

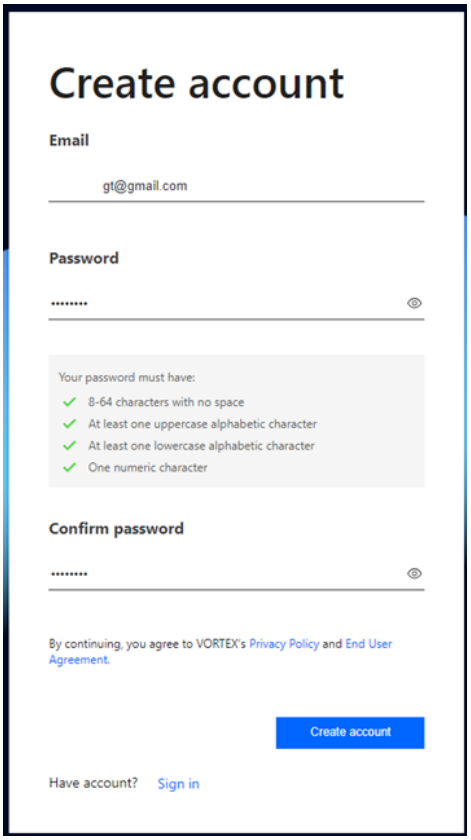
The first time you use VORTEX, you, as a VORTEX service owner, must establish a VORTEX service. To do so, you can use one of the following two methods:

Creating a VORTEX account & adding devices (via the web portal)

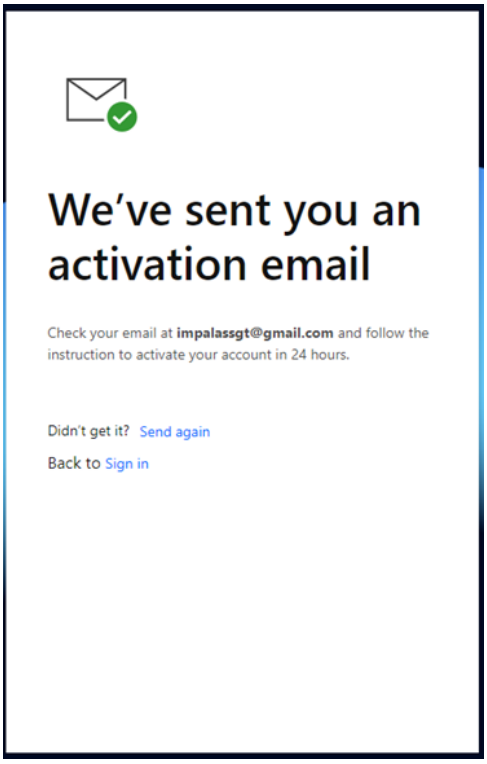
1. Visit https://portal.vortexcloud.com/#/login and click **Create account**.

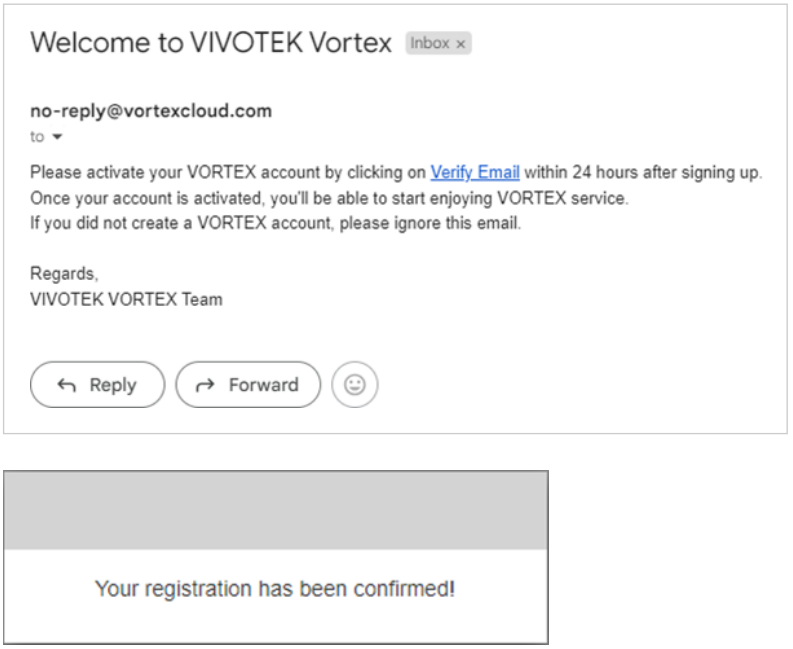


2. Enter an email address and set up your password according to the rules. Then, click **Create account.**

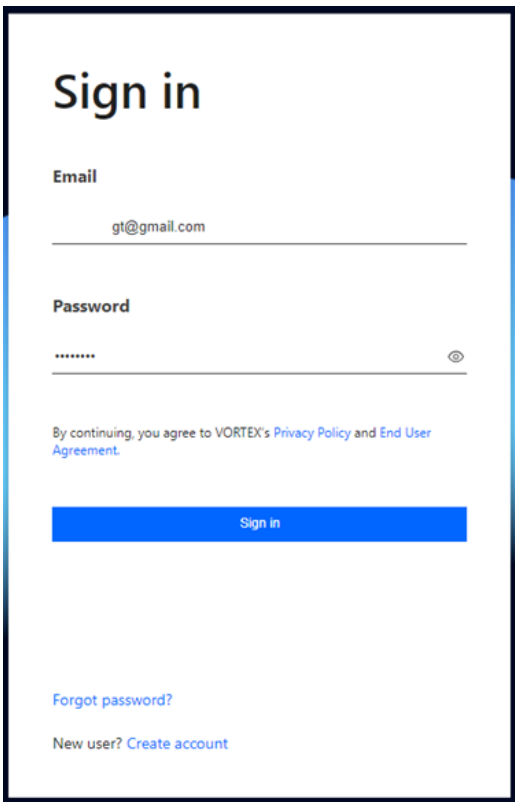


3. The VORTEX system sent an activation email to you. In the Inbox of the email you used in Step 2, click **Verify Email**. The browser will display a confirmation message.

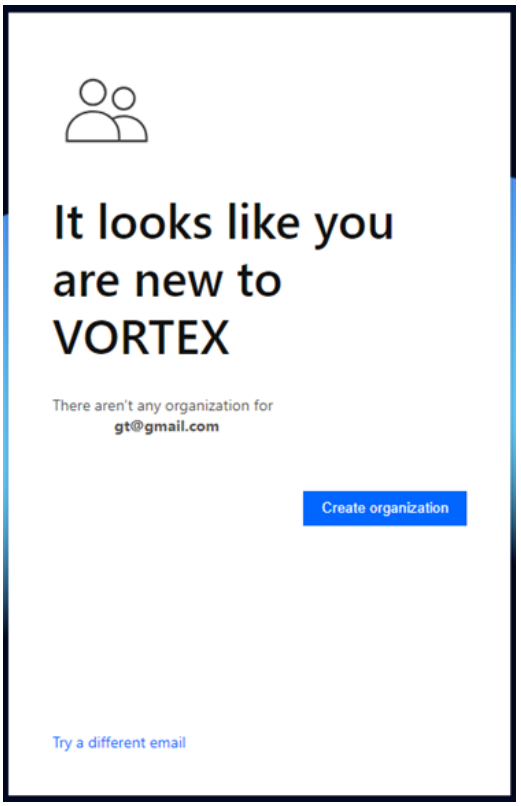




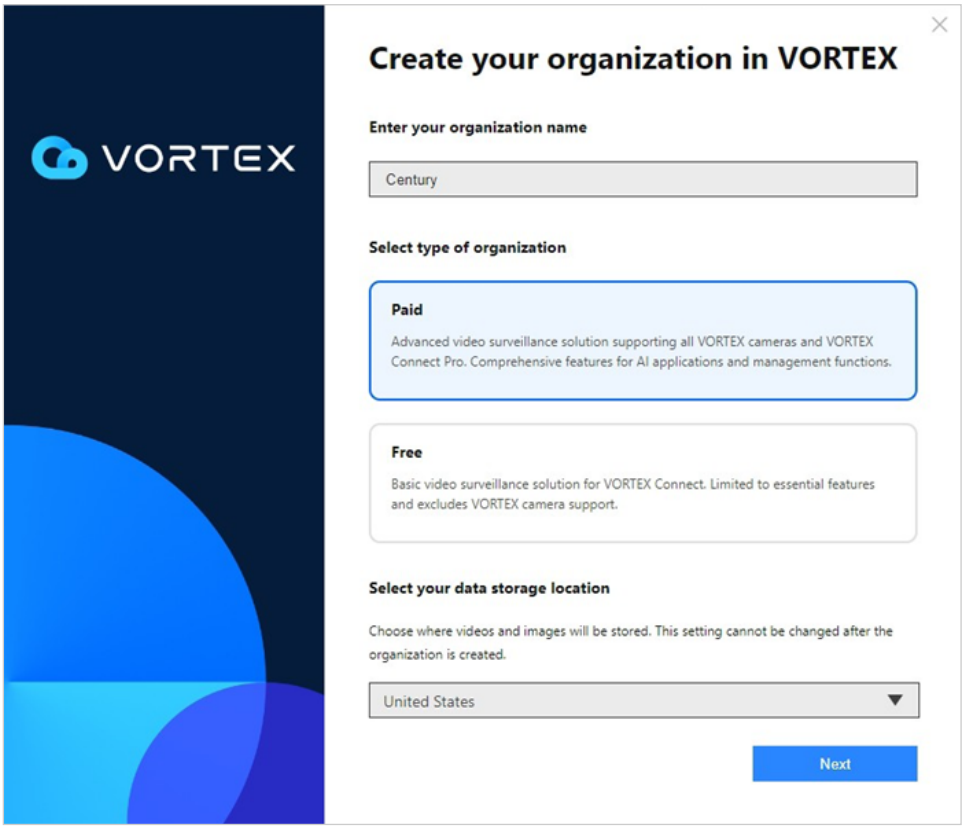
4. Return to the VORTEX sign-in page, enter your email address and password as needed. Then, click **Sign in**.



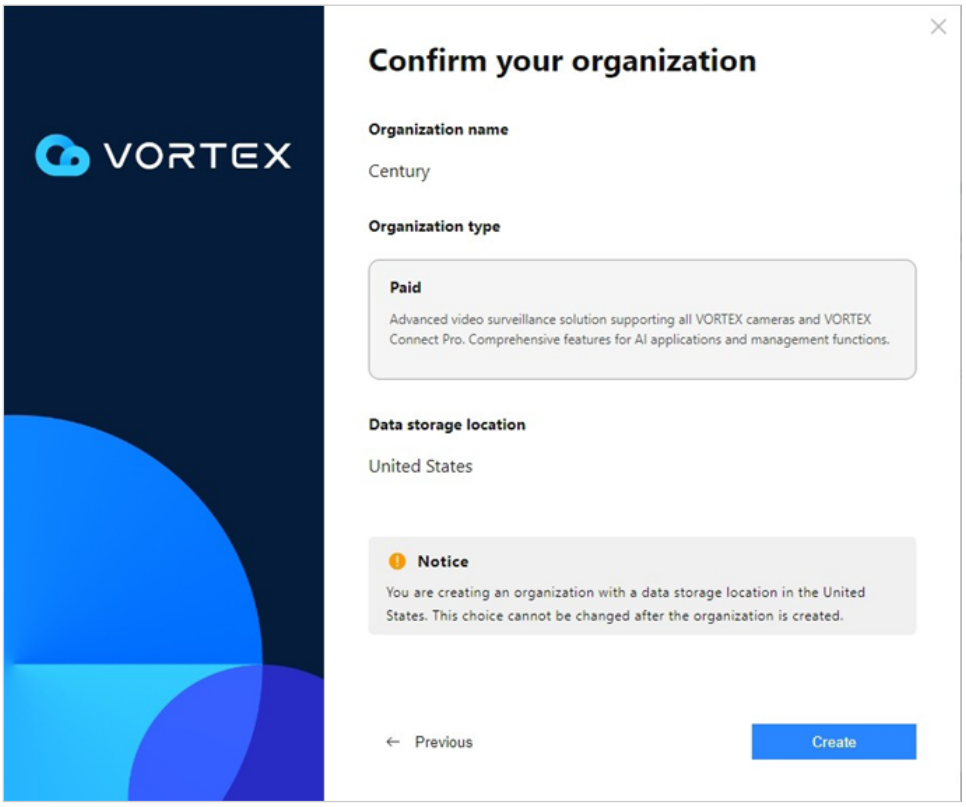
5. Because you are new to VORTEX and you do not belong to any organization, a message below will appear asking you to create an organization (service).



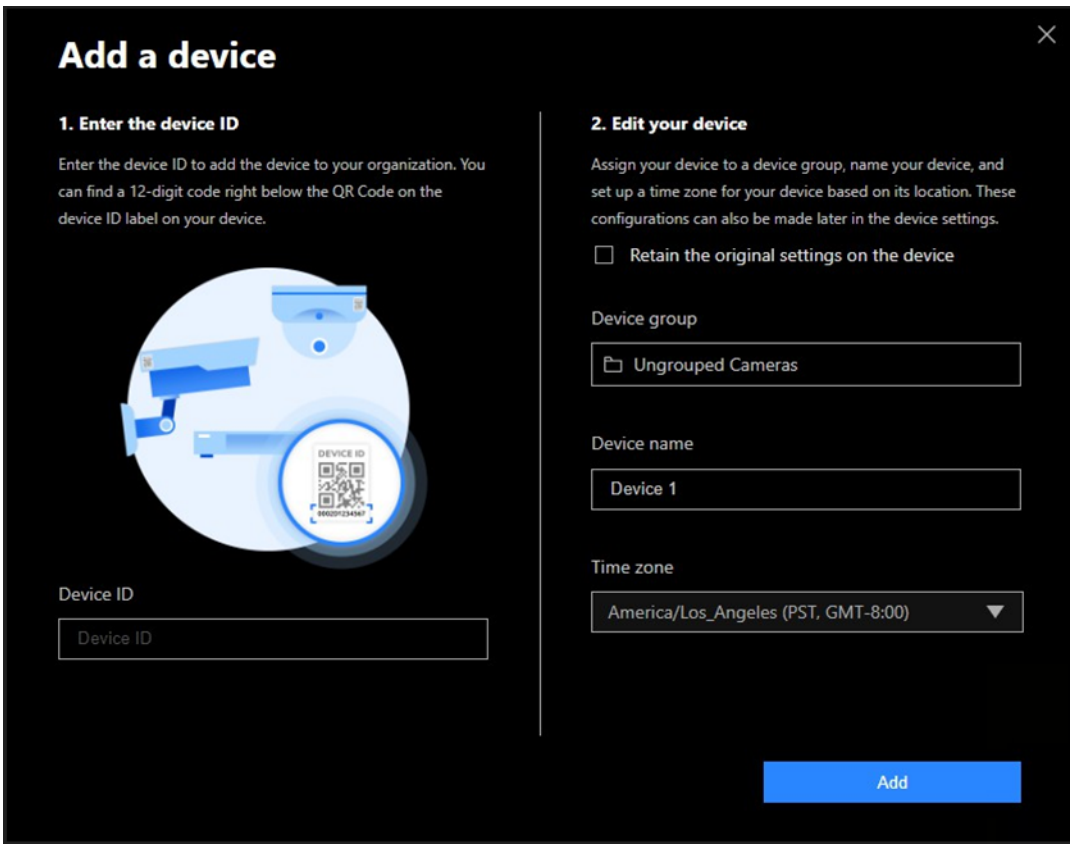
6. Enter your organization name, select a region, select an organization type (paid or free), and then click **Next**.

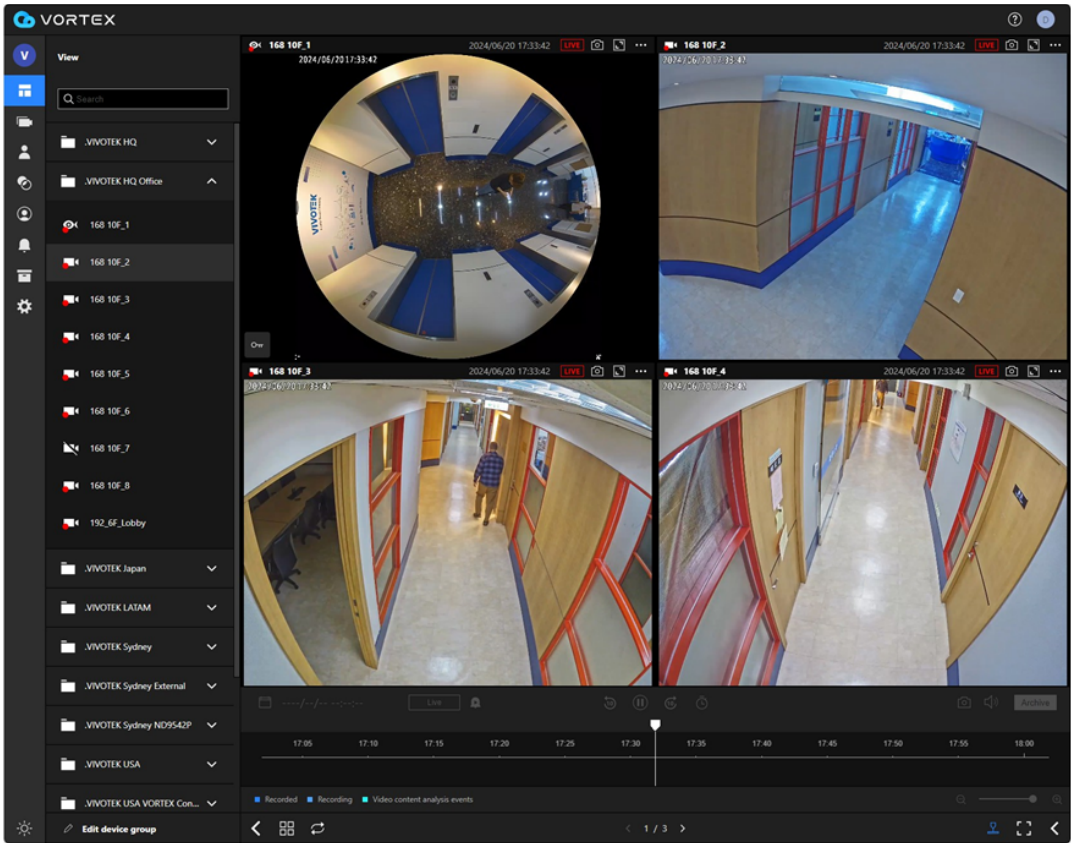


7. Review if the information you entered is correct, and then click **Create**.



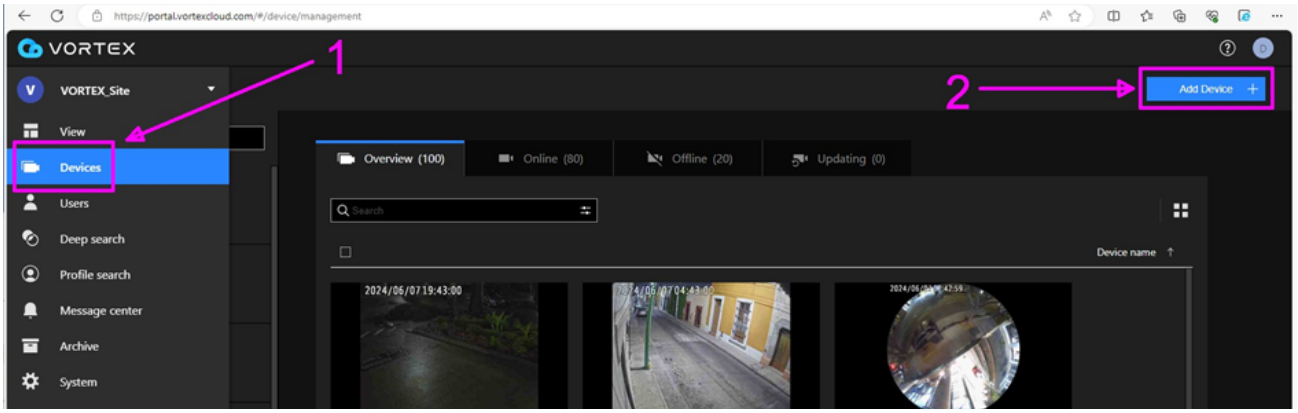
8. Start adding your devices to be used in your organization by entering Device ID (MAC address) and other required information.





Example of an existing organization after adding devices

You can always add devices at any time by clicking **Devices** > **Add device** on the upper- right corner of the web portal.



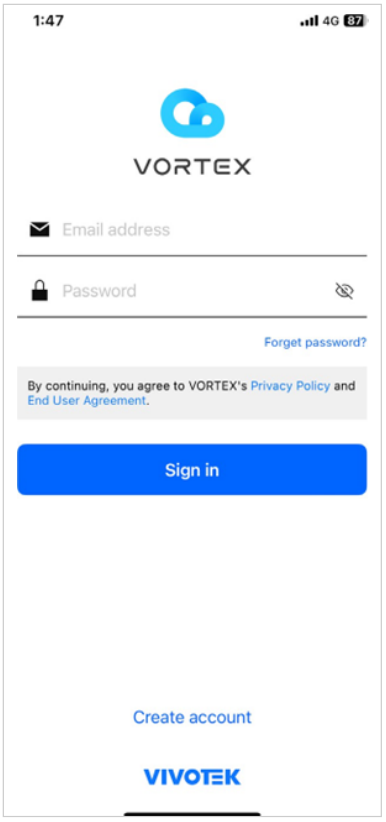
Creating a VORTEX account & adding devices (via the mobile app)

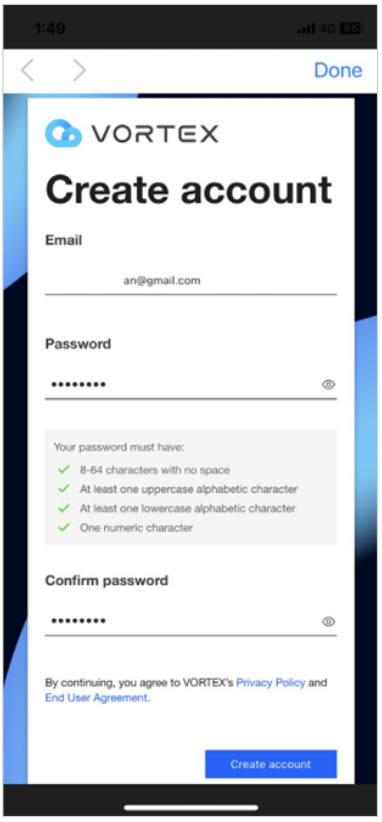
1. Install VORTEX from App Store or Google Play by scanning one of the following QR codes via your mobile device.

Available on the iPhone App Store

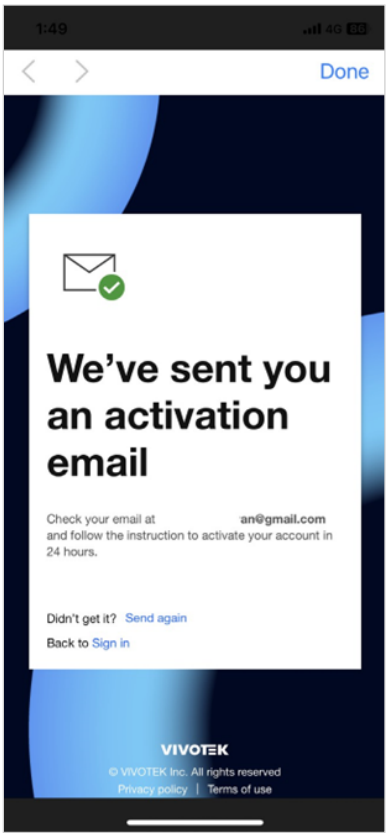
ANDROID APP ON Google play

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

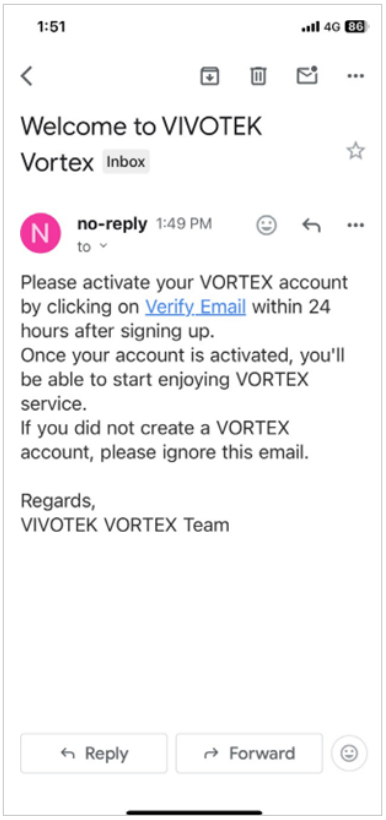




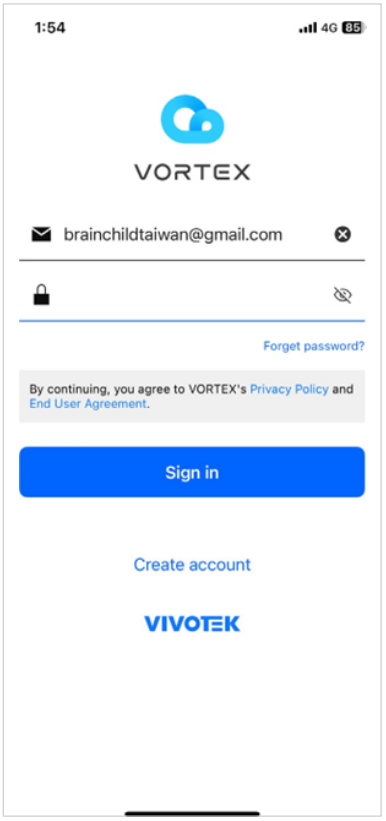
3. Tap **Create account**, and follow the instructions of the message appearing below.



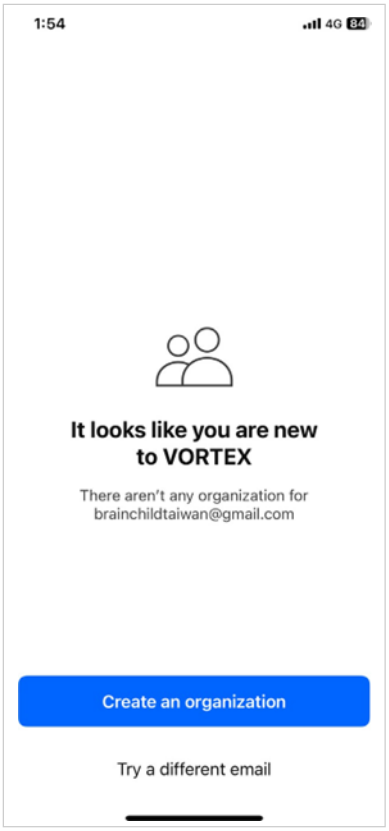
4. Tap **Verify Email**, and a confirmation message will appear in the browser.

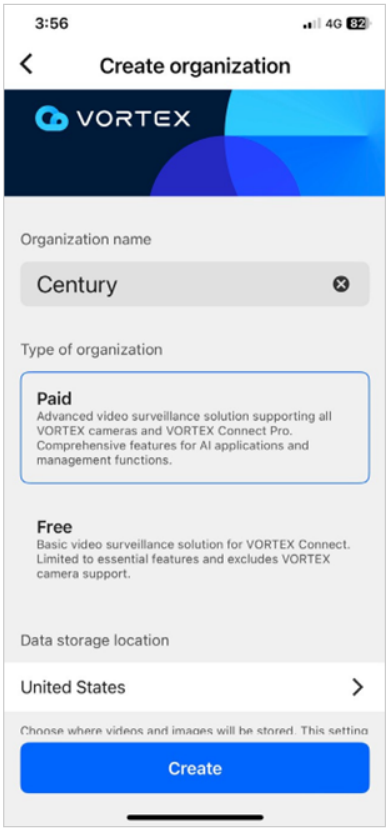


5. Return to the VORTEX app, and then enter the email and password to sign in.

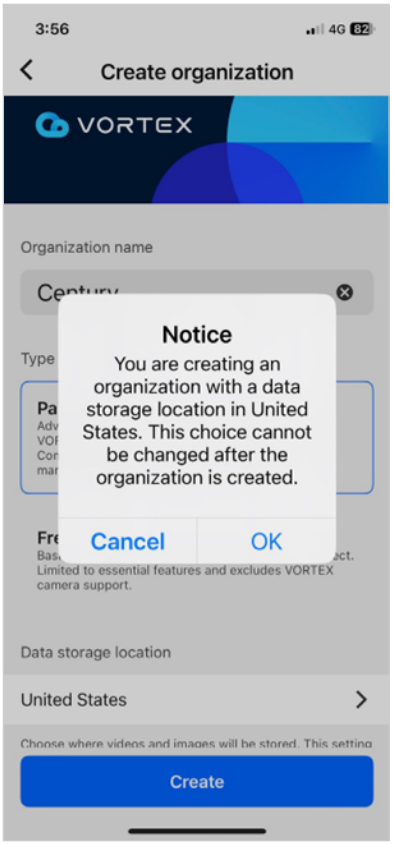


6. Tap **Create an organization** and enter the organization details.

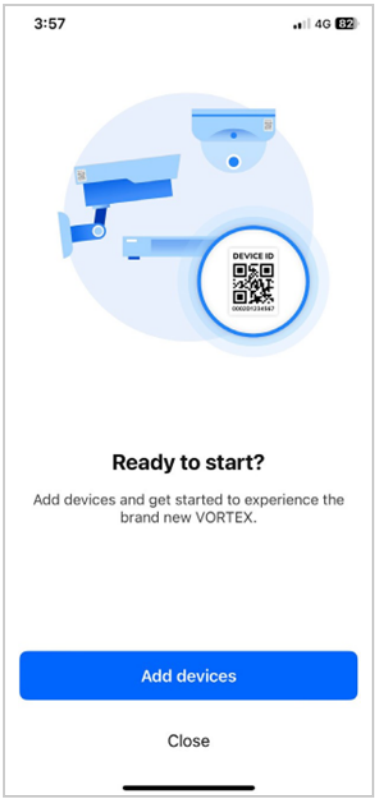




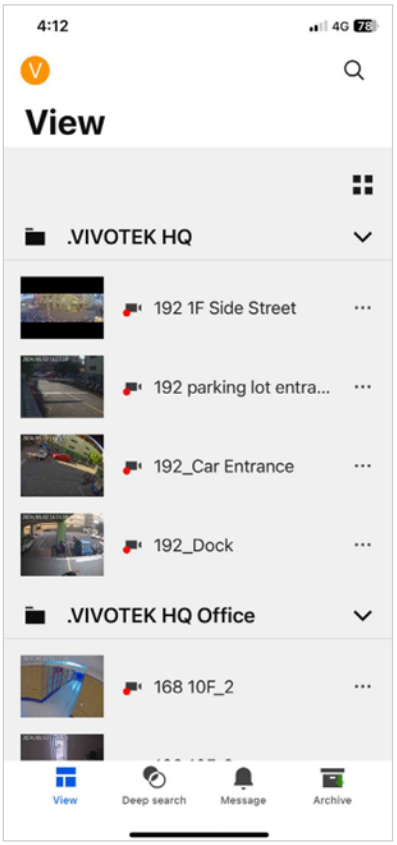
7. Note that once you select a region and tap **OK**, you cannot change the region again.

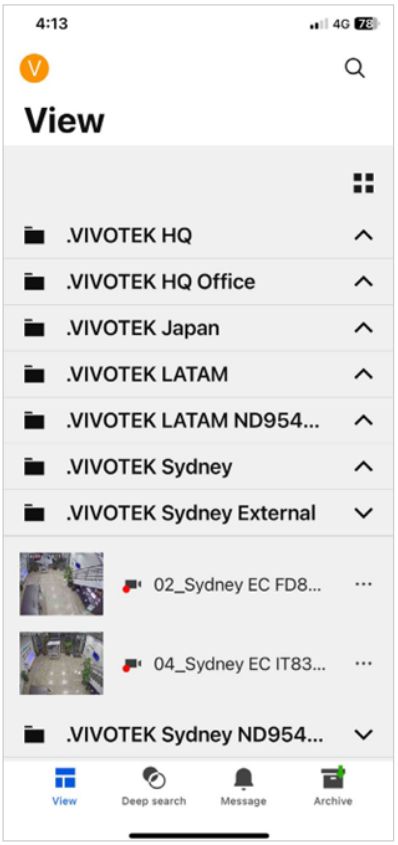


8. Tap **Add devices** as needed.



9. Once devices are added to your organization, you can view cameras on your mobile device like the ones below.





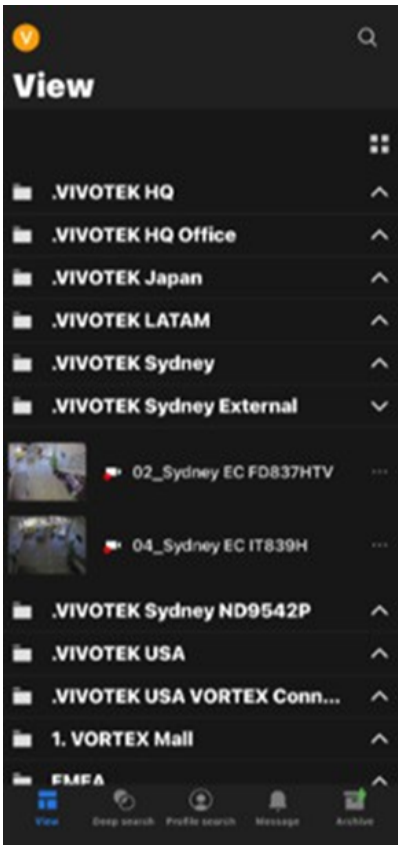
NOTE

When using a mobile device to add devices to your organization, you can scan a device QR code in addition to entering its device ID.

Example of a device ID on a VIVOTEK packaging box

Example of a device ID on a VIVOTEK camera

- A device ID can also be on a VIVOTEK NVR device. See the next section for details.
- In addition to scanning a QR code, you can manually type in a MAC address to add a device.
- You can always add devices at any time by tapping the organization icon > **+ Add devices** on the upper-left corner of the mobile app.

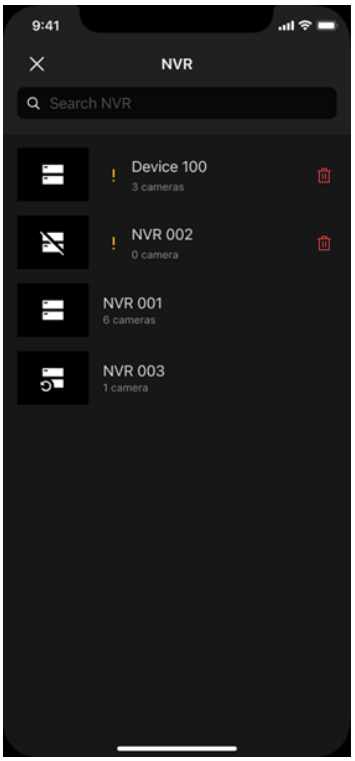


NOTE

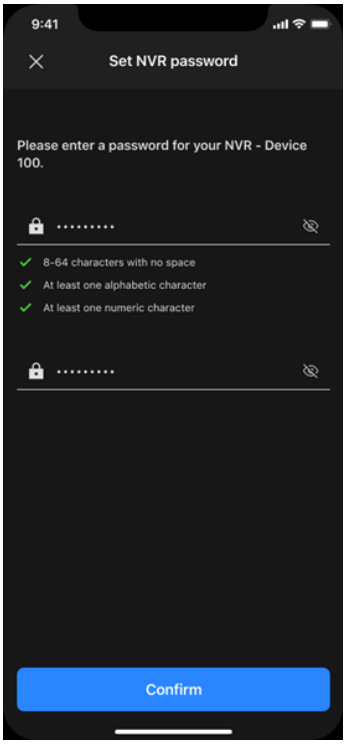
If you press the reset button on a camera in an organization, the camera will be removed from the organization. All camera data (SD card / cloud videos) will also be removed.

Adding a VIVOTEK NVR device

1. Tap the organization icon, and then go to your organization information page.
2. Click the NVR icon to check your NVR status.
3. Click the NVR device with the exclamation mark.

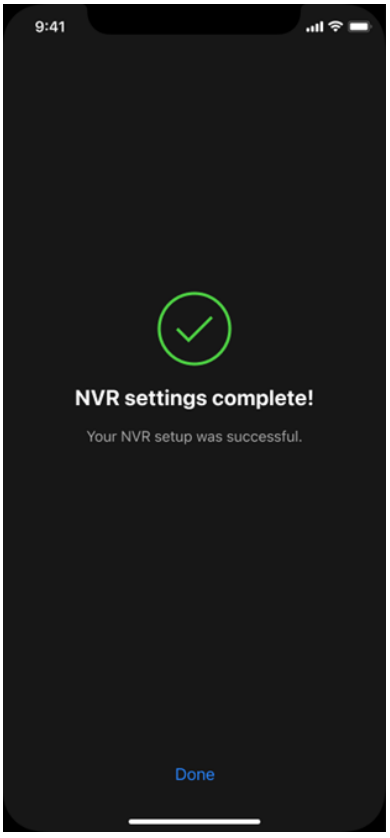


4. Set the password for the NVR by typing in a password.



5. Wait for the volume setup process to complete.

6. The wizard ends.



Joining a VORTEX service

3

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.

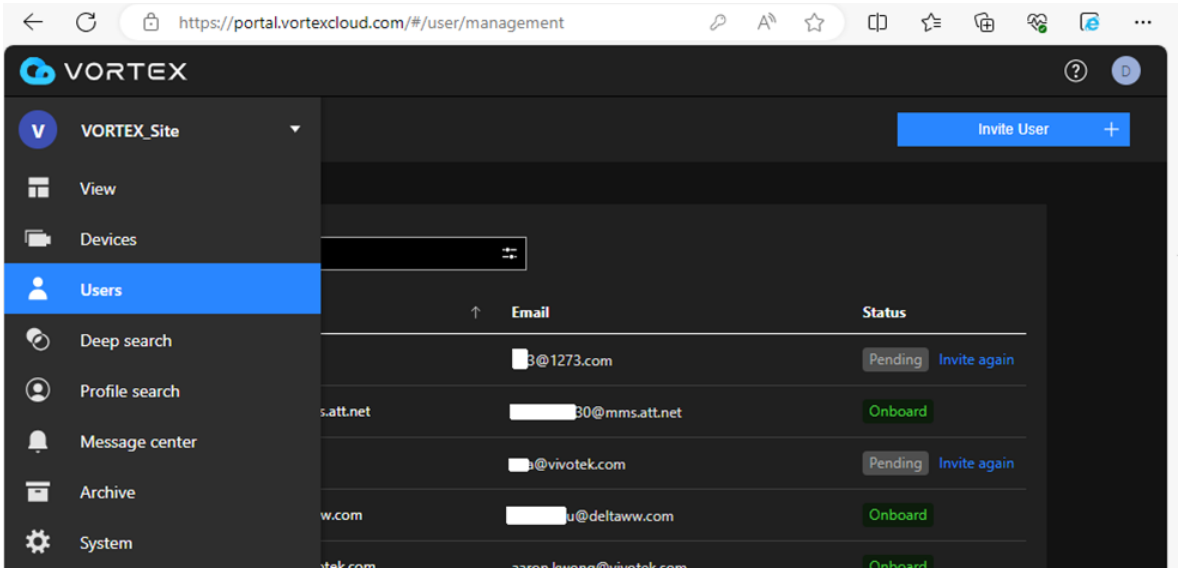
Adding a VORTEX account via the web portal

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

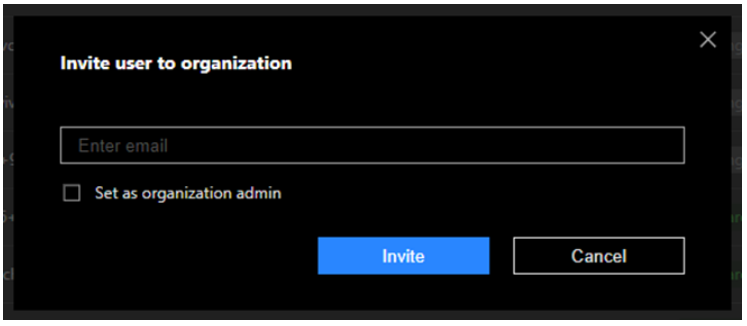
Adding a VORTEX account by invitation

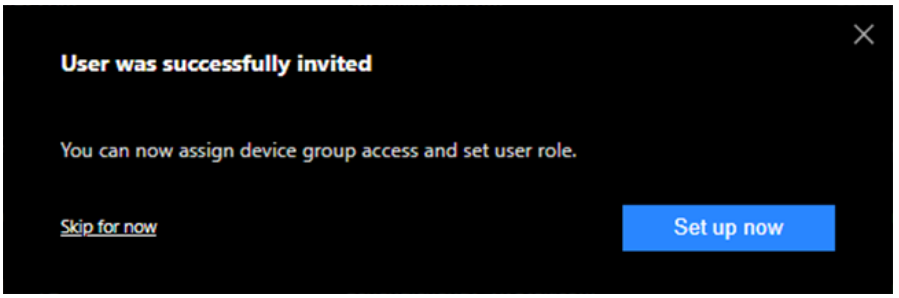
If you are the owner of a VORTEX organization, you can send an invitation email to invite a person to join your organization as a user at the user privilege you specify.

1. On the Users page, click **Invite User**.

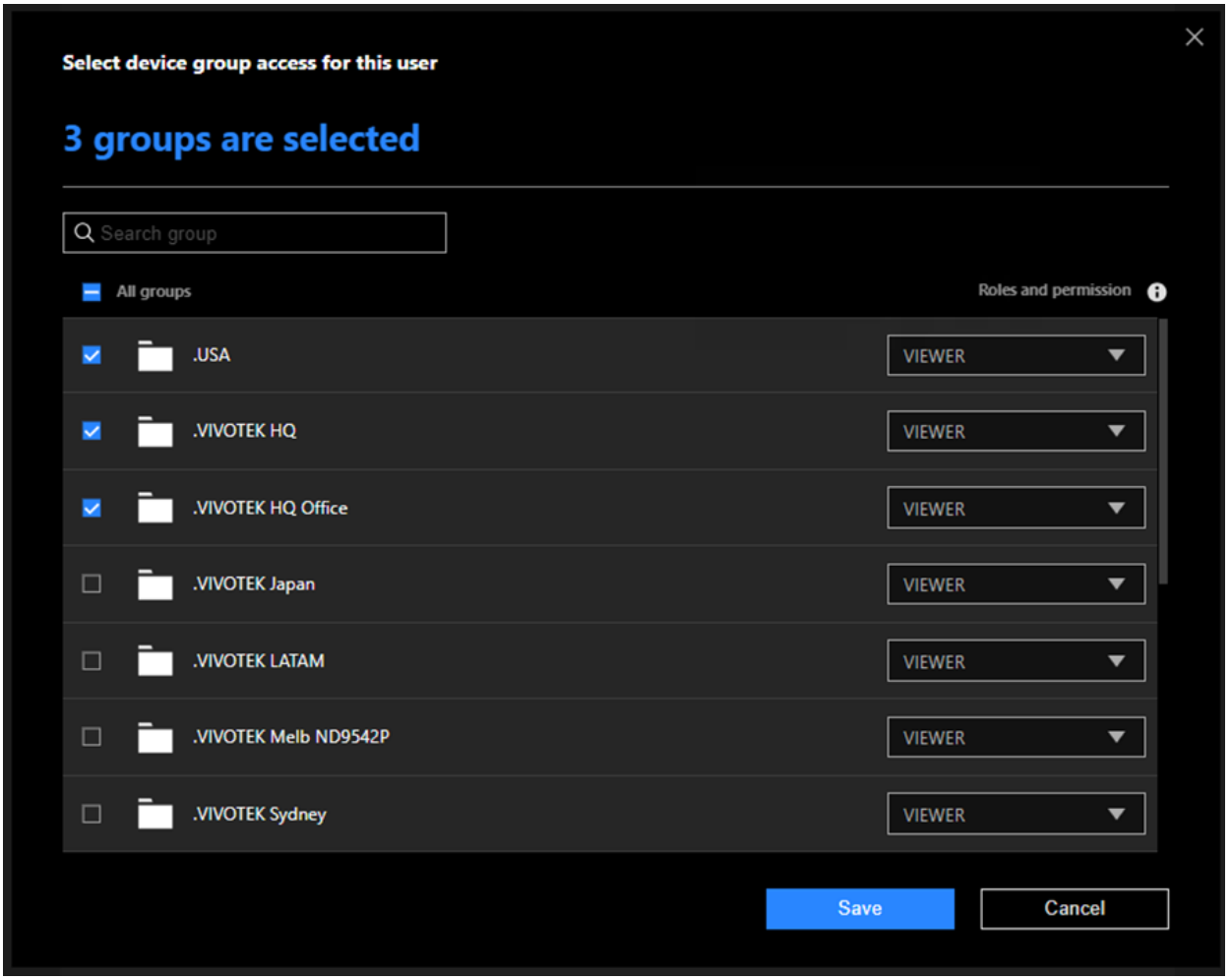


2. Enter the user email address and click **Invite**.





3. Click **Set up now** to decide the user access right as needed.

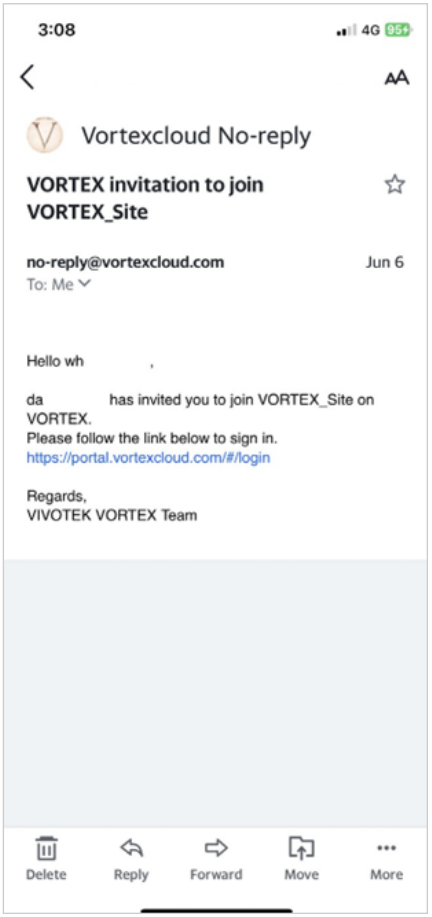


The table below shows the user type and their access level in VORTEX. You can refer to this table to set up user type and user access right.

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.

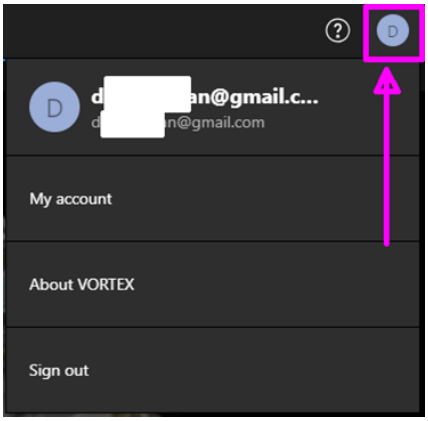


User management is not available in the mobile app. So, you cannot invite a user via the mobile app.

Managing your account

4

On the upper-right corner of the workspace when using the web portal, you can find a personal icon (example shown below). Click it and you will see the following four items:

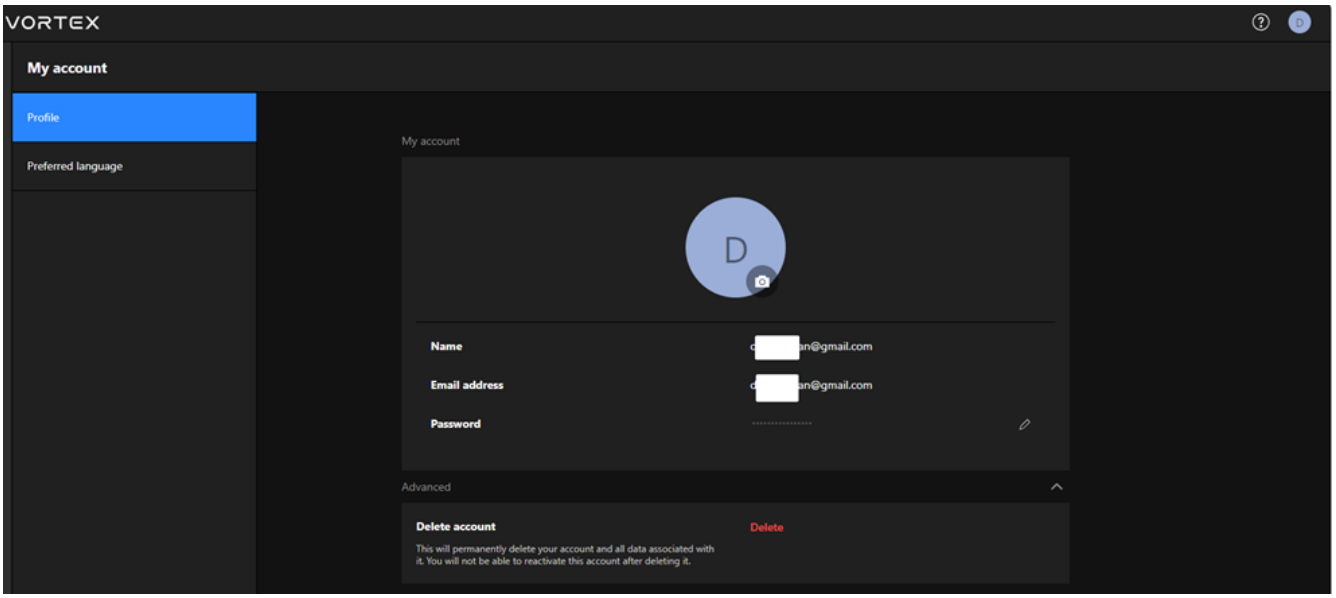


First letter of your email address:

The English letter in the circle shows the 1st letter of your email address.

My account:

- On the Profile tab, you can change your password or remove your account from the organization.
- On the Preferred language tab, you can change the software display language.



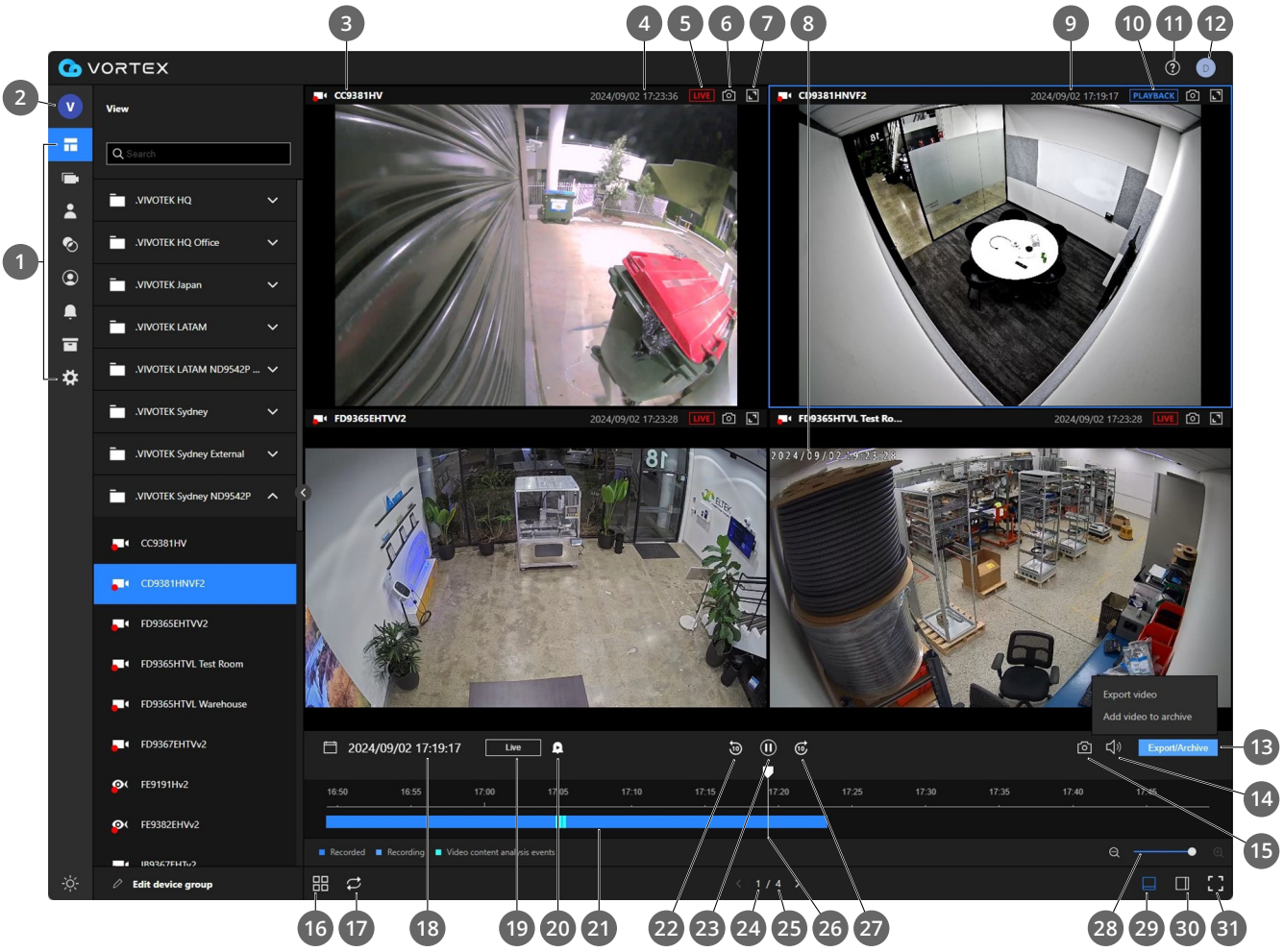
About VORTEX: Shows privacy policy, terms of use, and software version number.

Sign out: You can log off from the system here.

View

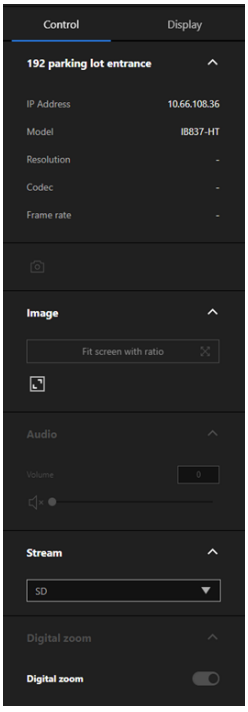
5

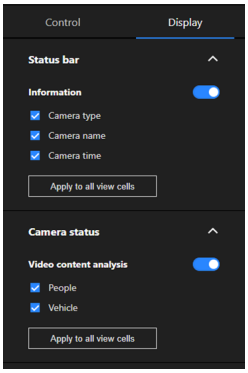
The VORTEX live view feature provides real-time access to all connected cameras. Simply click a designated group to view live footage from your cameras.



1. **Side menu:** Provides various tool options.
2. **Organization name:** Shows the current organizaton in use.
3. **Video title:** Shows the video title name.
4. **Timestamp:** Shows the current local time of a video.
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:** Shows the current date and time in your local region.
9. **Show the timestamp.**

10. **PLAYBACK:** Shows a recorded video segment.
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.
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. **Timestamp:** 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. **Show and drag a recorded video segment.**
22. **Fast rewind:** Fast backward to a video timestamp 10 seconds ago.
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:** Current playback point.
27. **Fast forward:** Fast forward to a video timestamp 10 seconds later.
28. **Timeline zoom-in/out.**
29. **Show/Hide timeline panel.**
30. **Show/Hide control panel** (Control panel and display panel are shown below).
31. **Enter fullscreen** (press Esc to exit).



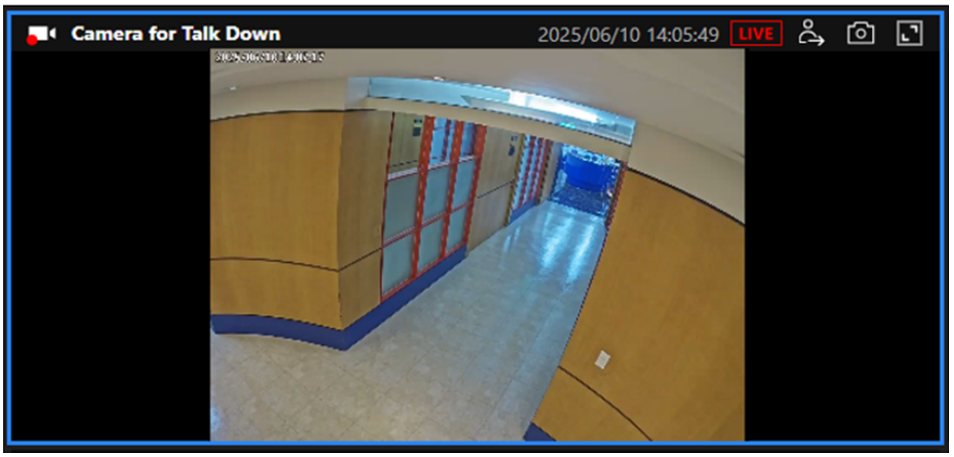


- **Control panel:** shows network connection info and model name. You can also control image ratio, audio volume, stream quality and digital zoom (if available).
- **Display panel:** lets you decide how you want to display the information on camera type, name, and time. You can also decide if to turn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

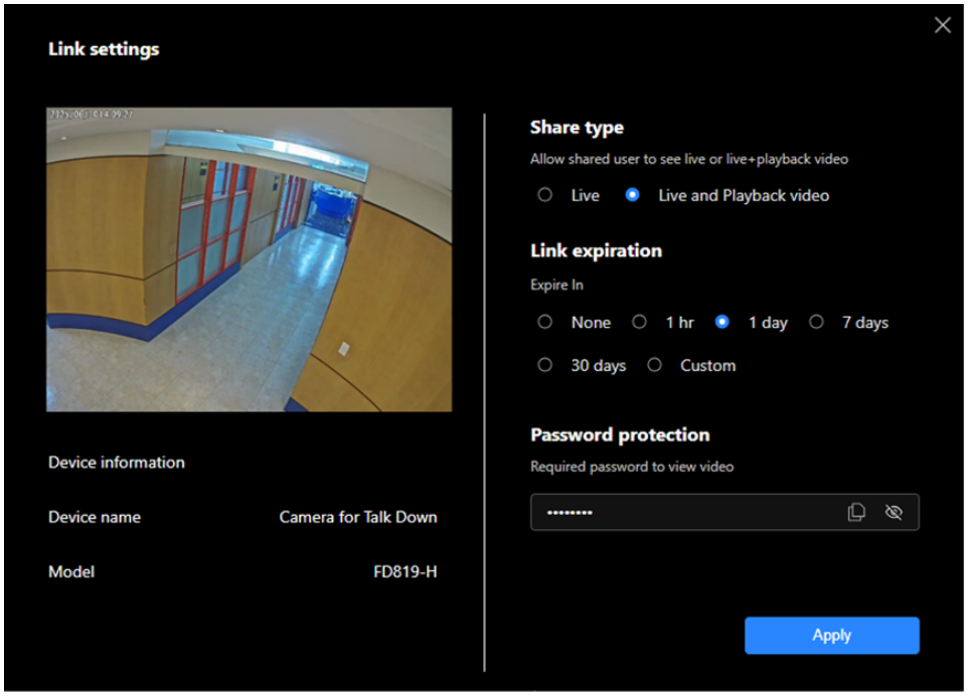
Sharing device live view and playback

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.

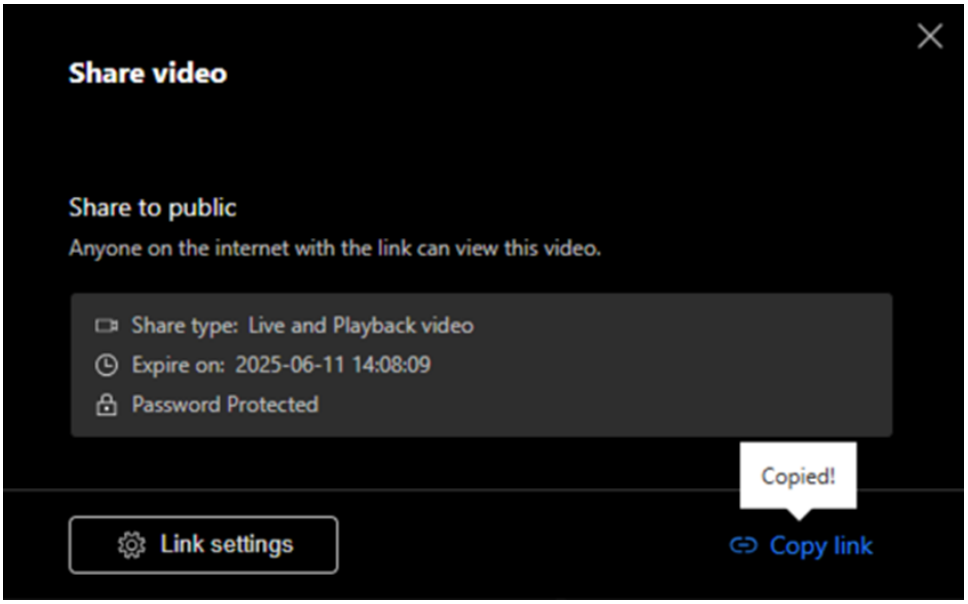


2. In the link setting page.



- Choose a **share type**
  Live: Share only the live stream of the camera.
  Live and Playback: Share both the live stream and past video footage.
- Set an **expiration date** and **password(mandatory)** for the shared link to control access.
- Then, click **Apply** to generate the share link.

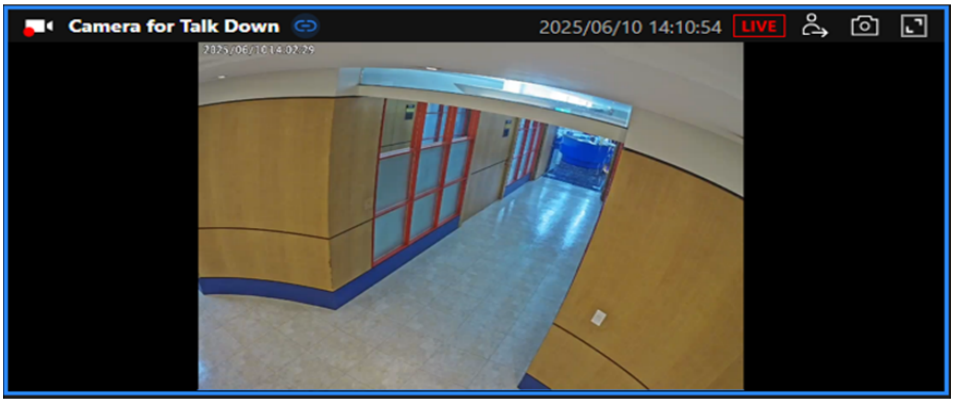
3. The shared link information will be displayed. Click Copy link to copy the URL.



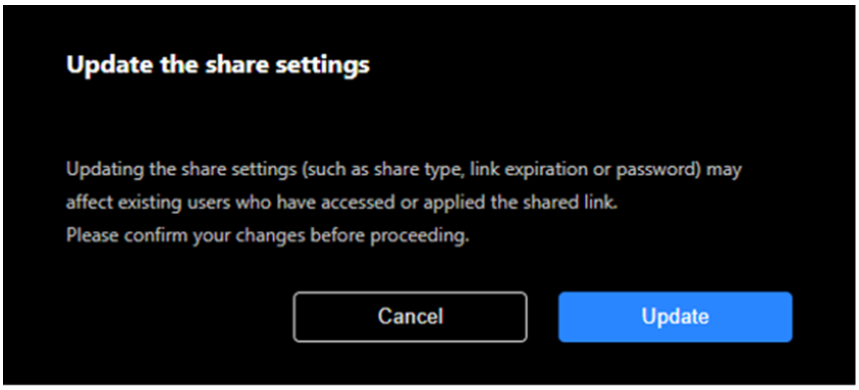
4. Share the URL (copied link) with the external parties.

5. 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.

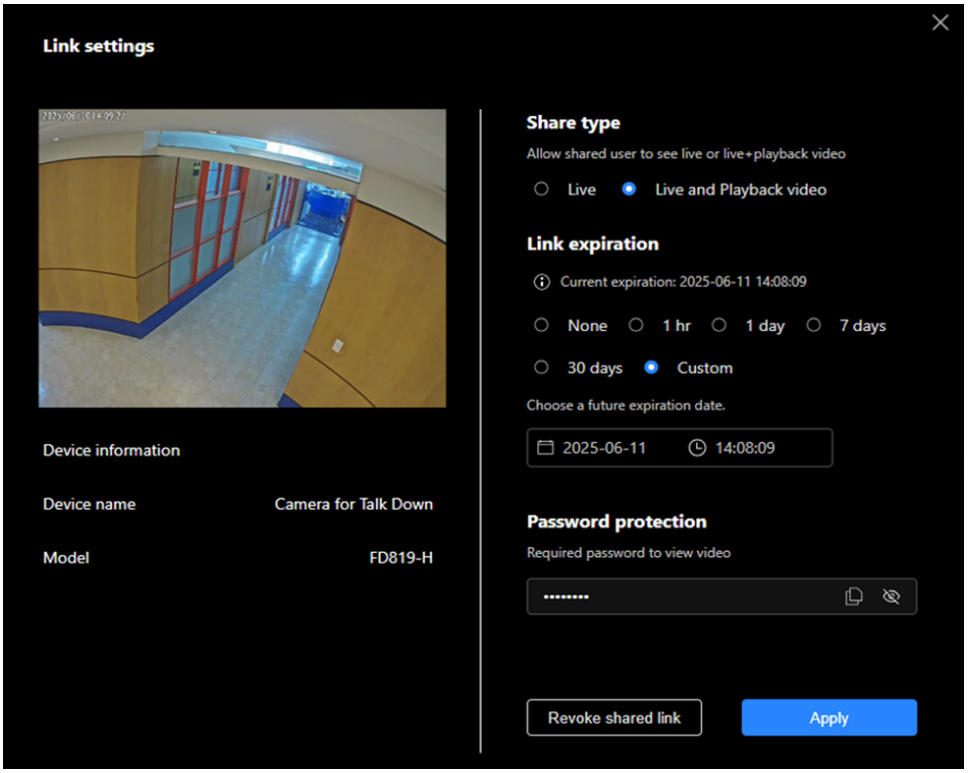
6. A camera with an active shared link will display a blue mark on its view cell.



7. 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.



8. 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.

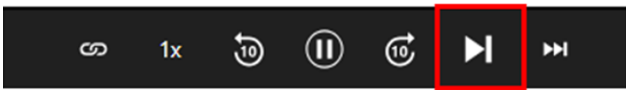


Frame by Frame Playback

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

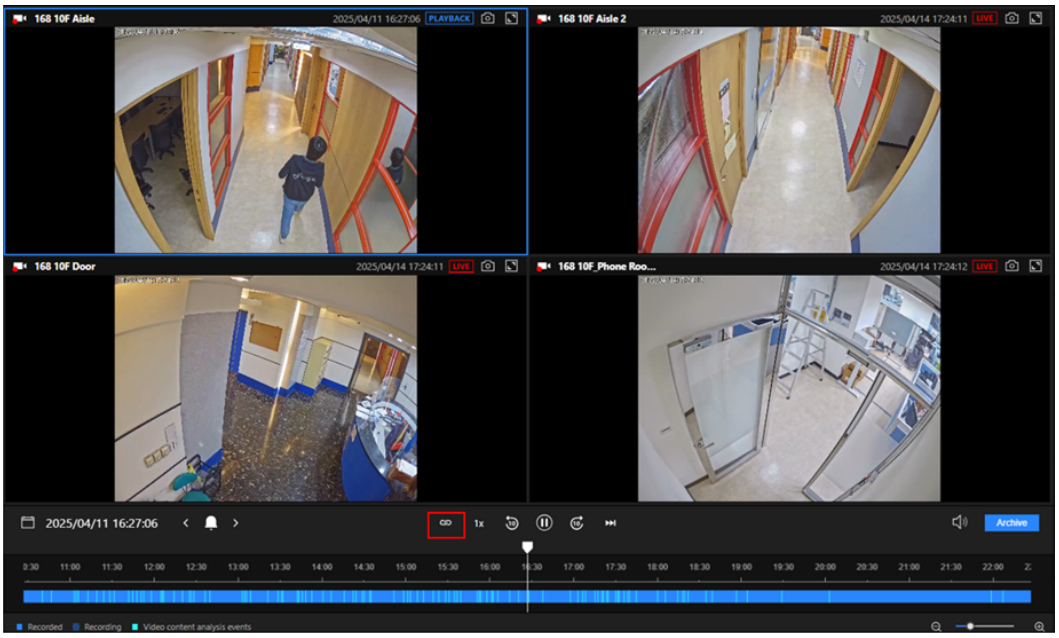
Synchronized playback supports up to four cameras playing recordings simultaneously in the same view, helping users quickly grasp the full view of an event.

1. Focus on a single camera view cell in the playback mode, you can then enable synchronized playback.

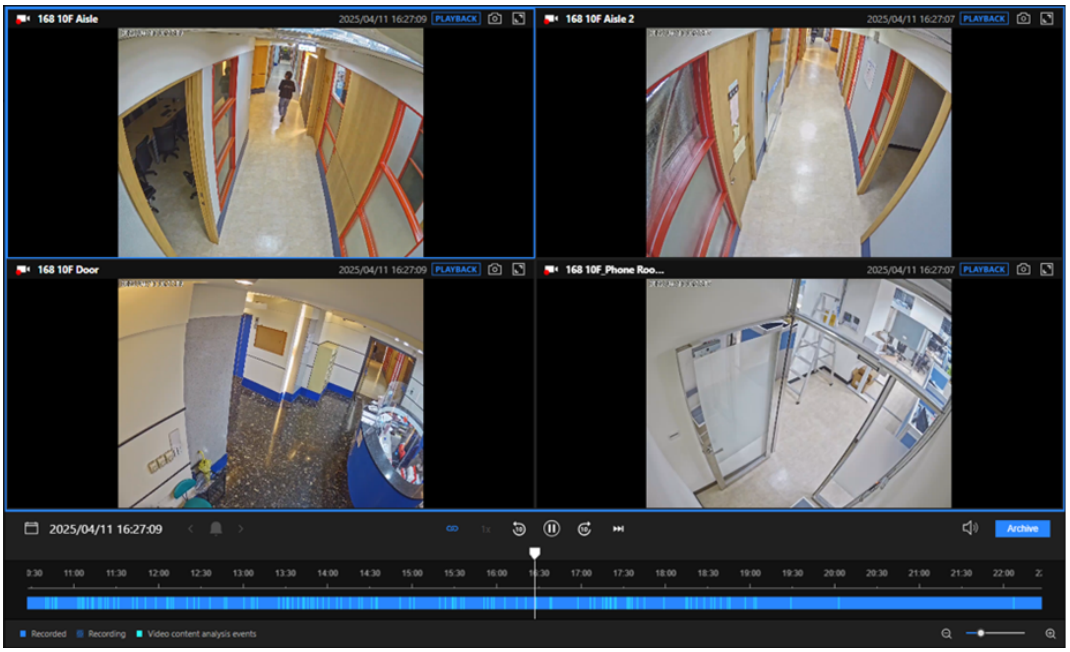
Note

Synchronized playback supports only the following layouts: 2x2, 1P+3, and 3V.

2. Click the Synchronized Playback icon ( )



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



Note

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.

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 (⏭)

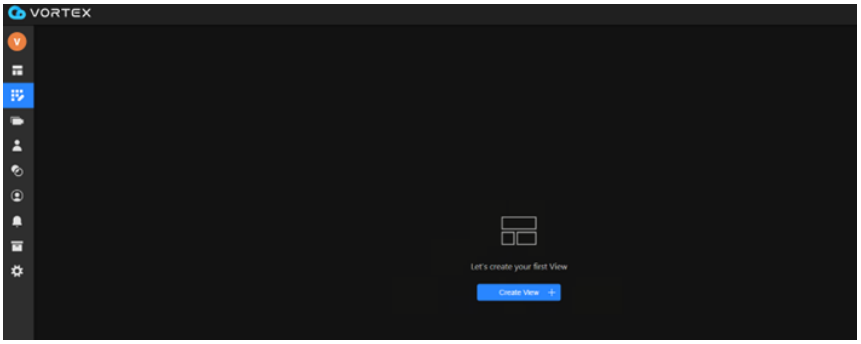
Customized view

6

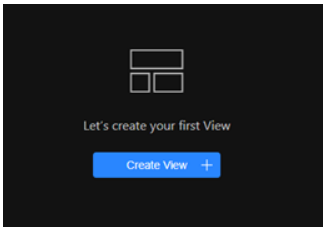
Customized view is a feature for users to create personalized view by grouping cameras from different sites into a single view page. Therefore, users can conveniently monitor live or playback footage from multiple camera groups on one unified page.

Create a customized view

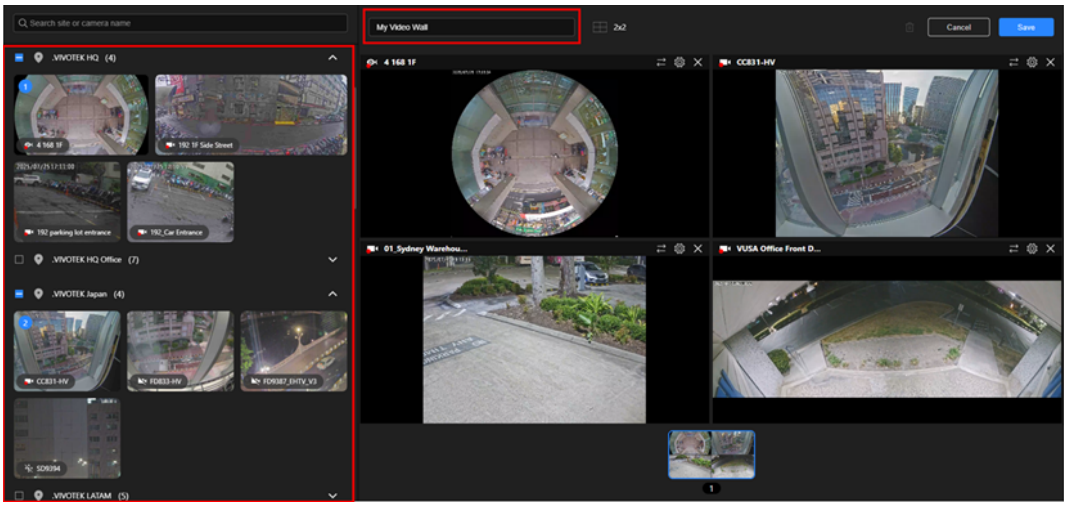
1. Click the Customized View icon, on the side menu.



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

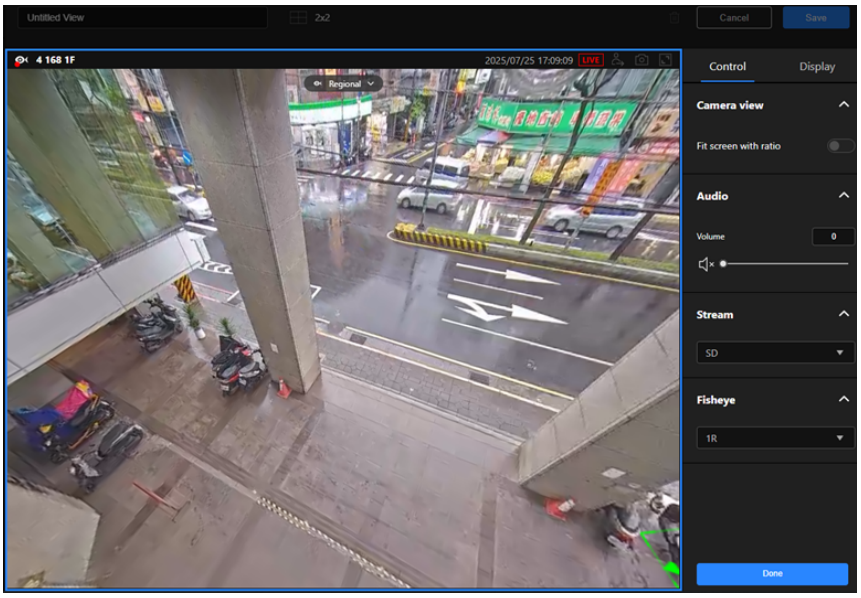


3. Name your customized view and select cameras from the left panel. Once selected, the cameras will be added to your customized view shown on the right panel immediately.

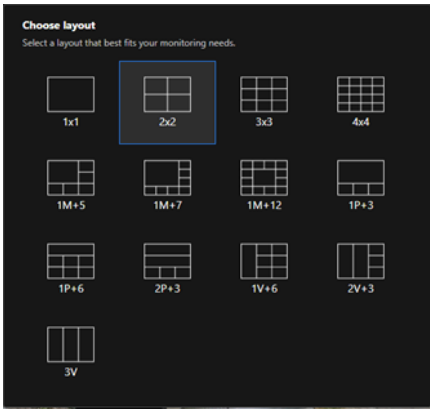


4. To configure the preferences for your selected cameras, click setting icon on each view cell. After completing the configuration, click Done.

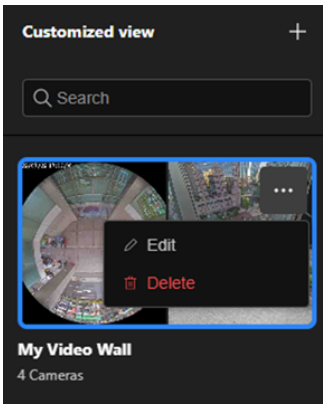
- Fit screen with ratio
- Audio volume
- Stream (SD, HD)
- Fishey dewarp (for fisheye camera only)
- Zoom in/ out



5. Click Layout icon 2x2 to choose your preferred layout.



6. You can also move the positions of the cameras on your customized view by clicking .
7. Once you're done configuring, click Save. You customized view is now created. Your customized view will reflect your preferred layout and camera positions. Additionally, the preferences for each view cell will be displayed when you focus on it.
8. You can enter the Edit mode and change the configurations for your customized view anytime.

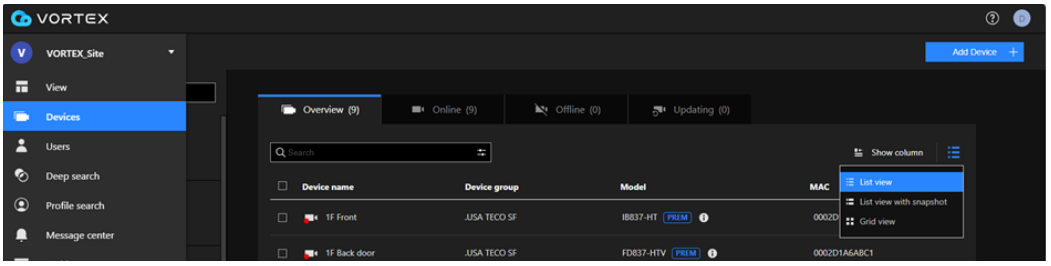


9. Please note that the configuration changes will only be saved when made in the Edit mode.

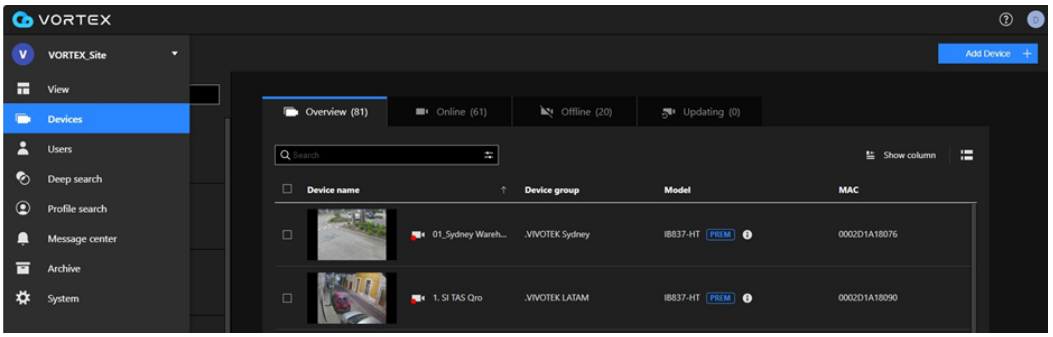
Devices

7

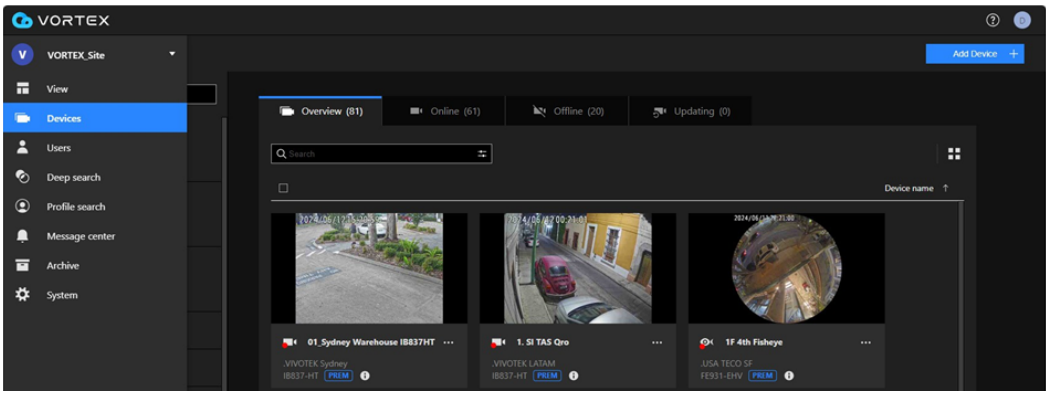
The VORTEX Devices pages show all available cameras, NVRs, and other devices used by an organization in List view, List view with snapshot, and Grid view. For each device, the device name, device group, model name, MAC address, and other settings can be found on this page.



List view



List view



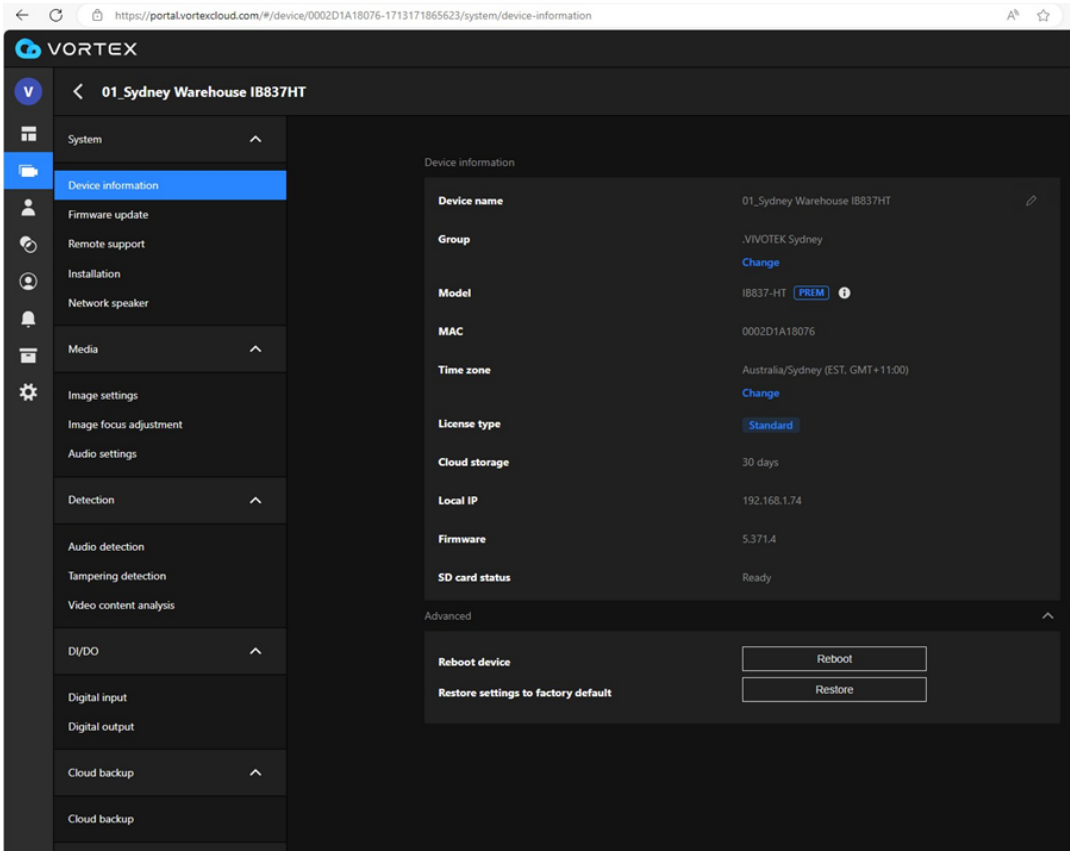
Grid view

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.

System > Device information on VORTEX camera

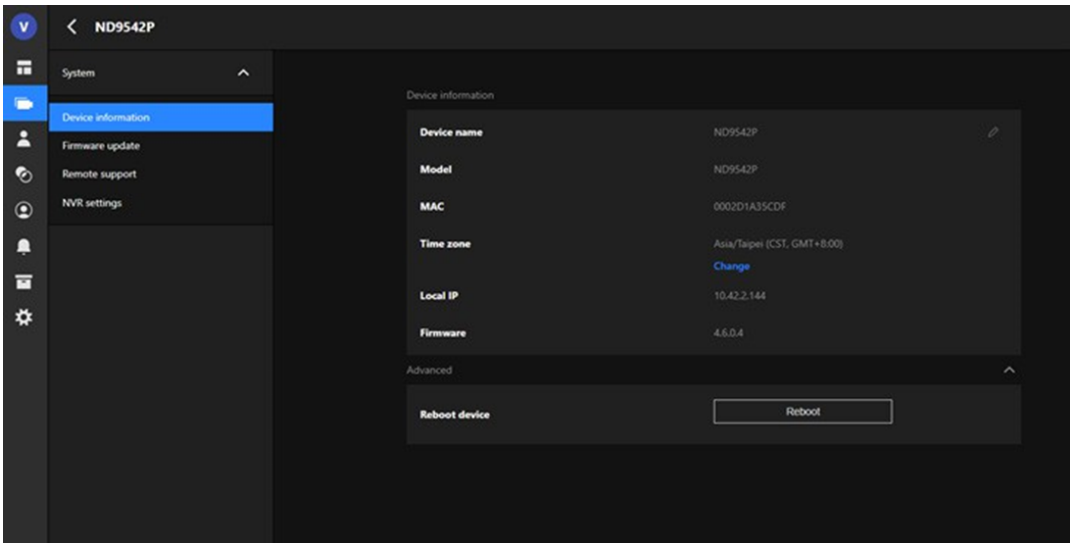
If you click Settings, the device information, its corresponding options, and other categorized options (as shown on the left of the workspace) will appear:



Device information

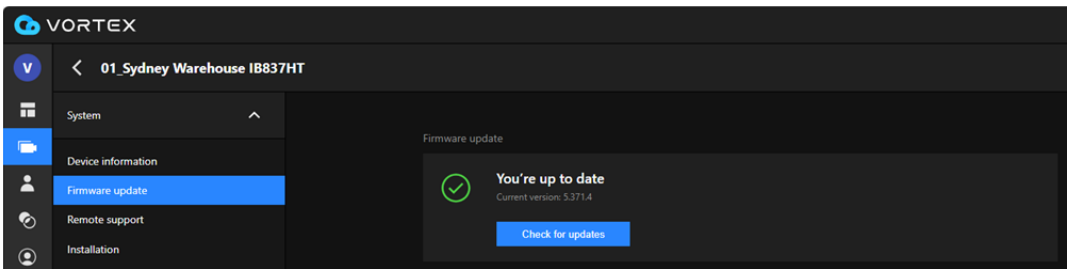
System > Device information on VIVOTEK NVR

If you click Settings, the device information, its corresponding options, and other categorized options (as shown on the left of the workspace) will appear:



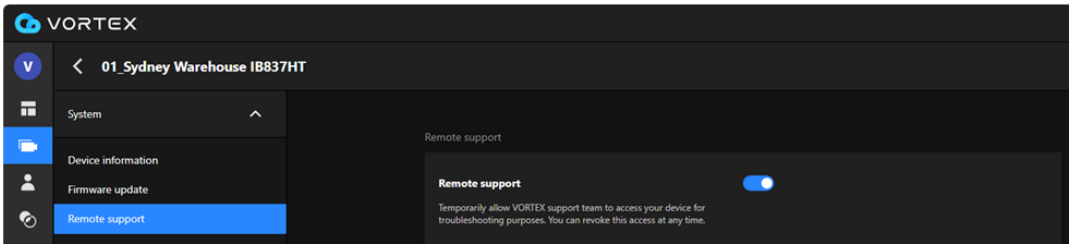
System > Firmware update for both VORTEX camera & VIVOTEK NVR

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



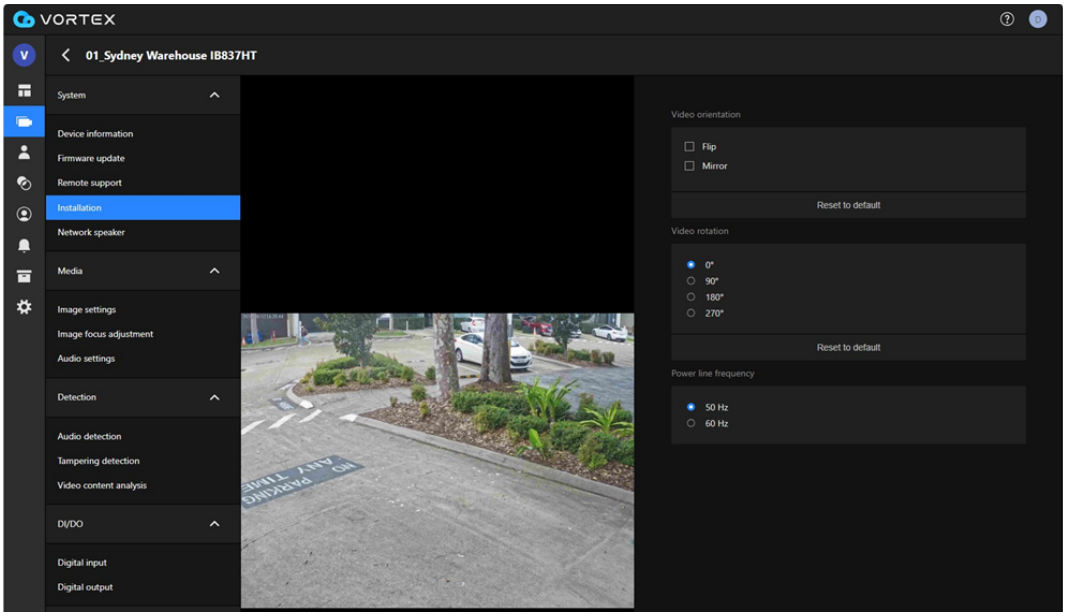
System > Remote support

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.

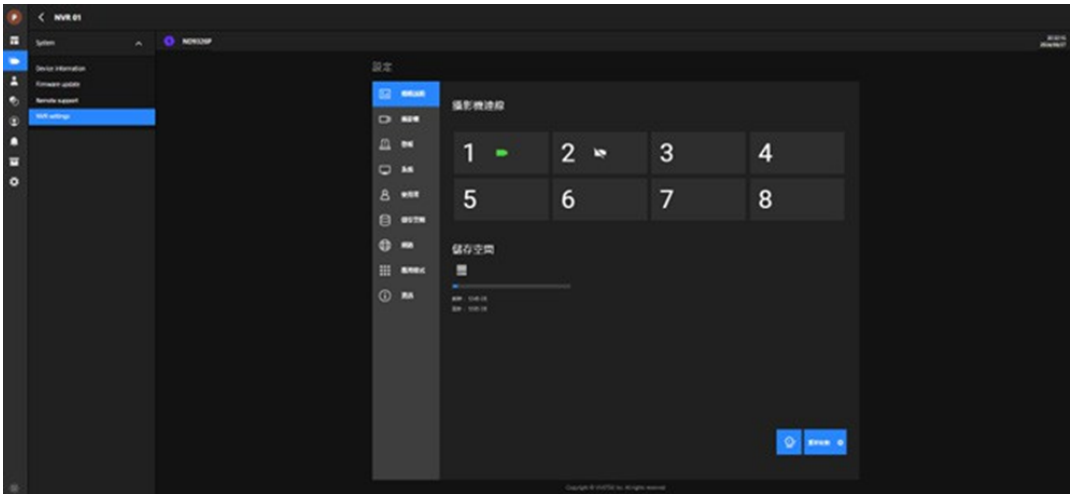


System > Network speaker

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.

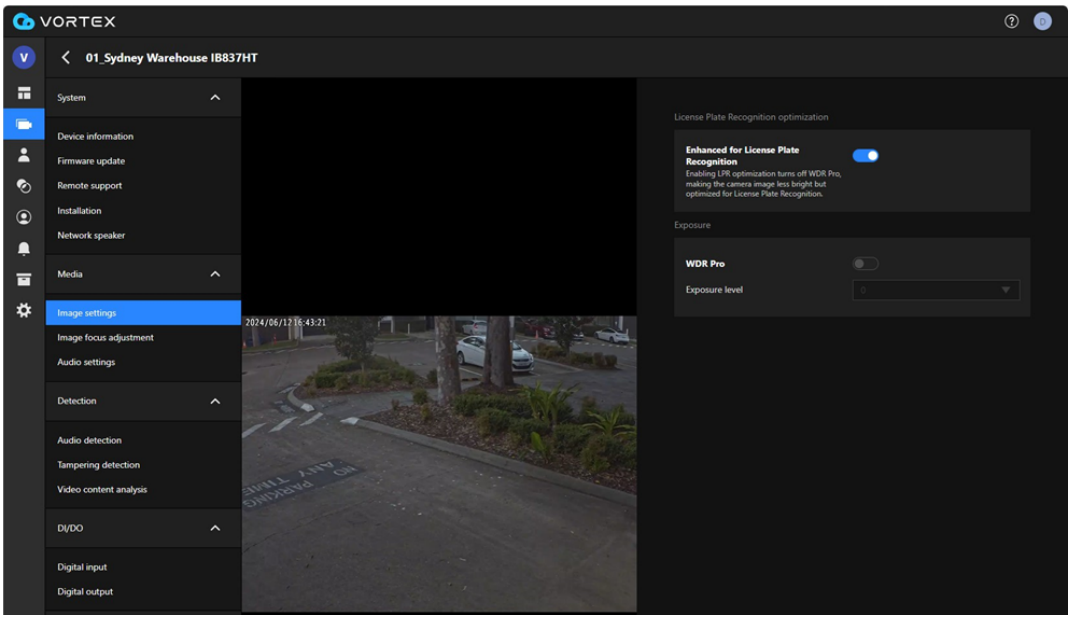
System > NVR settings

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



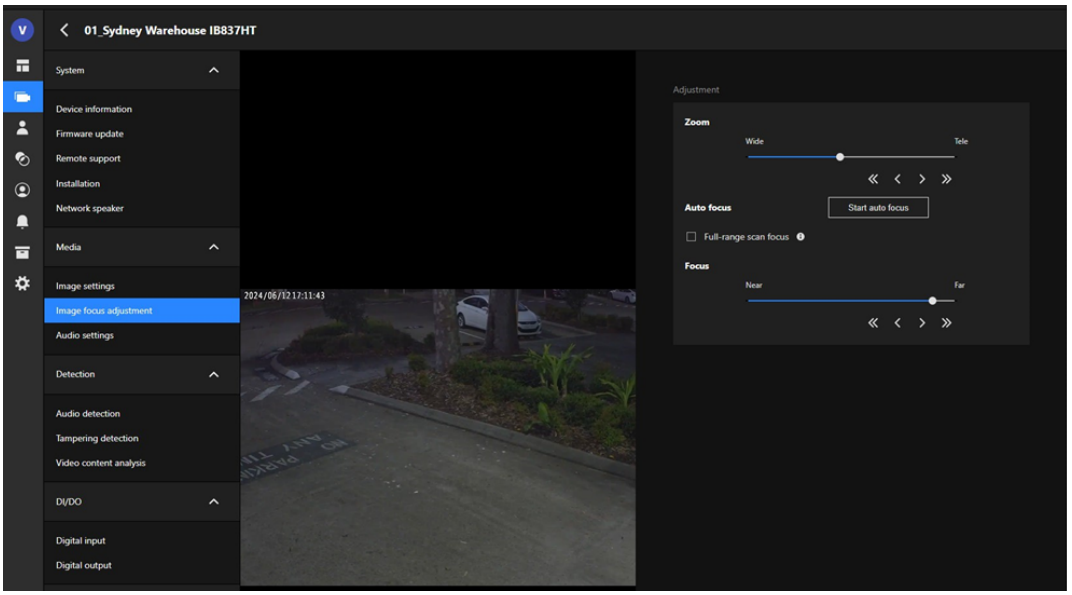
Media > Image settings

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

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.

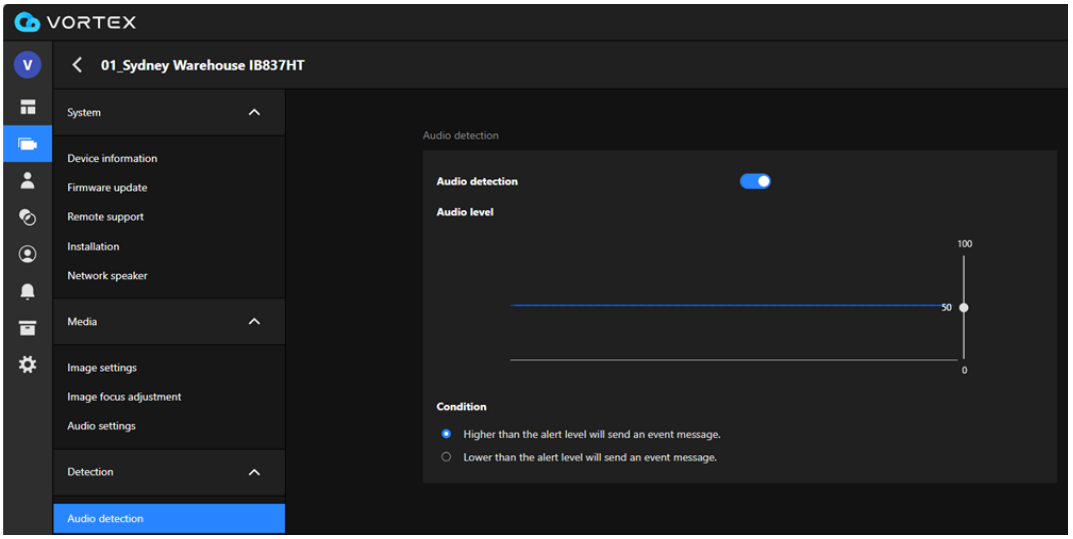


Media > Audio settings

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

This is how you decide if you want to trigger an event based on the audio volume level. Drag the circle to decide the audio point to trigger the event.

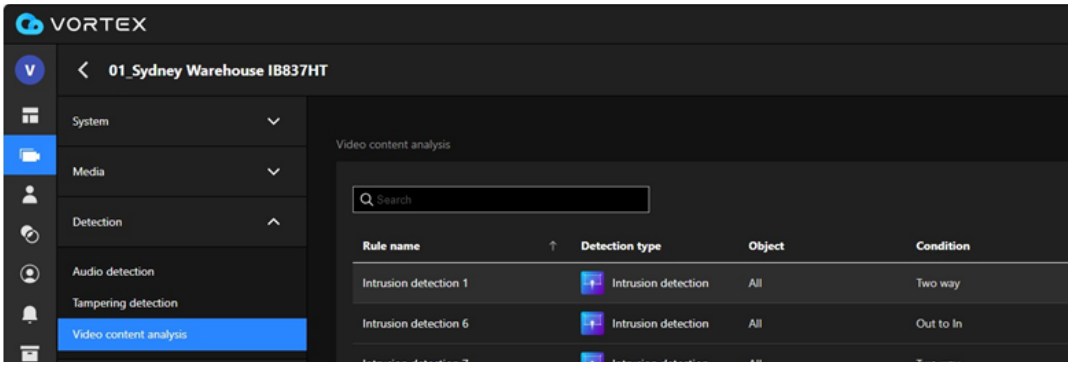


Detection > Tampering detection

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

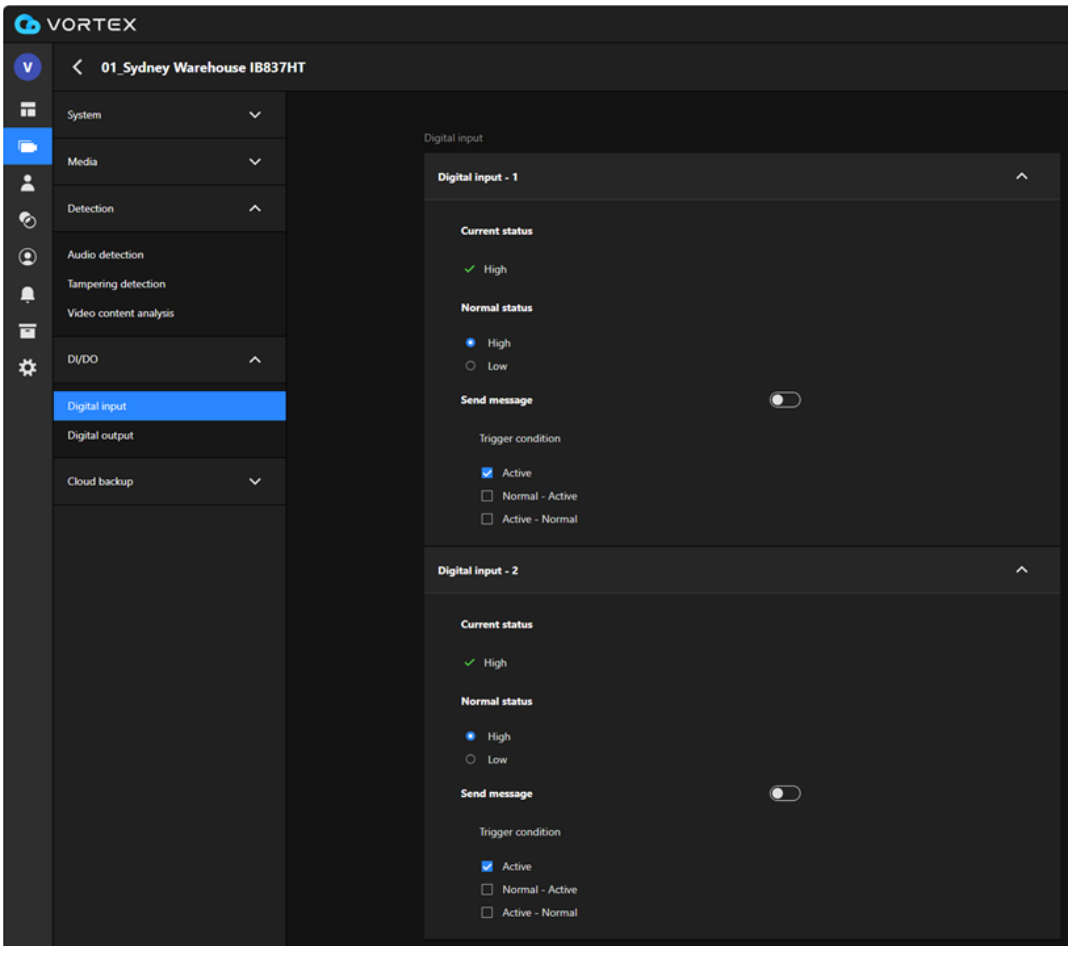
Detection > Video content analysis

This is where all video content analysis rules are stored. You can click "..." and select an option for editing.



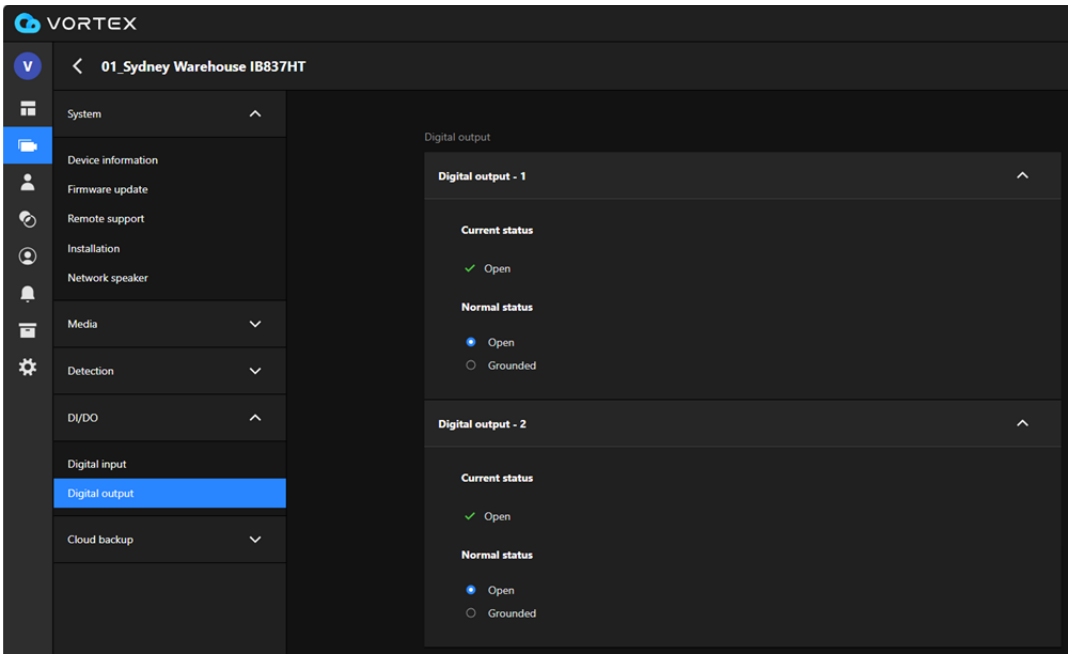
DI/DO > Digital input

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.



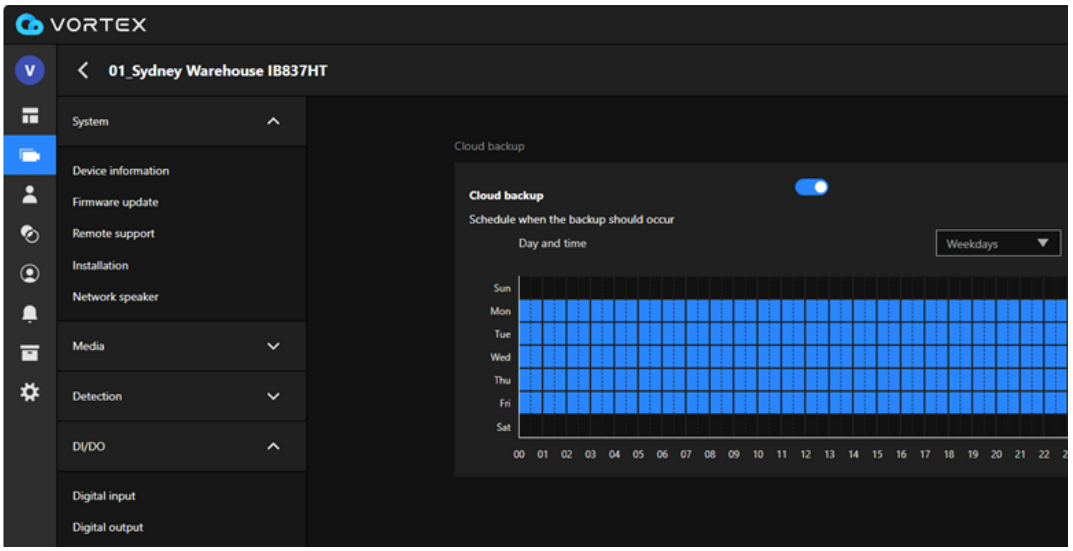
DI/DO > Digital output

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.



Cloud backup > Cloud backup

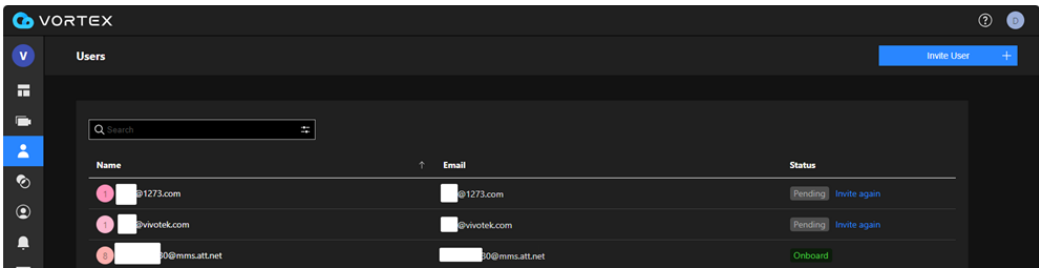
Enable Cloud backup by sliding the toggle button. When enabled, videos will be stored in the cloud storage. Set your desired schedule to back up your video footage to the cloud by selecting an option from the drop-down list or dragging the mouse across the screen.

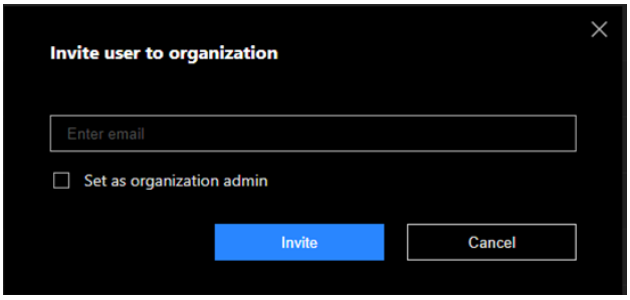


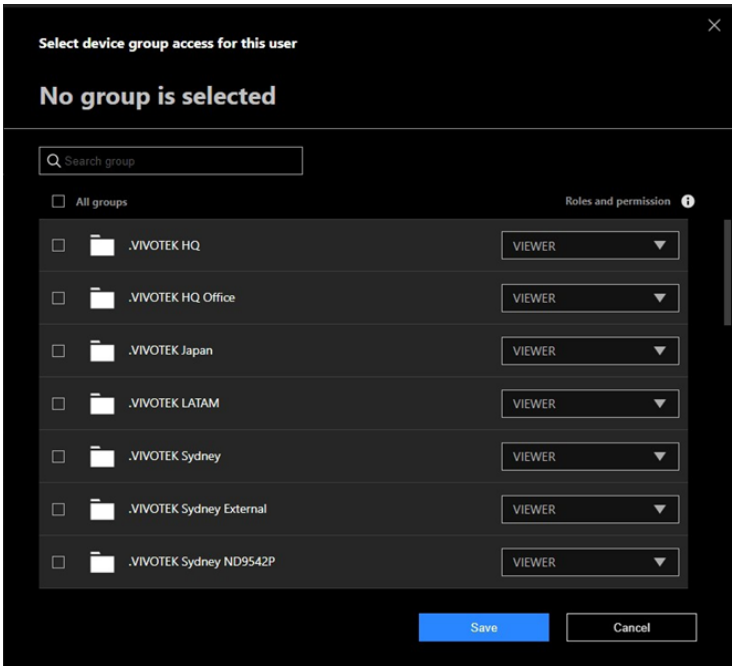
Users for VORTEX camera & VORTEX Connect Pro

8

Select users by inviting them. To do so, click the "Invite User" button on the upper-right corner. Then, you can select what devices the user can use.







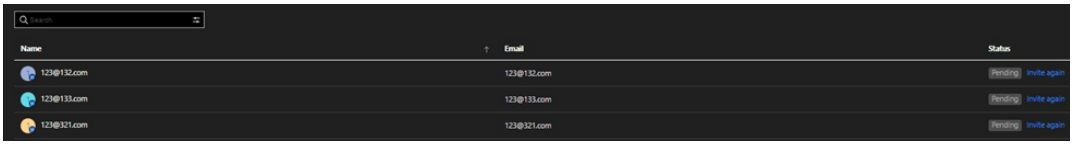
NOTE

- Only the owner and an administrator can invite a user to be an administrator.
- User access rights can be set or edited on this Users page.

Users for VORTEX Connect

9

Select users by inviting them. Since VORTEX Connect is a free service, once you invite a user successfully, you cannnot assign the user to any certain devices only.



Deep Search

10

Deep Search is a post-search function that allows users to efficiently search objects (people or vehicles) in recorded videos. Application scenarios include searching for a thief in a department store, a lost child in a station, or a suspect vehicle.

With AI capability, the video content is analyzed in real-time, and objects and their attributes are extracted in advance as metadata. With Deep Search, you do not have to have many human eyes to watch recorded videos of many cameras frame by frame just to search, for example, a person wearing a red T-shirt and blue jeans. The search time may decrease tremendously from days to minutes.

The key feature of VORTEX Deep Search is that the core of video analytics is done at the edge (edge AI computing), not on the cloud server side. The onboard video analytics detect and track objects (both essential and premium cameras) and extract the object's

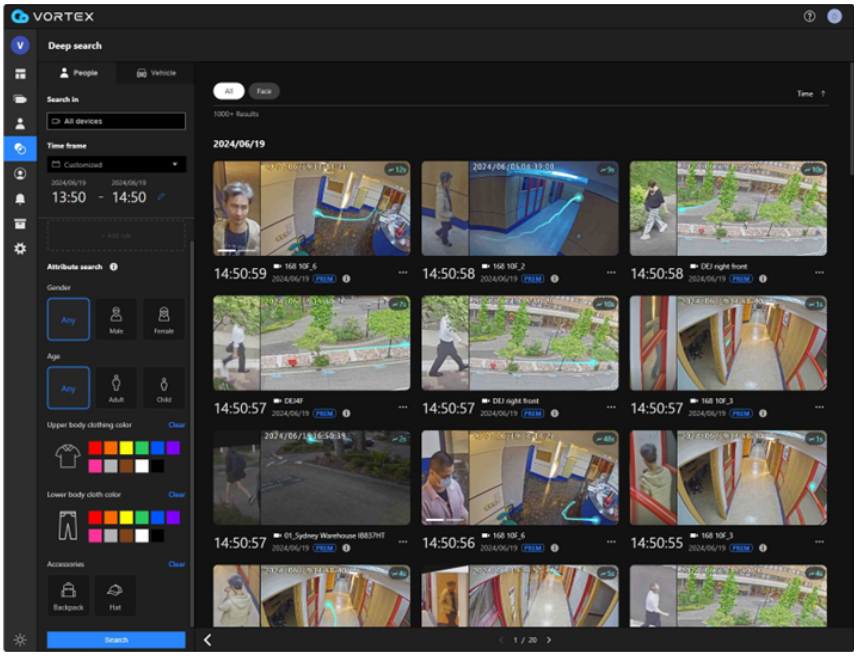
attributes (premium camera only). Then, deep search is based on video analytics metadata to search the object, so the search performance is dramatically faster than that of a server- based solution.

Note

VORTEX Connect PRO does not support Deep Search at this moment.

Using Deep Search

On the left side menu, click "Deep search". The default search results will display. Note that the default settings are people search, search in all cameras, and the search time interval (time frame) is the last one hour. Therefore, the default search results show people appeared in all cameras in the VORTEX organization in the last one hour.



Example of the default Deep Search results

Using Deep Search to search for people

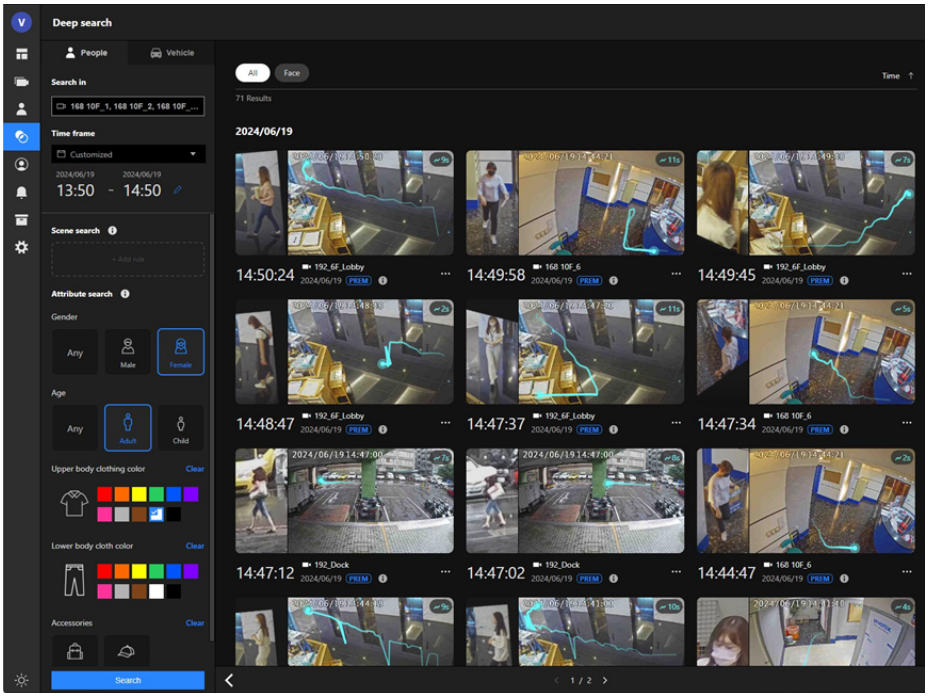
1. On the left side menu, click "Deep search".
2. Set up your search criteria based on the following condition(s) as shown on the VORTEX left panel:

- Which camera(s) to search
- 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

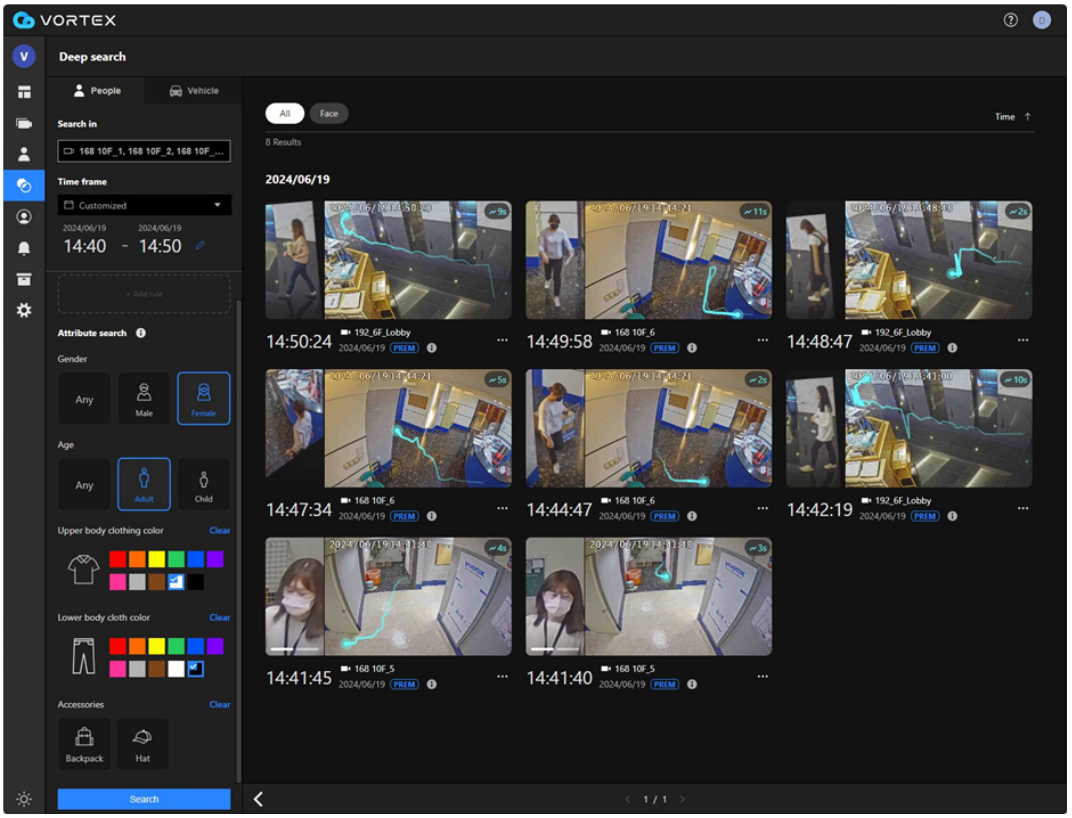
3. Click "Search".
4. The search results appear. Note the following:

- Each search result is composed of two parts. The left image is a representative snapshot of the object (a person) in the detected and tracked time interval, while the right one is a snapshot of the camera view.
- The moving path of the person is overlaid on the right image to let users easily know how the person is moving in the captured time interval.

5. Click the scene snapshot of a search result to open the playback page, and the recorded video with the person in the scene will be played. Click "Archive" to save the video as needed.



6. You can also narrow down your search by adding more search criteria (e.g., shorten the time frame) as needed.



Using Deep Search to search for vehicles

1. On the left side menu, click "Deep search".
2. Set up your search criteria based on the following condition(s) as shown on the VORTEX left panel:

- Which camera(s) to search
- 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)

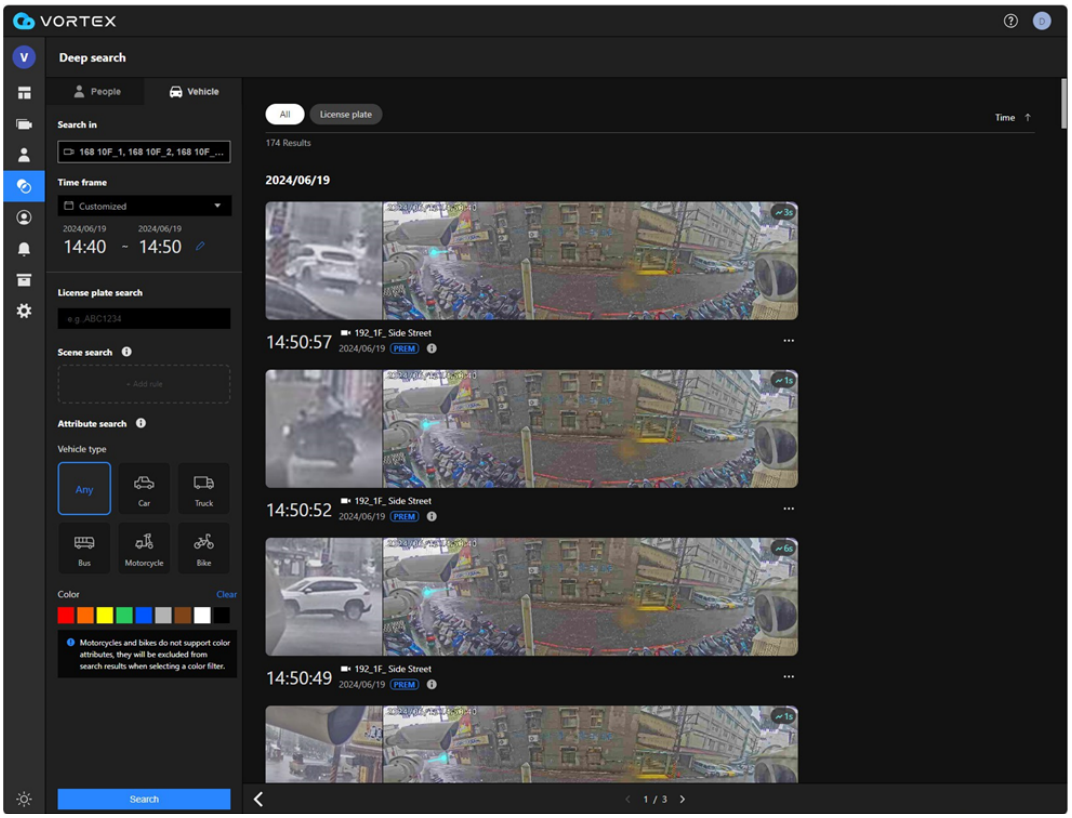
3. Click "Search".
4. The search results appear (including licence plate number if you click "License plate").

Note the following:

- Each search result is composed of two parts. The left image is a representative snapshot of the object (a vehicle) in the detected and tracked time interval, while the right one is a snapshot of the camera view.

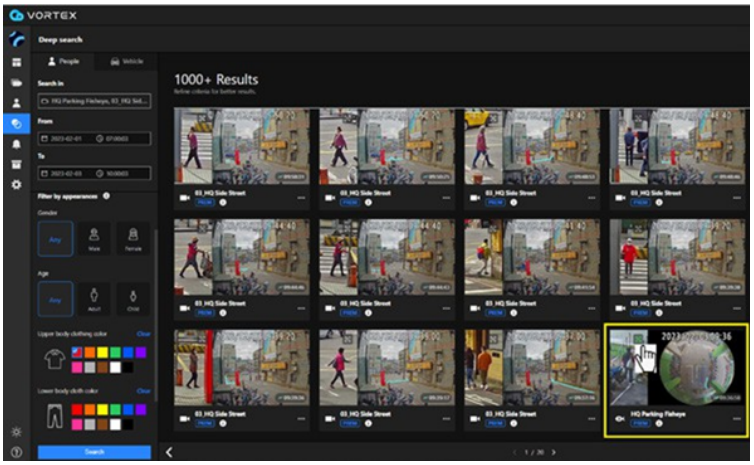
- The moving path of the vehicle is overlaid on the right image to let users easily know how the vehicle is moving in the captured time interval.

5. Click the scene snapshot of a search result to open the playback page, and the recorded video with the vehicle in the scene will be played.



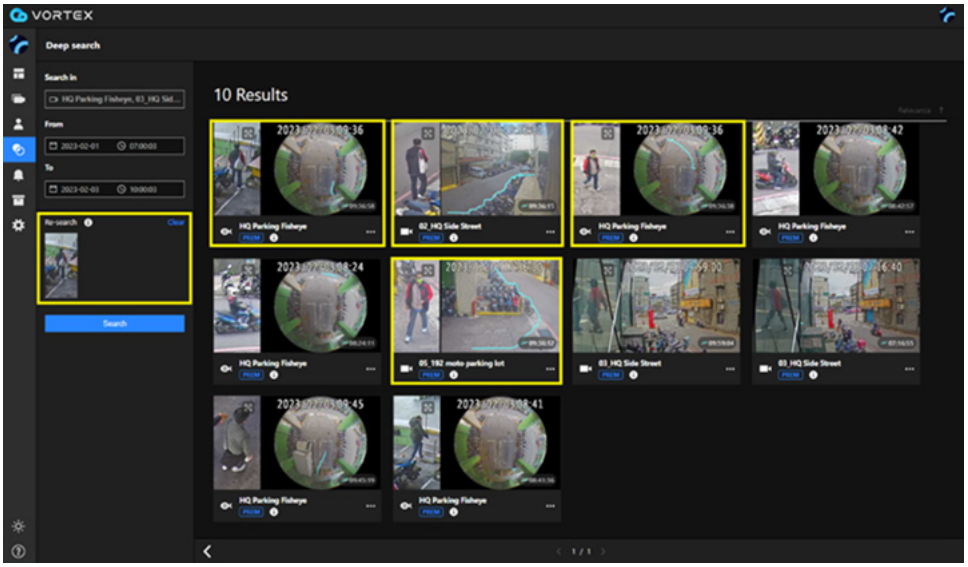
Using Re-Search

The Re-Search function is based on the technology of person re-identification (Re-ID). When you find a person in the search results, you can use Re-Search to search for this person by his/her snapshot across all selected cameras. As the example shows, you can click a person snapshot of interest to do Re-Search.



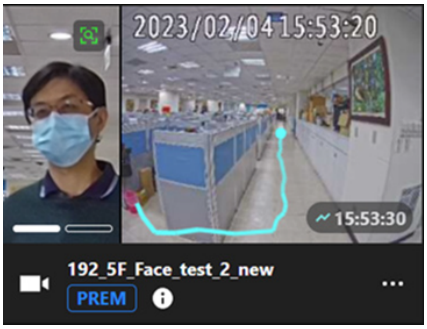
Click a person snapshot of interest to do Re-Search.

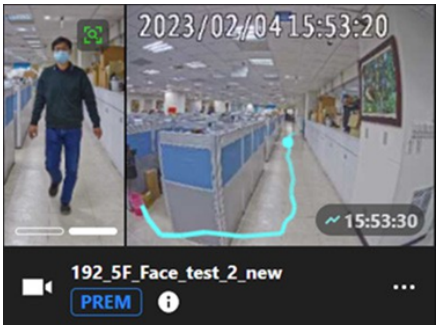
The example below uses the selected snapshot to do Re-Search. Among the 10 search results, it is confirmed that the first three video clips and the sixth video clip are the same person captured by different cameras. It shows that Re-Search helps cross-camera search efficiently.



Person re-identification (Re-ID)

When a person's face's resolution is good enough to provide face features, there will be two snapshots on the left. One image is the face snapshot, and the other is the whole body snapshot. You can click the white bar at the bottom of the snapshot to switch between the two images. The face features, if available, will also be used for the search of a person.



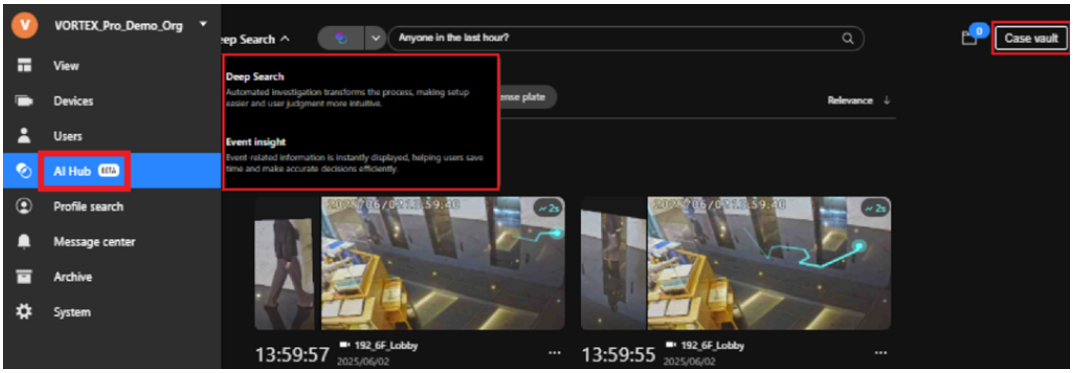


AI Hub

11

AI Hub is a centralized platform within VORTEX designed to unify and streamline all AI-powered surveillance features. It provides users with a single interface to access Deep Search, Event insight, and Case Vault, making surveillance operations more efficient and intuitive.

Note
AI Hub will be released initially as a beta version



Deep Search

Deep Search allows users to quickly find relevant video footage based on specific objects or contextual information. It includes two main modes:

Search by Text

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

Best practice

We suggest structuring queries as follows:
[Person or vehicle] + [action/descriptor] + [optional connector] + [optional second descriptor] + [optional location]

Example:
Person wearing a black jacket with sunglasses at 7 am on the street.
Person carrying a large backpack with headphones in the library.

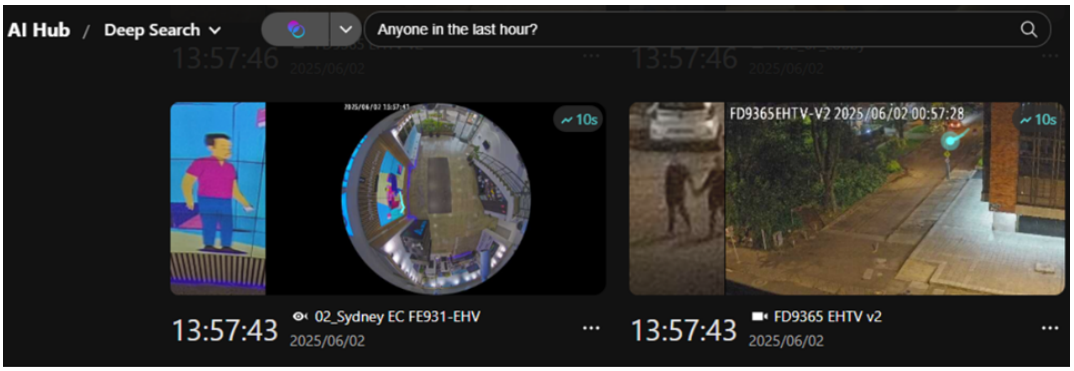
Supported languages

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).

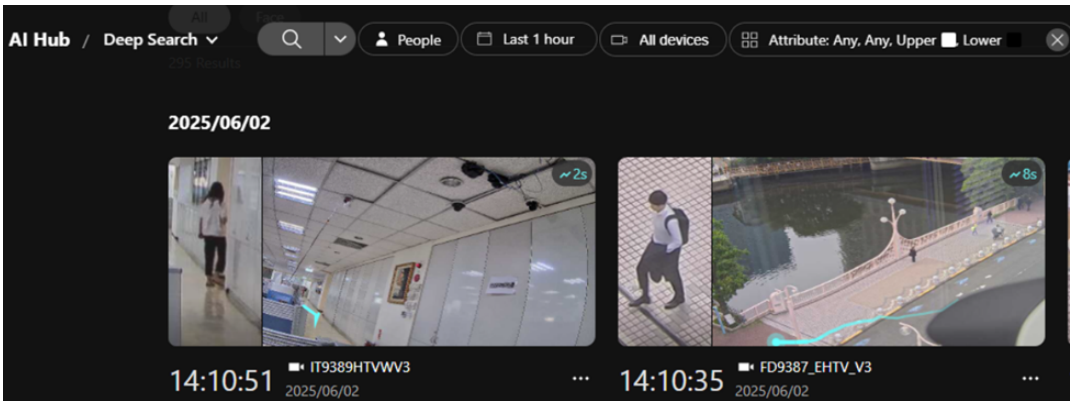
Known Limitations:

- Accuracy decreases when searching for multiple people simultaneously.
- Difficult to identify small objects (e.g., phones, wallets, earbuds).
- May return imprecise results for action-based scenes (e.g., running or waving).



Search by Filter

This traditional filter-based search allows users to refine results by object type (e.g., person, vehicle), appearance attributes, tags, time range, and camera location. It is useful for precise filtering when specific conditions are known.

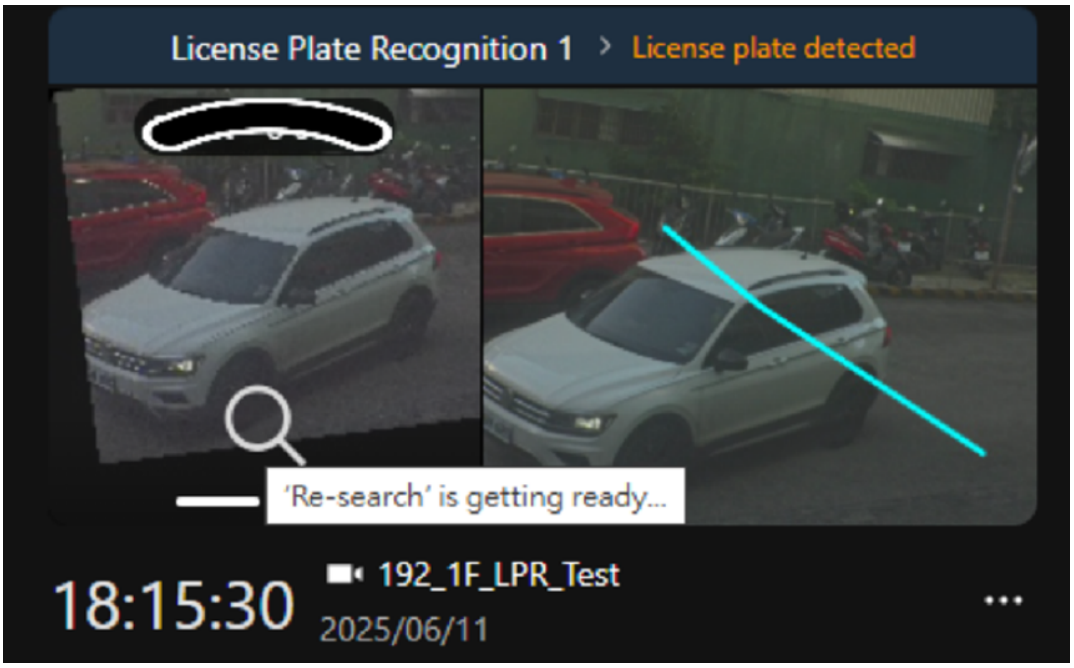


Event Insight

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.

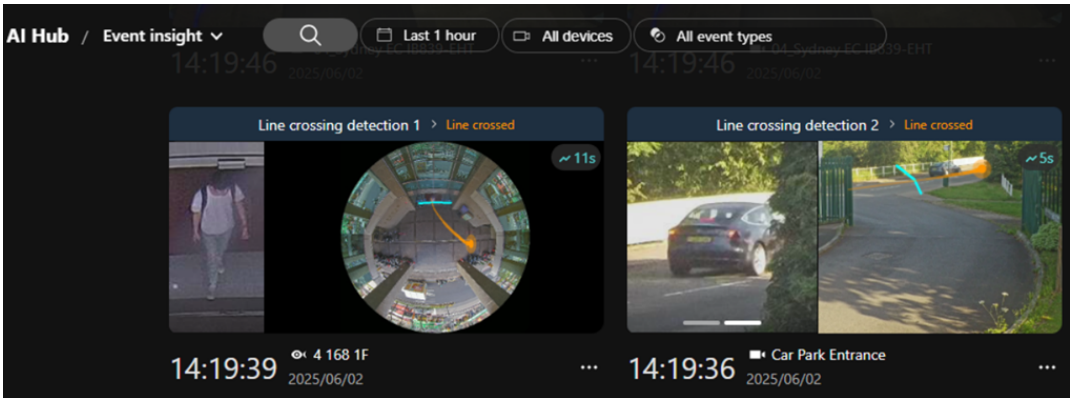
Known Limitations:

- 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.

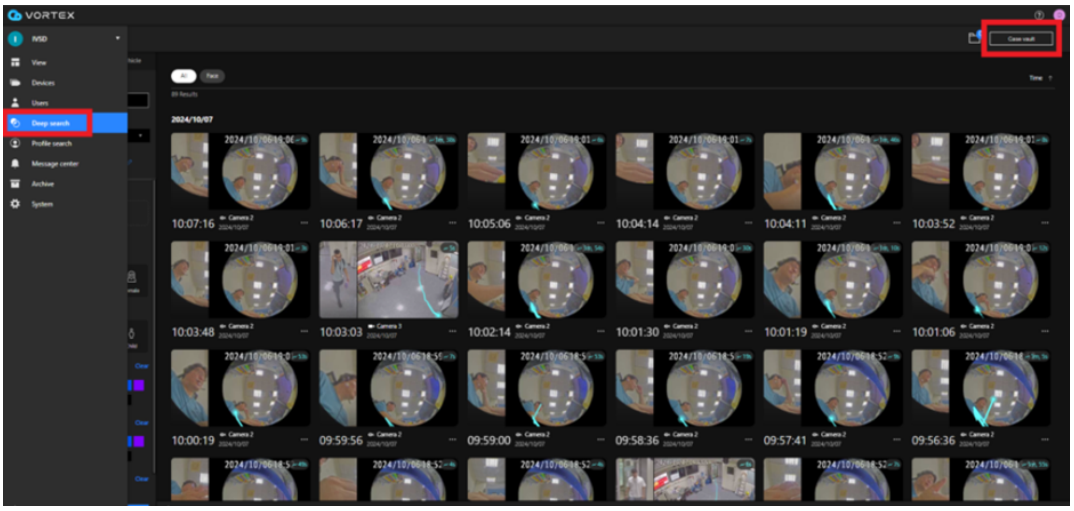


Case Vault

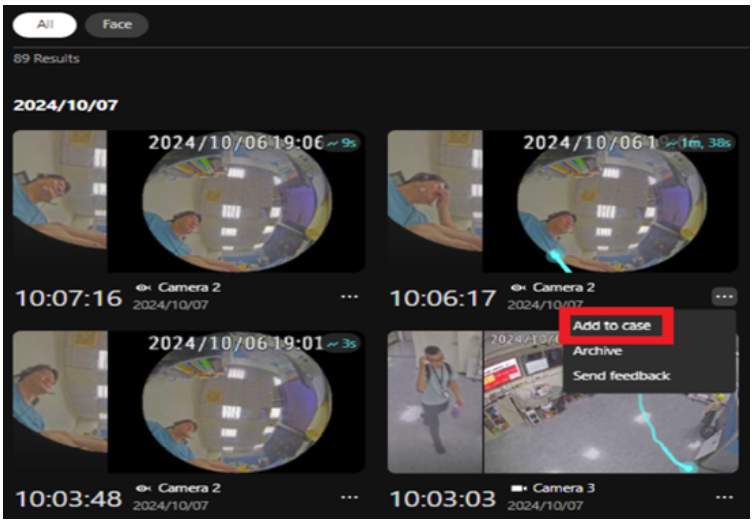
Case Vault is designed for securely storing and organizing critical footage related to investigations. Users can group video clips, add notes, and collaborate with team members — all within a dedicated case management space. This improves workflow for incident review, evidence sharing, and long-term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

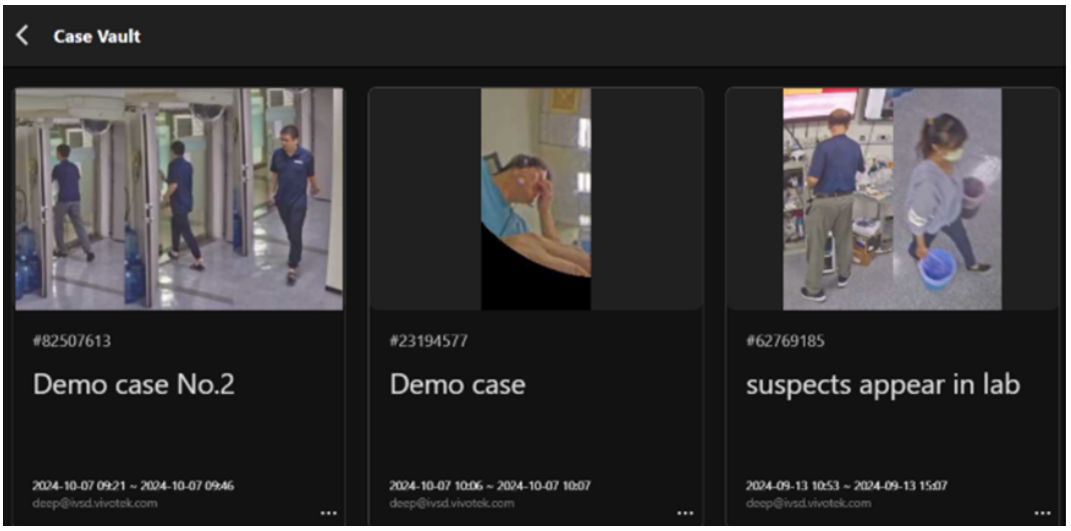


2. Create a New Case:
    1. Two ways to create a new case:
    2. Add one specific event to a case:
    3. Click more button of the specific event you need, and click "Add to case"



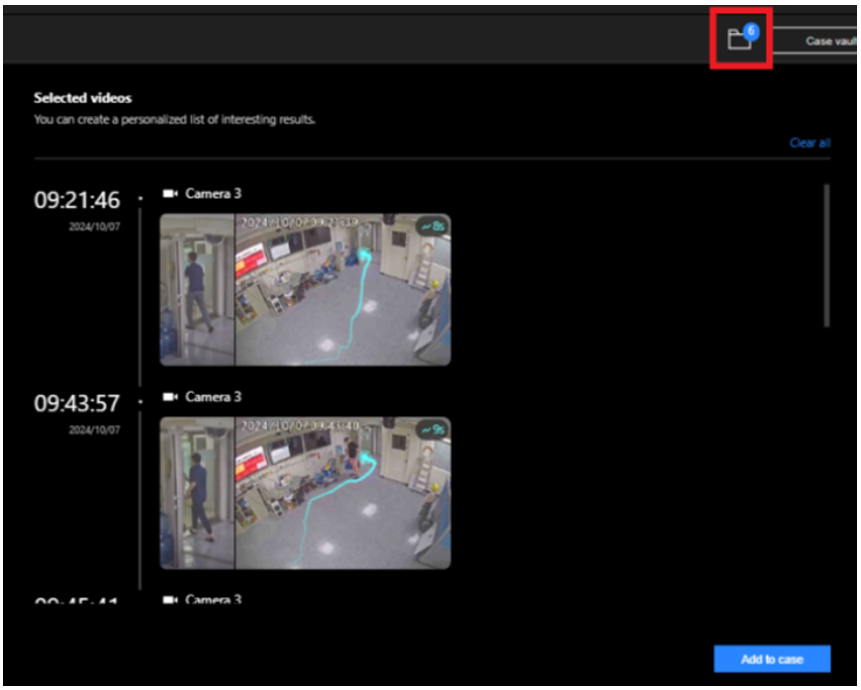
4. Add this event either to "New case" or the "Existing case", and click "Add" to next step

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

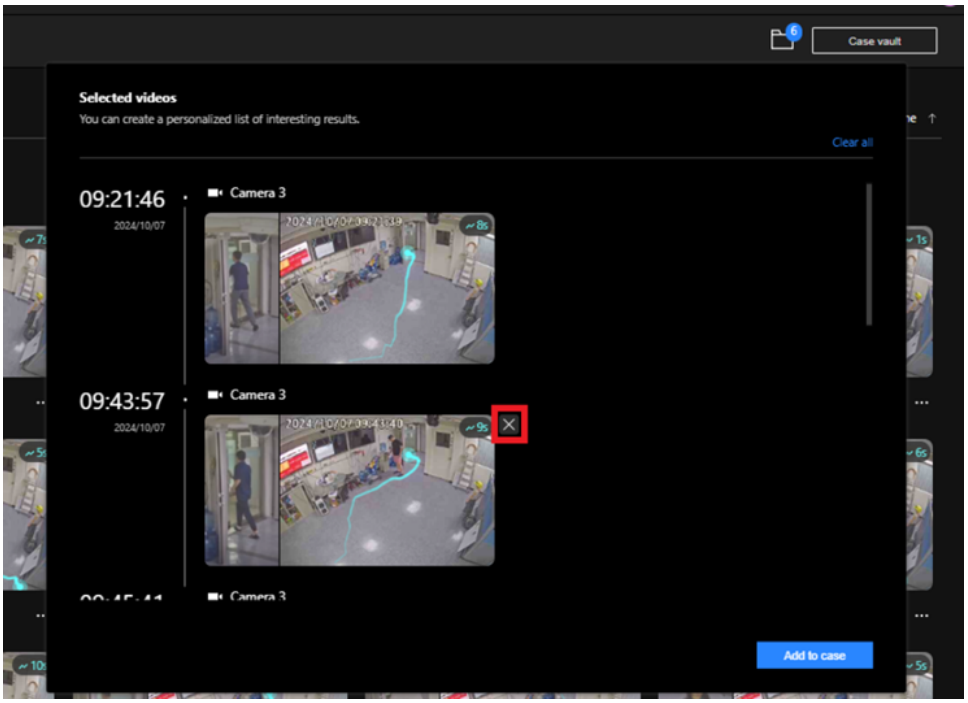


3. Add a series of events to a new case
    1. Select events by click checkbox to this new case

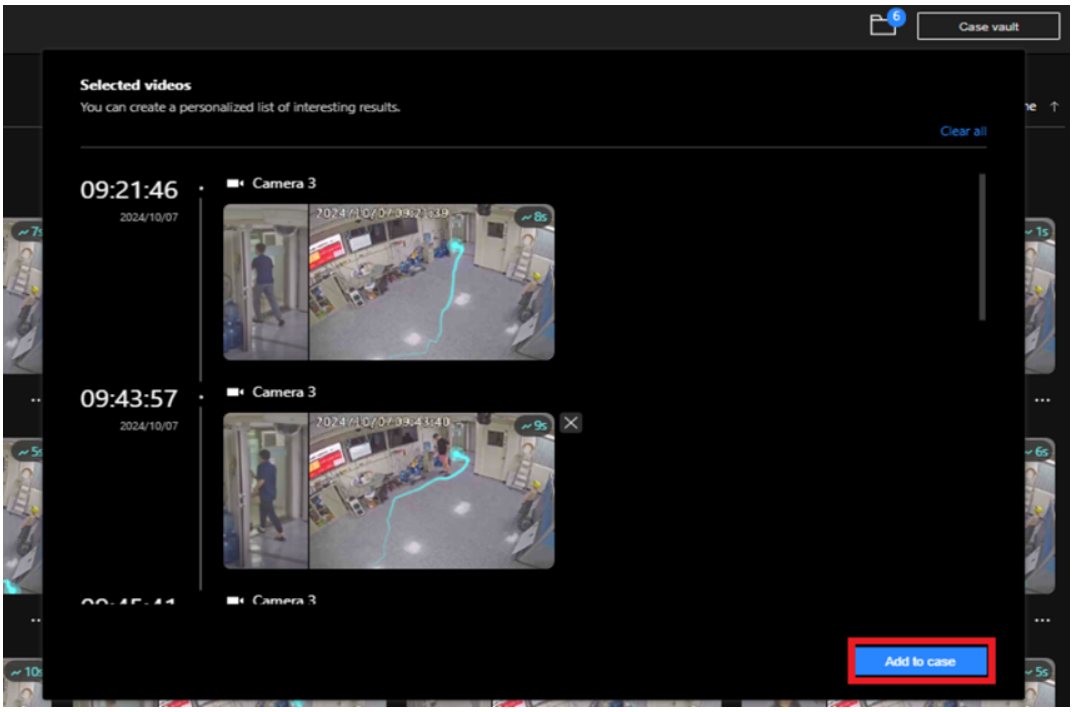
    2. You can find those selected videos has been added to the folder



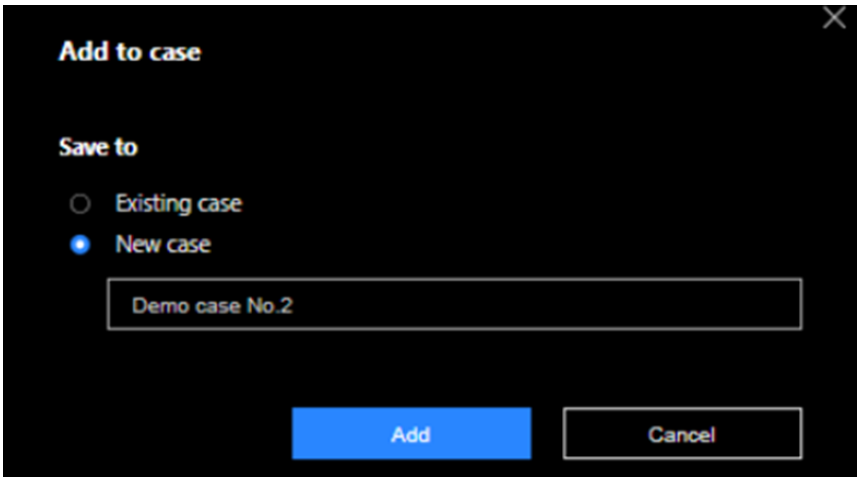
3. If there's any video you don't need, you can delete it by click "Delete" button next to the video thumbnail



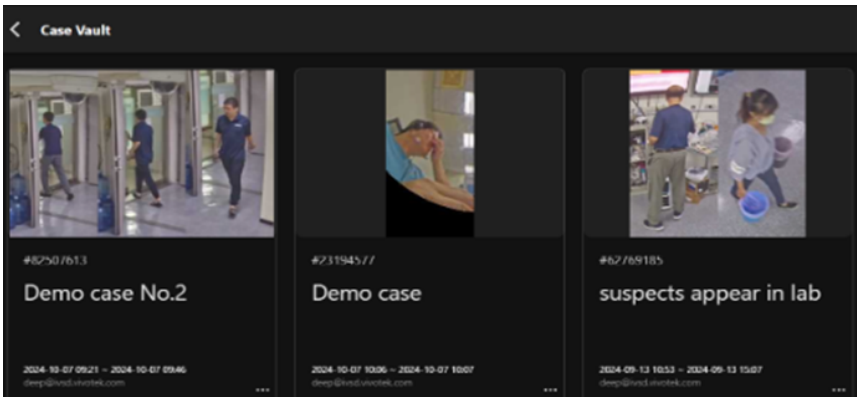
4. Click "Add to case" to the next step



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



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

12

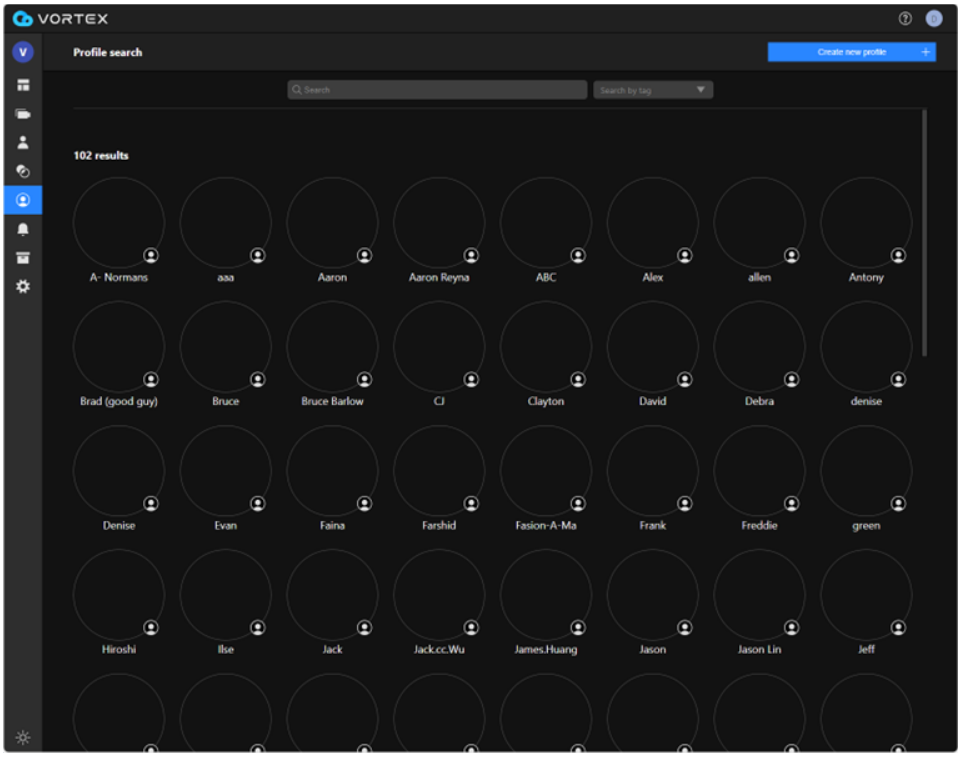
Profile Search allows users to create profiles with a person's facial image(s) and search for that person by those facial image(s) in the profile. A user can upload a profile's facial images from a computer or save them from a Deep Search result. Users can search for the person in the recorded videos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

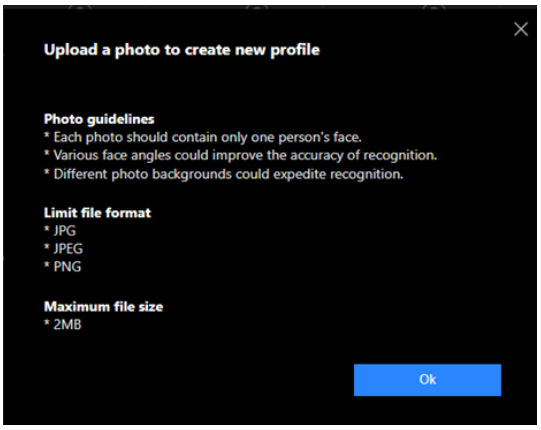
Creating a profile

Clicking the VORTEX's left-side menu "Profile search" displays the existing created profiles and number of search results. (In the manual, the cover images are intentionally black due to portrait rights and privacy rights.)

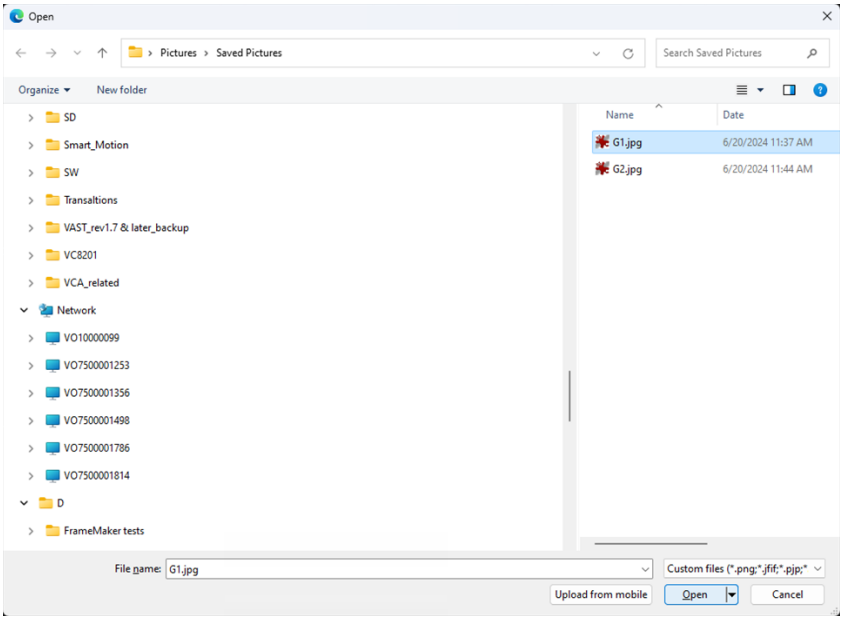
Note
VORTEX Connect PRO does not support Profile Search at this moment.



1. Click "Create new profile".
2. Read the instructions as shown on the screen carefully, and then click Ok.

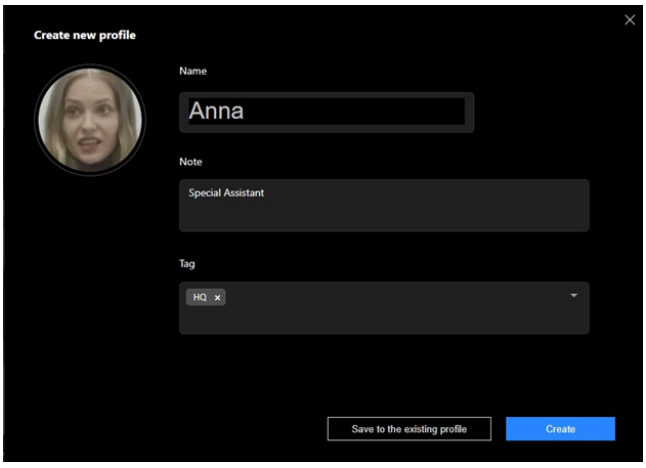


3. Select an image file and click "Open".



4. Enter the following information, and click "Create" to add this person as a new profile or click "Save to the existing profile" to amend more informaition to an existing person's profile.

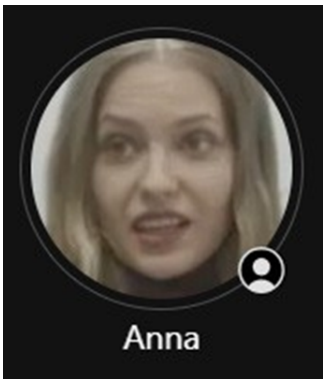
- Name: Last name, and/or First name
- Note: A description of this person
- Tag: Add multiple tags for easy cataloging and searching



Note

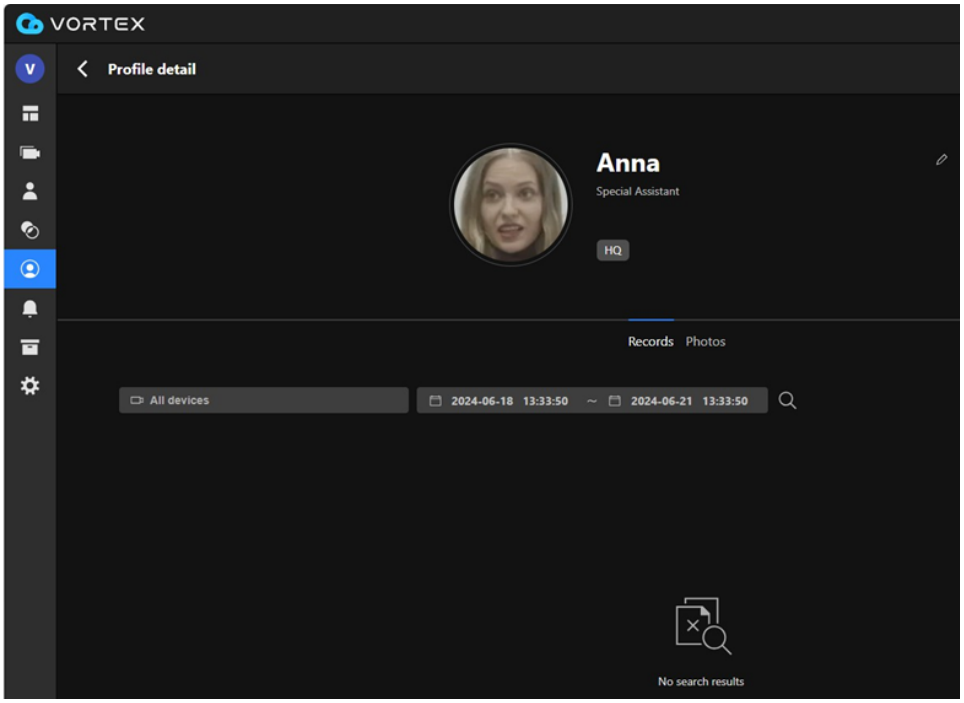
You can also add a facial image from Deep Search results to a profile.

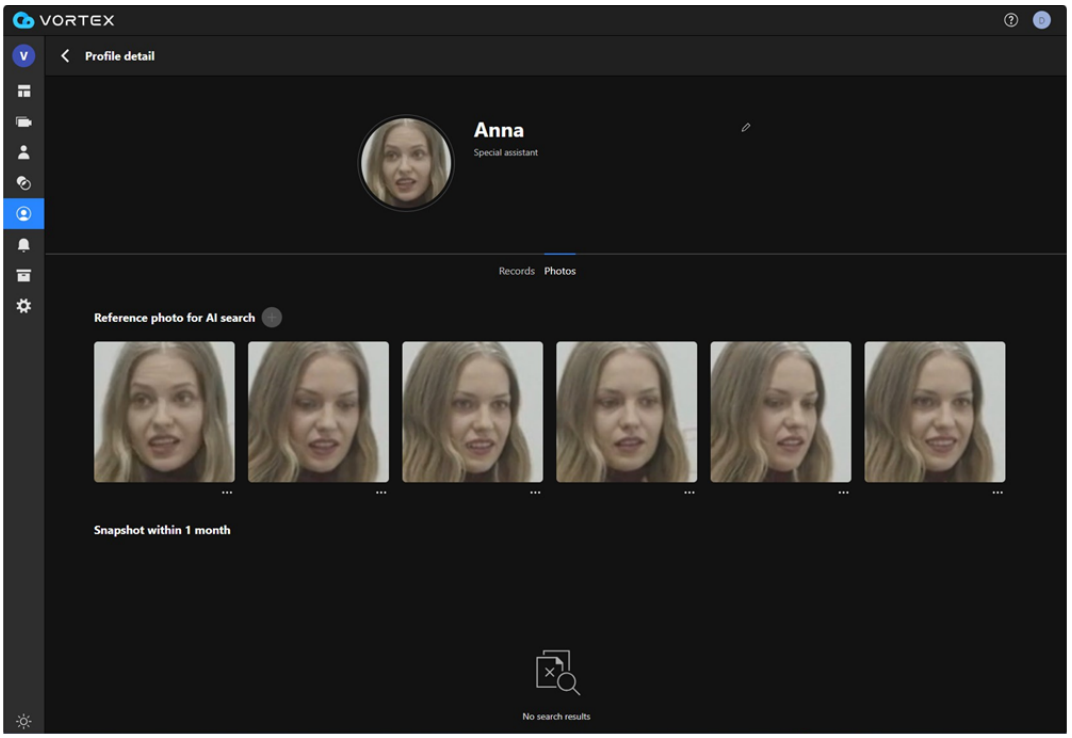
5. The facial image will display as a new search result in the workspace. Click the image thumbnail (cover image) to see the profile detail and search options (Records and Photos).



Using Profile Search to search for a particular person

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.




VORTEX
Profile detail
Anna
Special assistant
Records
Photos
Reference photo for AI search
Snapshot within 1 month
No search results

Message center

13

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.

Device event

Here you have three filters as the conditions for your search:

Device

Select which device group(s) you want to filter events for.

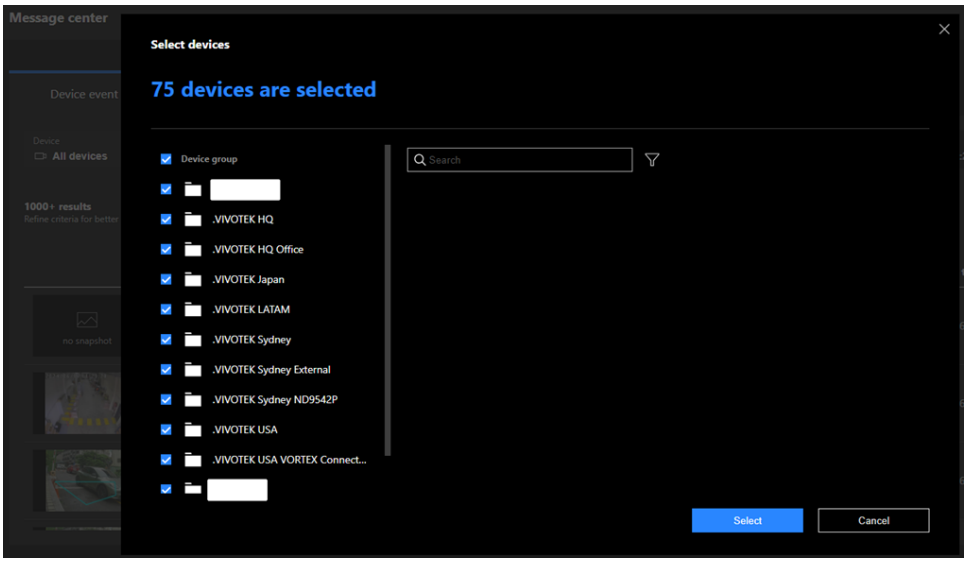
Event type

Select the event types (generated from cameras or NVRs) you want to see when reviewing the filtered videos.

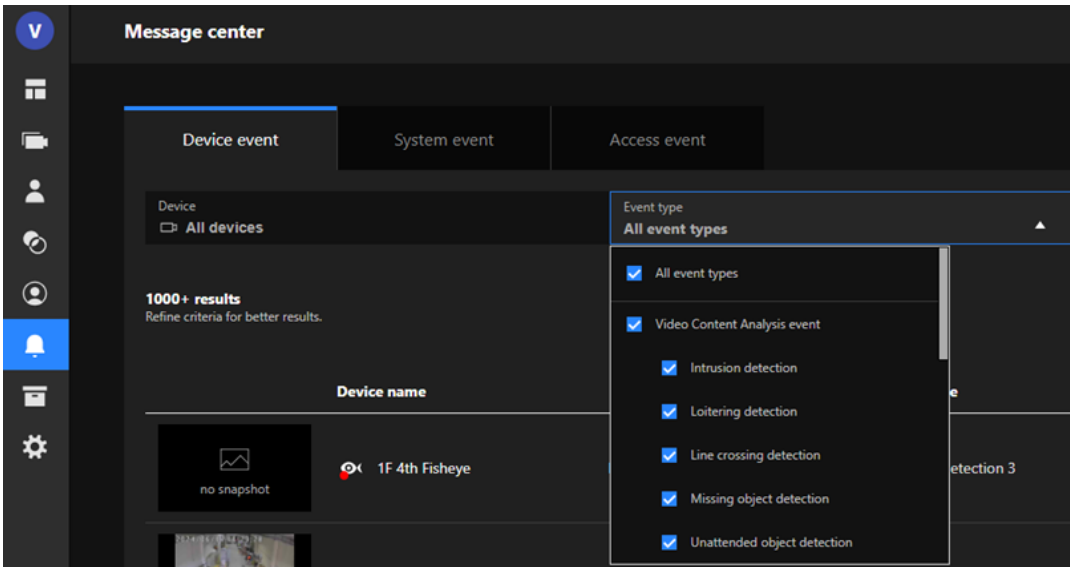
- Video Content Analysis event types
- General event types

Time frame

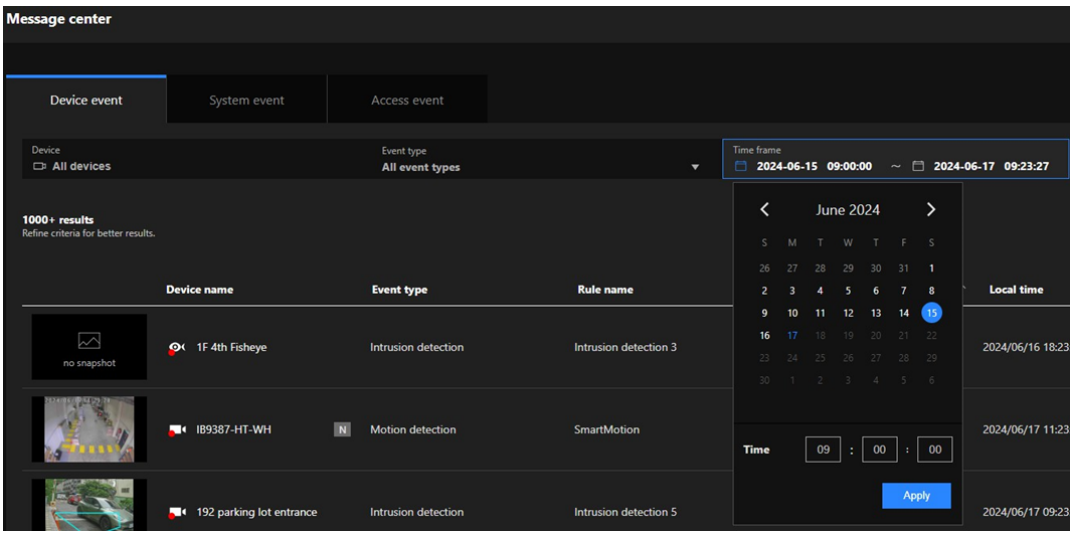
Set a specific time range to narrow down or widen your search results.



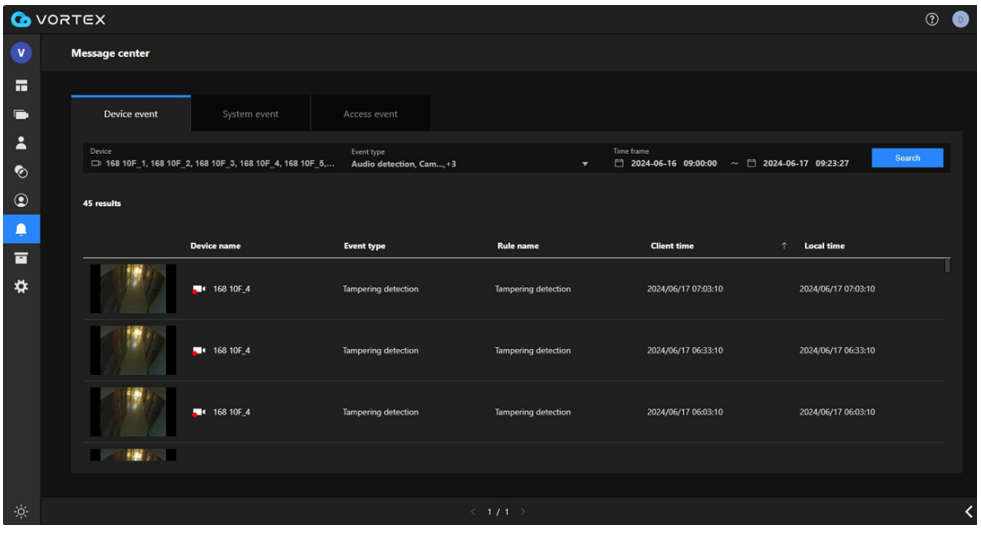
Select device group(s)



Select event type(s)



Select time frame



Example of 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.)

System event

Here you can look for system-related issues such as offline by using three filters as the conditions for your search. Once you set your search criteria, click the Search button to get the search results.

Device

Select which device groups(s) you want to filter events for.

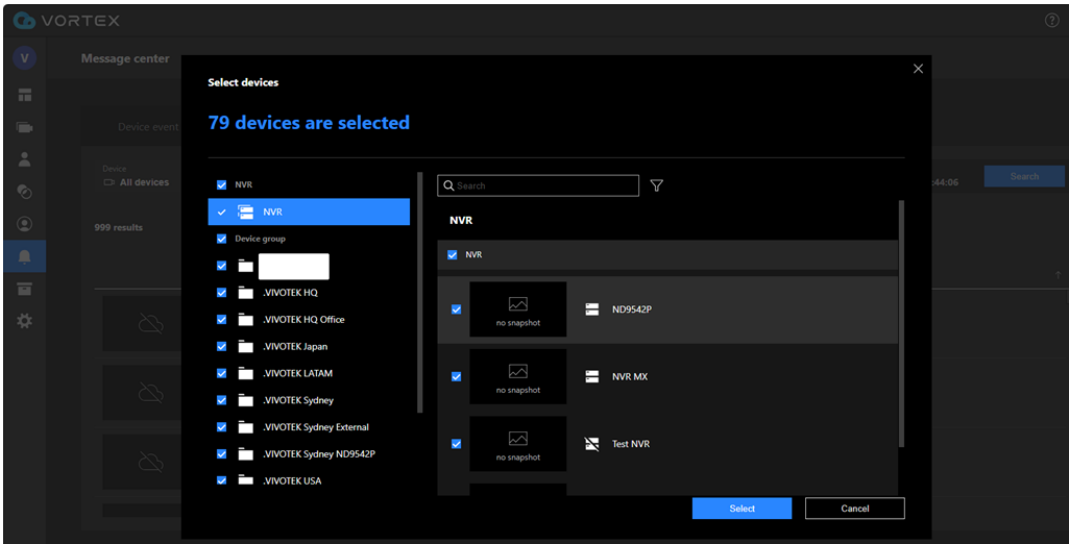
Event type

Select the event types (from cameras or NVRs) you want to see when reviewing the filtered videos.

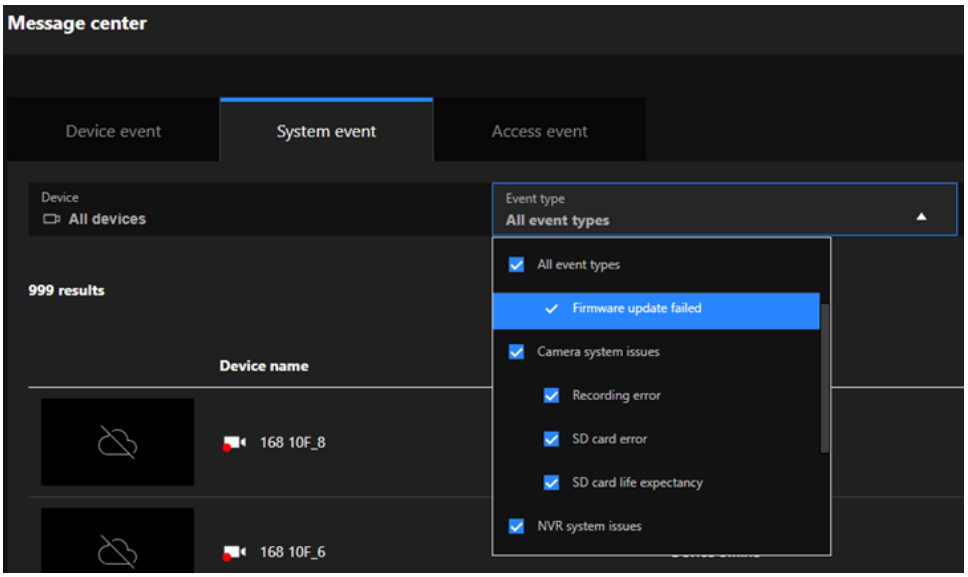
- General system event types
- Camera system event types
- NVR system event types

Time frame

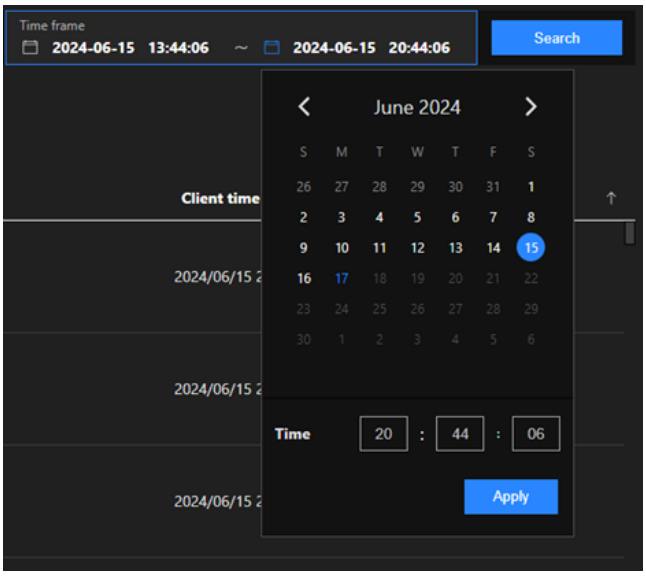
Set a specific time range to narrow down or widen your search results.



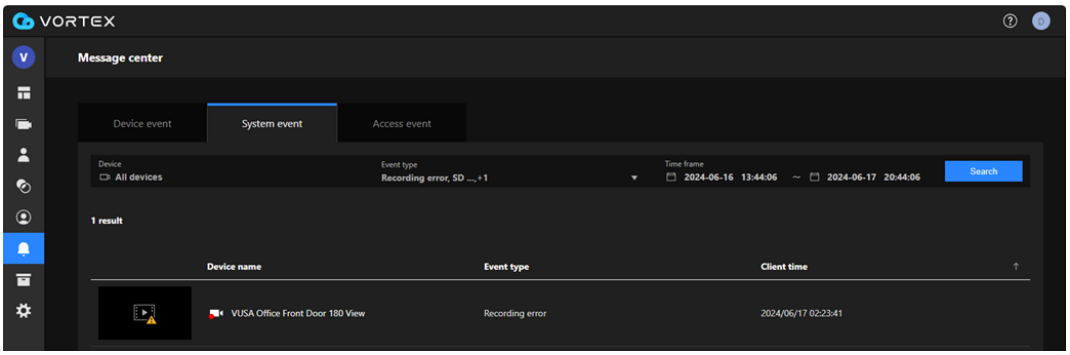
Select device group(s)



Select event type(s)



Select time frame



Example of search results

Access event

VORTEX can integrate with an access control system, so here you can look for access related issues such as door open by using four filters (including card holder name) as the conditions for your search. Once you set your search criteria, click the Search button to get the search results.

Access control point

Select where (access control points such as door and elevator) the access control devices are installed, so you want to filter events for.

Event type

Select the event types (such as , device tempered, and lockdown) you want to see when reviewing the filtered videos.

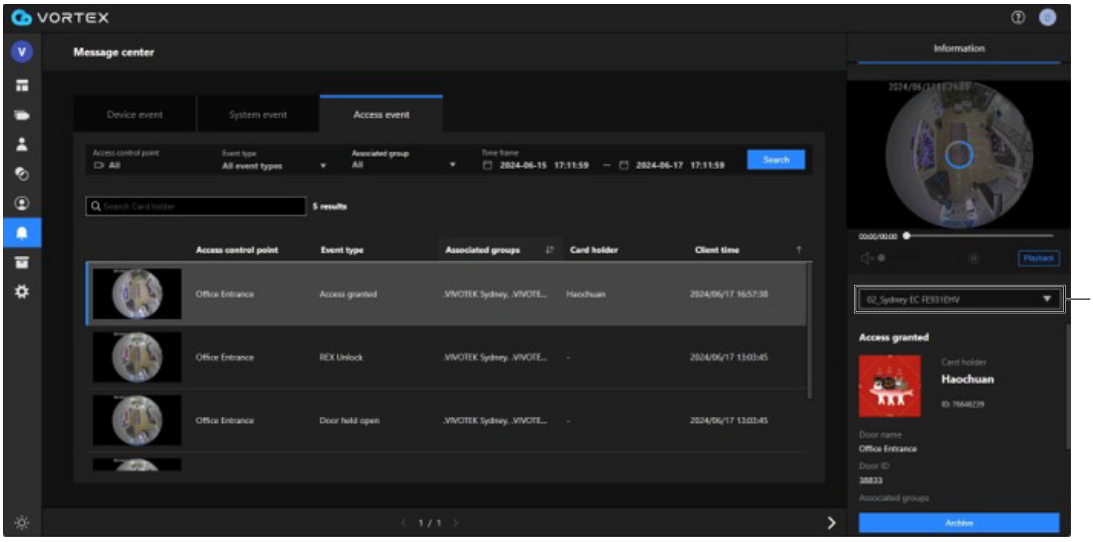
- Door event types
- Device tempered event types
- Lockdown event types

Associated group

Select the group to which the access control device belongs.

Time frame

Set a specific time range to narrow down or widen your search results.

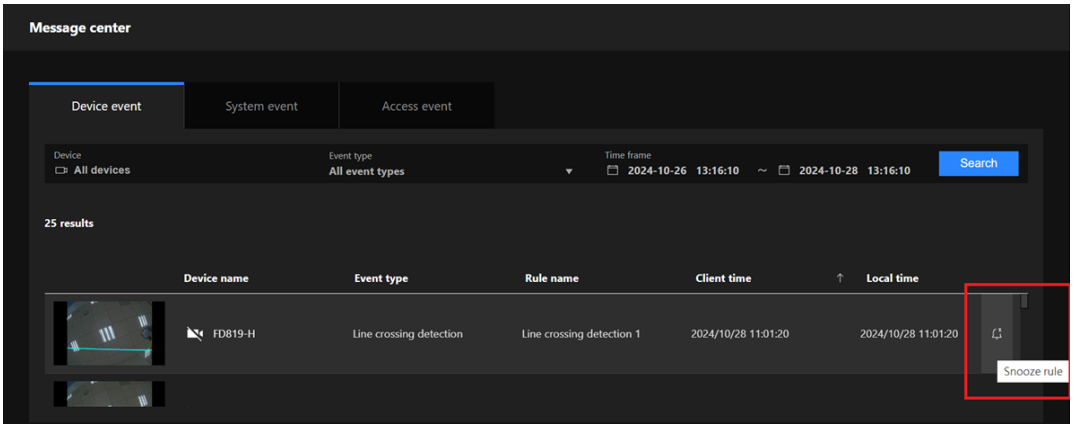


Example of search results

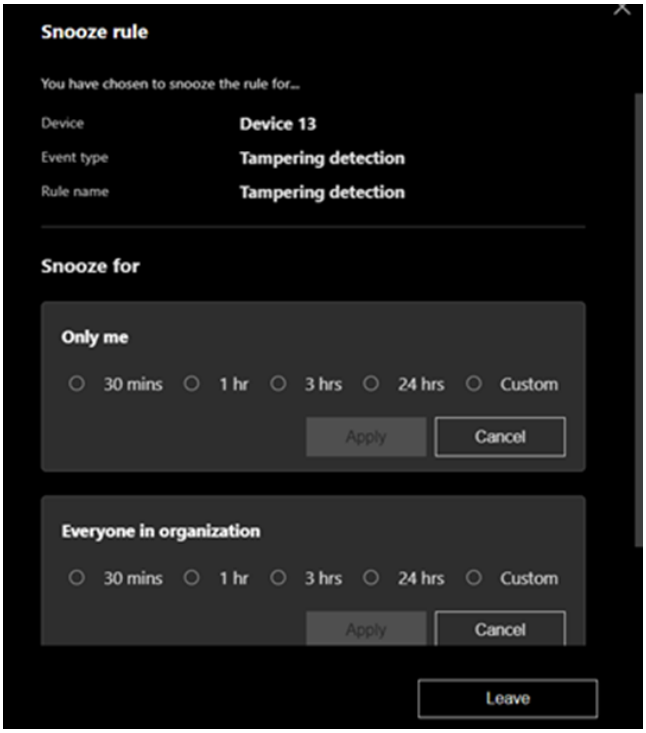
Snooze single rule

[Web Portal]

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



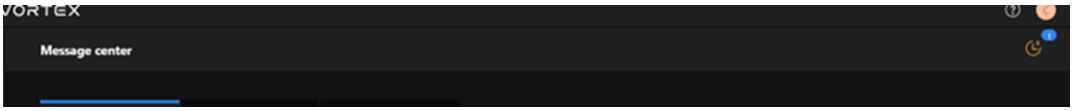
Once you go into snooze rule setting, you will have the option to set schedule, to choose whether to snooze the alarm just for yourself or the entire organization.



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”.

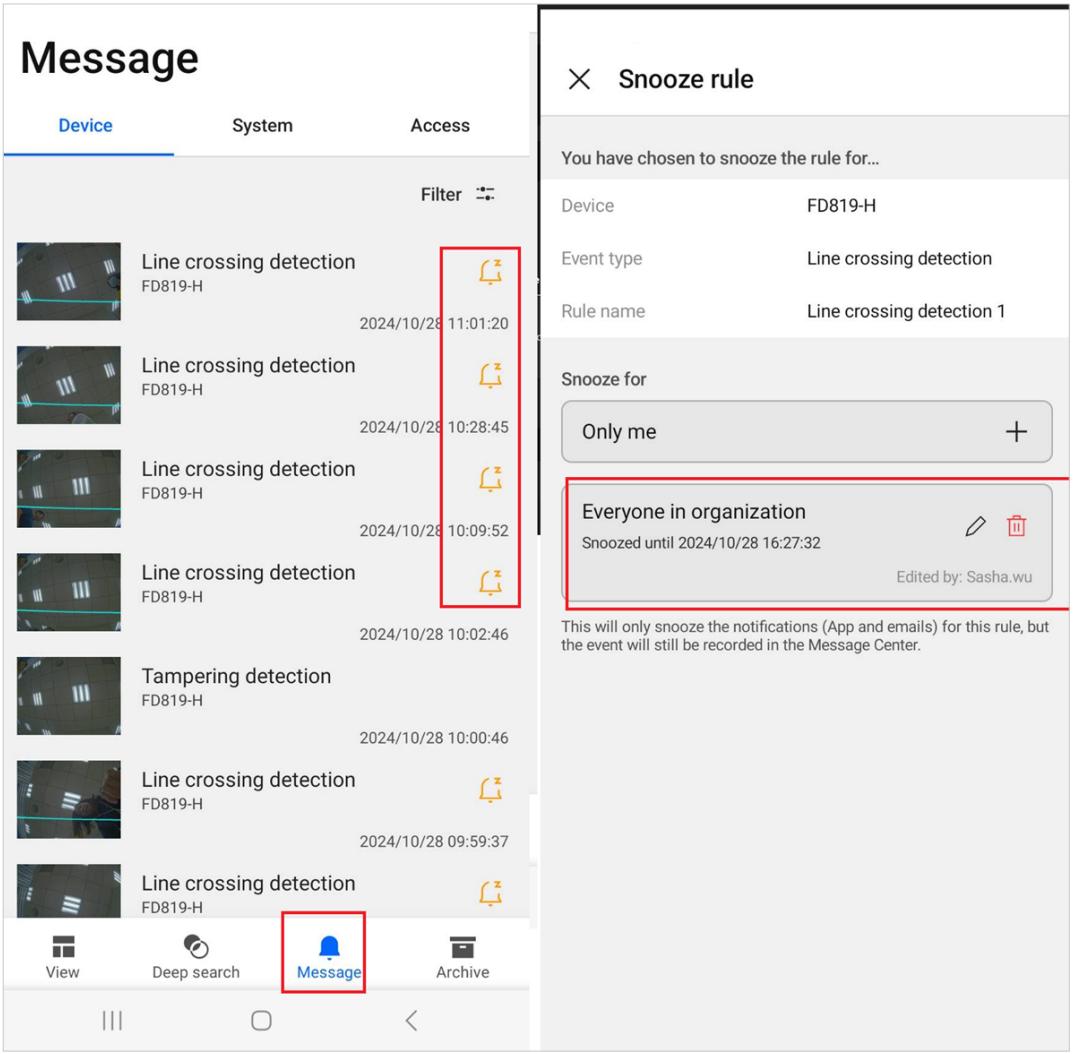
Role “supervisor” and up have the authority to snooze a rule for the entire organization.

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 poral, 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.



Archive

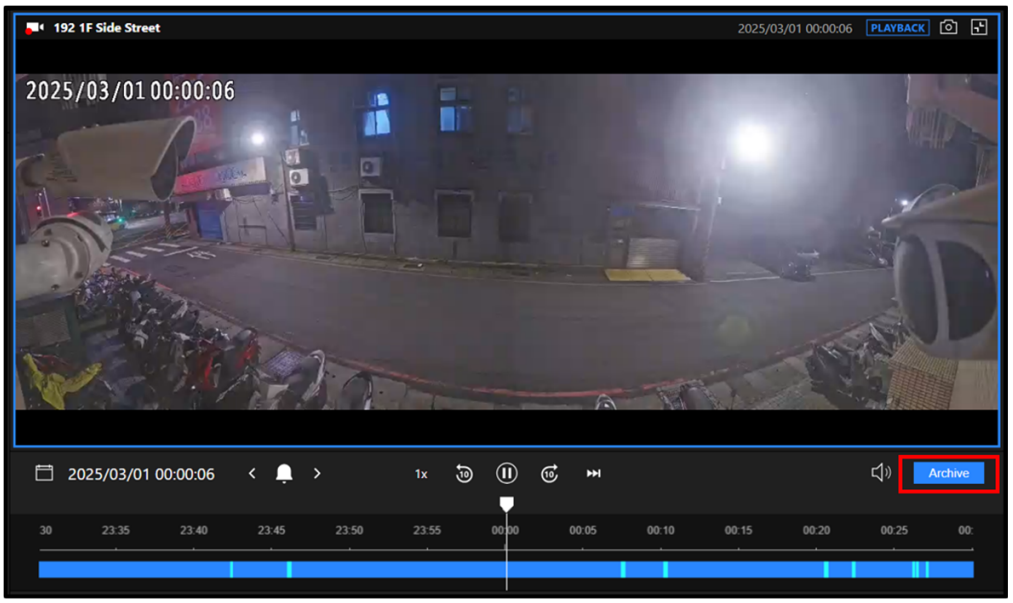
14

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.

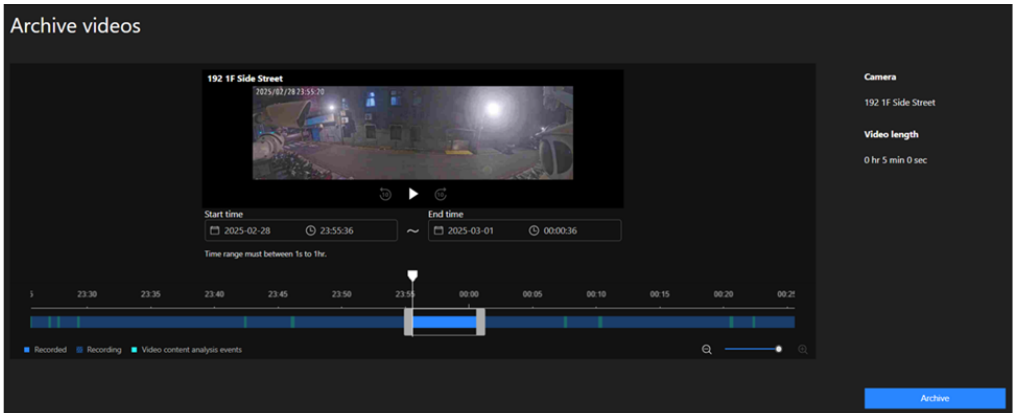
Create archived video clips

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.

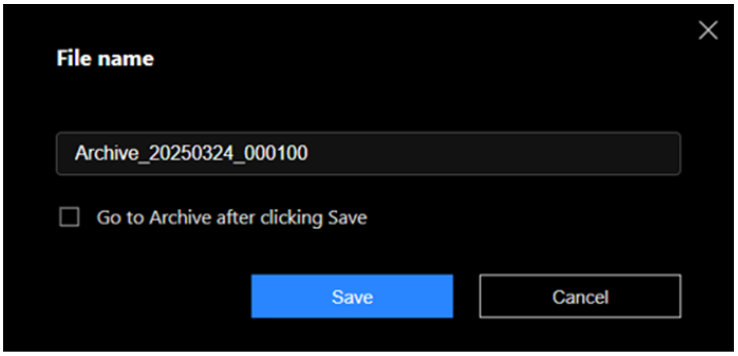
1. Click "Archive"



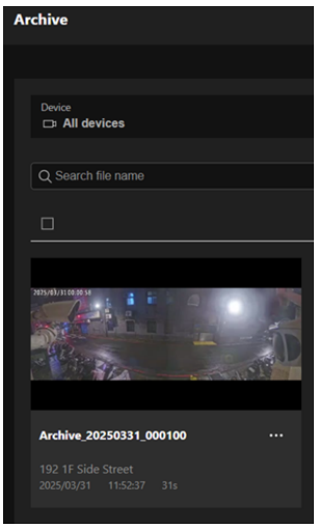
2. Set the start and end time for the key moment to create the archived file. The duration can range from 1 second to 1 hour. Beside using the date time picker, you can also adjust the interval in the timeline to select the time range. After selecting the time range, click "Archive".



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".



4. Find the file in Archive page.



NOTE

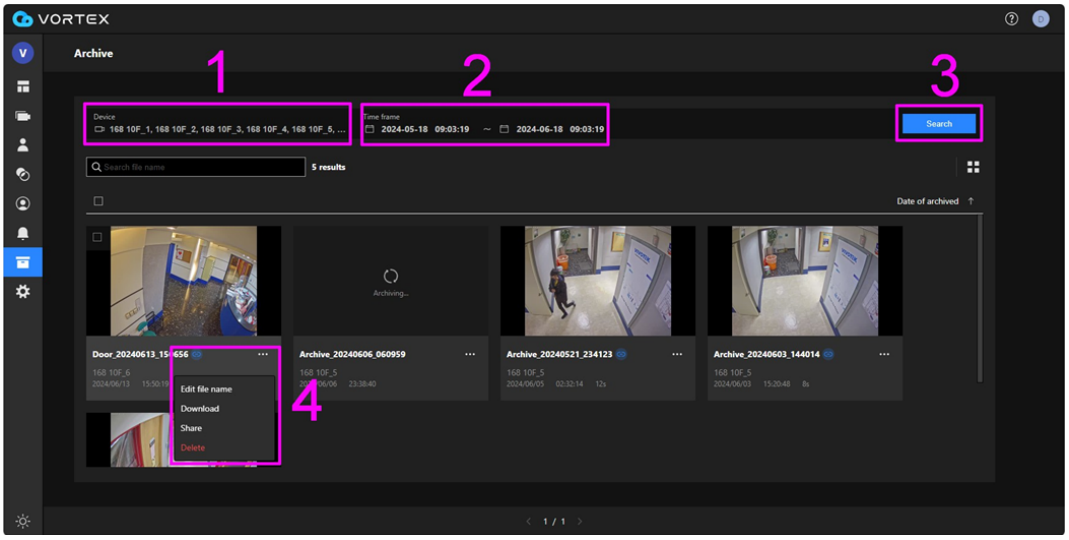
VORTEX Apps also support create archive file. Click the **Archive** icon ( ) to start the creation process on View, Deep Search and Message page.

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:

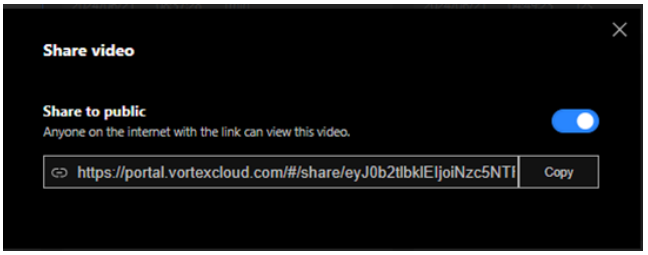
Click the "All devices" button to select cameras, and set the time frame. Then, click the "Search" button.



Example of search results

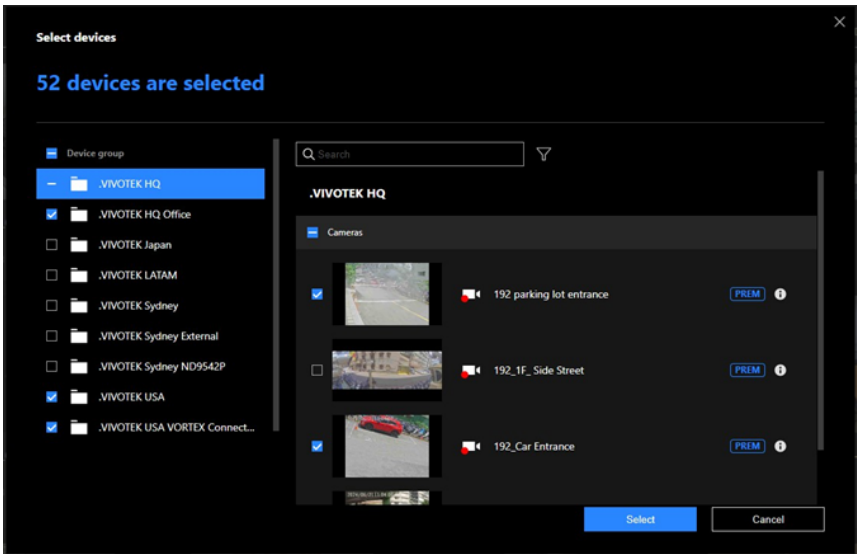
Once you have found the archived video you're looking for, you can click the "..." icon in the video cell. This will pop up a window that allows you to edit the file name of the archived video, download the video directly to your computer, share the video, and delete it.

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.



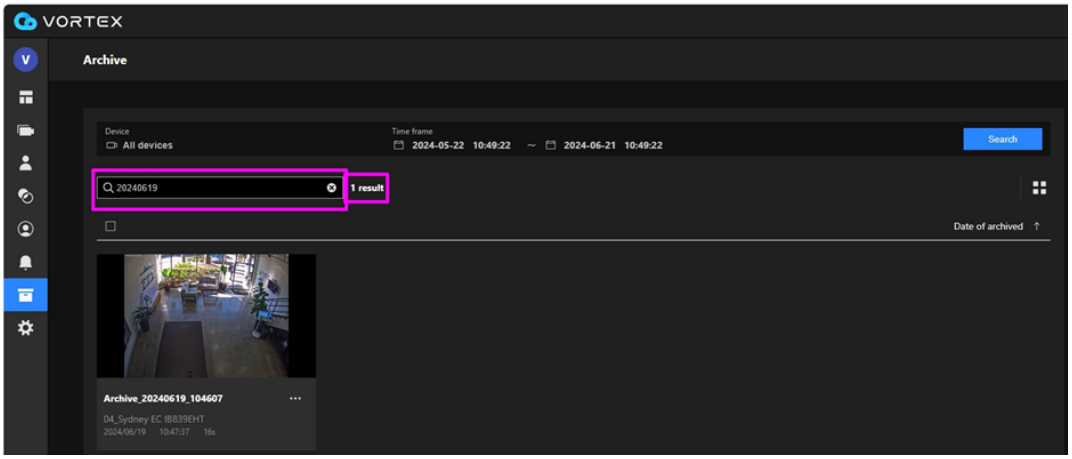
2. Search by camera(s) in group(s):

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.

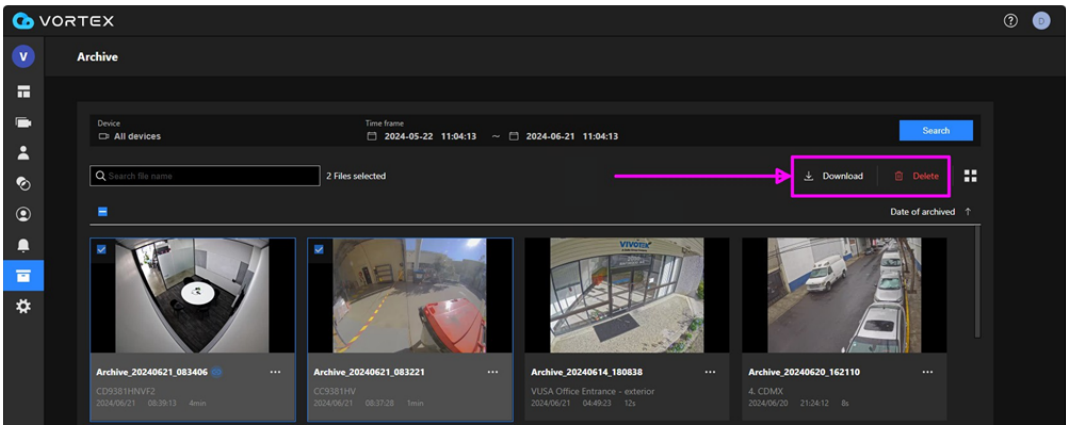


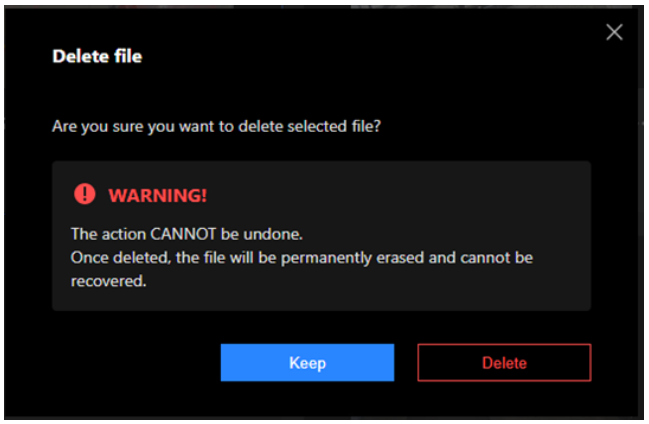
3. Search by video file name:

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.

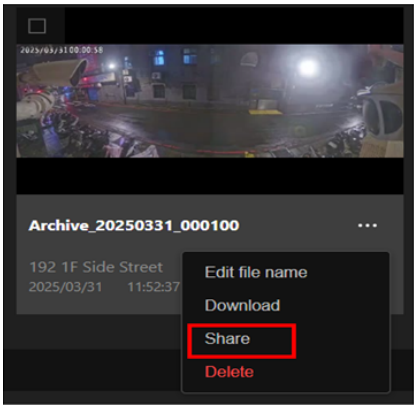




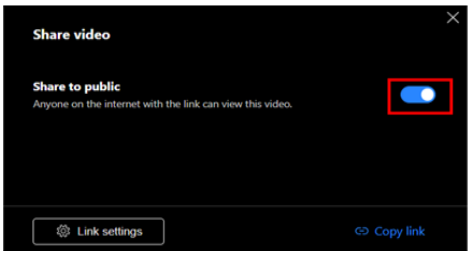
Sharing archived files

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

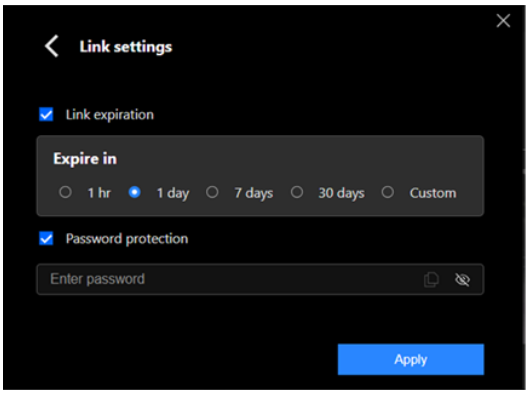
1. Go to the **Archive** page
2. Locate the archive file you want to share and click the **More** icon (...).
3. Select **Share**.



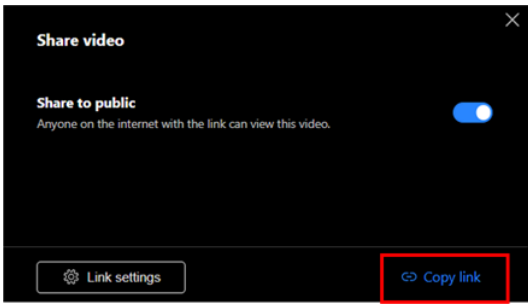
4. A configuration window will appear.
5. Toggle the **Share to public** switch to enable sharing. A shareable link will be generated.



6. Click **Link Settings** to set a **password** and **expiration date** for the link, if needed.



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

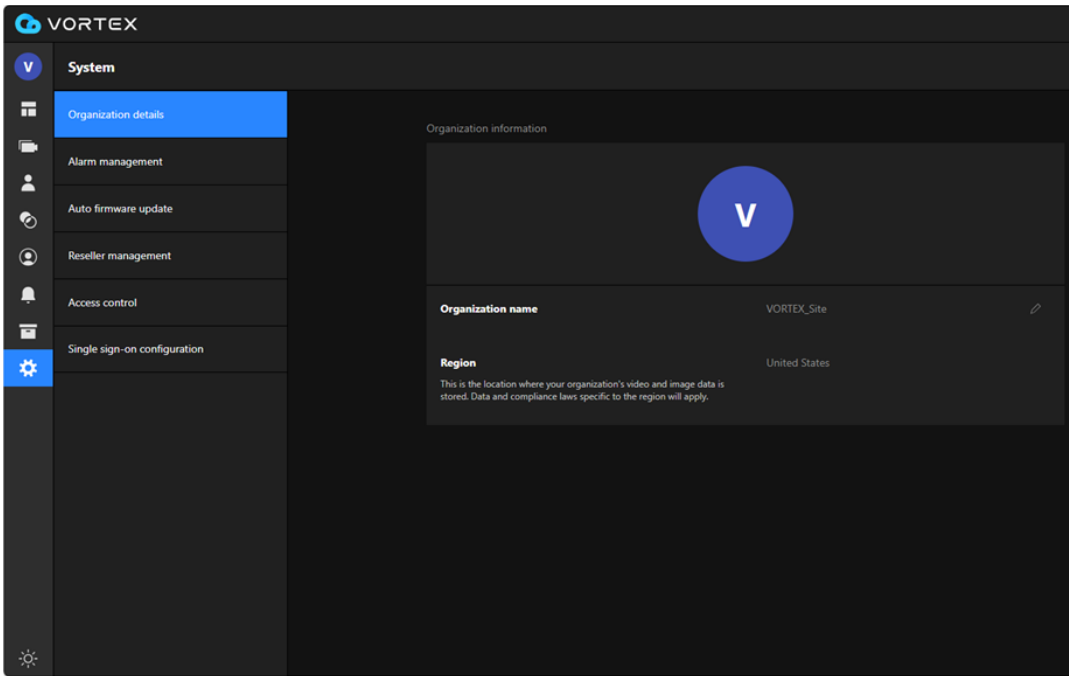
System

15

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

Organization details

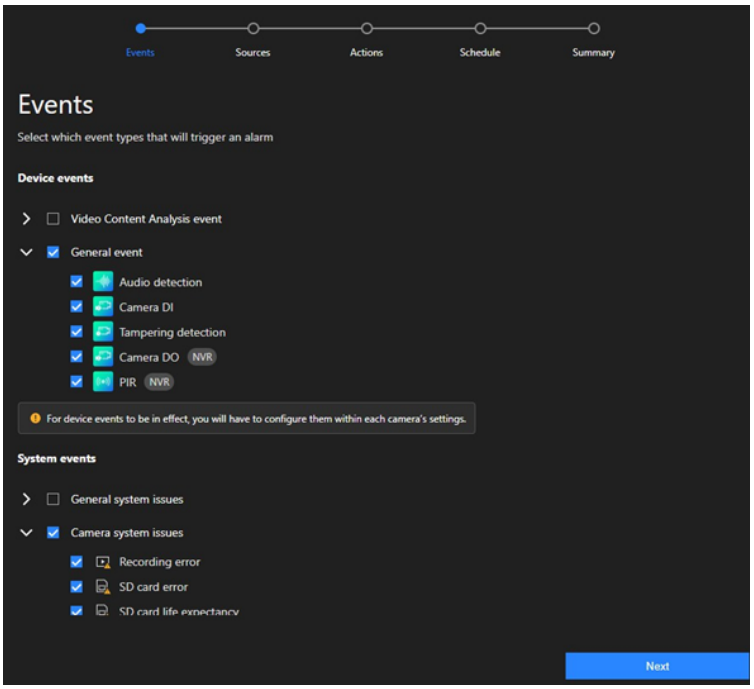
You can change your organization name here if you are an organization owner, administrator, or supervisor. In addition, only the VORTEX organization owner can transfer ownership to another user and can delete the organization when all devices are deleted.



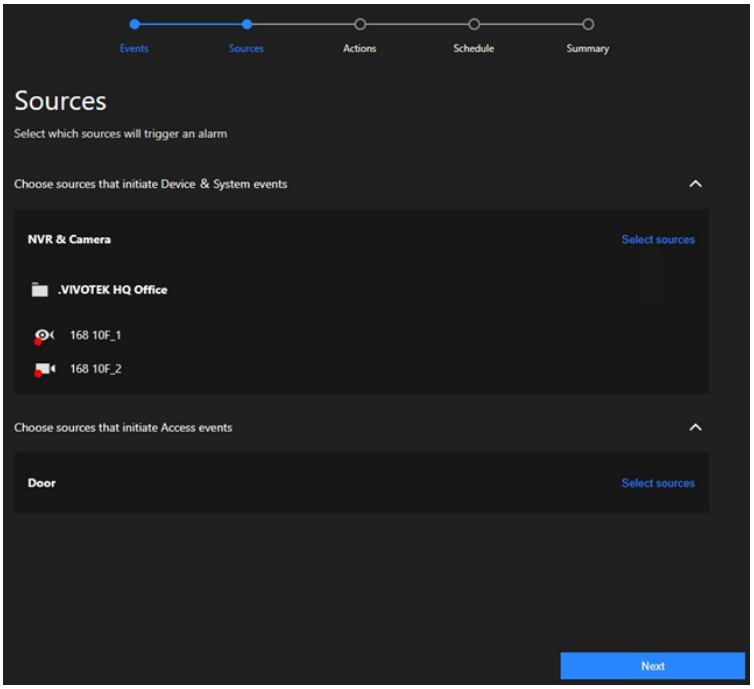
Alarm management

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:

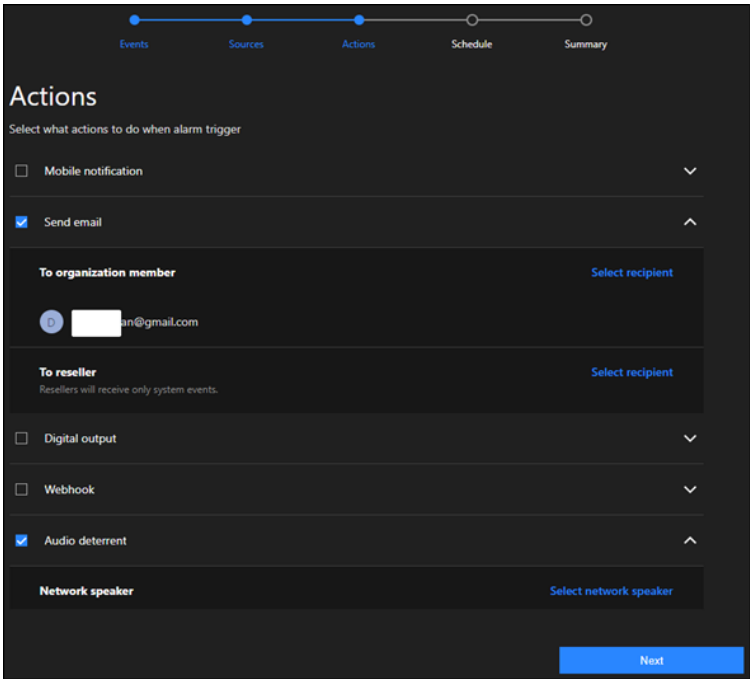
1. Select the event(s) and issue(s) you want to be notified of, and then click NEXT.



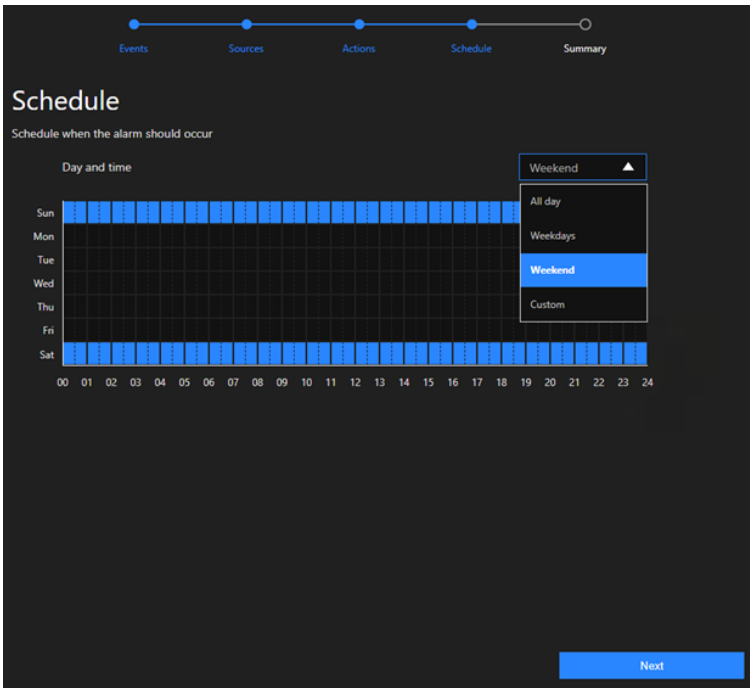
2. Select the source(s) to trigger the alarm, and then click NEXT.



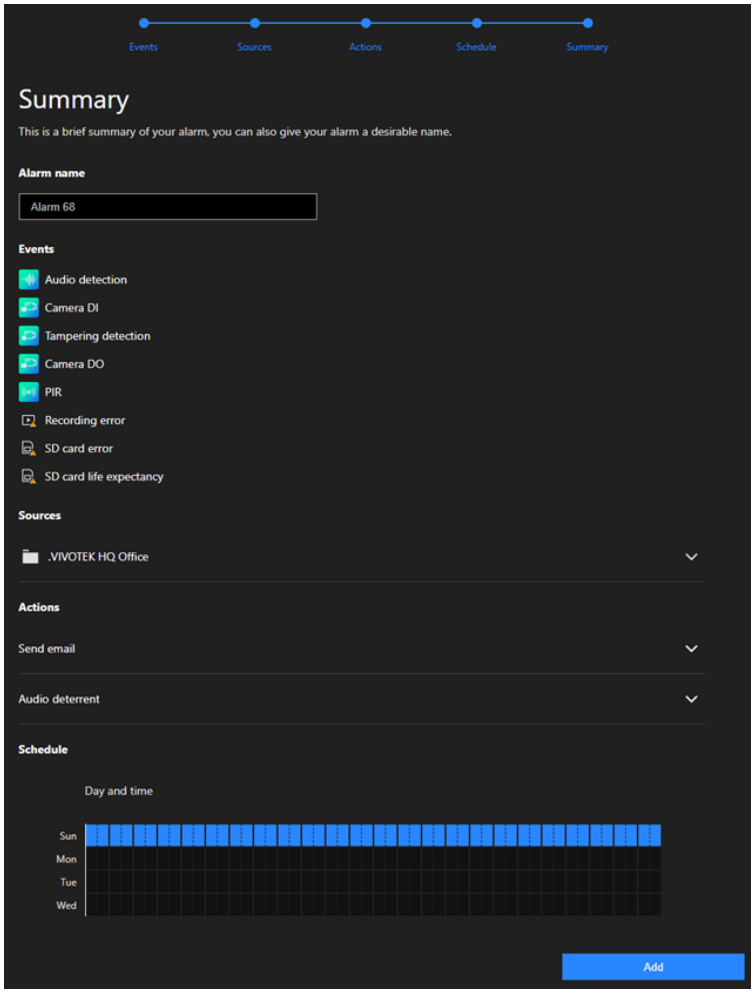
3. Select the actions(s) the alarm will trigger, and then click NEXT.



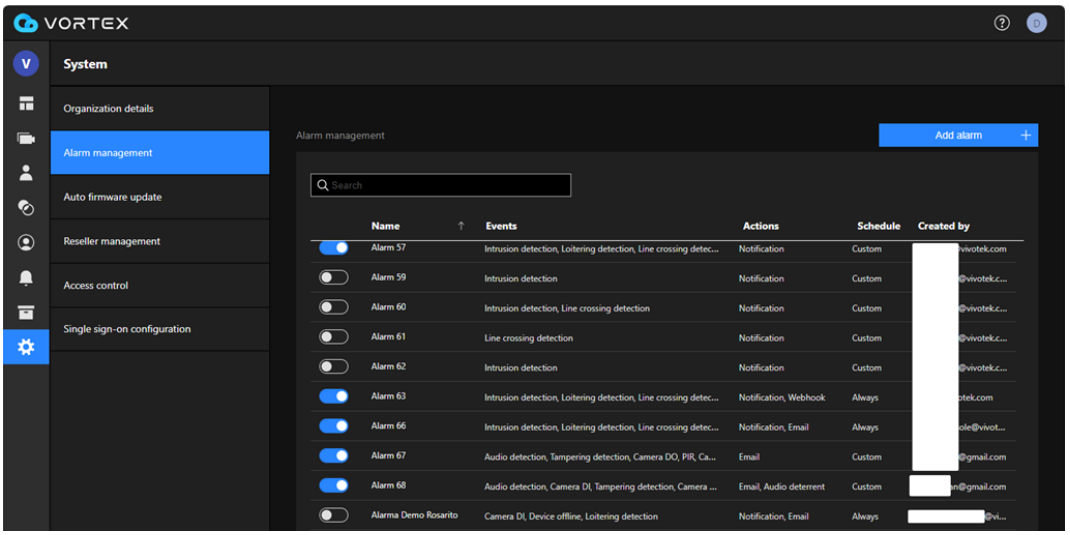
4. Select the time frame the alarm is on.

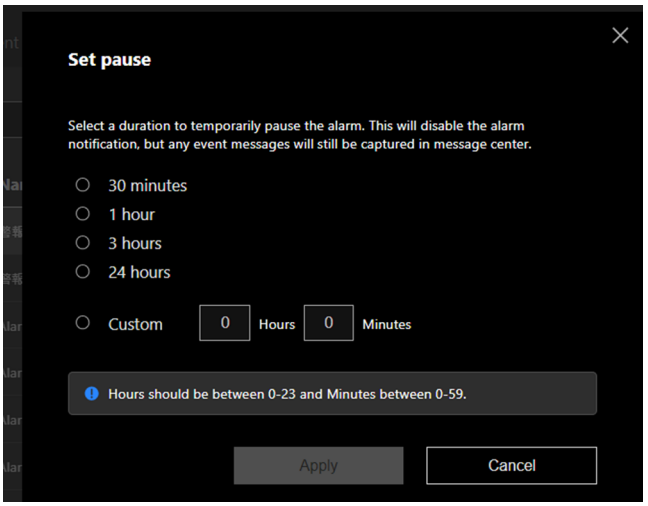


5. Check if all the items you select are correct. If yes, click Add.

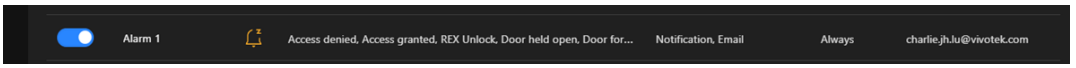


Now, you can move the slider (ON/OFF) to decide whether to enable the alarm you just created.

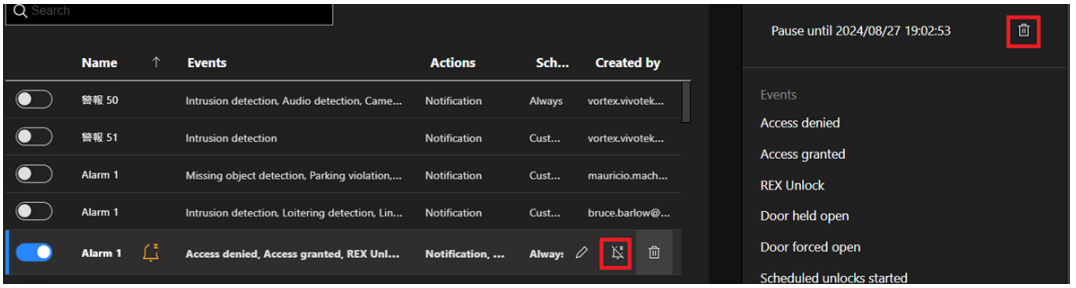




An indicator will tell you which alarm is paused.

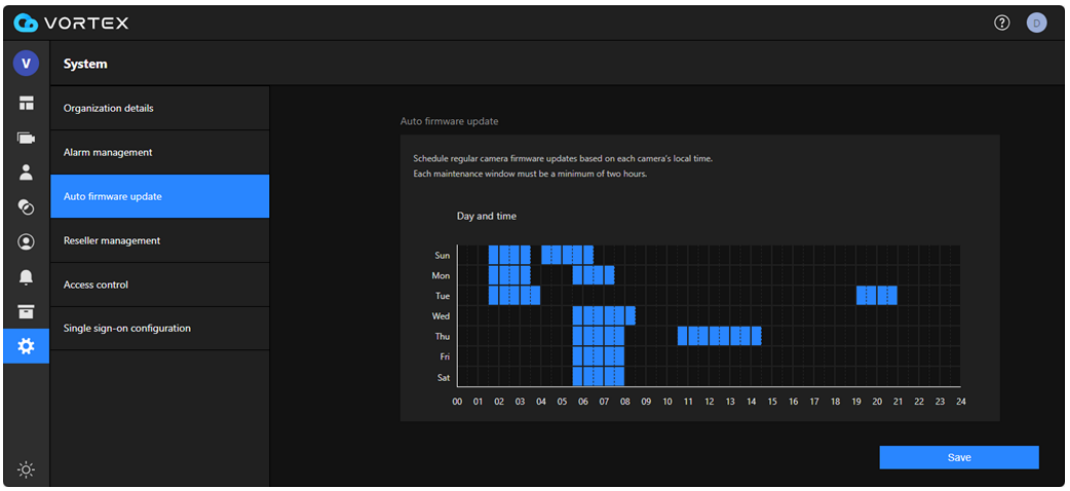


If you would like to resume the alarm before the schedule up, you can manually stop the pause using the same snooze icon or from the right panel.



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).



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:

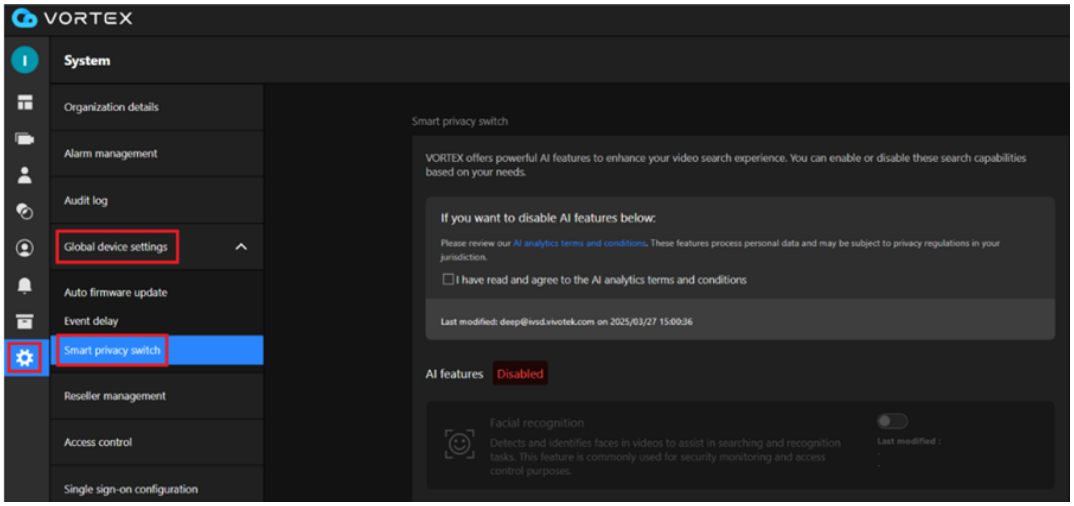
Once the agreement is signed, users can enable or disable these AI features based on local legal requirements and their specific needs. This will help ensure that the use of AI-driven surveillance is carried out within the legal framework for their region.

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

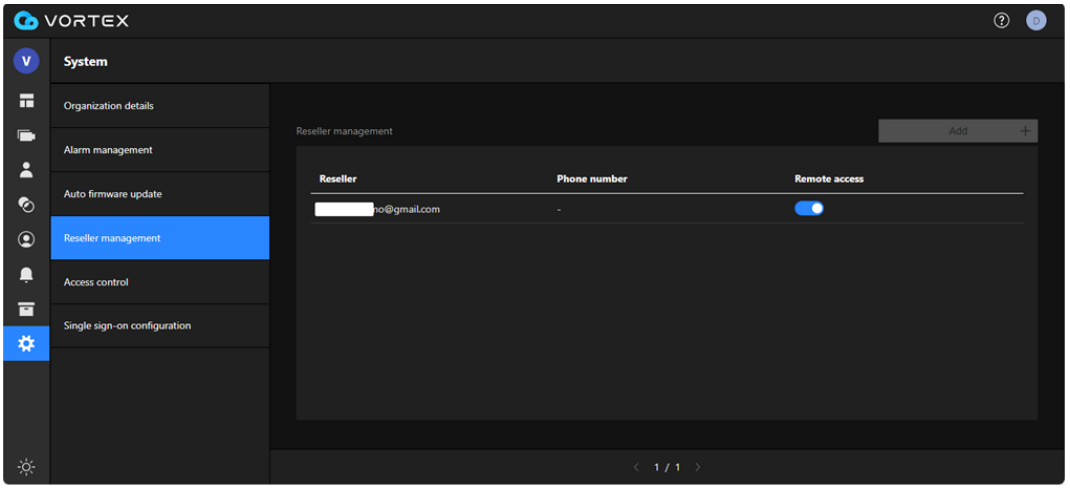
When **Facial Recognition** is disabled, the organization will no longer receive facial-related data. The affected areas are as follows:

- **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.

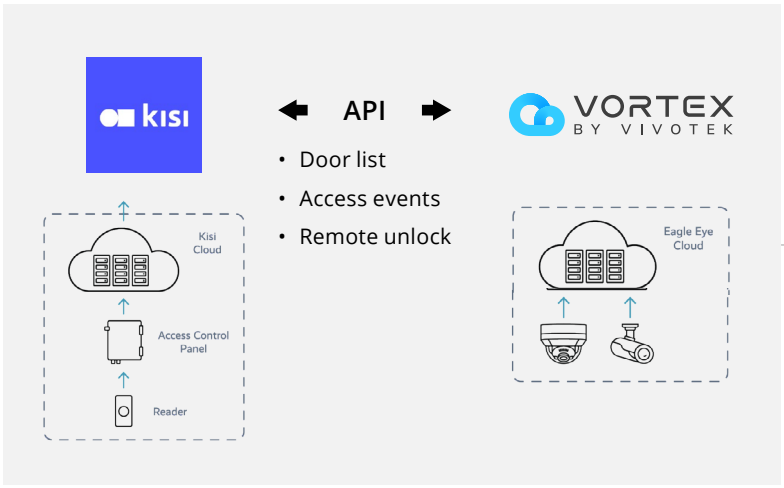
Reseller management

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

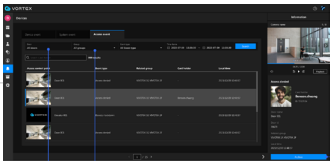


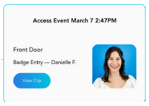
Access control Integration – Kisi

System Overview

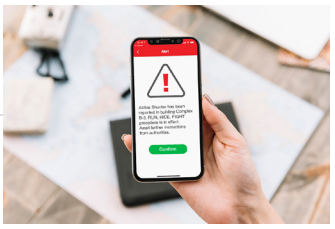


- **Access Events Integration with Native video**





- **Real-time Access Event Notification**

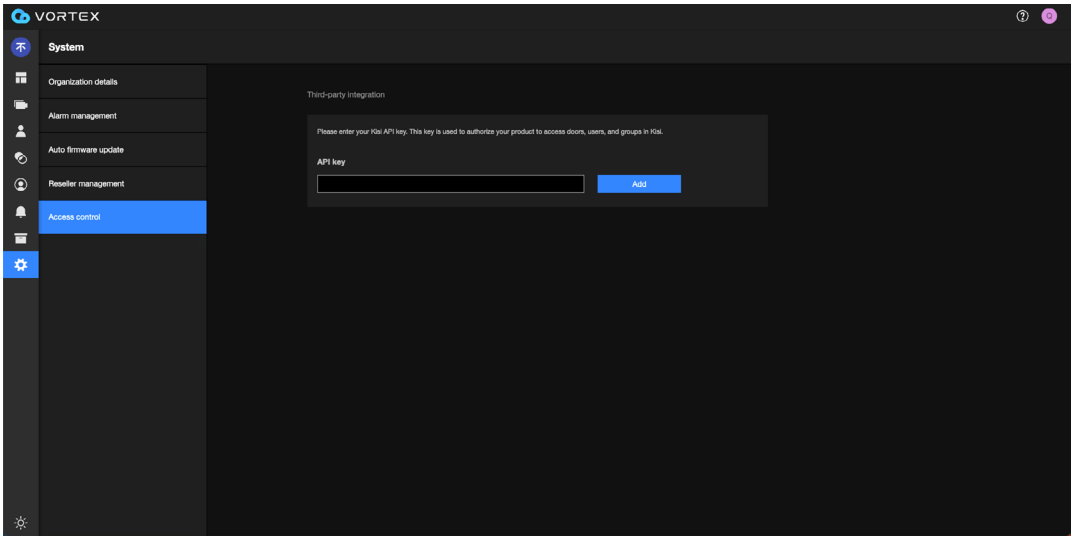


- **Remotely Unlock Doors (Phase 2)**

API integration

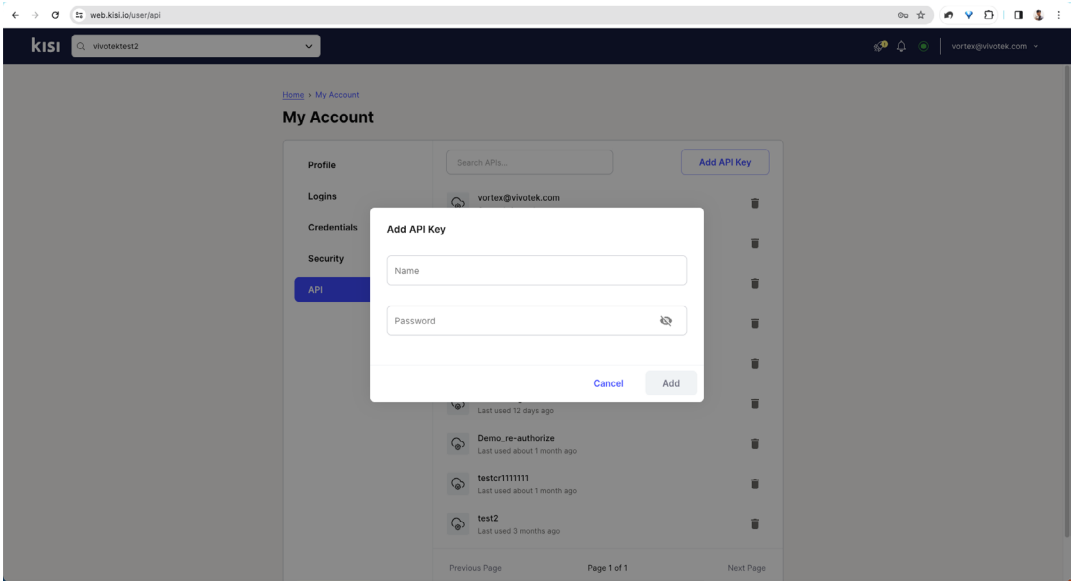
Goal

Enable VORTEX to retrieve the list of Kisi's doors and access events; allow control of Kisi's doors through VORTEX (Phase 2).

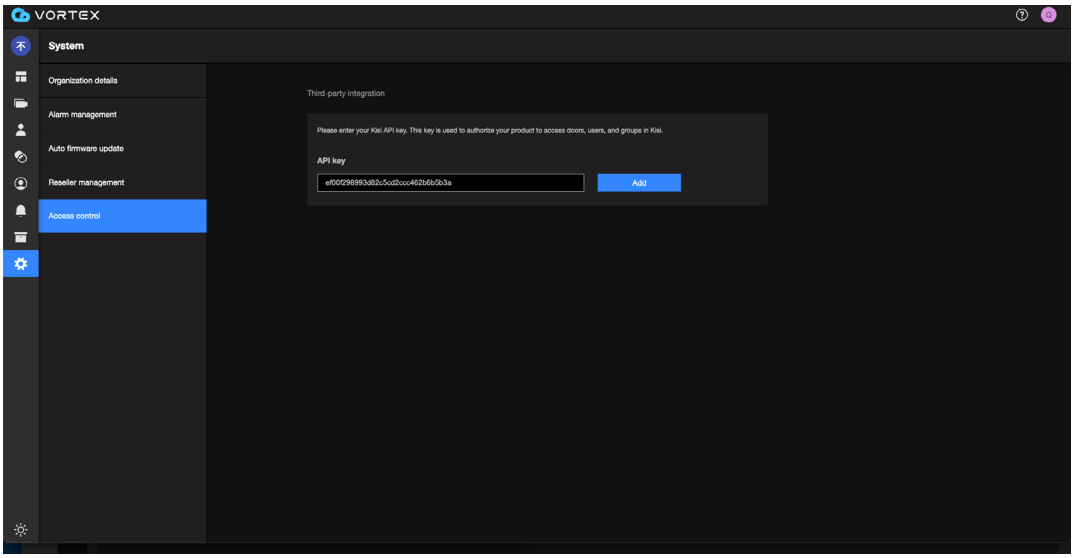


Feature Guide

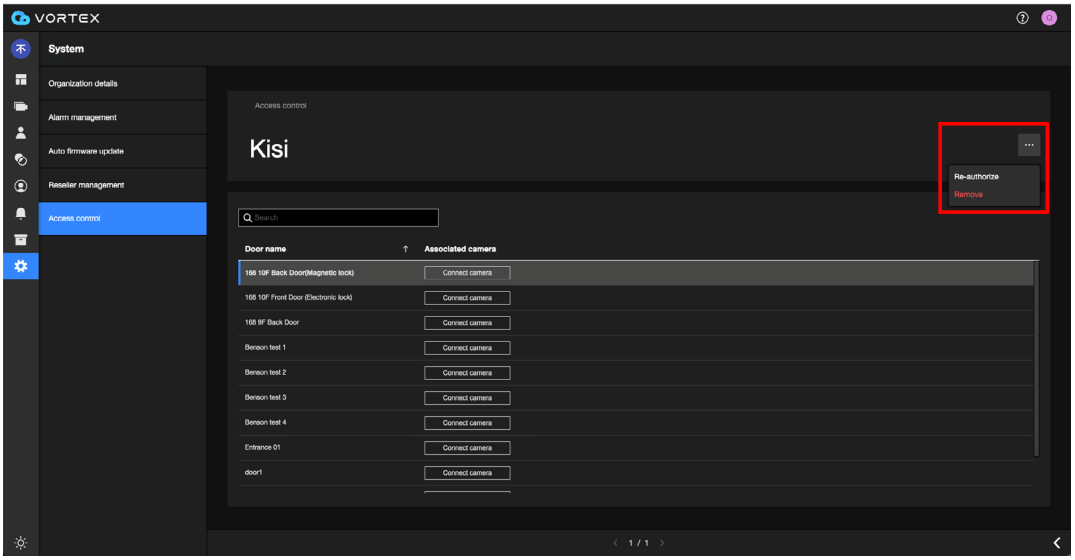
1. Go to Kisi platform, generate a Kisi API key
   - Generate an API key | Kisi Product Documentation



2. Go to VORTEX > System > Access control, paste Kisi API Key and click Add
   - Only Owner/Admin can operate this function
   - An API Key must be generated on the Kisi platform



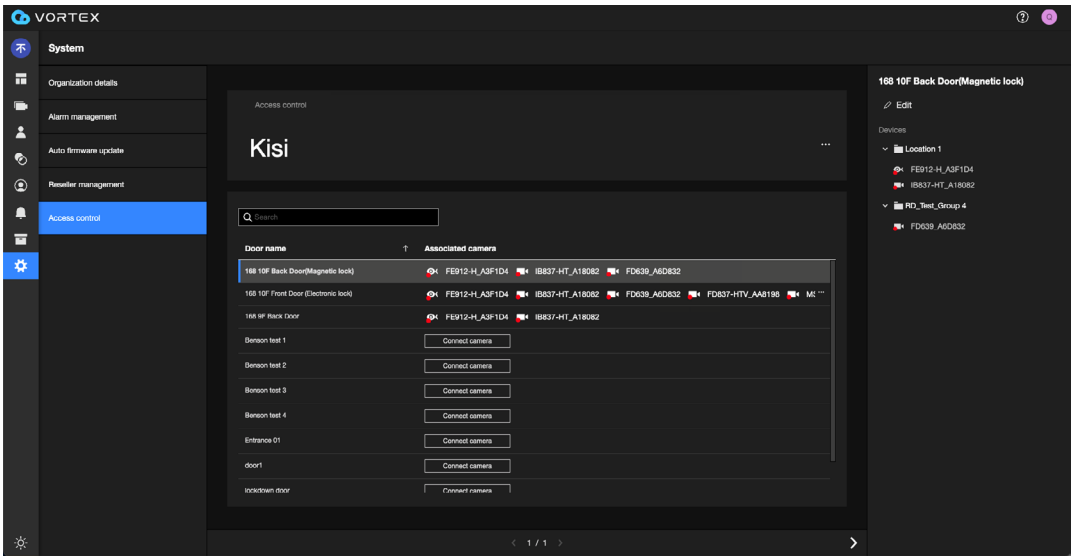
3. If you need to change the Kisi API Key, or if you want to remove the integration with Kisi, you can do so through the 'More option' button.
   - If a user removes this API Key on the Kisi platform, they will no longer be able to use the integrated services on VORTEX.
   - A single VORTEX Org. can only integrate with one Kisi Org.



Associate Cameras with Doors

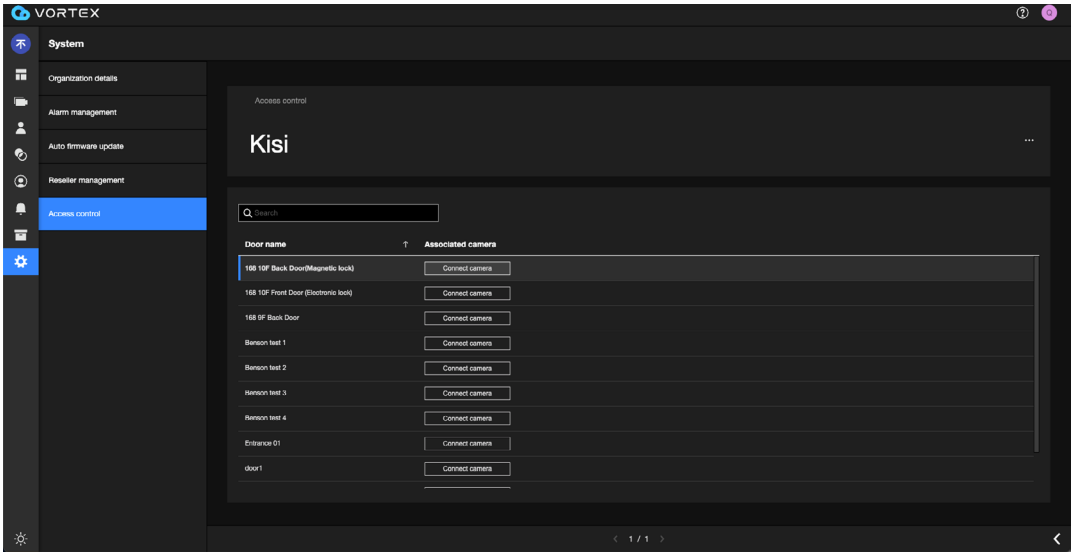
Goal

Allow VORTEX to receive access events from Kisi and integrate them with camera information.

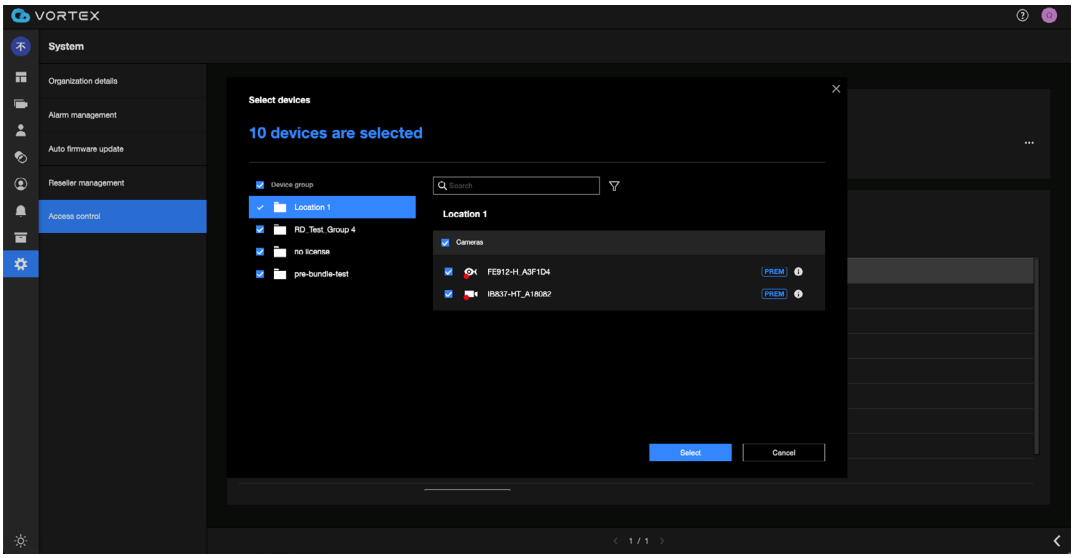


Feature Guide

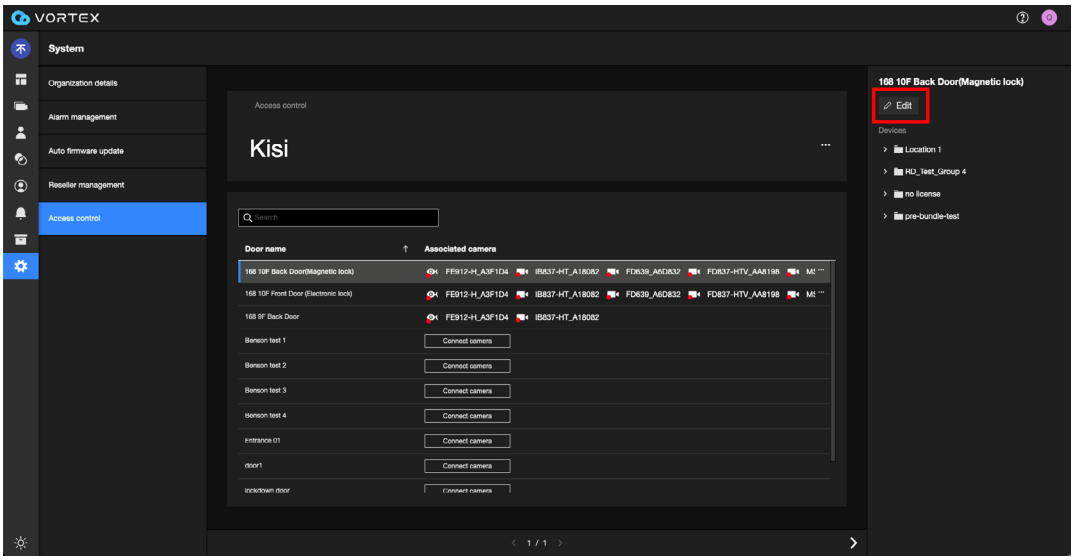
1. On the door you want to associate, click ”Connect camera“
   - Only Owner/Admin can operate this function
   - This page lists all the doors in the Kisi org



2. Select the cameras you want to associate with this door
   - Each door can be associated with up to 10 cameras
   - A door that has been associated with a camera can also be associated with other cameras



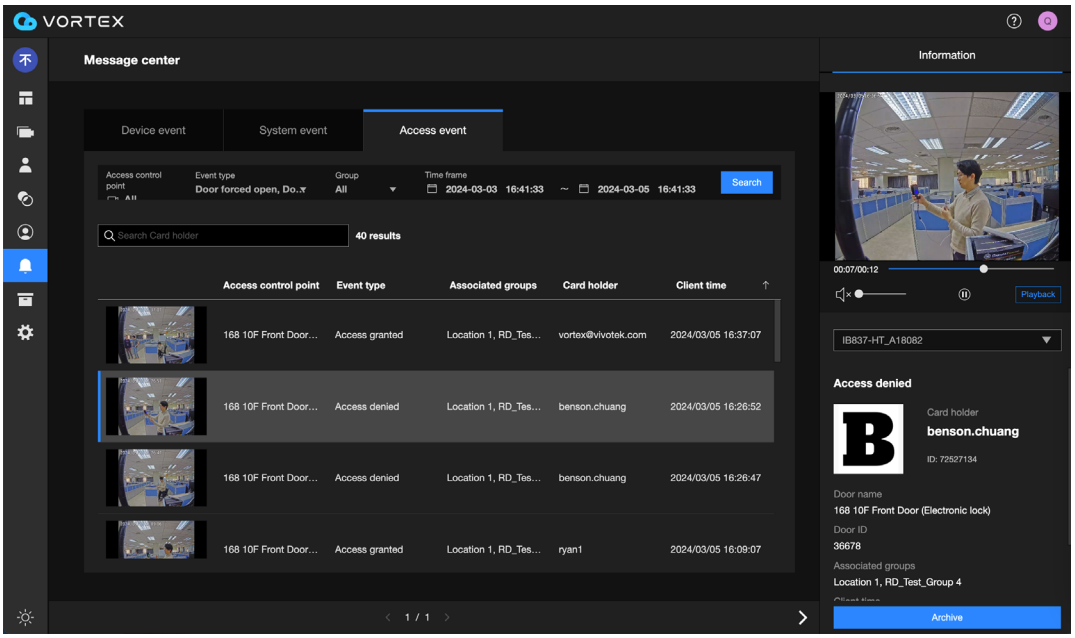
3. If adjustments are needed after the settings are complete, you can make changes through the “Edit” button
   - Users can add/edit/disassociate the cameras associated with doors
   - After users add/edit/delete doors on the Kisi platform, VORTEX will reflect the corresponding changes based on the adjustments



Access Events Integration with Native video

Goal

- Allow users to access an instant and comprehensive view of integrated info. from both systems.
- Link access control data to video surveillance data to verify if someone entering is the person they claim to be.



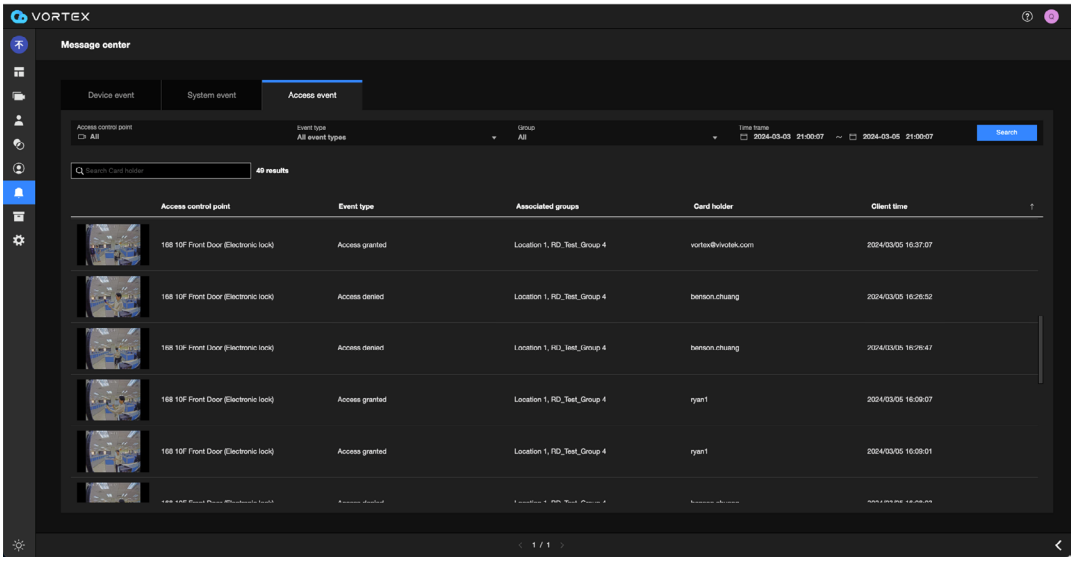
Event Types

	Event	Description	Doc.
Door event	Access granted	User-granted access to unlock an access-controlled door	Add credentials
	Access denied	User-denied access to unlock an access-controlled door	
	REX unlock	Request to exit (REX) is triggered and unlocks a door	Configure REX
	Door forced open	Access controlled or locked door is opened without a request to exit (REX) detected or a user who has been granted access	Configure Door Contact Sensor
	Door held open	Detects an unlock, but the contact sensor reports the door being open longer than the duration set by the Kisi organization admin.	
	Schedule unlocks started/ ended	Unlock schedules you have set on Kisi start or end	Set unlock schedules
Device tempered	Reader tempered	Based on a magnet built into the device and the mounting plate. If unmounted while powered this triggers a tamper event	Temper detection
	Controller tempered	The controller detects tamper based on its Weigand board slot. If the device is rebooted this also triggers a tamper alert	

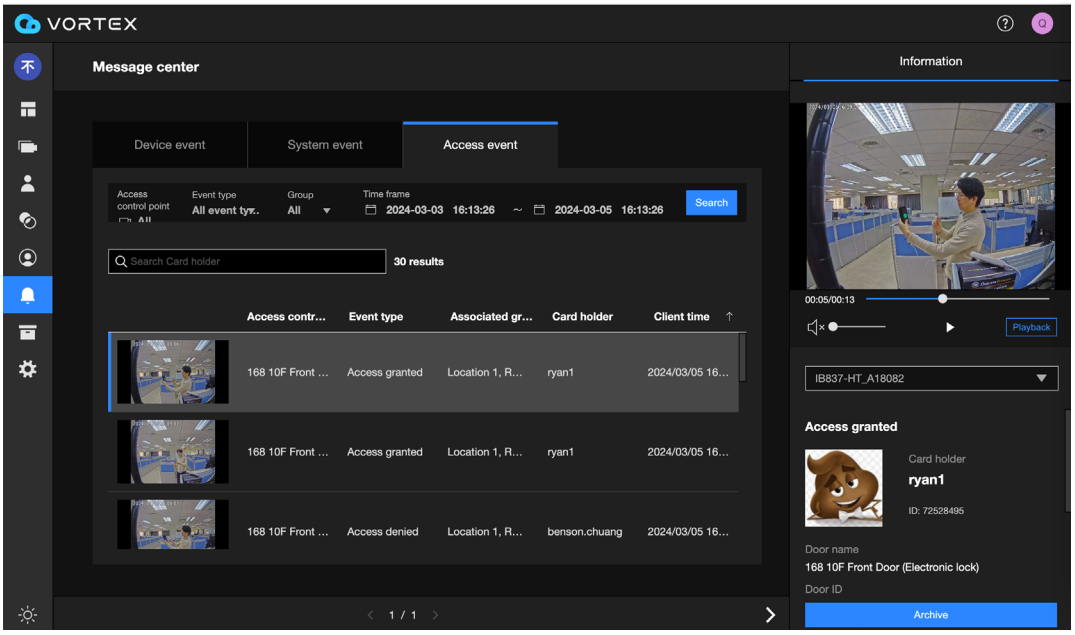
Lockdown	Door lockdown	Prevent users from entering or exiting a specific door	Enable door lockdown
	Place lockdown	Prevent users from entering or exiting any Kisi-enabled door in that particular place.	Enable place-wide lockdown
	Elevator lockdown	Lock a certain elevator stop for everyone	Enable elevator stop lockdown

Feature Guide - Web

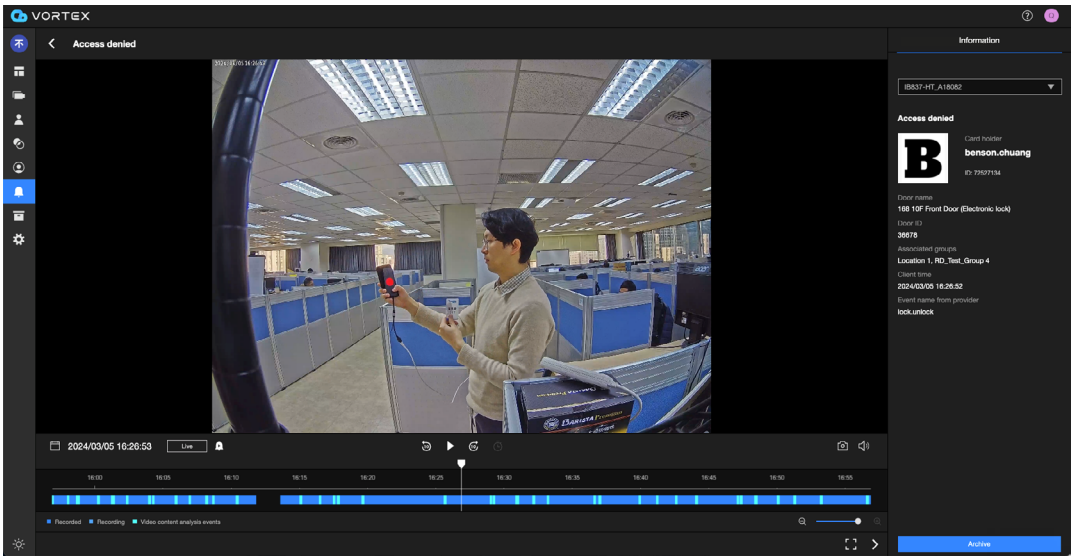
1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
   - Currently, the retention period for events is the same as for Cameras, which is 30 days (Longer retention will be implemented soon)
   - In the Search Filter, 'Group' refers to the location of the Camera, which also represents the location of the Access Control Point (the two are already associated).
   - The event time provided by Kisi is always UTC +00:00, without the actual local time. VORTEX defines this as Client time.

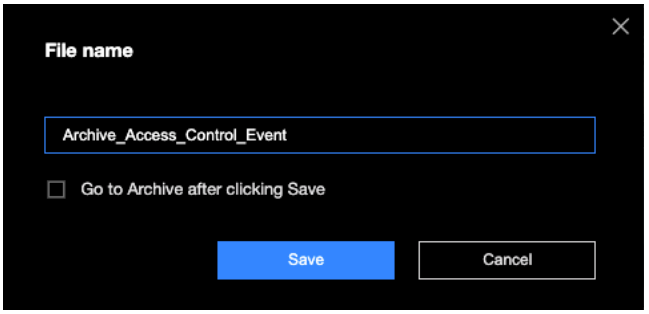


2. Select an access event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
   - If this door is linked to multiple cameras, you can choose a specific camera through the dropdown options below the footage.
   - For events not triggered by personnel authorized with Kisi, the Card Holder field will not display any names.



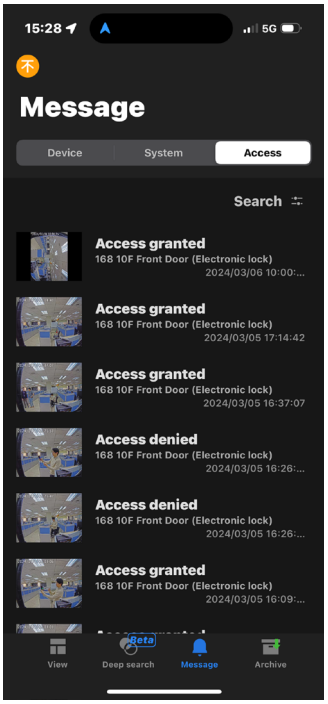
3. You can view the footage through playback, or archive this event footage and sharing with others.

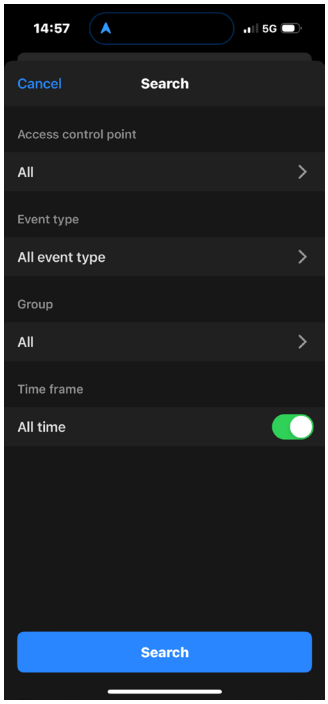




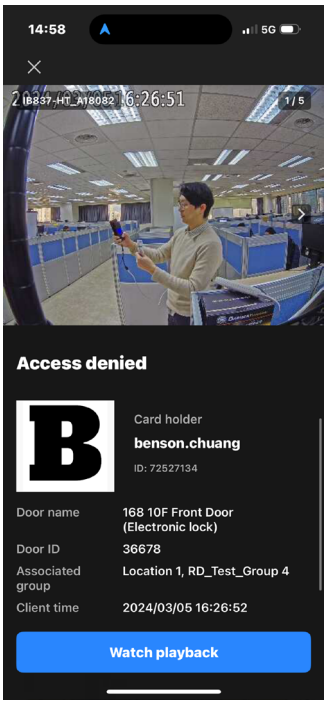
Feature Guide – Mobile App

1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
   - Currently, the retention period for events is the same as for Cameras, which is 30 days (Longer retention will be implemented soon)
   - In the Search Filter, 'Group' refers to the location of the Camera, which also represents the location of the Access Control Point (the two are already associated).
   - The event time provided by Kisi is always UTC +00:00, without the actual local time. VORTEX defines this as Client time.

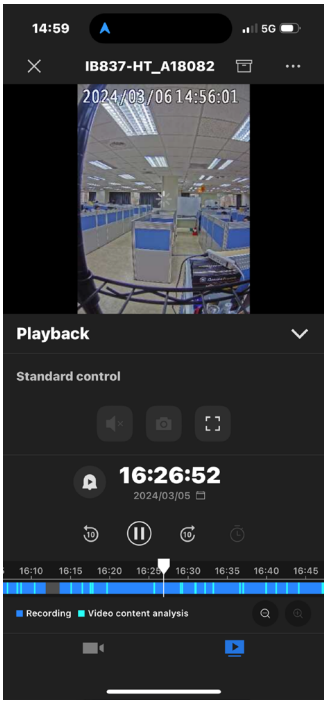


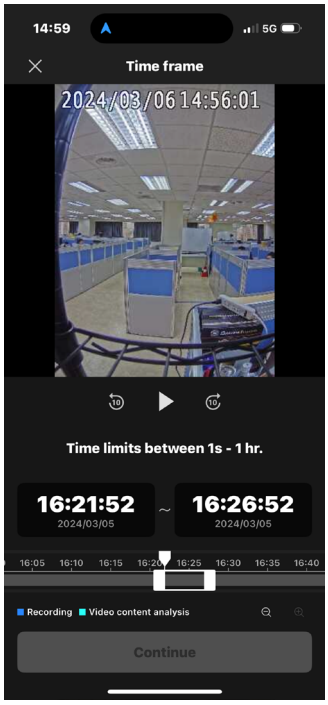


2. Select an access event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
   - If this door is linked to multiple cameras, you can choose a specific camera through swiping the snapshots.
   - For events not triggered by personnel authorized with Kisi, the Card Holder field will not display any names.



3. You can view the footage through playback, or archive this event footage and sharing with others.

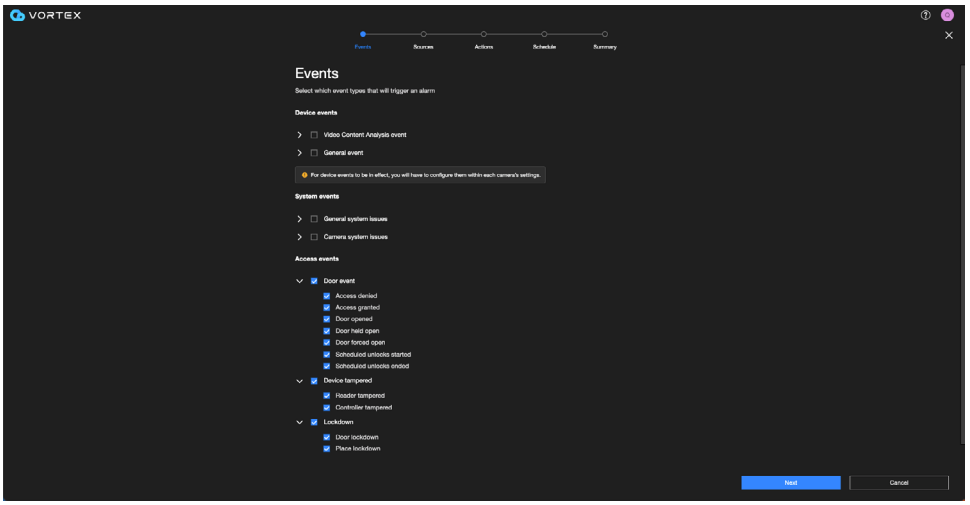


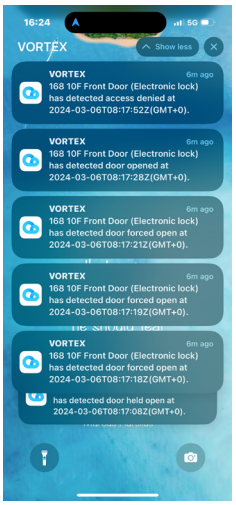


Alarm settingsand Real-time Notification

Goal

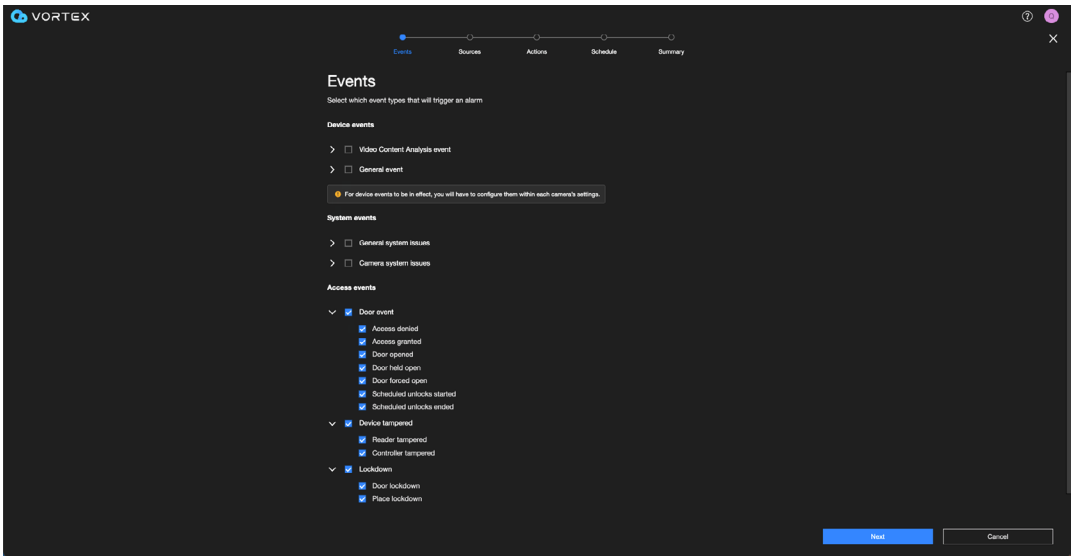
- Allow Owner/Administrators to set alarms for Access events in Alarm Management, allowing designated personnel to receive real-time push notifications and email notifications.



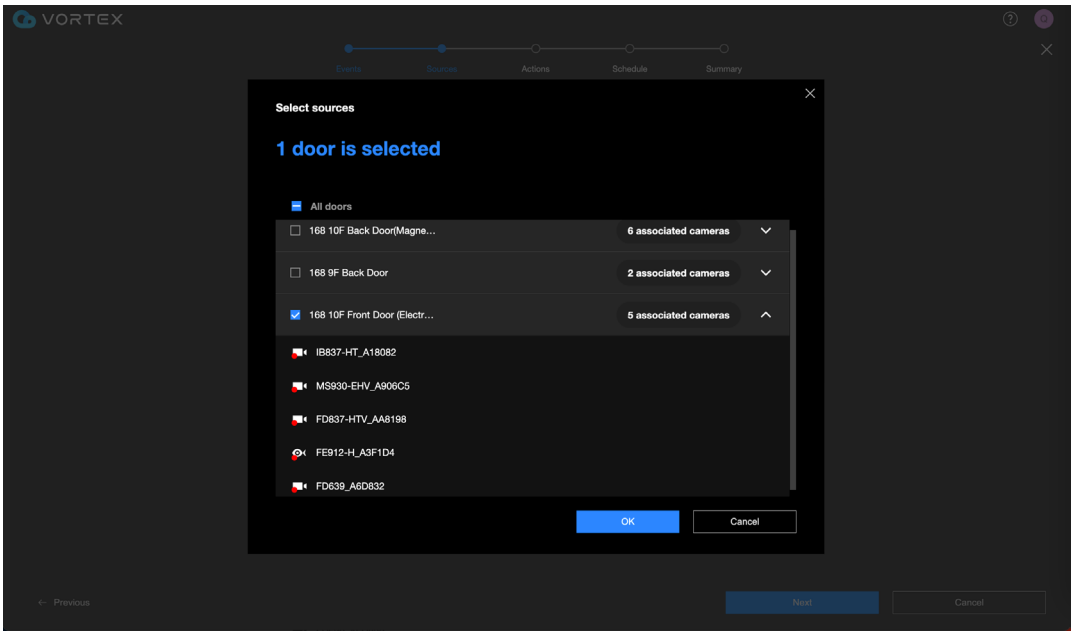


Feature Guide - Web

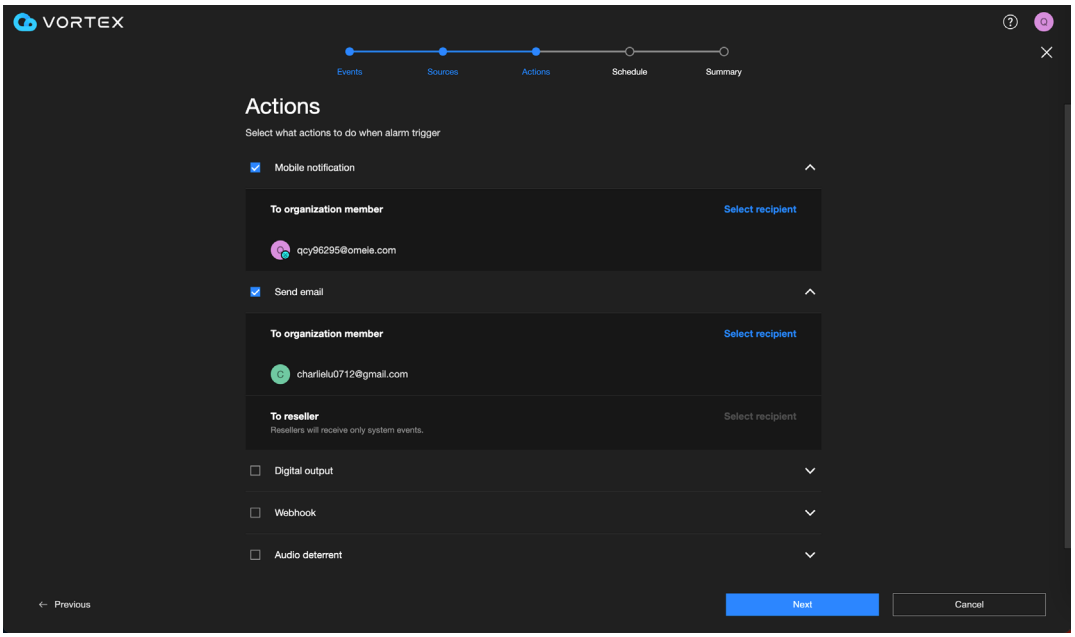
1. Go to System > Alarm Management > Add alarm
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Access event
   - Users who are not integrated with Access Control will still see the Access events option on this page; however, no alarms will be generated upon setting completion (currently, Alarm Management's design does not display the supportable events based on the type of device a user has)



2. In the next step - Sources, select the doors that initiate Access events.
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Sources for the Door
   - Only doors that are already associated with cameras will appear in this list
   - Click the expand button to view the cameras associated with this door

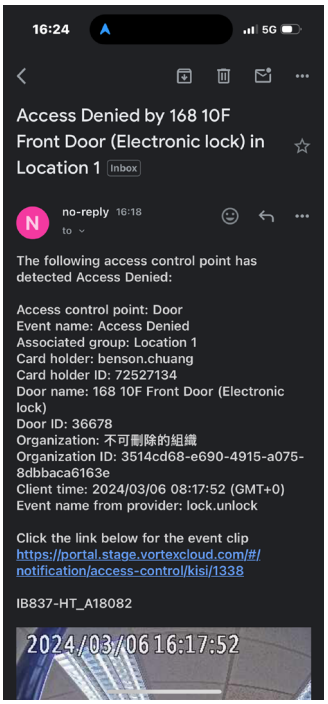


3. In the next step - Actions, select the doors that initiate Access events.
   - The design logic here is the same as the existing Alarm Management.
   - Access events only support Mobile notification and Send emails. Other Actions are not supported.
   - The remaining steps, Schedule and Summary, follow the same design logic and operate in the same manner as they currently do.



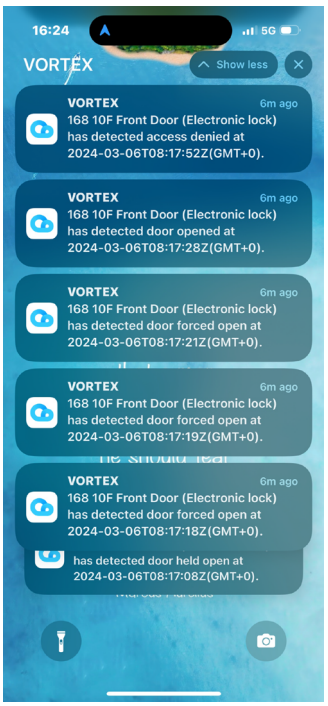
Feature Guide – Email Notification

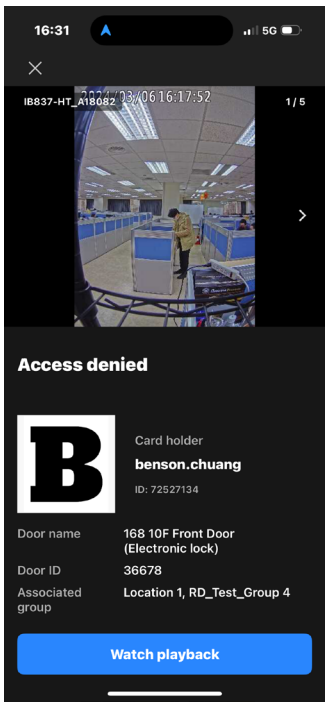
- Designated personnel received email notification.
- If a door is associated with multiple cameras, the email will display snapshots from these cameras.



Feature Guide – Mobile App

- Designated personnel received real-time push notification.
- Access events that may result in a continuous state will only trigger an alarm notification the first time they occur, such as 'Door held open' and 'Door forced open.

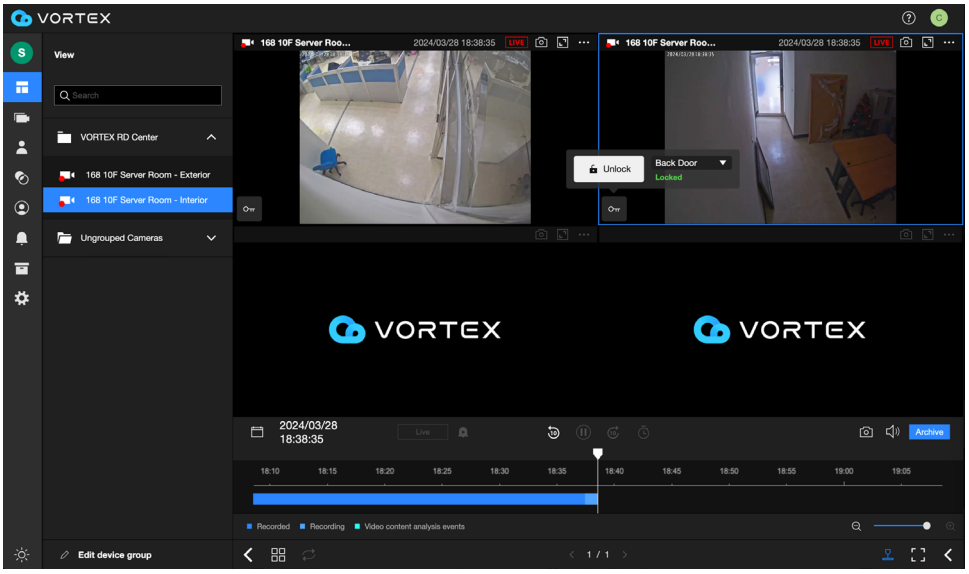


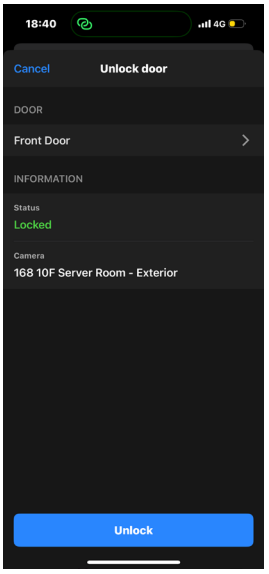


Remote Unlock Doors

Goal

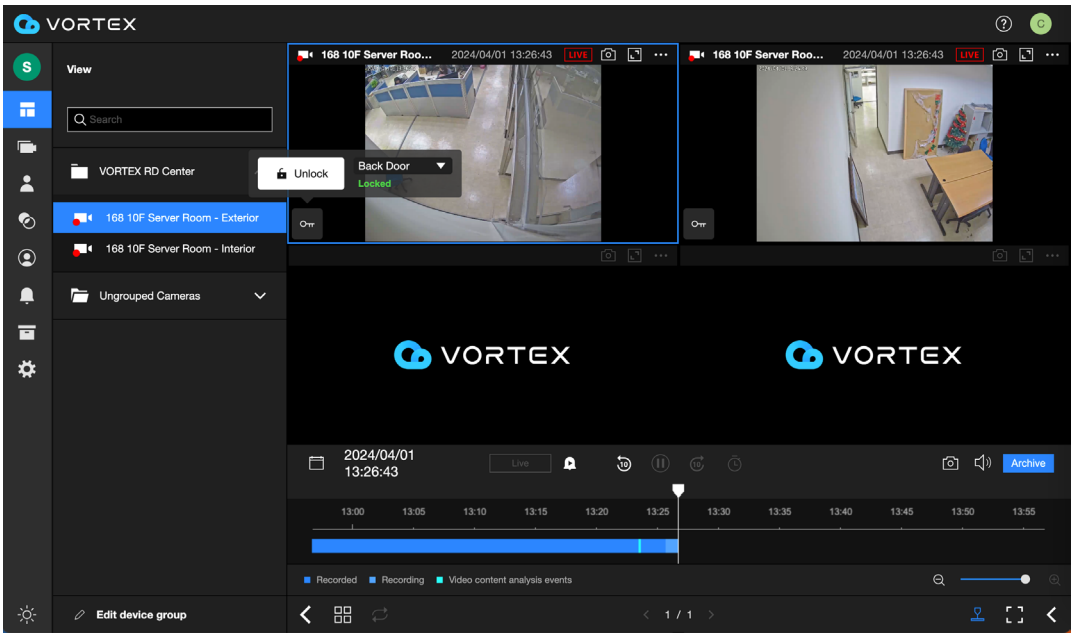
Allow owner/admin/supervisor to assist with daily access needs remotely and manage doors during emergency situations without having to be physically present on-site.



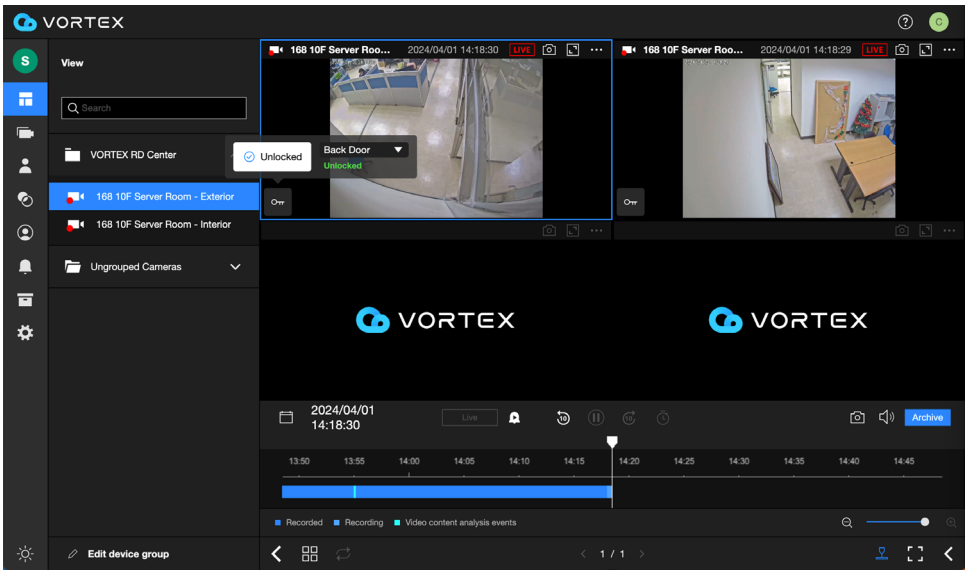


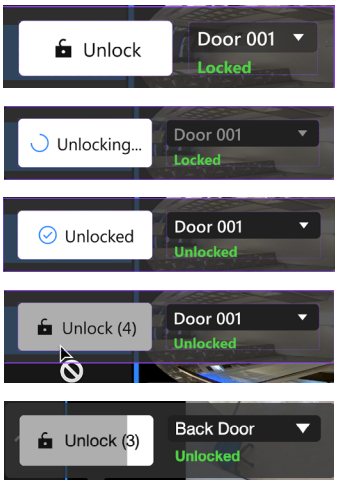
Feature Guide - Web

1. Go to Live View. Cameras that have been associated with doors display “key icon” on respectively view cell.
   - When this camera is associated with multiple doors, a dropdown will appear to select a specific door.
   - The order of Doors within the dropdown is sorted by ASCII.
   - There are 4 Door statuses:
     1. Locked
     2. Unlocked
     3. Locked down
     4. Offline
   - If this Door is in Locked down or Offline status, the Remote unlock will not be possible (the button will be disabled).



2. Click on the unlock button on the door you wish to operate the remote unlock.
   - After clicking the unlock button, one must wait for 7 seconds (including UI response time) before proceeding with the next operation.

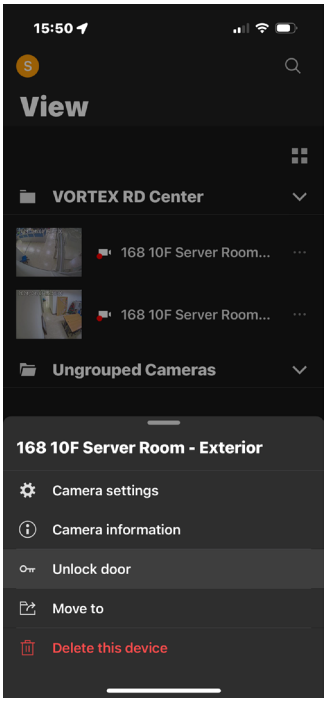


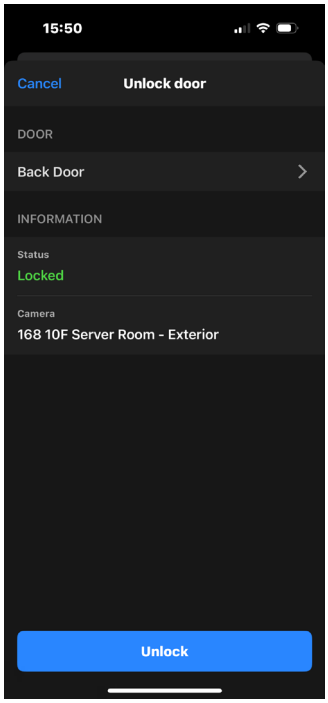


Feature Guide – Mobile App

1. Go to Live View. Cameras that have been associated with doors display” Unlock door” option in more option.
   - When this camera is associated with multiple doors, a dropdown will appear to select a specific door.
   - The order of Doors within the dropdown is sorted by ASCII.
   - There are 4 Door statuses:
     1. Locked
     2. Unlocked
     3. Locked down
     4. Offline

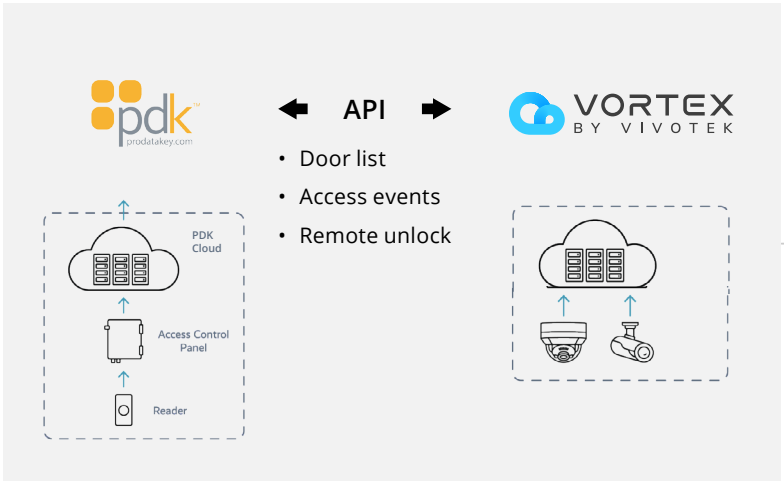
- If this Door is in Locked down or Offline status, the Remote unlock will not be possible (the button will be disabled).



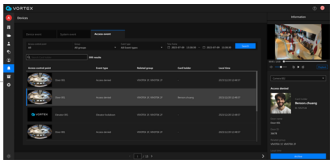


Access control Integration – PDK

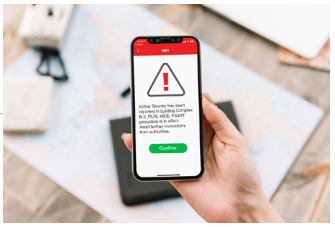
System Overview



- **Access Events Integration with Native video**



- **Real-time Access Event Notification**

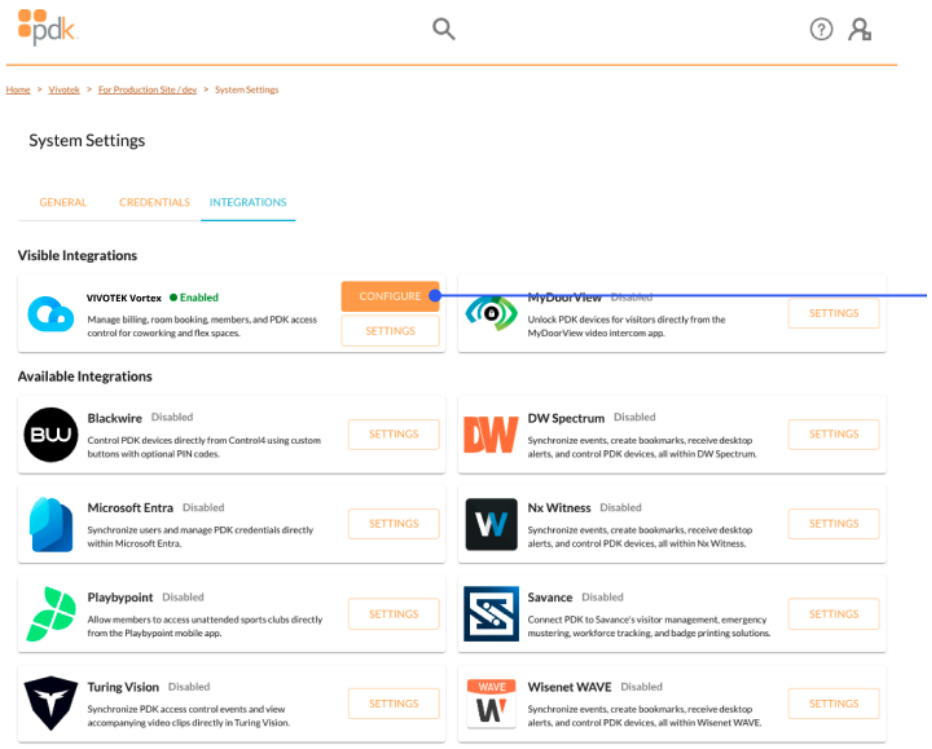


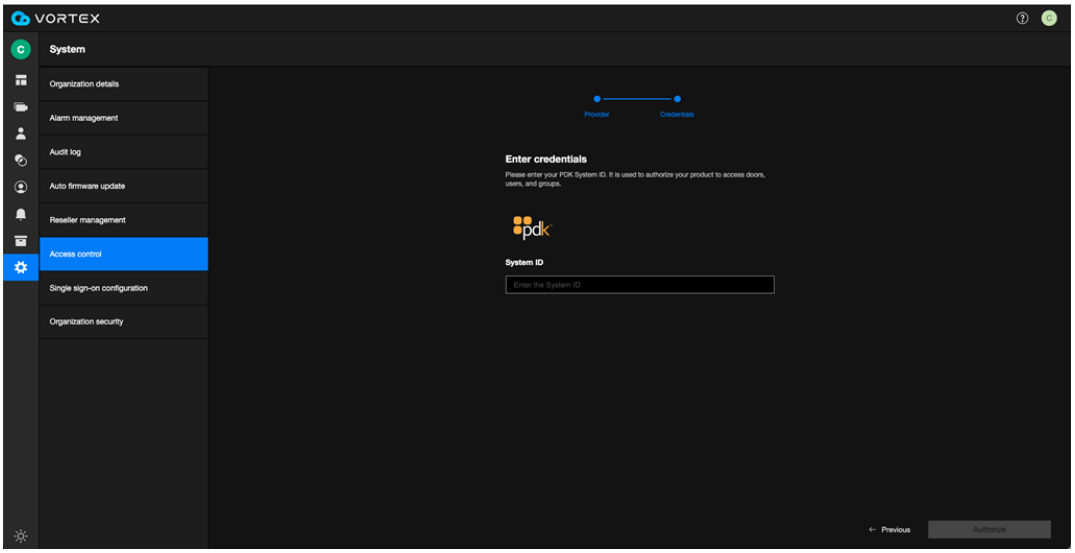
- **Remotely Unlock/Lock Doors**

API integration

Goal

- Enable VORTEX to retrieve the list of PDK's doors and access events; Allow control of PDK's doors through VORTEX.

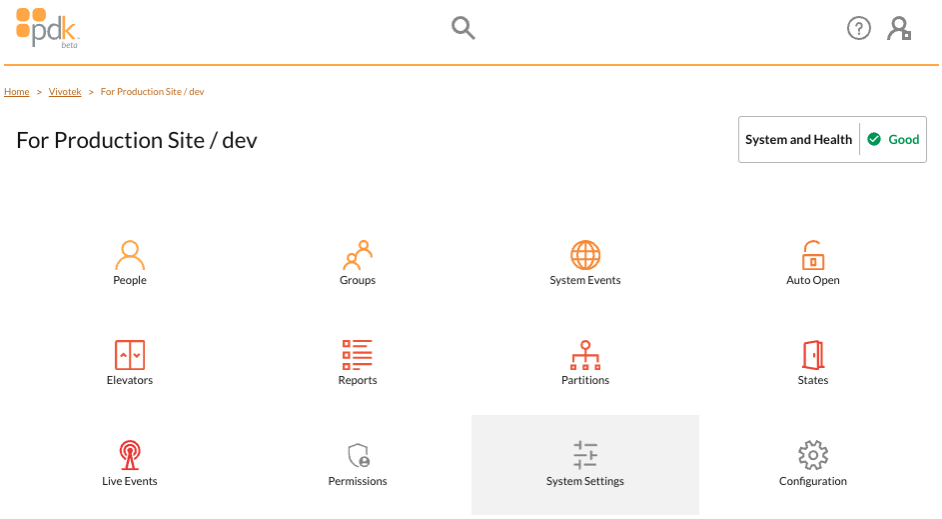


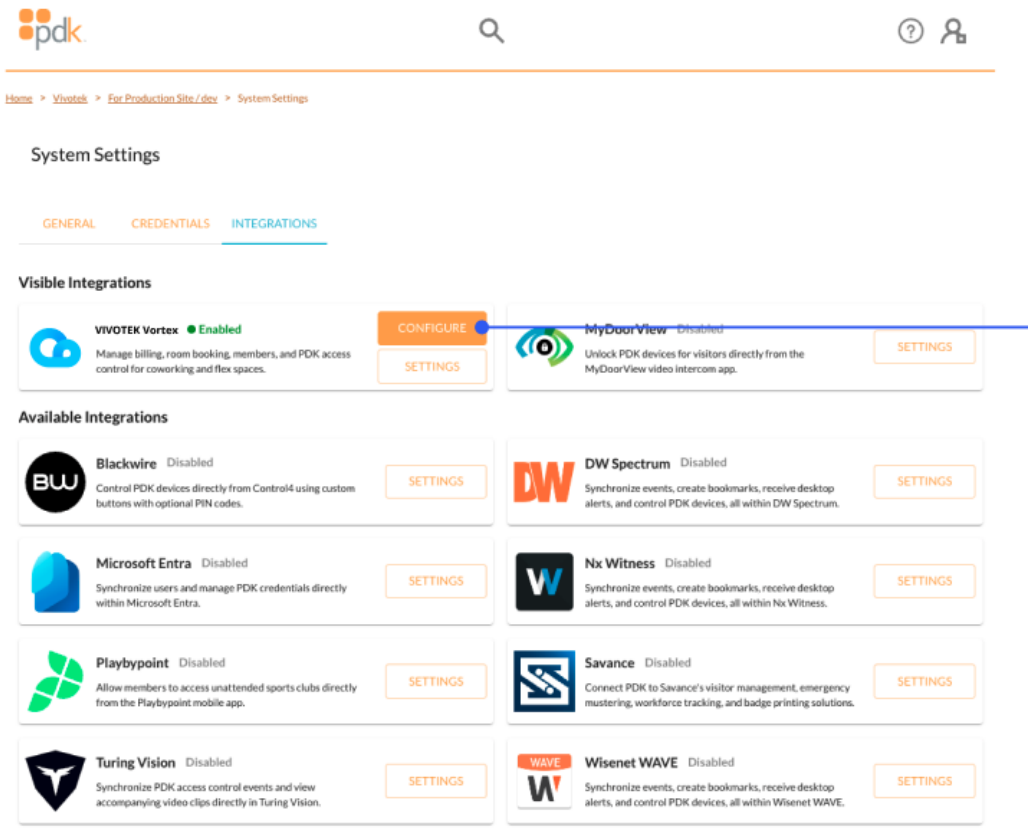


Method A – PDK Marketplace Tile (Recommended)

1. Go to PDK platform > System Settings > Integrations
   - Dealers and customers will be able to easily and securely pass their system ID to your application via the configuration URL.

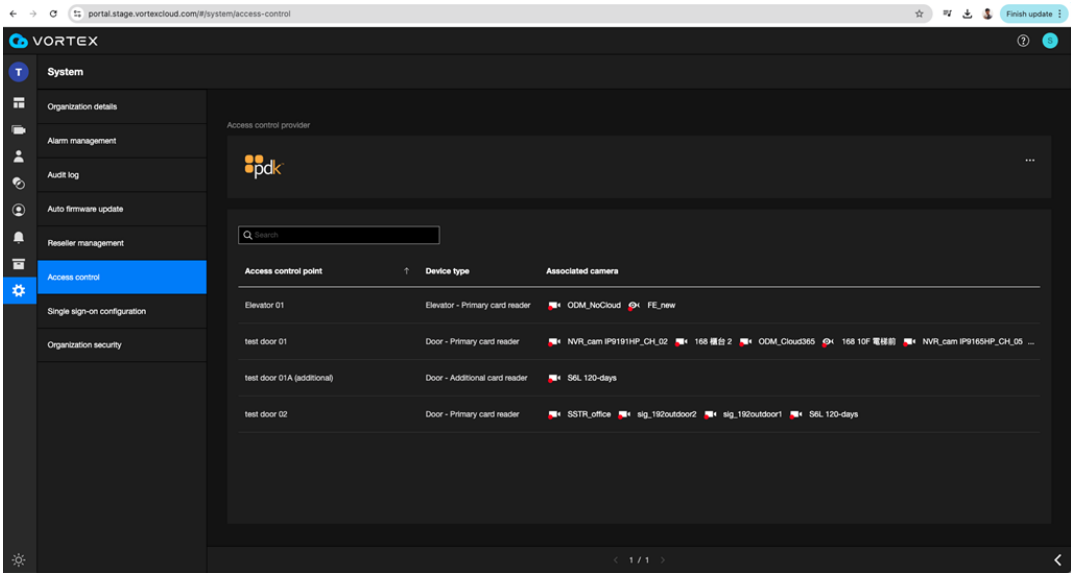
- With Method A, the integration can be completed with a single click, eliminating the need for manual operations like Method B, which also poses security risks.





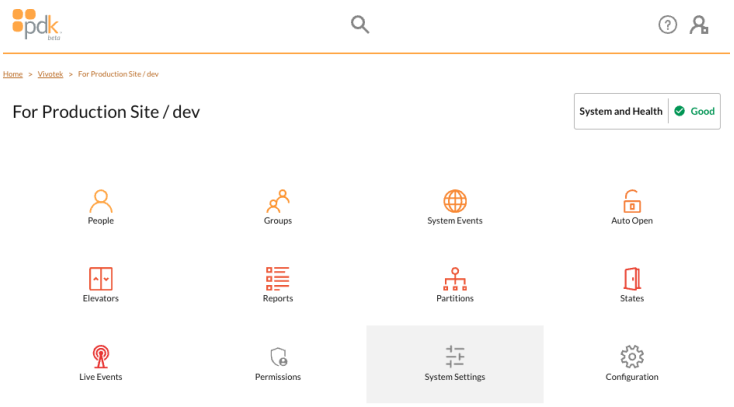
2. Click “CONFIGURE” button to directly complete integration between PDK and VORTEX.

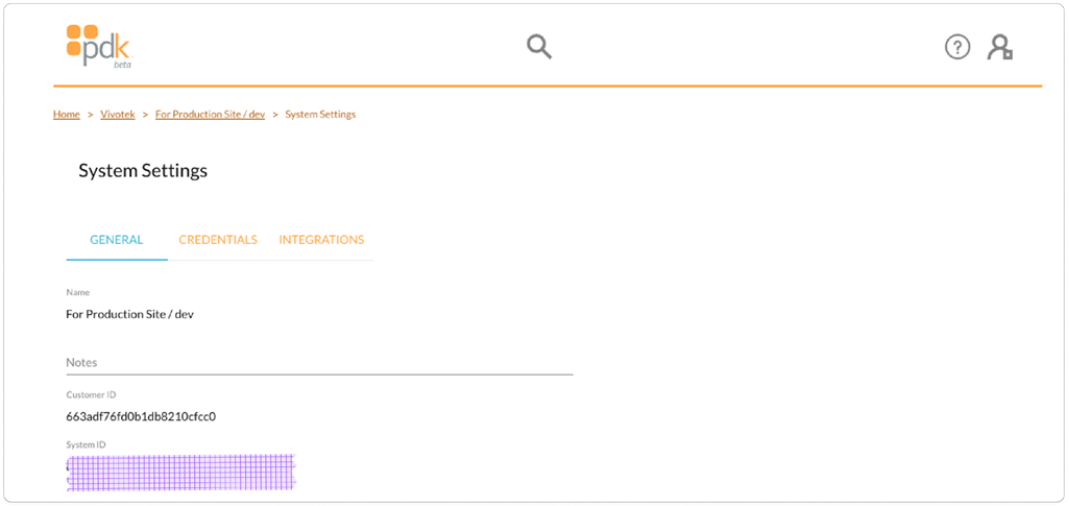
- Only PDK Integrator/Admin and VORTEX Owner/Admin can operate this function.
- A single VORTEX Org. can only integrate with one PDK Org.
- A VORTEX org. can only integrate with one access control provider and cannot have both Kisi and PDK integrations at the same time. (This limitation will be addressed once the multi-organizations feature is implemented in the future.)



Method B

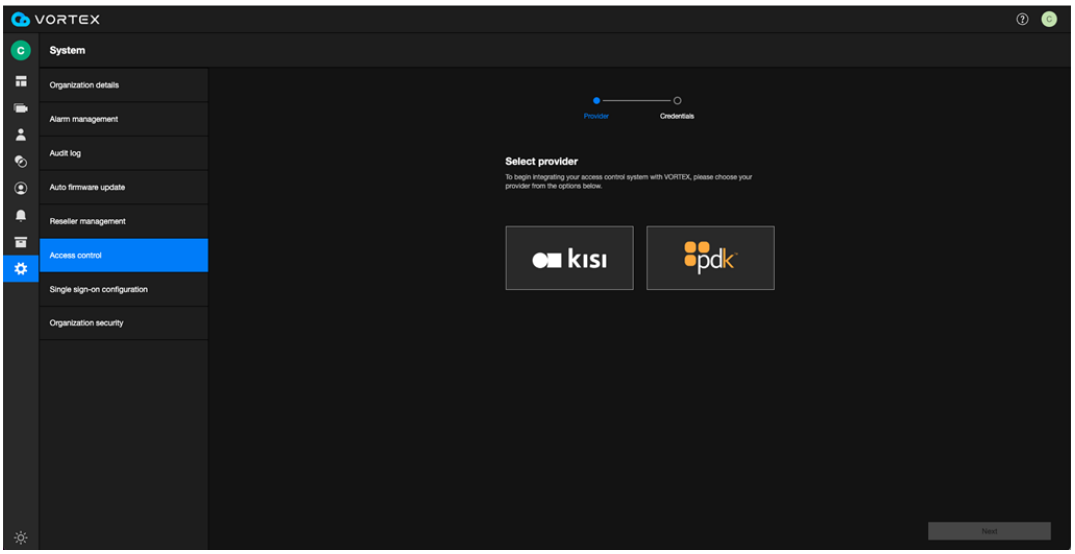
1. Go to PDK platform > System Settings
2. Copy “System ID”

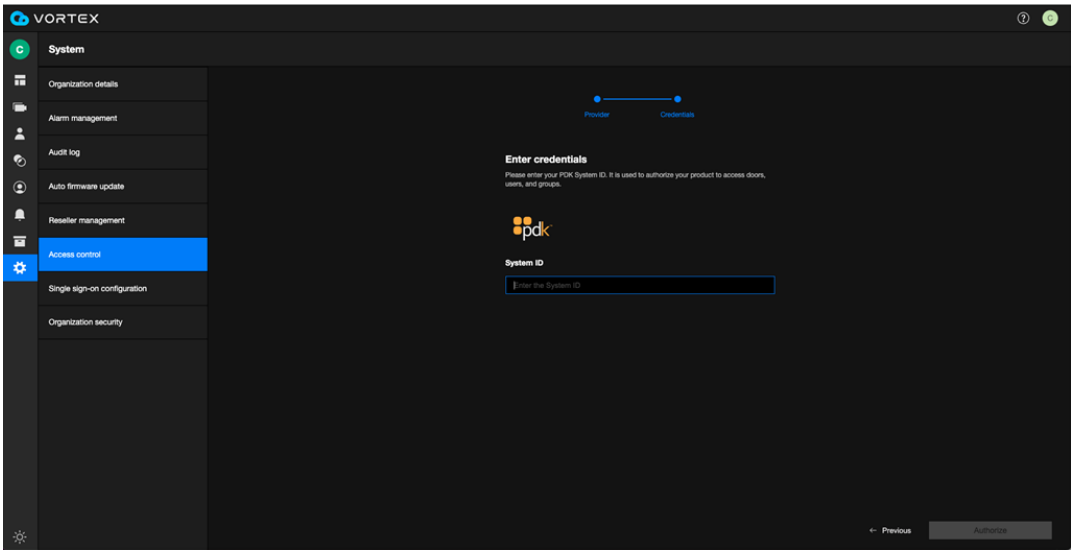




3. Go to VORTEX > System > Access control, Choose PDK logo.
4. Paste PDK System ID and click Add.
   - Only VORTEX Owner/Admin can operate this function.

- A single VORTEX Org. can only integrate with one PDK Org.
- A VORTEX org. can only integrate with one access control provider and cannot have both Kisi and PDK integrations at the same time. (This limitation will be addressed once the multi-organizations feature is implemented in the future.)

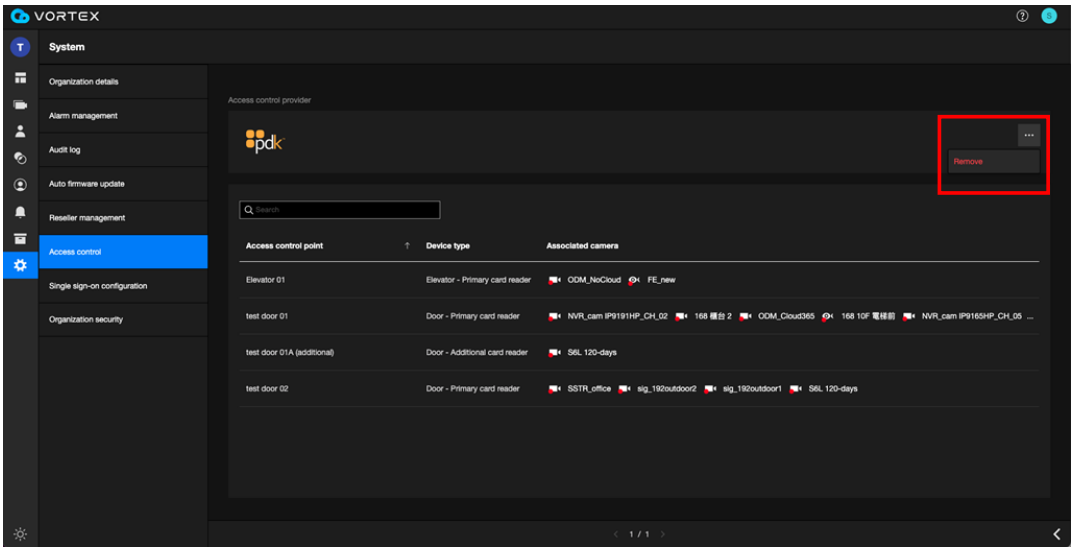




Delete Integration

If you decide to remove the integration with PDK, click the 'More option' button.

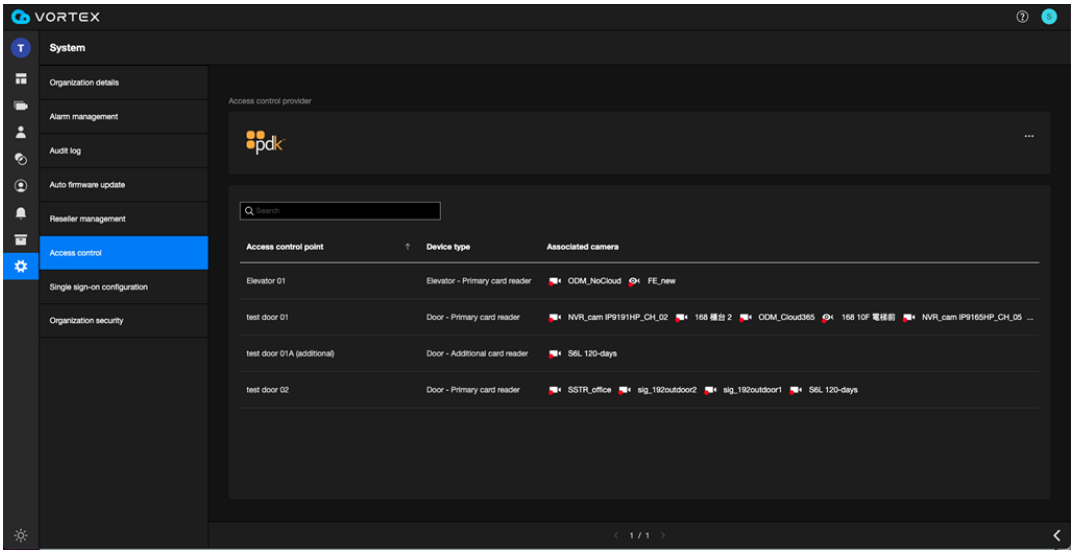
- After the integration is removed, all previously edited settings and access events history will be deleted.



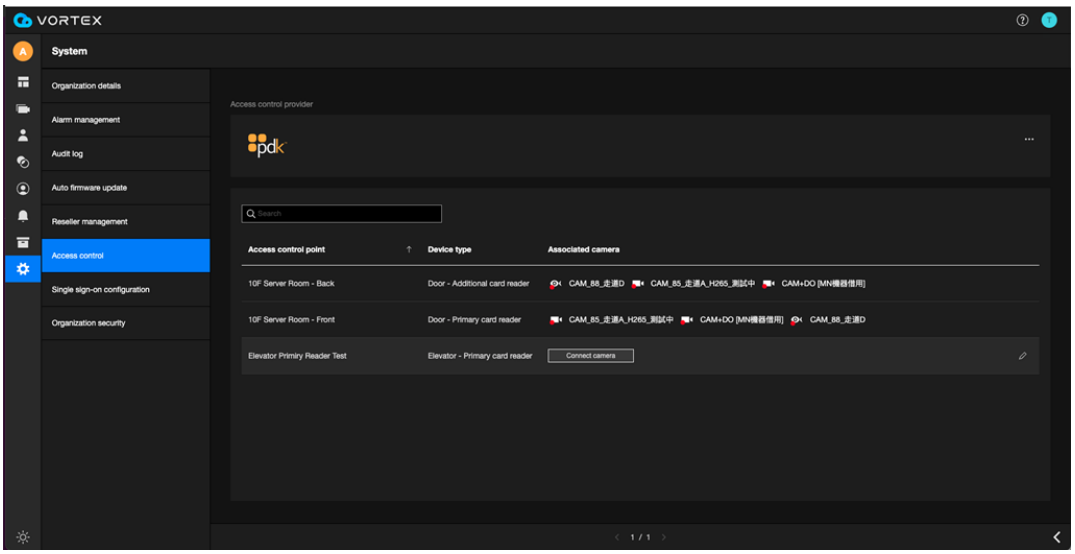
Associate Cameras with Doors

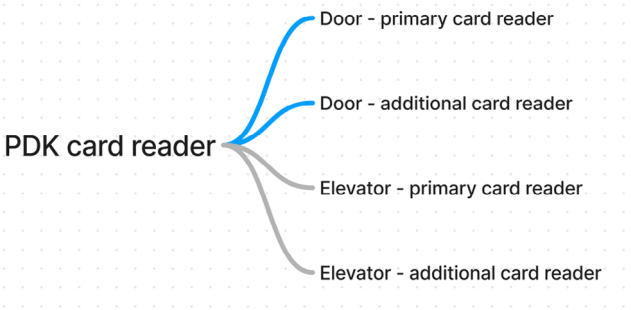
Goal

To associate events from PDK with VORTEX Cameras, the Owner/Admin must first link PDK doors with VORTEX Cameras.



1. On the door you want to associate, click ”Connect camera“
   - Only Owner/Admin can operate this function
   - This page lists all the doors and elevators in the PDK org
   - PDK’s Device Type supports both Door and Elevator, and each can be further categorized as Primary or Additional. Learn more details on PDK’s Device Type design.

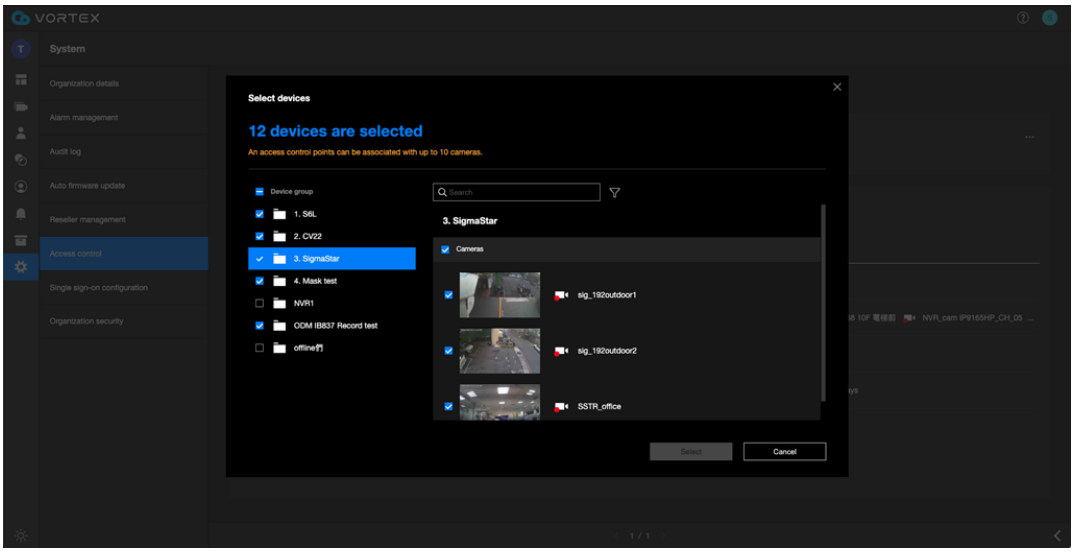




2. Select the cameras you want to associate with this door.

   Many-to-many design:

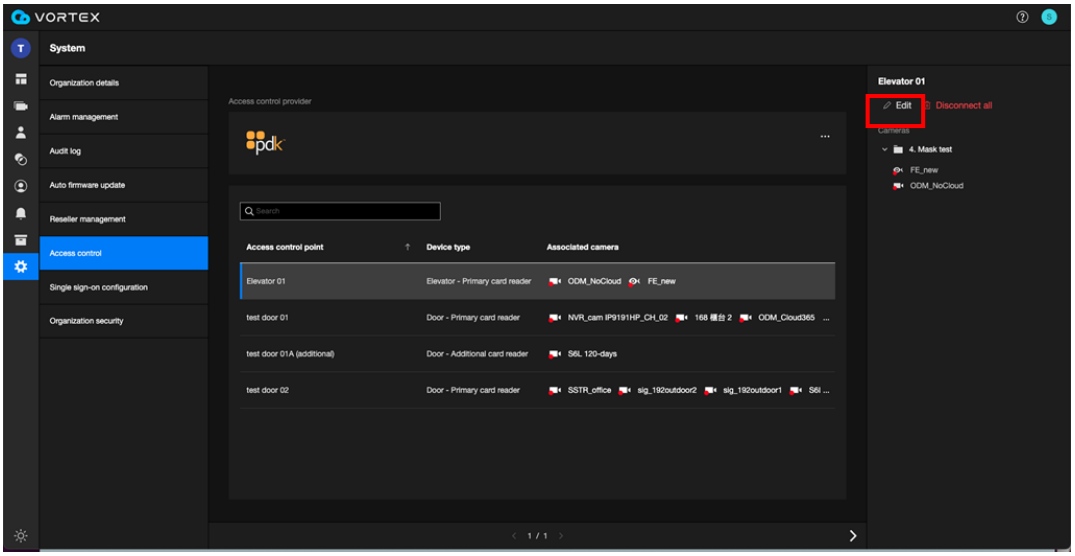
   - Each door can be associated with up to 10 cameras.
   - The same camera can be associated with multiple different doors at the same time.



3. If adjustments are needed after the settings are complete, you can make changes through the “Edit” button.

   - Users can add/edit/disconnect the cameras associated with doors

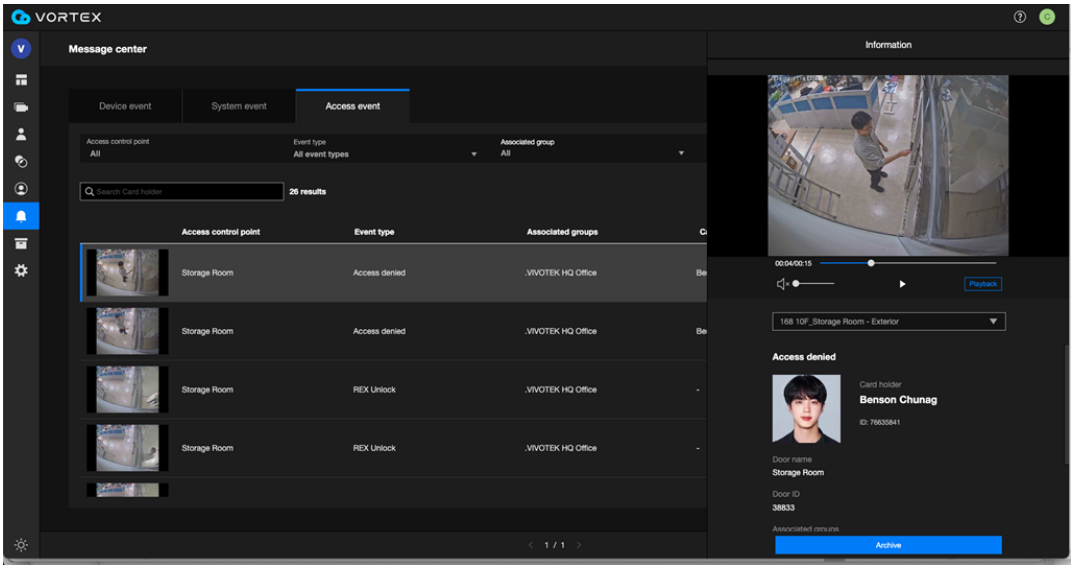
- If users add/edit/delete doors on the PDK platform, VORTEX will reflect the corresponding changes based on the adjustments
- Each time the Owner/Admin enters this page, VORTEX will check if the integration with PDK is functioning properly. If the integration is interrupted, an error message will be displayed here.



Access Events Integration with Native video

Goal

- Allow users to access an instant and comprehensive view of integrated info. from both systems.
- Link access control data to video surveillance data to verify if someone entering is the person they claim to be.



Event Type Difference - PDK vs. Kisi

Type	PDK	Kisi	Remark
Shared Events	Access granted	Access granted	
	Access denied	Access denied	
	REX unlock	REX unlock	
	Door forced open	Door forced open	
	Door held open	Door held open	
	Schedule unlocks started/ ended	Schedule unlocks started/ ended	
PDK Exclusive Events	Force Close	X	
	Force Open	X	
	Scheduled unlocks override	X	
Kisi Exclusive Events	X	Reader tampered	PDK device doesn't support tamper detection design
	X	Controller tampered	
	X	Door lockdwon	The design of PDK's API utilizes a single API, 'device.forceclose. on/off,' to cover both scenarios: Lockdown and Do Not Disturb. Currently, it is not possible to distinguish between these scenarios through the API. Therefore, the Lockdown scenario in PDK is uniformly represented by the Force Close event.
	X	Place lockdown	
	X	Elevator lockdown	

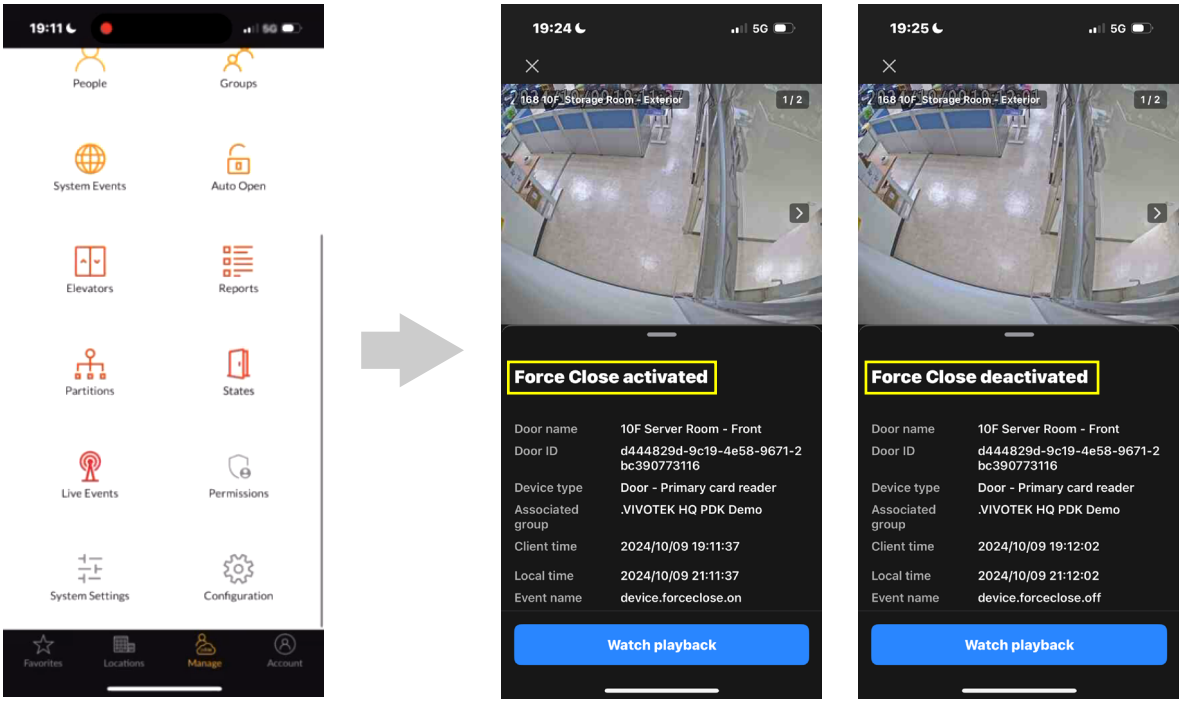
PDK Event Types

	Event	Description	Prerequisite & Doc.
Existing event	Access granted	User-granted access to unlock an access-controlled door	• Credential Self-Help • Adding People & Credentials
	Access denied	User-denied access to unlock an access-controlled door	
	REX unlock	Request to exit (REX) is triggered and unlocks a door	• Set up a REX
	Door forced open	Access controlled or locked door is opened without a request to exit (REX) detected or a user who has been granted access	• What's door forced open? • What's door held open? • Set up Door Position Sensor(DPS)
	Door held open	Detects an unlock, but the contact sensor reports the door being open longer than the duration set by the PDK organization admin.	
	Schedule unlocks started/ ended	Unlock schedules you have set on PDK start or end	• Auto Open overview
PDK exclusive event	Force Close	User activates the card reader into 'Do Not Disturb' or 'Lockdown' or "Force Close" mode through app activation or event rule settings in the PDK system.	• Do Not Disturb • Lockdwon • Event rules
	Force Open	User activates the card reader into 'Force Toggle' or "Force Close" mode through app activation or event rule settings in the PDK system.	• Event rules • Doors and Devices States
	Scheduled unlocks override	During the lock/unlock schedule period, user activates the card reader into 'Force Toggle' mode through app activation or event rule settings in the PDK system.	

PDK exclusive event - Force Close (by App Activation)

PDK App Activation - “Do Not Disturb(DND)”

- **Scenario:** Part of the building is under construction and you want to prevent employees from accessing that part of the building while the construction is under way, so you enable DND on the doors leading. Even when valid credentials are presented, users are not able to access these areas.

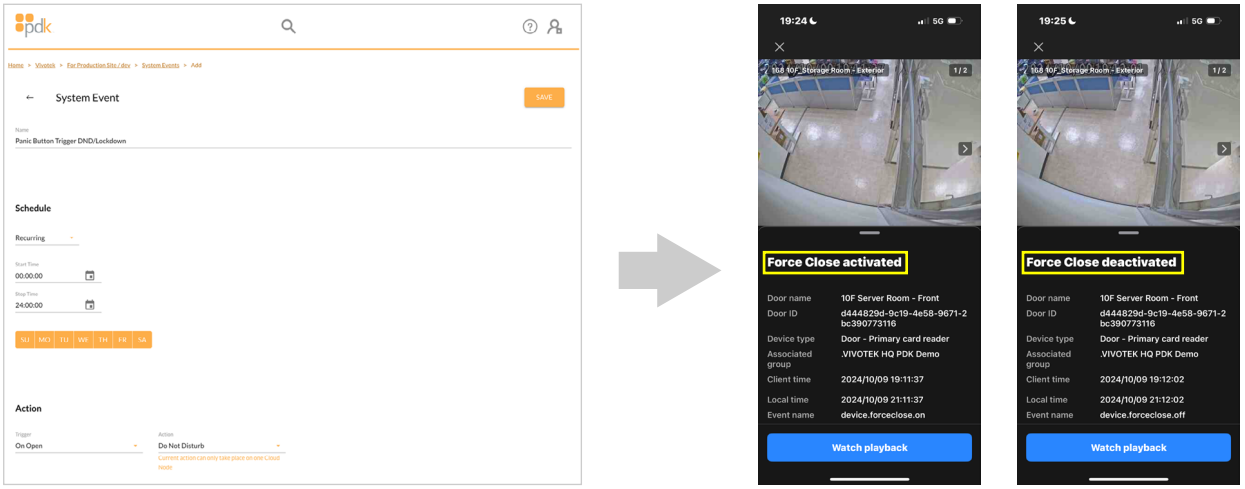


VORTEX Received and Display the Event

PDK exclusive event - Force Close (by Event Rule)

Triggered by PDK Event Rule Configuration

- **Scenario:** A panic button connected to the PDK controller is pressed during an active threat, triggering a system lockdown. A system event rule places all doors in a DND state, preventing potentially dangerous movement throughout the building.

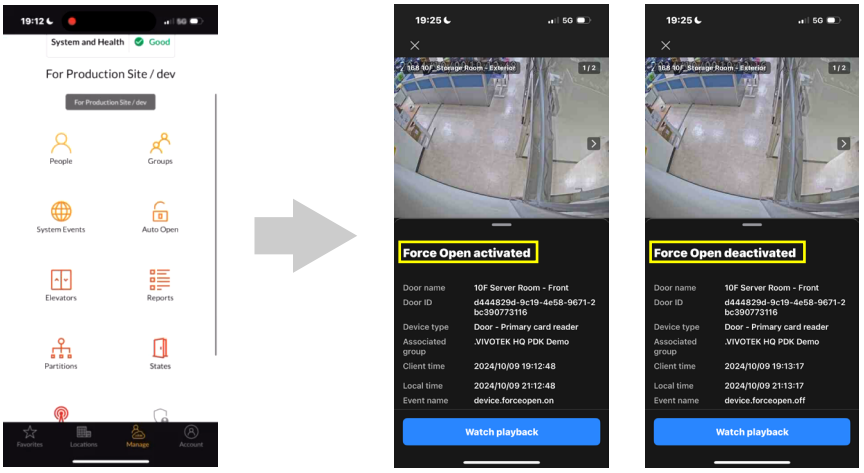


VORTEX Received and Display the Event

PDK exclusive event - Force Open (by App Activation)

App Activation - “Force Toggle”

- **Scenario:** You want to leave a door open temporarily during a public event, so you use force toggle to unlock the door and leave it unlocked. When the event is over, you use force toggle again to return the door to its normal locked state.

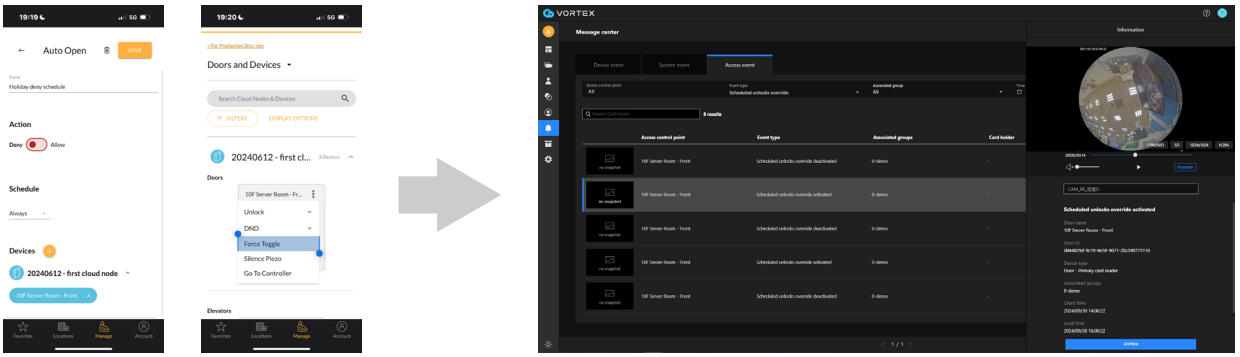


VORTEX Received and Display the Event

PDK exclusive event - Scheduled unlocks override (by App Activation)

App Activation - “Force Toggle”

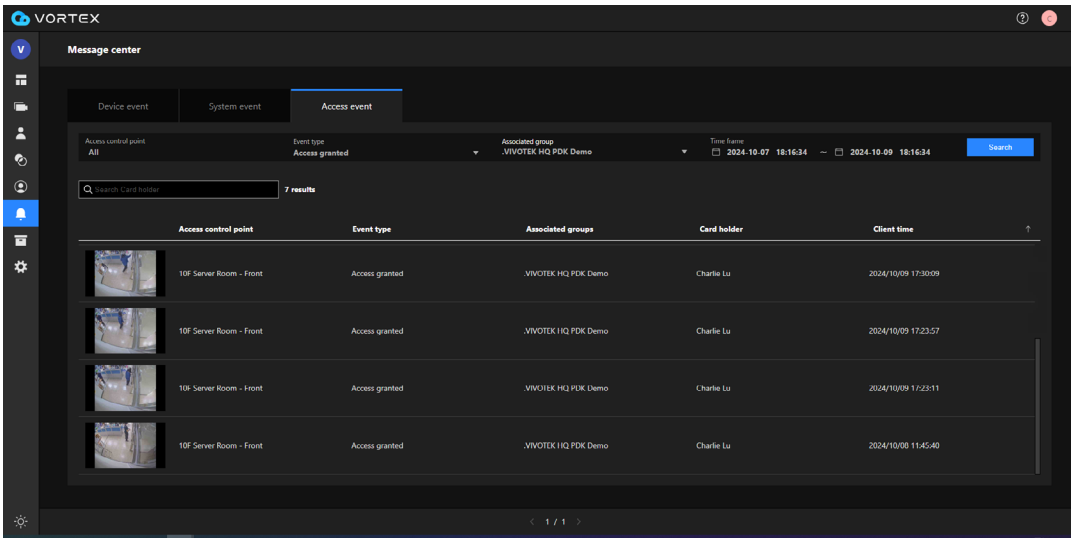
- **Scenario:** When the Auto Open Schedule is manually overridden, the system sends a notification to remind the user. For example, a school might set an Auto-Open Deny Schedule on a national holiday to prevent anyone from entering. However, if there's an urgent maintenance task requiring access, the administrator can activate the 'Force Toggle' function via the PDK App to manually open the door. In this case, an 'Auto Open Schedule Override Activated' event will trigger a notification.



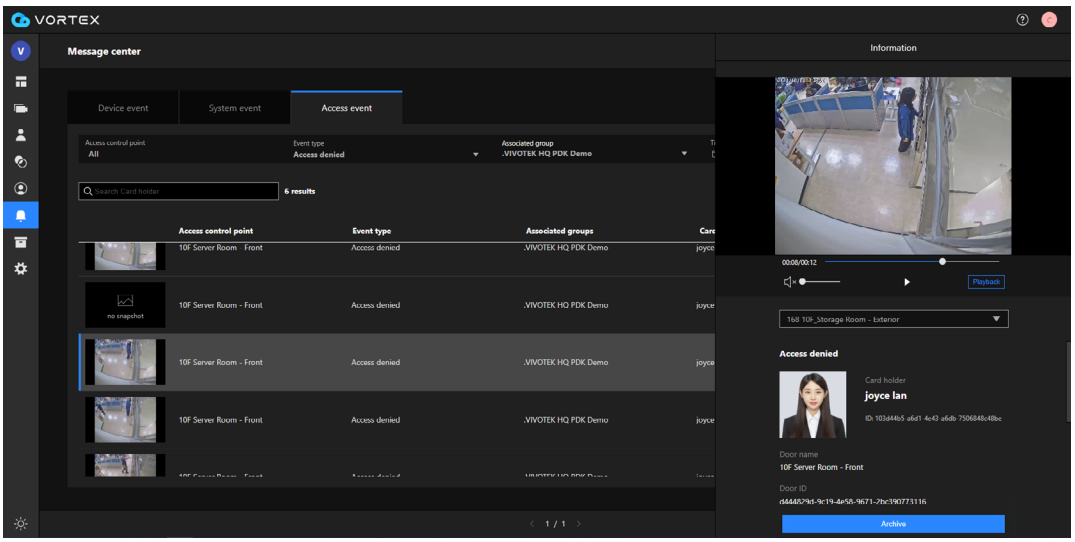
VORTEX Received and Display the Event

View access event in Message Center

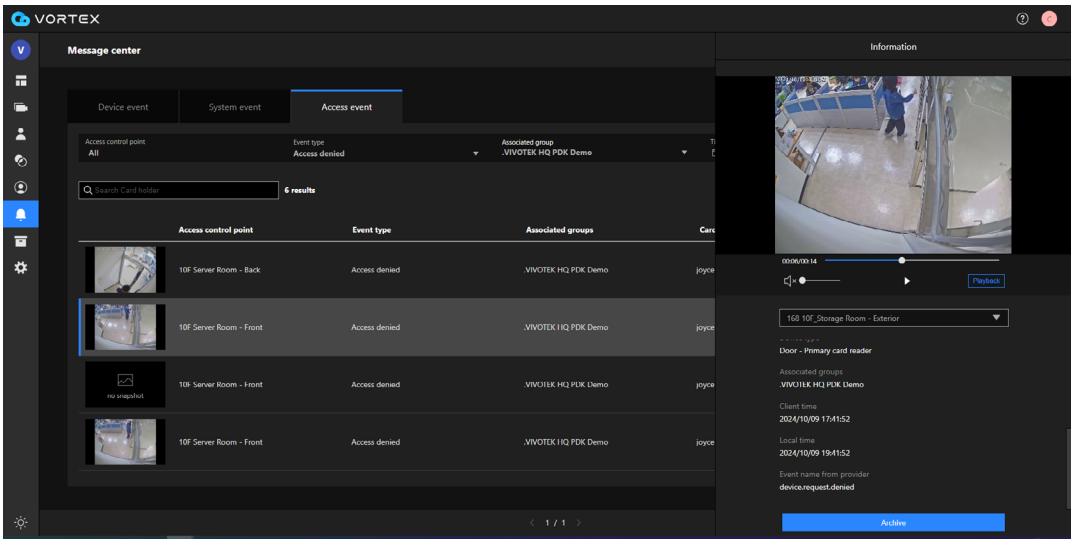
1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, the time range, and the card holder by setting filter criteria.
   - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with extended access dependent on the cloud backup plan purchased by the end-user.
   - In the Search Filter, 'Group' refers to the location of the Camera, which also represents the location of the Access Control Point (the two are already associated).



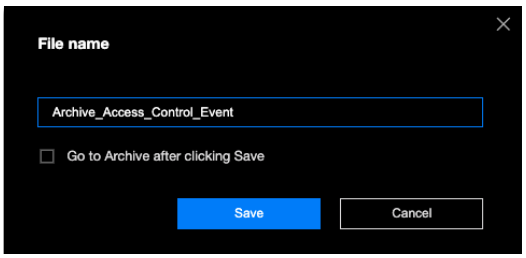
2. Select an access event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
   - If this door is linked to multiple cameras, you can choose a specific camera through the dropdown options below the footage.
   - For events not triggered by personnel authorized with PDK, the Card Holder field will not display any names.



3. Scroll down on the event panel on the right to view more detailed information.
   - To match PDK's Device Type design, a new Device Type field is added, so users can know the data source of the event.
   - PDK provides the local time when the event is triggered, so this field has been added.

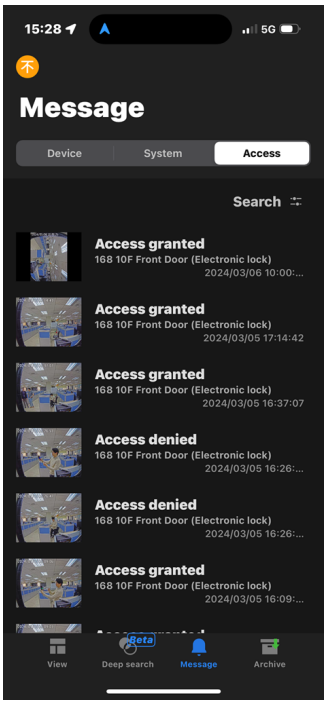


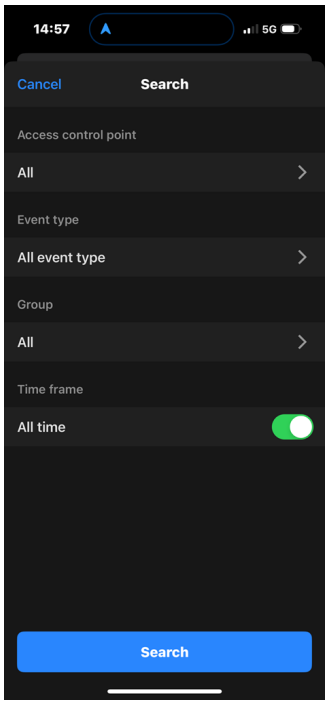
4. You can view the footage through playback, or archive this event footage and sharing with others



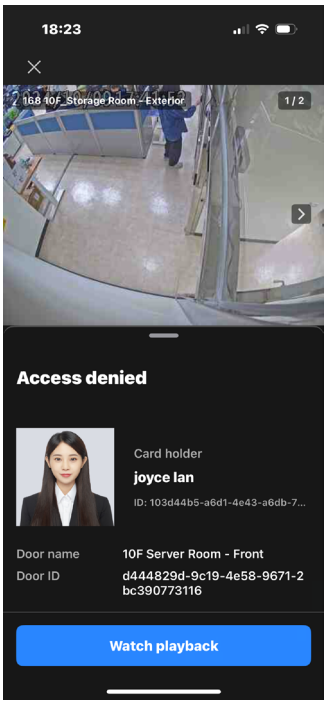
Mobile App

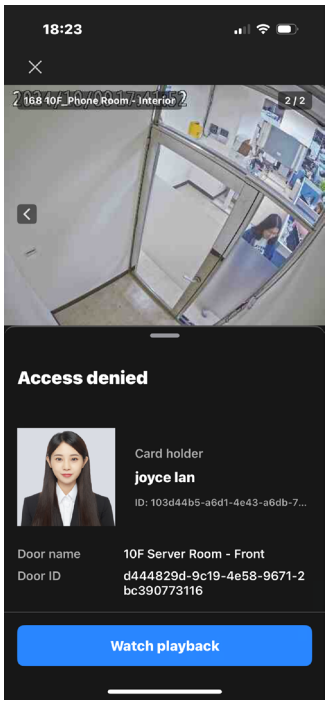
1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
   - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with extended access dependent on the cloud backup plan purchased by the end-user.
   - In the Search Filter, 'Group' refers to the location of the Camera, which also represents the location of the Access Control Point (the two are already associated).

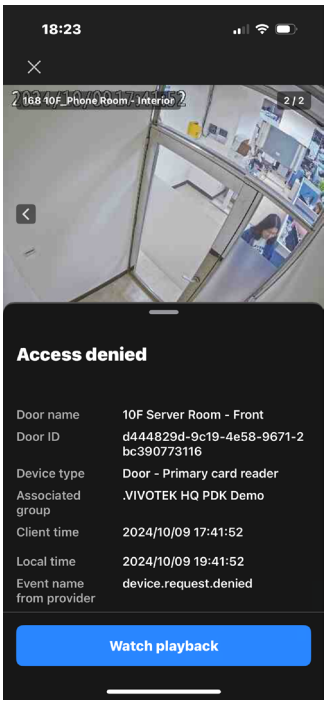




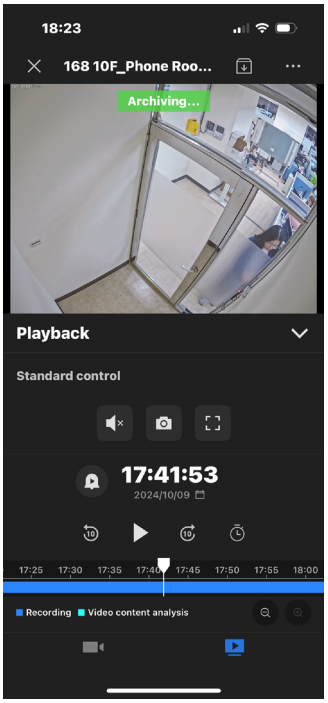
2. Select an access event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
   - If this door is linked to multiple cameras, you can choose a specific camera through swiping the snapshots.
   - For events not triggered by personnel authorized with PDK, the Card Holder field will not display any names.
   - To match PDK's Device Type design, a new Device Type field is added, so users can know the data source of the event.
   - PDK provides the local time when the event is triggered, so this field has been added.

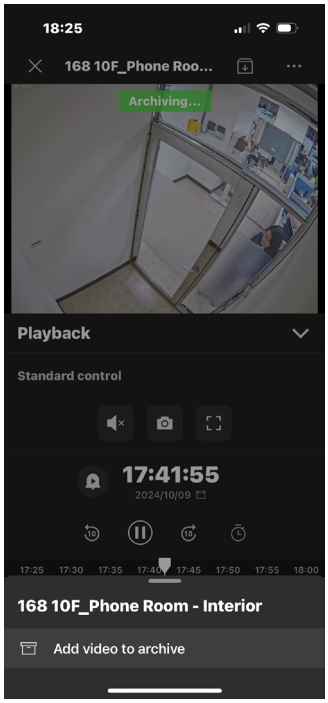


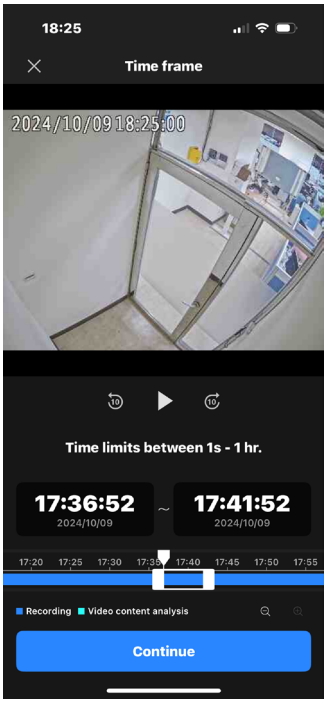




3. You can view the footage through playback, or archive this event footage and sharing with others.



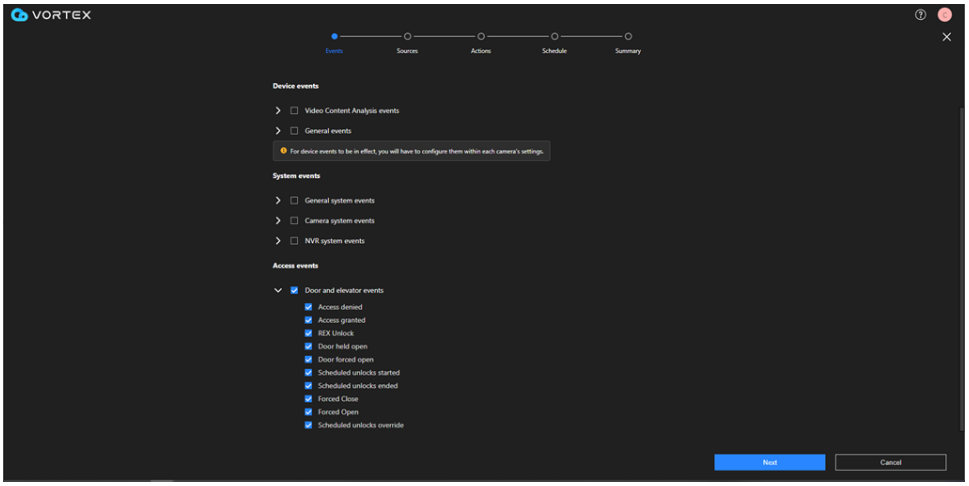


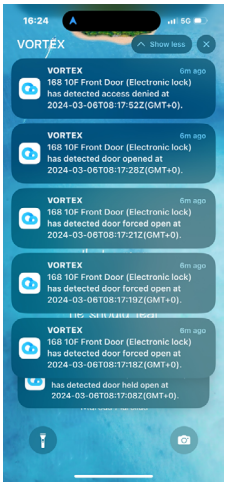


Alarm settingsand Real-time Notification

Goal

Allow Owner/Administrators to set alarms for Access events in Alarm Management, allowing designated personnel to receive real-time push notifications and email notifications.

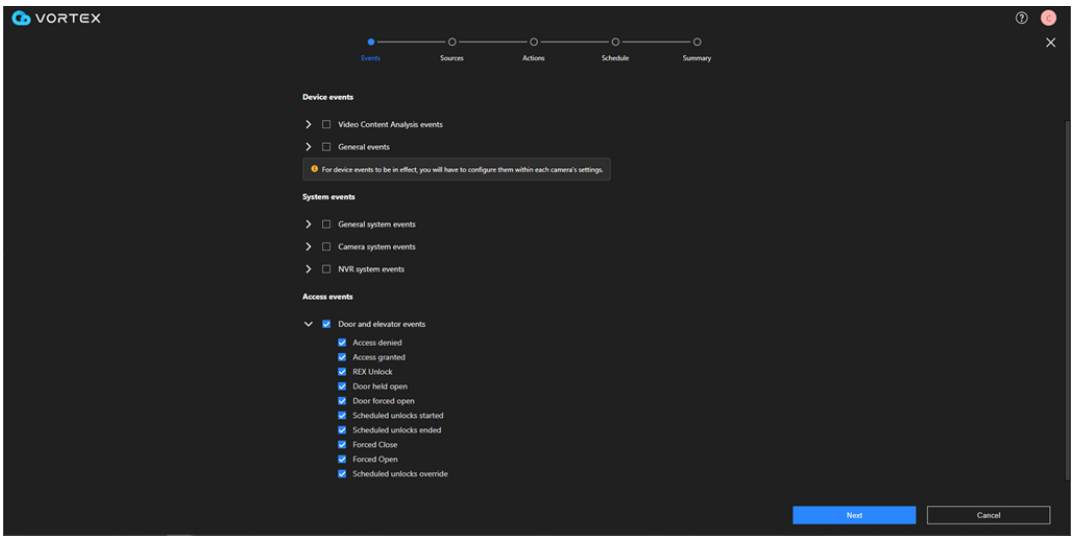




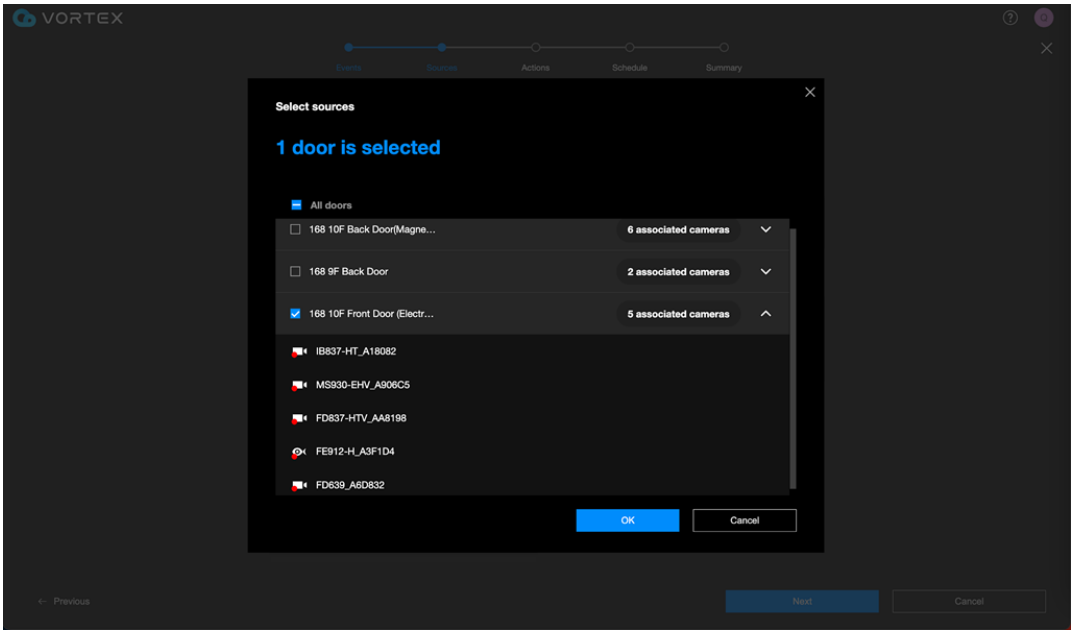
Web Portal

1. Go to System > Alarm Management > Add alarm
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Access event.

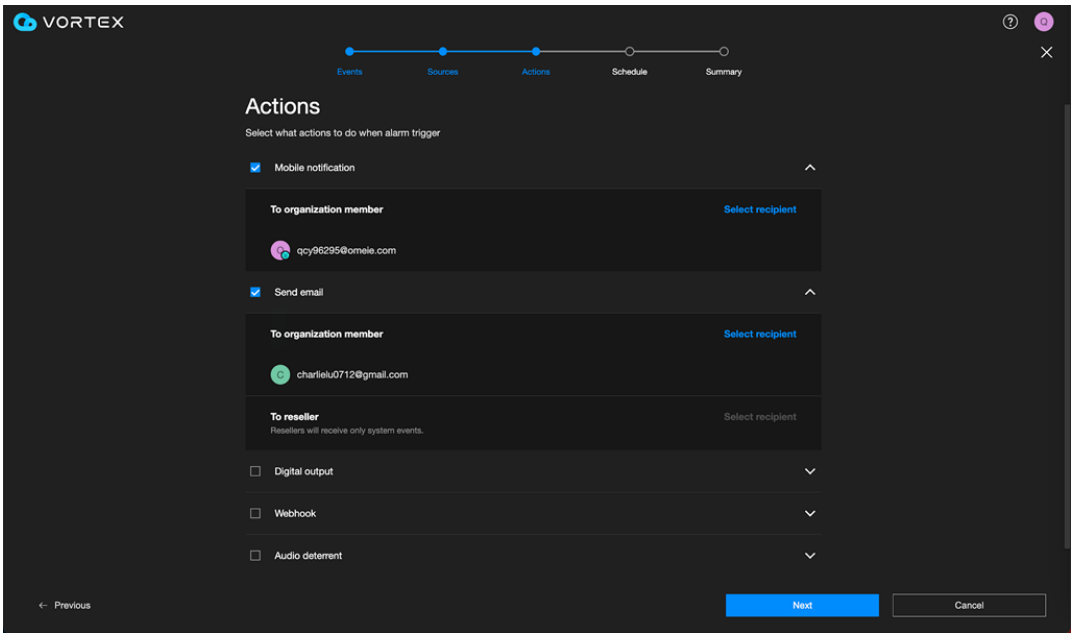
- Users who are not integrated with Access Control will still see the Access events option on this page; however, no alarms will be generated upon setting completion (currently, Alarm Management's design does not display the supportable events based on the type of device a user has).



2. In the next step - Sources, select the doors that initiate Access events.
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Sources for the Door.
   - Only doors that are already associated with cameras will appear in this list.
   - Click the expand button to view the cameras associated with this door.



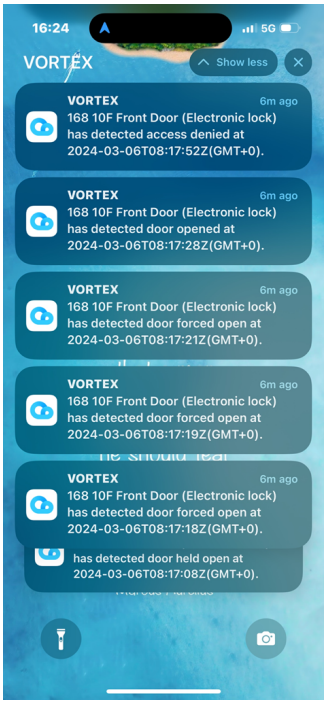
3. In the next step - Actions, select the actions and designated personnel to receive notification.
   - The design logic here is the same as the existing Alarm Management.
   - Access events only support Mobile notification and Send emails. Other Actions are not supported.
   - The remaining steps, Schedule and Summary, follow the same design logic and operate in the same manner as they currently do.

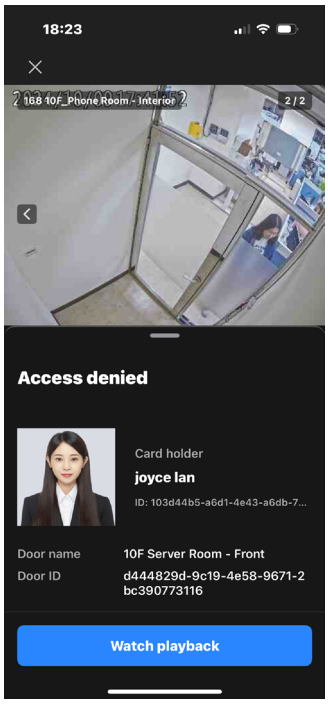


Mobile App

Designated personnel received real-time push notification.

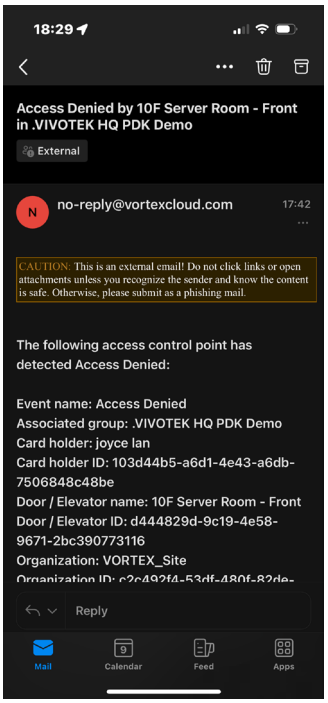
- Access events that may result in a continuous state will only trigger an alarm notification the first time they occur, such as 'Door held open' and 'Door forced open'.

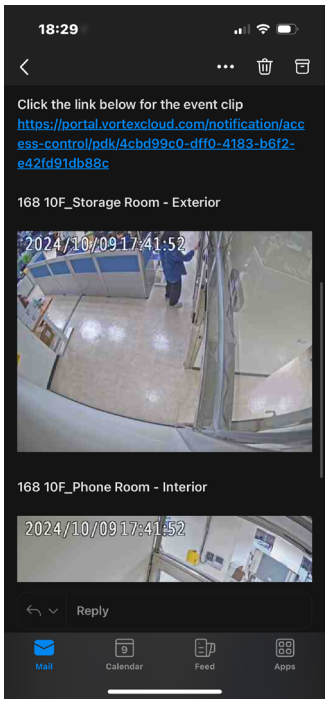




Designated personnel received email notification.

- If a door is associated with multiple cameras, the email will display snapshots from these cameras.

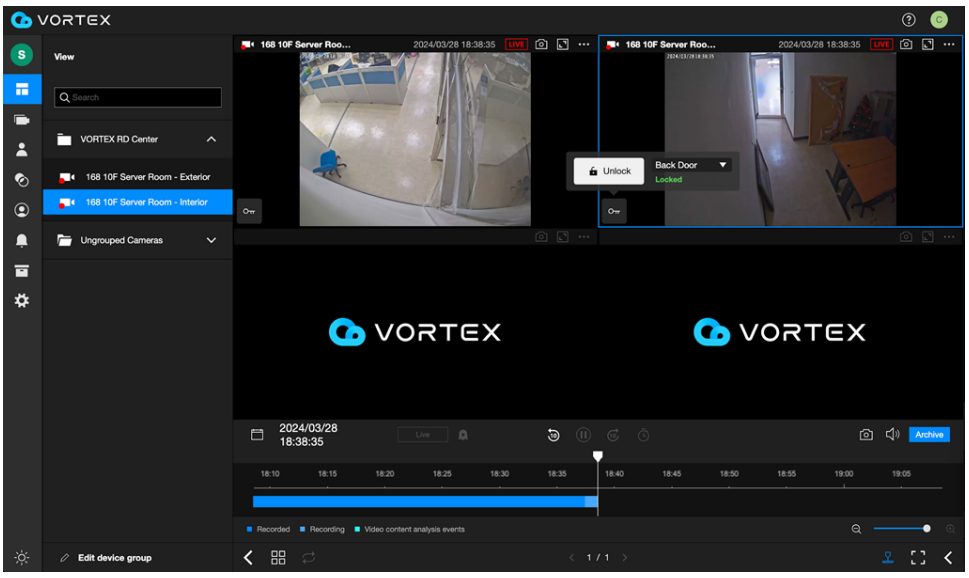


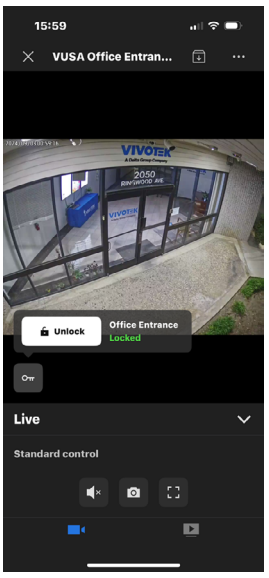


Remote Unlock/Lock Doors

Goal

Allow owner/admin/supervisor to assist with daily access needs remotely and manage doors during emergency situations without having to be physically present on-site.

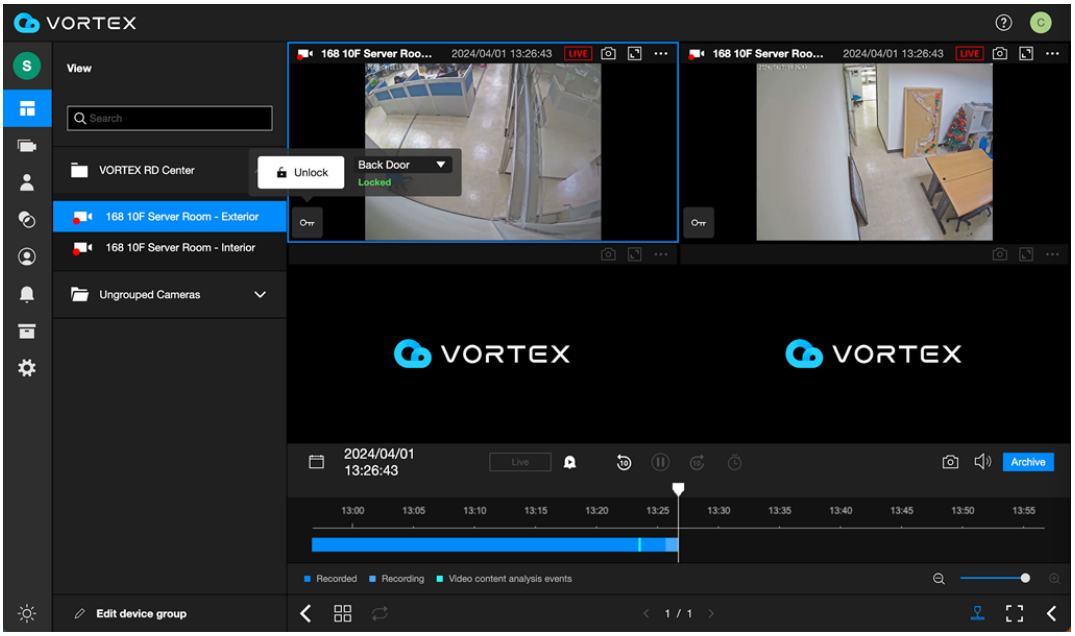




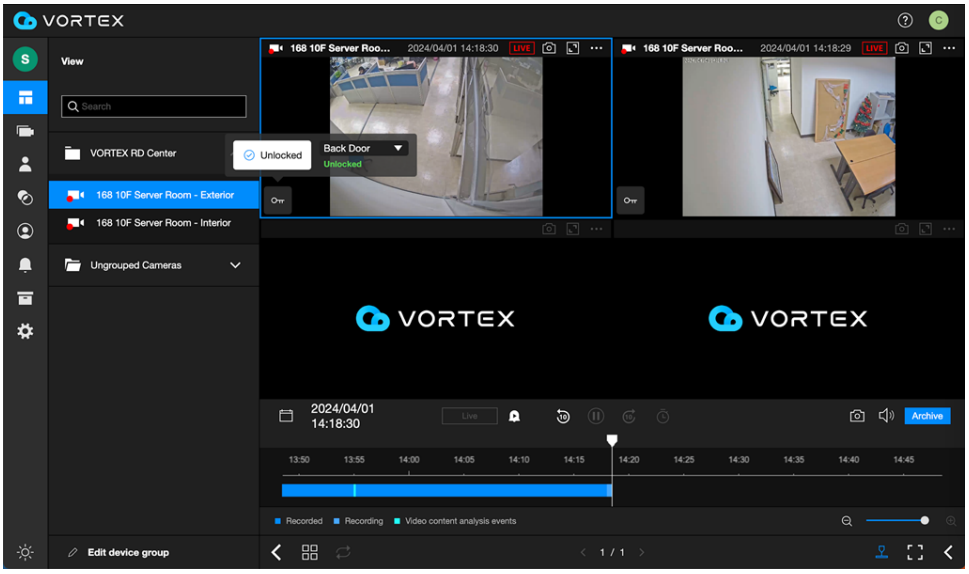
Web Portal

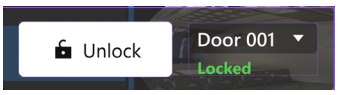
1. Go to Live View. Cameras that have been associated with doors display “key icon” on respectively view cell.
   - When this camera is associated with multiple doors, a dropdown will appear to select a specific door.
   - The order of Doors within the dropdown is sorted by ASCII.

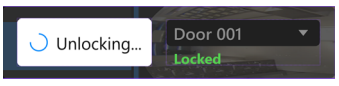
- There are 4 Door statuses:
  1. Locked
  2. Unlocked
  3. Force Close
  4. Disconnection
- If this Door is in Force Close or Disconnection status, the Remote unlock/lock will not be possible (the button will be disabled).

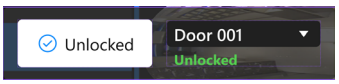


2. Click on the unlock/lock button on the door you wish to operate the remote door management.
   - If the door is in a locked status, the button will display 'Unlock'. Conversely, if the door is in an unlocked status, the button will display 'Lock'.
   - After clicking the unlock or lock button, an UI effect will be displayed.



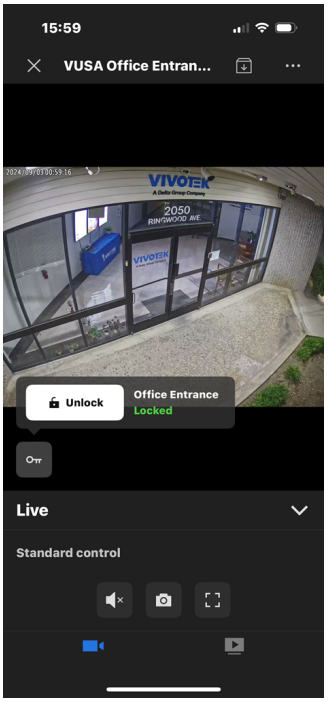


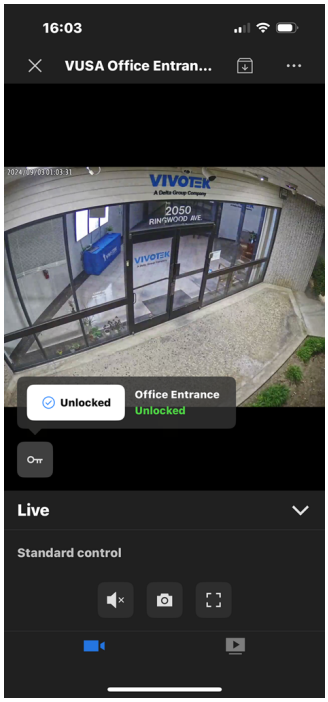




Mobile App

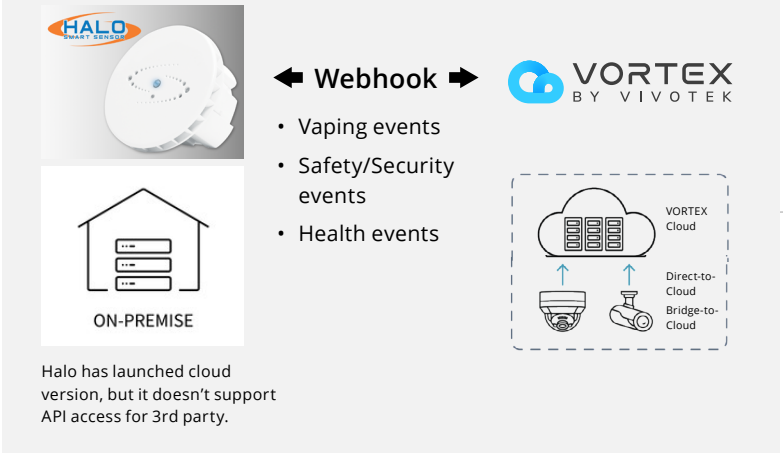
1. Go to Live View. Cameras that have been associated with door(s) would display a key icon. Click “Unlock” or “Lock”.
   - There are 4 Door statuses:
     1. Locked
     2. Unlocked
     3. Force Close
     4. Disconnection
   - If this Door is in Force Close or Disconnection status, the Remote unlock/lock will not be possible (the button will be disabled).
   - If the door is in a locked status, the button will display 'Unlock'. Conversely, if the door is in an unlocked status, the button will display 'Lock’.



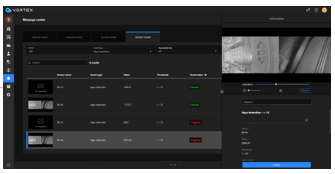


Smart Sensor Integration – Halo

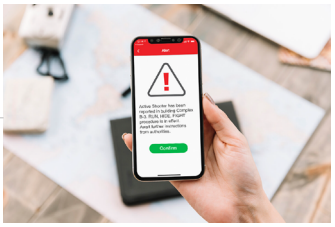
System Overview



- **Sensor Events Integration with Camera Videos**



- **Real-time Sensor Event Notification**

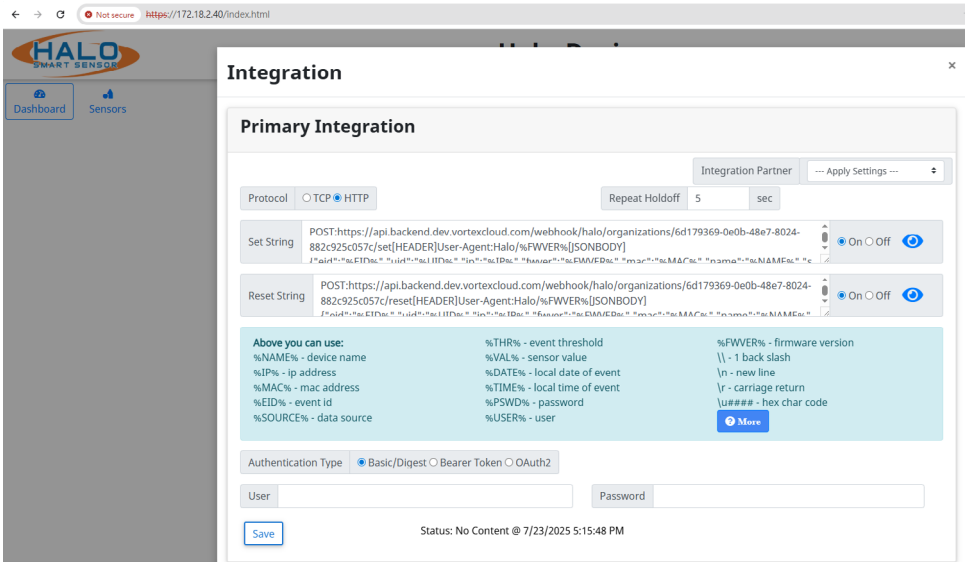


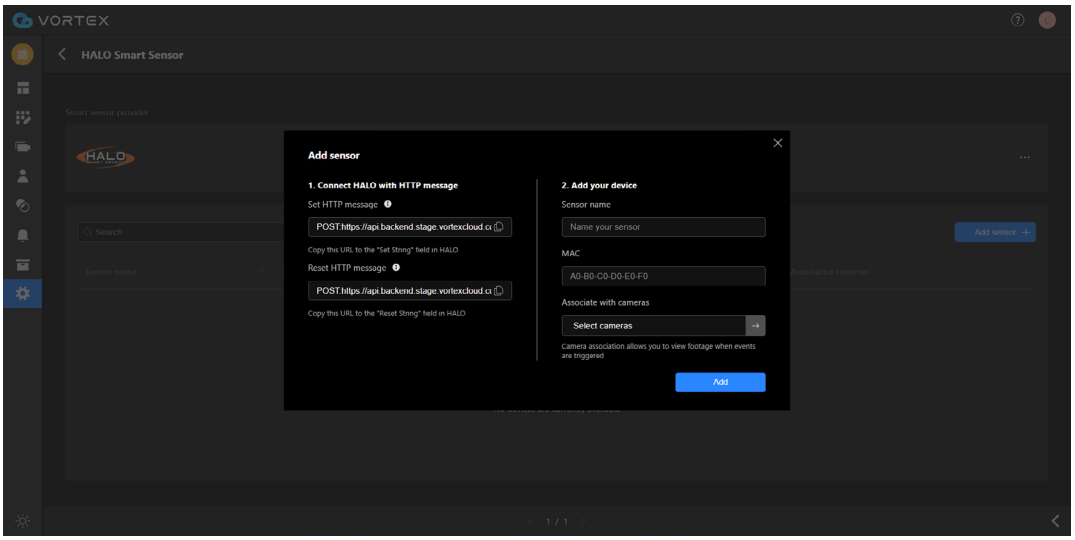
- **Trigger-Action Automation**

Integration Setup

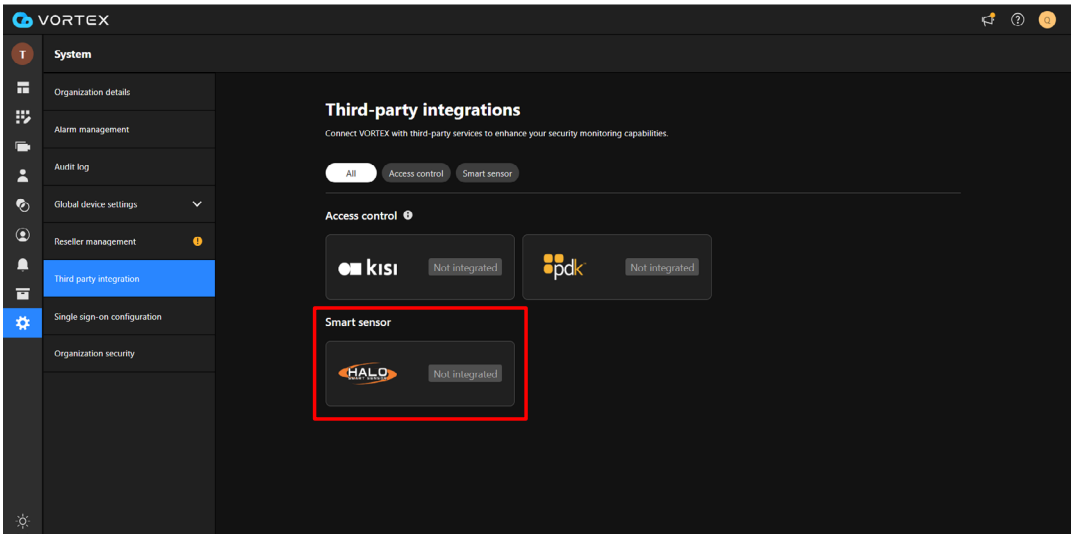
Goal

Enable VORTEX to retrieve sensor events from Halo's webhook (a method to automatically send event data to VORTEX in real time via a HTTP message.)

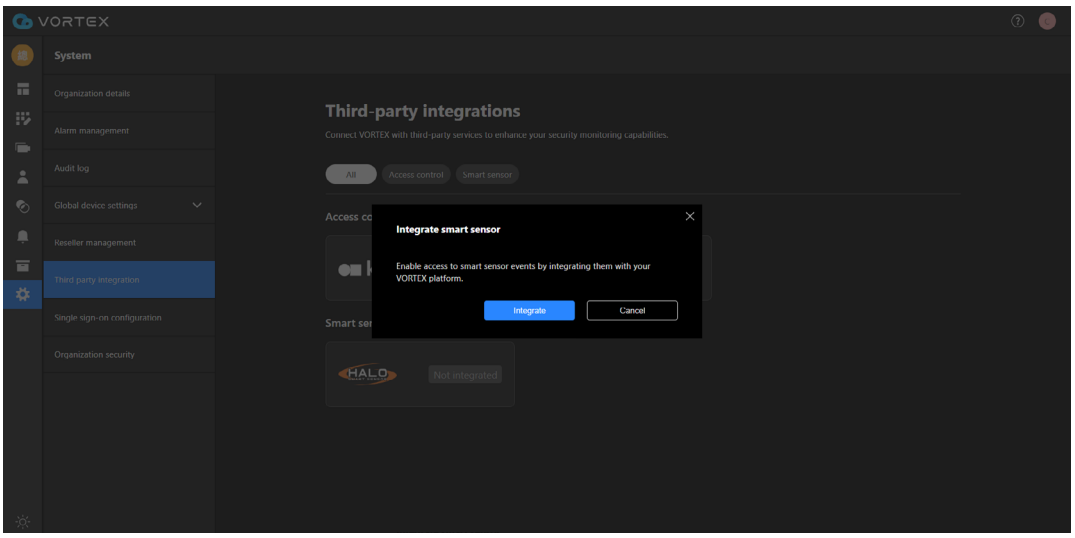




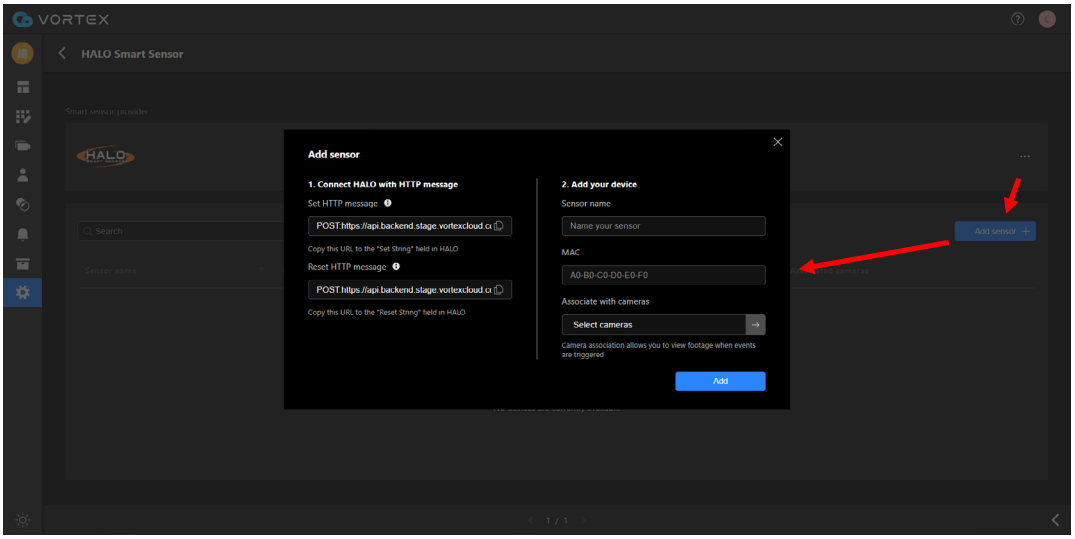
1. Go to System > Third party integration and select Halo Smart Sensor.



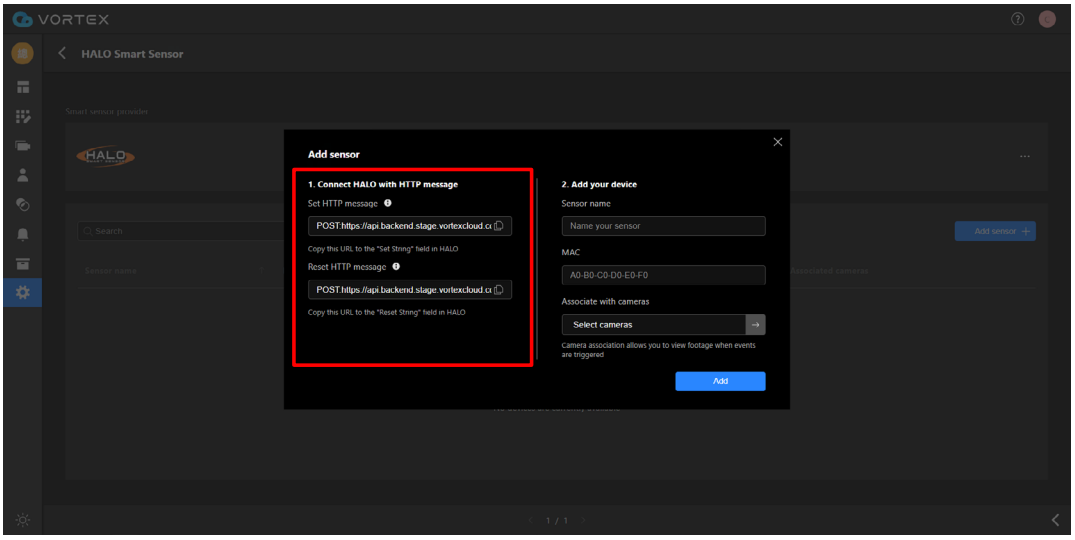
2. Click Integrate. and it will take you directly to the configuration page.



3. Click Add sensor button to open the configuration window.



4. Copy and paste the two HTTP messages into the 'Set String' and 'Reset String' fields in HALO to configure the sensor to send data to VORTEX.
   - Set HTTP message: VORTEX receives a triggered event when the threshold condition is met.
   - Reset HTTP message: VORTEX receives a cleared event when the threshold condition is no longer met.

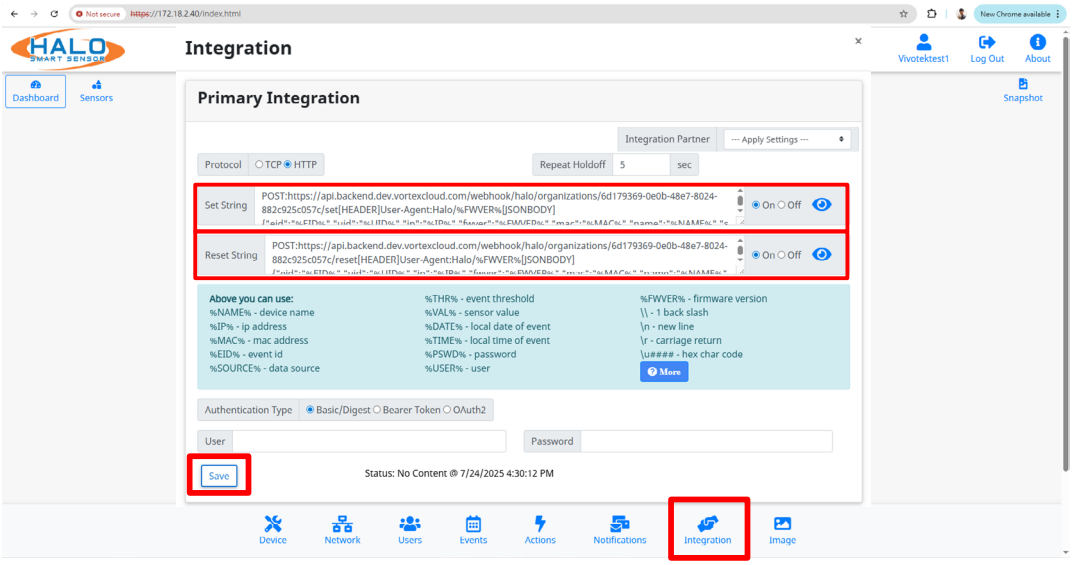


What is the HTTP message?

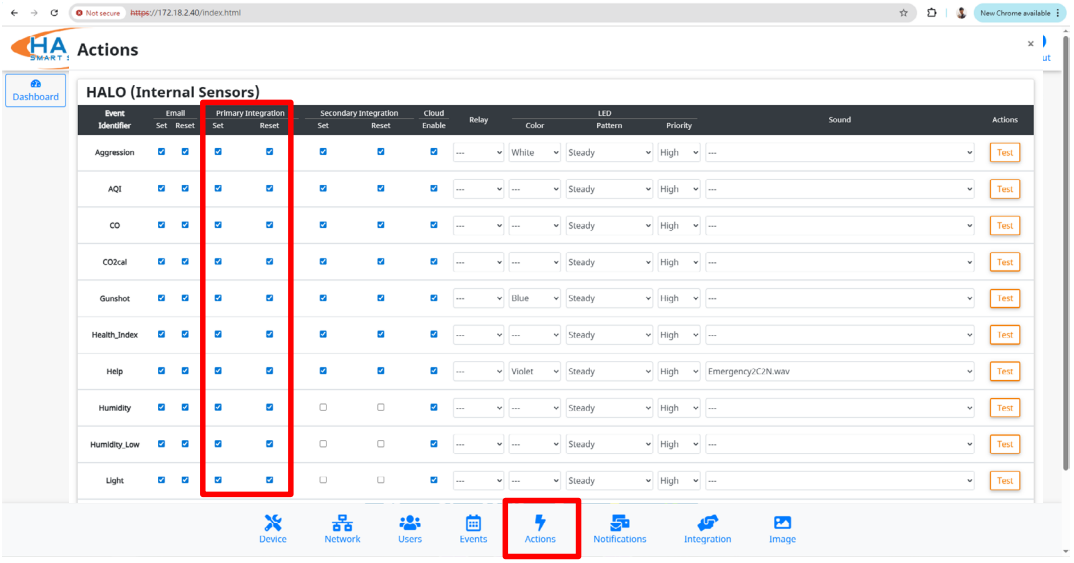
To integrate your HALO smart sensor with VORTEX, you need to configure the HTTP message settings. This will allow HALO to push sensor event data to VORTEX in real-time via a webhook.

A webhook is a mechanism that allows one system (HALO) to automatically send data to another system (VORTEX) when specific events occur. Instead of waiting for VORTEX to request data, HALO pushes the sensor events directly to VORTEX using an HTTP message.

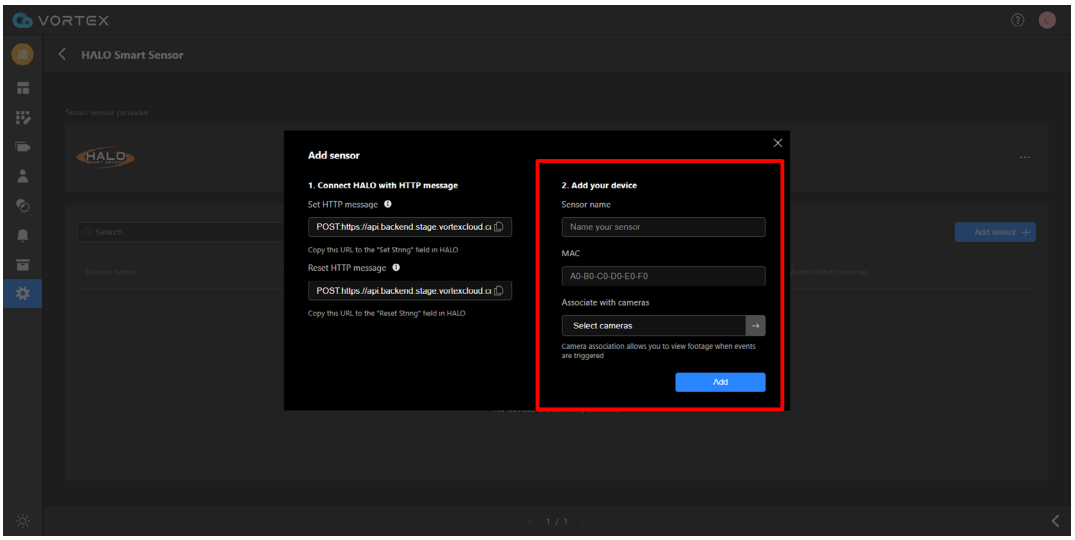
4. Copy and paste the two HTTP messages into the 'Set String' and 'Reset String' fields in HALO to configure the sensor to send data to VORTEX.
   4.1. Log in to your Halo device and click Integration.
   4.2. Paste VORTEX Set HTTP message into the Set String field in HALO and select the ‘On’ checkbox.
   4.3. Paste VORTEX Reset HTTP message into Reset String field in HALO and select the ‘On’ checkbox.
   4.4. Click Save. (Not necessary to adjust other settings.)



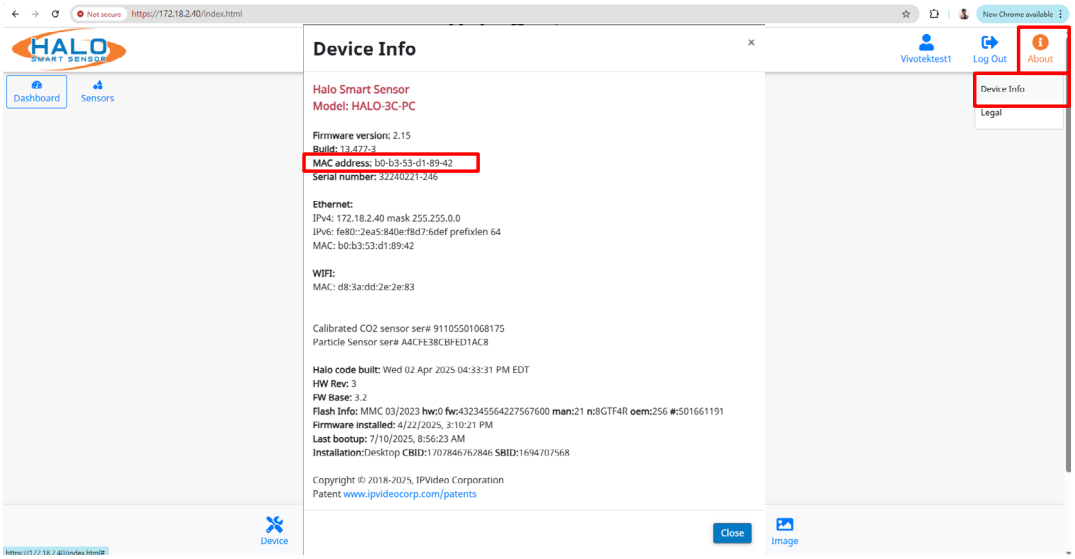
   4.5. Click Actions and ensure that the checkboxes for Set and Reset under Primary Integration for each Event Identifier are selected.



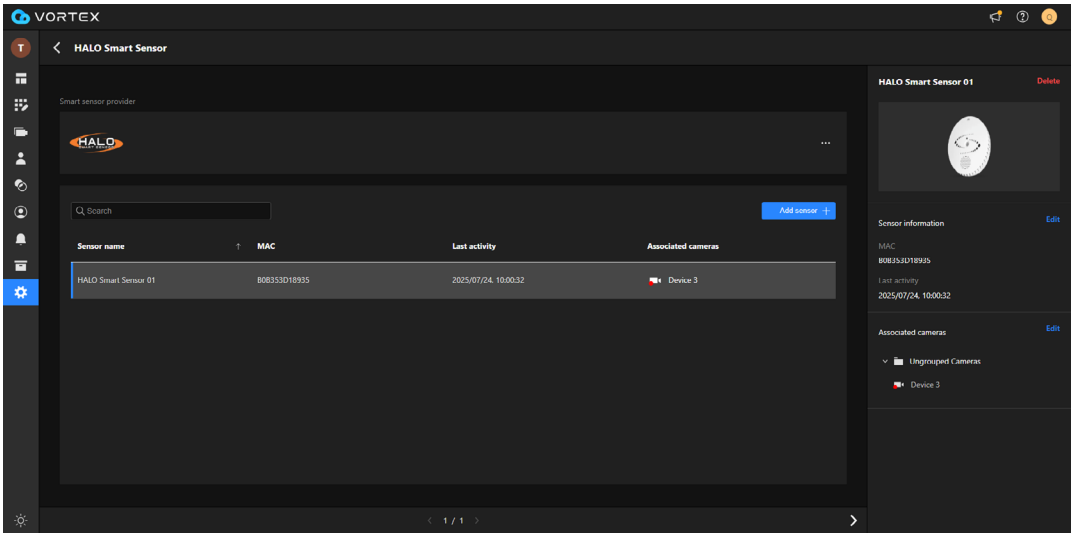
5. Add the HALO Smart Sensor device to VORTEX:
   - Sensor name: Name your sensor (this will not overwrite the original name of the HALO device).
   - MAC: Enter the MAC address of your HALO Smart Sensor.
   - Associate with cameras: Camera association allows you to view footage when events are triggered.
     - Many-to-many design: A sensor can be associated with up to 10 cameras. The same camera can be associated with multiple different HALO Smart Sensors at the same time.



You can find the MAC address of your HALO Smart Sensor here:

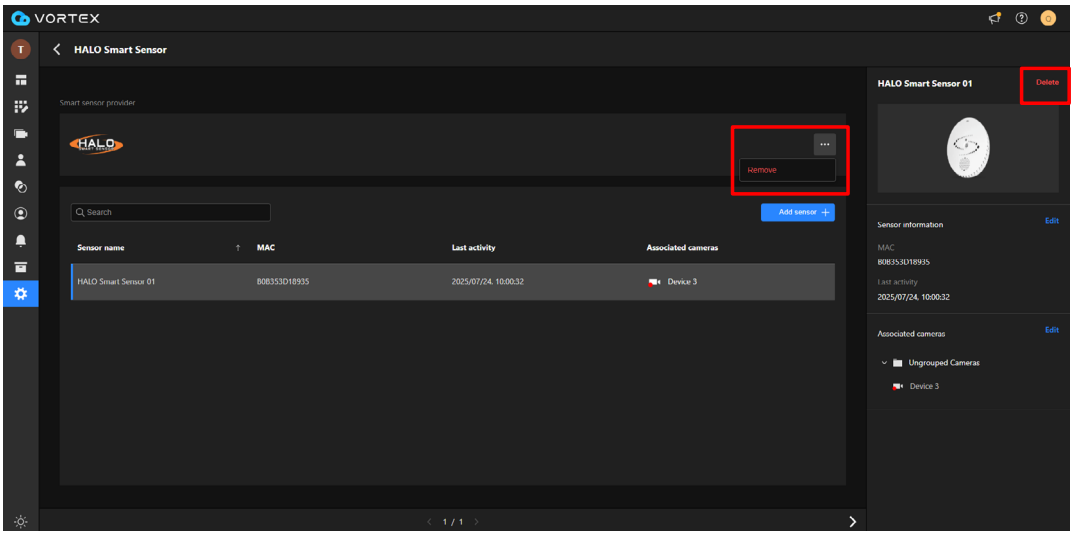


After successfully adding the HALO Smart Sensor to VORTEX, you will see the information you just configured displayed on the page.



When there is a need to remove HALO from the VORTEX integration, there are two methods:

- Remove all HALO smart sensors integrated with VORTEX at once, along with the sensor event history stored in the message center for all sensors.
- Remove a single HALO Smart Sensor, along with the sensor event history stored in the message center for that specific device.



Sensor Events Integration with Camera Videos

Goal

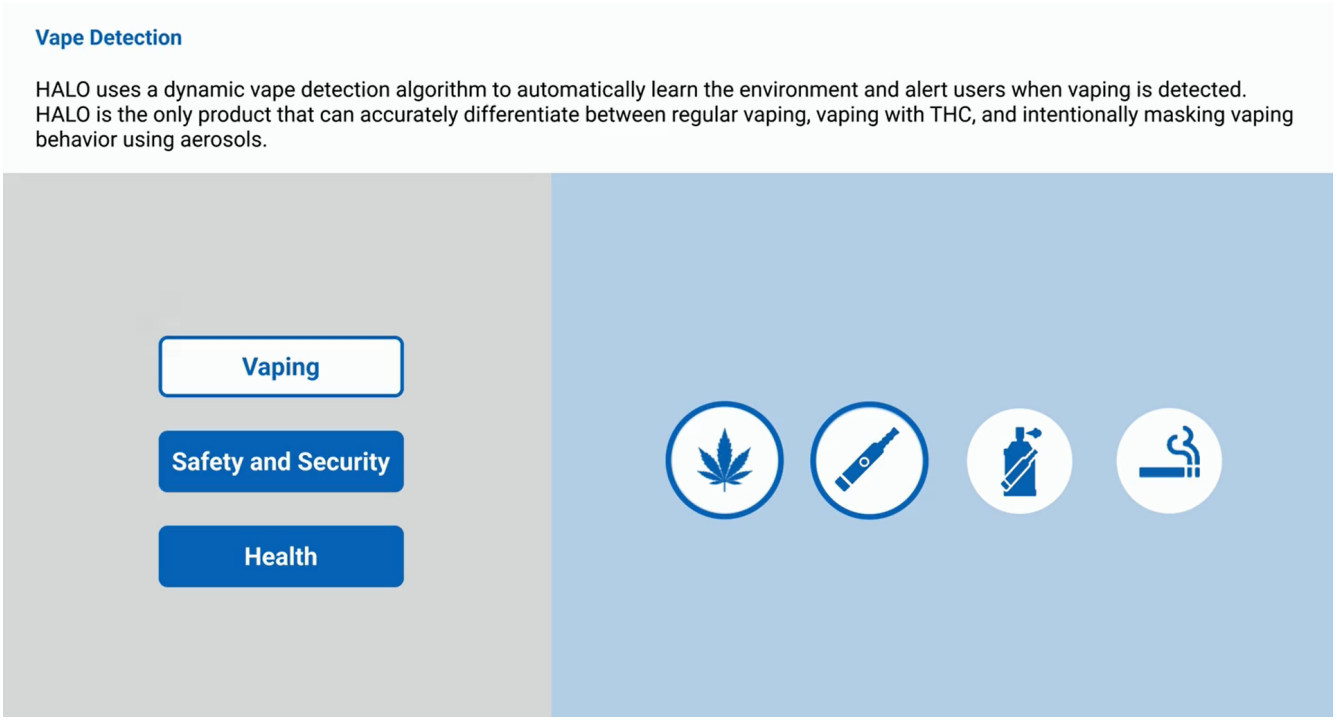
- Allow users to access an instant and comprehensive view of integrated info. from both systems.
- Allow users to use camera video footage as evidence to respond to sensor events.

Supported Event Type

- All the HALO senor events are supported by VORTEX. (Currently 26 event types in total.)
- HALO categorizes them into the following three main categories.

Vaping	Safety and Security	Health
• Vape detection • THC detection • Smoking detection • Air masking detection	• Help sounds • Aggression sounds • Gunshot detection • Loud sound • Motion detection • High occupancy count • Light level • Panic button • Device tamper	• Temperature • Humidity • Health index • Air quality index • CO • CO2 • TVOC • PM1 • PM10 • PM2.5 • NO2 • NH3 • Pressure

Vaping Events

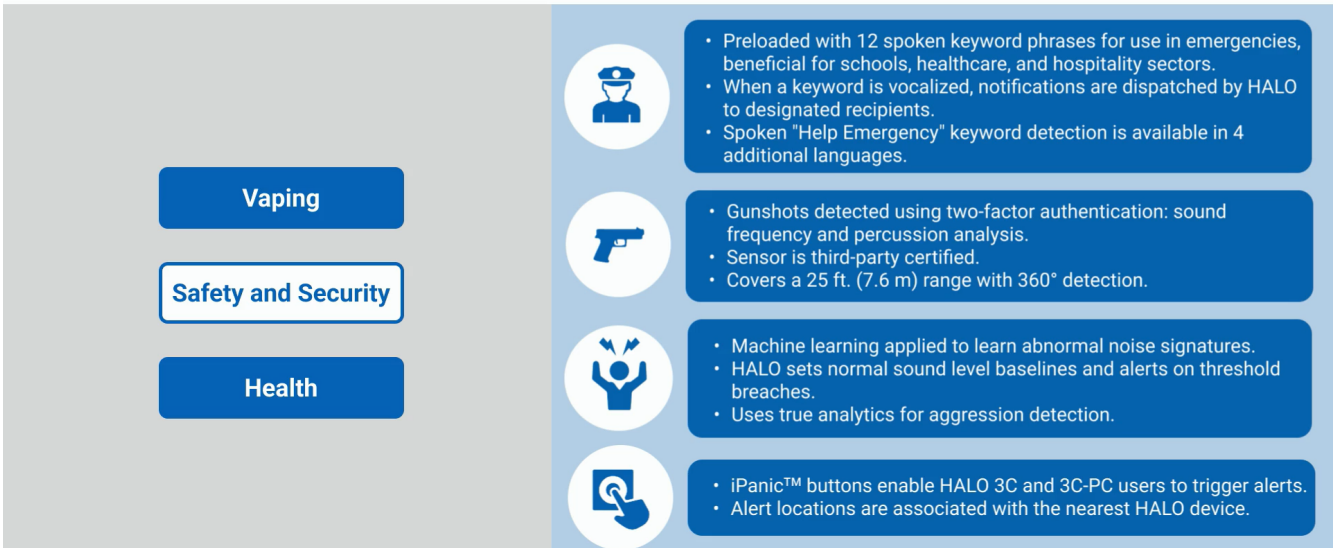


Event Group	Halo Event Name	VORTEX Event Name	Description
Vaping	Vape	Vape detection	HALO uses a Dynamic Vape Detection algorithm to automatically learn the environment and alert when Vaping is detected. HALO is the only product that can alert and differentiate between Vaping, Vaping with THC, and intentionally masking Vaping behavior by using aerosols to cover up Vaping
	THC	THC detection	MARIJUANA (THC) is the chemical component found in marijuana. The HALO Smart Sensor is the only sensor that is able to trace THC oil given off by vape pens, along with the other traditional smoking methods.
	Smoking	Smoking detection	PM10 (µm particulates).
	Masking	Air masking detection	This is when someone is trying to hide their vaping activity – they will typically spray cologne or other aerosols

Safety and Security Events

Safety and Security

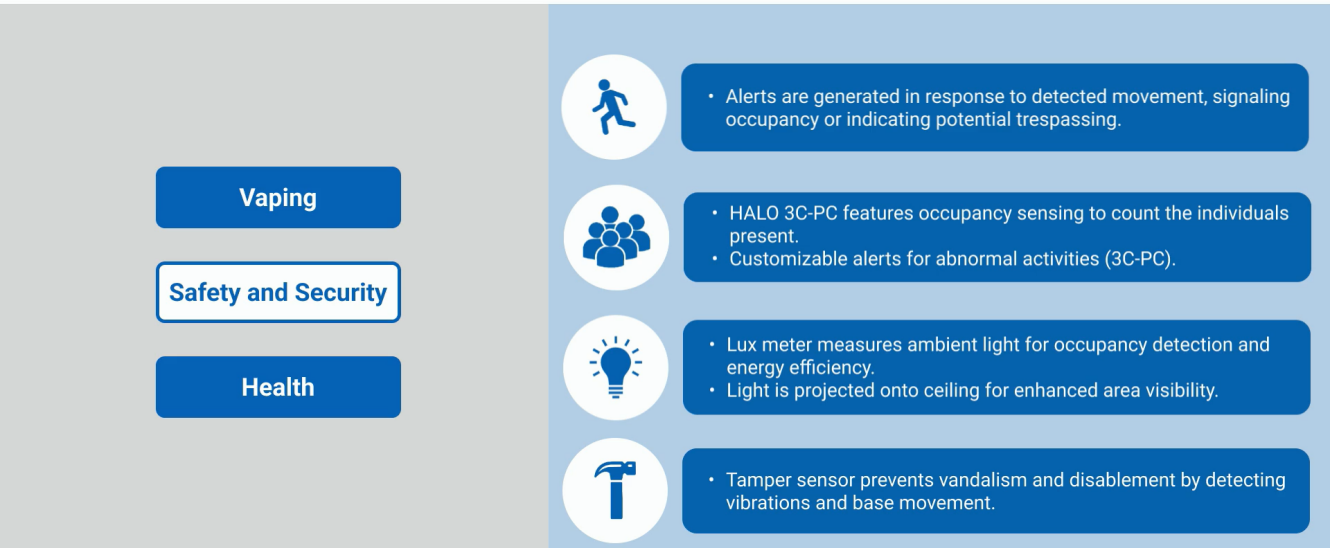
Safety and security events are set up to detect spoken keywords, gunshots, bullying and the signals from iPanic™ buttons. These events usually require immediate attention.



Event Group	Halo Event Name	VORTEX Event Name	Description
Safety and Security	Help	Help sounds	HELP (SPOKEN KEYWORD) - Each HALO device comes preloaded with 5 spoken keyword phrases. These keywords can be used by anyone in times of stress or need. This is especially helpful in schools where bullying is a problem, teachers who are in need of assistance, nurses and hospital patients, hotel personal, etc. Whenever the keyword is said aloud, HALO will send notifications to those who have been designated to receive these alerts.
	Gunshot	Gunshot detection	Identify gunshots and the location with two-factor authentication using frequency sound pattern and percussion. This sensor is 3rd party certified. Each device has a 25 ft range with 360° radius detection.
	Aggression	Aggression sounds	Learns the signature of abnormal noise in a room by applying Machine Learning. HALO learns what normal sound levels are and alerts when a threshold above normal is detected for a specified length of time. HALO applies aggression detection through true analytics.
	Panic	Panic button	HALO 3C users can trigger alerts via an external 3rd party panic button or via the HALO cloud app. The location of the trigger is associated to the HALO device in closest proximity

Safety and Security

Motion sensing, people counting, light levels, and tamper events provide valuable insights when conditions deviate from the norm. For example, detecting motion and lights at 2 AM indicates that someone is occupying the space when no one should be there.

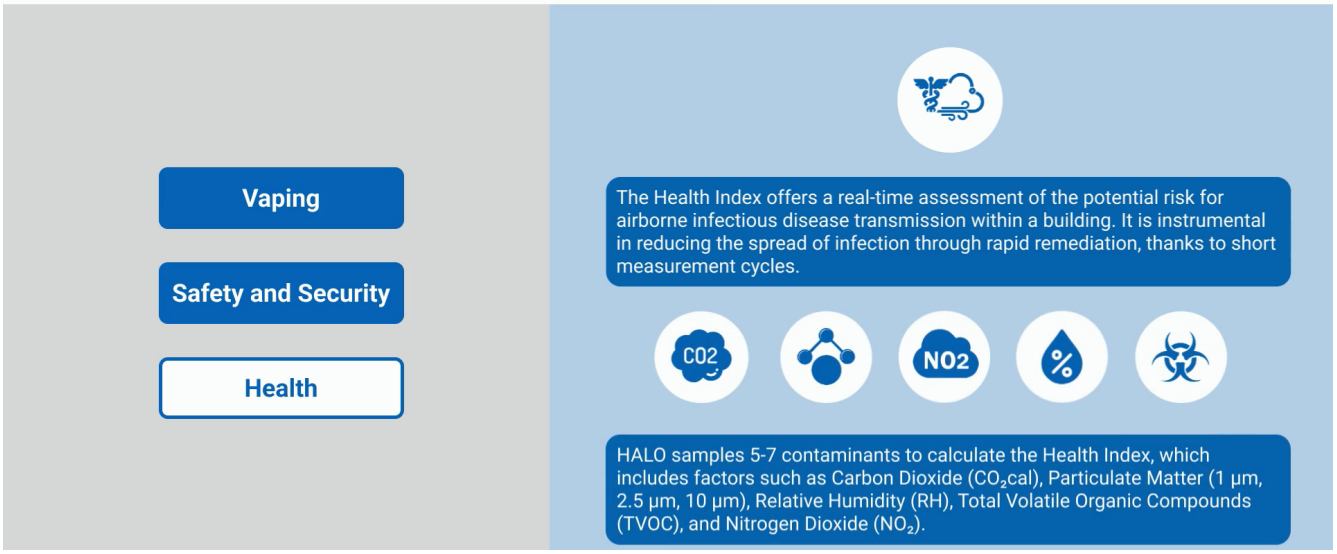


Event Group	Halo Event Name	VORTEX Event Name	Description
Safety and Security	Motion	Motion detection	Identify and alert on movement for occupancy and trespassing.
	Occupancy	High occupancy Count	Identify how many people are within the HALO location and configure to alert on abnormalities.
	Light	Light level	Measured in Lux, HALO can identify the light level in a particular location. This can be helpful when detecting occupancy, improving emergency efficiency, and coupling with other sensors to identify an intrusion. HALO 3C comes with a literal HALO of LED-colored lighting options that can be programmed to show escape routes for safety such as a red, yellow, and green pattern. Create unique colors for different alerts such as purple for Air Quality alerts or blue for Health alerts. The lights themselves are projected onto the ceiling around the HALO for extended visibility
	Tamper	Device tamper	HALO uses a tamper sensor to prevent vandalism and disabling of the HALO by identifying vibrations caused by striking the HALO, throwing things at it, or even moving the ceiling tile HALO is mounted in.

Health

Health Index

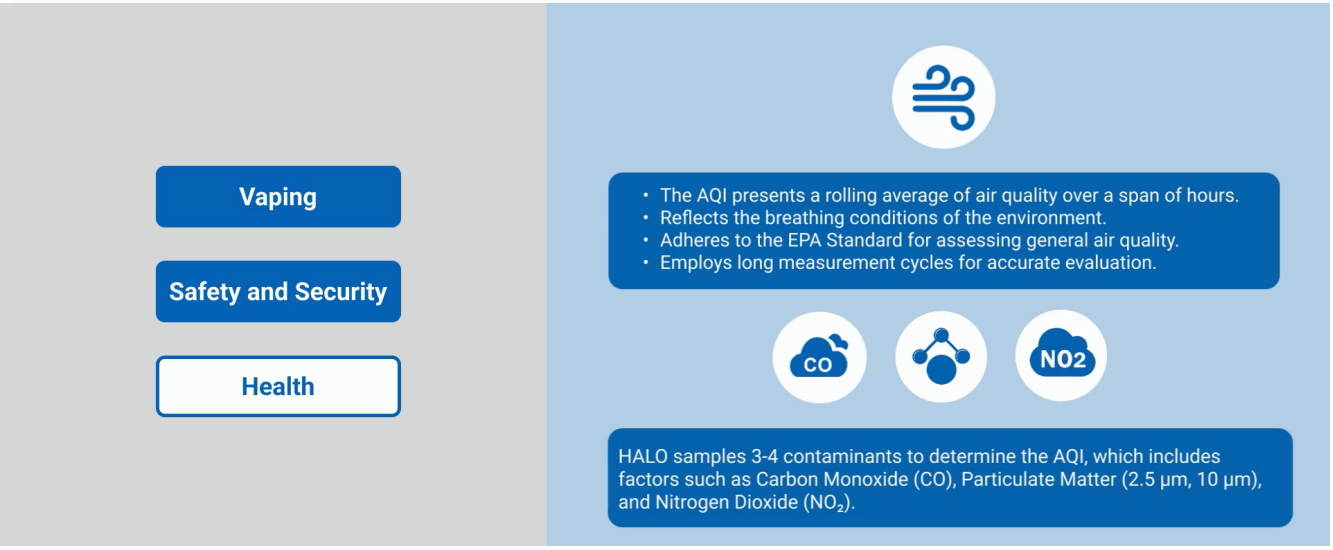
The Health Index comprises 5 to 7 sensors that show the transmissibility of viral diseases in real-time, based on CDC standards.



Event Group	Halo Event Name	VORTEX Event Name	Description
Health	Temp_C	Temperature	These levels can affect more than your comfort. High temperatures and excessive humidity promote mold and mildew growth. These can cause structural damage to your workplace and cause allergy-like symptoms in those with sensitivities. Monitoring these levels can help you prevent facility and health problems and tip you off to potential sources like structural weaknesses and leaks.
	Temp_C_Low	Temperature	
	Temp_F	Temperature	
	Temp_F_Low	Temperature	
	Humidity	Humidity	
	Humidity_Low	Humidity	
	Health_Index	Health index	Health Index provides a real-time indication of the potential risk for the spread of airborne infectious disease in a building. Used to Reduce the Spread of Infection. Short Measurement Cycles for Fast Remediation. Number of Contaminants Sampled in HALO: 6-7. Health Index Factors: Carbon Dioxide (CO_2) • Particulate Matter (1 µm, 2.5 µm, 10 µm) • Humidity (RH) • Volatile Organic Compounds (VOC) • Nitrogen Dioxide (NO_2)

Air Quality Index

The Air Quality Index (AQI) uses 3 to 4 sensors, averaged over 24 hours, to determine if contaminants threaten air quality according to EPA standards.

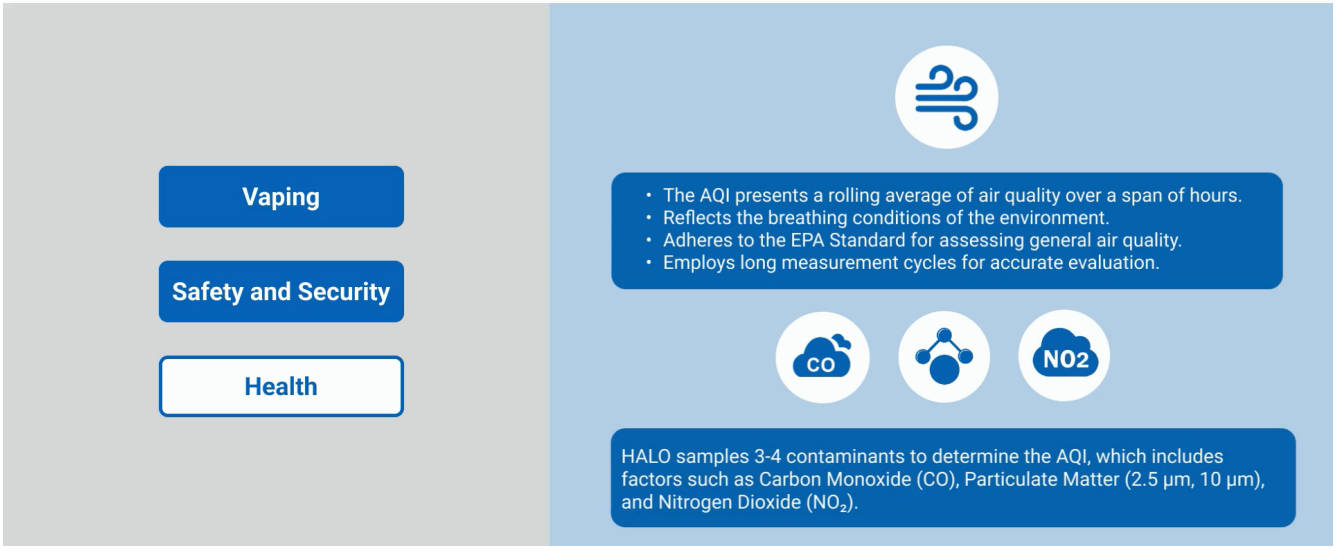


Event Group	Halo Event Name	VORTEX Event Name	Description
Health	AQI	Air quality index	Air Quality Index provides a rolling average of the quality of the air you are breathing over the course of a few hours. The standard for EPA to Measure Air Quality. Long Measurement Cycles for General Air Quality. Number of Contaminants Sampled in HALO: 4-5. Air Quality Index Factors: Particulate Matter (2.5 µm, 10 µm) • Carbon Monoxide (CO) • Nitrogen Dioxide (NO_2)
	CO	CO	By now, most people are aware of the deadly effects of high concentrations of this odorless, colorless gas. Exposure to lower levels sometimes given off by fuel burning appliances can also cause adverse reactions, including confusion and memory loss.
	CO2cal	CO2	While the effects of high levels of CO2 were long thought to be benign, research has found that concentrations as low as 1,000 ppm can affect people's cognitive function and decision-making performance. The greatest source of indoor CO2 is people themselves, as it's a byproduct of our respiratory function. Coupled with poor ventilation, this commonly leads to high levels of CO2 in many workplaces.

Health	TVOC	TVOC	The acronym stands for volatile organic compounds, gases emitted from a variety of materials that can have short- and long-term health effects. Concentrations of many VOCs can be up to 10 times higher indoors than outdoors. Sources of VOCs include many common products, including cleaning fluids, disinfectants, paints, and varnishes. Burning fuels like wood and natural gas also produce VOCs. Short-term exposure to low levels of VOCs can cause throat irritation, nausea, fatigue, and other minor complaints. Long-term exposure to high concentrations of VOCs has been linked to more severe respiratory irritation as well as liver and kidney damage. Products can emit VOCs even when they're in storage, though to a lesser extent than when they're actively being used.

Air Quality Index

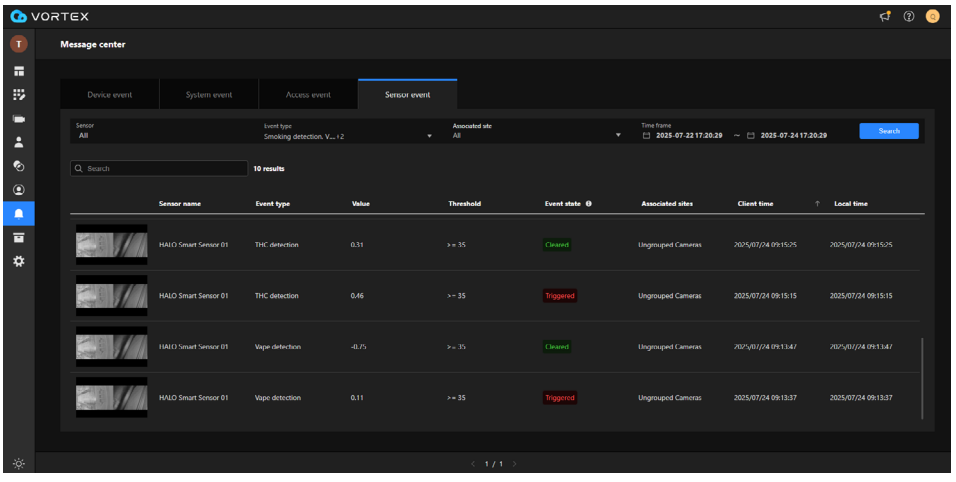
The Air Quality Index (AQI) uses 3 to 4 sensors, averaged over 24 hours, to determine if contaminants threaten air quality according to EPA standards.



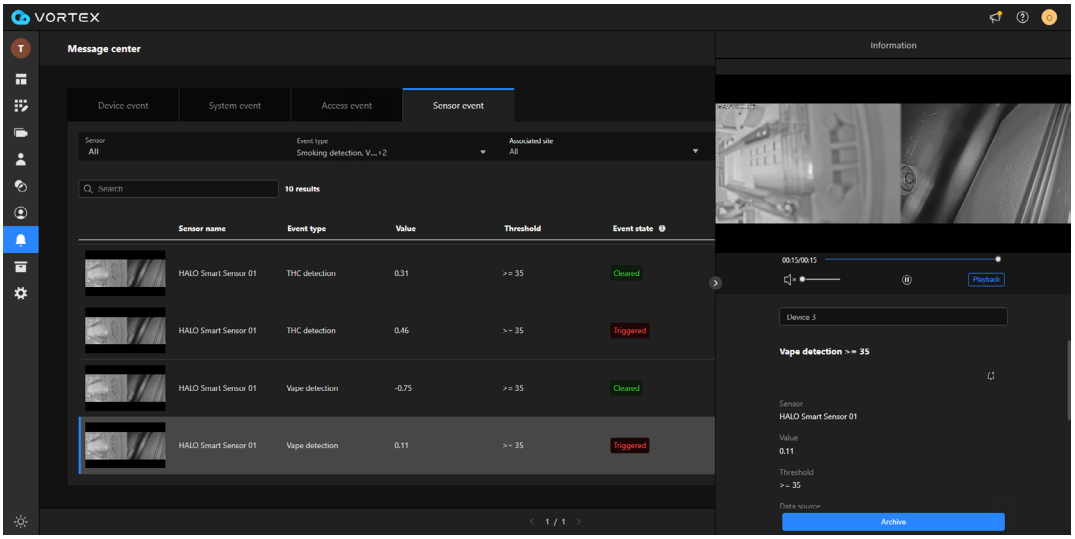
Event Group	Halo Event Name	VORTEX Event Name	Description
Health	PM1	PM1	Particulate matter, or PM, is a mix of particles and droplets in the air. PM varies in shape and size, but those of 10 micrometers in diameter or smaller can adversely affect your health because they can be inhaled. PM 2.5 refers to fine particulate matter – with a diameter of two-and-one-half microns or less. Sufficient exposure to PM can irritate the eyes, nose, throat, and lungs, leading to allergy-like symptoms and shortness of breath in otherwise healthy people. It can also exacerbate existing medical problems, such as asthma and heart disease. PM 2.5 is considered the world's single biggest environmental health risk. Indoor PM levels can be influenced by outdoor sources like vehicle exhaust, wildfires, and power plant emissions. But many indoor activities produce PM as well: cooking, burning fireplaces, and smoking are just a few common sources..
	PM10	PM10	
	PM2.5	PM2.5	
	NO2	NO2	NO2 ppb.
	NH3	NH3	Ammonia ppm.
	Pressure	Pressure	Pressure (hPa).

View Sensor event in Message Center

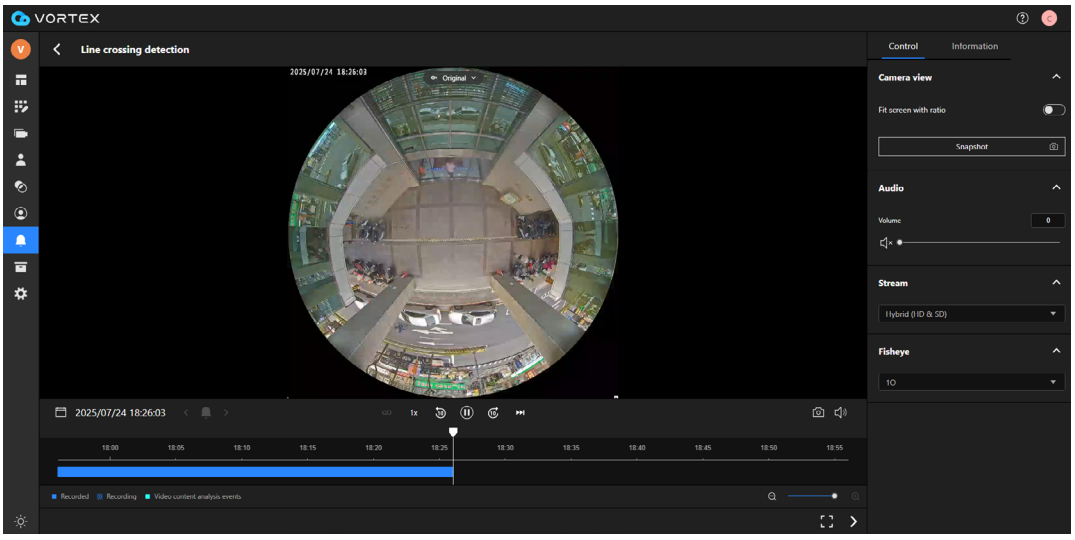
1. Go to the Message Center and select the 'Sensor Event' tab. You can search for the event types you want to view, filter by the associated sites, and adjust the time range by setting the filter criteria. You can also further narrow your search by using the search box to find specific event values or thresholds.
   - Each event has an event state, which can be one of the following two statuses:
     - **Triggered:** The threshold conditions have been met.
     - **Cleared:** The threshold conditions are no longer met.
   - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with extended access dependent on the cloud backup plan purchased by the end-user.

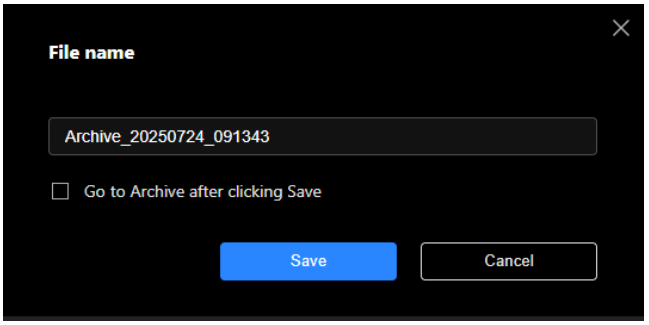


2. Select an sensor event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
   - If this sensor is linked to multiple cameras, you can choose a specific camera through the dropdown options below the footage.



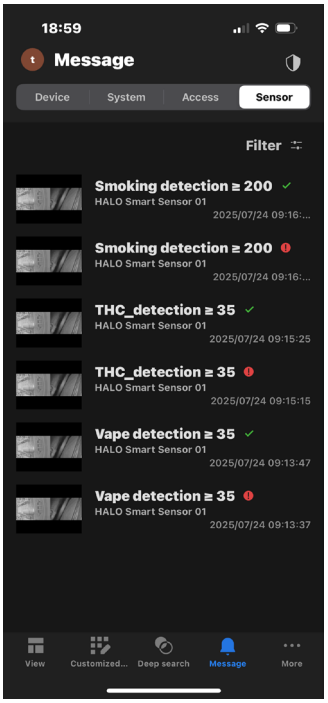
3. You can view the footage through playback, or archive this event footage and sharing with others.

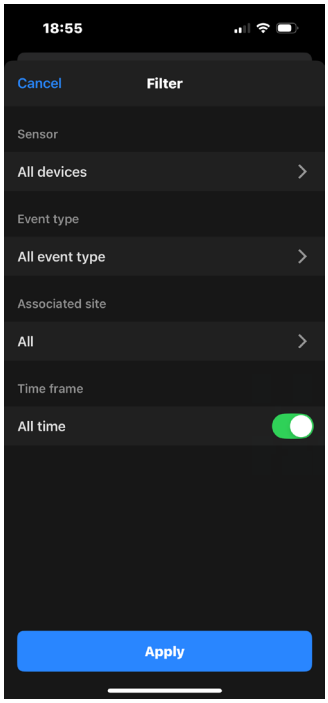




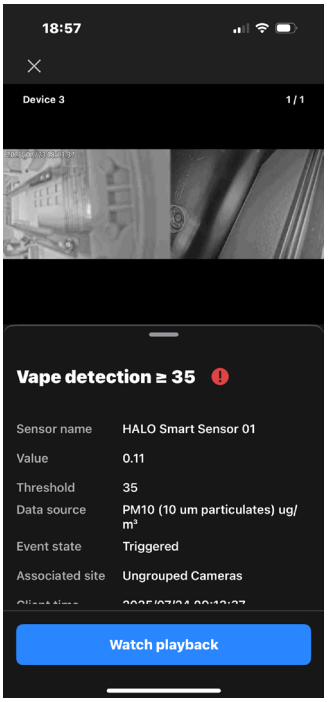
Mobile App

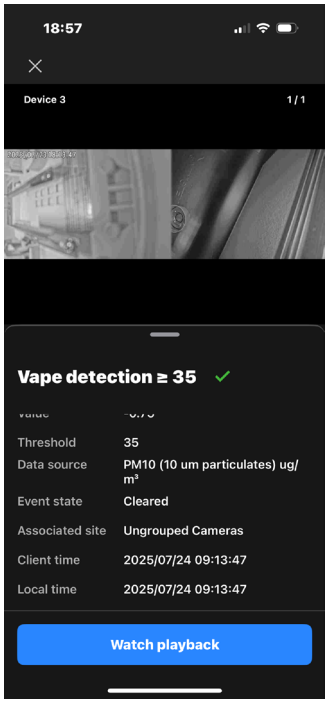
1. Go to the Message Center and select the 'Sensor Event' tab. You can search for the event types you want to view, filter by the associated sites, and adjust the time range by setting the filter criteria.
   - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with extended access dependent on the cloud backup plan purchased by the end-user.



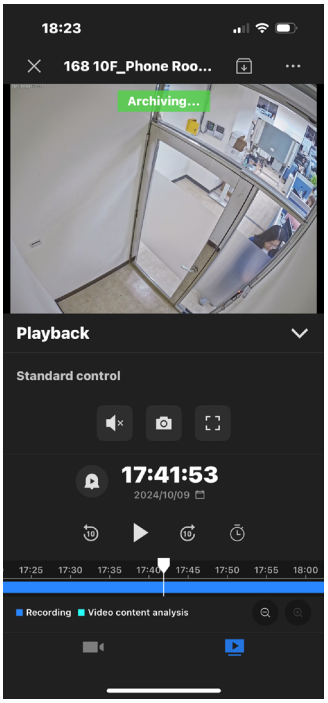


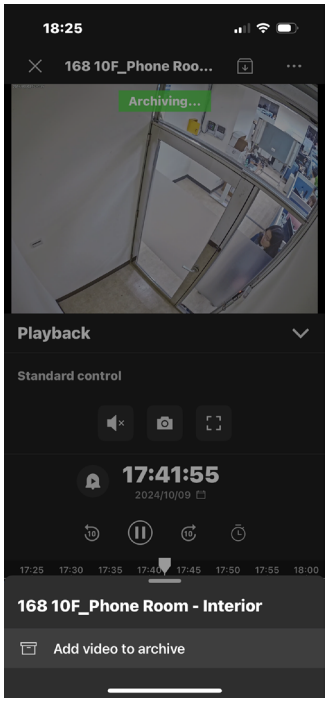
2. Select an access event and view both the surveillance and sensor event data simultaneously through the camera footage and the event info below.
   - If this door is linked to multiple cameras, you can choose a specific camera through swiping the snapshots.

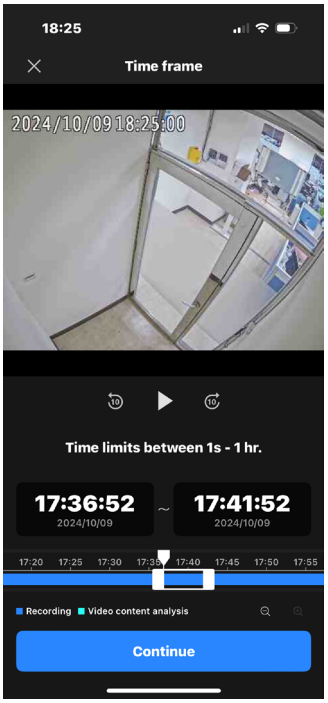




3. You can view the footage through playback, or archive this event footage and sharing with others.



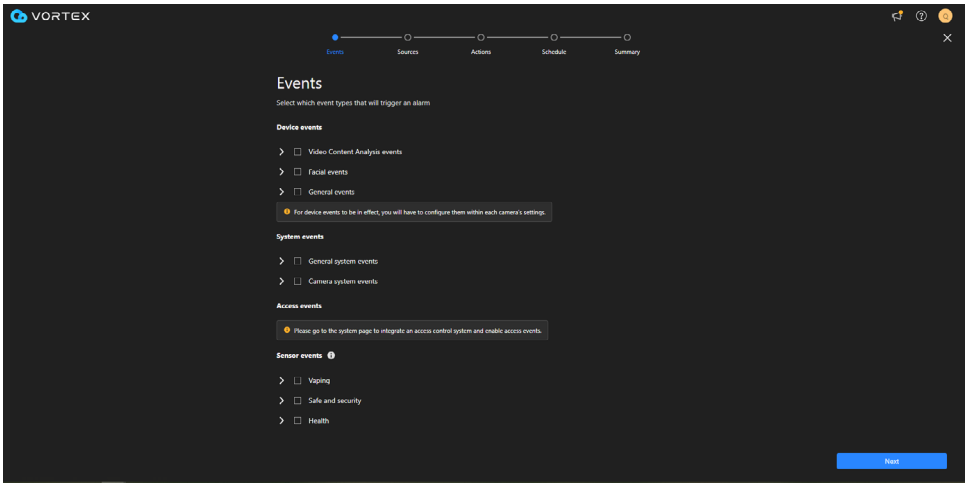




Alarm settingsand Real-time Notification

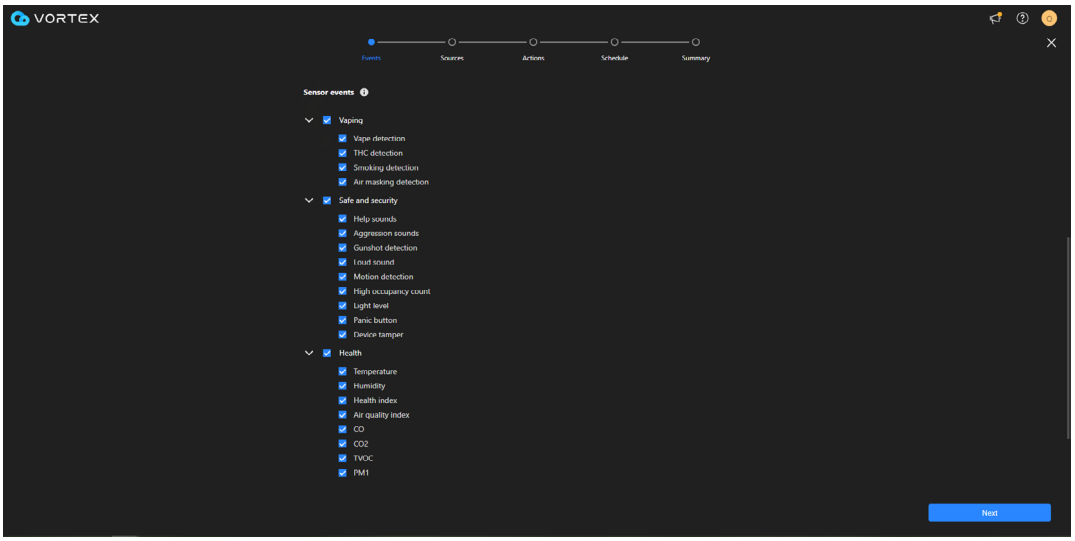
Goal

Allow Owner/Administrators to set alarms for Sensor events in Alarm Management, allowing designated personnel to receive real-time push notifications and email notifications.

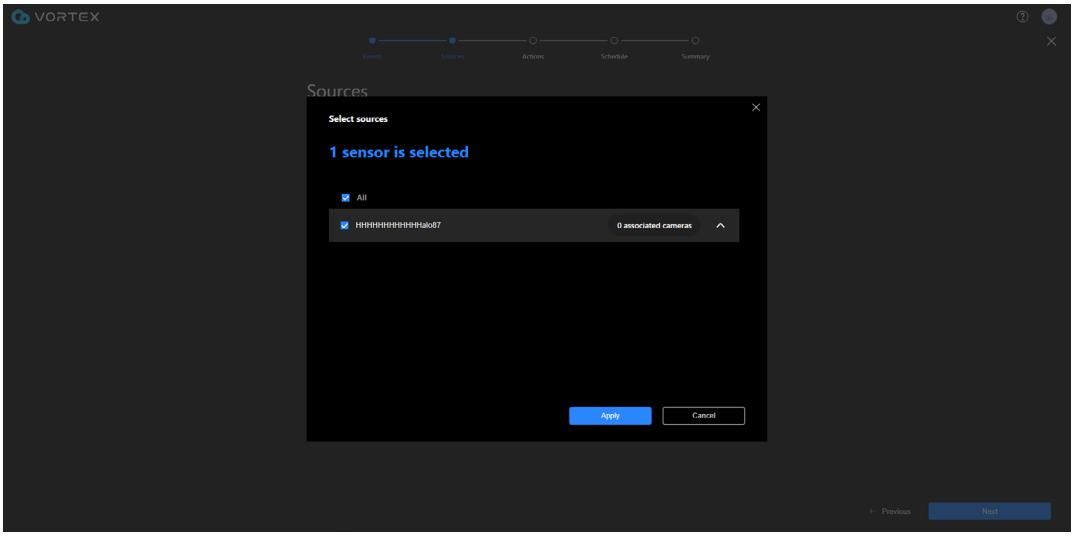


Web Portal

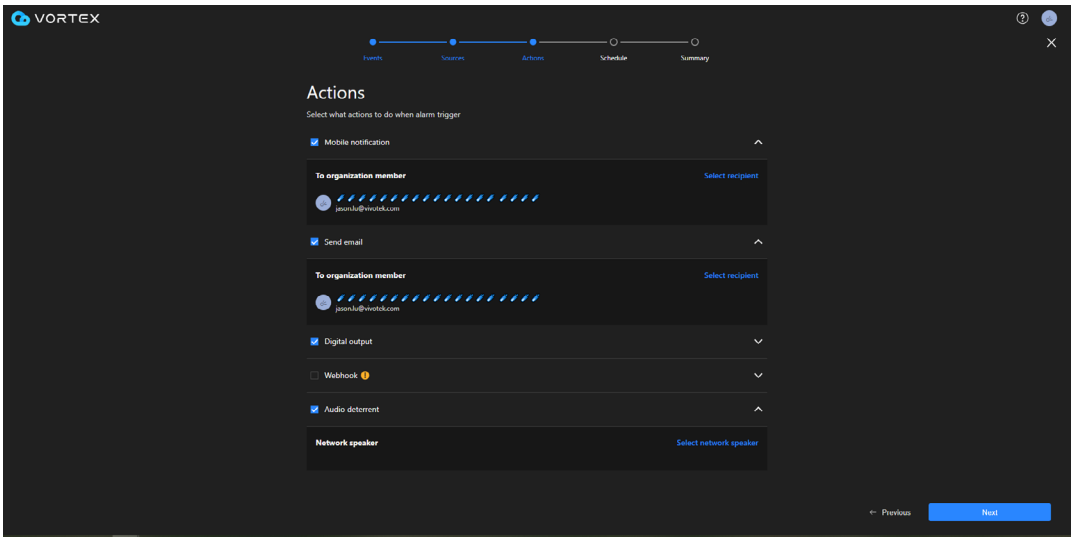
1. Go to System > Alarm Management > Add alarm
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Sensor event



2. In the next step - Sources, select the doors that initiate Sensor events.
   - The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Sources for the Sensor.
   - Click the expand button to view the cameras associated with this door.

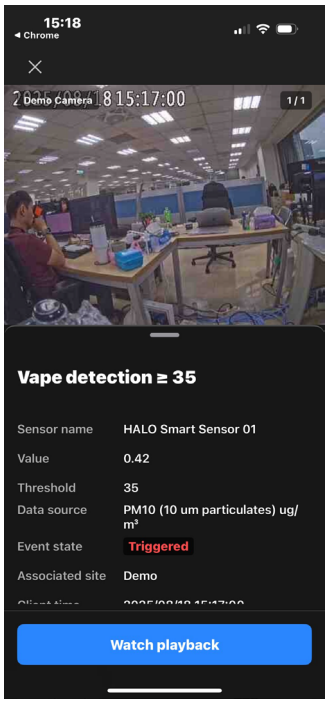


3. In the next step - Actions, select the actions and designated personnel to receive notification.
   - The design logic here is the same as the existing Alarm Management.
   - Webhook action is currently not supported by Smart Sensor events.
   - The remaining steps, Schedule and Summary, follow the same design logic and operate in the same manner as they currently do.



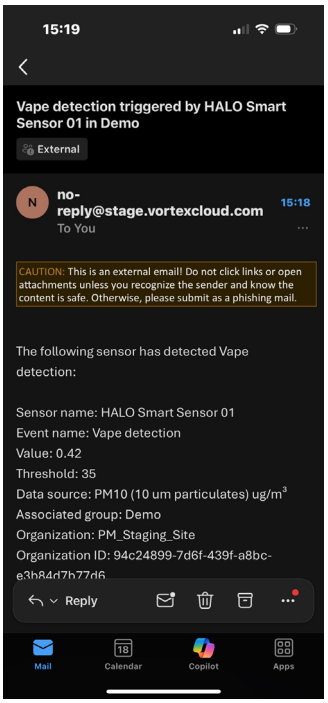
Mobile App

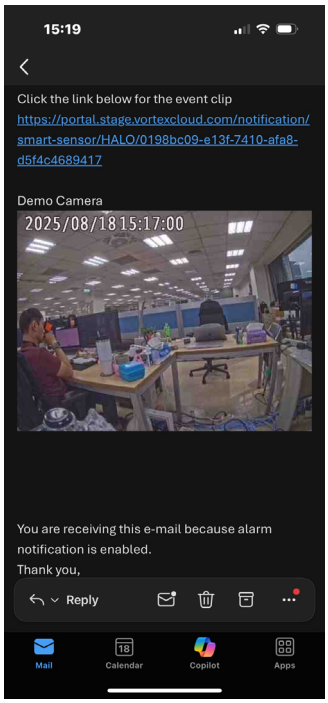
Designated personnel received real-time push notification.



Designated personnel received email notification.

- If a sensor is associated with multiple cameras, the email will display snapshots from these cameras.





Trigger-Action Automation

Goal

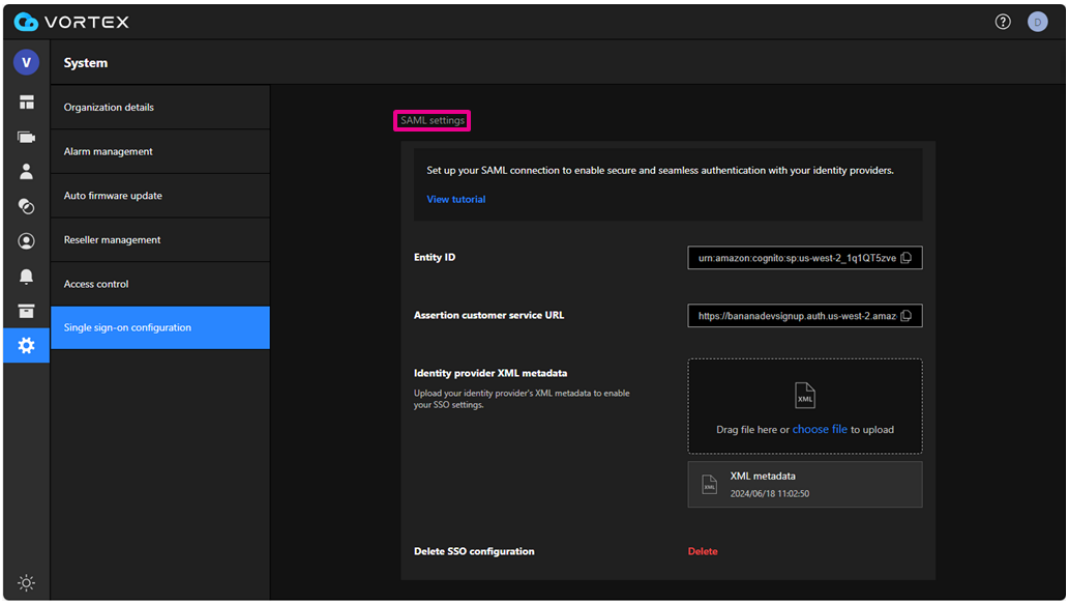
Integrates Halo Smart Sensor with VORTEX Alarm Management to automatically trigger specific physical security actions based on sensor events. Possible examples include, but not limited to:

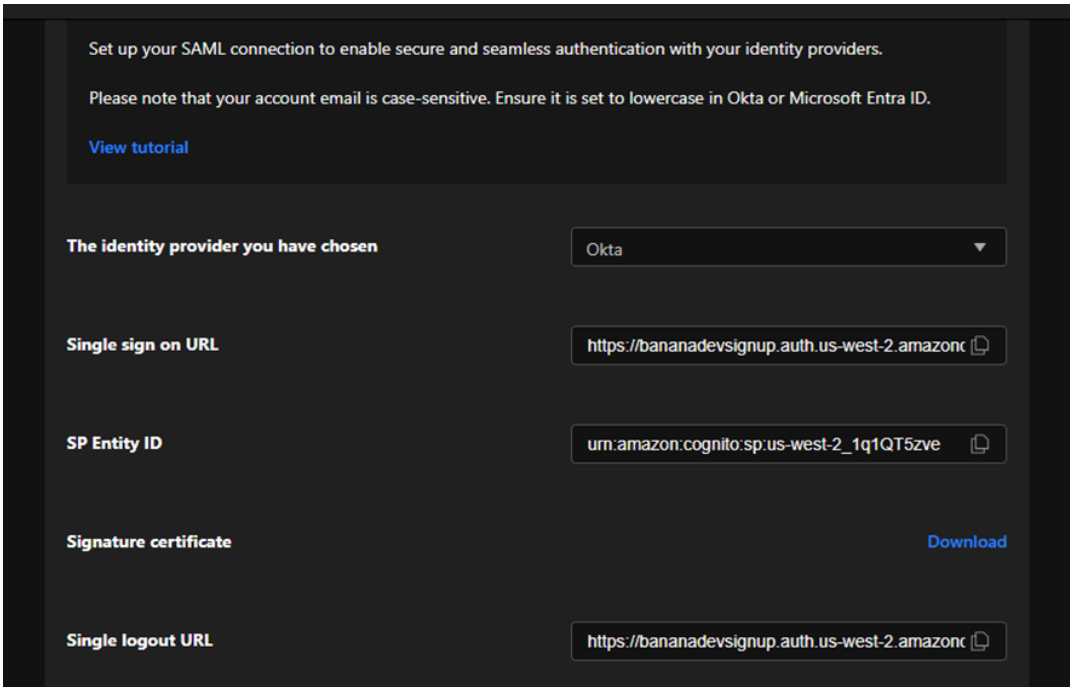
Event Type	Physical Security Actions
Vape / Smoking / THC / Masking	• Triggers pre-recorded voice alert on the Network Speaker to remind users of the smoking ban. • Talk-down feature provides immediate verbal warnings.
Gunshot Detection	• Remote lockdown of specific doors via the VORTEX mobile app. • Talk-down feature on the Network Speaker to provide warnings or guide evacuation.
Spoken Keyword Detection	• Triggers pre-recorded evacuation message through the Network Speaker. • Remote unlock of specific doors via the VORTEX mobile app. • Activates emergency lights through Digital Output.
Aggression Detection	• Triggers pre-recorded de-escalation message through the Network Speaker. • Talk-down feature provides real-time verbal warnings.

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.



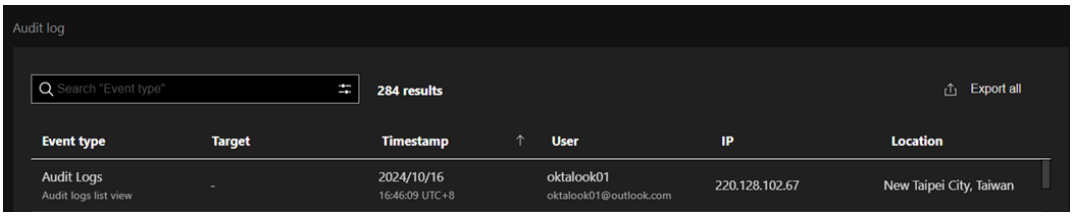


Audit log

Audit log tracks the activities within the organisation, for example, access to the organisation, 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.



License

16

Customers can scale at their own pace—benefiting from enhanced cloud management, advanced AI features, and flexible, cost-effective storage options.

- **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.
- **Camera licensing plans**
  - xStd License – Ideal for customers scaling beyond 128 channels, offering advanced user management and flexible cloud storage.
  - xPro License – Full AI-powered capabilities, including Deep Search, and an exclusive 10-year warranty for VORTEX Cameras. With advanced AI capabilities, xPro offers greater flexibility to meet your operational needs—without any additional integration costs.

For users aiming to enhance security coverage and data retention, we highly recommend adding a cloud storage license. It provides comprehensive recording backup securely stored in the cloud. Our cloud storage licenses are available for duration of 30, 60, 90, 120, 180, and 365 days, with each duration offered for terms of 1, 3, 5 or 10 years. This ensures continuous access to data for review or incident recovery as needed.

Additionally, to enable your VORTEX network speaker, you will require a corresponding network speaker license. It is also available for a duration of 1, 3, 5, and 10 years

License-required feature

17

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

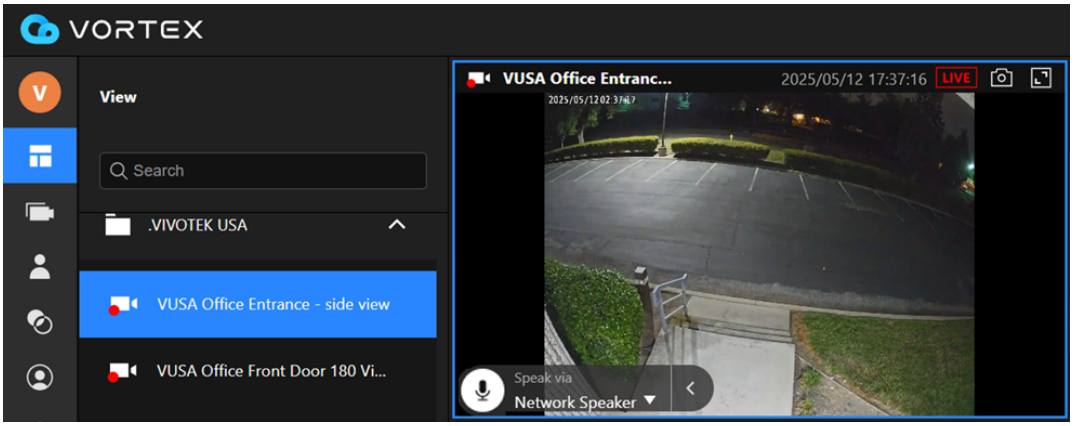
System Integrators can follow the RX9502 setup guide to update the device's firmware, converting it into a dedicated VORTEX Cloud Bridge. Once added to your VORTEX organization, the RX9502 is able to detect and bring in LAN-connected VIVOTEK speakers into the VORTEX portal.

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

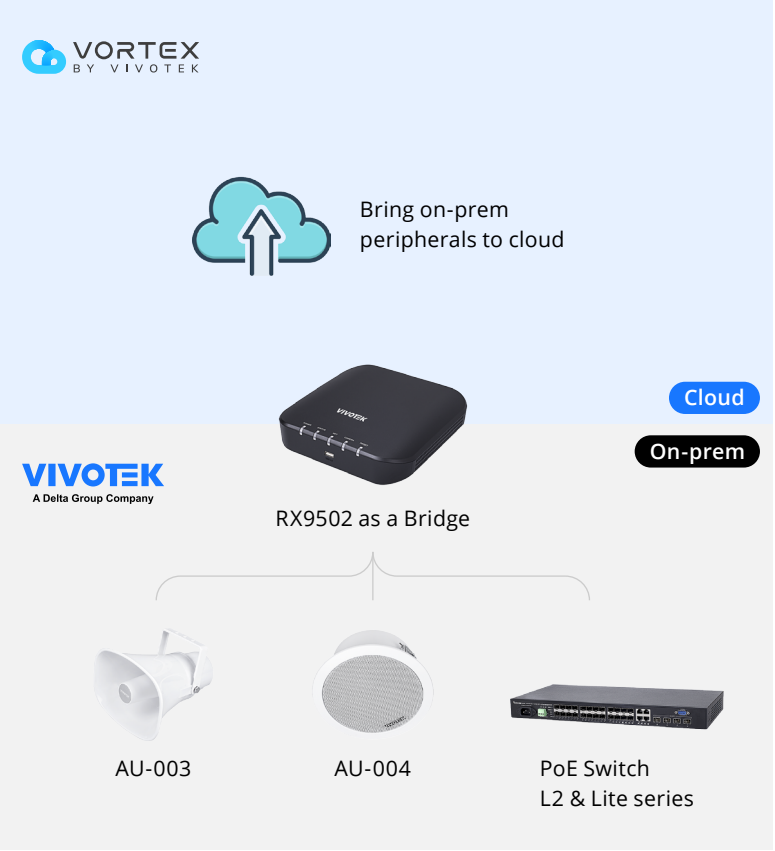
Resources & Further Reading

- **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

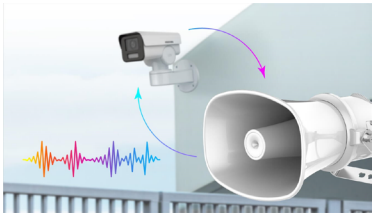
- **AU-003:**
  https://www.vivotek.com/products/accessories/network_audio_devices/au-003
- **AU-004:**
  https://www.vivotek.com/products/accessories/network_audio_devices/au-004
- **RX9502:**
  https://www.vivotek.com/products/network_video_recorder_and_appliance/video_decoder/rx9502

Integration Overview

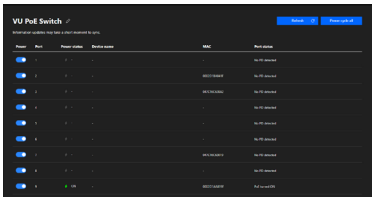


- **Talk Down**

- **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

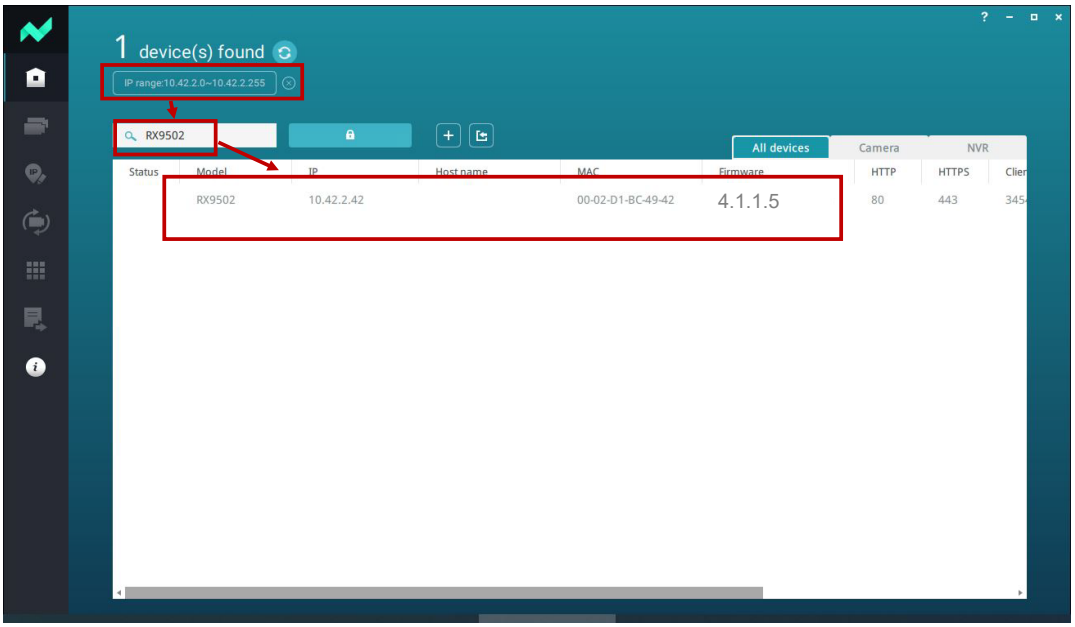
Important Note
The RX9502 will function only as a VORTEX Bridge with this firmware version. Its on-premise video receiver and decoder functions will not be available while using this firmware.

RX9502 Firmware Update

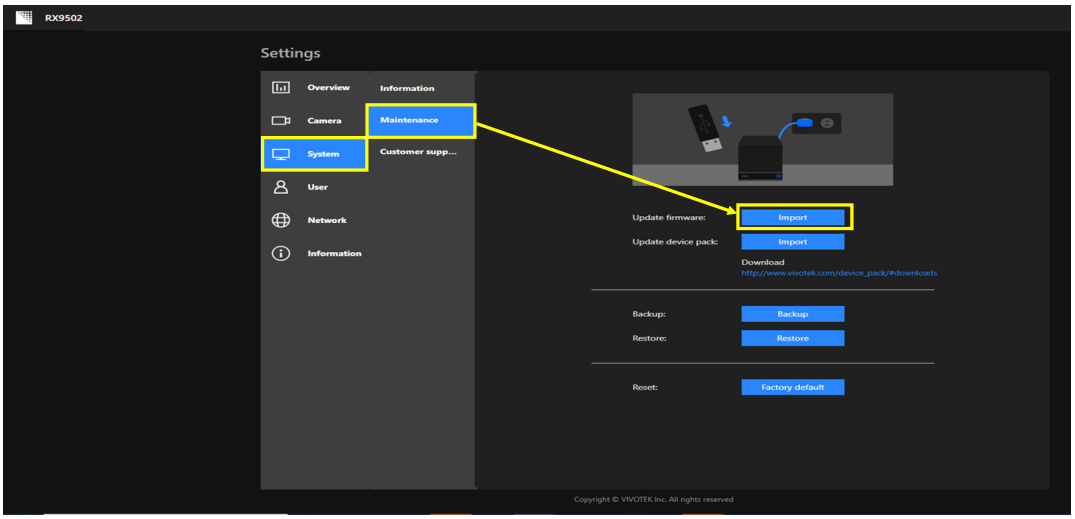
- **Using Shepherd to scan & access to RX9502 within LAN**
  Shepherd download:
  https://www.vivotek.com/en-US/products/software/shepherd
- **Firmware update**
  Double click on RX9502 via Shepherd
  Log-in RX9502 webUI > “System” > “Maintenance” > “Import” to “update firmware”

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.

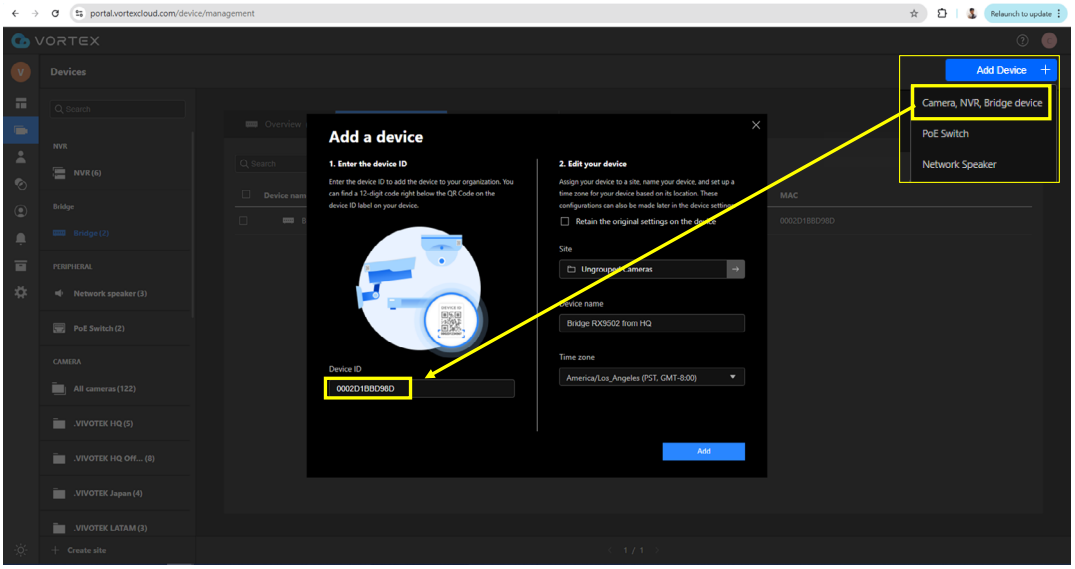


Upgrade RX9502 firmware with version **4.6.101.2.v08050800**

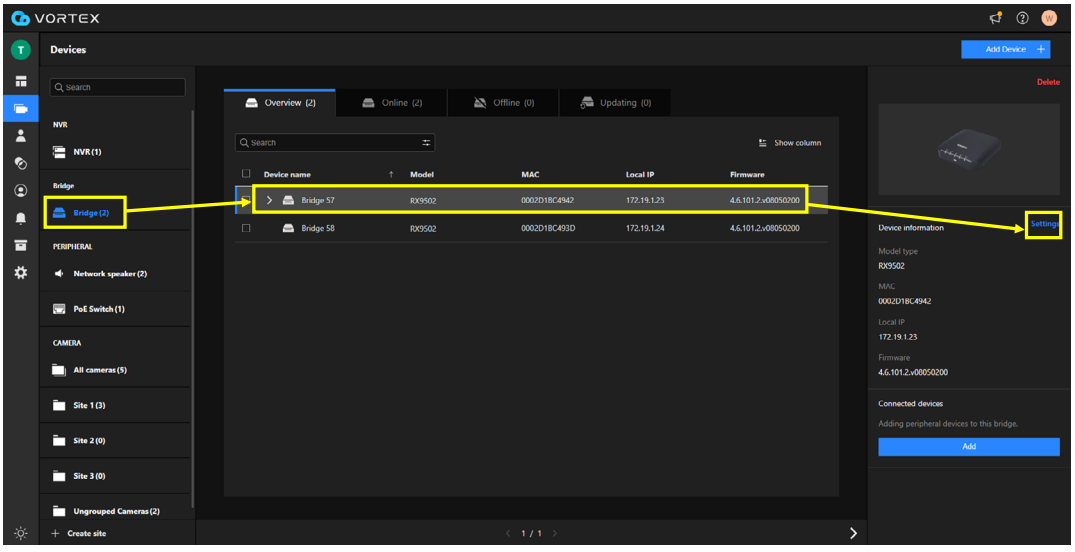
Add RX9502 in VORTEX as a bridge

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

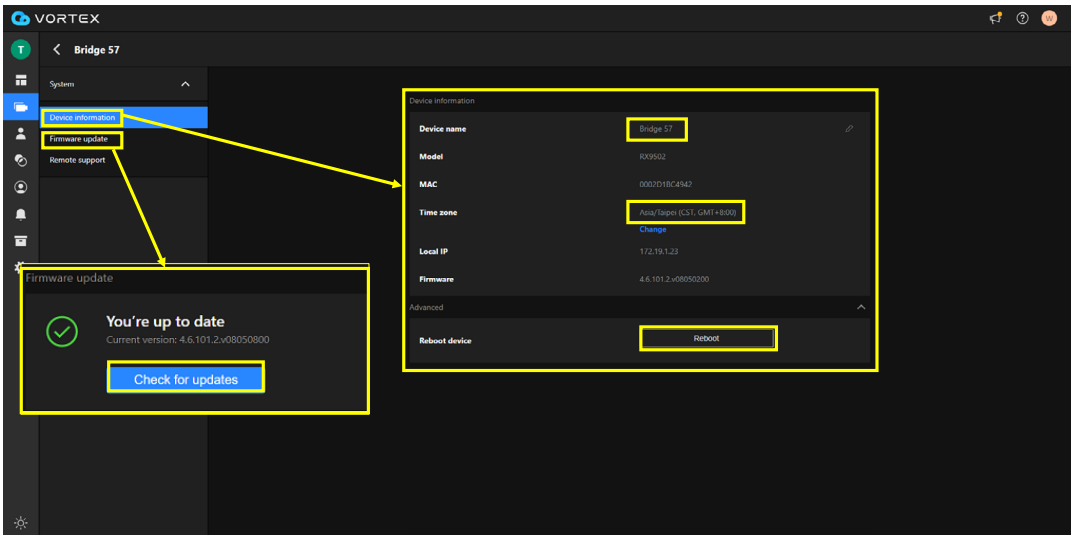
- **Set up**
  - “Device” > “Bridge” > “Setting”
    - Device Information:
      - Edit for Device name/Timezone and reboot
  - Firmware update:
    - Latest firmware update check



Add RX9502 by key-in the MAC address.



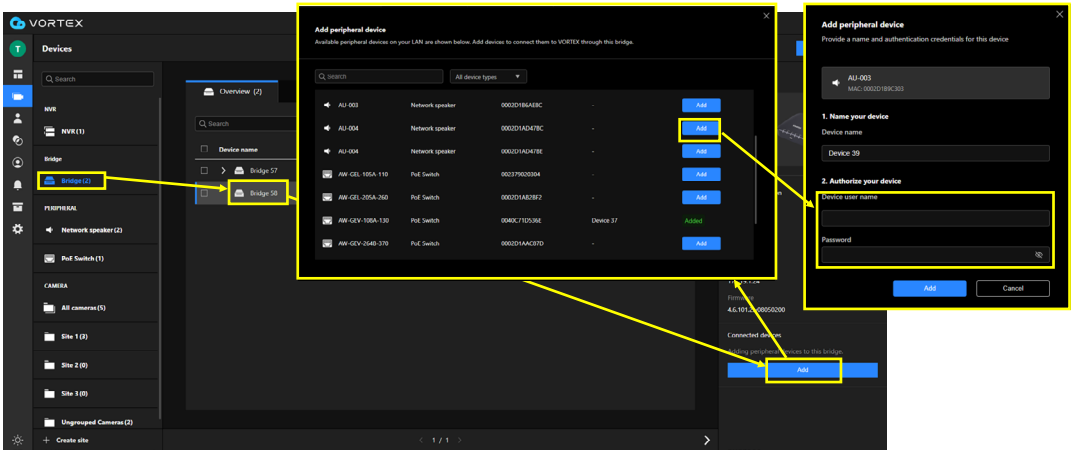
Verify and set-up the name/firmware/timezone if needed.



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

Search VIVOTEK Network Speaker and add it into VORTEX portal

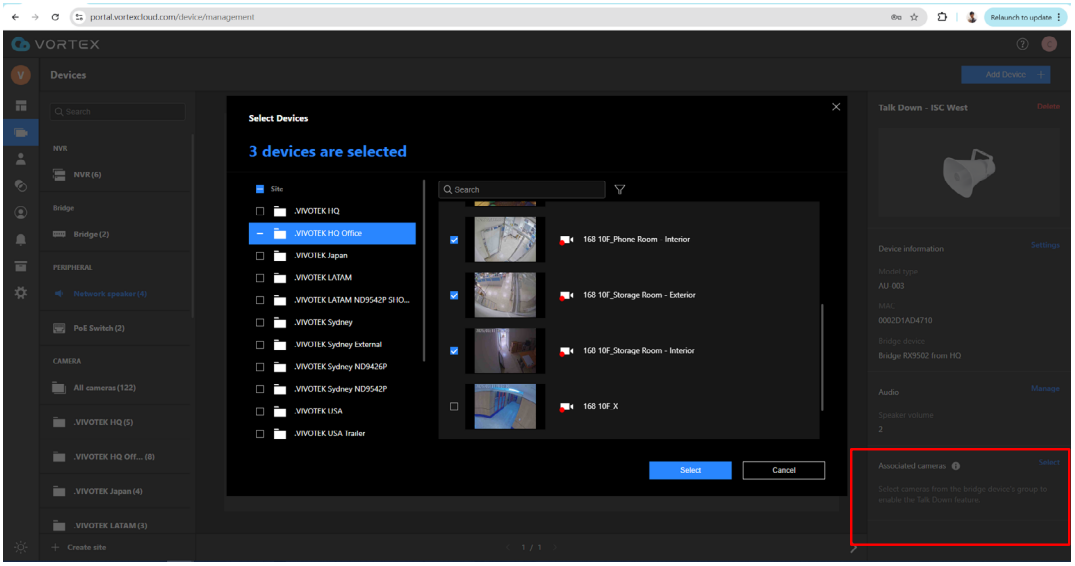
- **Log-in VORTEX > "Device" > "Bridge"**
  - Click on RX9502
- **Search for VIVOTEK Network Speaker and add it in VORTEX**
  - Click on "Add" (Under "bridge" > "connected devices")
  - Select the Network Speaker > "Add" > Authorize the device > "Add"
    - Default credential:
      Name: 1234
     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



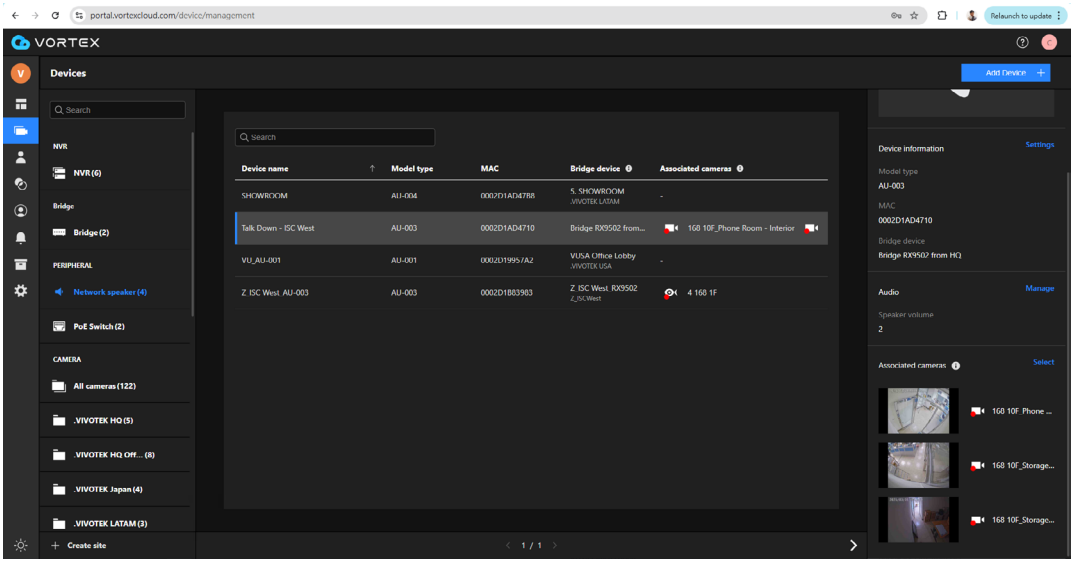
Bridge Network Speaker on VORTEX with RX9502.

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.

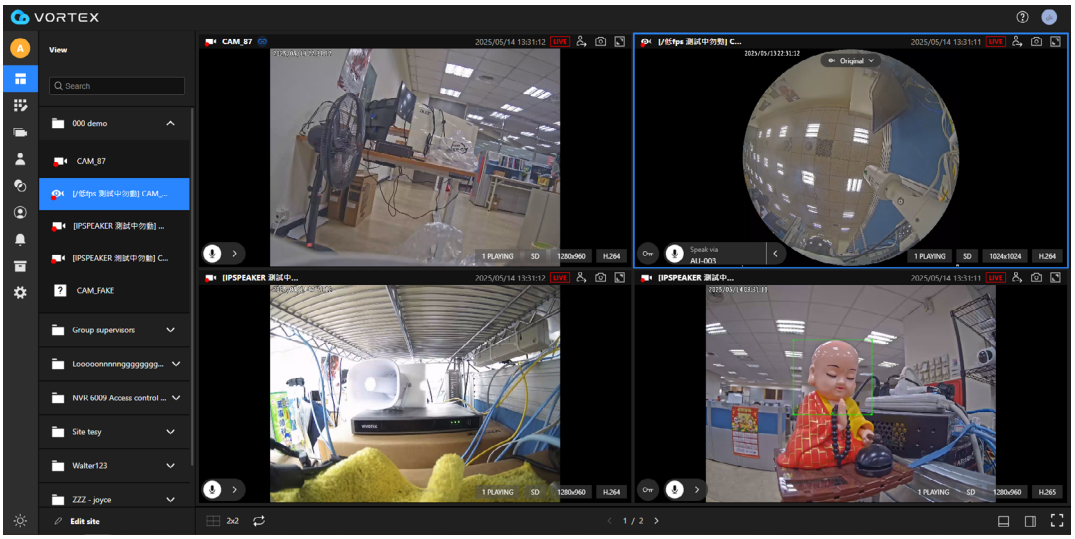


2. The association is completed and the result is displayed.

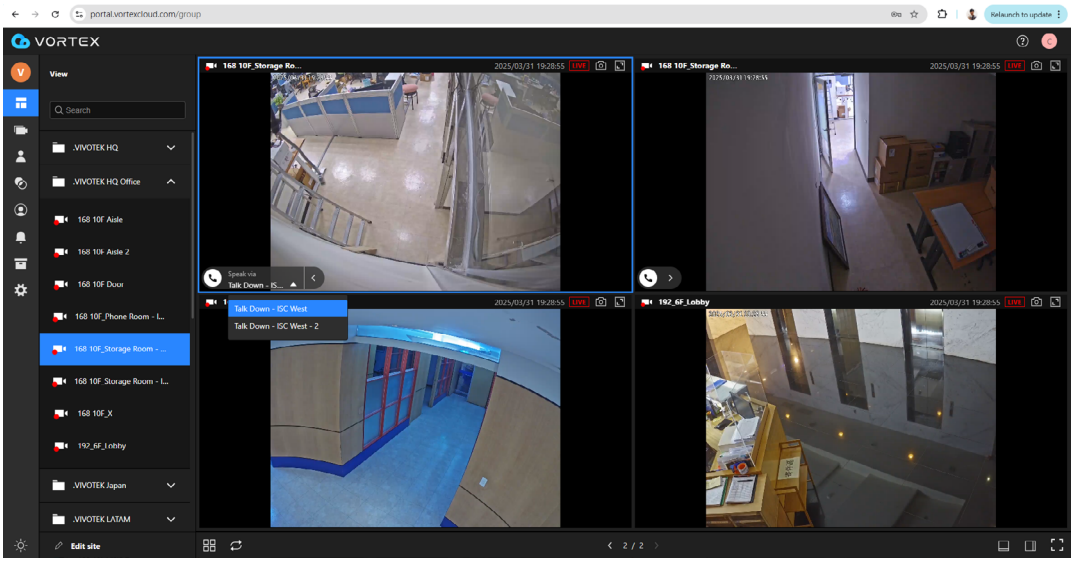


Operate Talk Down

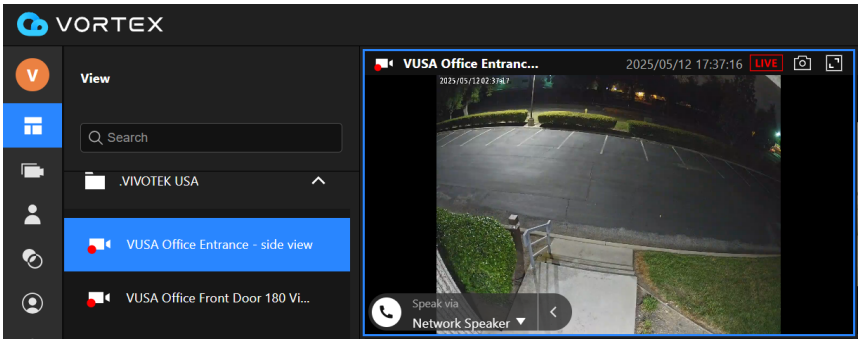
1. Go to Live page and you will see a Microphone icon displayed in the camera you associated with network speakers.

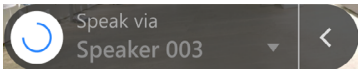


2. Click the arrow icon for dropdown list and choose the Network speaker you want to initiate talk down.

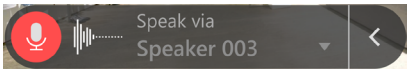


3. Click the microphone icon to start talk down. There are four possible states when you initiate the call.

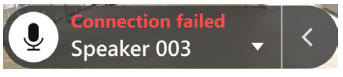




Connecting to the Network speaker



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

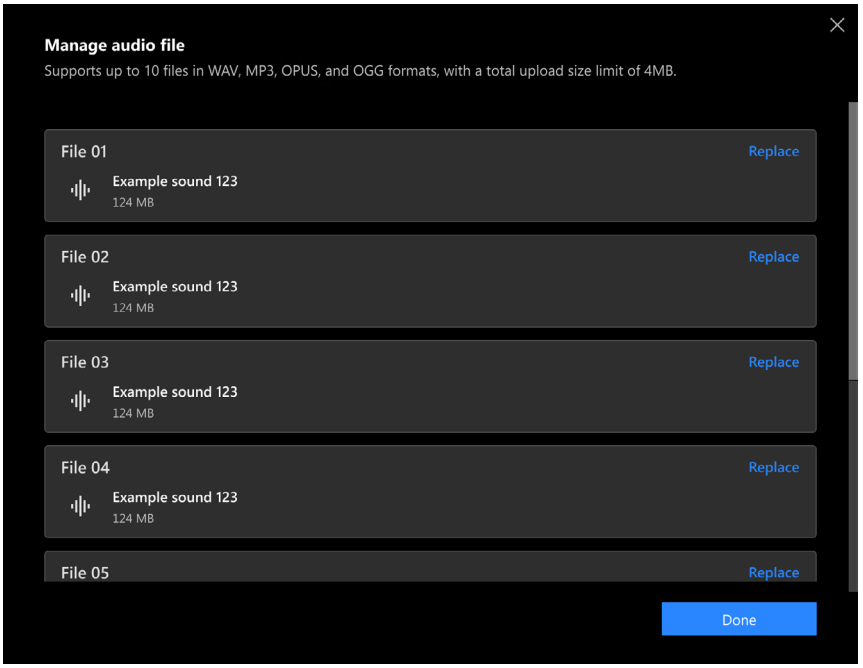


Unable to connect to the Network speaker

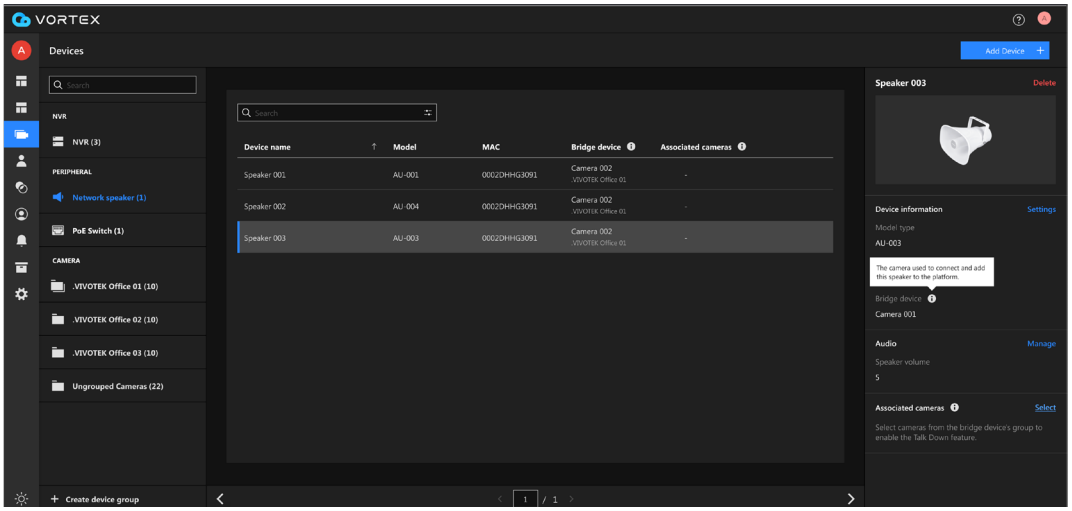
Manage Audio Files

Goal

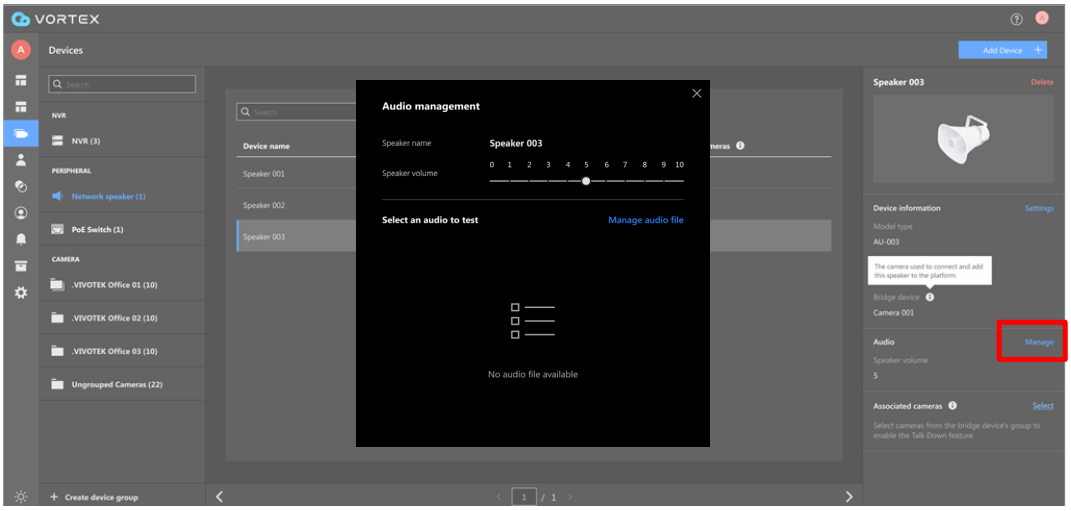
- Upload audio files to the network speaker to allow auto-play of specific files for different alarms to deter intruders.



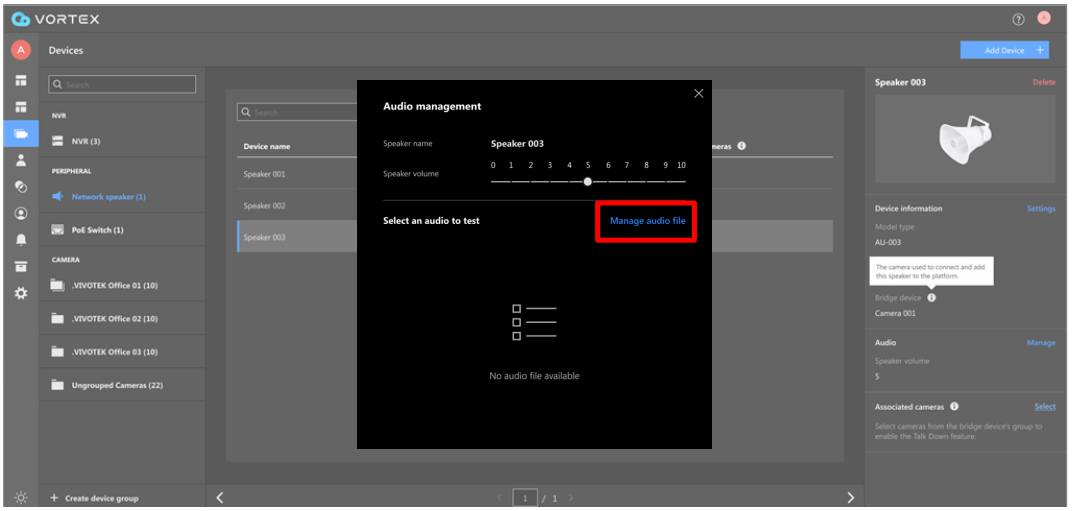
1. Select the network speaker to display the right panel for device management.



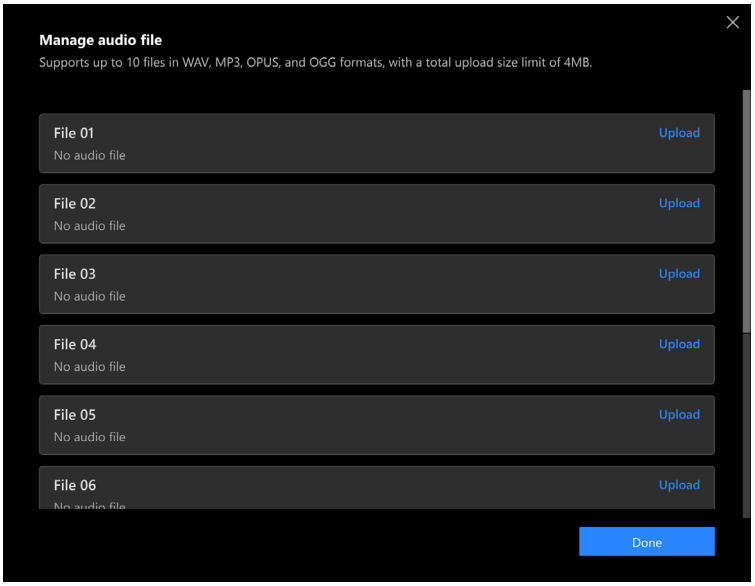
2. Select ‘Manage’ in the Audio section to open the Audio management window.



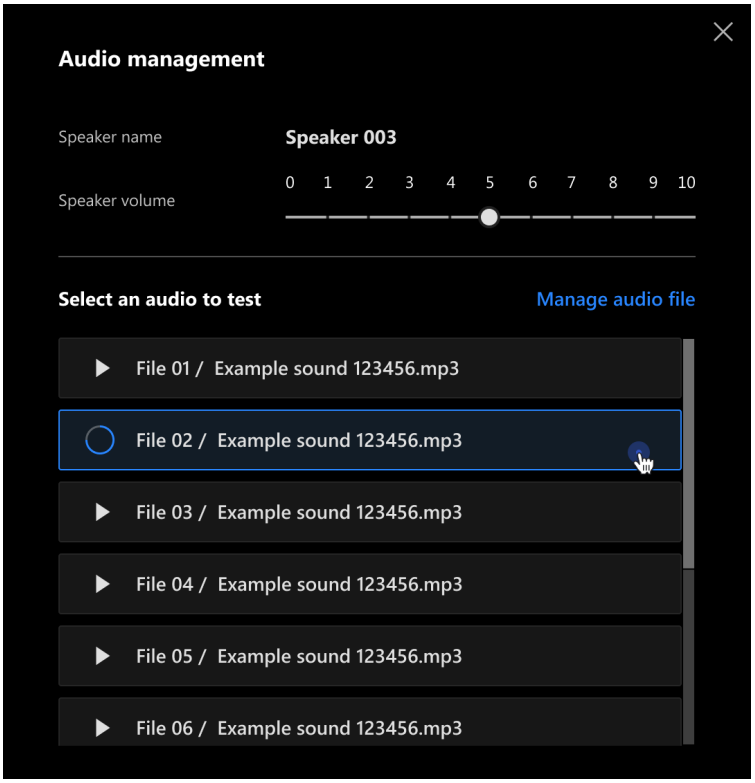
3. Select ‘Manage audio file’.



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.



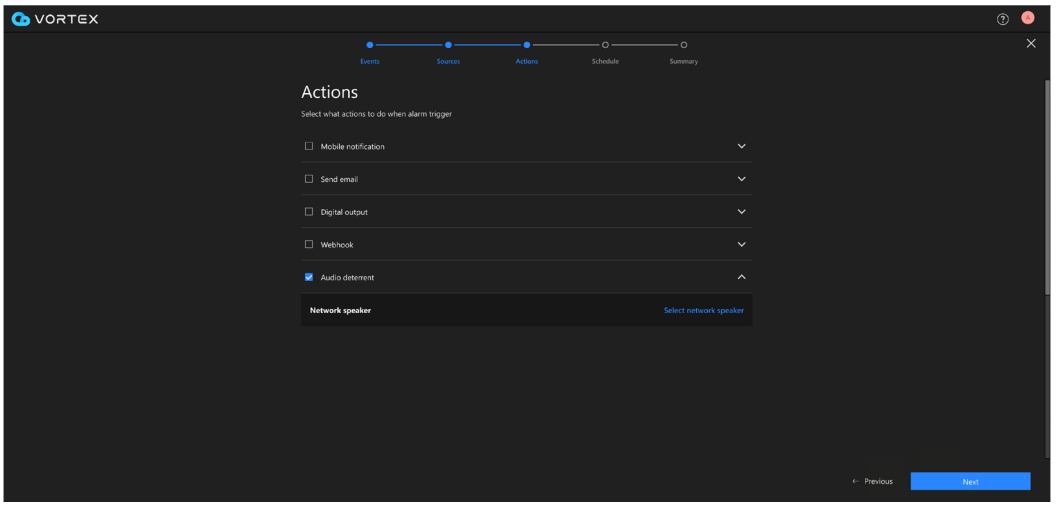
5. To test your audio files, click play icon.



Set Up Alarm Management for Audio Deterrent

Goal

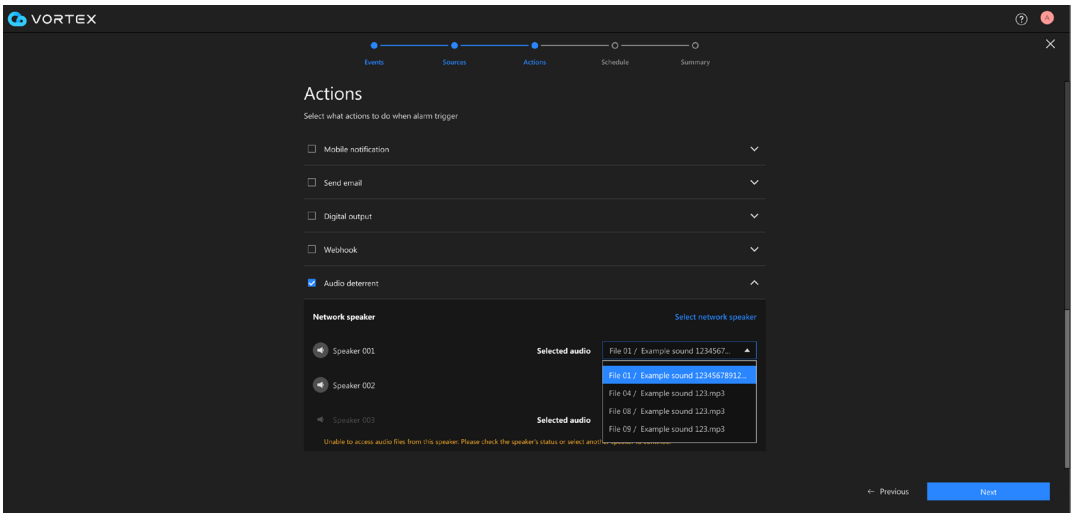
Configure network speaker as audio deterrent in Alarm Management, using the audio files uploaded to auto-play and deter intruders.



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
File 01 / Example sound 12345678912...
File 04 / Example sound 123.mp3
File 08 / Example sound 123.mp3
File 09 / Example sound 123.mp3
Speaker 003
Selected audio
Unable to access audio files from this speaker. Please check the speaker's status or select another speaker to continue.
← Previous
Next

VIVOTEK

A Delta Group Company

www.vivotek.com