

User Manual



Third-Party Integration

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 third-party integration features. In addition, you can check VORTEX FAQ on the web for more information.

Revision History

Document Version	Release Date	Comment
1.0	2026-07-31	Initial release.

Table of Contents

1 Introduction	P5
2 Legal Information & Terms of Service	P6
3 System Requirements	P7
4 Third-Party Integration	P8
Access Control Integration – Kisi	
API Integration	
Associate Cameras with Doors	
Access Events Integration with Native Videos	
Alarm Settings and Real-Time Notifications	
Remote Unlock Doors	
Access control Integration – PDK	
API Integration	
Associate Cameras with Doors	
Access Events Integration with Native Videos	
Alarm Settings and Real-Time Notifications	
Remote Unlock/Lock Doors	
Access Control Integration – Brivo	
API Integration	
Associate Cameras with Doors	
Access Events Integration with Camera Videos	
Alarm Settings and Real-Time Notifications	
Smart Sensor Integration – Halo	
Integration Setup	
Sensor Events Integration with Camera Videos	
Alarm Settings and Real-Time Notifications	
Trigger-Action Automation	

Introduction

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

Legal Information & Terms of Service

2

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

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

1. Privacy Policy

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

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

2. End User License Agreement (EULA)

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

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

3. Terms and Conditions

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

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

System Requirements

Before using VORTEX, have the following items ready:

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

NOTE

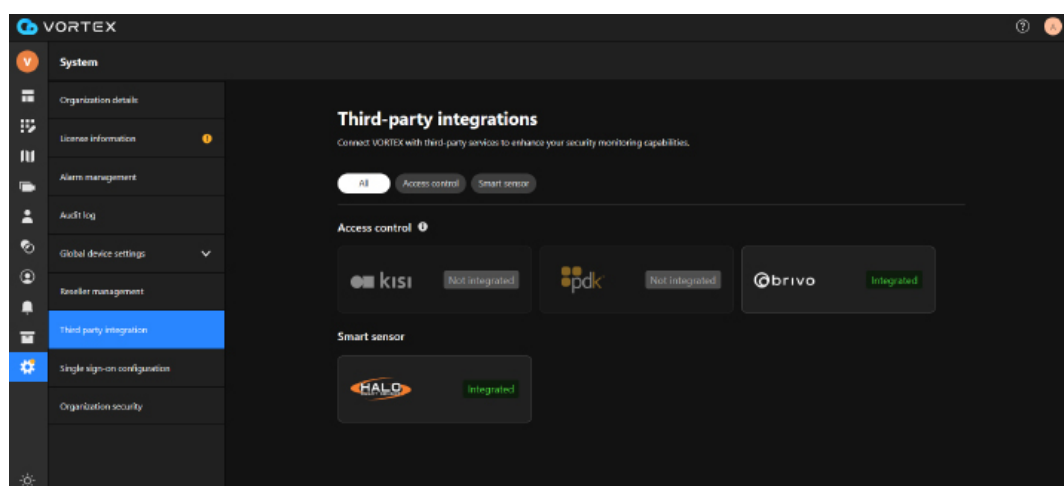
An internet connection is also a must. Otherwise, VORTEX cameras and the VORTEX service cannot communicate with the VORTEX servers, so you will not be able to use important features such as video storage, live view for real-time monitoring, or any of the other functionalities offered by the service.



Third-Party Integration

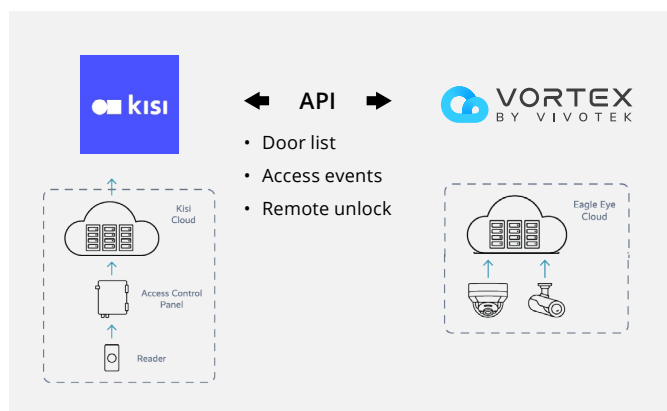
VORTEX supports integration with selected third-party platforms, including access control systems and smart sensors. These integrations allow external events to be incorporated into VORTEX for centralized monitoring and alarm management.

Navigate to **System > Third-Party Integration** to view supported integrations and their current status.

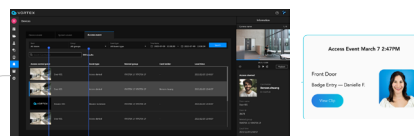


Access Control Integration – Kisi

System Overview



- Access Events Integration with Native video



- Real-time Access Event Notification



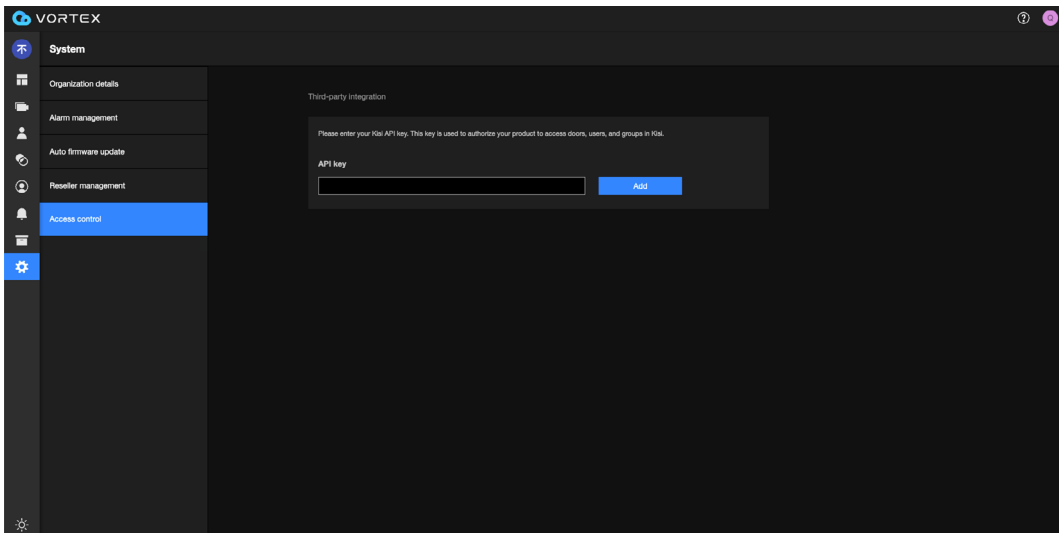
- Remotely Unlock Doors (Phase 2)



API Integration

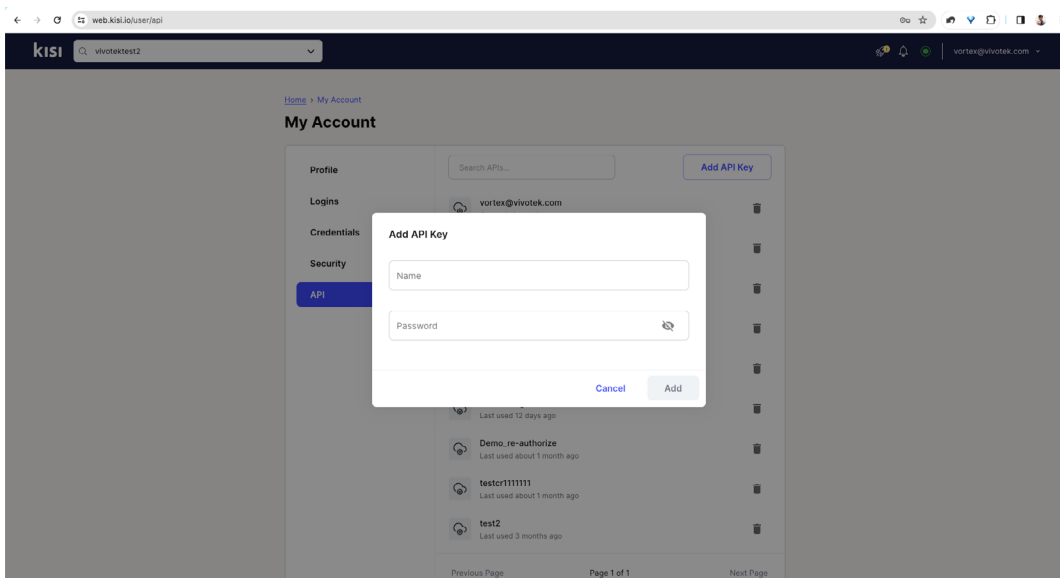
Goal

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

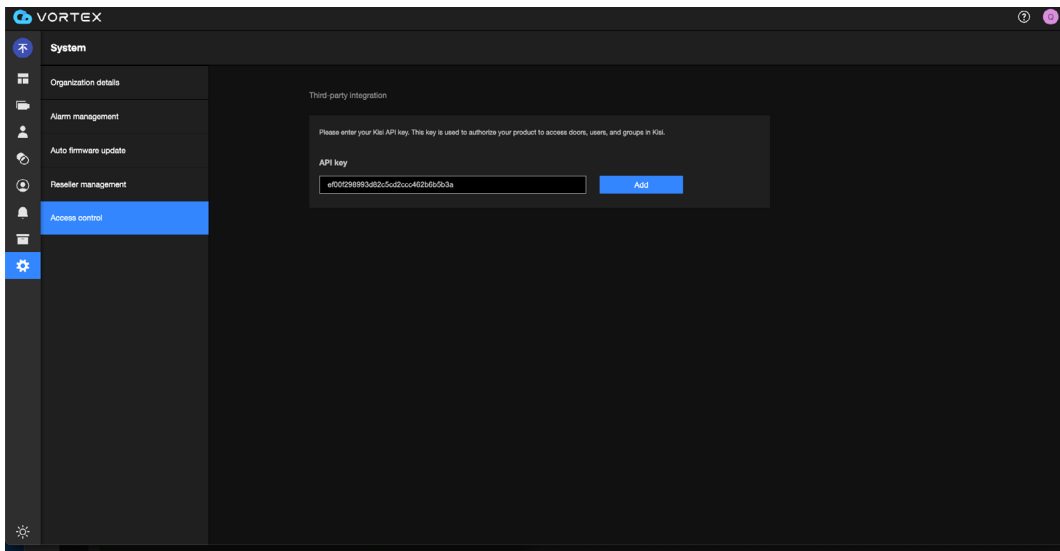


Feature Guide

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

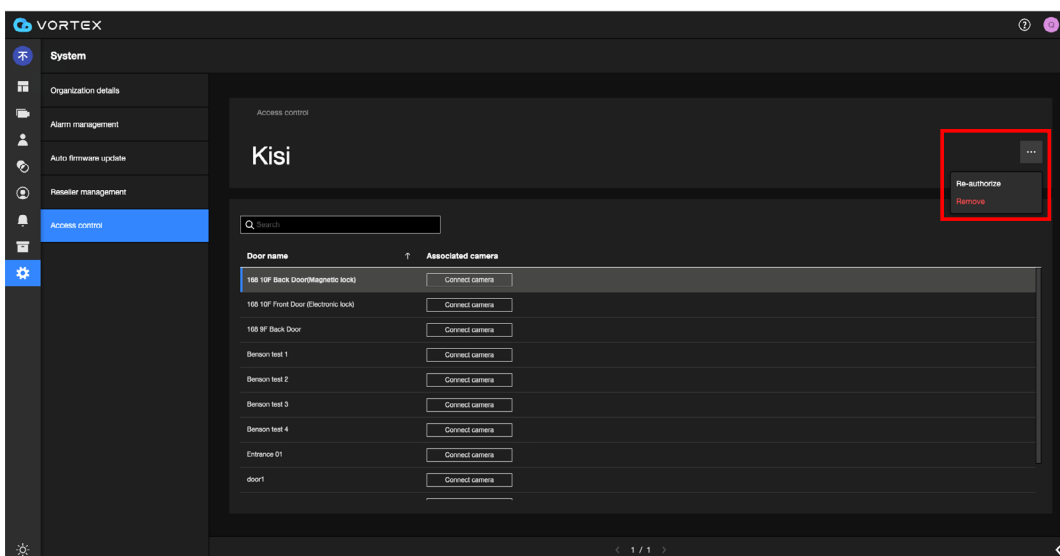


2. Go to VORTEX > System > Access control, paste Kisi API Key and click Add
 - Only Owner/Admin can operate this function
 - An API Key must be generated on the Kisi platform



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.

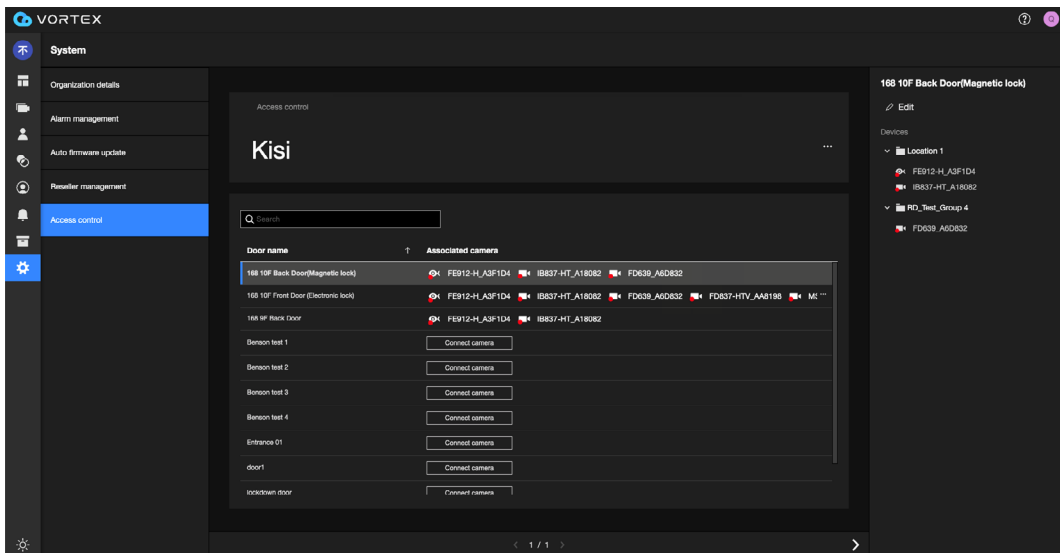
- If a user removes this API Key on the Kisi platform, they will no longer be able to use the integrated services on VORTEX.
- A single VORTEX Org. can only integrate with one Kisi Org.



Associate Cameras with Doors

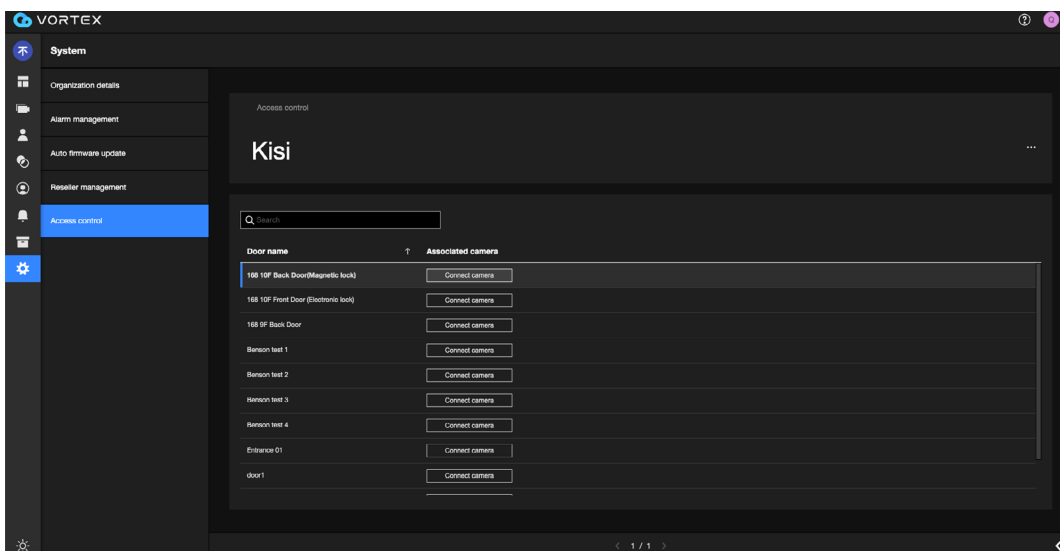
Goal

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

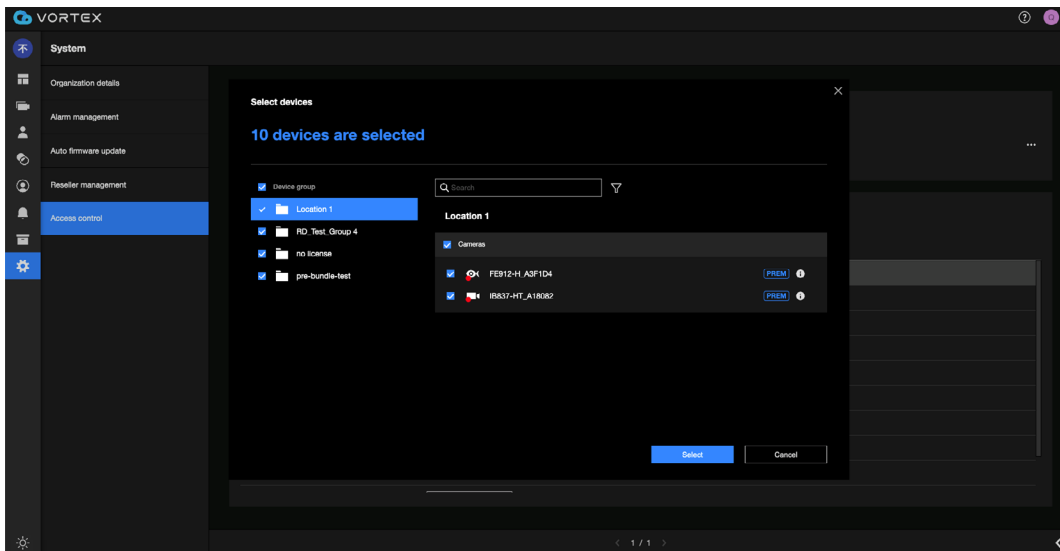


Feature Guide

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

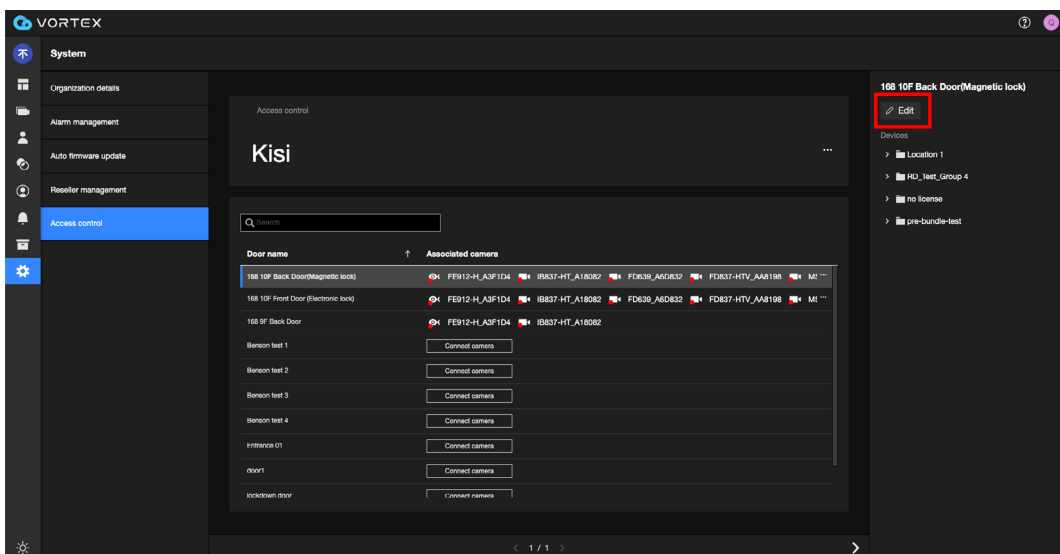


2. Select the cameras you want to associate with this door
 - Each door can be associated with up to 10 cameras
 - A door that has been associated with a camera can also be associated with other cameras



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

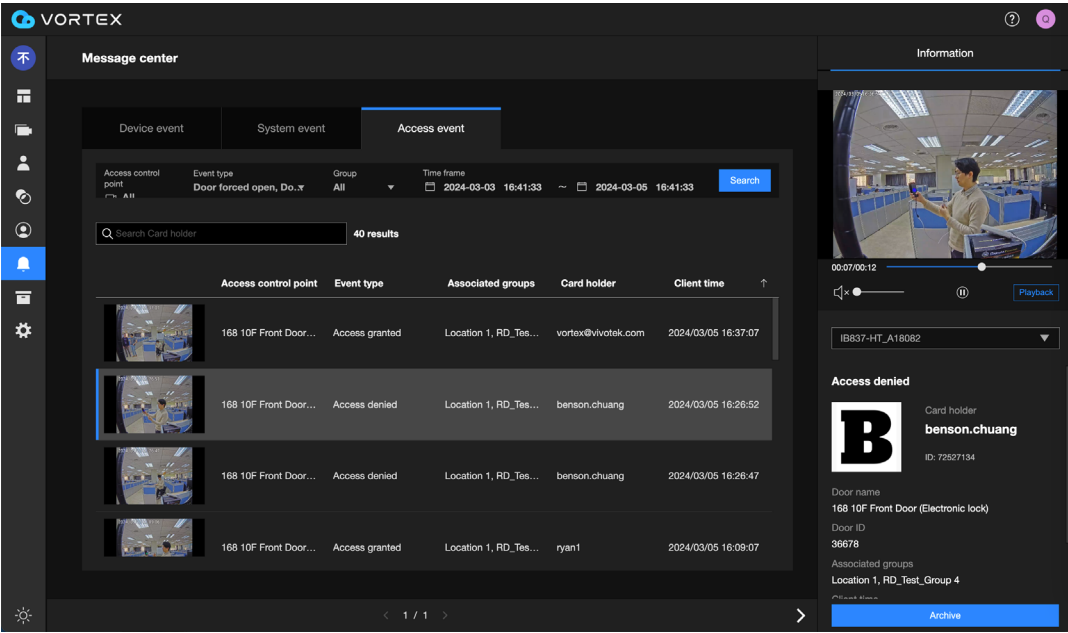
- Users can add/edit/disassociate the cameras associated with doors
- After users add/edit/delete doors on the Kisi platform, VORTEX will reflect the corresponding changes based on the adjustments



Access Events Integration with Native Videos

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.



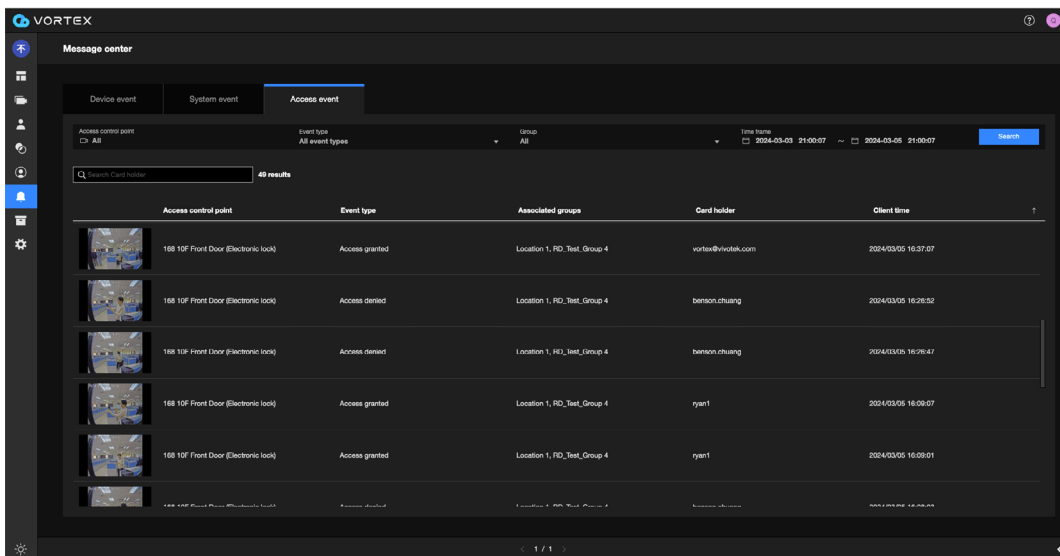
Event Types

	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	

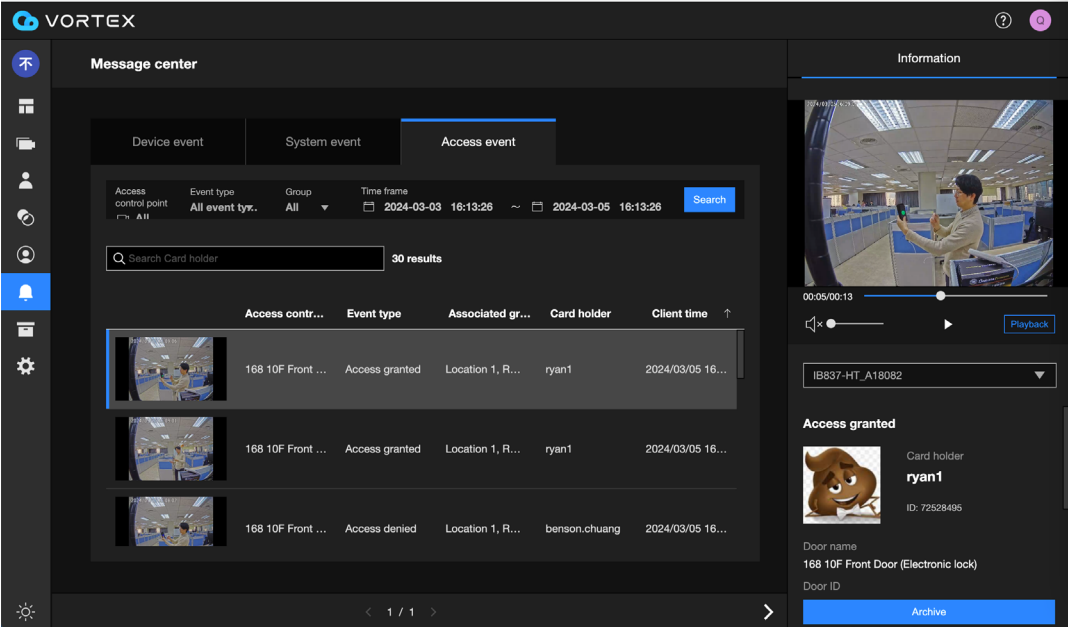
Lockdown	Door lockdown	Prevent users from entering or exiting a specific door	Enable door lockdown
	Place lockdown	Prevent users from entering or exiting any Kisi-enabled door in that particular place.	Enable place-wide lockdown
	Elevator lockdown	Lock a certain elevator stop for everyone	Enable elevator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

Feature Guide - Web

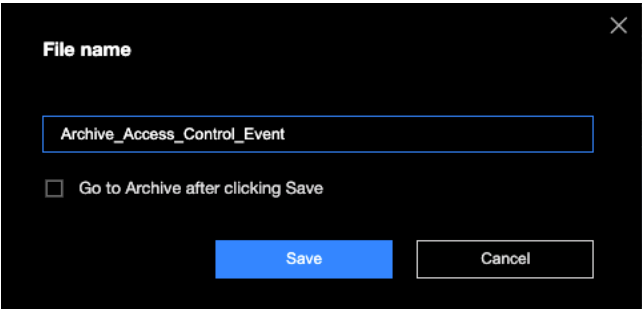
- Go to Message Center and select "Access event" tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
 - Currently, the retention period for events is the same as for Cameras, which is 30 days (Longer retention will be implemented 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.



- 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.

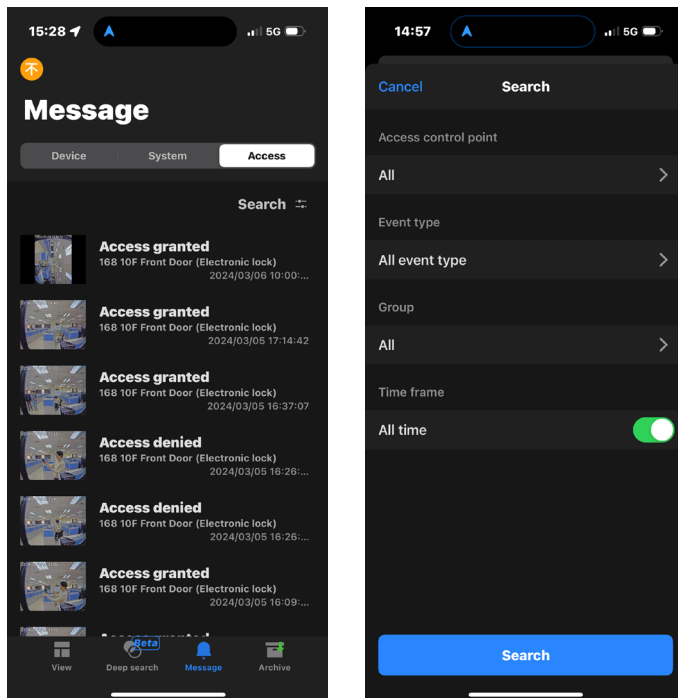


3. You can view the footage through playback, or archive this event footage and sharing with others.

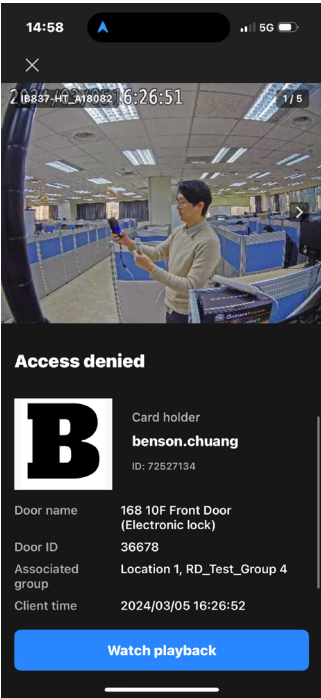


Feature Guide – Mobile App

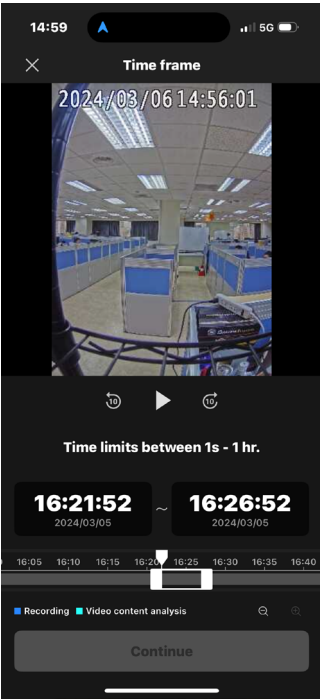
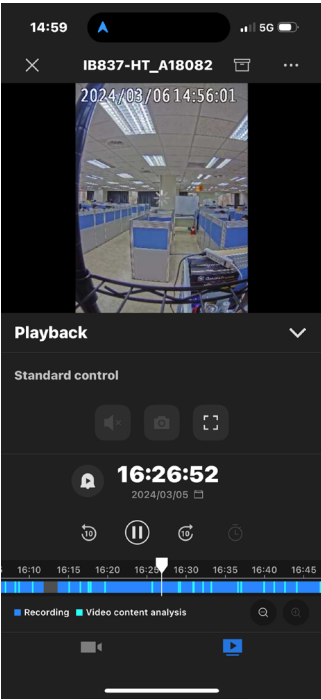
- Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
 - Currently, the retention period for events is the same as for Cameras, which is 30 days (Longer retention will be implemented 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.



- 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.



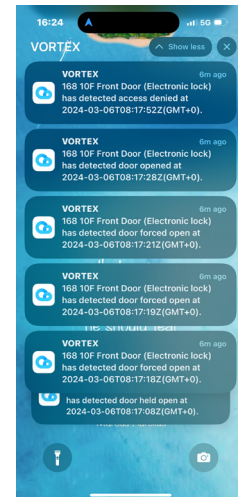
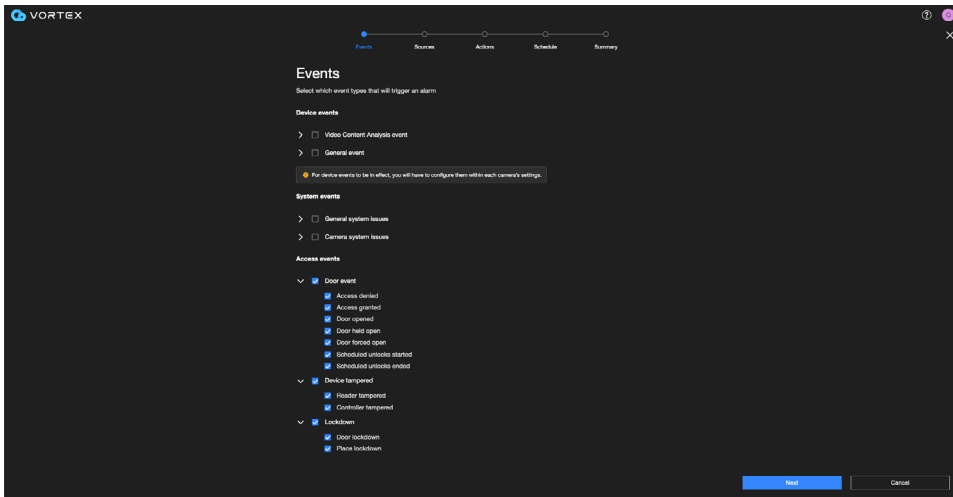
3. You can view the footage through playback, or archive this event footage and sharing with others.



Alarm Settings and Real-Time Notifications

Goal

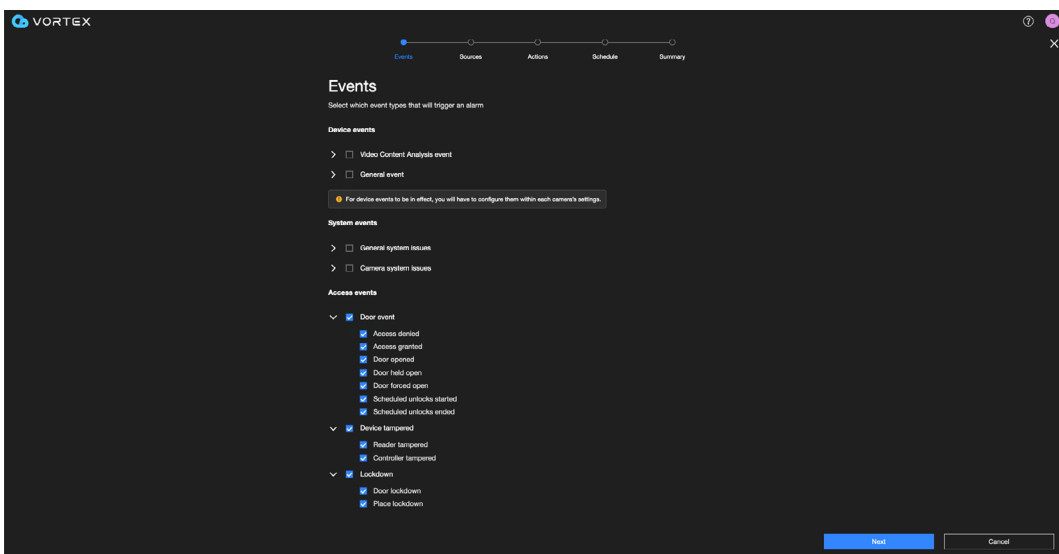
- Allow Owner/Administrators to set alarms for Access events in Alarm Management, allowing designated personnel to receive real-time push notifications and email notifications.



Feature Guide - Web

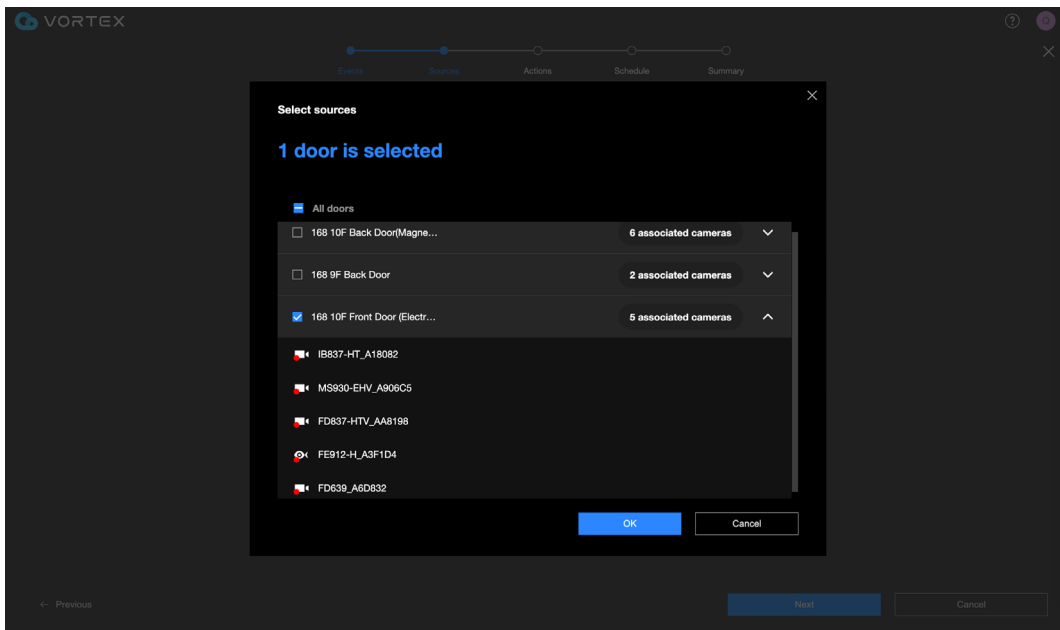
1. Go to System > Alarm Management > Add alarm

- 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)



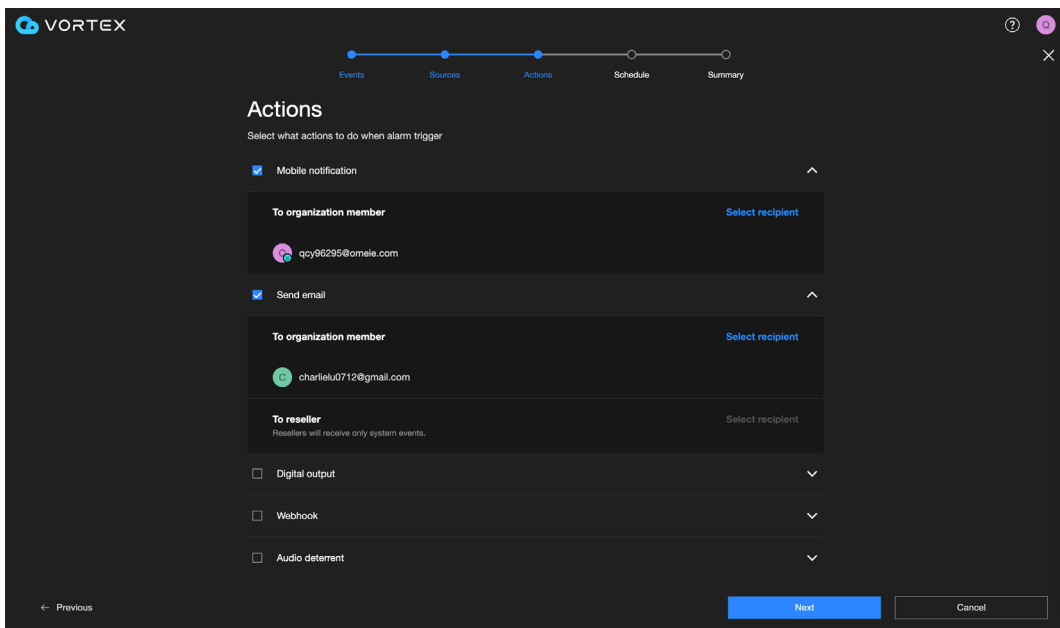
2. In the next step - Sources, select the doors that initiate Access events.

- 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



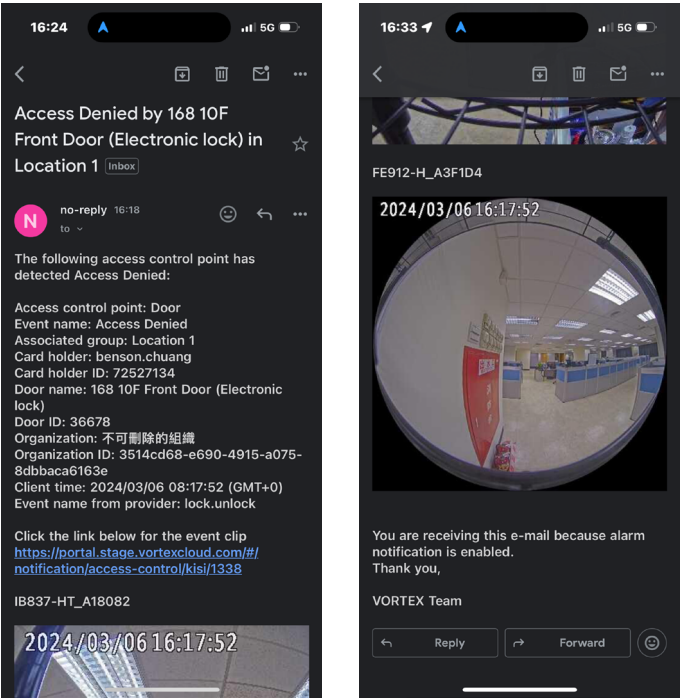
3. In the next step - Actions, select the doors that initiate Access events.

- 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.



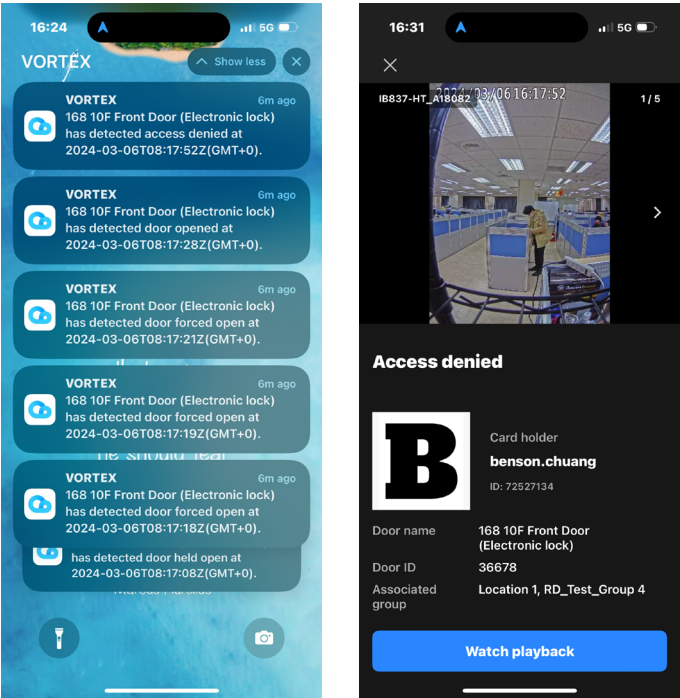
Feature Guide – Email Notification

- 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

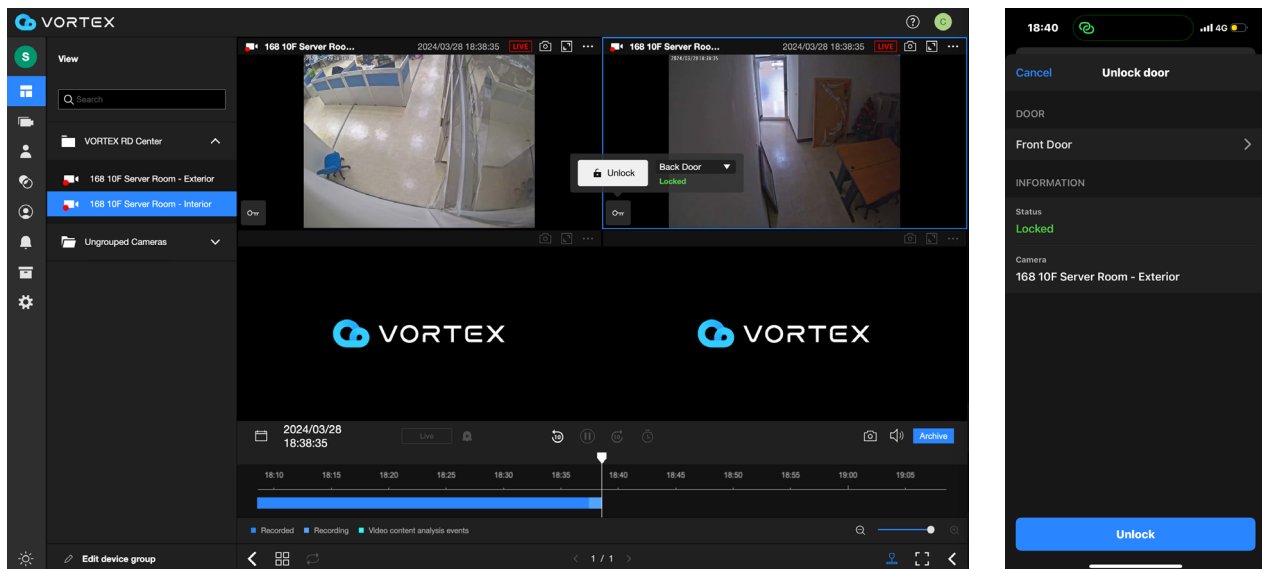
- Designated personnel received real-time push notification.
- Access events that may result in a continuous state will only trigger an alarm notification the first time they occur, such as 'Door held open' and 'Door forced open'.



Remote Unlock Doors

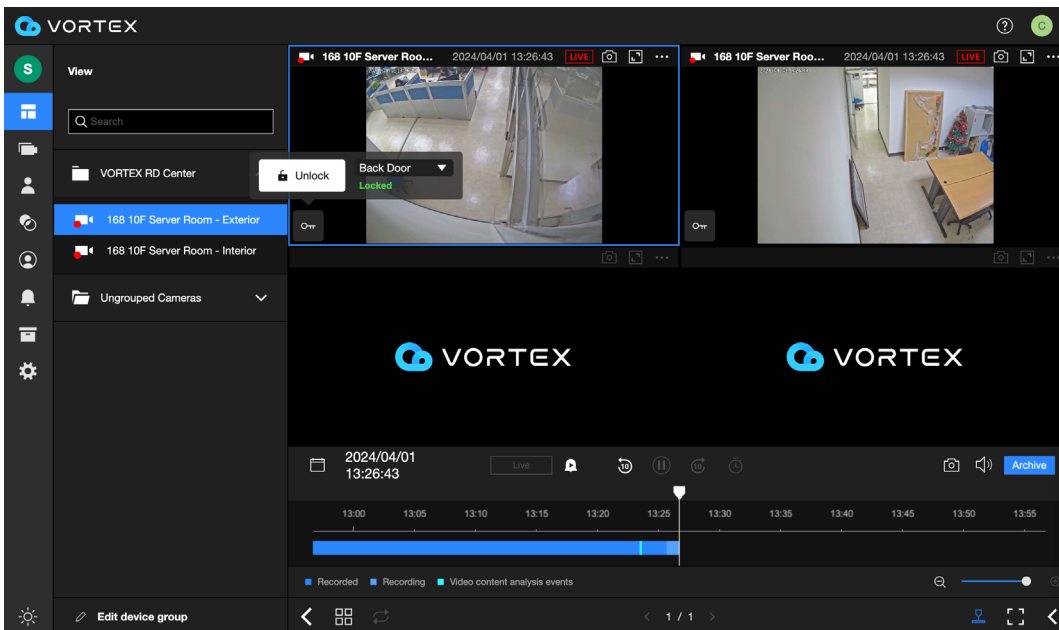
Goal

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.



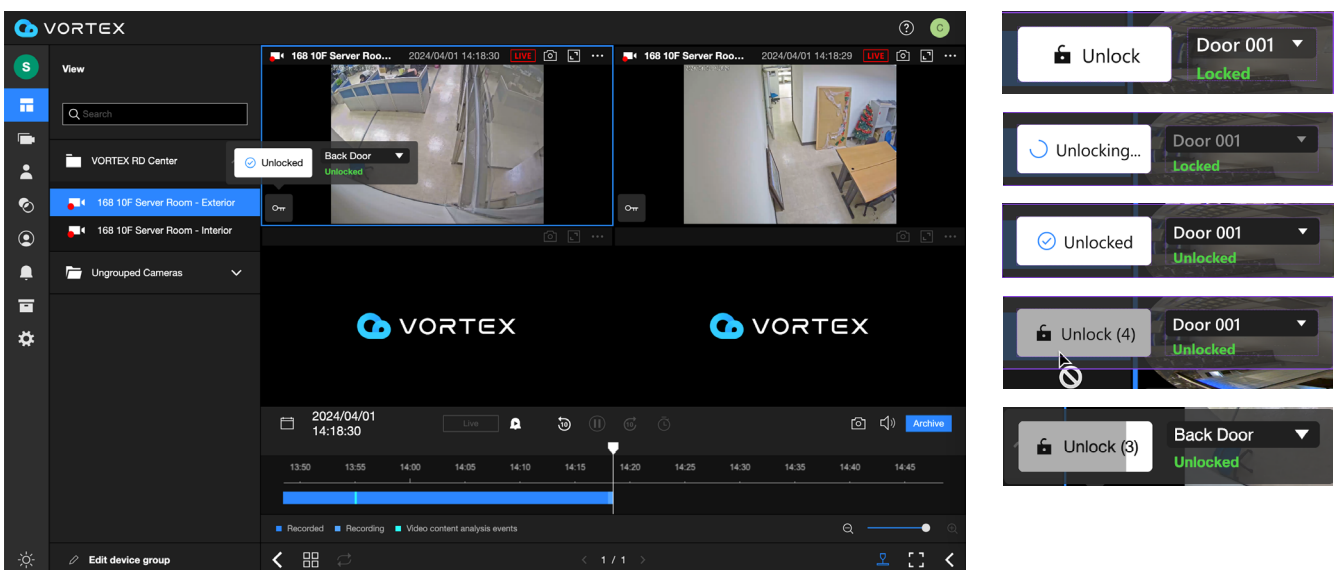
Feature Guide - Web

- 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:
 - Locked
 - Unlocked
 - Locked down
 - 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.

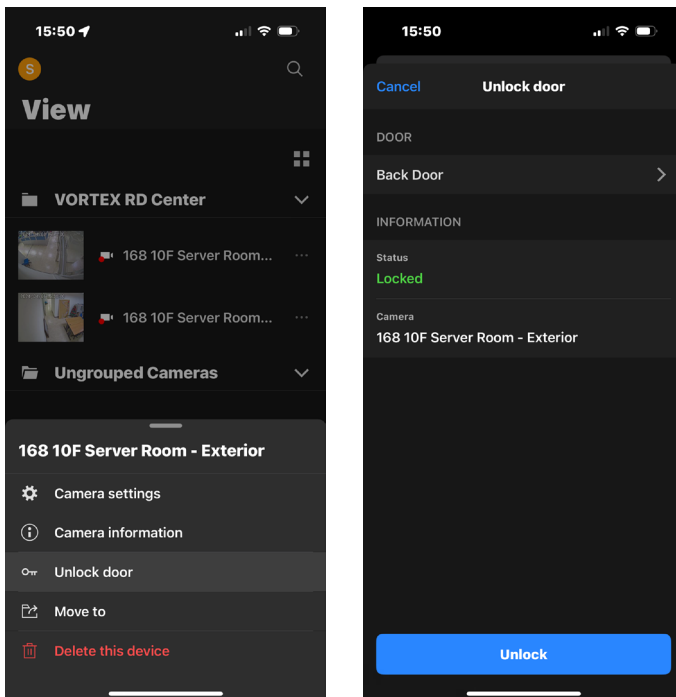
- After clicking the unlock button, one must wait for 7 seconds (including UI response time) before proceeding with the next operation.



Feature Guide – Mobile App

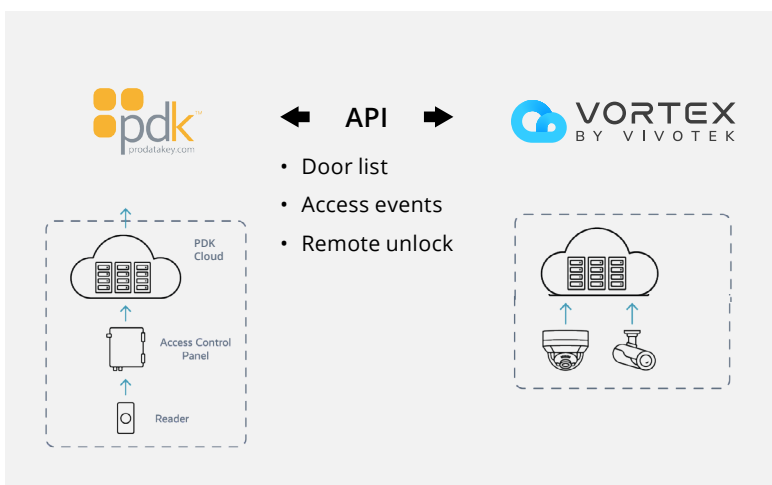
- Go to Live View. Cameras that have been associated with doors display "Unlock door" option in more option.
 - When this camera is associated with multiple doors, a dropdown will appear to select a specific door.
 - The order of Doors within the dropdown is sorted by ASCII.
 - There are 4 Door statuses: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

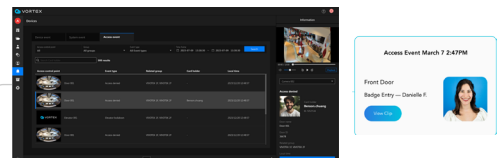


Access control Integration – PDK

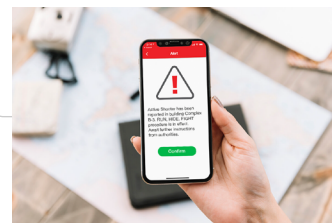
System Overview



- Access Events Integration with Native video



- Real-time Access Event Notification



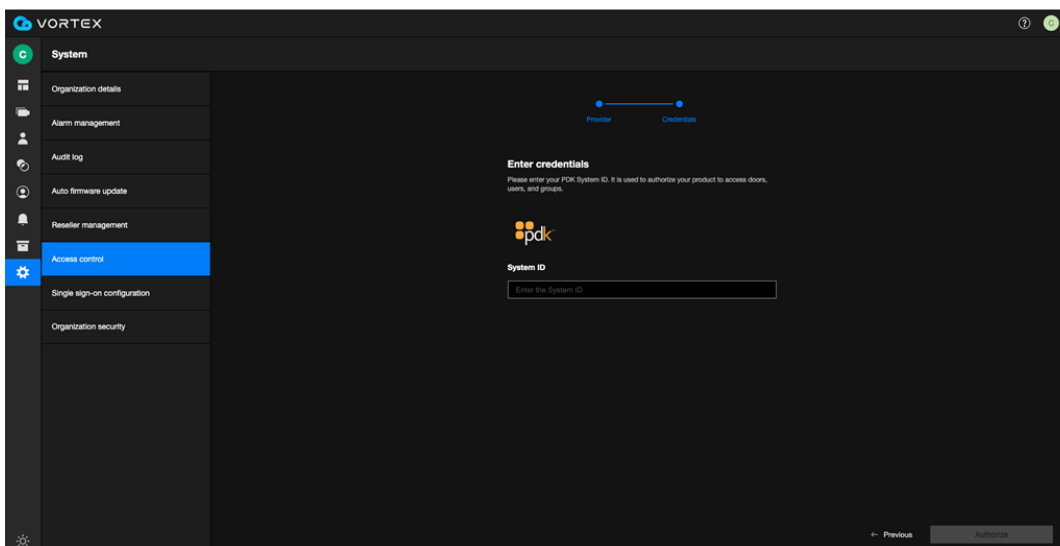
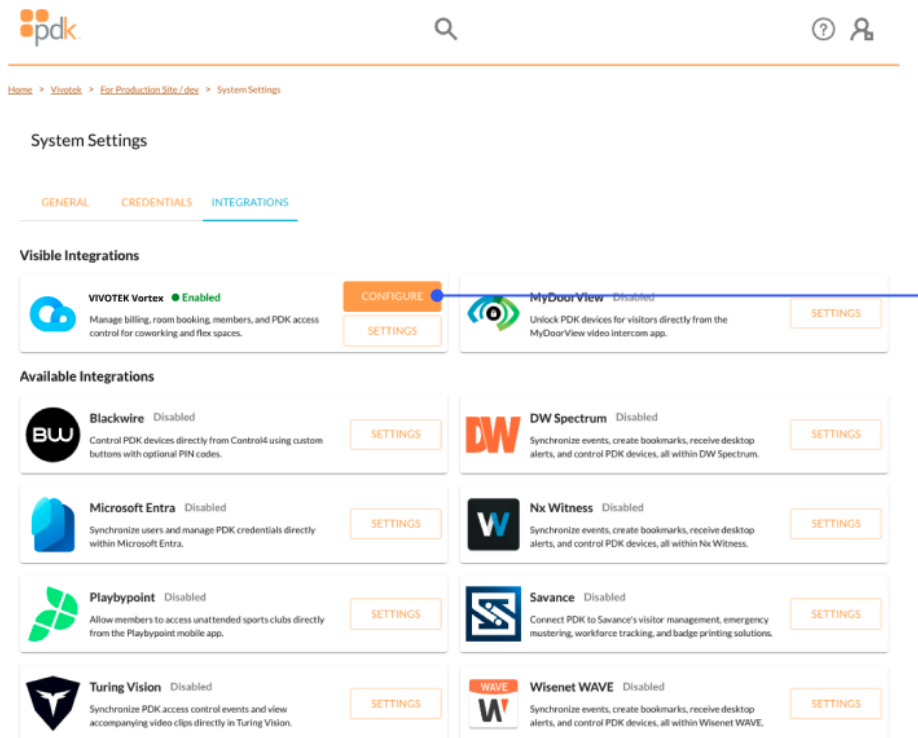
- Remotely Unlock/Lock Doors



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.

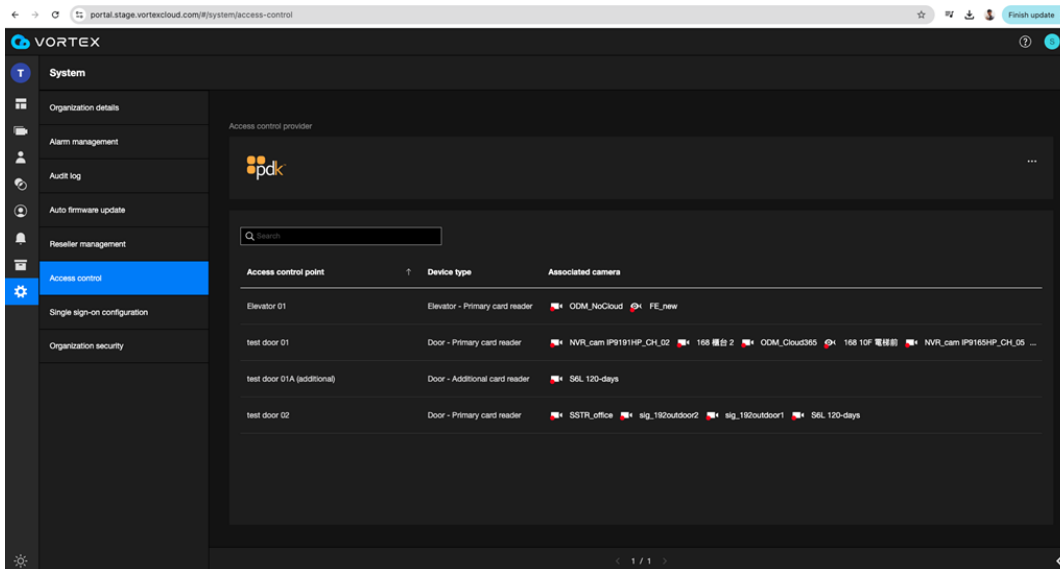
The screenshot shows the PDK beta web interface. At the top, there's a navigation bar with the PDK logo, a search icon, and user profile icons. Below the navigation bar, the breadcrumb trail reads: Home > Vivotek > For Production Site / dev. The main heading is "For Production Site / dev". To the right, a "System and Health" status box shows "Good".

The main content area displays a grid of icons for various system functions: People, Groups, System Events, Auto Open, Elevators, Reports, Partitions, States, Live Events, Permissions, System Settings (highlighted), and Configuration.

Below this grid, the "System Settings" page is shown with the "INTEGRATIONS" tab selected. Under "Visible Integrations", there are two entries: "VIVOTEK Vortex" (Enabled) and "MyDoorView" (Disabled). A blue arrow points from the "CONFIGURE" button of the VIVOTEK Vortex entry to the "MyDoorView" entry. Below this, the "Available Integrations" section lists several other integrations, all marked as "Disabled": Blackwire, DW Spectrum, Microsoft Entra, Nx Witness, Playbypoint, Savance, Turing Vision, and Wisenet WAVE. Each entry includes a brief description and a "SETTINGS" button.

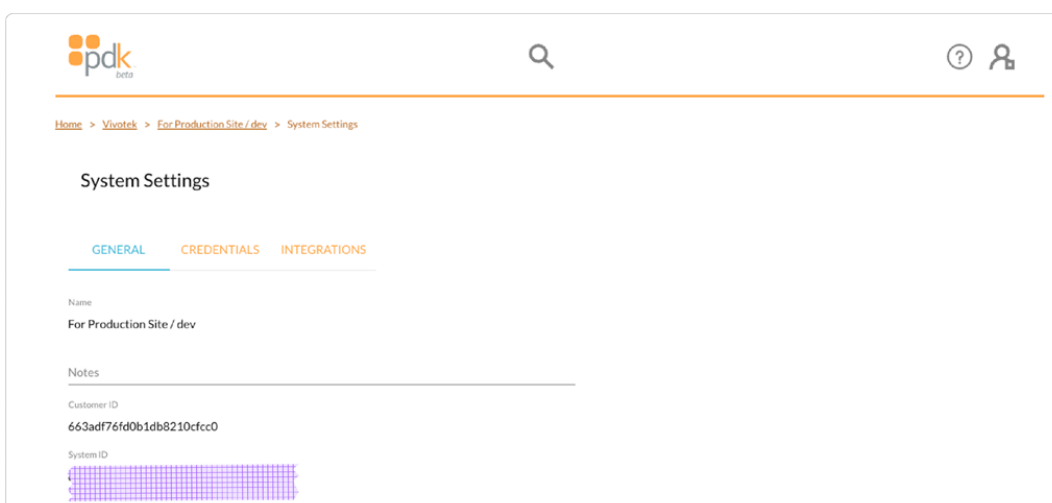
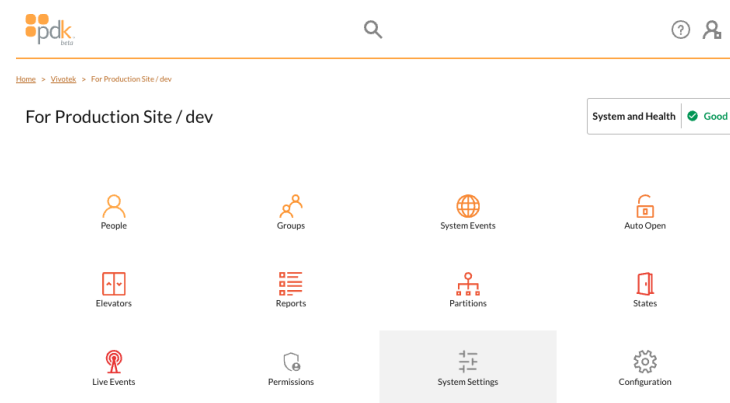
2. Click "CONFIGURE" button to directly complete integration between PDK and VORTEX.

- 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.)



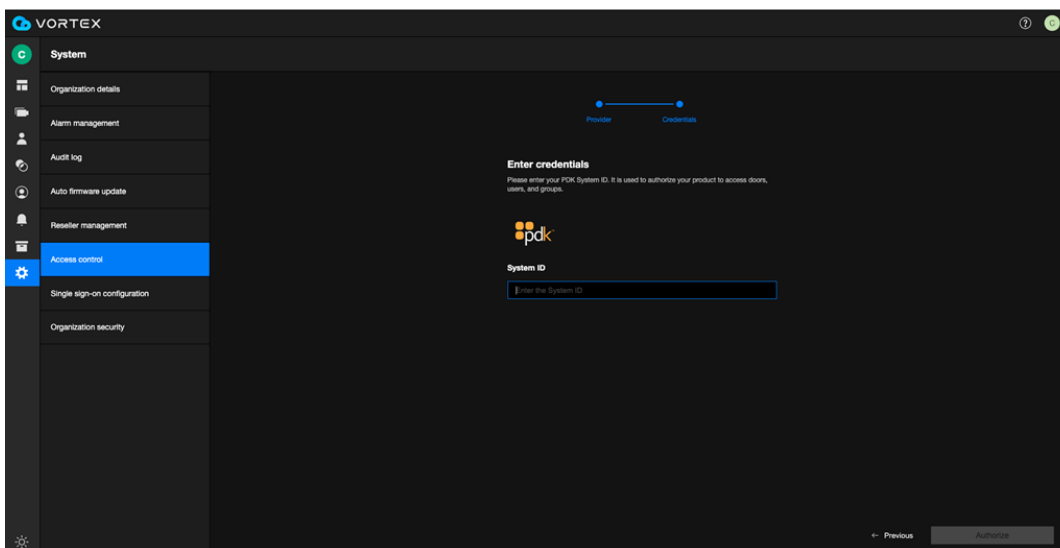
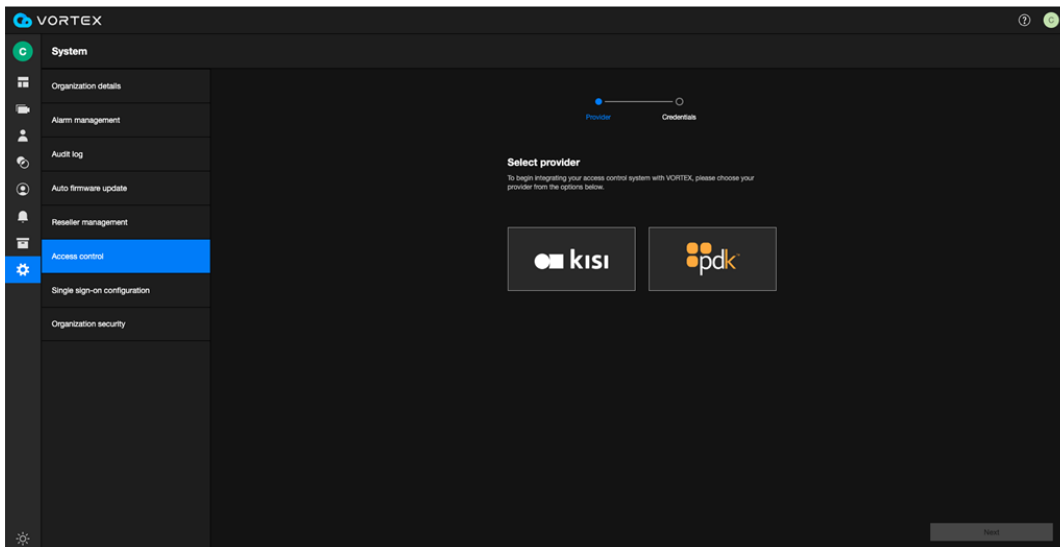
Method B

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.

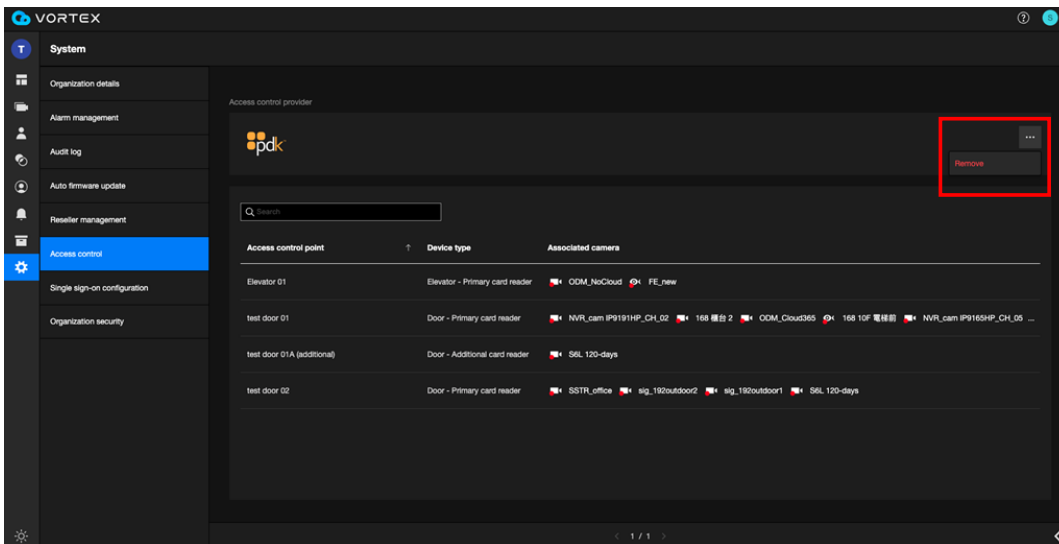
- A single VORTEX Org. can only integrate with one PDK Org.
- A VORTEX org. can only integrate with one access control provider and cannot have both Kisi and PDK integrations at the same time. (This limitation will be addressed once the multi-organizations feature is implemented in the future.)



Delete Integration

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

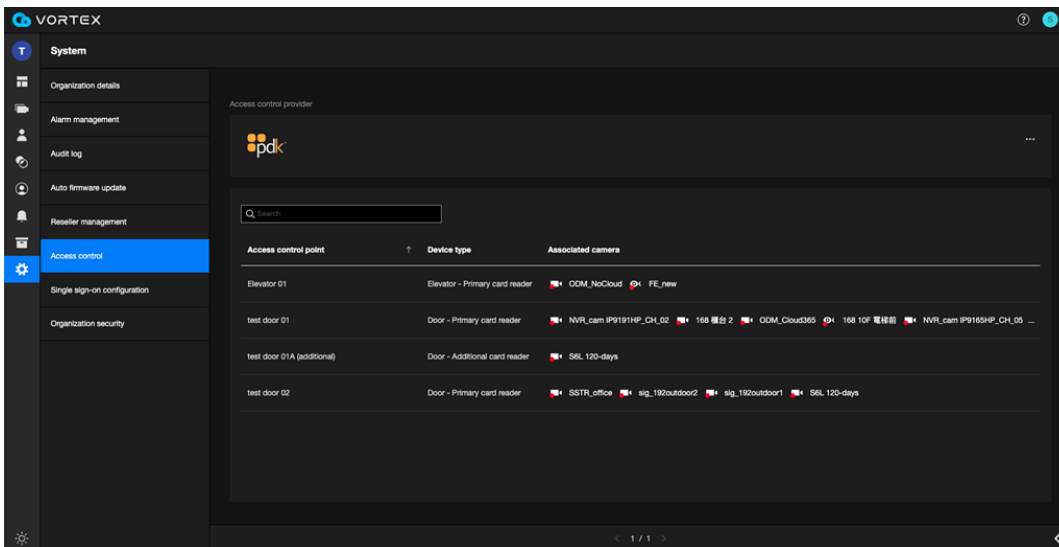
- After the integration is removed, all previously edited settings and access events history will be deleted.



Associate Cameras with Doors

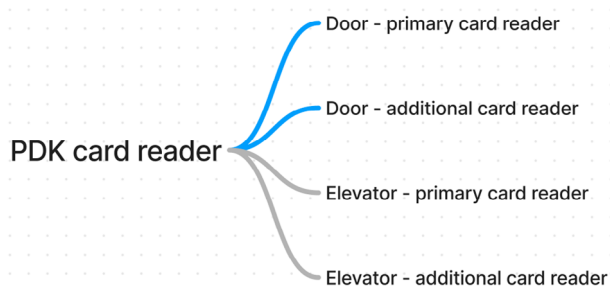
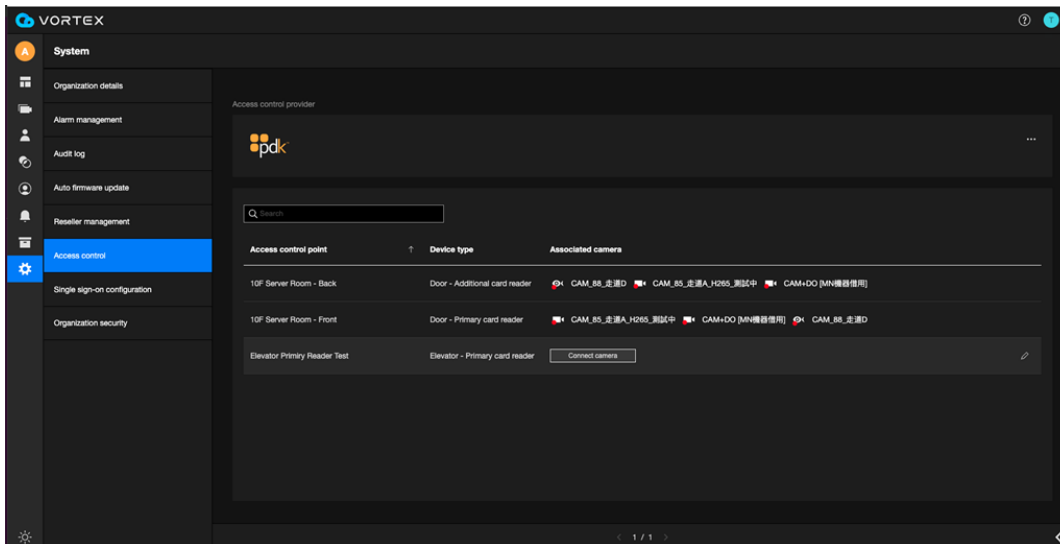
Goal

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"

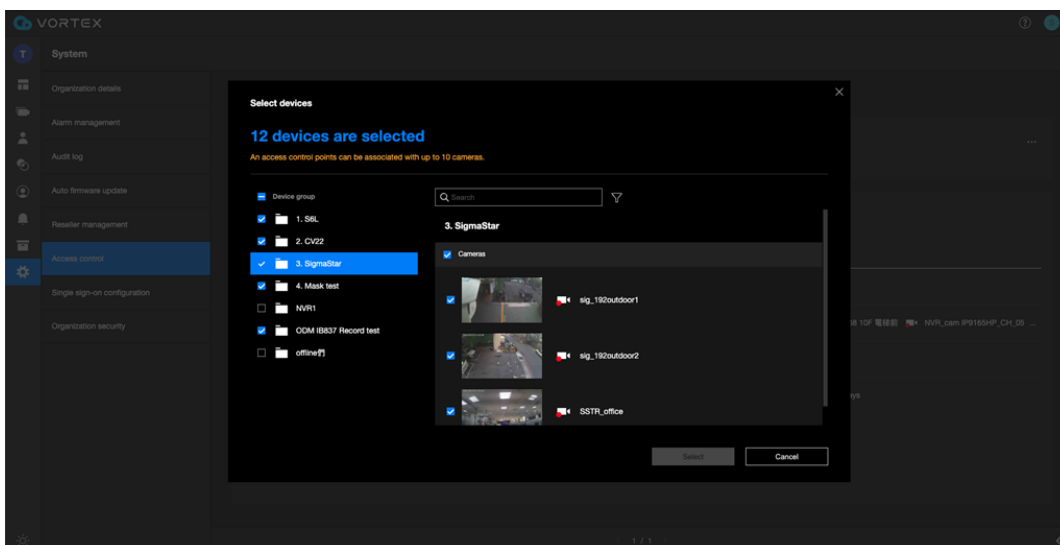
- Only Owner/Admin can operate this function
- This page lists all the doors and elevators in the PDK org
- PDK's Device Type supports both Door and Elevator, and each can be further categorized as Primary or Additional. Learn more details on PDK's Device Type design.



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

Many-to-many design:

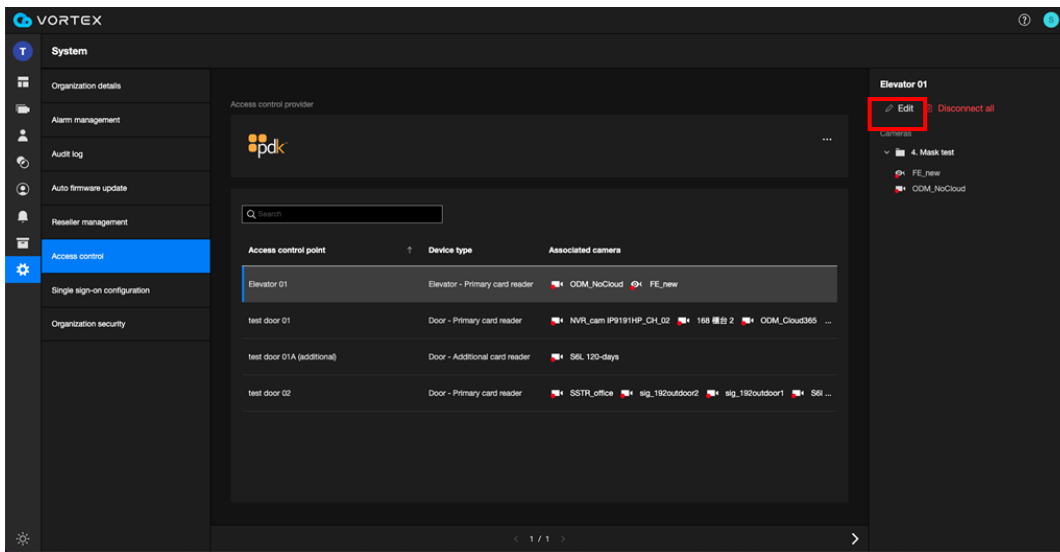
- Each door can be associated with up to 10 cameras.
- The same camera can be associated with multiple different doors at the same time.



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

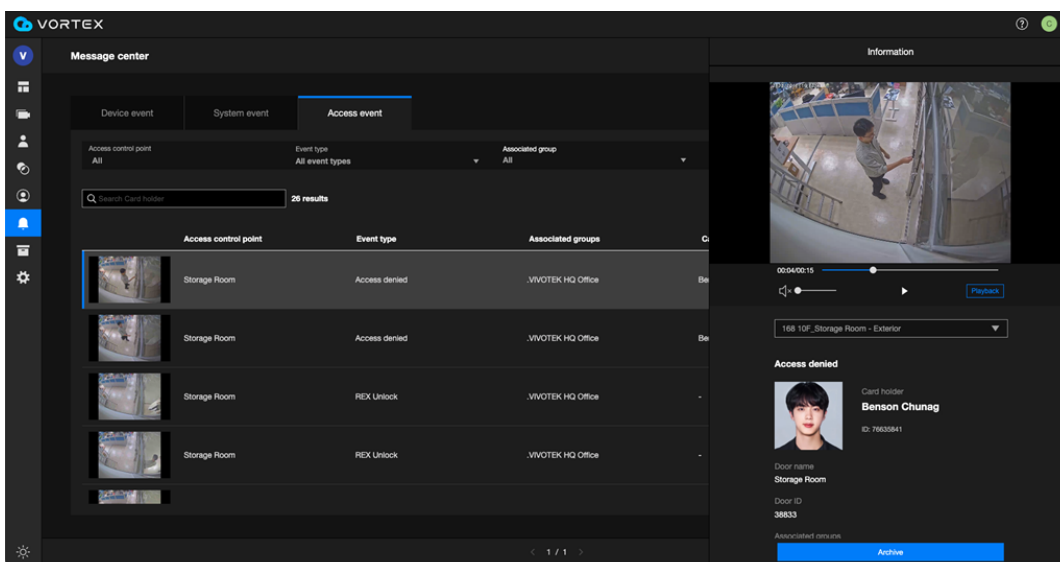
- If users add/edit/delete doors on the PDK platform, VORTEX will reflect the corresponding changes based on the adjustments
- Each time the Owner/Admin enters this page, VORTEX will check if the integration with PDK is functioning properly. If the integration is interrupted, an error message will be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



Access Events Integration with Native Videos

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 lockdown	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	

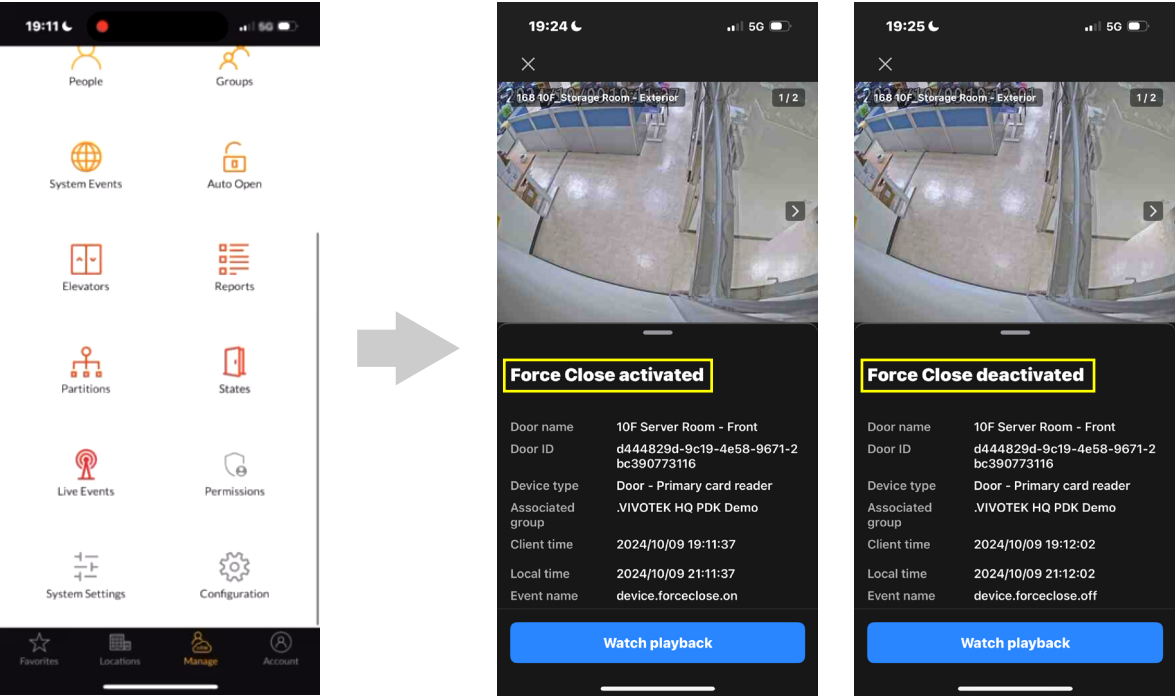
PDK Event Types

	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 • Lockdown • 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.

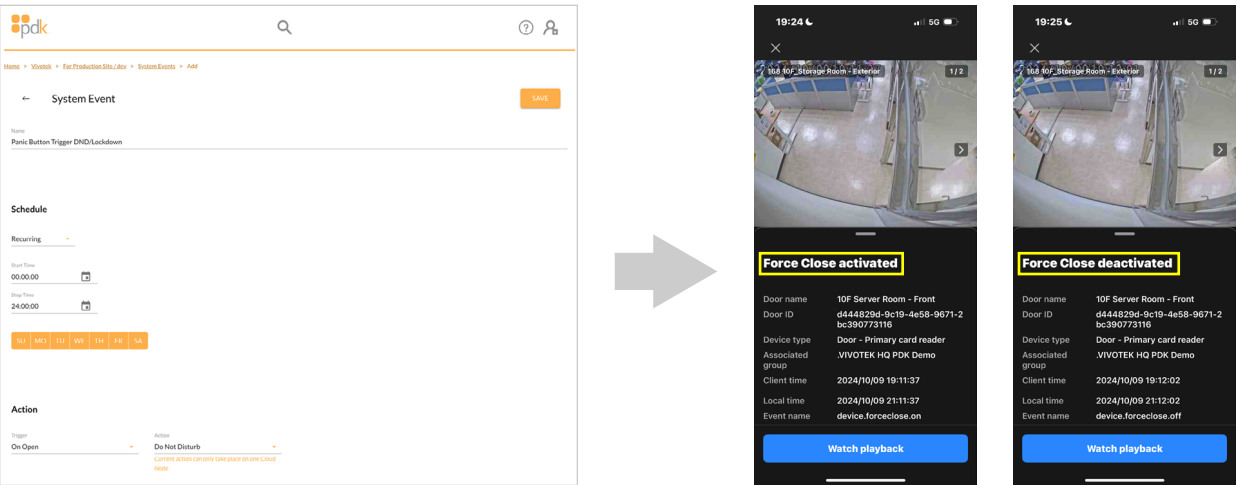


VORTEX Received and Display the Event

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.

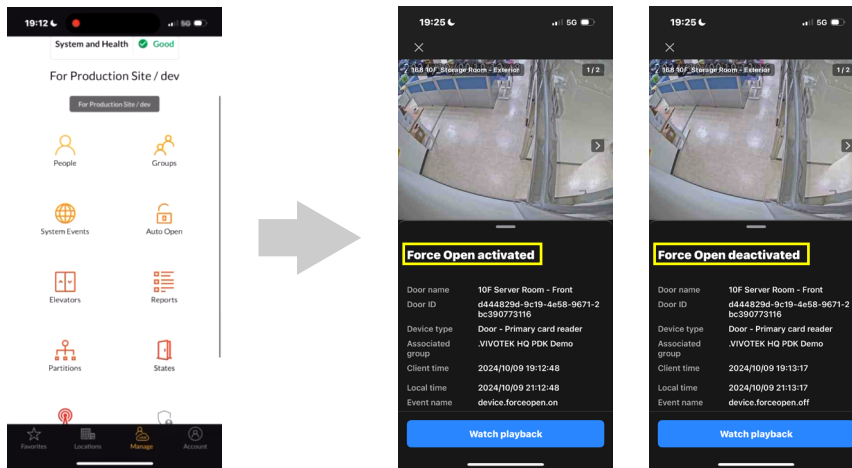


VORTEX Received and Display the Event

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.

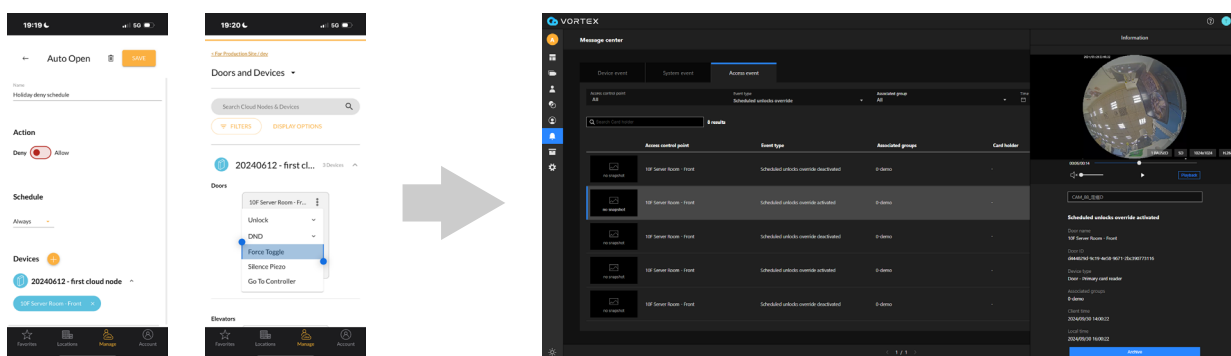


VORTEX Received and Display the Event

PDK Exclusive Event - Scheduled Unlocks Override (by App Activation)

App Activation - "Force Toggle"

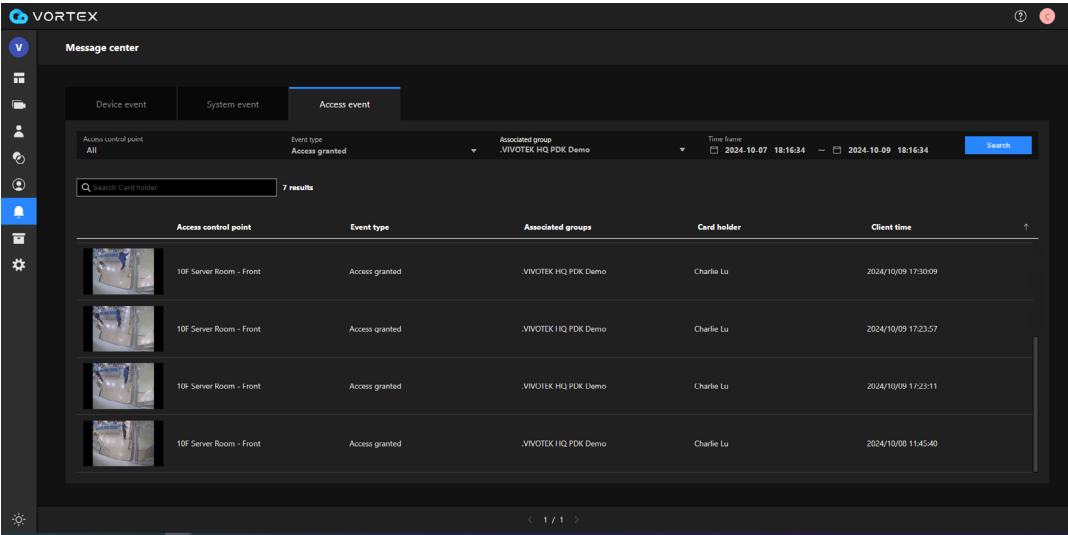
- **Scenario:** When the Auto Open Schedule is manually overridden, the system sends a notification to remind the user. For example, a school might set an Auto-Open Deny Schedule on a national holiday to prevent anyone from entering. However, if there's an urgent maintenance task requiring access, the 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.



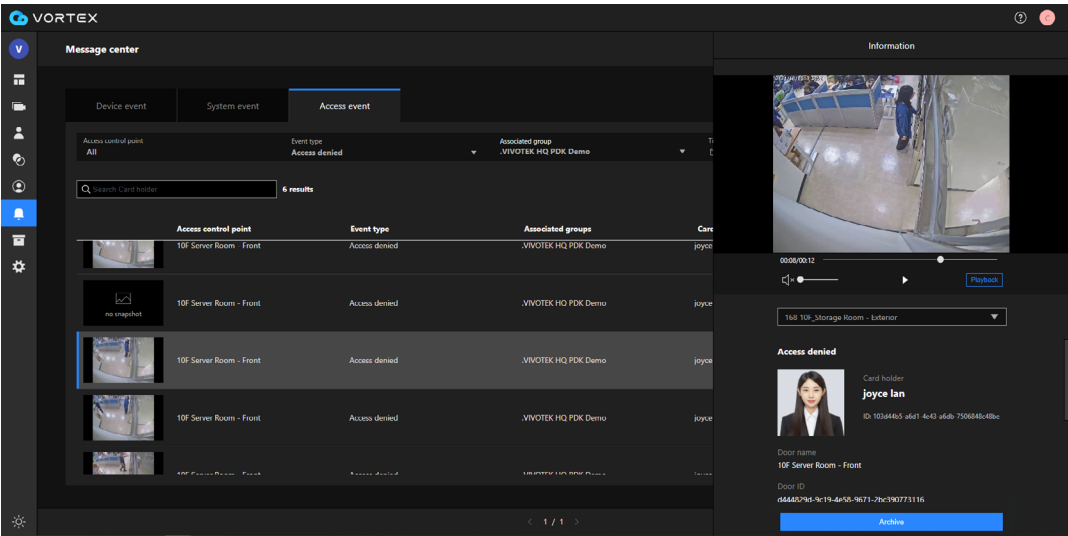
VORTEX Received and Display the Event

View Access Event in Message Center

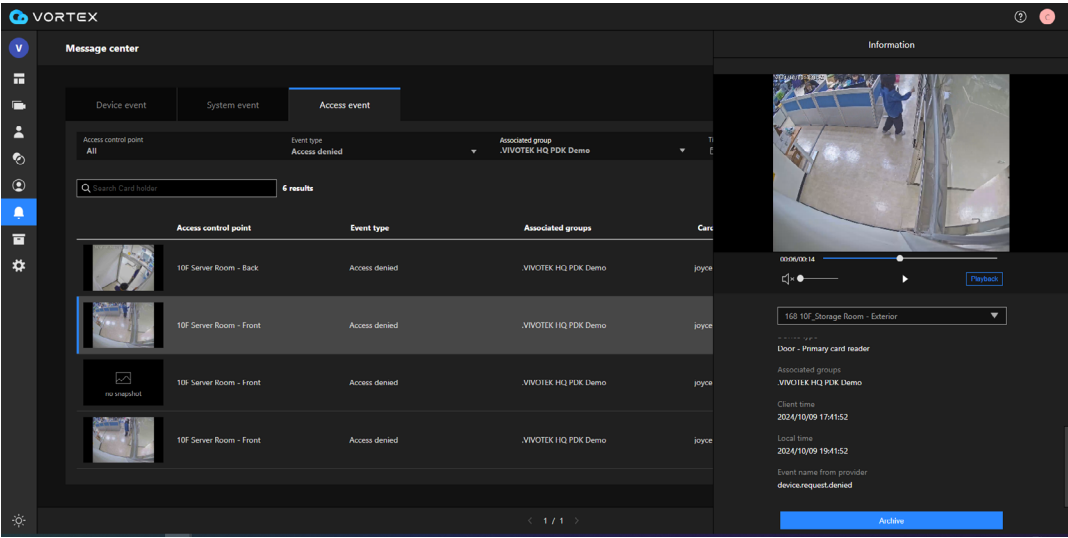
1. Go to Message Center and select "Access event" tab. You can search for the event types you want to see, the groups they belong to, the time range, and the card holder by setting filter criteria.
 - The retention period for event logs is one year. Camera playback footage is accessible for a minimum 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).



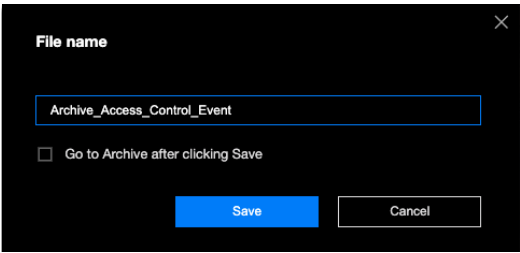
2. Select an access event and view both the surveillance and access event data simultaneously through the camera footage and the event info below.
- If this door is linked to multiple cameras, you can choose a specific camera through the dropdown options below the footage.
 - For events not triggered 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.

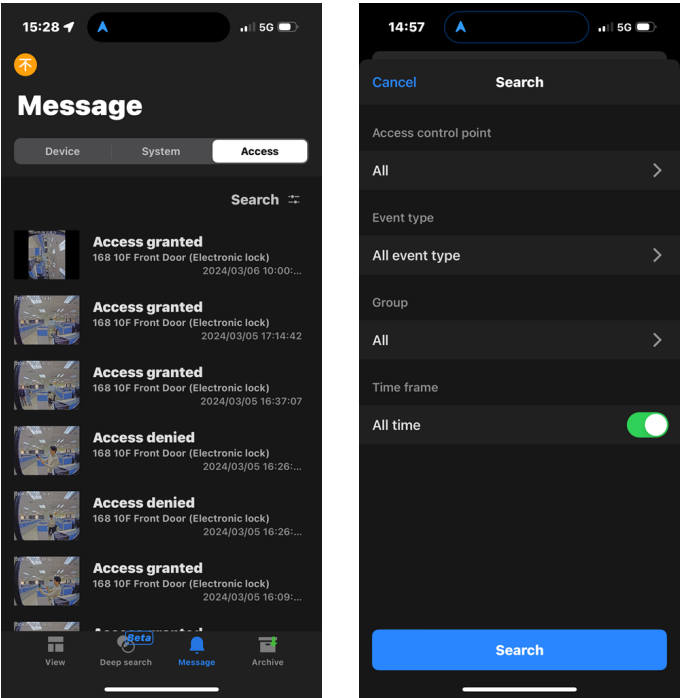


4. You can view the footage through playback, or archive this event footage and sharing with others

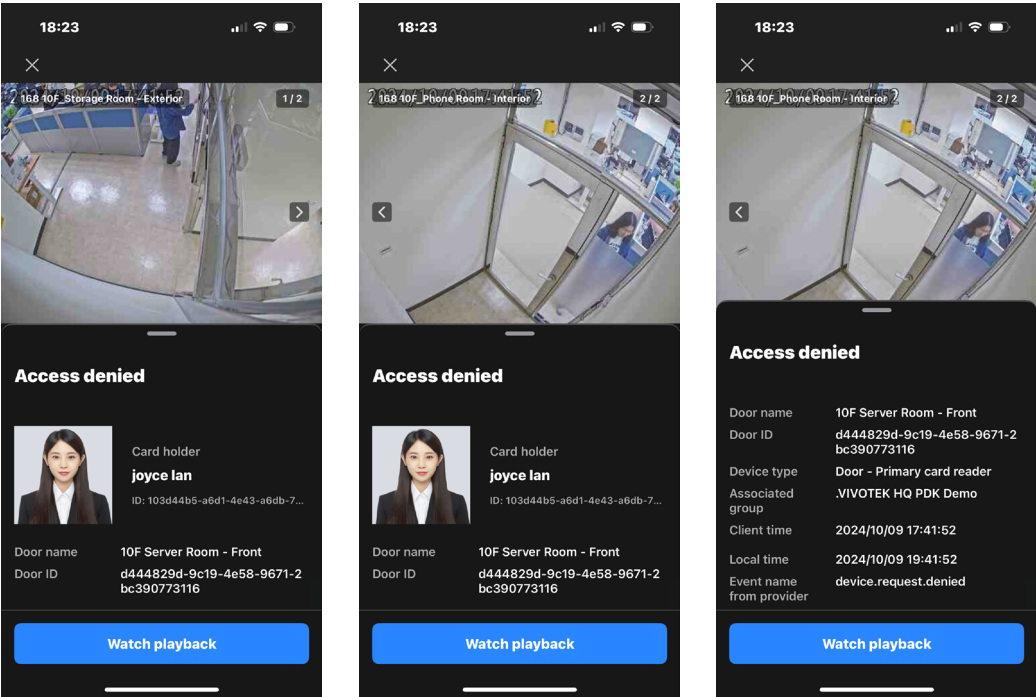


Mobile App

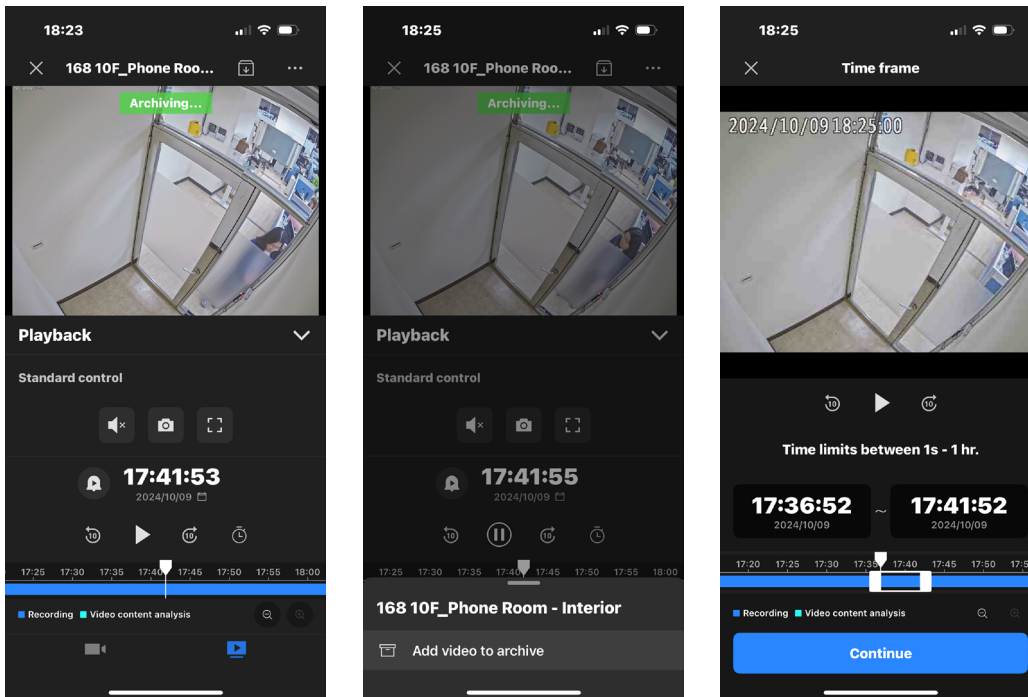
1. Go to Message Center and select "Access event" tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
 - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with 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.



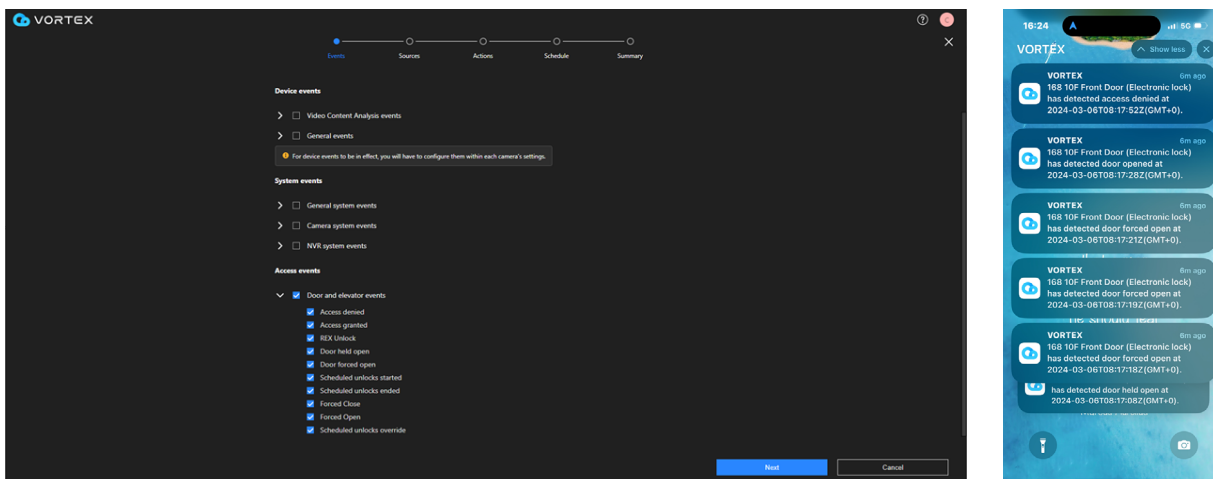
3. You can view the footage through playback, or archive this event footage and sharing with others.



Alarm Settings and Real-Time Notifications

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.

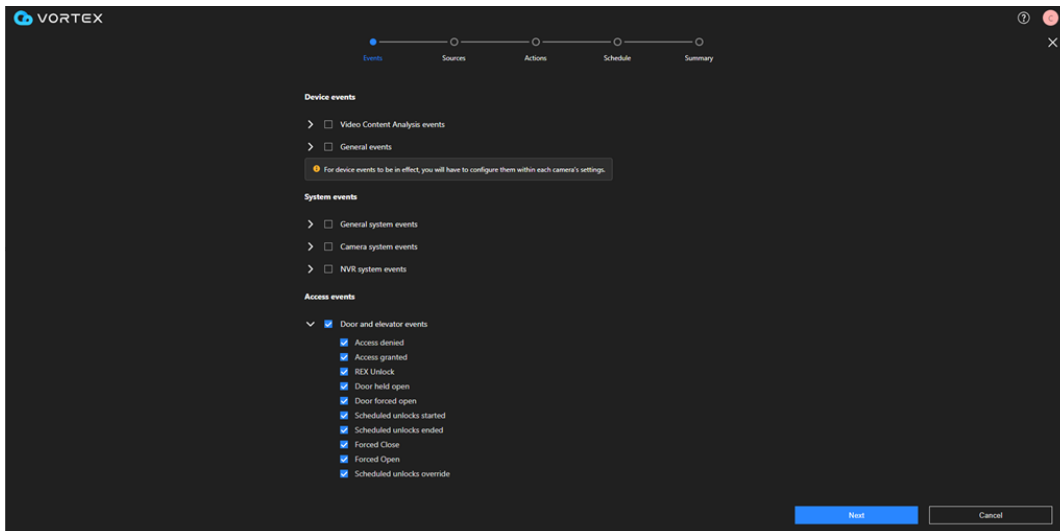


Web Portal

1. Go to System > Alarm Management > Add alarm

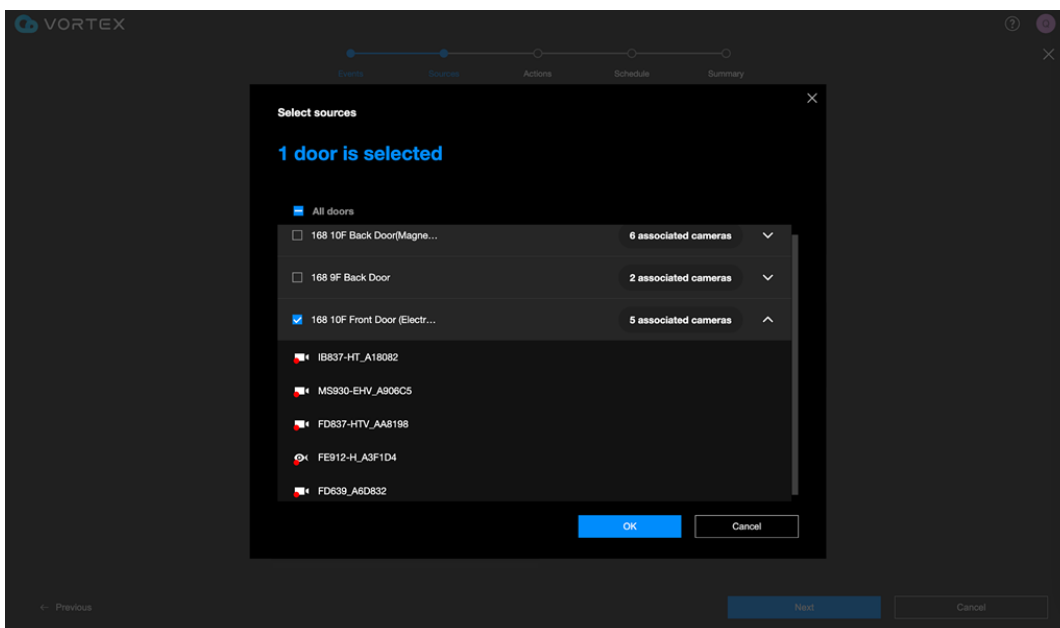
- The design logic here is the same as the existing Alarm Management, with the difference being the addition of the Access event.

- 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).



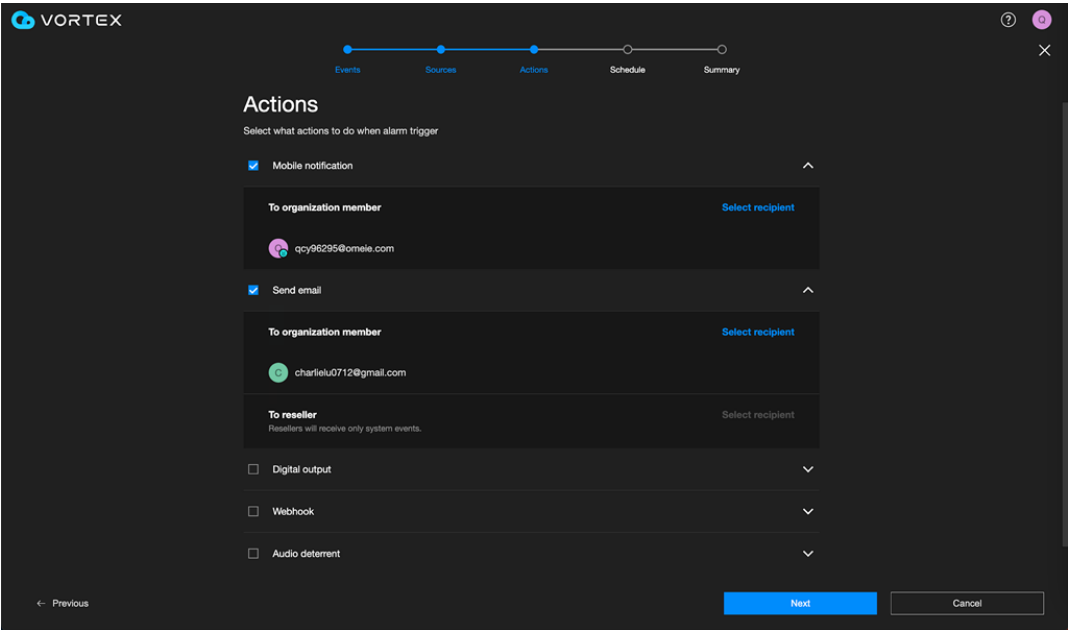
2. In the next step - Sources, select the doors that initiate Access events.

- 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.

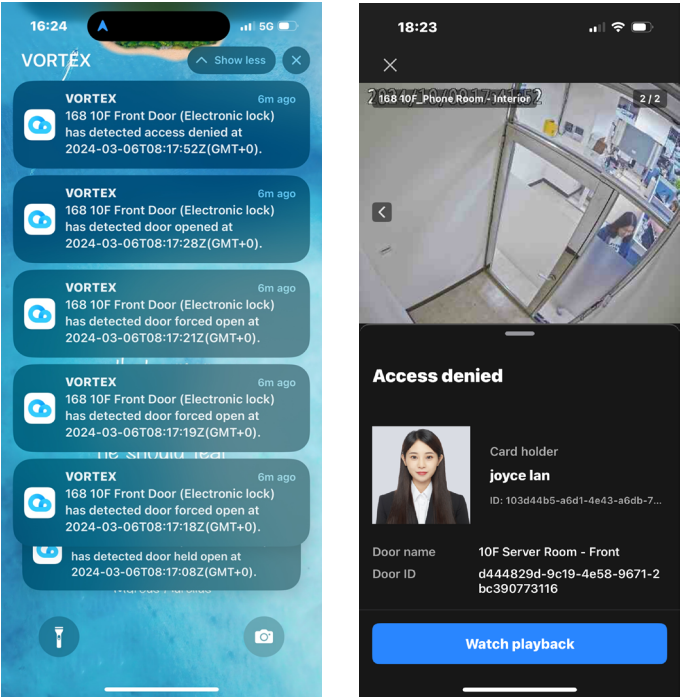
- The design logic here is the same as the existing Alarm Management.
- Access events only support Mobile notification and Send emails. Other Actions are not supported.
- The remaining steps, Schedule and Summary, follow the same design logic and operate in the same manner as they currently do.



Mobile App

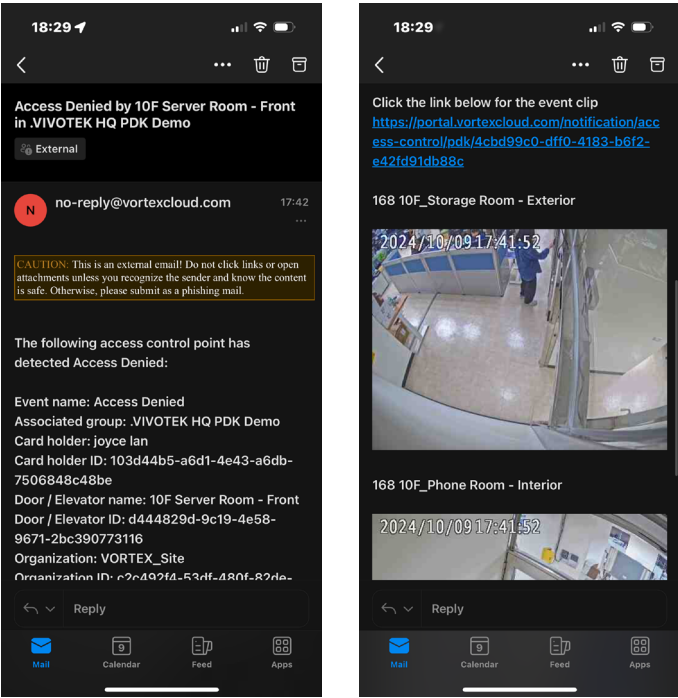
Designated personnel received real-time push notification.

- 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.

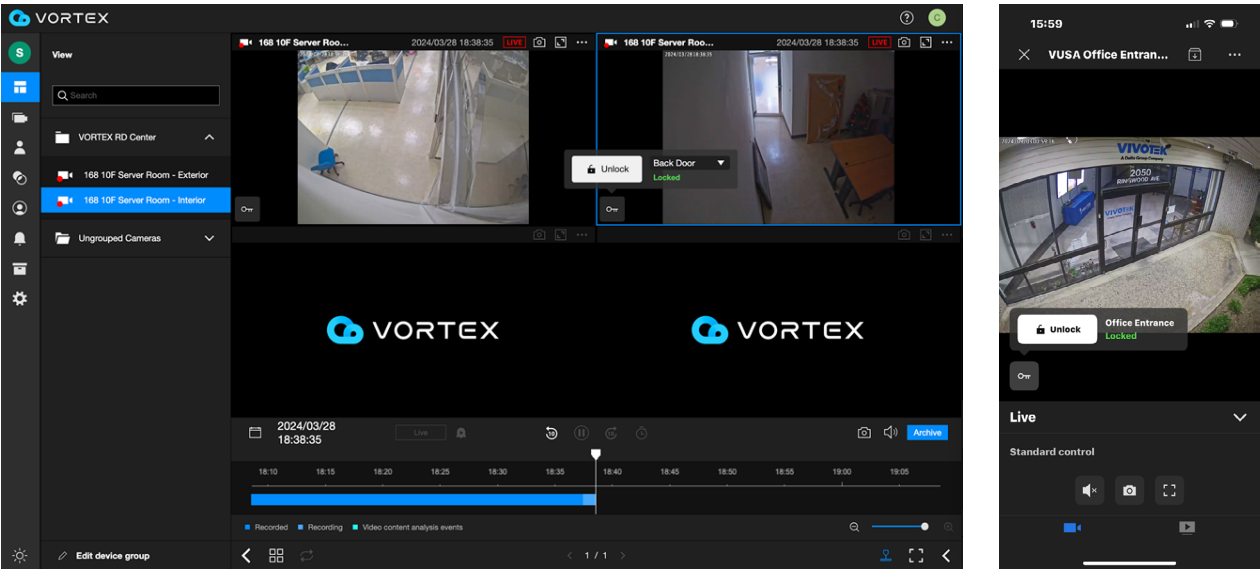
- If a door is associated with multiple cameras, the email will display snapshots from these cameras.



Remote Unlock/Lock Doors

Goal

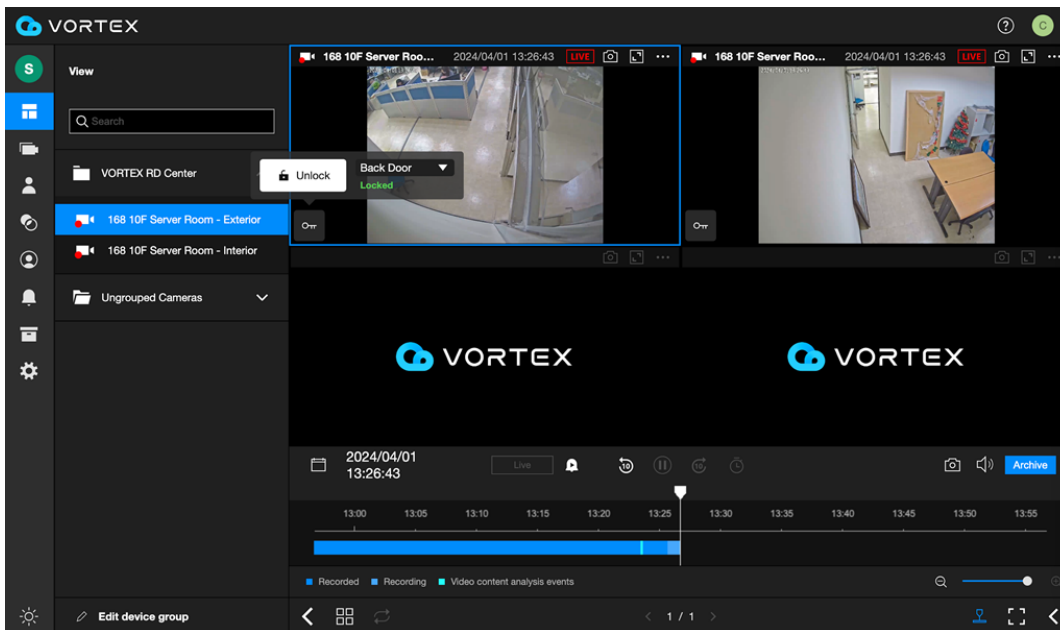
Allow owner/admin/supervisor to assist with daily access needs remotely and manage doors during emergency situations without having to be physically present on-site.



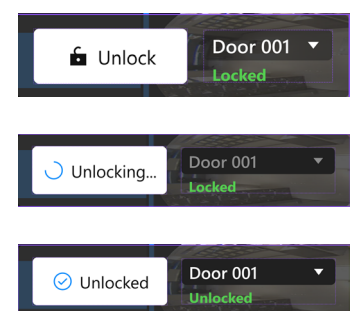
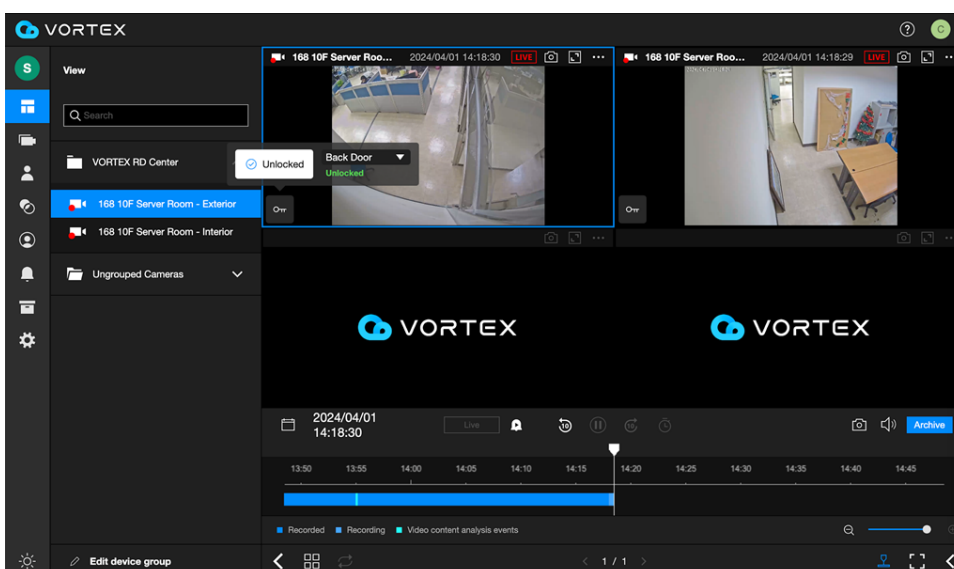
Web Portal

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).

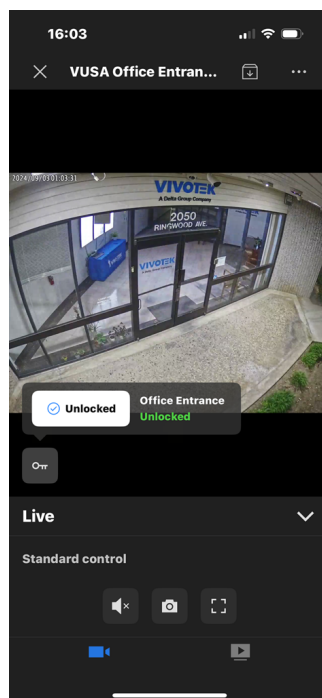
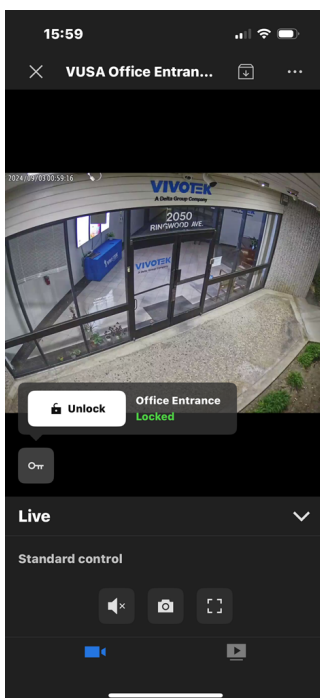


2. Click on the unlock/lock button on the door you wish to operate the remote door management.
 - If the door is in a locked status, the button will display 'Unlock'. Conversely, if the door is in an unlocked status, the button will display 'Lock'.
 - After clicking the unlock or lock button, an UI effect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



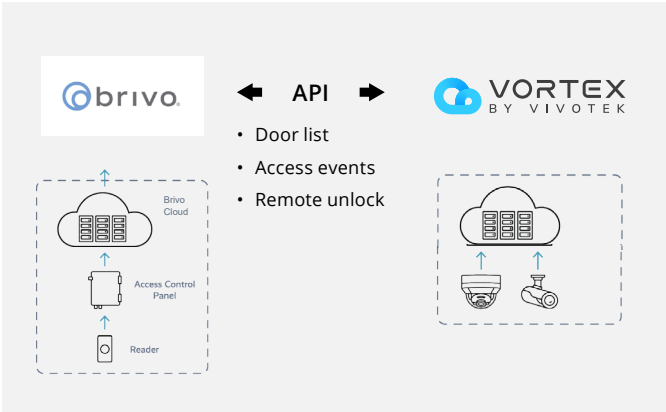
Mobile App

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'.

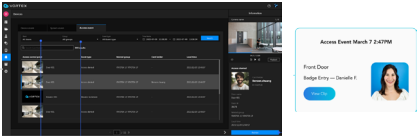


Access Control Integration – Brivo

System Overview



• Access Events Integration with Camera Video



• Real-time Access Event Notification



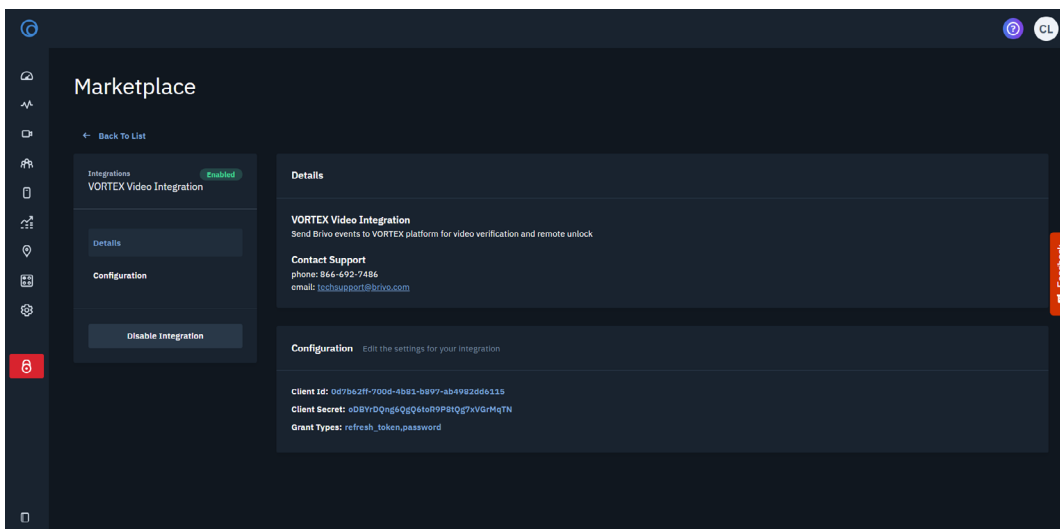
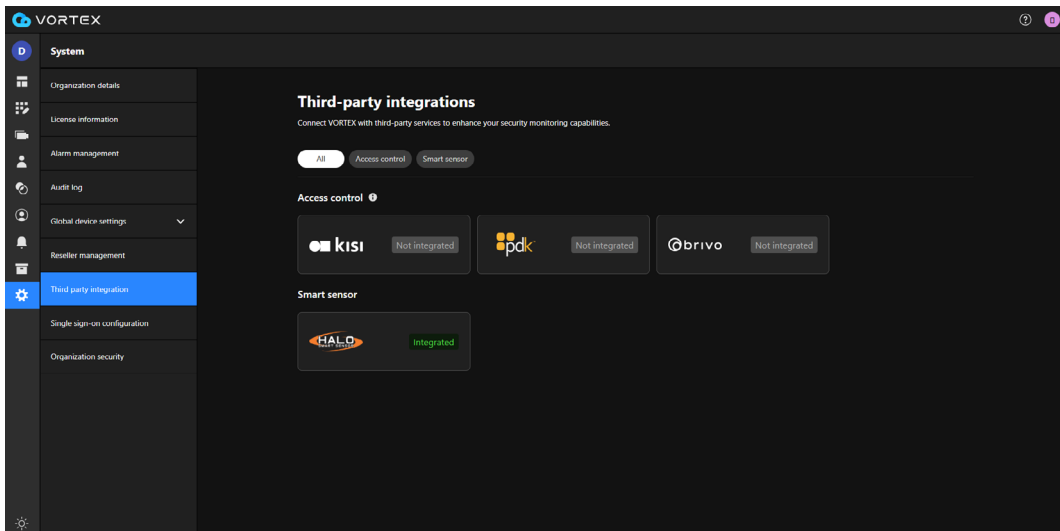
• Remote Unlock / Doors



API Integration

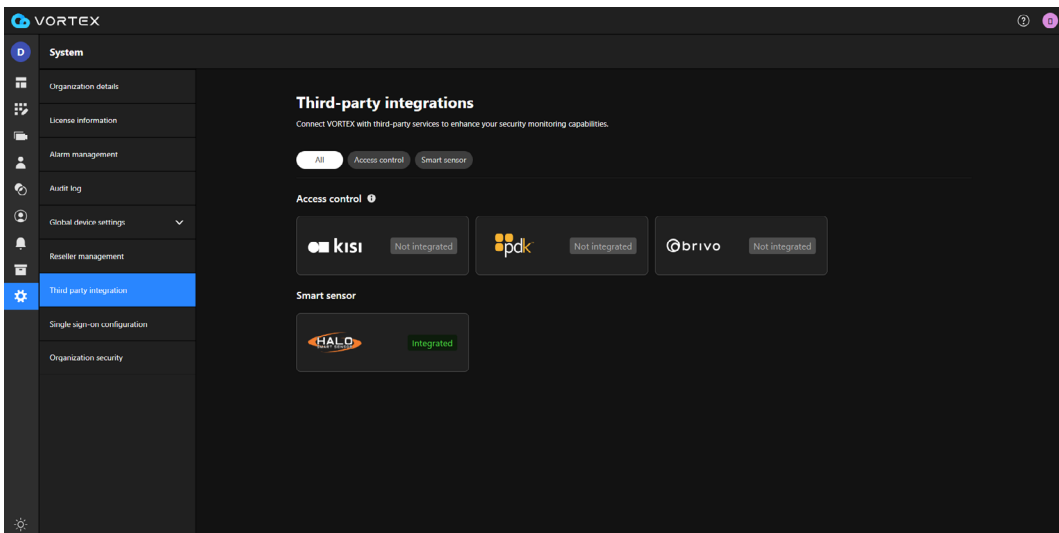
Goal

Enable VORTEX to retrieve the list of Brivo's doors and access events; allow control of Kisi's doors through VORTEX.

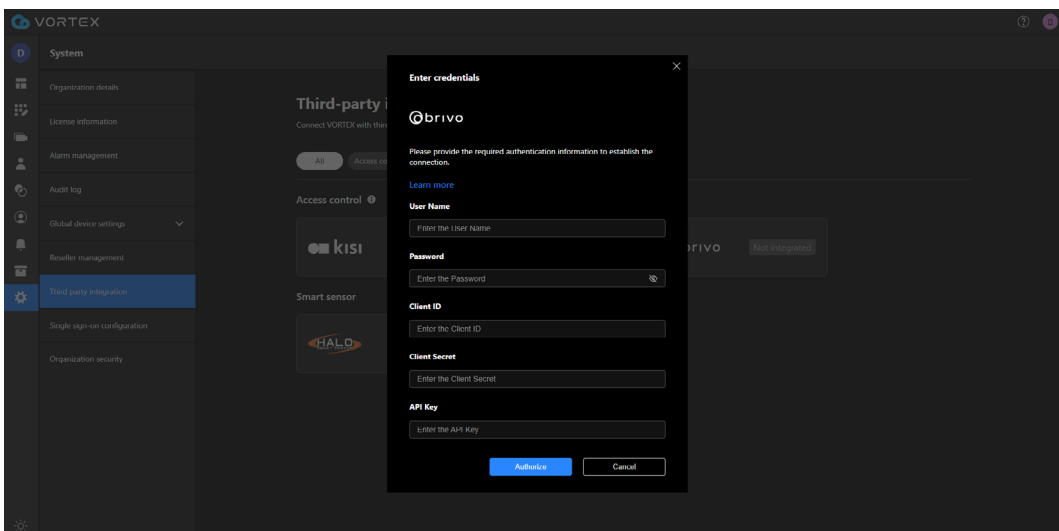


Feature Guide

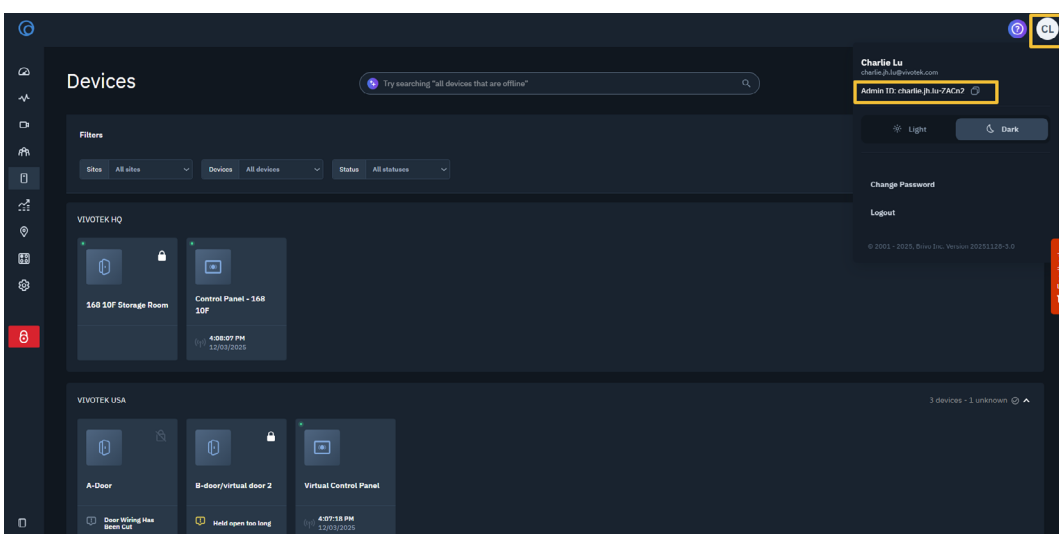
1. Go to System > Third party integration and select Brivo.



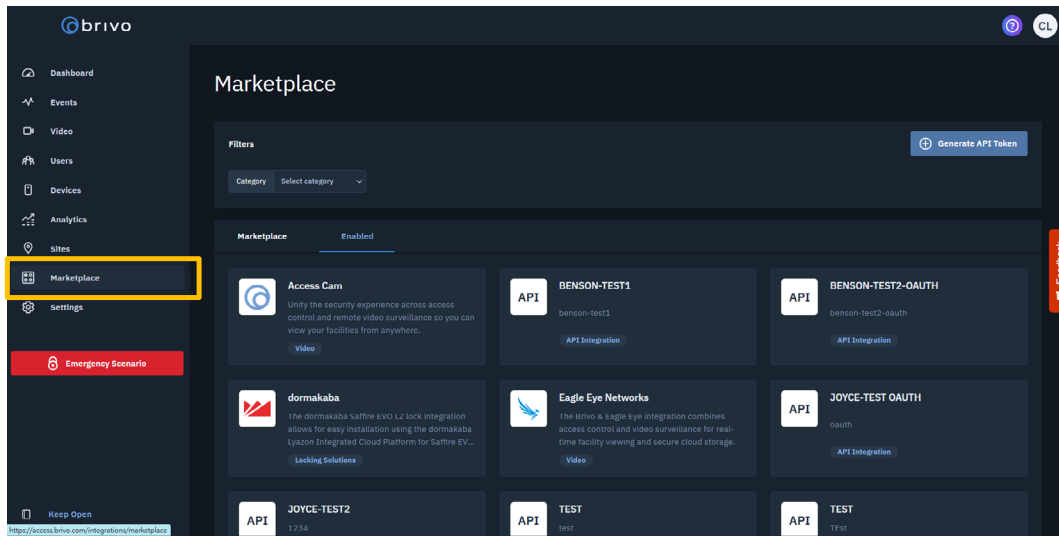
2. Go to Brivo portal for obtaining your User Name(Admin ID), Client ID, Client Secret.



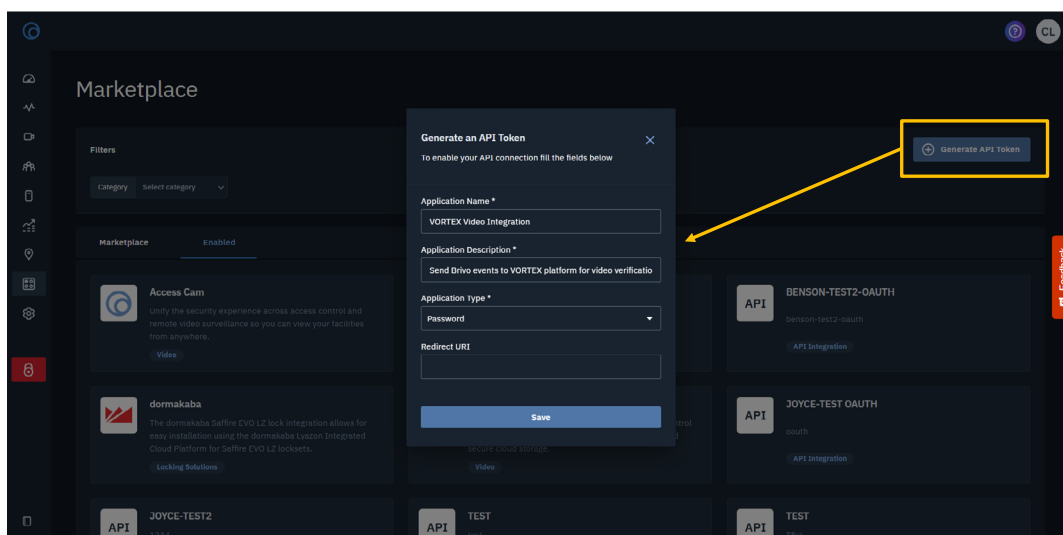
3. In the Brivo portal, click your avatar in the top-right corner. Copy your Admin ID and paste it into the User Name column in VORTEX.



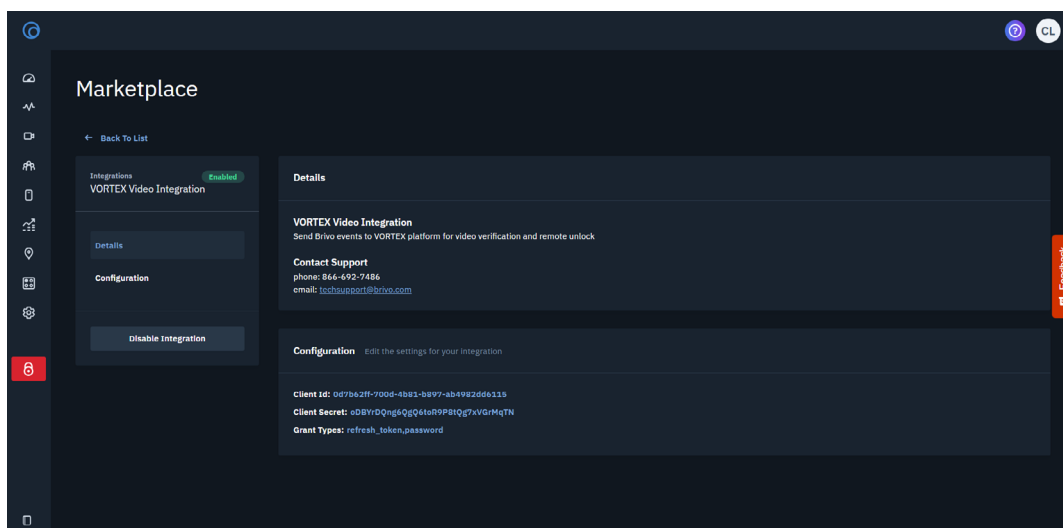
4. To obtain your Client ID and Client Secret, first go to the Marketplace.



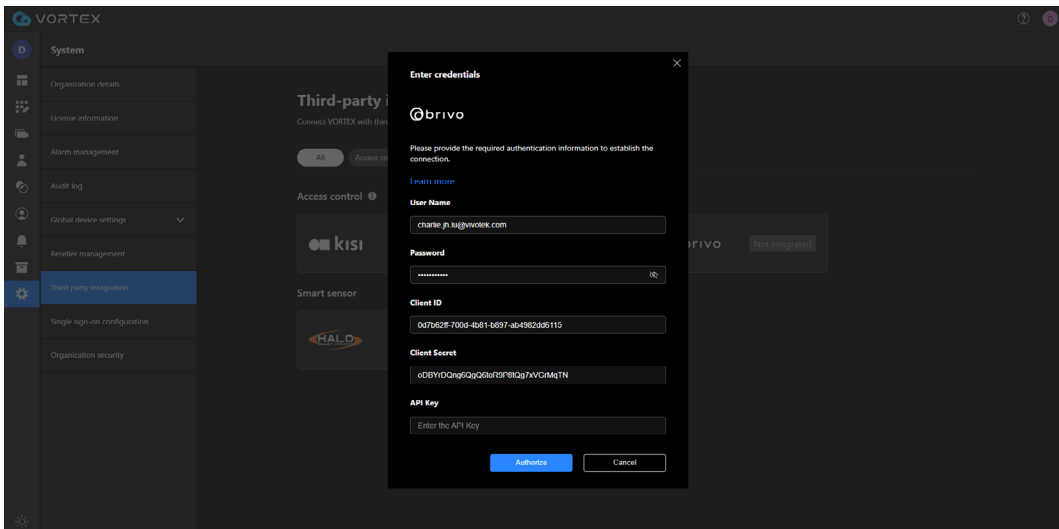
5. Click “Generate API Token,” enter your desired Application Name and Application Description, select **Password** in **Application Type** dropdown, and click “Save.”



6. Select the Application you just created. Copy the **Client ID** and **Client Secret** and paste them to VORTEX.



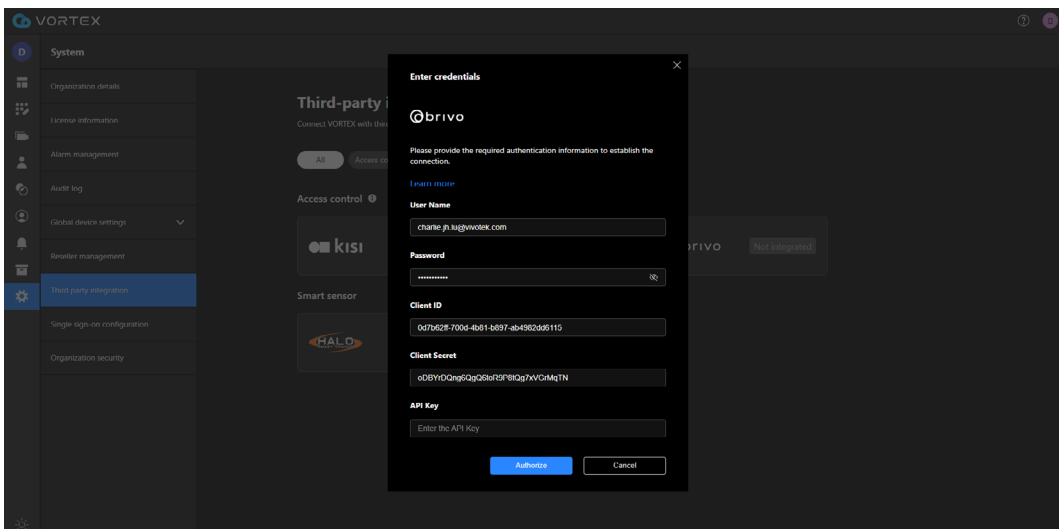
7. To obtain your Client ID and Client Secret, first go to the Marketplace.



8. Contact your Brivo dealer to receive an API Key via email reply. Enter your API Key here and click Authorize button to complete the setup.

{User},

The Brivo Onair API has been enabled on your account. Your API key is:



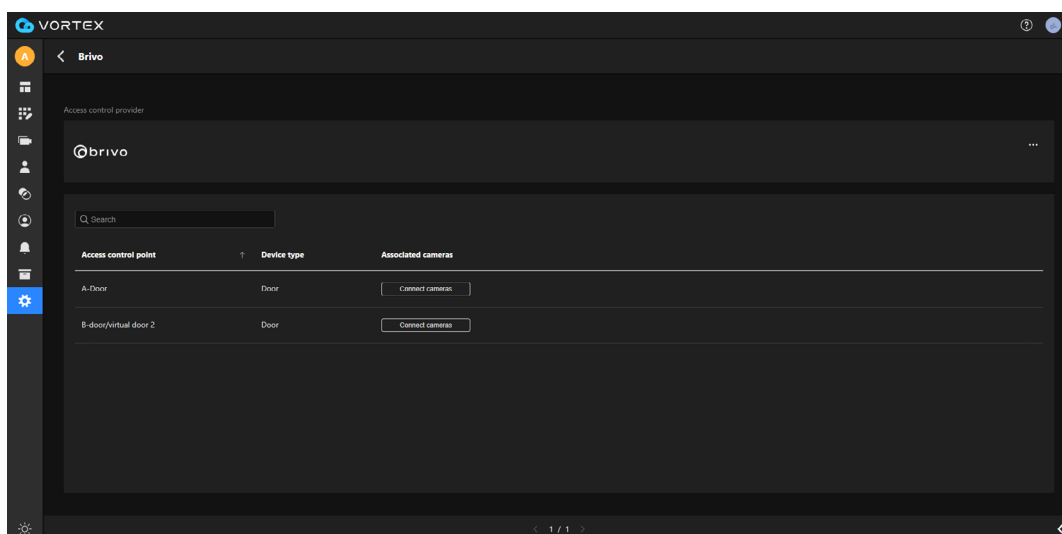
- For internal testing, you may directly use the below Brivo Access API Key obtained through the VORTEX PM: seegbccafv8mmgz5a4getn7q
- Alternatively, you can register on the Brivo developer site below to obtain your own Brivo Access API Key: <https://developer.brivo.com/apps/mykeys>

NOTE

- Brivo Access Api usage may carry an additional fee.
- Brivo grants 100,000 Api calls a month.

For details regarding Brivo Access API subscription fees and other information, end-users should contact their SI or Brivo directly.

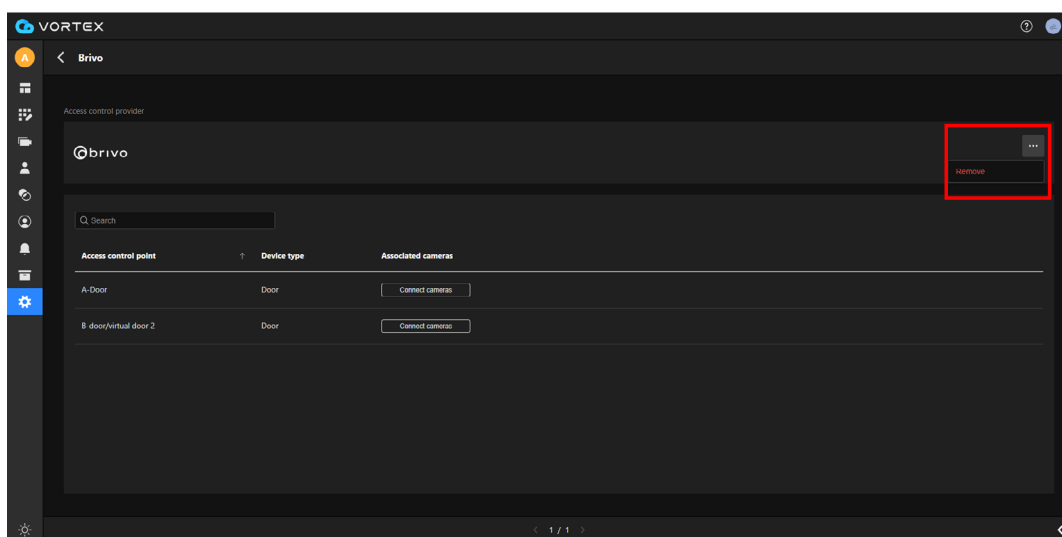
9. Once completed, the access control points(doors) from your Brivo portal will appear on this page immediately.



Delete Integration

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

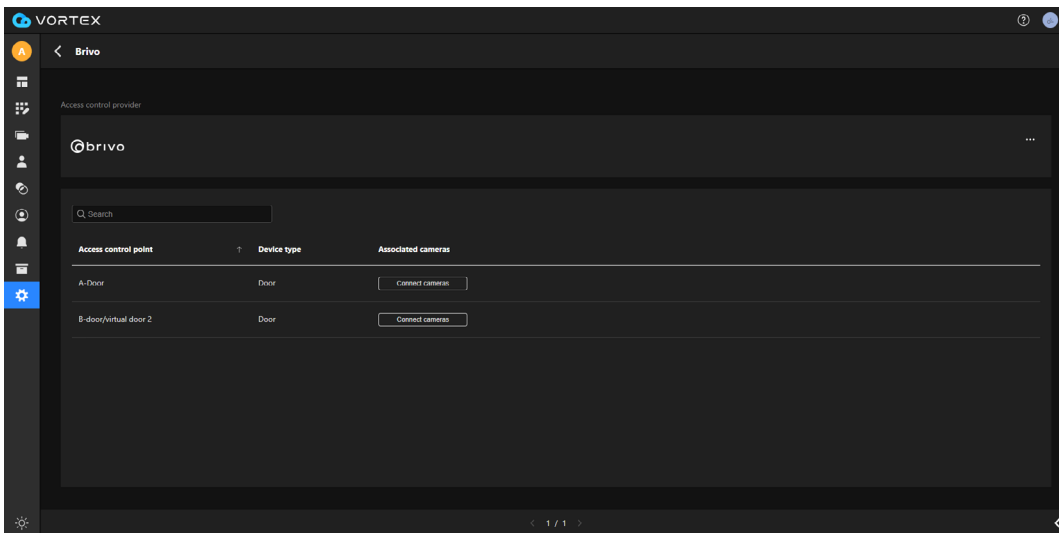
- After the integration is removed, all previously edited settings and access events history will be deleted.



Associate Cameras with Doors

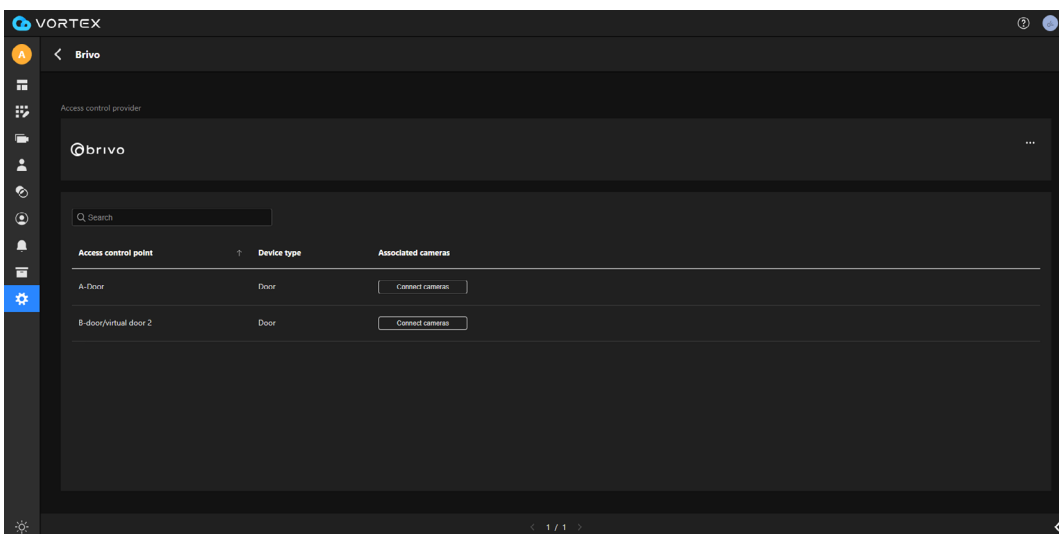
Goal

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



Feature Guide

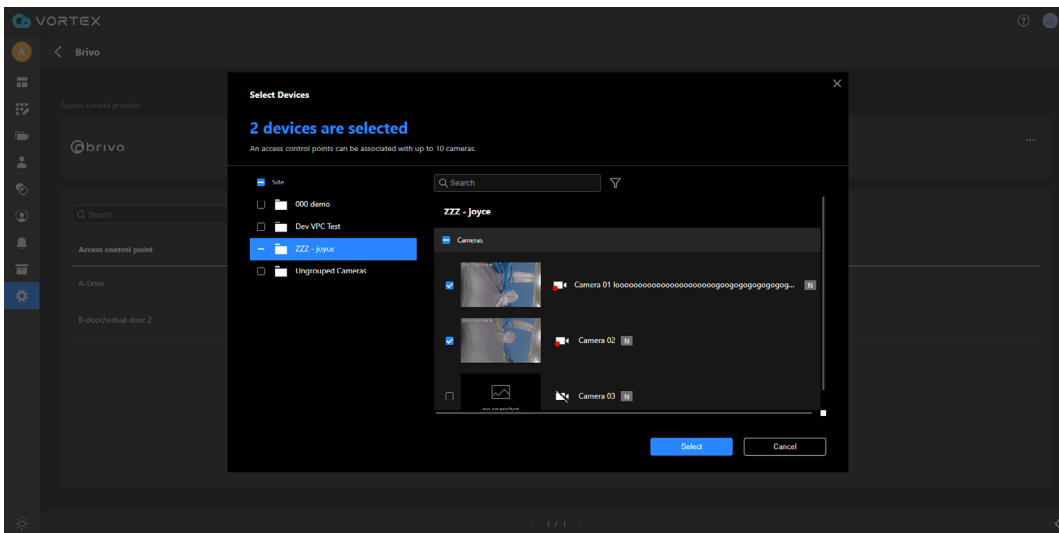
1. On the door you want to associate, click "Connect camera."
 - Only Owner/Admin can operate this function.
 - This page lists all the doors in the Brivo org.



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

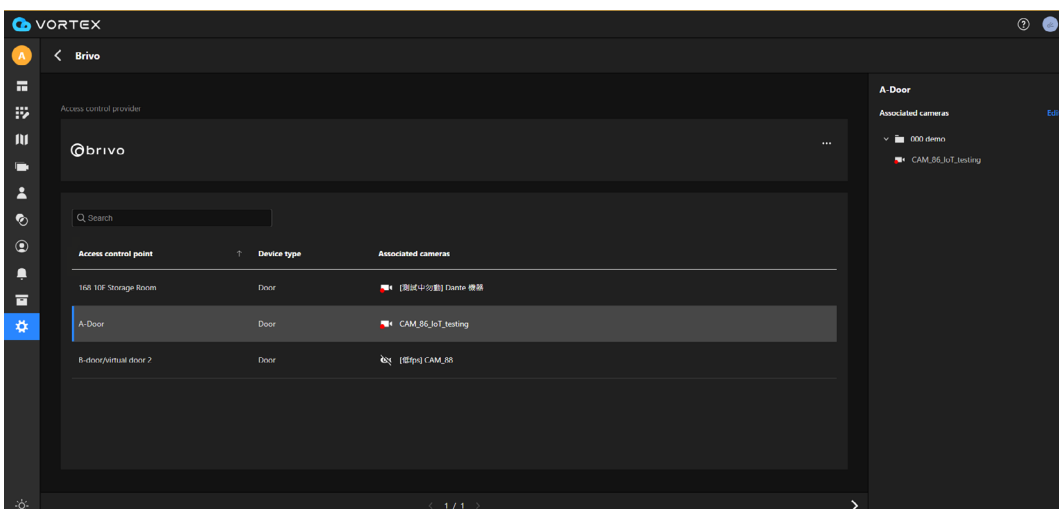
Many-to-many design:

 - 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

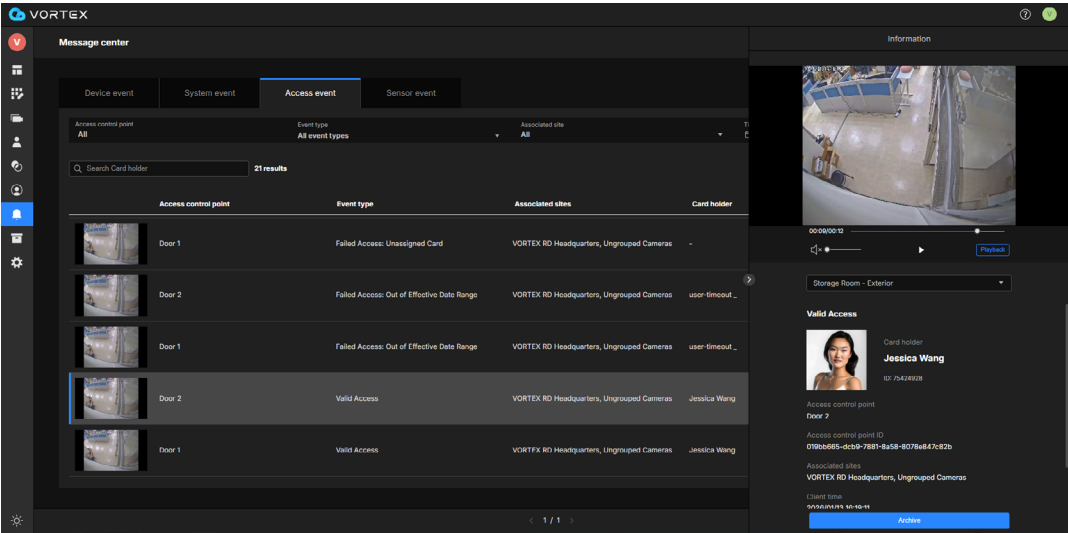
- Users can add/edit/disassociate the cameras associated with doors
- If users add/edit/delete doors on the Brivo platform, VORTEX will reflect the corresponding changes based on the adjustments
- Each time the Owner/Admin enters this page, VORTEX will check if the integration with Brivo is functioning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



Access Events Integration with Camera Videos

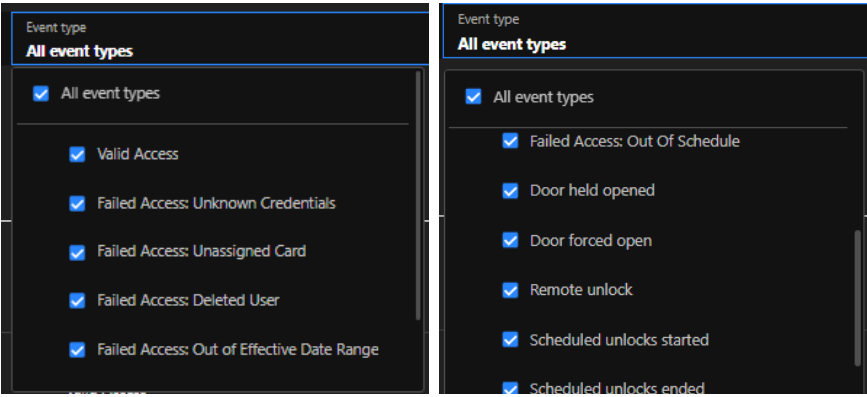
Goal

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



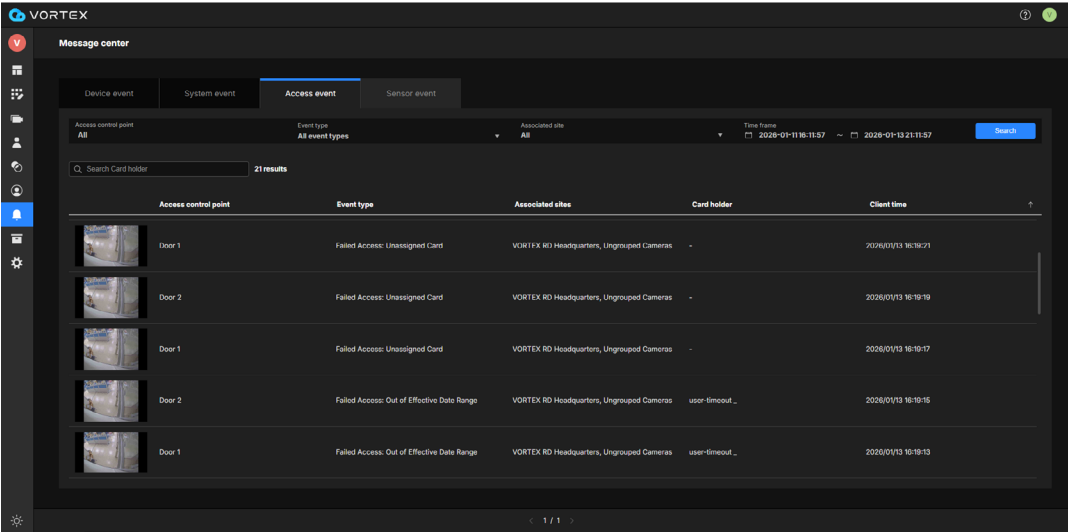
Brivo Event Types

VORTEX Event Name	Card Holder & Card ID Display
Valid Access	V
Failed Access: Unknown Credentials	
Failed Access: Unassigned Card	
Failed Access: Deleted User	
Failed Access: Out of Effective Date Range	V
Failed Access: Unauthorized Door	V
Failed Access: User Suspended	V
Remote unlock	
Failed Access: Out of Schedule	V
Door held open	
Door held open resolved	
Door forced open	
Scheduled unlocks started	
Scheduled unlocks ended	
Controller tempered active	
Controller tempered cleared	

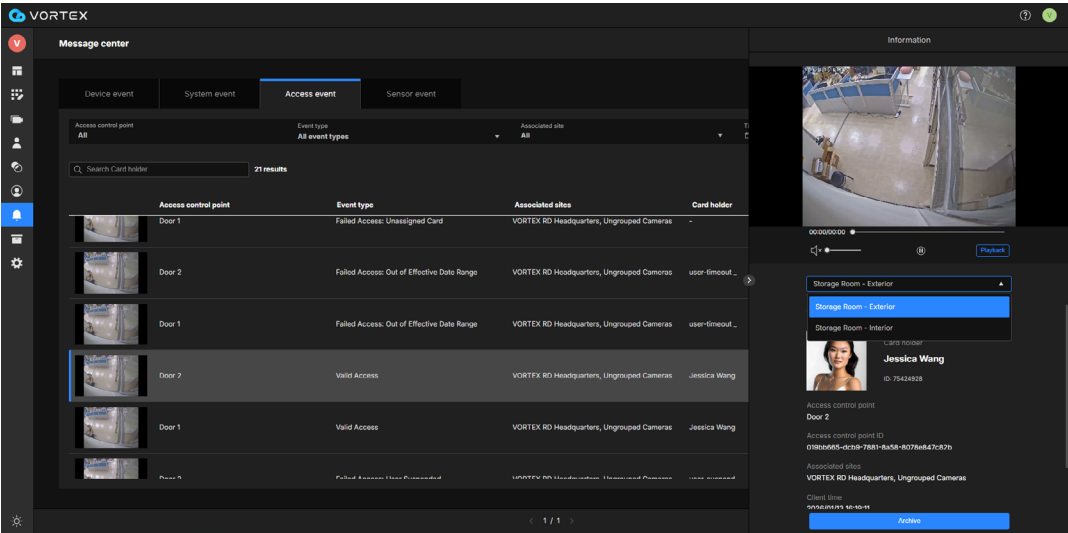


View Access Event in Message Center

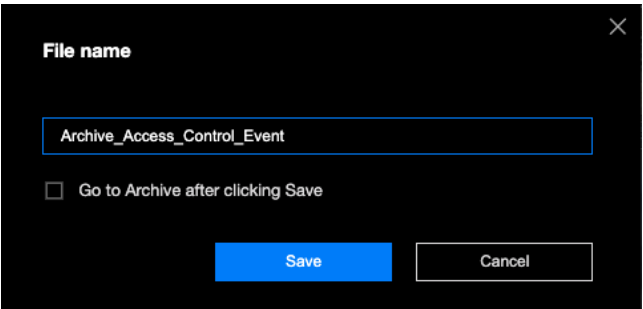
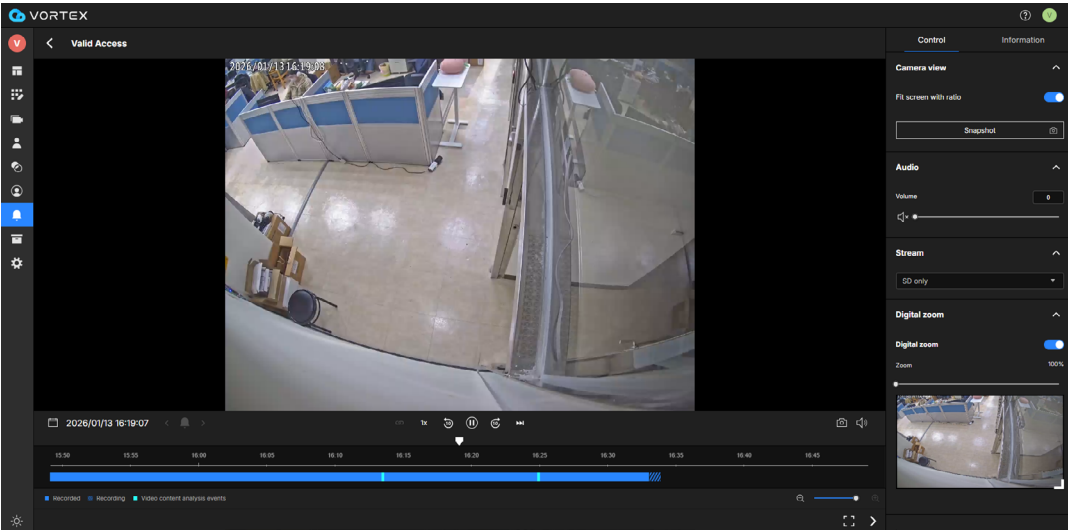
1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
 - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with extended access dependent on the cloud backup plan purchased by the end-user.
 - In the Search Filter, ‘Associated site’ 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 Brivo, the Card Holder field will not display any names and photos.

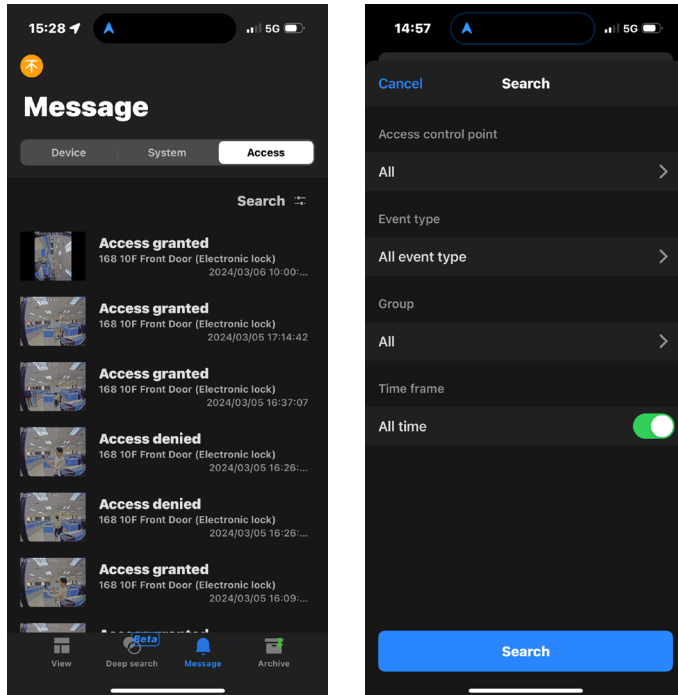


3. You can view the footage through playback, or archive this event footage and sharing with others.

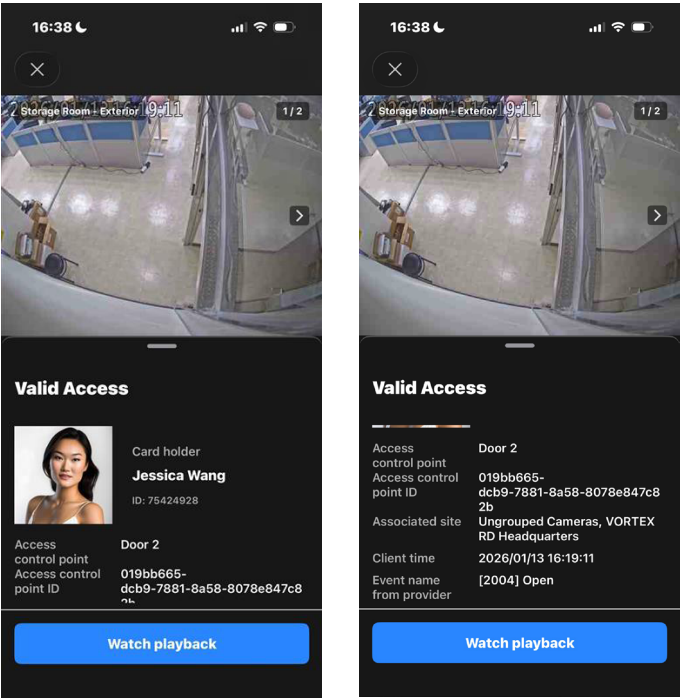


Feature Guide – Mobile App

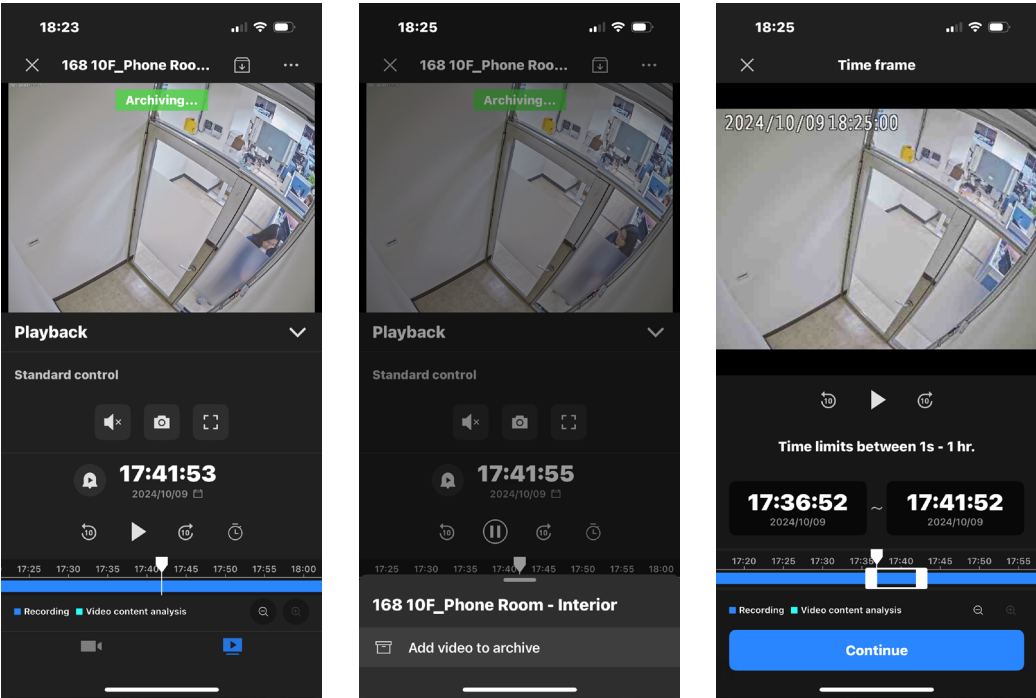
1. Go to Message Center and select “Access event” tab. You can search for the event types you want to see, the groups they belong to, and the time range by setting filter criteria.
 - The retention period for event logs is one year. Camera playback footage is accessible for a minimum of 30 days, with 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 Brivo, the Card Holder field will not display any names and photos.



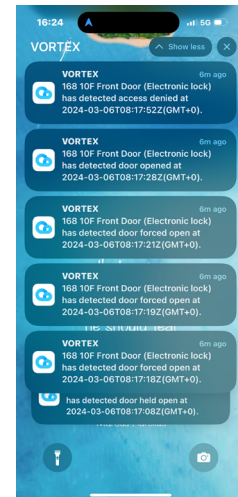
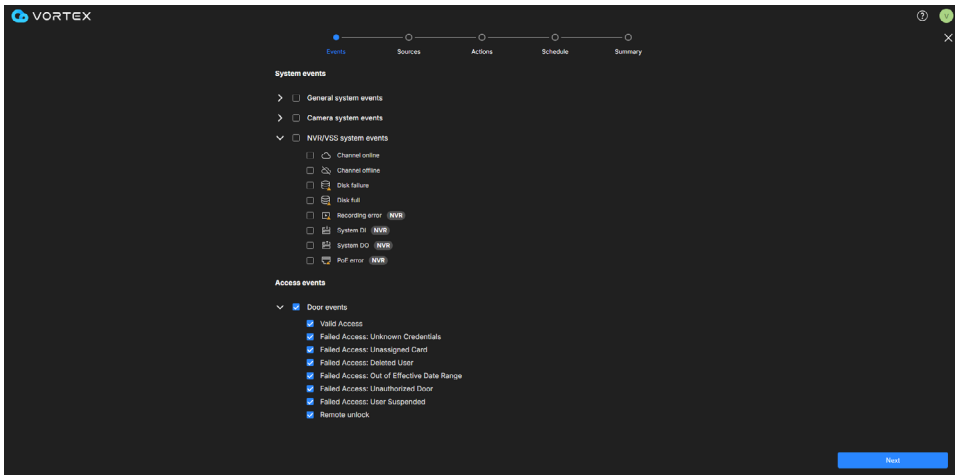
3. You can view the footage through playback, or archive this event footage and share with others.



Alarm Settings and Real-Time Notifications

Goal

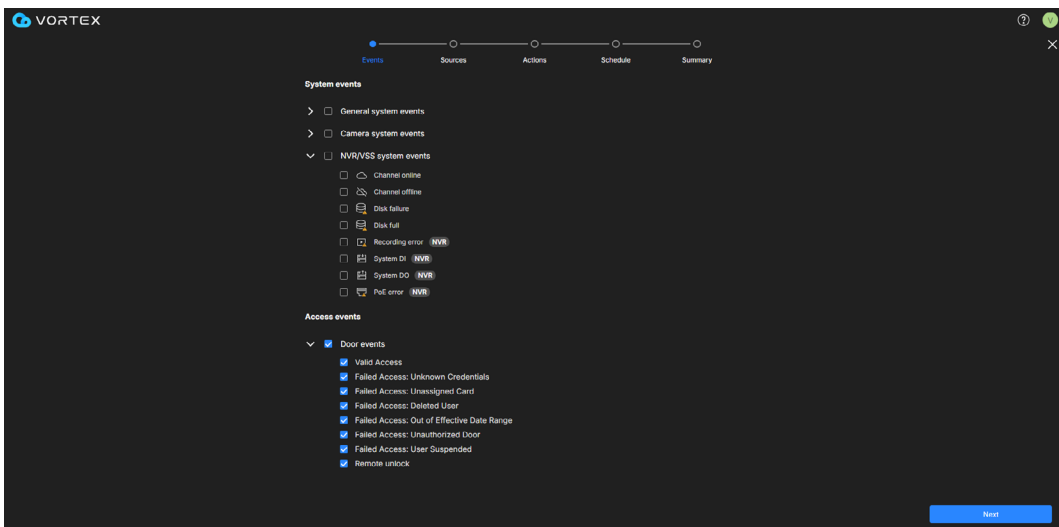
- Allow Owner/Administrators to set alarms for Access events in Alarm Management, allowing designated personnel to receive real-time push notifications and email notifications.



Feature Guide - Web Portal

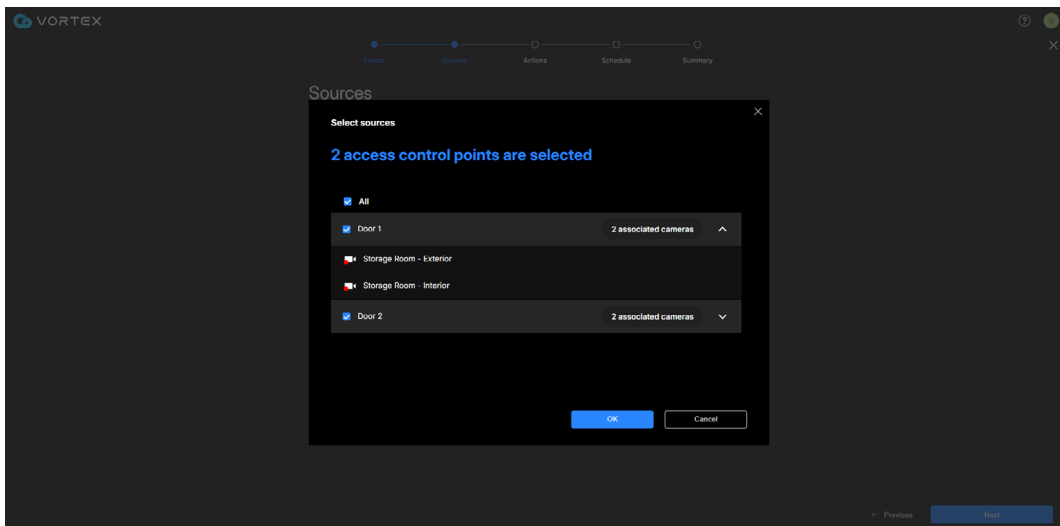
1. Go to System > Alarm Management > Add alarm

- 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)



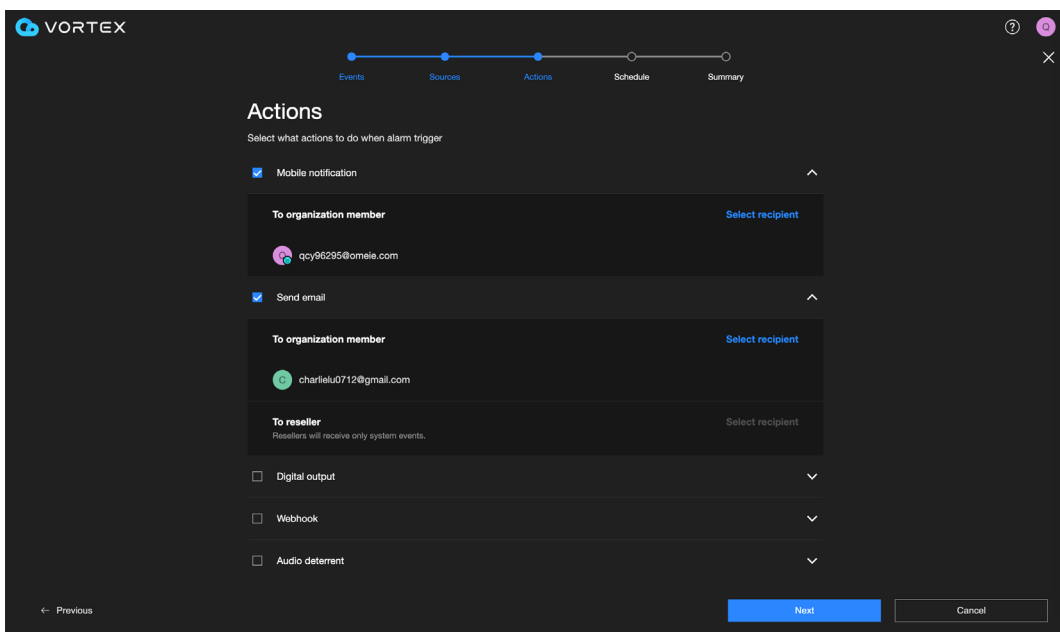
2. In the next step - Sources, select the doors that initiate Access events.

- 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



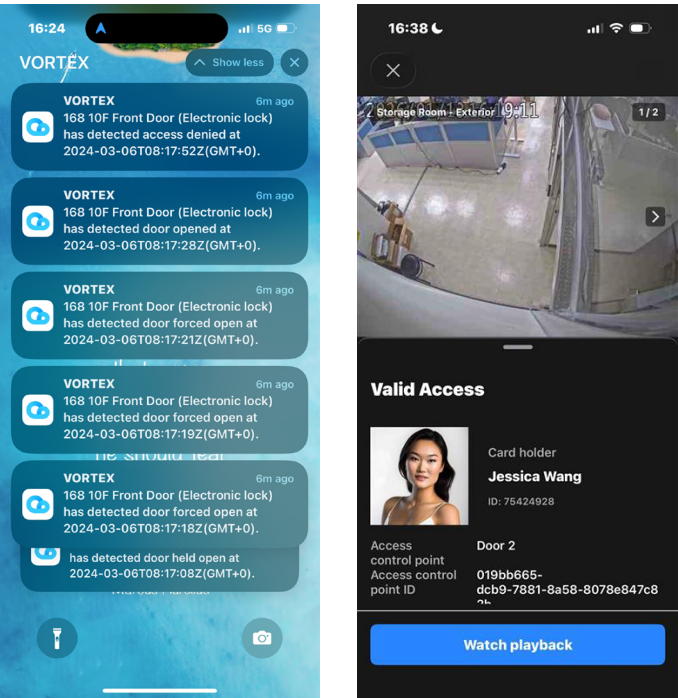
3. In the next step - Actions, select the actions and designated personnel to receive notification.

- The design logic here is the same as the existing Alarm Management.
- Access events support Mobile notification, Send emails, Digital output, and Audio deterrent. Only the Webhook is not supported yet.
- The remaining steps, Schedule and Summary, follow the same design logic and operate in the same manner as they currently do.

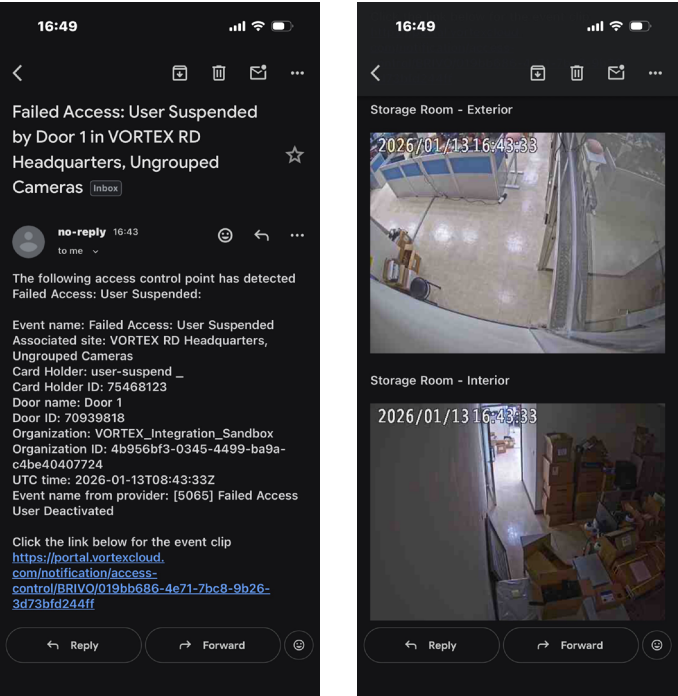


Feature Guide – Mobile App

- Designated personnel received received push notification.



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

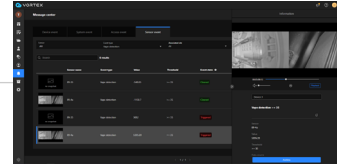


Smart Sensor Integration – Halo

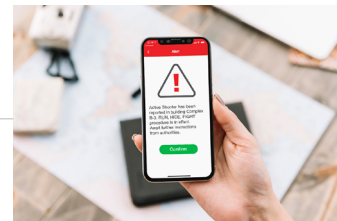
System Overview



- 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.)

HALO SMART SENSOR

Dashboard Sensors

Integration

Primary Integration

Integration Partner: **VORTEX** Apply Settings

Protocol: ☐ TCP ☒ HTTP Repeat Holdoff: 5 sec

Set String: POST:https://api.backend.dev.vortexcloud.com/webhook/halo/organizations/6d179369-0e0b-48e7-8024-882c925c057c/set[HEADER]User-Agent:Halo/%FWVER%[JSONBODY]

Reset String: POST:https://api.backend.dev.vortexcloud.com/webhook/halo/organizations/6d179369-0e0b-48e7-8024-882c925c057c/reset[HEADER]User-Agent:Halo/%FWVER%[JSONBODY]

Above you can use:

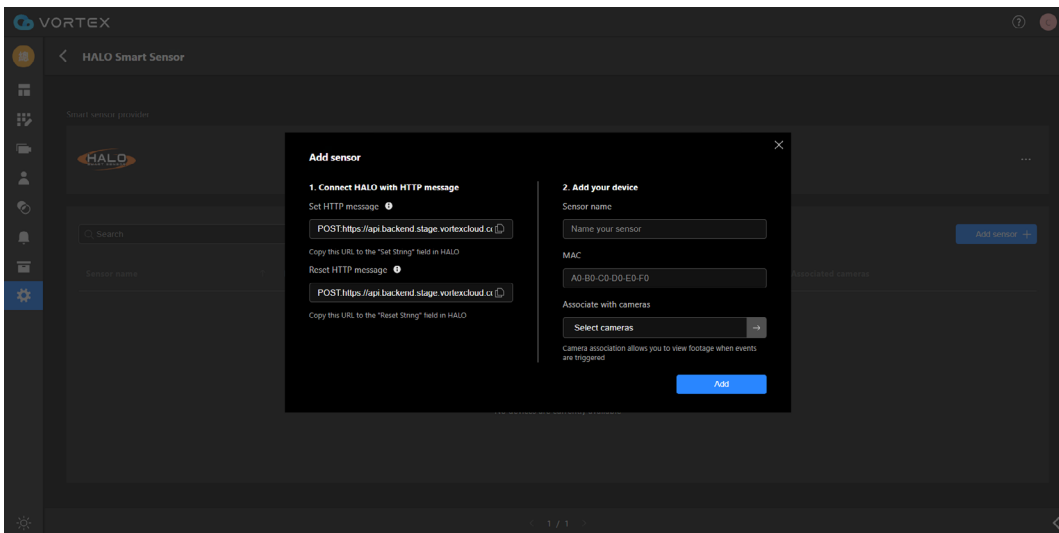
%NAME% - device name	%THR% - event threshold	%FWVER% - firmware version
%IP% - ip address	%VAL% - sensor value	\\ - 1 back slash
%MAC% - mac address	%DATE% - local date of event	\n - new line
%EID% - event id	%TIME% - local time of event	\r - carriage return
%SOURCE% - data source	%PSWD% - password	\u#### - hex char code
	%USER% - user	

Authentication Type: ☒ Basic/Digest ☐ Bearer Token ☐ OAuth2

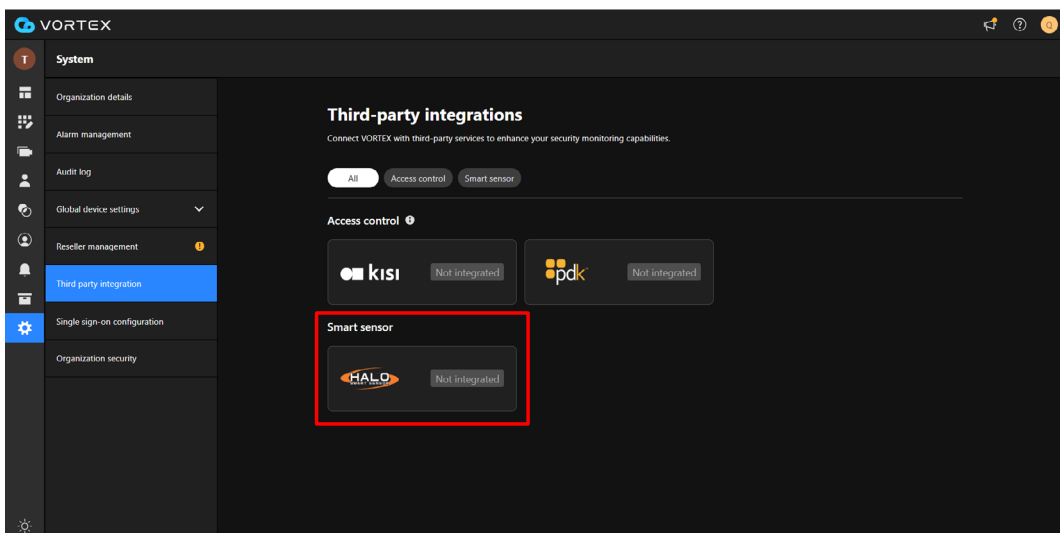
User: Password:

Save

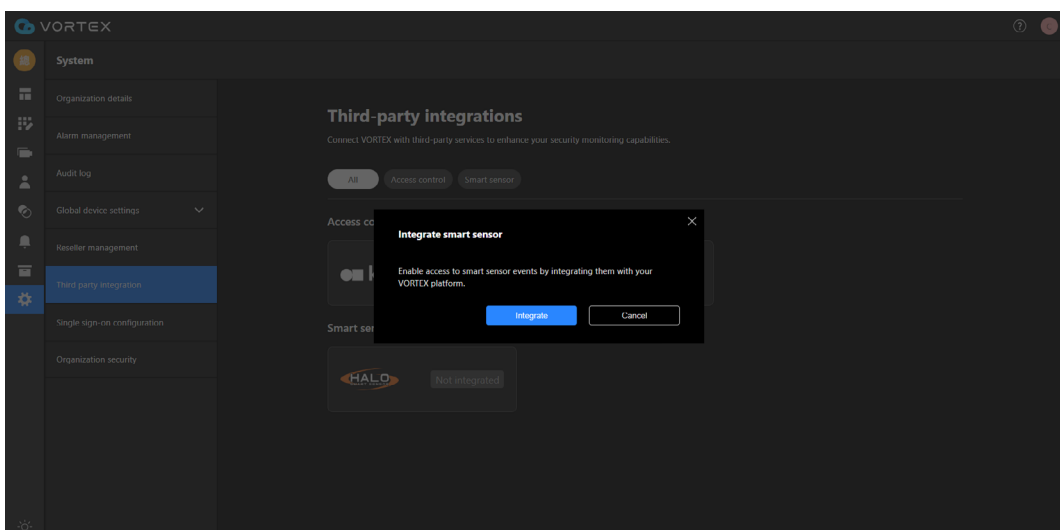
Status: No Content @ 7/23/2025 5:15:48 PM



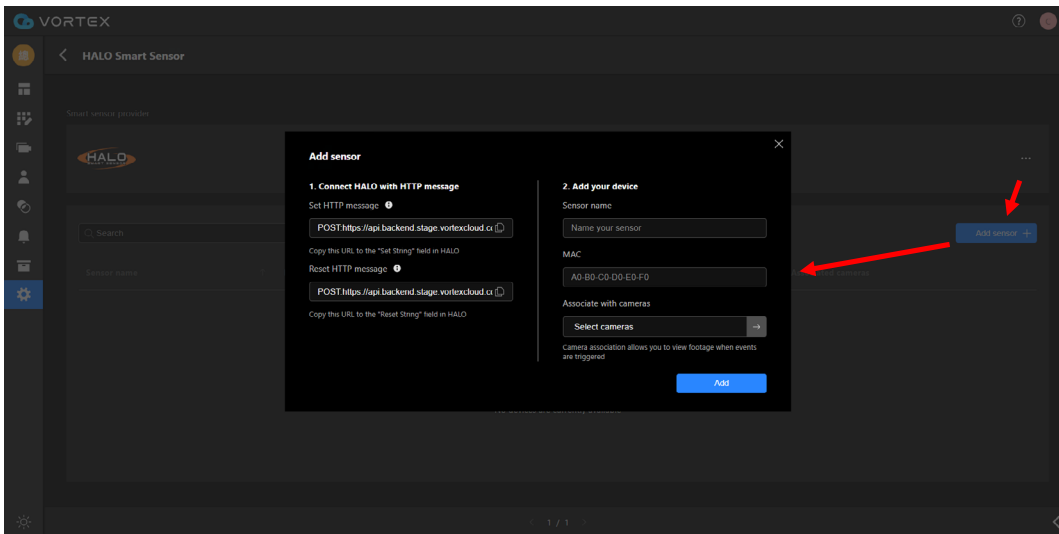
1. Go to System > Third party integration and select Halo Smart Sensor.



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

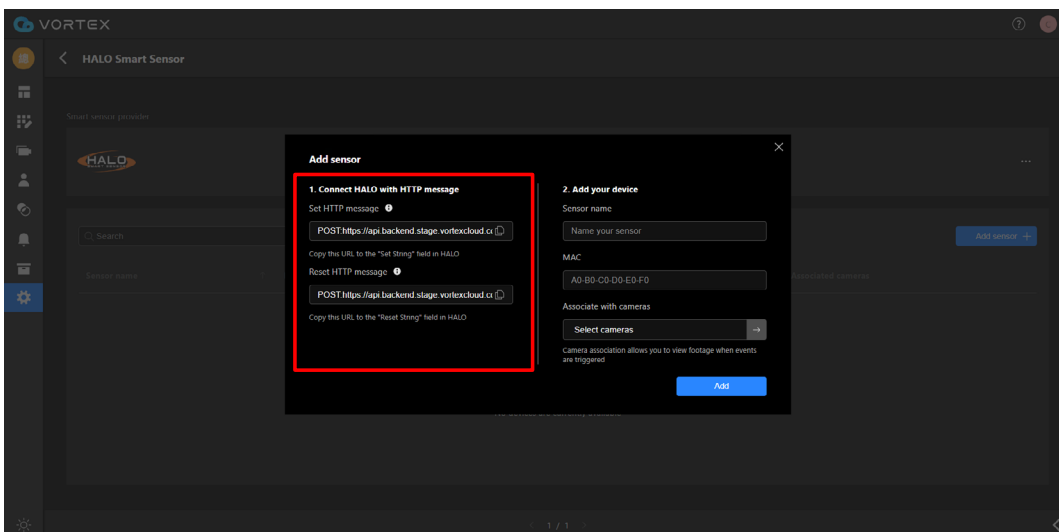


3. Click Add sensor button to open the configuration window.



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.

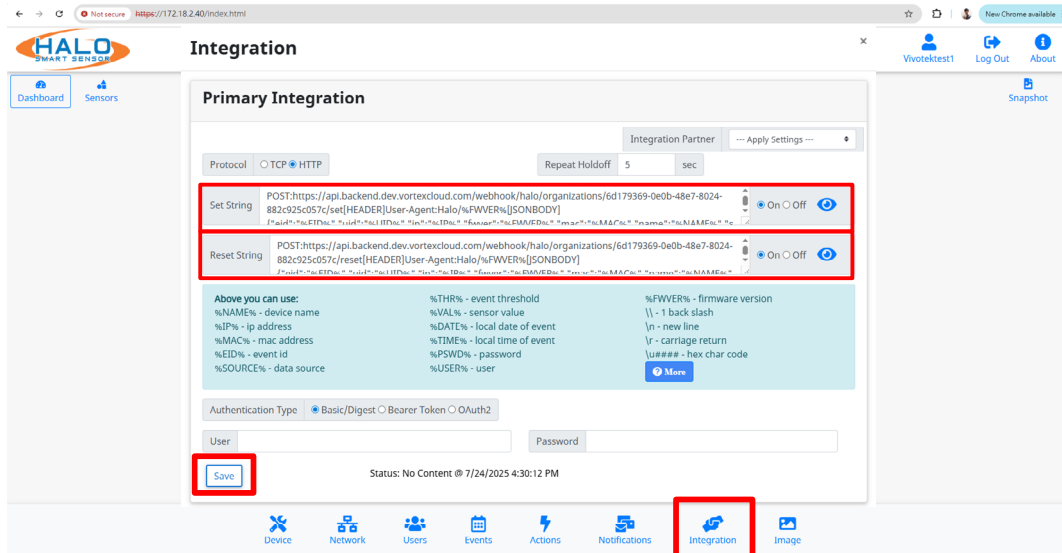
4. Copy and paste the two HTTP messages into the 'Set String' and 'Reset String' fields in HALO to configure the sensor to send data to VORTEX.

4.1. Log in to your Halo device and click Integration.

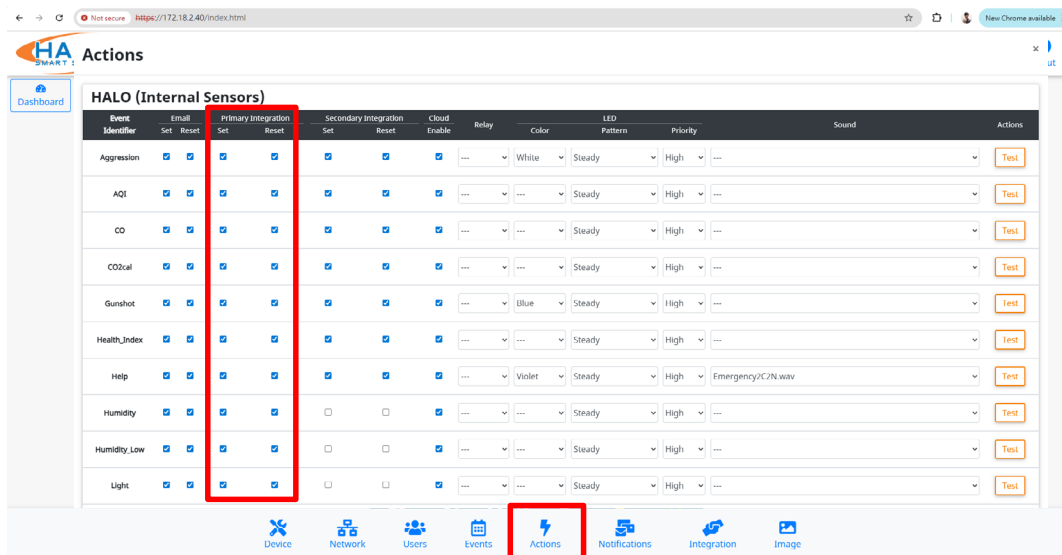
4.2. Paste VORTEX Set HTTP message into the Set String field in HALO and select the 'On' checkbox.

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.)

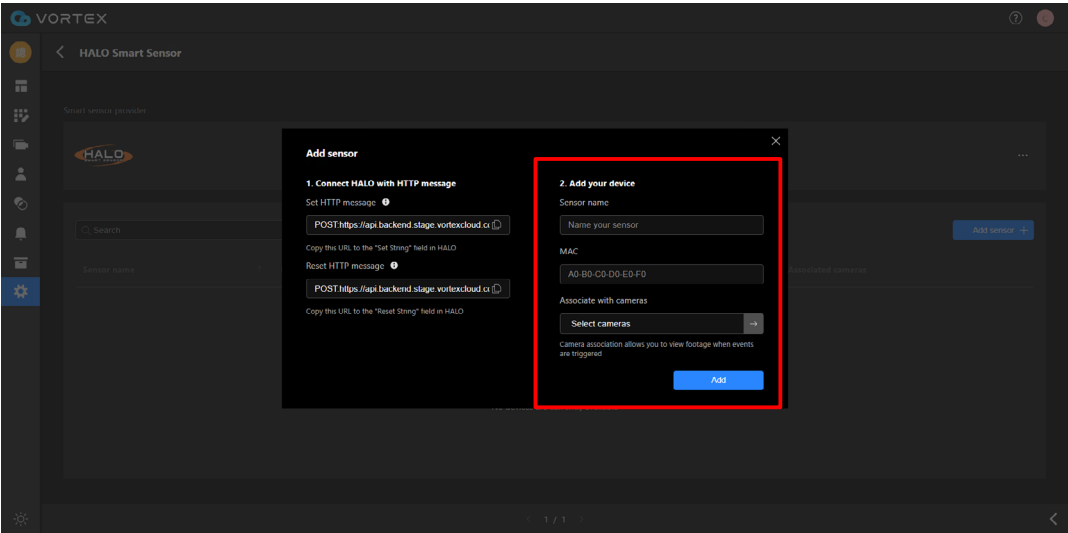


4.5. Click Actions and ensure that the checkboxes for Set and Reset under Primary Integration for each Event Identifier are selected.

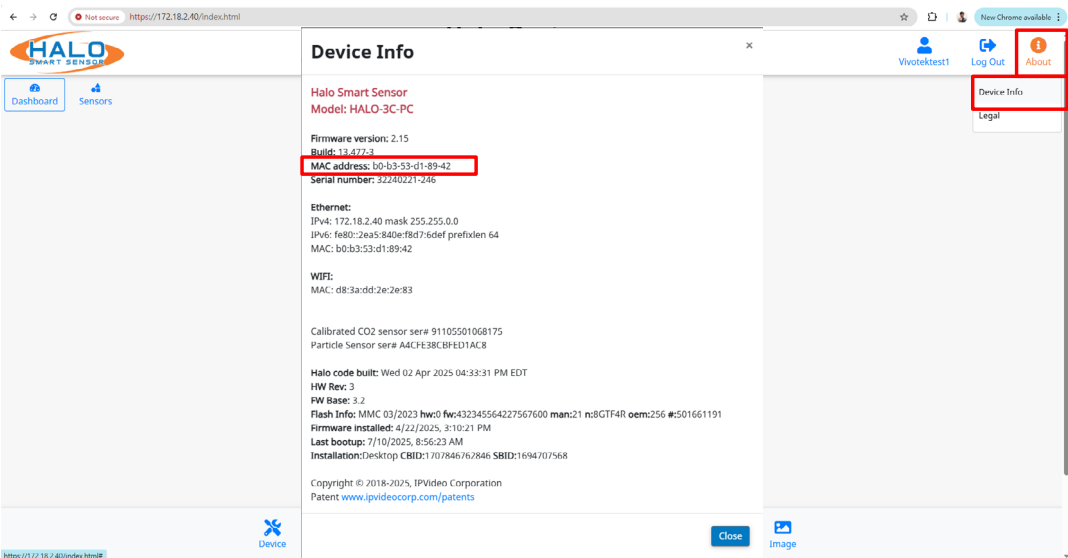


5. Add the HALO Smart Sensor device to VORTEX:

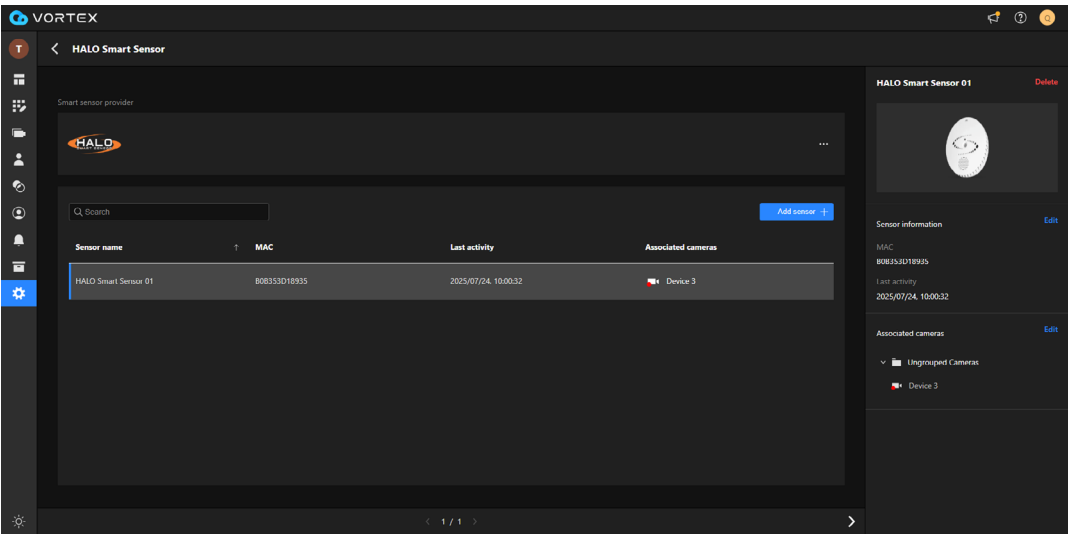
- Sensor name: Name your sensor (this will not overwrite the original name of the HALO device).
- MAC: Enter the MAC address of your HALO Smart Sensor.
- Associate with cameras: Camera association allows you to view footage when events are triggered.
- Many-to-many design: A sensor can be associated 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:

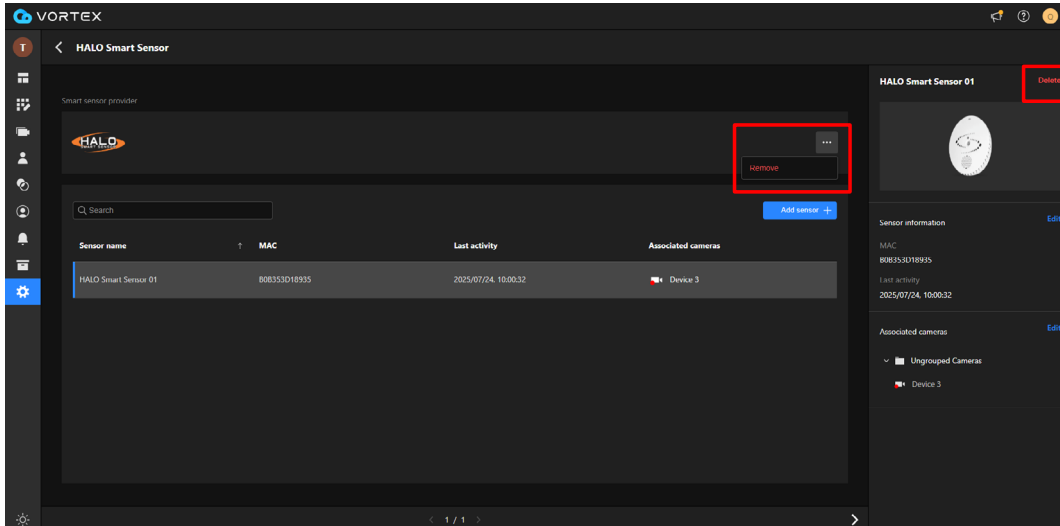


After successfully adding the HALO Smart Sensor to VORTEX, you will see the information you just configured displayed on the page.



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 sensor 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

Vape Detection

HALO uses a dynamic vape detection algorithm to automatically learn the environment and alert users when vaping is detected. HALO is the only product that can accurately differentiate between regular vaping, vaping with THC, and intentionally masking vaping behavior using aerosols.



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.

Vaping

Safety and Security

Health



- Preloaded with 12 spoken keyword phrases for use in emergencies, beneficial for schools, healthcare, and hospitality sectors.
- When a keyword is vocalized, notifications are dispatched by HALO to designated recipients.
- Spoken "Help Emergency" keyword detection is available in 4 additional languages.



- Gunshots detected using two-factor authentication: sound frequency and percussion analysis.
- Sensor is third-party certified.
- Covers a 25 ft. (7.6 m) range with 360° detection.



- Machine learning applied to learn abnormal noise signatures.
- HALO sets normal sound level baselines and alerts on threshold breaches.
- Uses true analytics for aggression detection.

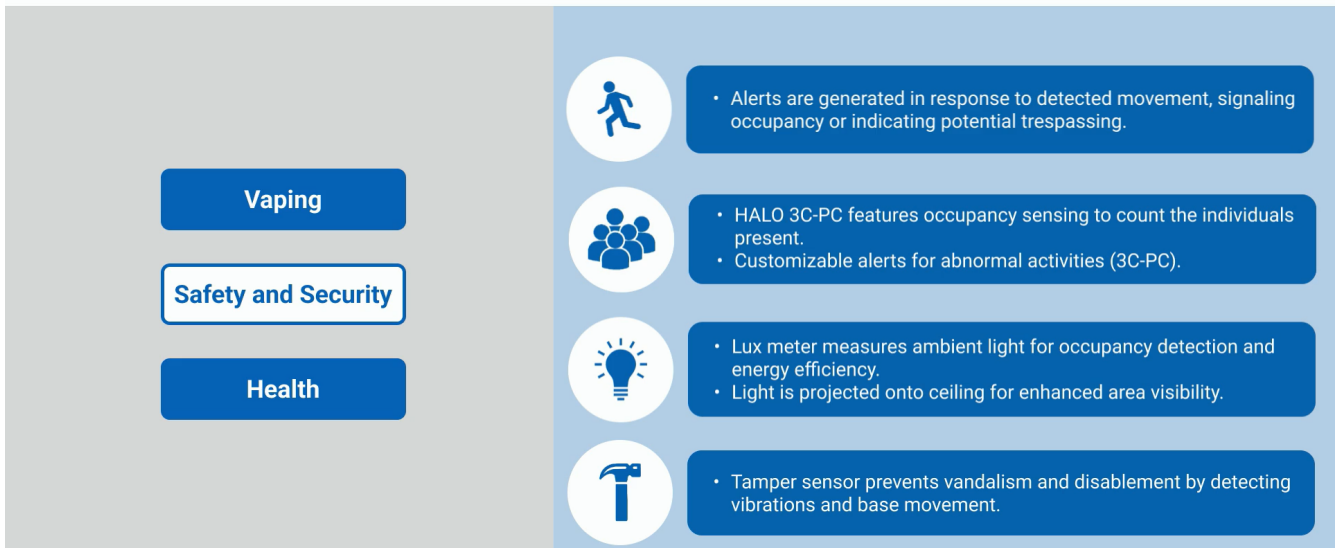


- iPanic™ buttons enable HALO 3C and 3C-PC users to trigger alerts.
- Alert locations are associated with the nearest HALO device.

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.

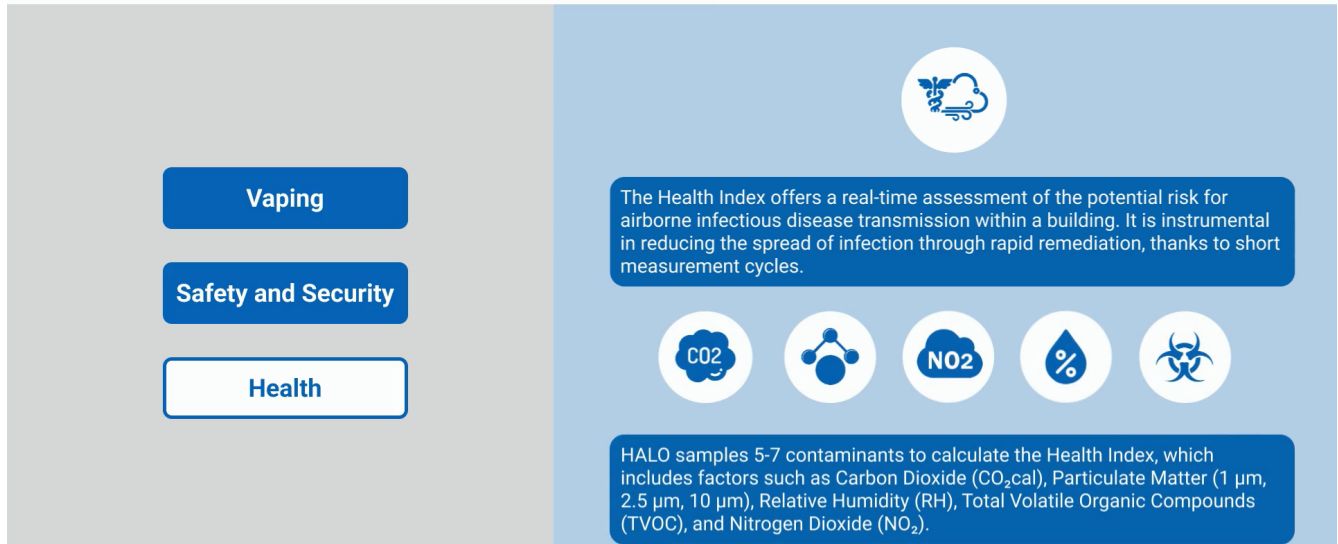


Event Group	Halo Event Name	VORTEX Event Name	Description
Safety and Security	Motion	Motion detection	Identify and alert on movement for occupancy and trespassing.
	Occupancy	High occupancy Count	Identify how many people are within the HALO location and configure to alert on abnormalities.
	Light	Light 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.



Vaping

Safety and Security

Health

The Health Index offers a real-time assessment of the potential risk for airborne infectious disease transmission within a building. It is instrumental in reducing the spread of infection through rapid remediation, thanks to short measurement cycles.

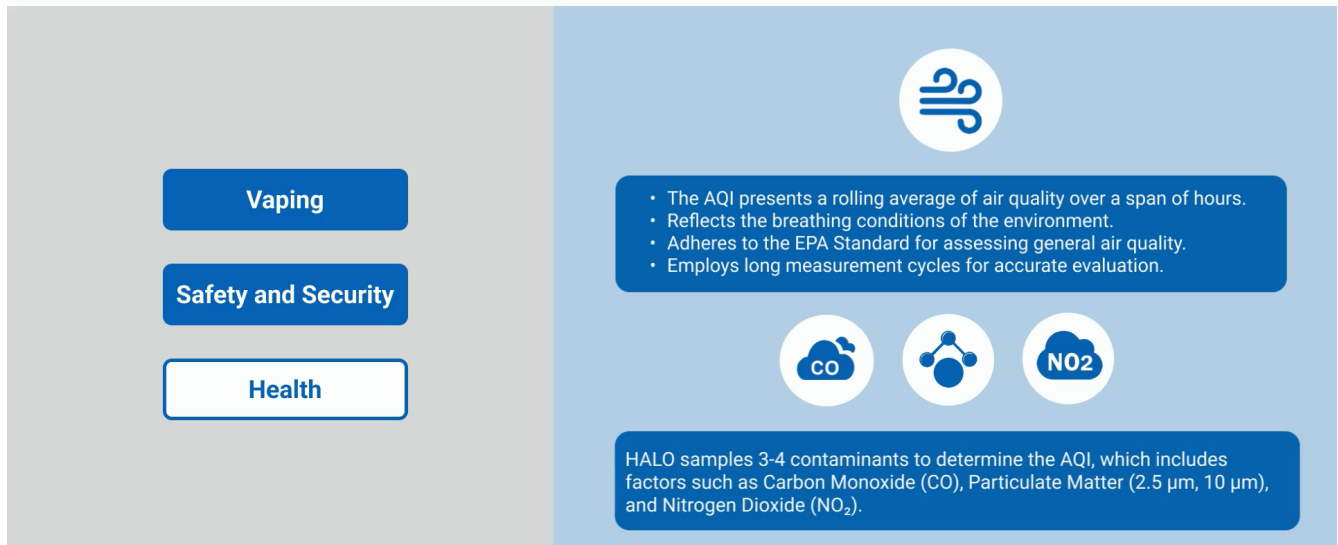
CO₂ • Particulate Matter (1 µm, 2.5 µm, 10 µm) • Humidity (RH) • Volatile Organic Compounds (TVOC) • Nitrogen Dioxide (NO₂)

HALO samples 5-7 contaminants to calculate the Health Index, which includes factors such as Carbon Dioxide (CO₂cal), Particulate Matter (1 µm, 2.5 µm, 10 µm), Relative Humidity (RH), Total Volatile Organic Compounds (TVOC), and Nitrogen Dioxide (NO₂).

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.

Vaping

Safety and Security

Health



- The AQI presents a rolling average of air quality over a span of hours.
- Reflects the breathing conditions of the environment.
- Adheres to the EPA Standard for assessing general air quality.
- Employs long measurement cycles for accurate evaluation.



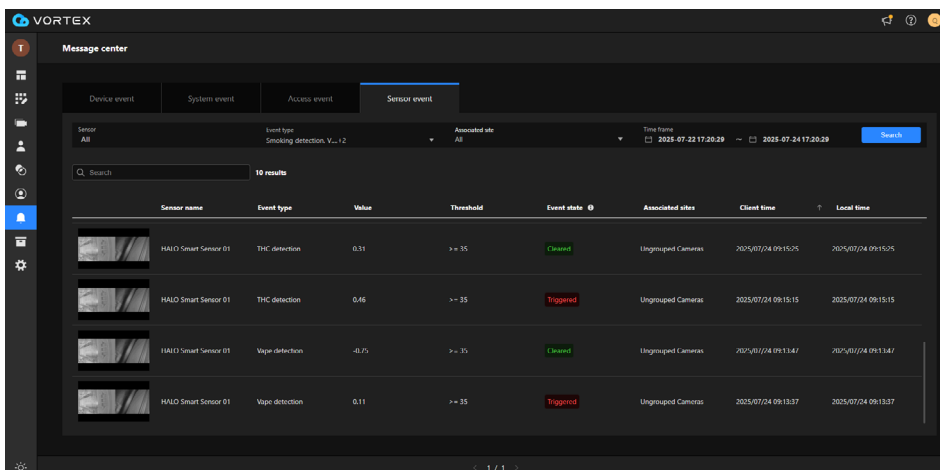
HALO samples 3-4 contaminants to determine the AQI, which includes factors such as Carbon Monoxide (CO), Particulate Matter (2.5 µm, 10 µm), and Nitrogen Dioxide (NO₂).

71

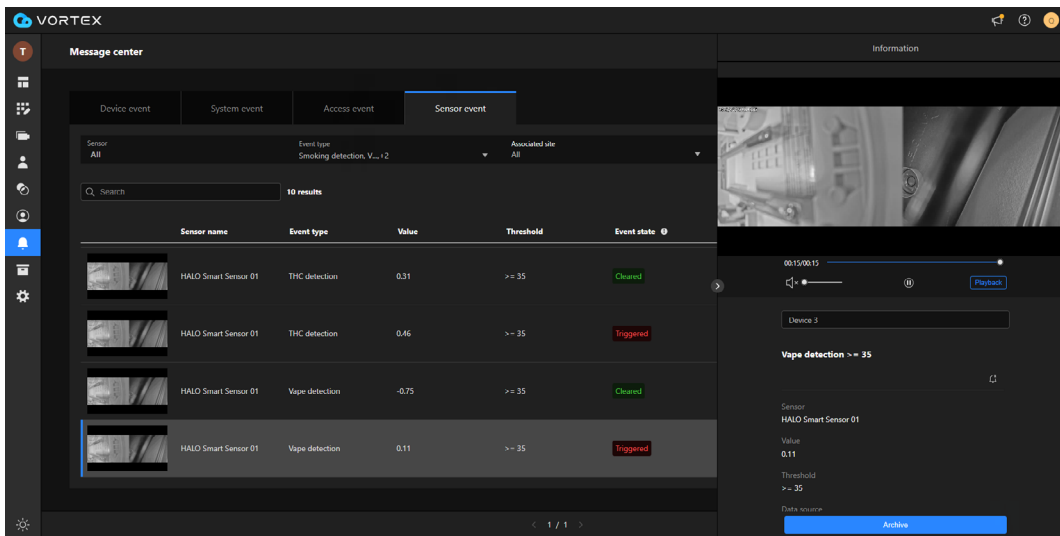
Event Group	Halo Event Name	VORTEX Event Name	Description
Health	PM1	PM1	Particulate matter, or PM, is a mix of particles and droplets in the air. PM varies in shape and size, but those of 10 micrometers in diameter or smaller can adversely affect your health because they can be inhaled. PM 2.5 refers 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	
	NH3	NH3	Ammonia ppm.
	Pressure	Pressure	Pressure (hPa).

View Sensor event in Message Center

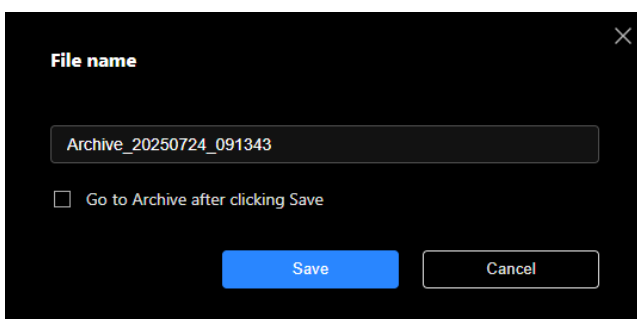
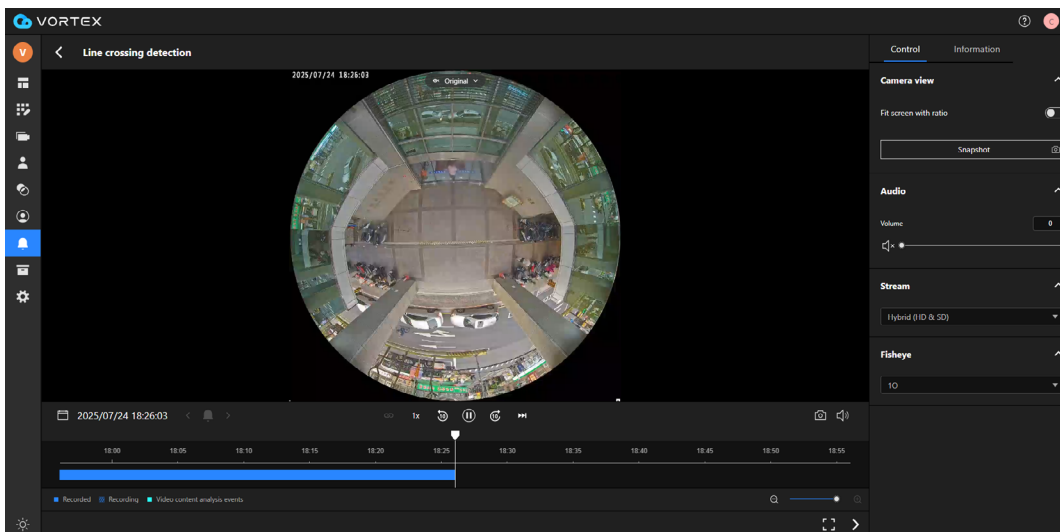
- Go to the Message Center and select the 'Sensor Event' tab. You can search for the event types you want to view, filter by the associated sites, and adjust the time range by setting the filter criteria. You can also further narrow your search by using the search box to find specific event values or 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.

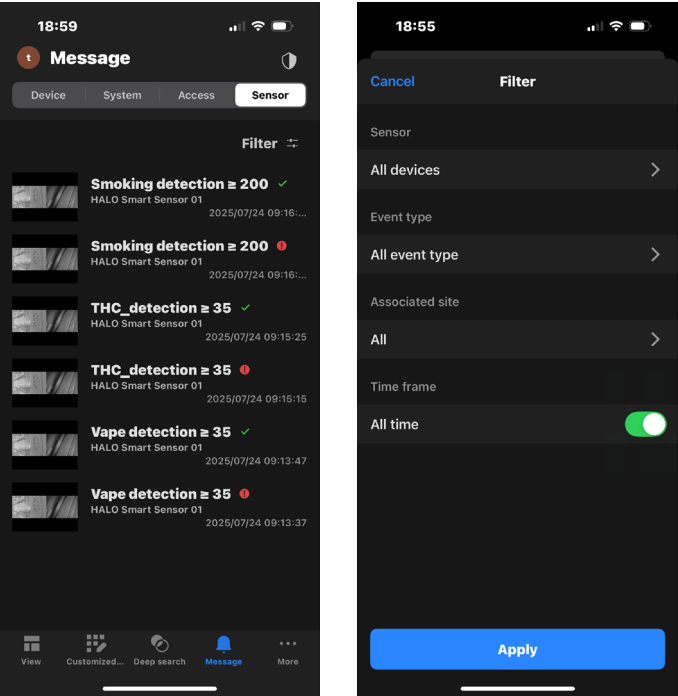


3. You can view the footage through playback, or archive this event footage and sharing with others.

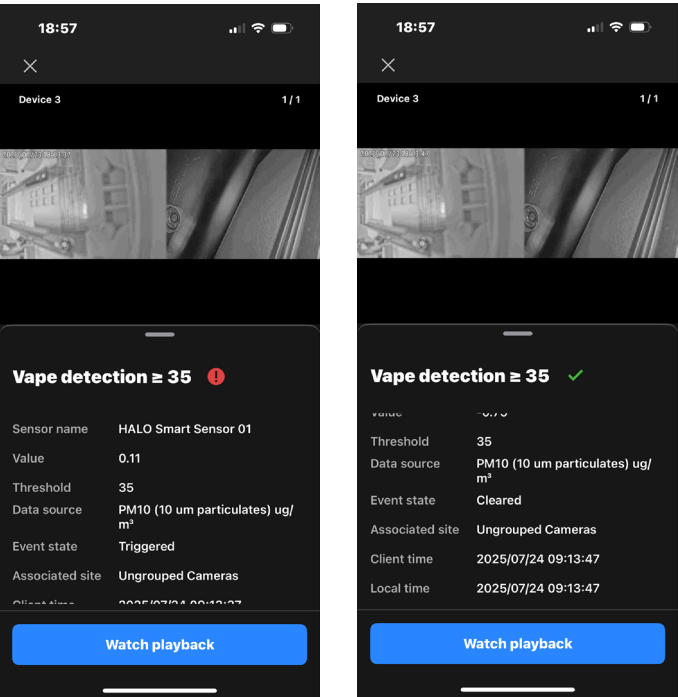


Mobile App

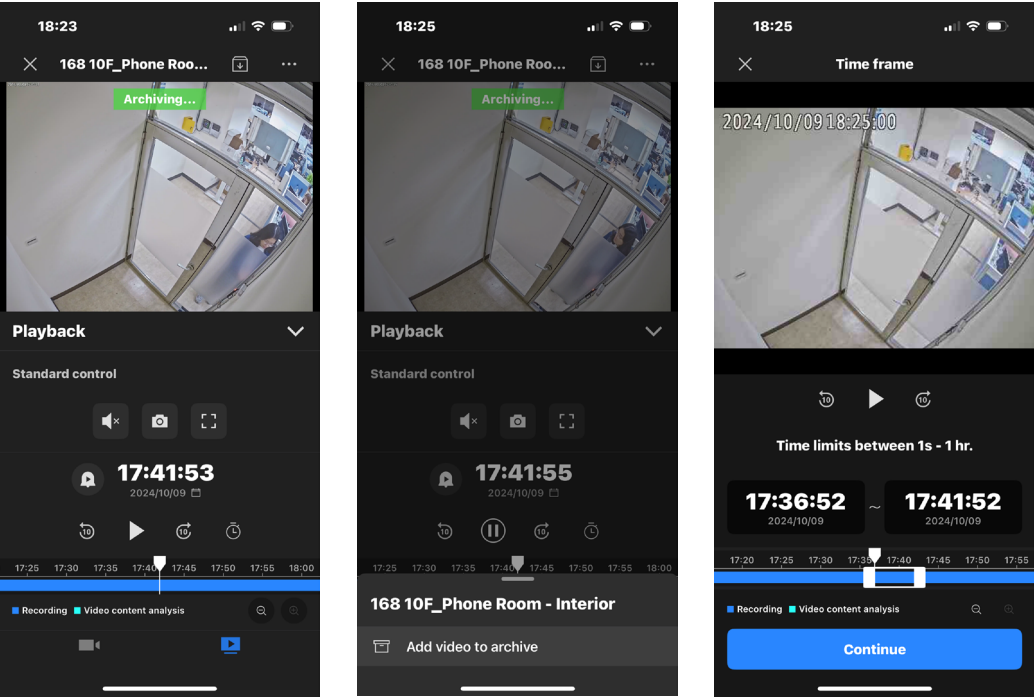
1. Go to the Message Center and select the 'Sensor Event' tab. You can search for the event types you want to view, filter by the associated sites, and adjust the time range by setting the filter criteria.
- The retention period for event logs is one year. Camera playback footage is accessible for a 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.



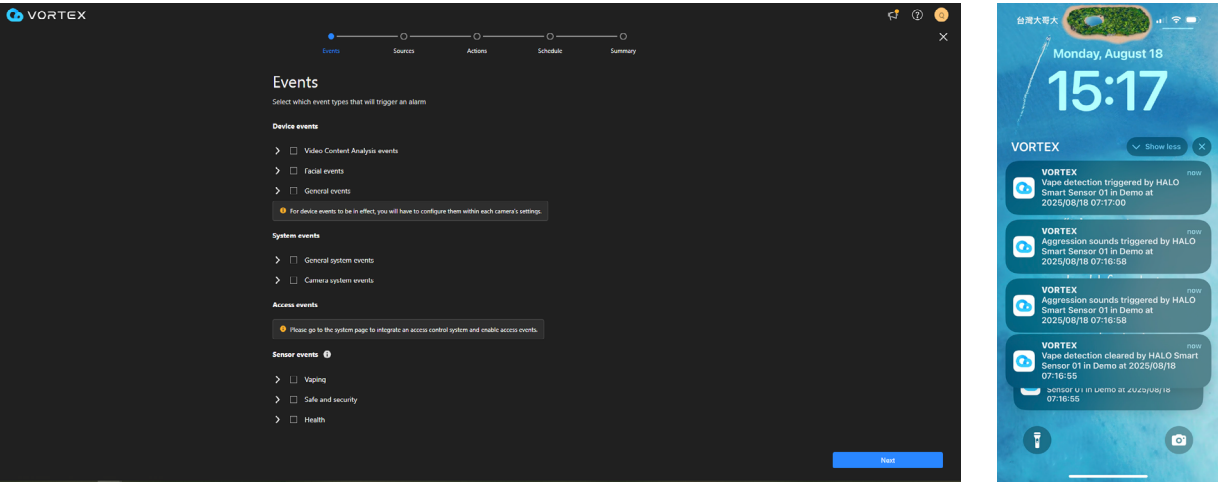
3. You can view the footage through playback, or archive this event footage and sharing with others.



Alarm Settings and Real-Time Notifications

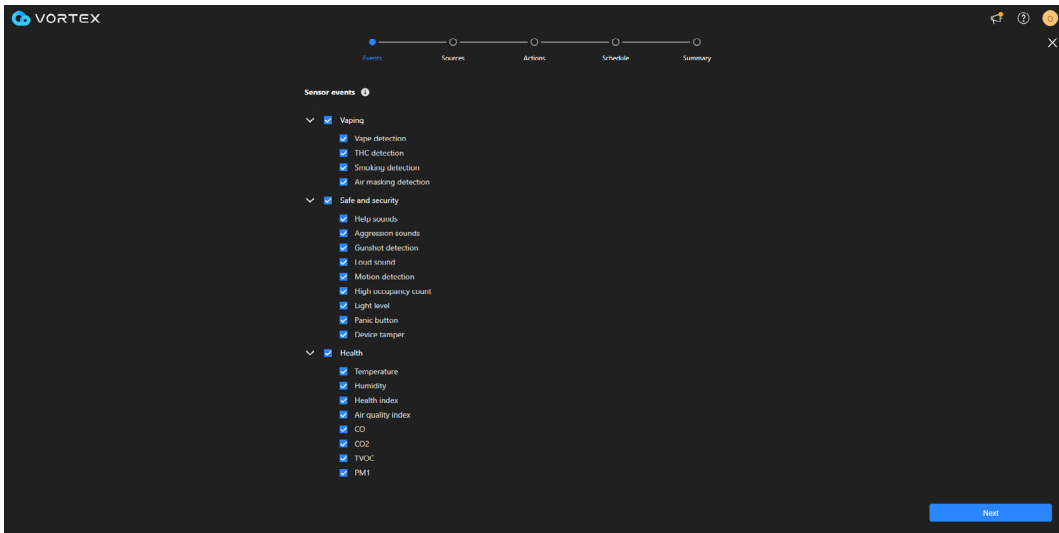
Goal

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



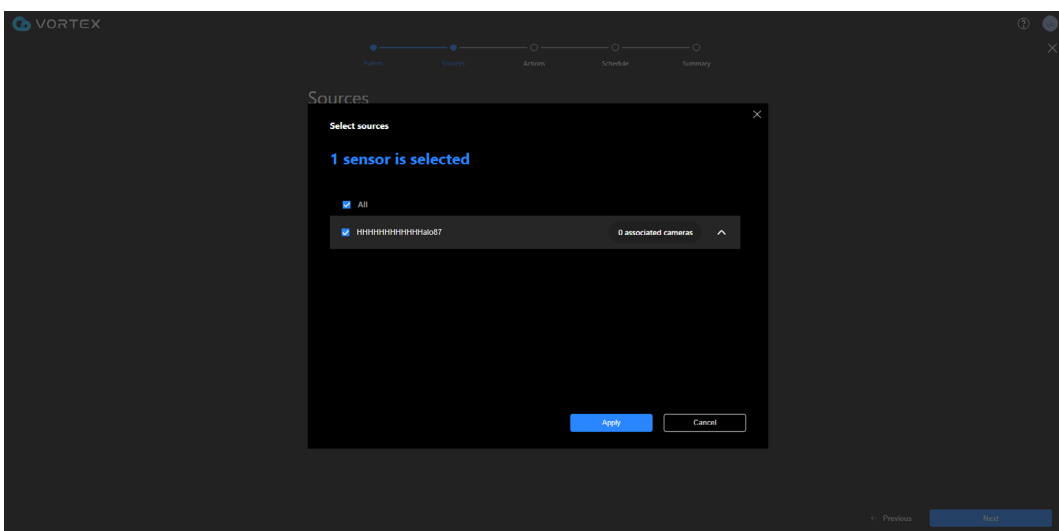
Web Portal

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



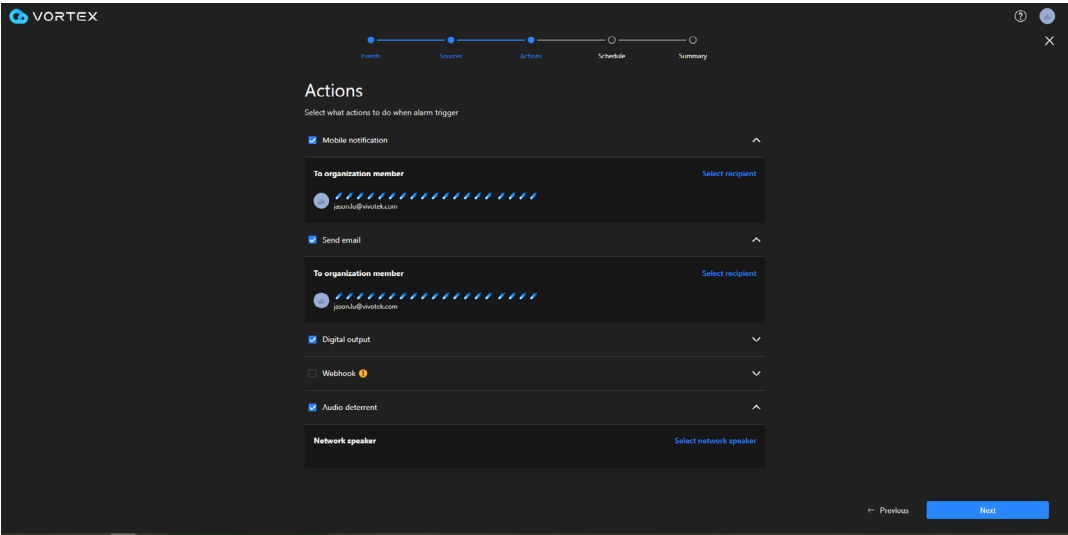
2. In the next step - Sources, select the doors that initiate Sensor events.

- 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.



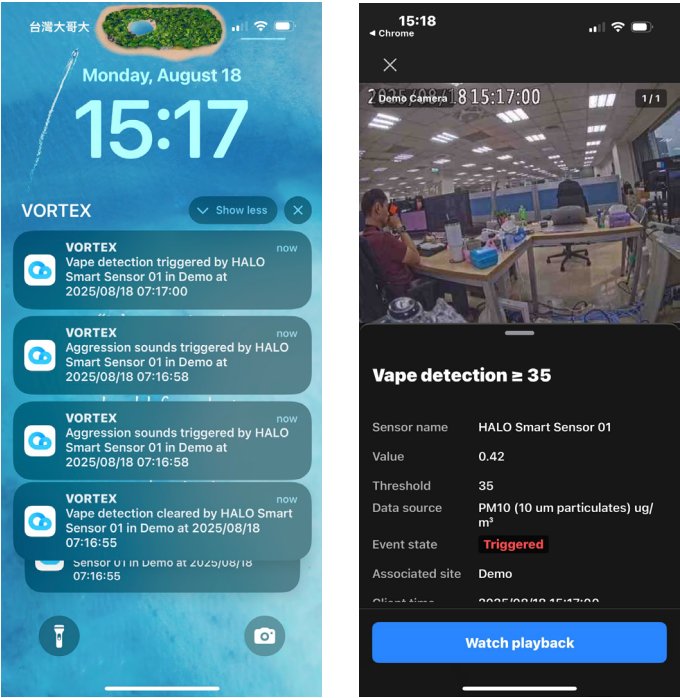
3. In the next step - Actions, select the actions and designated personnel to receive notification.

- 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.



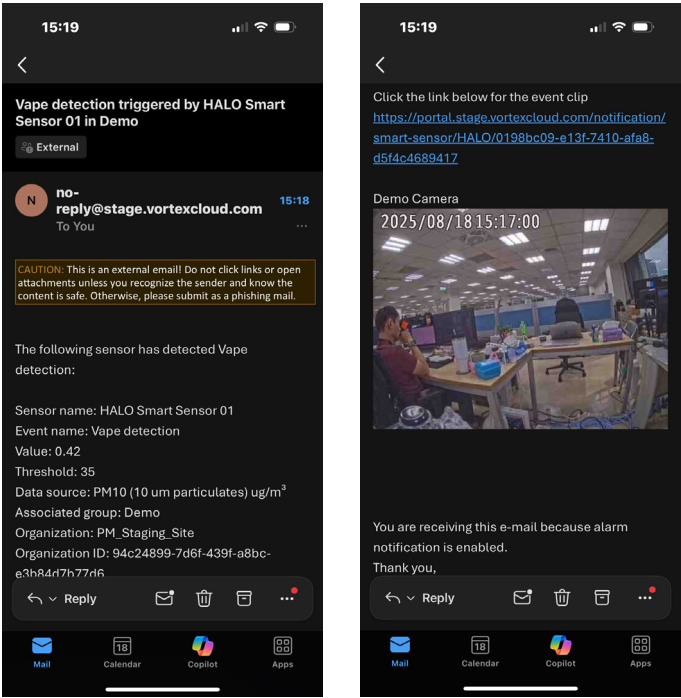
Mobile App

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.



www.vivotek.com

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