ViOnyx Web Server

USER GUIDE

Version 1.1.0

English

EN 102.00.VQF12-R

suprema

SECURITY & BIOMETRICS

CONTENTS

Getting Started 5

Certificate installation 5

Set password 10

Sign in 11

Understanding the User Interface 13

Main menu quick access 13

Information and tools 14

View Live 15

Live view basic layout 15

Select channel and view mode 15

Zooming 16

Rotate the screen 17

Screen capture 17

Full-screen mode 18

AI display options 18

Open the Face Shot panel 19

When video does not play 20

Manage AI Events 21

Set Up User Tracking Events 21

Set Up Intrusion Detection Events 28

Set Up Line-Crossing Detection Event 35

Set Up People Counting Event 43

Set Up Access Control Events 50

Edit and Delete AI Events 59

AI Rule Settings 60

Manage Schedules 67

Advanced Settings 71

Configure the Camera 74

Configure Video Profile 74

Configure Camera Settings 77

Configure Privacy & Overlay Settings 81

Configure Date and Time 85

Configure Network Settings 87

Set Up RS-485 98

Integrate RTSP and ONVIF 106

Manage Users 108

Set Up Facial Authentication 108

Add Users 108

Edit and Delete Users 115

User Search and View 118

Manage Access Control 122

Manage Doors 122

Manage Access Levels 128

Control Doors 134

Set Door Rules 136

Configure System 144

Update Camera Information 144

Upgrade Firmware 146

Maintain the Camera 148

Upload Audio Clips 152

Update Administrator Account Password 154

Manage Operators 156

View System Logs 160

System Log Types 165

Appendices 174

Disclaimers 174

Copyright Notice 175

Getting Started

After installing the ViOnyx camera, complete the initial setup through a web browser. This document explains all required steps, from certificate installation to setting the administrator password and logging in.

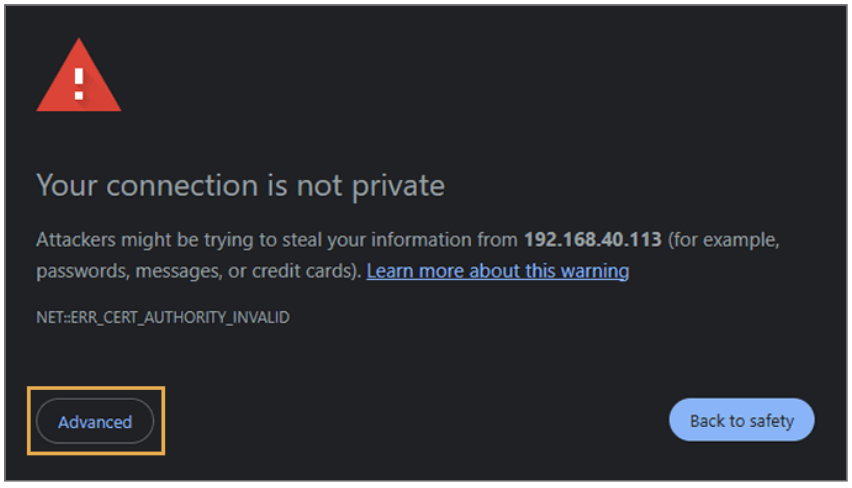
> **Info**
> If the camera does not obtain an IP address after a factory reset, it changes to the default IP address (`https://192.168.1.100`). Connect to that address in your web browser.

Certificate installation

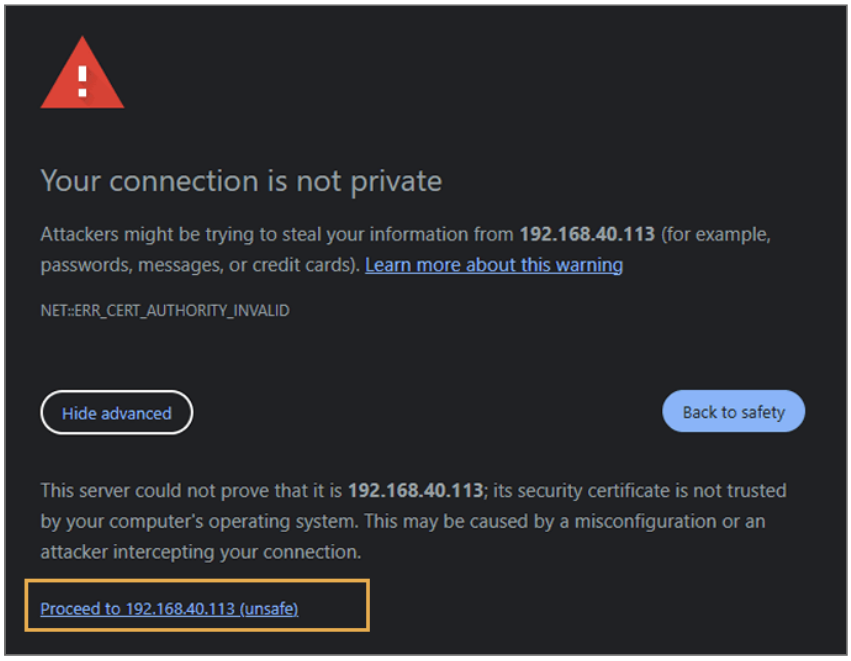
The ViOnyx Web Server uses a secure HTTPS connection. A security warning appears the first time you connect because the camera uses a self-signed certificate. Learn how to connect to the web server securely without warnings after adding the certificate to the Windows trusted store.

1 Download certificate

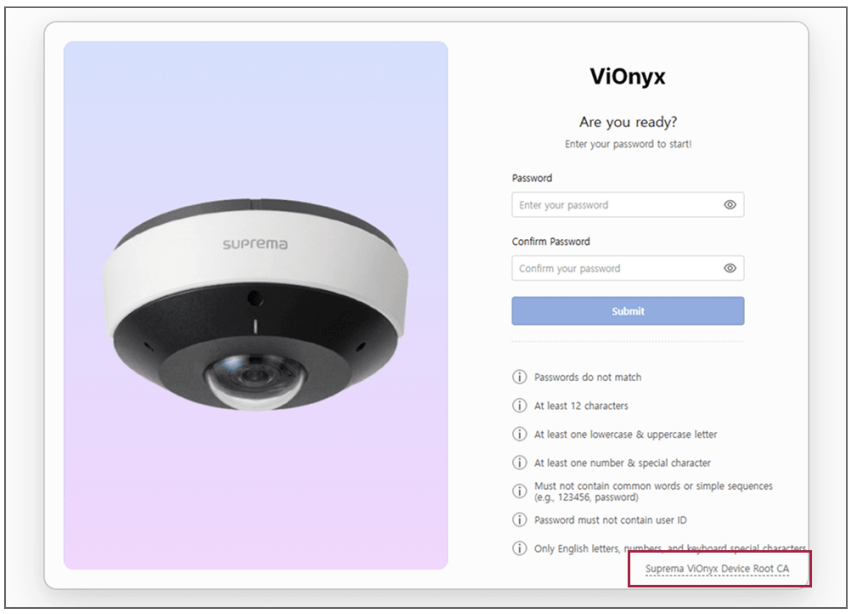
1. Connect to the camera in your web browser using the assigned IP address (`https://{IP_address}`).
2. If the warning message "**Your connection is not private**" appears, click **Advanced** at the bottom.



3. Expand the **Advanced** section, then click **Proceed to** `https://{IP_address}` **(unsafe)** or a similar link to continue.



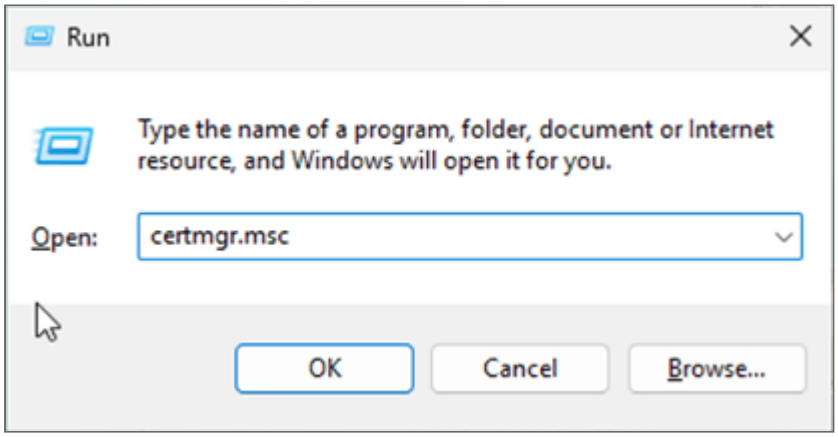
4. Click the **Suprema ViOnyx Device Root CA** link at the bottom of the password setup screen.



5. Save the certificate file `Suprema_ViOnyx_Device_{serial-number}_Root_CA.crt` locally.

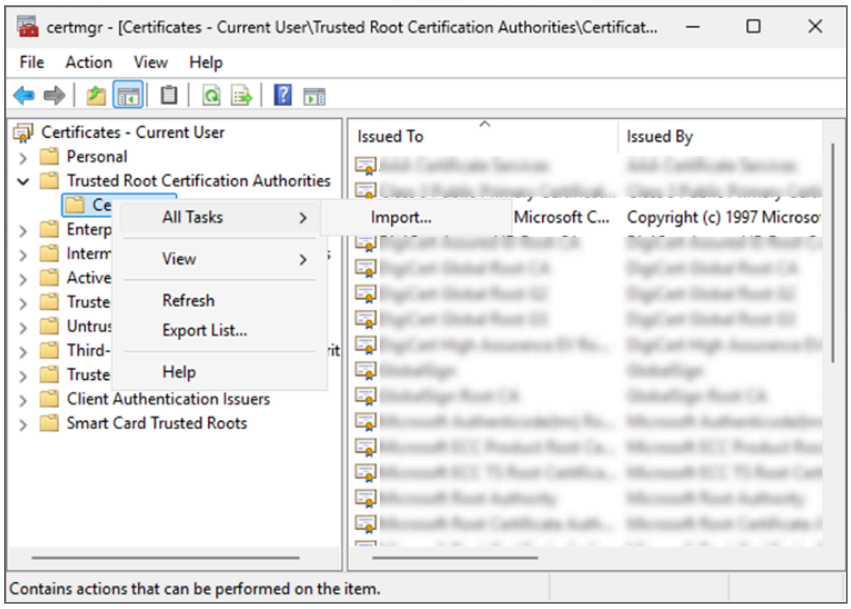
2 Open the Windows management console

1. Press Start + `R` to open the Run window.
2. Type `certmgr.msc`, then press `Enter` to open the **Management Console**.

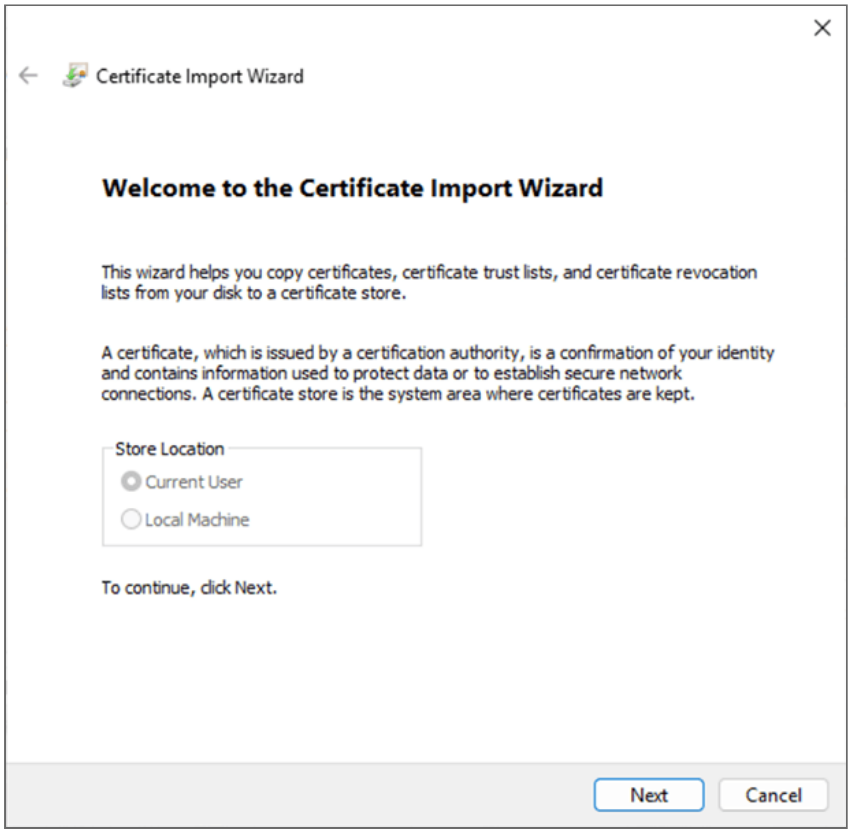


3 Run the certificate import wizard

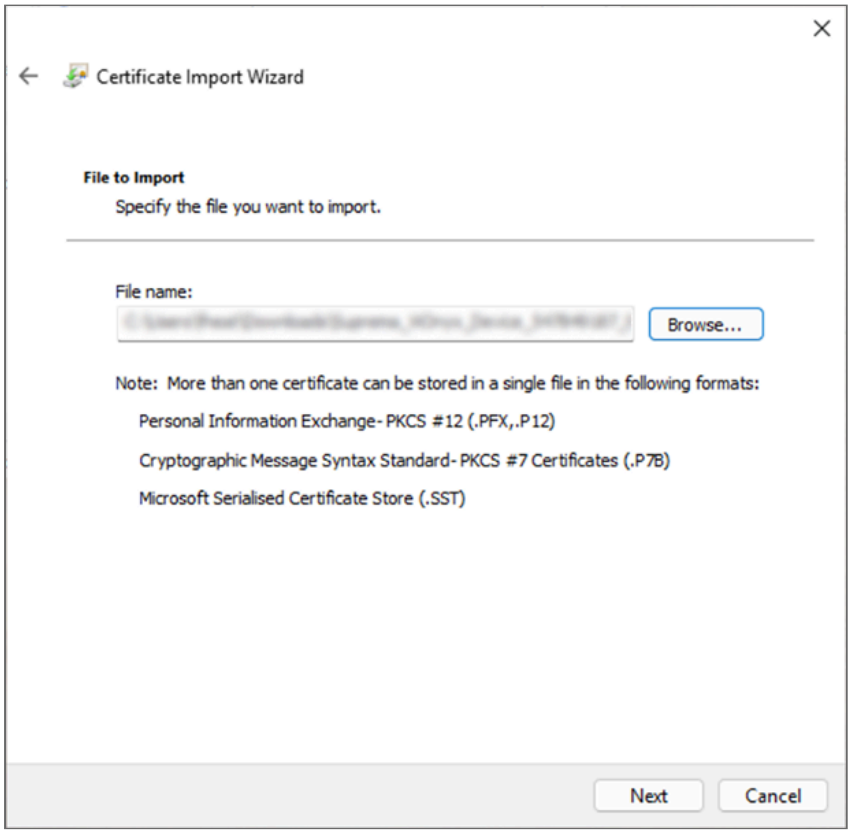
1. In the left panel of the **Management Console**, expand **Trusted Root Certification Authorities**.
2. Right-click **Certificates** under it, then select **All Tasks** → **Import**.



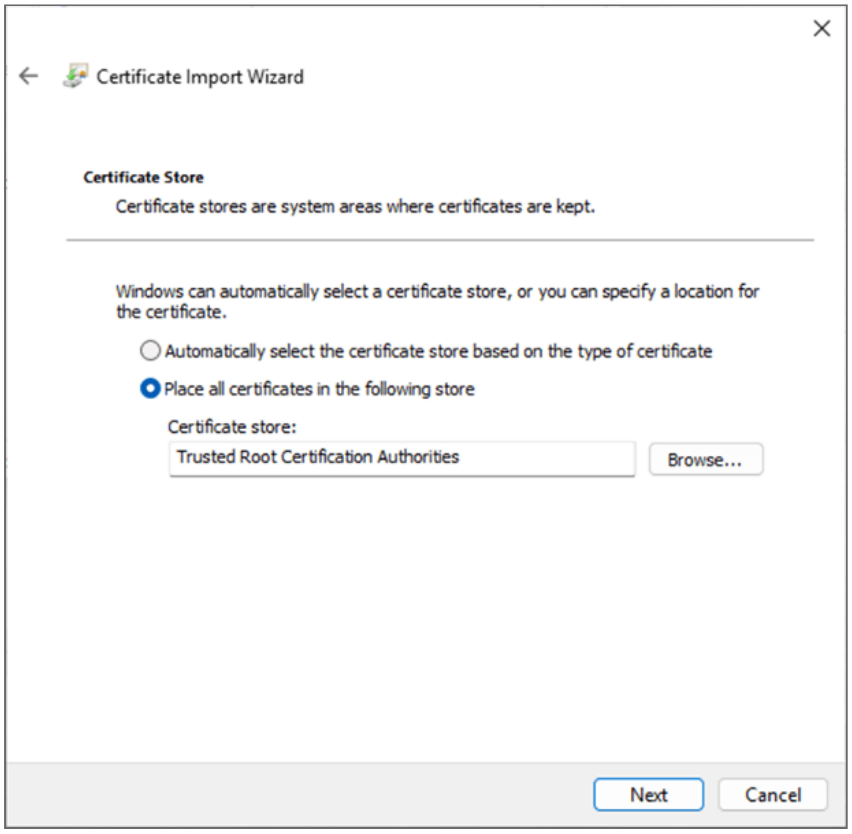
3. In the Certificate Import Wizard, click **Next**.



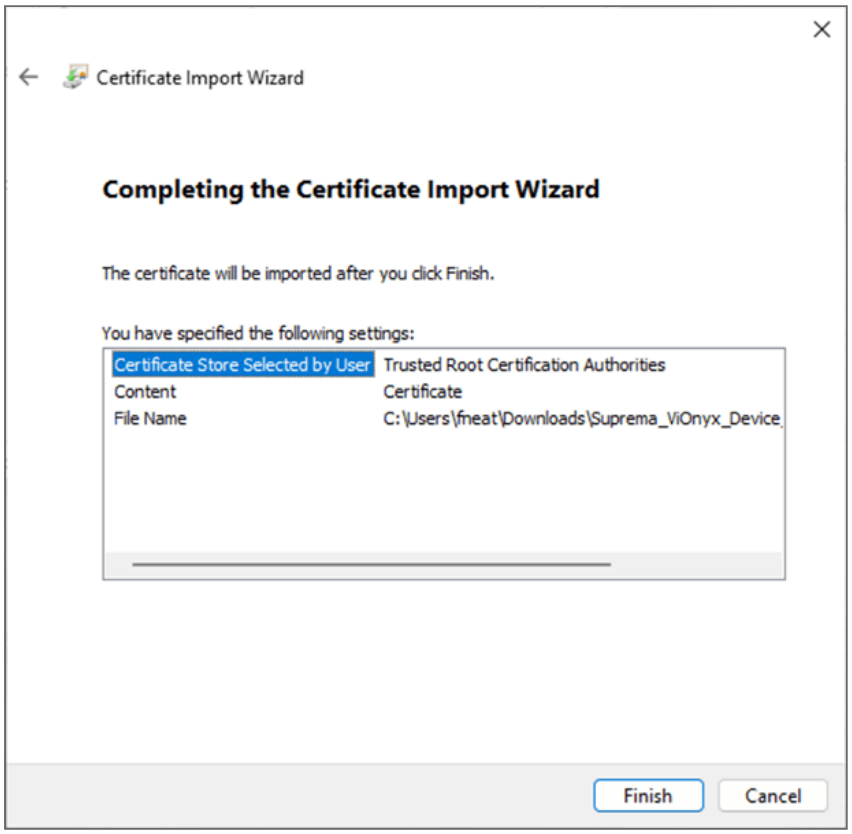
4. Click **Browse** and select the saved certificate file Suprema_ViOnyx_Device_547849187_Root_CA.crt.



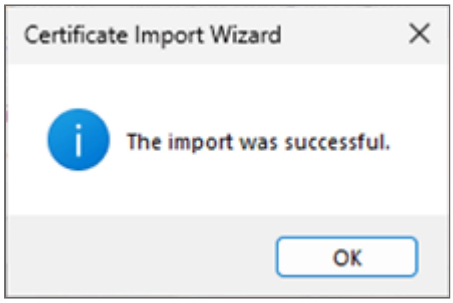
5. Click **Next**.
6. Select **Place all certificates in the following store**.
7. Make sure **Certificate store** is set to **Trusted Root Certification Authorities**.



8. Click **Next**.
9. Click **Finish** to complete the certificate import.

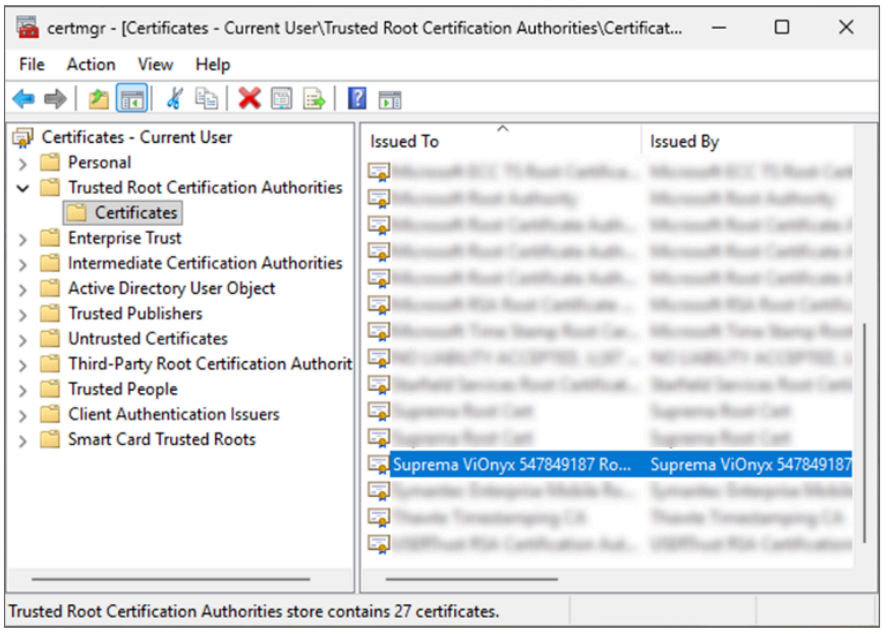


10. If a security warning appears, click **Yes**.
11. When the certificate import success message appears, click **OK**.



4 Verify certificate installation

In the Management Console, select **Trusted Root Certification Authorities** → **Certificates** to confirm that the imported certificate appears in the list.

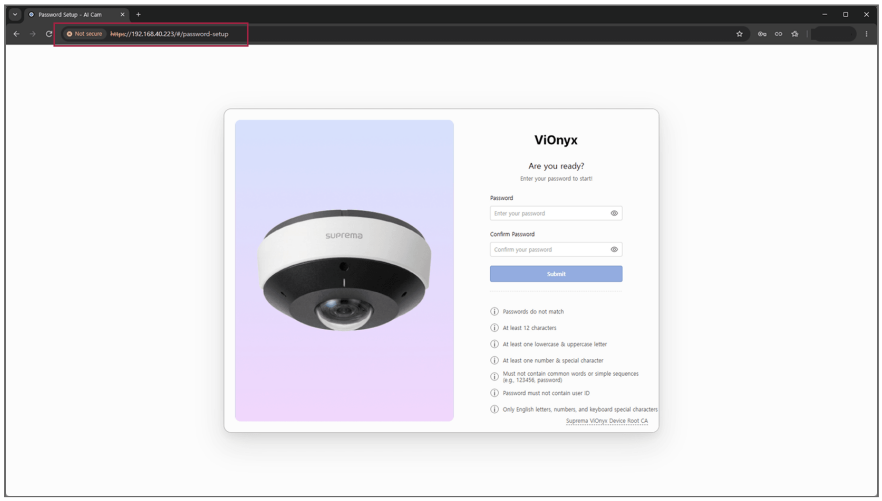


After certificate installation completes, fully close and restart the web browser, then reconnect using the camera's IP address. You now connect securely without a security warning.

Set password

Set a strong password for security when logging in for the first time. ViOnyx enforces a strong password policy to protect system security.

1. Connect to the camera in your web browser using the assigned IP address (`https://{IP_address}`).



2. On the password setup page, enter a new password in the **Password** input field.
3. Re-enter the same password in the **Confirm Password** field.
4. Make sure the password you entered meets all of the following requirements.
5. When all conditions are met, **Submit** becomes active. Click the button to finish setting your password.

Password requirements

The password must meet all of the following requirements:

- The values in the **Password** and **Confirm Password** fields must match exactly.
- The password must be at least 12 characters long. Maximum length: 64 characters.
- Include at least one lowercase letter (`a-z`) and one uppercase letter (`A-Z`).
- Include at least one digit (`0-9`) and one special character.

  > *Example special characters:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

- Do not include sequences of 4 or more consecutive characters (e.g., `1234` , `abcd`) or 4 or more identical characters.
- The username (case-insensitive) must not be included in the password.

  > *admin, Admin, ADMIN, Admin123! etc.*

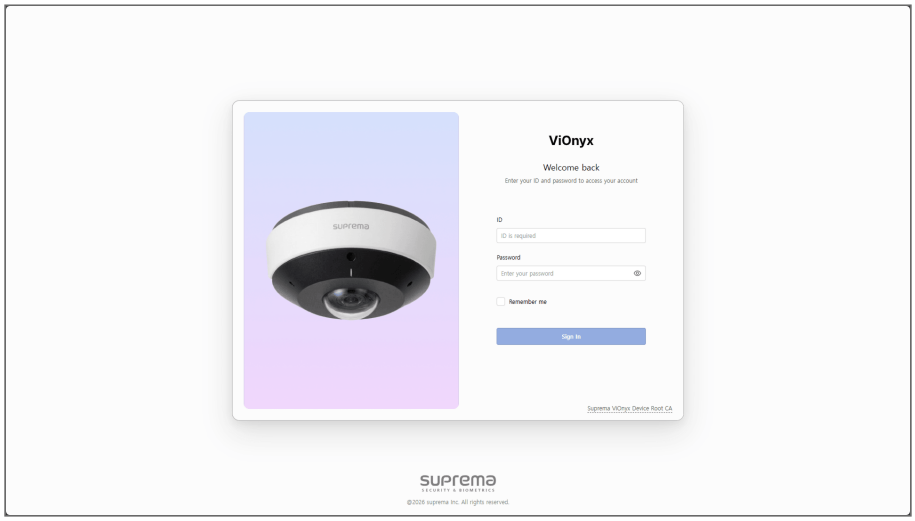
- Common weak passwords such as `password` , `qwerty` , `123456` are not allowed.
- Use only English letters, numbers, and special characters from an English keyboard.

Caution

Store the password you set in a safe place. If you lose the password, initialize the camera.

Sign in

After the password is set, you will be automatically redirected to the sign in page. Enter the administrator ID and the password you set to access the ViOnyx Web server.



1. Enter **admin** in the **ID** input field.
2. Enter the password you set in the **Password** input field.
3. Click **Sign In**.

After successful sign in, the ViOnyx Web Server opens the **Live** page.

> **Info**
> Change the administrator ID (admin) in **System** → **Account**.

Next step

Explains the main features and how to use the **Live** menu.
Configure AI events to monitor specific situations detected by the camera.
Use the camera's settings to maintain optimal image quality for the shooting environment, configure the network, and apply security and privacy policies.
Register users to enable the AI face recognition feature.
Systematically manage device information, firmware, maintenance, accounts, audio, and logs to effectively operate the camera system.

Understanding the User Interface

After signing in to ViOnyx Web Server, the main menu appears at the top. Menus provide quick access to features. This page explains the web server interface structure and each menu's role.



Main menu quick access

The top-left shows the ViOnyx Web Server logo and main menu icons. Features provided by each menu are listed below.

Menu icon	Menu name	Description
	Live	View live video from the camera.
	Settings	Change camera and web server settings.
	AI&Rule	Set AI events and rules.
	People	Add and manage camera system users.
	Access	Link doors, access levels, and user permissions to manage access control. This menu is in beta.
	System	Manage device information, accounts, audio, logs, and other system settings.

> **Info**
> Support for the **Access** menu is included in firmware version 1.1.0 or later.

Information and tools

The top-right shows camera info, language selection, a shortcut to the user guide, and a logout button.

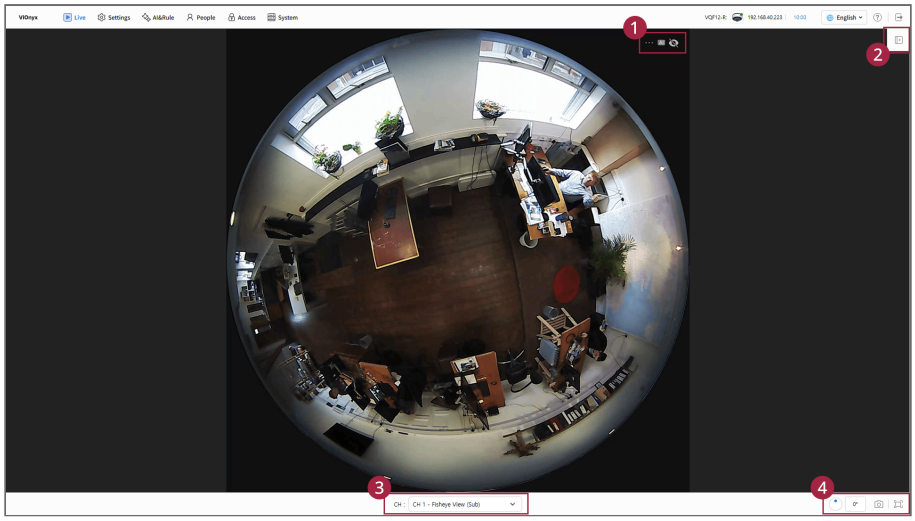
Menu icon	Menu name	Description
	Camera information	View the connected camera's name, status, and IP address. Click **IP Address** to view device information.
10:00	Session time	View the current logged-in administrator's session time. You are automatically logged out when the session time is exceeded.
	Language selection	Change the web interface language.
	User guide shortcut	View the user guide.
	Logout	Log out.

View Live

Use the ViOnyx Web Server **Live** menu to view live camera video. Select the desired channel and view mode, then zoom or view in full screen.

Live view basic layout

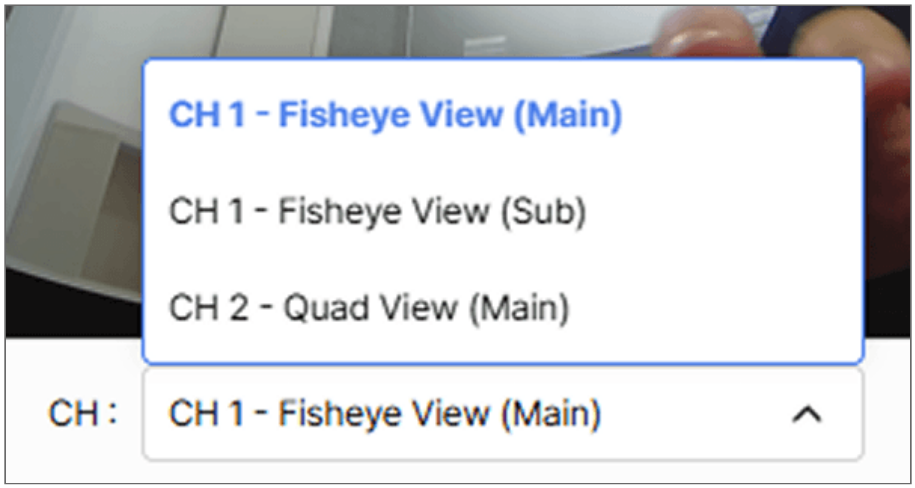
When first entering the **Live** menu, the video appears in the following default state.



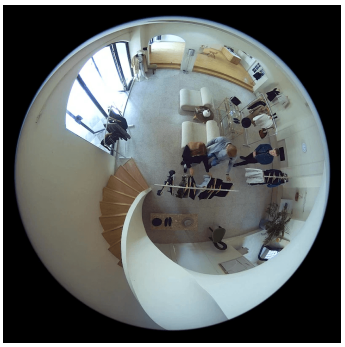
Item	Component	Description
1	AI	- AI features are disabled. Click the icon to enable AI features. - Click ••• and adjust the setting to show or hide AI events and user boxes.
2		Open the **Face Shot**(Face Shot) panel.
3	CH	Select the view mode available for each channel.
4		Rotate the live video.
		Capture the live video.
		View the live video in full screen.

Select channel and view mode

ViOnyx Web Server provides multiple channels and view modes. Select the desired channel and view mode from the **CH** dropdown at the bottom of the screen.



Supported channels and view modes

Channel	View mode	Description	Example
1ch	Fisheye View (Main/ Sub)	Original fisheye-lens video for the primary channel	
2ch	Quad View (Main)	4-split view for the panorama channel	

Info

- Each channel's Main and Sub streams provide different resolutions. Main is the high-quality stream; Sub is the low-quality stream.
- The image is an example screen. The actual screen may differ.

Zooming

Use the mouse to zoom in and out.

- Scroll up: Zoom in
- Scroll down: Zoom out
- Double-click: Return to original size (1x)

> **Info**
>
> - Zoom range: 1x ~ 8x.
> - Zoom uses digital magnification, so the image may become blurry at high zoom levels.

Rotate the screen

Click and drag to rotate the live video. Or enter the rotation angle directly in the input field to the right of the button.



Screen capture

Click to capture the live video. The captured image is saved in the `capture_{ch1|ch2}_{main|sub}_{YYYY-MM-DDTHH-MM-SS}.jpeg` format.



Full-screen mode

Use full-screen mode to view the video in a larger size. Click ⛶ at the bottom right of the screen.



- View-mode changes and zoom remain available in full-screen mode.
- To exit full screen mode, press the ESC key or click ⤡ again.

AI display options

Click ••• at the top right of the screen to set AI display options for the live video.



- **Event Box Popup**: When an AI event occurs, the event appears as a pop-up at the top left of the live video.
- **User Box Popup**: When a face is detected through an AI event, the user box appears as a pop-up at the bottom right of the live video.
- **Default Opacity**: Adjust the opacity of event pop-ups and user pop-ups.
- **Reference Point**: Show a reference point above the person detection box in the live video. Enable this option to show a legend at the top right of the video.
  - Light blue dot (🔵): Center of the box.
  - Red dot (🔴): 80% from the top along the box's long axis. If the camera is installed on the ceiling facing down, it appears near the person's feet.

Info

- The pop-up stays visible for the time set in the **Display Time** option (in seconds).
- The **Reference Point** option can be used only when the AI feature (AI 👁) is enabled.
- Firmware version 1.1.0 or later includes support for the **Default Opacity** and **Reference Point** options.

Open the Face Shot panel

If you enabled the AI event feature, you can check faces detected through the camera. To open the **Face Shot** panel, click at the top right of the screen.



Click the tool icons at the top of the **Face Shot** panel to use these features:

- / : Pause or resume Face Shot.
- : Filter Face Shot results.
- : Expand the **Face Shot** panel to full screen.

> **Info**
> For more information about AI event and rule settings, see Manage AI Events.

When video does not play

If the camera video does not load, follow these steps to check the network connection.

1. Check the camera and network connections.
2. Press **Refresh (F5)** in your web browser.
3. The system automatically tries to reconnect.

Manage AI Events

Setting AI events and rules lets the camera automatically execute required actions for detected situations. Create an AI event for each situation, then link the action for the event to an AI rule.

Create AI events for surveillance goals such as motion, zone intrusion, line crossing, people count, and door approach. In AI rules, specify audio, webhook, and relay actions, and apply schedules to limit when actions run. Adjust facial authentication options in advanced settings for your environment.

> **Info**
> To use AI events, set at least one facial area that applies to all events.

Set Up User Tracking Events

Create user tracking events to detect entry into restricted areas. Optionally add face areas to prioritize face tracking in specific zones; registered users are automatically identified.

When to use this?

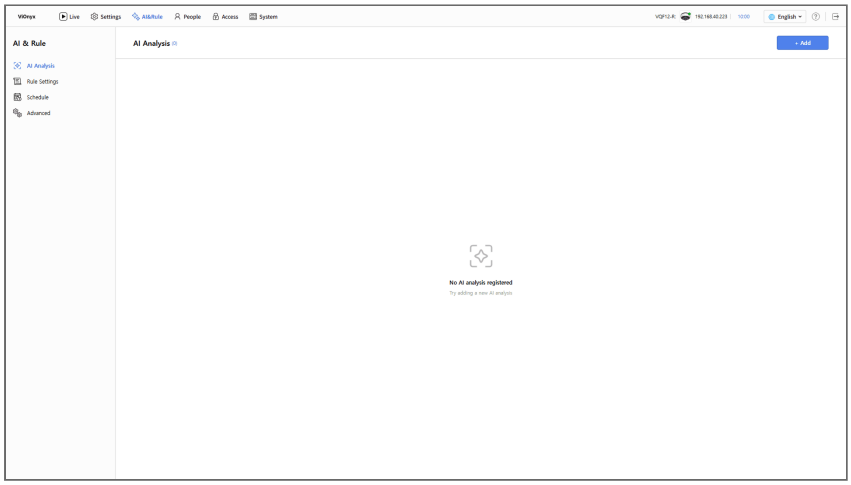
- Monitor entry and exit of employees or customers registered to the entry area.
- Monitor access to secure areas (meeting rooms, storage).
- Track customer flow into specific store corners (new products, event zones).

Create people tracking events

Create user tracking events to track people's movement in real time in Live View. Additionally, setting face areas recognizes registered users and identifies who moved.

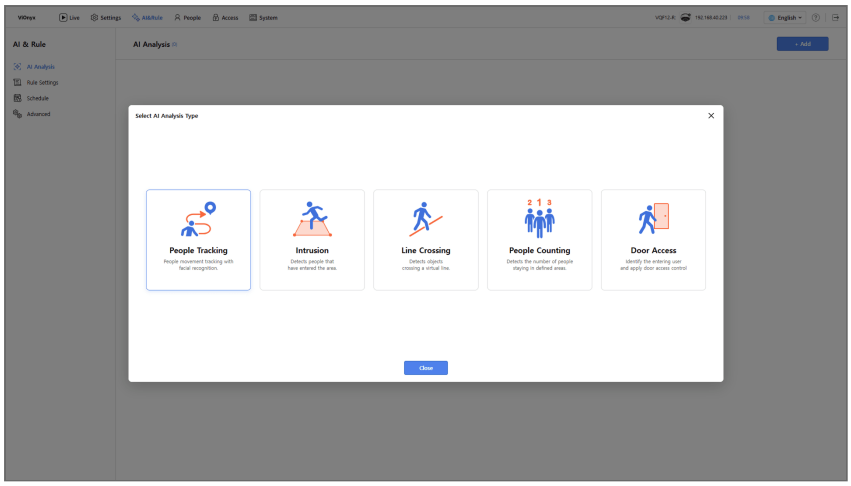
1 Start event creation

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.

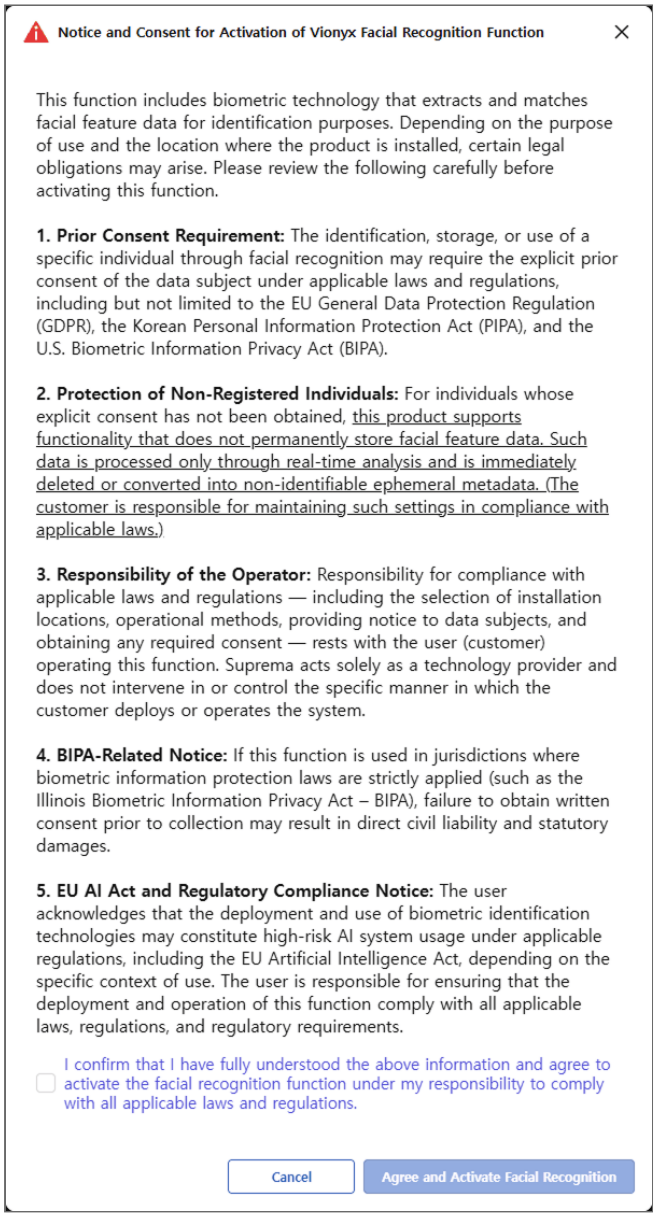


3. Click **+ Add** at the top right of the screen.

4. Click **People Tracking** in the **Select AI Analysis Type** window.

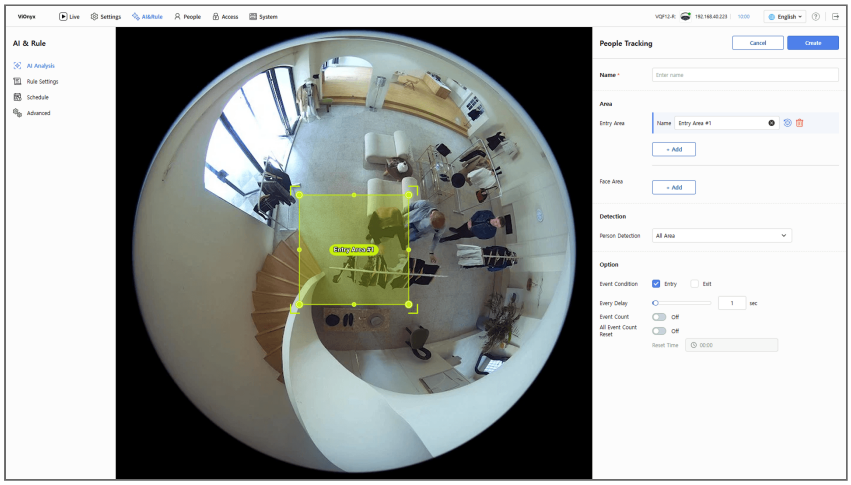


5. When the **Notice and Consent for Activation of Vionyx Facial Recognition Function** pop-up appears, review the details, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- To use the Facial Authentication feature, comply with local regulations. Cannot proceed without consent.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once. Subsequent AI event creation assumes consent.

6. Complete the necessary settings in the right **People Tracking** panel.

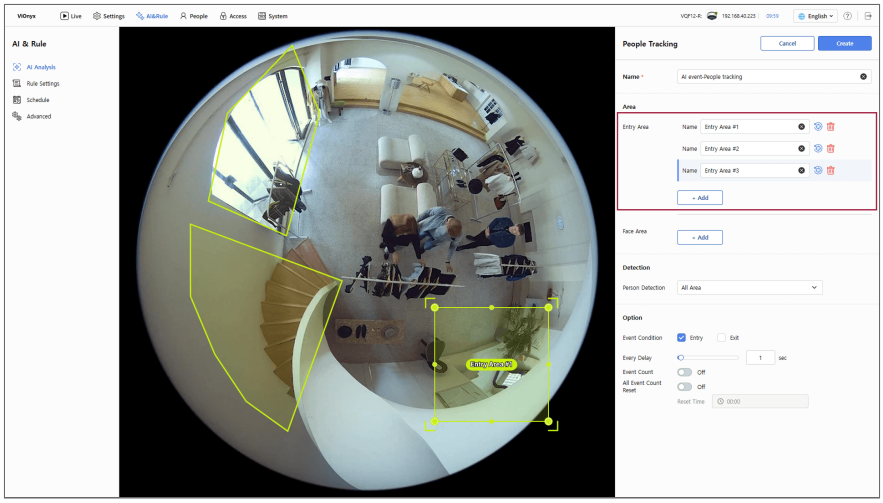


2 Set event name

Enter the AI event name in the **Name** input field. The name can be up to 64 characters long.

3 Entry area settings

Define the entry area to track. The camera detects entries and exits in the configured area. Set at least one virtual line. Click **+ Add** to add up to 10. A yellow box appears in Live view. Drag the corners or points with the mouse to adjust the shape. Drag the center to move the line.



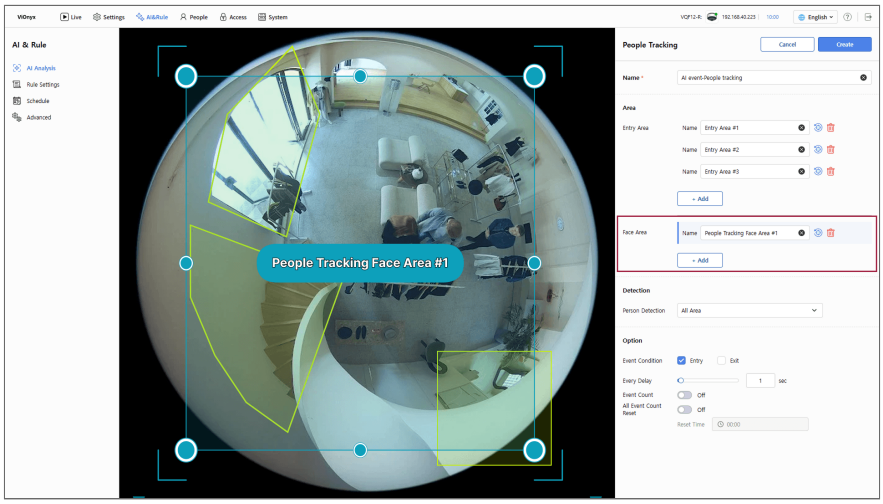
- **Name**: Edit the entry area name. Assign a clear, descriptive name. The entry area name appears on mouse hover in Live view.

Info

- Click to reset the shape and size of the configured entry area.
- Click to delete an added entry area.

4 Face area settings (optional)

Define the area for face detection. When set, the system prioritizes face tracking in that area. Set the face area to include the entry area. If the face area does not include the entry area, the camera cannot recognize faces. Click **+ Add** to add up to 10 face areas. A blue box appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.



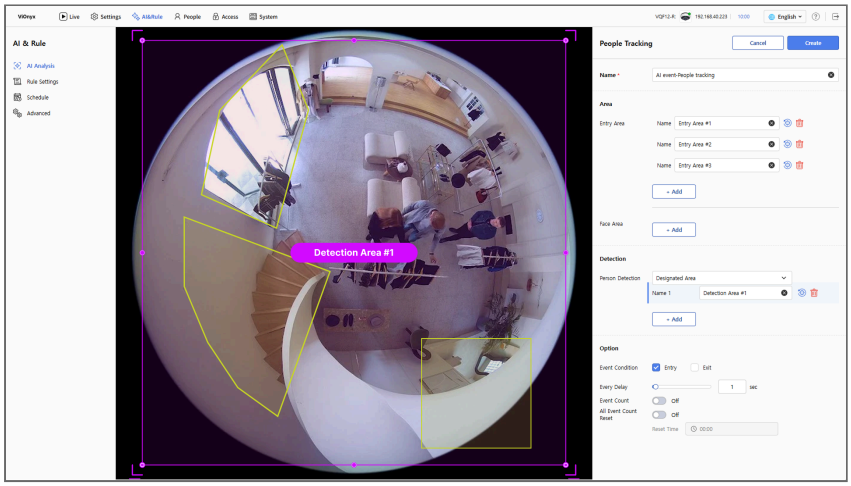
- **Name**: Edit the face area's name. Assign a clear, descriptive name. The face area name appears on hover in Live View.

> **Info**
>
> - Enrolled users are automatically identified in the **Live** menu and shown by name. Unenrolled users appear as **Unknown Face**.
> - Click to reset the configured face area's shape and size.
> - Click to delete an added face area.
> - In camera settings, if you use the **Adaptive AE mode** option, configure it so that the face area includes the position where a person would actually stand or pass by and their face is clearly visible.

5 Person detection settings (optional)

In the **Detection** section, select the area where the camera detects people. Narrow the detection area as needed to reduce false detections in irrelevant areas (hallway ends, windows, reflective surfaces, etc.).

- **All Area**: Default. Detects people across the entire screen. Available regardless of whether face areas are set.
- **Designated Area**: Detects people only within the area you specify. Available only when no face area is set. Set at least one virtual line. Click **+ Add** to add up to 10. A purple box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



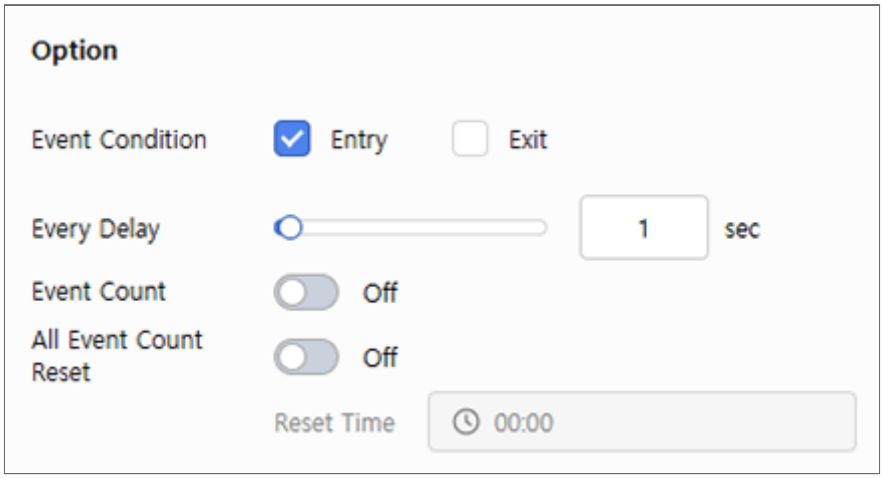
  - **Name**: Edit the name of the person detection area.

- **Face Area Only**: Detects people only within the face area. Available only when a face area is set.

> **Info**
>
> - Adding a face area while **Designated Area** is selected opens the **Notice** pop-up. Click **OK** to clear the designated detection area and switch to **Face Area Only**.
> - Deleting all face areas while **Face Area Only** is selected automatically switches to **All Area**.
> - In camera settings, when you use the **Adaptive AE mode** option, narrow the range to **Designated Area** or **Face Area Only**. Keep screens, photos, or posters with faces out of the detection area.
> - Click to initialize the shape and size of the person detection area.
> - Click to delete the added person detection area.
> - Firmware version 1.1.0 or later supports this feature.

6 Set event trigger conditions and event count settings

In the **Option** section, set the event trigger conditions and event count.



- **Event Condition**: Select the action that triggers an event. Optionally, select both **Entry** and **Exit**.

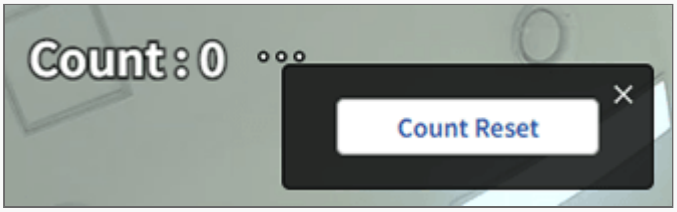
- **Every Delay**: Set the minimum duration to treat as an event. An event occurs only when the detection state lasts longer than the set time. It can be set up to a maximum of 60 seconds.

  > If too many events occur, increase the **Every Delay** value. Motion detected for less than the set time is not treated as an event, reducing unnecessary events.

- **Event Count**: Set to **On** to count the number of times people enter or exit the entry area. The system counts entries and exits separately. If multiple entry areas exist, it counts each area separately.

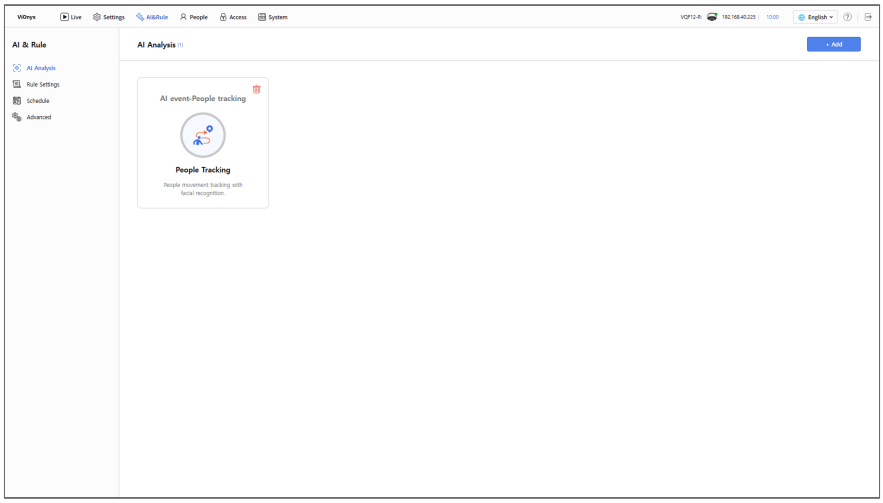
  > The system counts only the options selected under **Event Condition**. For example, if only **Entry** is selected, only entries appear as events, and the system records them in logs.

- **All Event Count Reset**: Set to **On** to initialize event counts for all entry areas daily at the specified time. The system initializes event counts for all entry areas at the time set in **Reset Time**.

> **Info**
>
> - If you set **Event Count** to **On**, **Live** menu will display **Count : N** for each entry area on the video. Click the ••• button and select **Count Reset** to initialize the event count manually.
>
> 
>
>
> - Support for event count options is included in firmware version 1.1.0 or later.

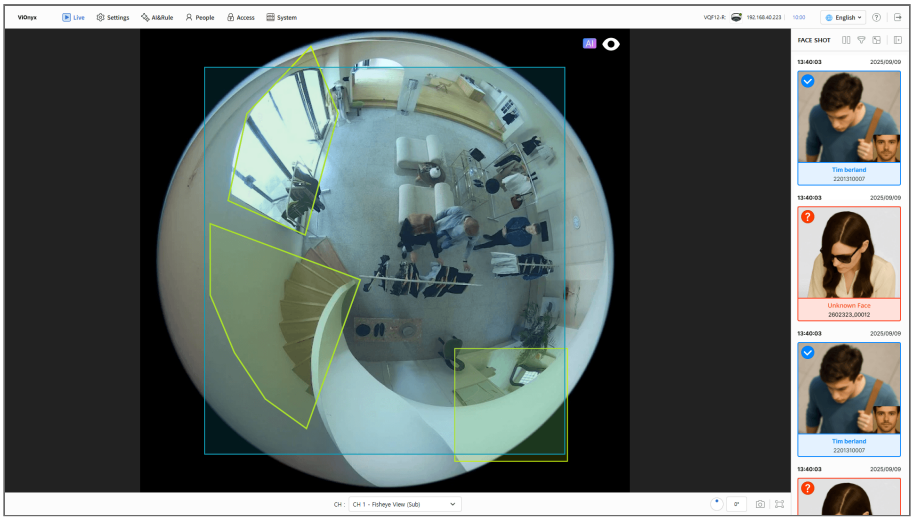
7 Save settings

After completing all settings, click **Create** in the top right. The interface returns to the previous screen, and the new AI event is added to the list.



Check in Live

Click the **Live** menu at the top left of the screen. Confirm the AI icon at the top right of the camera feed is on. The configured entry and face areas appear as overlays on the video. An event triggers whenever a person enters or exits an entry area. If face areas are set, the camera detects faces there; registered users are automatically identified, and their names appear.



Info

- Unenrolled users appear as **Unknown Face**. Registered users appear with their names.
- If the camera fails to recognize faces, enable the **Min Face Size Visualize** option. Alternatively, enlarge the face area or adjust the camera position.
- Poor lighting or backlight may prevent the camera from detecting faces. Improve area lighting or adjust the camera position and angle so faces are clearly visible.
- Faces must face the camera to be detected. Profile or rear views may not be detected.
- If no events occur in the entry area, verify that the face area includes it.

Set Up Intrusion Detection Events

An intrusion detection event generates a real-time event whenever a person enters or exits an administrator-defined area. Optionally add face areas to prioritize face tracking within those zones; enrolled users are automatically authenticated. Get real-time alerts when unauthorized people enter areas that require monitoring.

When to use this?

- Real-time intrusion detection for unauthorized people in areas that require security
- Get real-time alerts when someone enters outside business hours or an area that requires monitoring
- Detect when unregistered people enter a monitoring area
- Record and track access to high-risk areas.

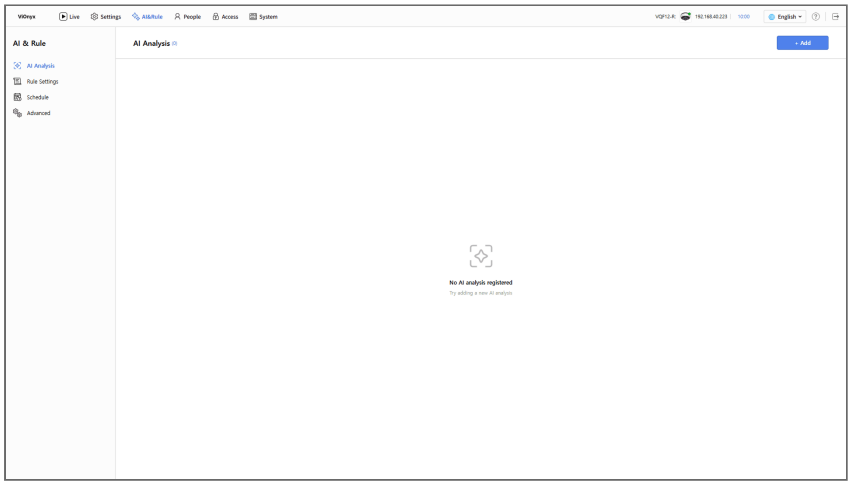
> **Info**
> Use this for purposes other than access control, and the camera does not determine whether access is restricted.

Create intrusion detection event

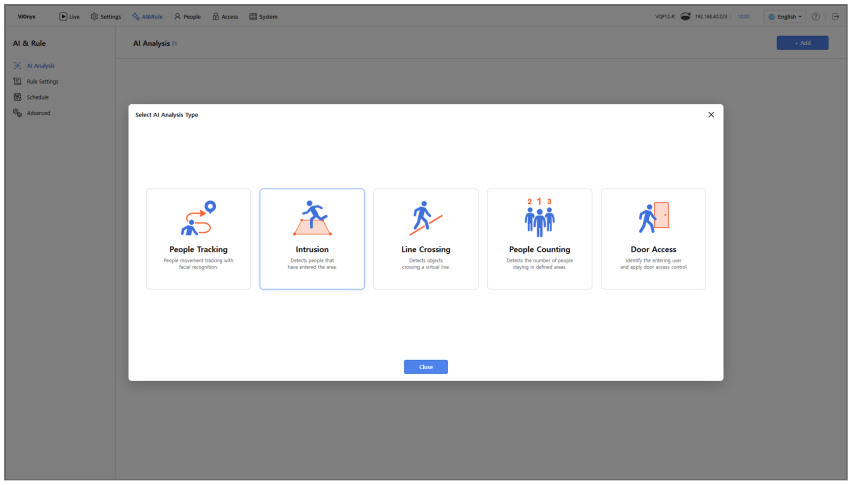
Creating an intrusion detection event lets the **Live** menu detect when a person enters a specific area and generate events. Also, setting a face area prioritizes face tracking in that area; enrolled users are automatically identified.

1 Start event creation

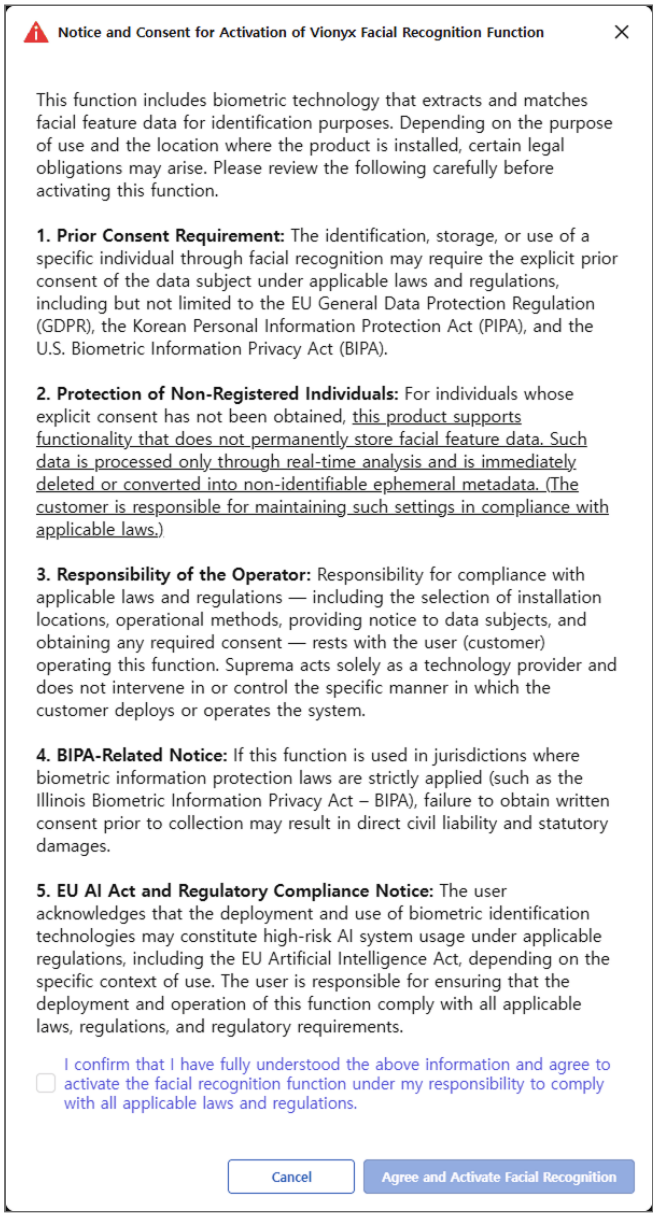
1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. Click **Intrusion** in the **Select AI Analysis Type** window.

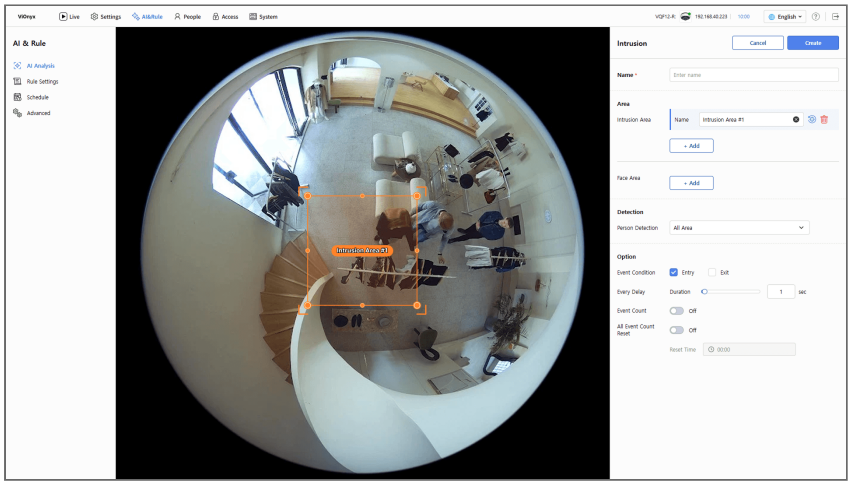


5. When the **Notice and Consent for Activation of Vionyx Facial Recognition Function** pop-up appears, review the details, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- To use the Facial Authentication feature, comply with local regulations. Cannot proceed without consent.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once. Subsequent AI event creation assumes consent.

6. Complete the required settings in the **Intrusion** panel on the right.

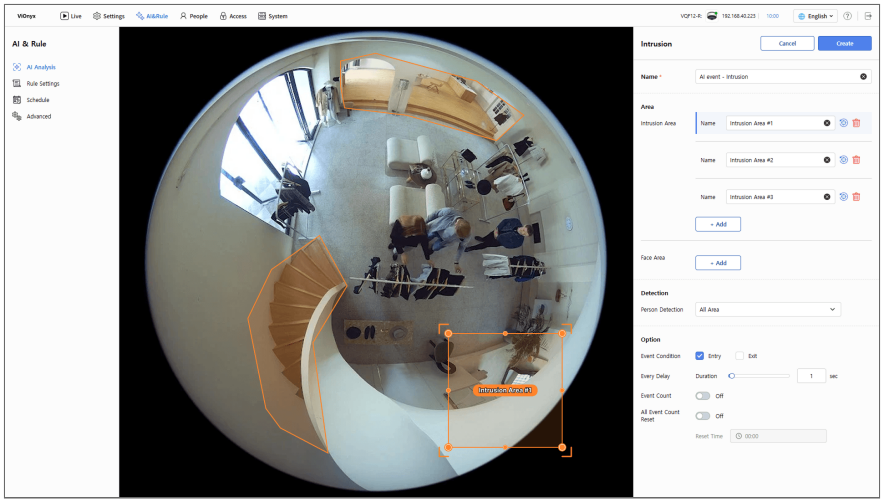


2 Set event name

Enter the AI event name in the **Name** input field. The name can be up to 64 characters long.

3 Intrusion area settings

Set the intrusion area. The camera detects entries and exits in the configured area. Set at least one virtual line. Click **+ Add** to add up to 10. An orange box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



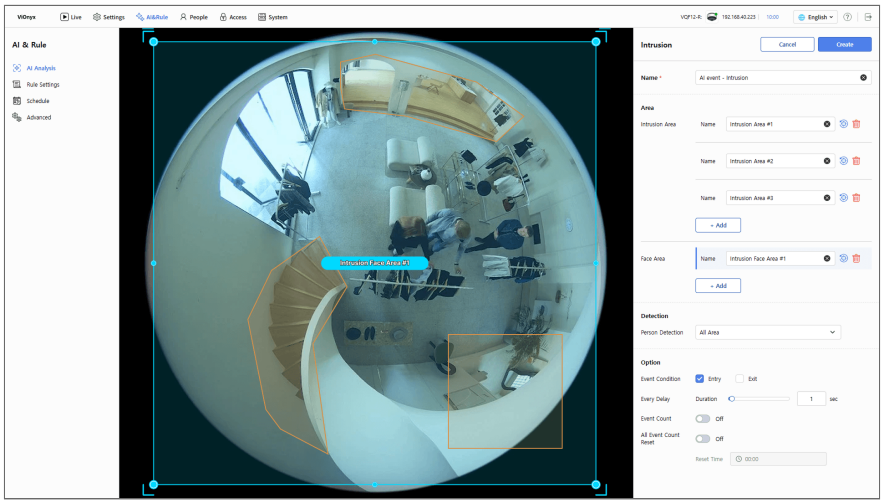
- **Name**: Edit the name of the intrusion area. Assign a clear, descriptive name. The intrusion area name appears on mouse-over in the live view.

Info

- To initialize the shape and size of a configured intrusion area, click .
- To delete an added intrusion area, click .

4 Face area settings (optional)

Define the area for face detection. When set, the system prioritizes face tracking in that area. Classify people detected in face areas as authenticated users or unauthorized persons to clearly identify authorized entrants and intruders. Face areas and intrusion areas can overlap. Click **+ Add** to add up to 10 face areas. A blue box appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.



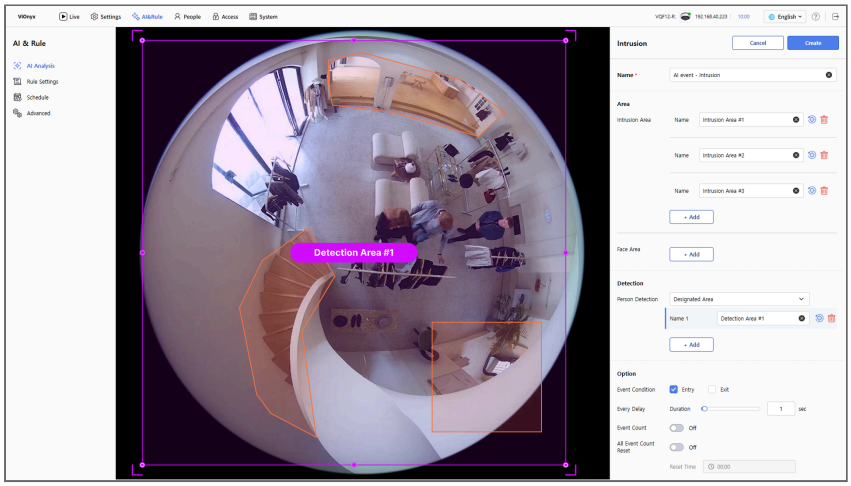
- **Name**: Edit the face area's name. Assign a clear, descriptive name. The face area name appears on hover in Live View.

> **Info**
>
> - Enrolled users are automatically identified in the **Live** menu and shown by name. Unenrolled users appear as **Unknown Face**.
> - Click to reset the configured face area's shape and size.
> - Click to delete an added face area.
> - In camera settings, if you use the **Adaptive AE mode** option, configure it so that the face area includes the position where a person would actually stand or pass by and their face is clearly visible.

5 Person detection settings (optional)

In the **Detection** section, select the area where the camera detects people. Narrow the detection area as needed to reduce false detections in irrelevant areas (hallway ends, windows, reflective surfaces, etc.).

- **All Area**: Default. Detects people across the entire screen. Available regardless of whether face areas are set.
- **Designated Area**: Detects people only within the area you specify. Available only when no face area is set. Set at least one virtual line. Click **+ Add** to add up to 10. A purple box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



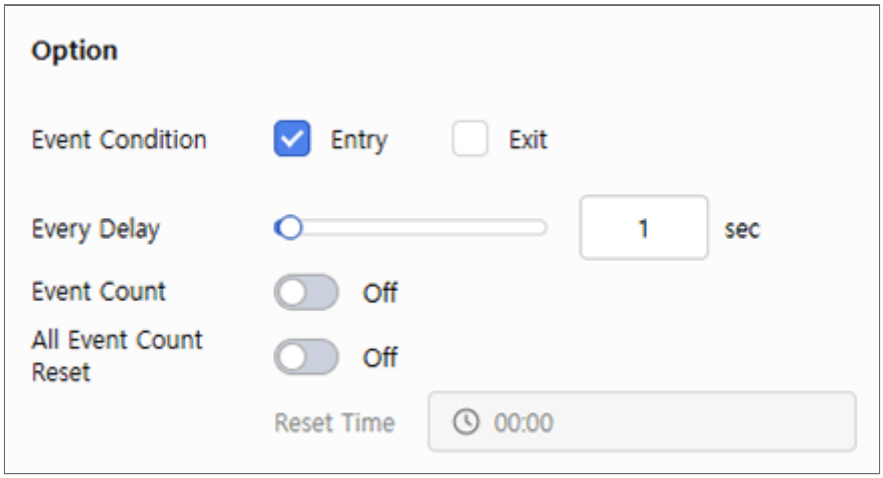
  - **Name**: Edit the name of the person detection area.

- **Face Area Only**: Detects people only within the face area. Available only when a face area is set.

> **Info**
>
> - Adding a face area while **Designated Area** is selected opens the **Notice** pop-up. Click **OK** to clear the designated detection area and switch to **Face Area Only**.
> - Deleting all face areas while **Face Area Only** is selected automatically switches to **All Area**.
> - In camera settings, when you use the **Adaptive AE mode** option, narrow the range to **Designated Area** or **Face Area Only**. Keep screens, photos, or posters with faces out of the detection area.
> - Click to initialize the shape and size of the person detection area.
> - Click to delete the added person detection area.
> - Firmware version 1.1.0 or later supports this feature.

6 Set event trigger conditions and event count settings

In the **Option** section, set the event trigger conditions and event count.



- **Event Condition**: Select the action that triggers an event. Optionally, select both **Entry** and **Exit**.

- **Every Delay**: Set the minimum duration to treat as an event. An event occurs only when the detection state lasts longer than the set time. It can be set up to a maximum of 60 seconds.

> If too many events occur, increase the **Every Delay** value. Motion detected for less than the set time is not treated as an event, reducing unnecessary events.

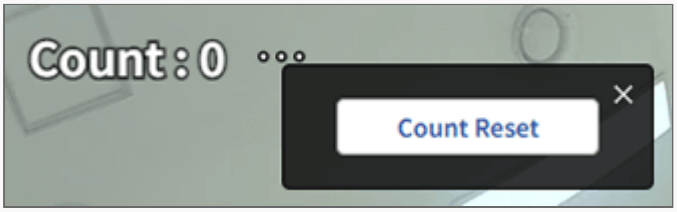
- **Event Count**: Set to **On** to count entries and exits for an intrusion area. The system counts entries and exits separately for each intrusion area.

> The system counts only the options selected under **Event Condition**. For example, if only **Entry** is selected, only entries appear as events, and the system records them in logs.

- **All Event Count Reset**: Set to **On** to initialize event counts for all intrusion areas daily at the specified time. The system initializes event counts for all intrusion areas at the time set in **Reset Time**.

Info

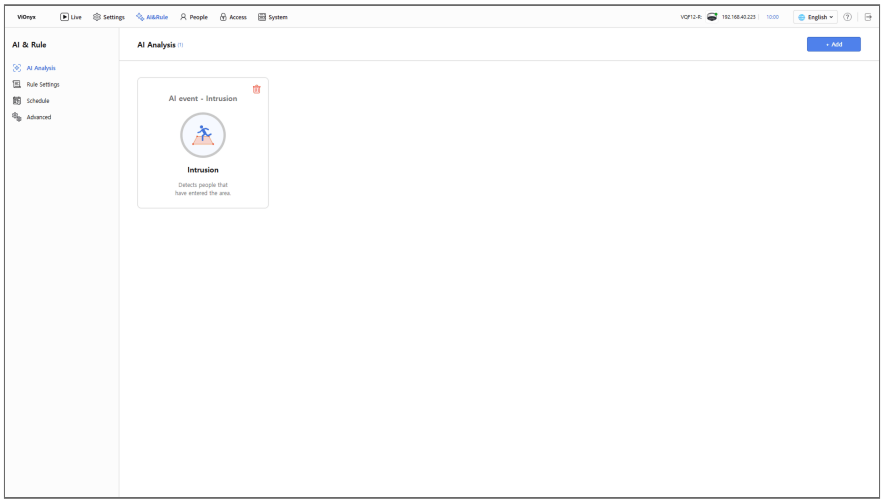
- If **Event Count** is set to **On**, in the **Live** menu, **Count : N** is displayed for each intrusion area above the video. Click the ••• button and select **Count Reset** to initialize the event count manually.



- Support for event count options is included in firmware version 1.1.0 or later.

7 Save settings

After completing all settings, click **Create** in the top right. The interface returns to the previous screen, and the new AI event is added to the list.



Check in Live

Click the **Live** menu at the top left of the screen. Confirm the AI icon at the top right of the camera feed is on. Configured intrusion areas and face areas are overlaid on the video. An event occurs whenever a person enters or exits an intrusion area. If face areas are set, the camera detects faces there; enrolled users are automatically identified and their names are displayed.



Info

- Unenrolled users appear as **Unknown Face**. Enrolled users appear with their name.
- Poor lighting or backlight may prevent the camera from detecting faces. Improve area lighting or adjust the camera position and angle so faces are clearly visible.
- Faces must face the camera to be detected. Profile or rear views may not be detected.

Set Up Line-Crossing Detection Event

Setting up a line-crossing detection event detects people who cross configured virtual lines and triggers real-time events. Specify the crossing direction (A→B, B→A, or both) to monitor a specific direction only. Optionally add a face area to prioritize face tracking; enrolled users are automatically identified.

When to use this?

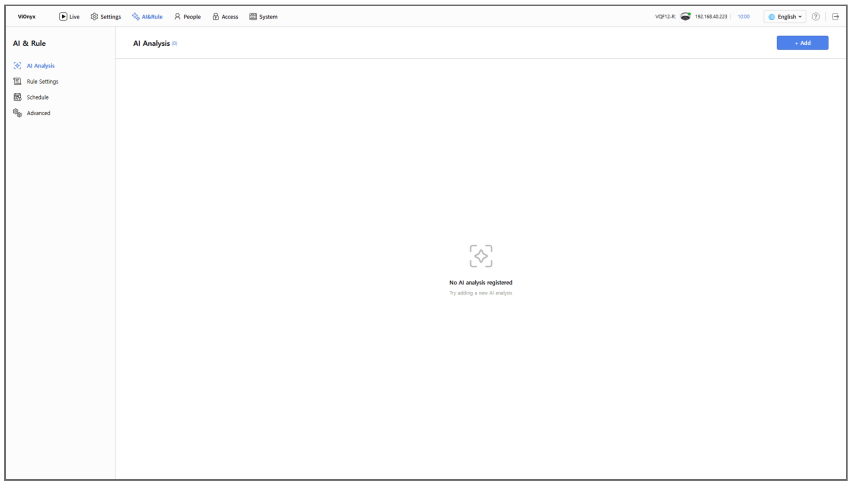
- Monitor and count doorway traffic
- Monitor entry in a specific direction only (detect one-way traffic)
- Detect entry into specific areas outside business hours
- Track left/right area movement relative to the line

Create line-crossing detection event

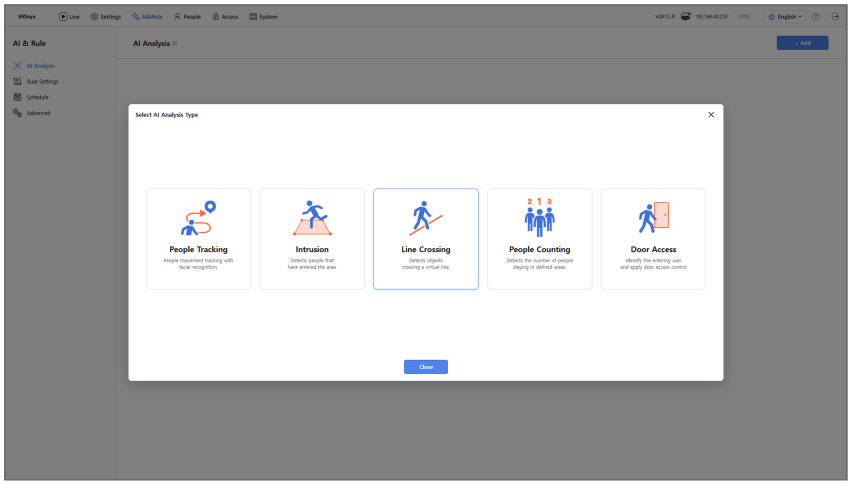
Use the **Live** menu to detect people crossing a configured line in a specific area and trigger events. Also, setting a face area prioritizes face tracking in that area; enrolled users are automatically identified.

1 Start event creation

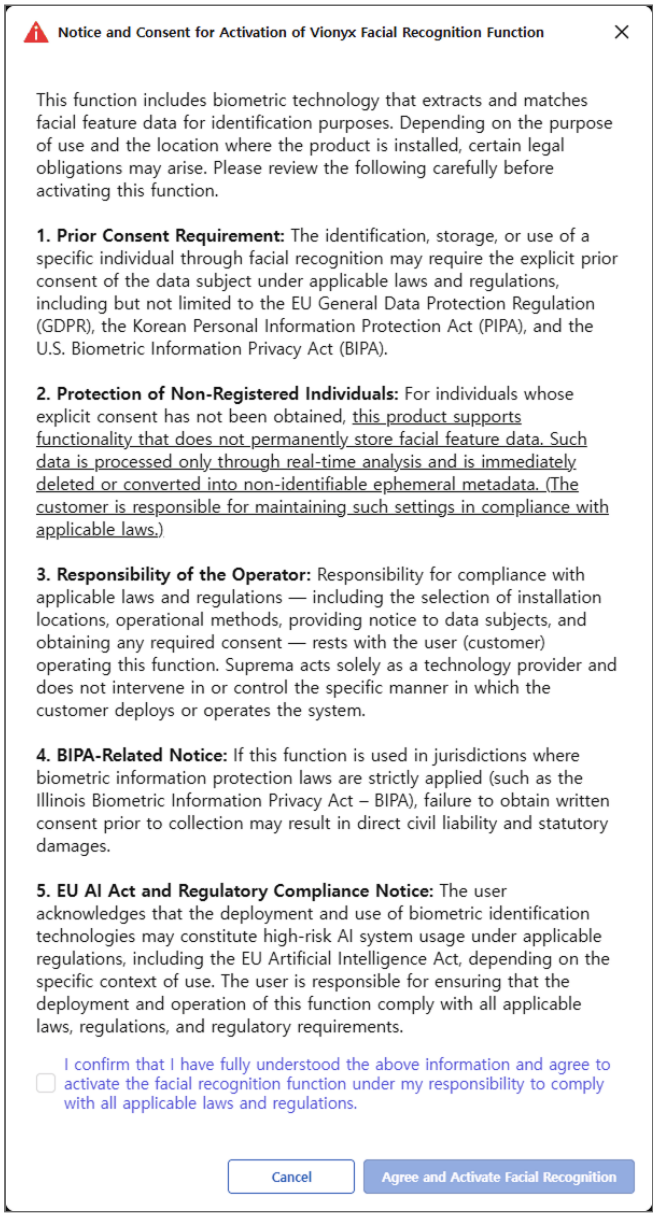
1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. In the **Select AI Analysis Type** window, click **Line Crossing**.

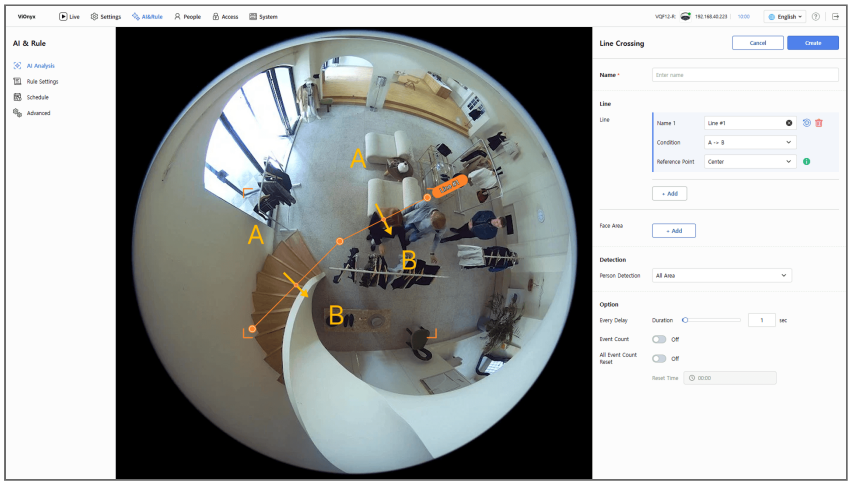


5. When the **Notice and Consent for Activation of Vionyx Facial Recognition Function** pop-up appears, review the details, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- To use the Facial Authentication feature, comply with local regulations. Cannot proceed without consent.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once. Subsequent AI event creation assumes consent.

6. Complete the required settings in the right **Line Crossing** panel.

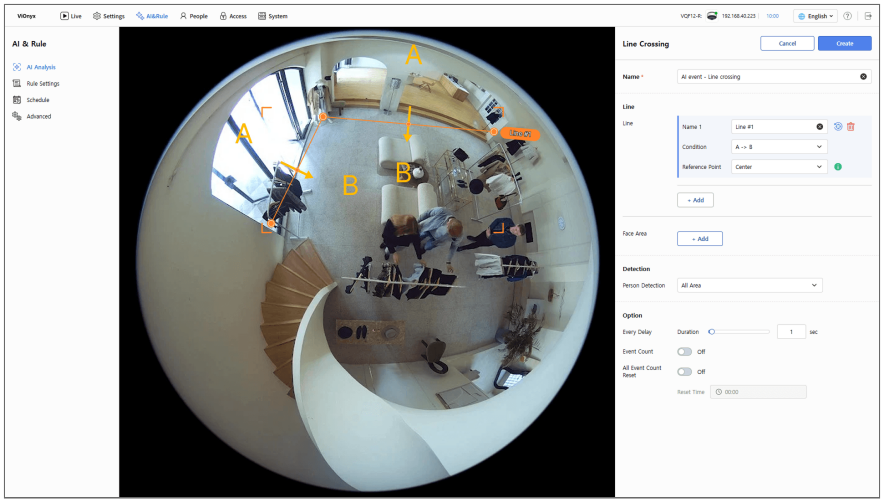


2 Set event name

Enter the AI event name in the **Name** input field. The name can be up to 64 characters long.

3 Virtual line settings

Place the virtual line at the appropriate location in Live View. The camera detects people crossing configured virtual lines and triggers events. Set at least one virtual line. Click **+ Add** to add up to 10. An orange line appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.

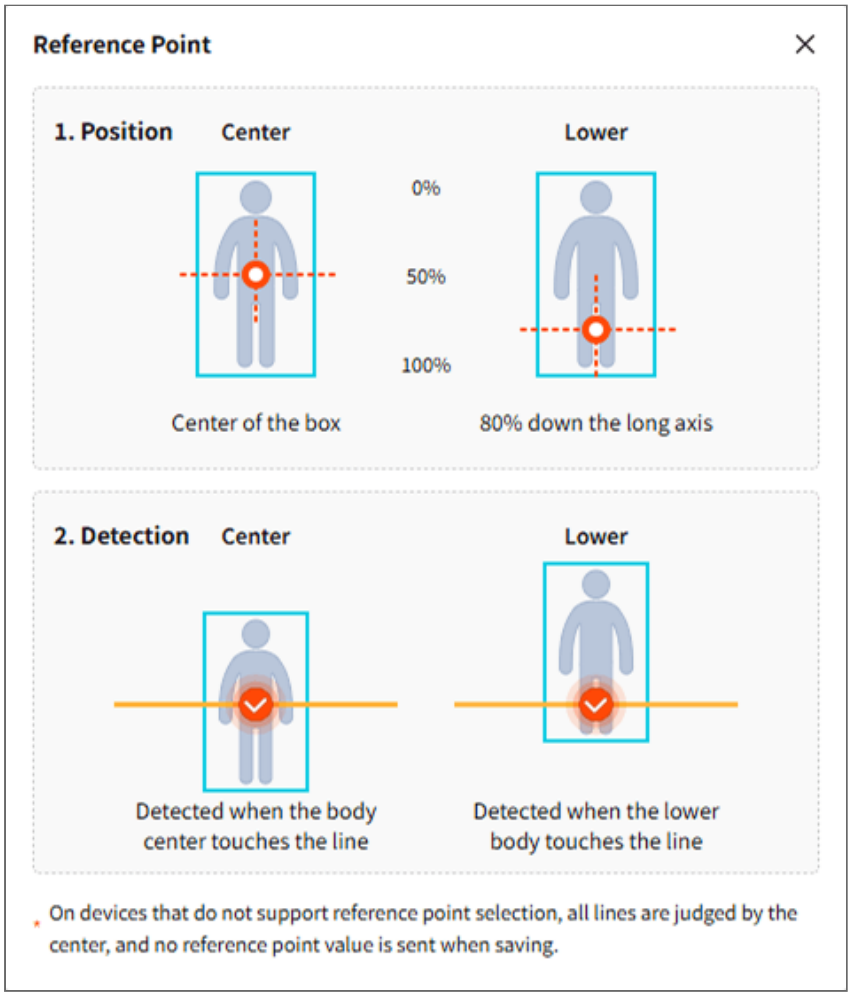


- **Name**: Edit the virtual line's name. Assign a clear, descriptive name. The virtual line name appears on hover in Live View.
- **Condition**: Set the crossing condition for the virtual line. Select one of the three direction options below.
  - **A -> B**: Trigger an event when crossing from A to B.
  - **B -> A**: Trigger an event when crossing from B to A.
  - **A <-> B**: Trigger an event when crossing in both directions.
- **Reference Point**: Select the reference point in the person detection box to determine whether a person crosses a virtual line. Set this per line. The default is **Center**.

– **Center**: Use the center of the box as the reference point. The system counts a crossing when the body center touches the line.

– **Lower**: Use the point 80% down from the top along the box's long axis. The system counts a crossing when the lower body touches the line. Select this option to trigger an event when feet cross the line, as if it were on the floor.

Click the icon to the right of **Reference Point** to view the location and detection criteria for each reference point in a diagram.

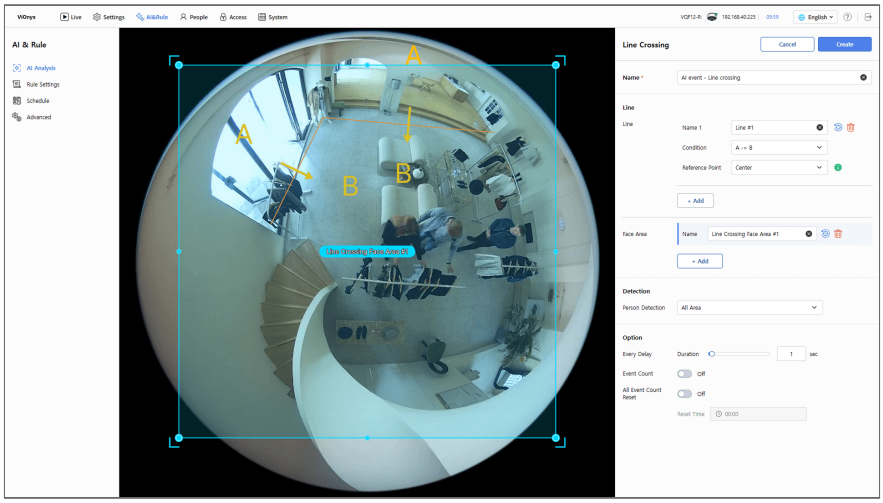


Info

- Support for the **Reference Point** option is included in firmware version 1.1.0 or later. On devices that do not support reference point selection, all line crossings use **Center**.
- **Lower** is a position calculated from the person detection box, not the actual foot position.
- Enable **Reference Point** in AI display options to check the reference point in the **Live** menu.
- Click to reset the configured virtual line's shape and size.
- Click to delete an added virtual line.

4 Face area settings (optional)

Define the area for face detection. When set, the system prioritizes face tracking in that area. Face areas can overlap with virtual lines. Click **+ Add** to add up to 10 face areas. A blue box appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.



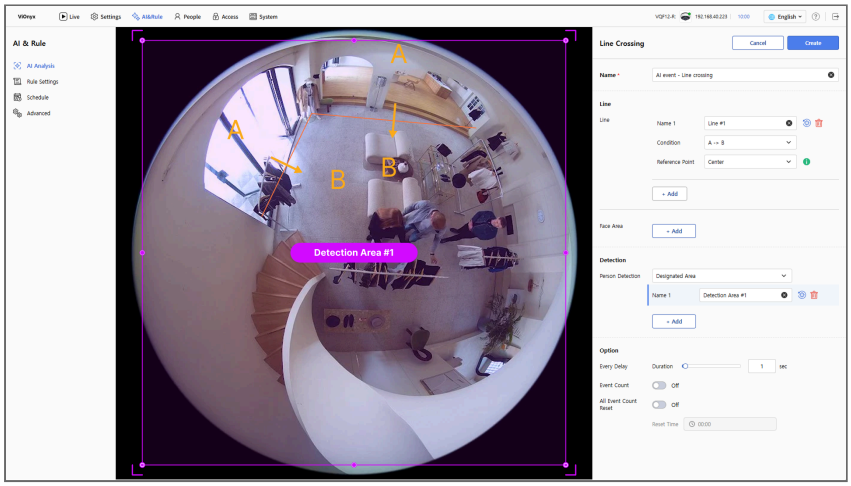
- **Name**: Edit the face area's name. Assign a clear, descriptive name. The face area name appears on hover in Live View.

> **Info**
>
> - Enrolled users are automatically identified in the **Live** menu and shown by name. Unenrolled users appear as **Unknown Face**.
> - Click to reset the configured face area's shape and size.
> - Click to delete an added face area.
> - In camera settings, if you use the **Adaptive AE mode** option, configure it so that the face area includes the position where a person would actually stand or pass by and their face is clearly visible.

5 Person detection settings (optional)

In the **Detection** section, select the area where the camera detects people. Narrow the detection area as needed to reduce false detections in irrelevant areas (hallway ends, windows, reflective surfaces, etc.).

- **All Area**: Default. Detects people across the entire screen. Available regardless of whether face areas are set.
- **Designated Area**: Detects people only within the area you specify. Available only when no face area is set. Set at least one virtual line. Click **+ Add** to add up to 10. A purple box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



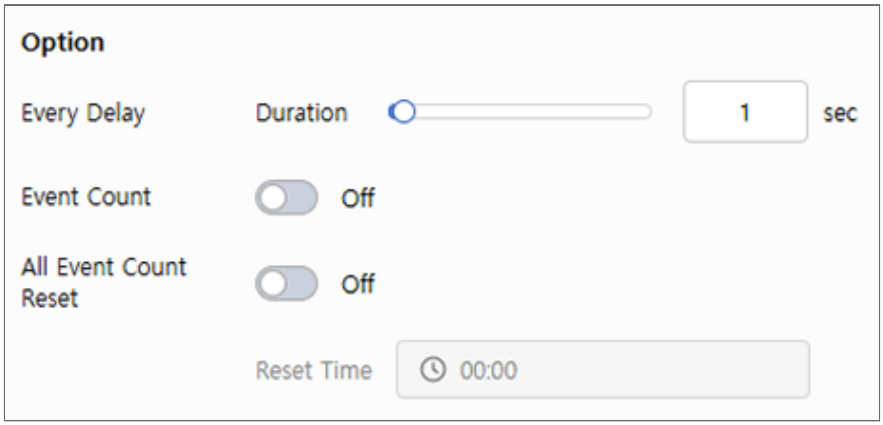
– **Name**: Edit the name of the person detection area.

- **Face Area Only**: Detects people only within the face area. Available only when a face area is set.

> **Info**
>
> - Adding a face area while **Designated Area** is selected opens the **Notice** pop-up. Click **OK** to clear the designated detection area and switch to **Face Area Only**.
> - Deleting all face areas while **Face Area Only** is selected automatically switches to **All Area**.
> - In camera settings, when you use the **Adaptive AE mode** option, narrow the range to **Designated Area** or **Face Area Only**. Keep screens, photos, or posters with faces out of the detection area.
> - Click to initialize the shape and size of the person detection area.
> - Click to delete the added person detection area.
> - Firmware version 1.1.0 or later supports this feature.

6 Set event trigger conditions and event count settings

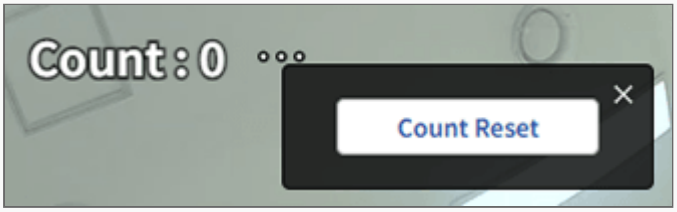
In the **Option** section, set the event trigger conditions and event count.



- **Every Delay**: Set the minimum duration to treat as an event. An event occurs only when the detection state lasts longer than the set time. It can be set up to a maximum of 60 seconds.

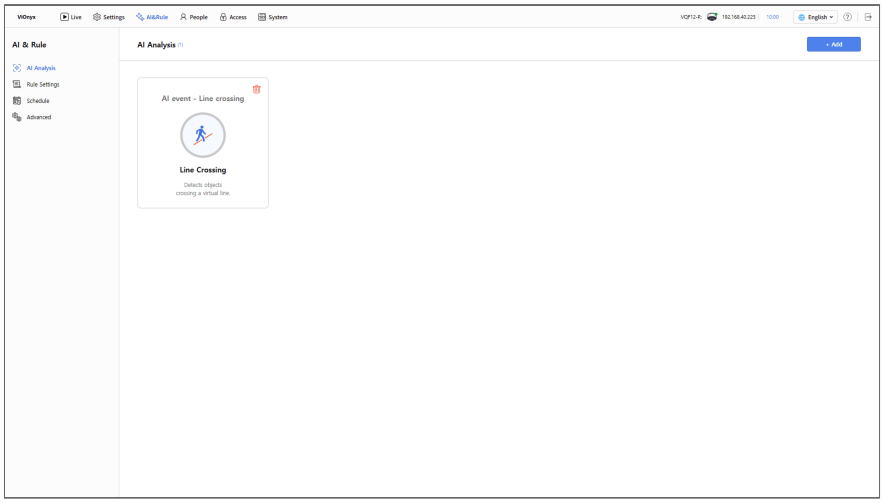
> If too many events occur, increase the **Every Delay** value. Motion detected for less than the set time is not treated as an event, reducing unnecessary events.

- **Event Count**: Set to **On** to count each line crossing. If multiple lines exist, count each line separately.
- **All Event Count Reset**: Set to **On** to initialize event counts for all lines daily at the specified time. Initialize event counts for all lines at the time set in **Reset Time**.

> **Info**
>
> - If you set **Event Count** to **On**, it is displayed in the **Live** menu above the video for each line in the **Count : N** format. Click the ••• button and select **Count Reset** to initialize the event count manually.
>
> 
>
>
> - Support for event count options is included in firmware version 1.1.0 or later.

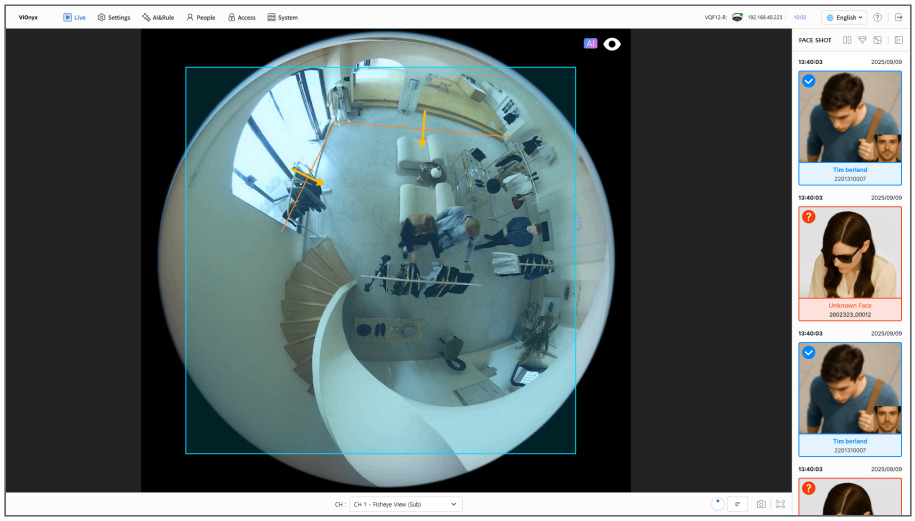
7 Save settings

After completing all settings, click **Create** in the top right. The interface returns to the previous screen, and the new AI event is added to the list.



Check in Live

Click the **Live** menu at the top left of the screen. Confirm the AI icon at the top right of the camera feed is on. Configured virtual lines and face areas are overlaid on the video. An event occurs each time a person crosses a virtual line. If face areas are set, the camera detects faces there; enrolled users are automatically identified and their names are displayed.



Info

- Unenrolled users appear as **Unknown Face**. Enrolled users appear with their name.
- Poor lighting or backlight may prevent the camera from detecting faces. Improve area lighting or adjust the camera position and angle so faces are clearly visible.
- Faces must face the camera to be detected. Profile or rear views may not be detected.

Set Up People Counting Event

Configure a people counting event to detect the number of people staying in designated areas. Add an optional face area to automatically authenticate enrolled users.

When to use this?

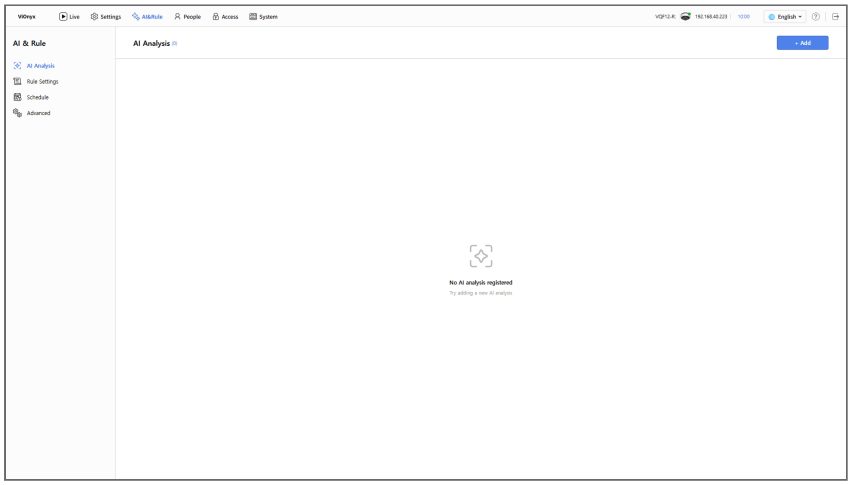
- When you want to monitor visitor counts in real time for a retail store or a specific area of a store.
- When you want to track the number of people in a specific area for crowd management.
- When you want to track entry and exit status for registered staff and VIP customers.
- When you want to manage access statistics for a specific area for security purposes.

Create people counting event.

After creating a people counting event, the **Live** menu detects the number of people staying in designated areas. Also, setting a face area prioritizes face tracking in that area; enrolled users are automatically identified.

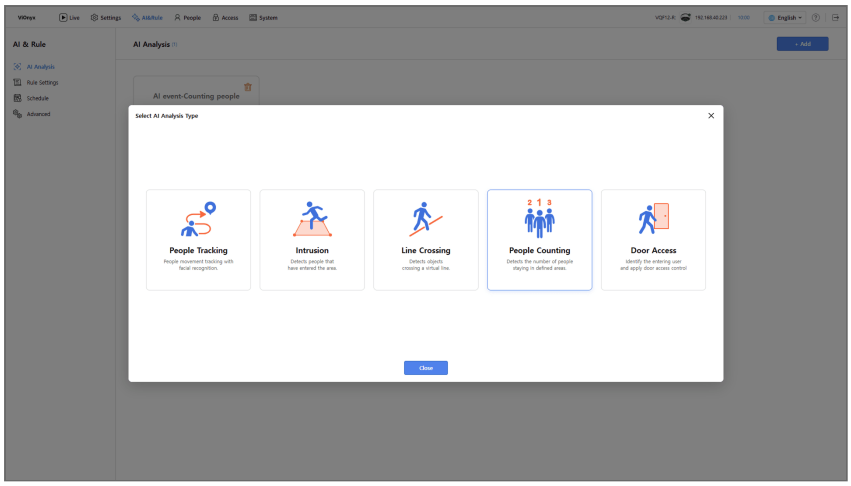
1 Start event creation

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.

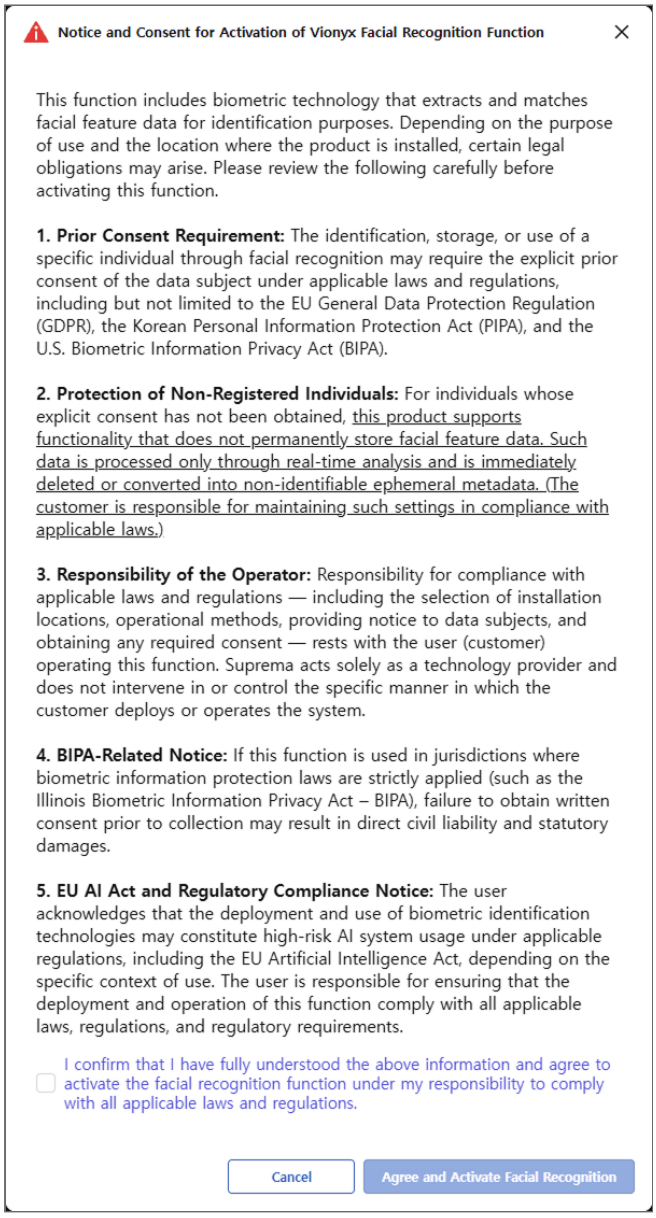


3. Click **+ Add** at the top right of the screen.

4. Click **People Counting** in the **Select AI Analysis Type** window.

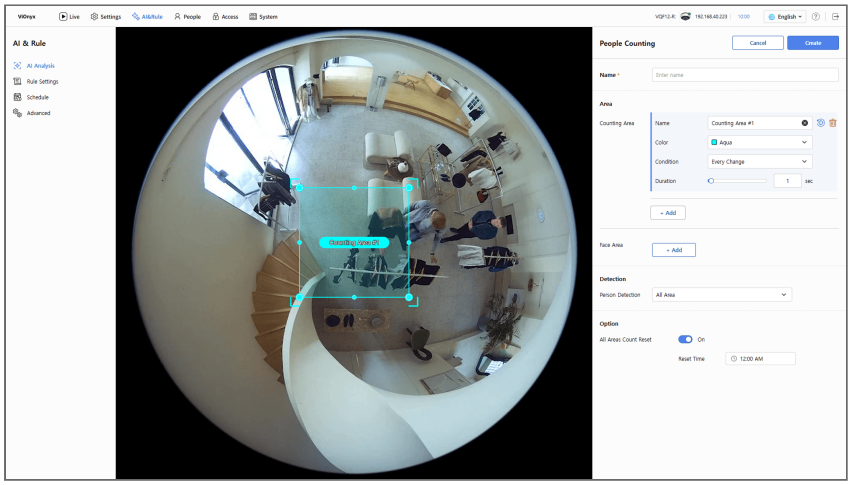


5. When the **Notice and Consent for Activation of Vionyx Facial Recognition Function** pop-up appears, review the details, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- To use the Facial Authentication feature, comply with local regulations. Cannot proceed without consent.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once. Subsequent AI event creation assumes consent.

6. Complete the required settings in the right **People Counting** panel.

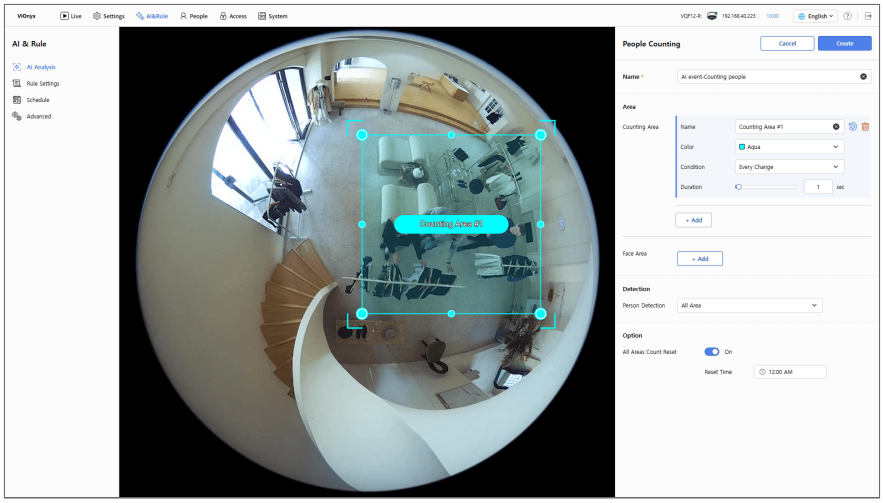


2 Set event name

Enter the AI event name in the **Name** input field. The name can be up to 64 characters long.

3 Set the counting area

Set counting areas in Live View. The camera counts people within configured counting areas in real time and triggers events. Set at least one virtual line. Click **+ Add** to add up to 10. Drag the corners or points of the counting area box in Live View to reshape it. Drag the center to move the line.



- **Name**: Edit the counting area's name. Assign a clear, descriptive name. The counting area's name appears on hover in Live View.
- **Color**: Select the counting area's color. The counting area appears in the selected color in Live View.
- **Condition**: Set the event trigger condition.
  - **Every Change**: Trigger an event whenever a person enters or leaves the counting area
  - **Count Limit**: Trigger an event when the number of people in the counting area exceeds the specified value (default: 10 people, maximum: 100 people)
- **Duration**: Set the minimum time the count in the counting area must satisfy the event condition. For example, if

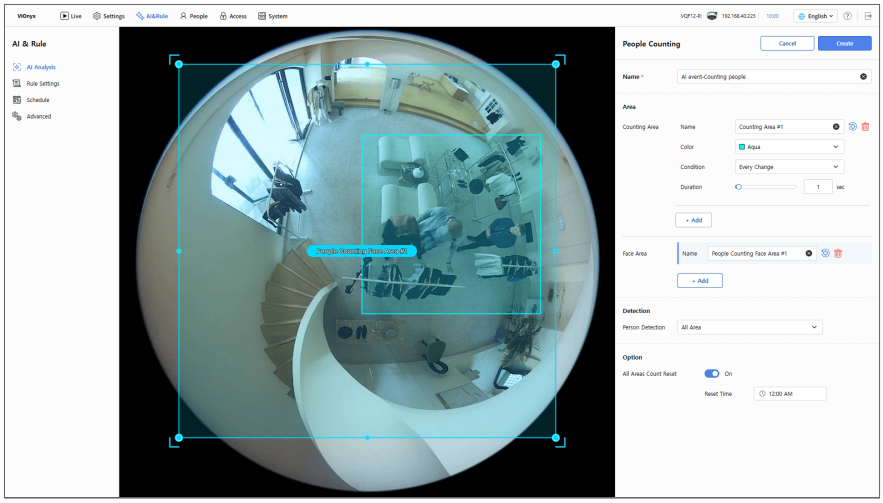
Duration is set to 5 seconds, a person must remain in the counting area for at least 5 seconds to trigger the event. It can be set up to a maximum of 60 seconds.

Info

- Click to reset the configured counting area's shape and size.
- Click to delete the added counting area.

4 Face area settings (optional)

Define the area for face detection. When set, the system prioritizes face tracking in that area. Face areas and counting areas can overlap. Click **+ Add** to add up to 10 face areas. A blue box appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.



- **Name**: Edit the face area's name. Assign a clear, descriptive name. The face area name appears on hover in Live View.

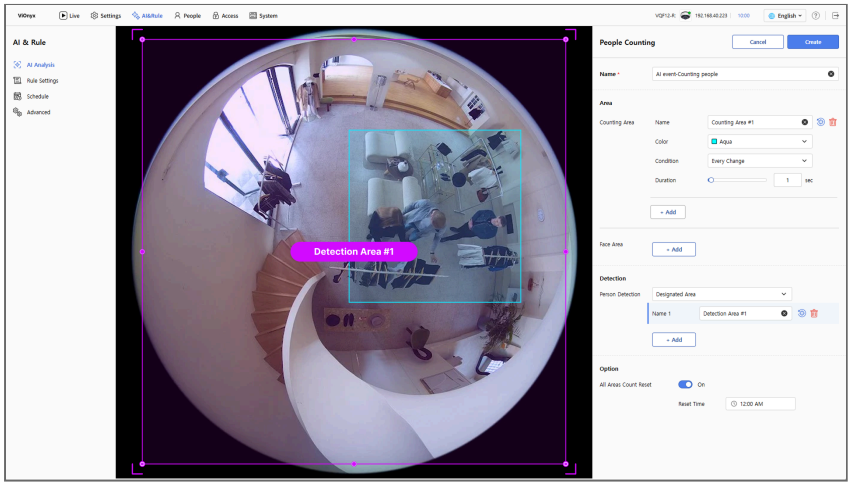
Info

- Enrolled users are automatically identified in the **Live** menu and shown by name. Unenrolled users appear as **Unknown Face**.
- Click to reset the configured face area's shape and size.
- Click to delete an added face area.
- In camera settings, if you use the **Adaptive AE mode** option, configure it so that the face area includes the position where a person would actually stand or pass by and their face is clearly visible.

5 Person detection settings (optional)

In the **Detection** section, select the area where the camera detects people. Narrow the detection area as needed to reduce false detections in irrelevant areas (hallway ends, windows, reflective surfaces, etc.).

- **All Area**: Default. Detects people across the entire screen. Available regardless of whether face areas are set.
- **Designated Area**: Detects people only within the area you specify. Available only when no face area is set. Set at least one virtual line. Click **+ Add** to add up to 10. A purple box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



  - **Name**: Edit the name of the person detection area.
- **Face Area Only**: Detects people only within the face area. Available only when a face area is set.

> **Info**
>
> - Adding a face area while **Designated Area** is selected opens the **Notice** pop-up. Click **OK** to clear the designated detection area and switch to **Face Area Only**.
> - Deleting all face areas while **Face Area Only** is selected automatically switches to **All Area**.
> - In camera settings, when you use the **Adaptive AE mode** option, narrow the range to **Designated Area** or **Face Area Only**. Keep screens, photos, or posters with faces out of the detection area.
> - Click to initialize the shape and size of the person detection area.
> - Click to delete the added person detection area.
> - Firmware version 1.1.0 or later supports this feature.

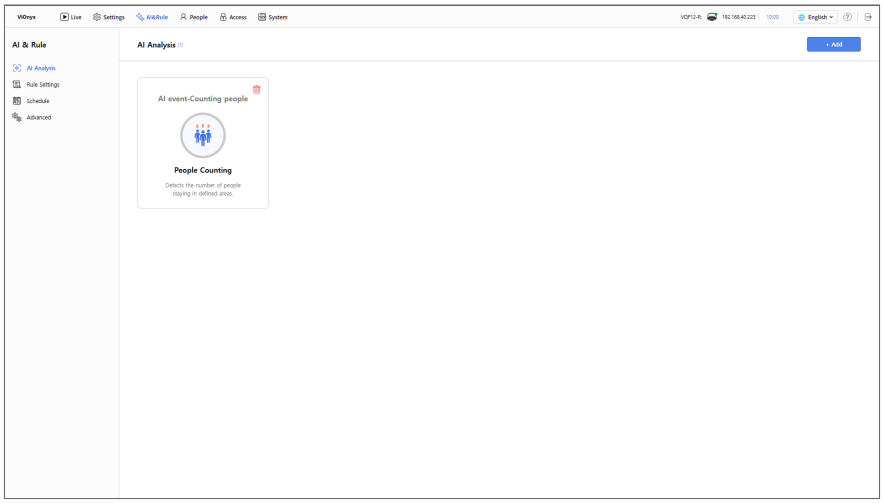
6 Counting reset settings

Set the condition to reset the people count in counting areas.

- **All Areas Count Reset**: Set to **On** to reset counts for all counting areas at the scheduled time. Counts for all counting areas reset at the time set in **Reset Time**.

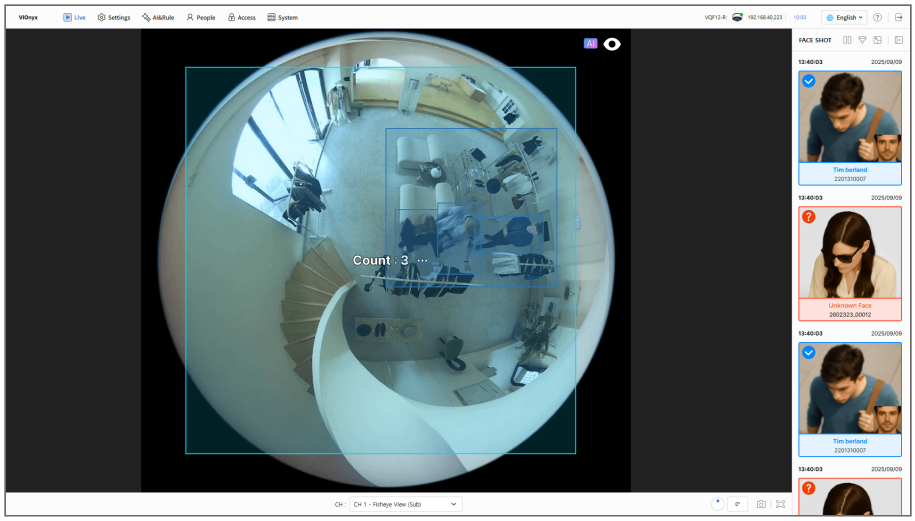
7 Save settings

After completing all settings, click **Create** in the top right. The interface returns to the previous screen, and the new AI event is added to the list.



Check in Live

Click the **Live** menu at the top left of the screen. Confirm the AI icon at the top right of the camera feed is on. Configured counting and face areas appear as overlays on the video. Displays the number of people in the counting area in the format **Count : N**. If face areas are set, the camera detects faces there; enrolled users are automatically identified and their names are displayed.



Info

- To reset the count manually, click ••• → **Count Reset**.



- Unenrolled users appear as **Unknown Face**. Enrolled users appear with their name.
- Poor lighting or backlight may prevent the camera from detecting faces. Improve area lighting or adjust the camera position and angle so faces are clearly visible.
- Faces must face the camera to be detected. Profile or rear views may not be detected.

Set Up Access Control Events

Access control events identify entrants with Facial Authentication, verify nearby people, and determine whether to allow access. Detect tailgating, where an unauthorized person follows an authenticated user, and exclude people exiting through the door from the assessment.

> **Info**
> Firmware version 1.1.0 or later supports access control events.

When to use this?

- When facial authentication verifies whether the person approaching the door is registered
- When you need to prevent tailgating, where an unauthorized person follows an authenticated user inside
- When evaluating only entrants and excluding people exiting from inside the door
- When linking follow-up actions, such as opening the door or outputting a warning prompt, based on the decision

> **Info**
> Access control events only **determine** whether to allow access and do not directly control the door relay. To open the door based on results, create an event, add the door, and link the event. For additional actions, such as voice prompts or webhook notifications, set up door rules.
>
> - For more information on door registration and management, refer to Manage Doors.
> - For more information on door rules, refer to Set Door Rules.

How access control events work

Access control events decide whether to allow access by combining the following elements. Before starting setup, review the role of each element.

Component	roles	Required
Validation Area	This is a wider area surrounding the access control zone. Check the number of people and identification status in this area to detect tailgating.	Yes
Door Access Area	This is the area directly in front of the door. When a person enters this area, the system treats it as an access attempt and starts evaluation.	Yes
Event Entry Line	This line determines who actually passes through the access door. Based on the selected direction, the system determines entry, exit, or both.	Yes
Face Area	This is the area that tracks faces first to identify users.	Option

The camera classifies people in the zone into one of the following states.

- **Identified**: Facial Authentication succeeded, and the person matches a registered user.

- **Unidentified**: Facial Authentication failed, or the person does not match a registered user. The Live menu shows unregistered people, people with covered faces, or people not facing the camera as **Unknown Face**.

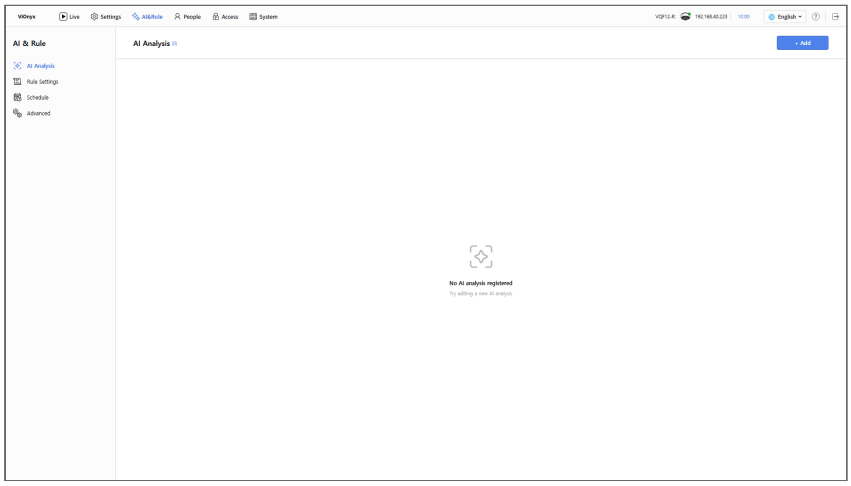
> **Caution**
>
> For security, the system does not treat an unrecognized person as an authenticated user. If a person is unidentified in the access control area, the system denies access.

Create access control event

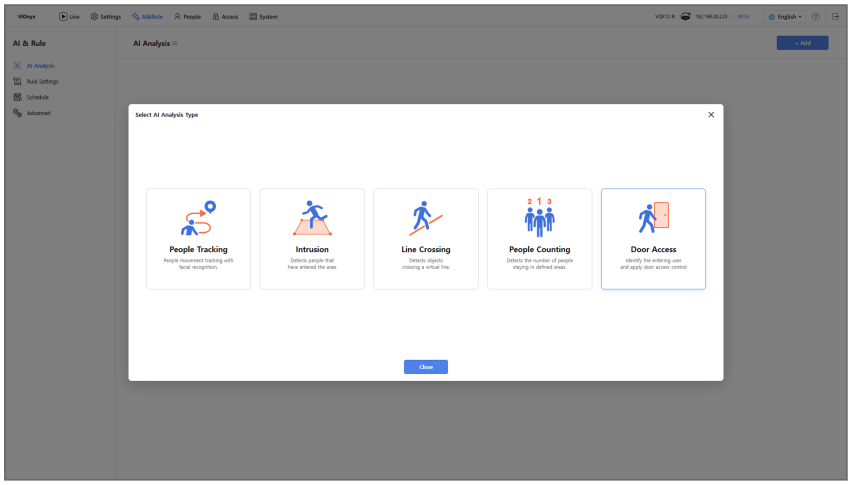
An access control event identifies users approaching the door in the **Live** menu and verifies tailgaters.

1 Start event creation

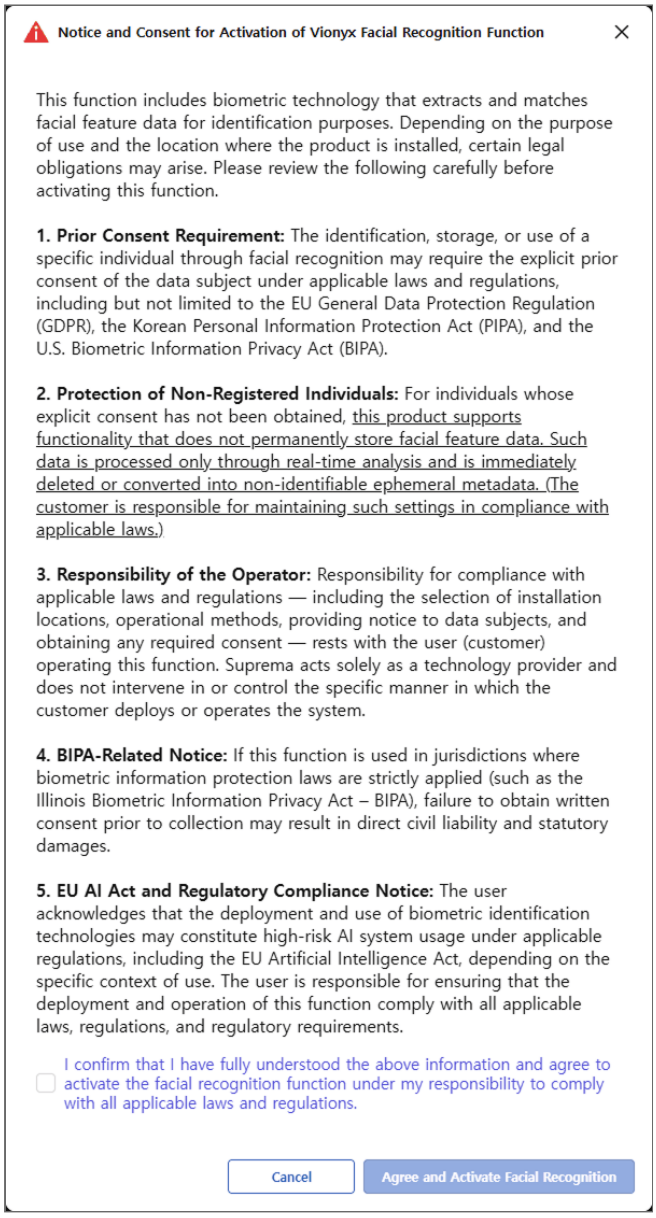
1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. In the **Select AI Analysis Type** window, click **Door Access**.

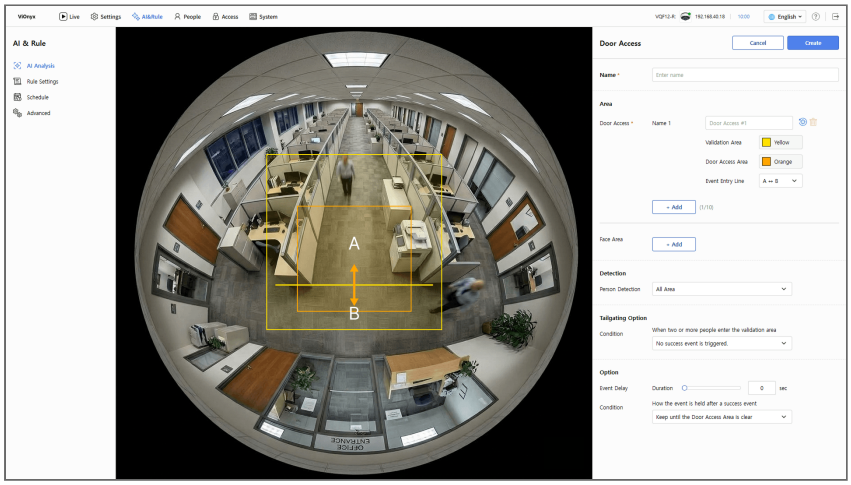


5. When the **Notice and Consent for Activation of Vionyx Facial Recognition Function** pop-up appears, review the details, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- The access control event uses Facial Authentication to identify users, so agree to use it before creating it.
- To use the Facial Authentication feature, comply with local regulations.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once. Subsequent AI event creation assumes consent.

6. Complete the required settings in the **Door Access** panel on the right.

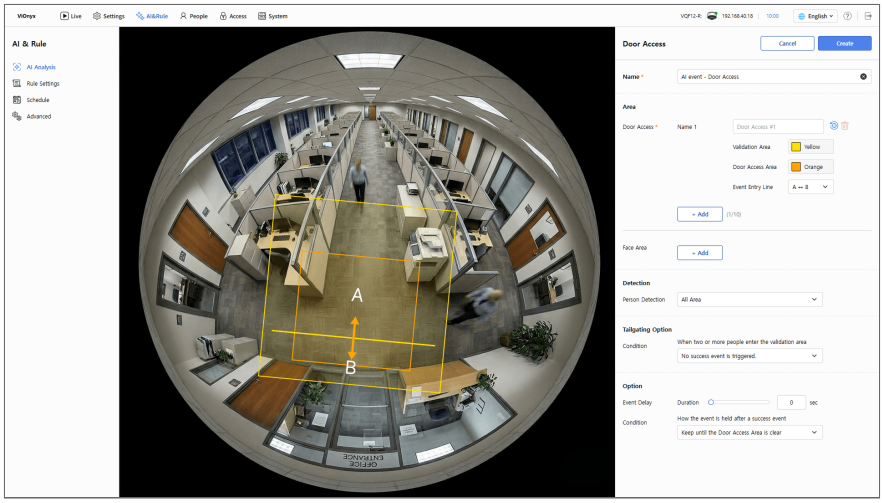


2 Set event name

Enter the AI event name in the **Name** input field. The name can be up to 64 characters long.

3 Access control area settings

In the **Area** section, set the validation area, access control area, and event entry line for the door location. Set at least one virtual line. Click **+ Add** to add up to 10. Each addition shows the three elements as a set in Live view. Drag corners or points to adjust the shape, and drag the center area to move it.



- **Name**: Edit the name of the access control area. Use a clear name, such as the door location.
- **Validation Area**(Yellow): Validation area surrounding the access control area. Set it wider than the access control area to detect fast approaches and tailgaters.
- **Door Access Area**(Orange): Set it directly in front of the door, where the person must pass to enter. When a person enters this area, the system determines access.
- **Event Entry Line**: This line determines who actually passes through the access door. Drag the points at both ends to place the line across the access control area. Then, select the crossing direction.
  - **A → B**: Detect only people crossing from A to B.

- **B → A**: Detect only people crossing from B to A.
- **A ↔ B**: Detect both directions. The system distinguishes between people entering and exiting.

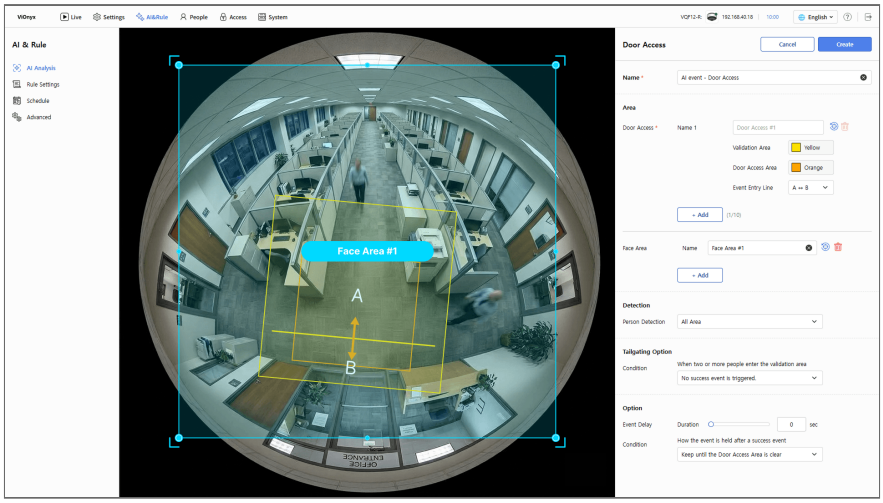
To detect only one direction, check the positions of A and B in Live View, then select **A → B** or **B → A**.

Info

- The verification area must fully include the access control area. Saving fails if the access control area extends outside the verification area.
- Extend the event entry line beyond the access control area, but keep it within the verification area.
- To initialize the shape and size of the configured area, click .
- To delete the added access control area, click .

4 Face area settings (optional)

Define the area for face detection. When set, the system prioritizes face tracking in that area to identify users. Set the face area where a person approaching the door is clearly visible from the front. Face areas and access control areas can overlap. Click **+ Add** to add up to 10 face areas. A blue box appears in Live View; drag corners or points to adjust the shape. Drag the center to move the line.



- **Name**: Edit the face area's name. Assign a clear, descriptive name. The face area name appears on hover in Live View.

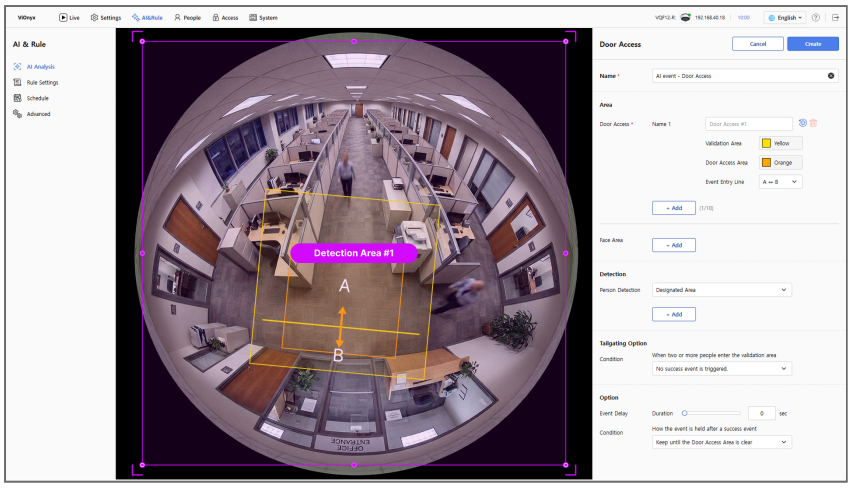
Info

- Enrolled users are automatically identified in the **Live** menu and shown by name. Unenrolled users appear as **Unknown Face**.
- Click to reset the configured face area's shape and size.
- Click to delete an added face area.
- In camera settings, if you use the **Adaptive AE mode** option, configure it so that the face area includes the position where a person would actually stand or pass by and their face is clearly visible.

5 Person detection settings (optional)

In the **Detection** section, select the area where the camera detects people. Narrow the detection area as needed to reduce false detections in irrelevant areas (hallway ends, windows, reflective surfaces, etc.).

- **All Area**: Default. Detects people across the entire screen. Available regardless of whether face areas are set.
- **Designated Area**: Detects people only within the area you specify. Available only when no face area is set. Set at least one virtual line. Click **+ Add** to add up to 10. A purple box appears in the live view; drag its corners or points with the mouse to adjust it to the desired shape. Drag the center to move the line.



  - **Name**: Edit the name of the person detection area.
- **Face Area Only**: Detects people only within the face area. Available only when a face area is set.

Info

- Adding a face area while **Designated Area** is selected opens the **Notice** pop-up. Click **OK** to clear the designated detection area and switch to **Face Area Only**.
- Deleting all face areas while **Face Area Only** is selected automatically switches to **All Area**.
- In camera settings, when you use the **Adaptive AE mode** option, narrow the range to **Designated Area** or **Face Area Only**. Keep screens, photos, or posters with faces out of the detection area.
- Click to initialize the shape and size of the person detection area.
- Click to delete the added person detection area.
- Firmware version 1.1.0 or later supports this feature.

6 Tailgating option settings

In the **Tailgating Option** section, select how the system determines access when 2 or more people are in the verification area. Options are listed from highest security to lowest.

- **No success event is triggered.**: If 2 or more people are in the verification area, the system denies access regardless of the identification results. This option fits areas where only one person must pass at a time.
- **Success event only when all individuals are valid.**: The system allows access only when it identifies everyone in the verification area as a registered user. The system denies access if anyone remains unidentified.
- **Success event if any identified individual is valid.**: The system allows access if at least one registered user is in the verification area. This option allows access with unidentified people, so it fits areas with frequent escorted visitors.
- **No effect on event triggering.**: The system ignores headcount in the verification area. It bases access only on the entrant's identification result.

The following shows the decision for each option when a registered user enters with others in the verification area.

Option	When only users with valid access permissions are present	When the list includes users with invalid access permissions
No success event is triggered.	Access denied	Access denied
Success event only when all individuals are valid.	Access granted	Access denied
Success event if any identified individual is valid.	Access granted	Access granted
No effect on event triggering.	Access granted	Access granted

> **Tip**
> For security-critical doors, use **Success event only when all individuals are valid.** or higher.

7 Set event trigger conditions

In the **Option** section, set the event trigger conditions.

- **Event Delay**: Set the minimum duration to treat as an event. An event occurs only when the detection state lasts longer than the set time. It can be set up to a maximum of 60 seconds.

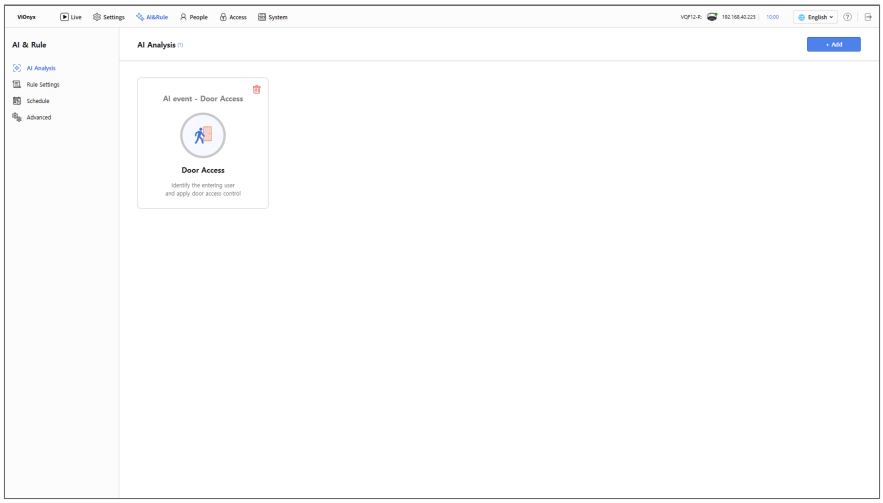
  > If events occur too often because people briefly pass in front of the door, increase the **Event Delay** value. Motion detected for less than the set time is not treated as an event, reducing unnecessary events.

- **Condition**: Select how long to keep the event after access is granted. While the event remains active, linked actions (for example, door opening) also remain active.
  - **Keep until the Door Access Area is clear**: Keep the event until no one remains in the access-controlled area. The door remains open while the authenticated user stays in front of it, without re-authenticating.
  - **Keep until the area is clear or a tailgating violation occurs**: Clear the event when the area is empty. Clear it immediately when an unauthorized person enters the verification area and violates the tailgating setting. This prevents unauthorized people from following someone in while the door is open.
  - **Trigger once on entry (no hold)**: Do not keep the event. Trigger it once each time someone enters the access-controlled area.

> **Info**
> If a registered user hesitates in front of the door and cannot enter, the door opens only after leaving and re-entering the access-controlled area. To reduce this inconvenience while maintaining security, select **Keep until the area is clear or a tailgating violation occurs**.

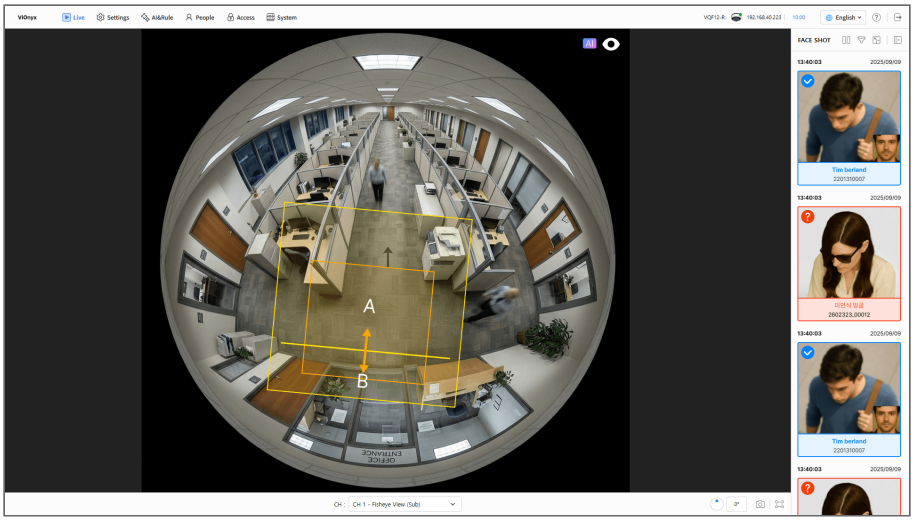
8 Save Settings

After completing all settings, click **Create** in the top right. The interface returns to the previous screen, and the new AI event is added to the list.



Check in Live

Click the **Live** menu at the top left of the screen. Confirm the AI icon at the top right of the camera feed is on. The configured verification area, access-controlled area, event entry line, and face area appear as overlays on the video. When someone enters the access-controlled area, the system triggers Access granted or Access denied based on identification and tailgating options.



Info

- Unenrolled users appear as **Unknown Face**. Enrolled users appear with their name.
- Poor lighting or backlight may prevent the camera from detecting faces. Improve area lighting or adjust the camera position and angle so faces are clearly visible.
- Faces must face the camera to be detected. Profile or rear views may not be detected. If the system cannot identify a face, it treats the person as unidentified and denies access.

Next step

The access control event determines only whether to grant access. Set door rules to execute additional actions such as voice prompts, webhook notifications, or warning lights.

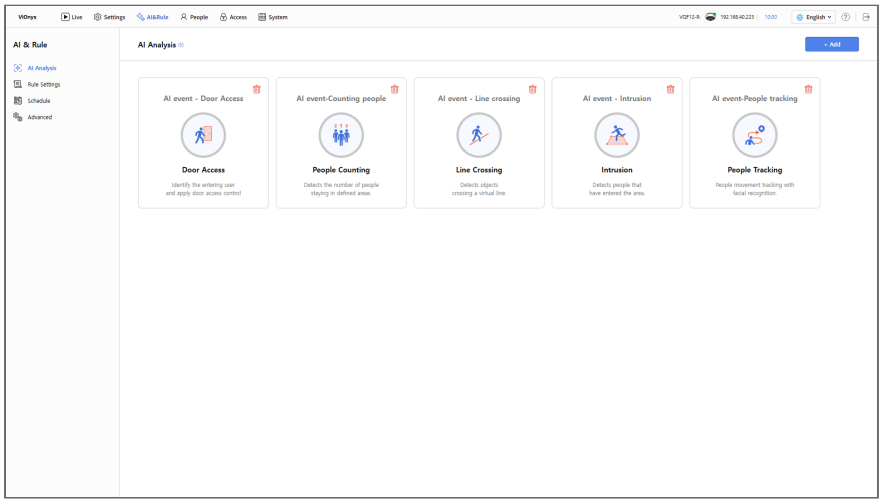
After creating an access control event, add the door and link the event. When access is granted, the relay connected to the door activates and opens the door.

Edit and Delete AI Events

Modify the settings of created AI events or delete events that are no longer needed.

Edit AI event settings

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.



3. Click the AI event to edit.
4. In the right panel, edit the AI event settings.
5. After you finish all settings, click **Update** in the upper right corner.

Return to the previous screen and confirm the modified event in the AI event list.

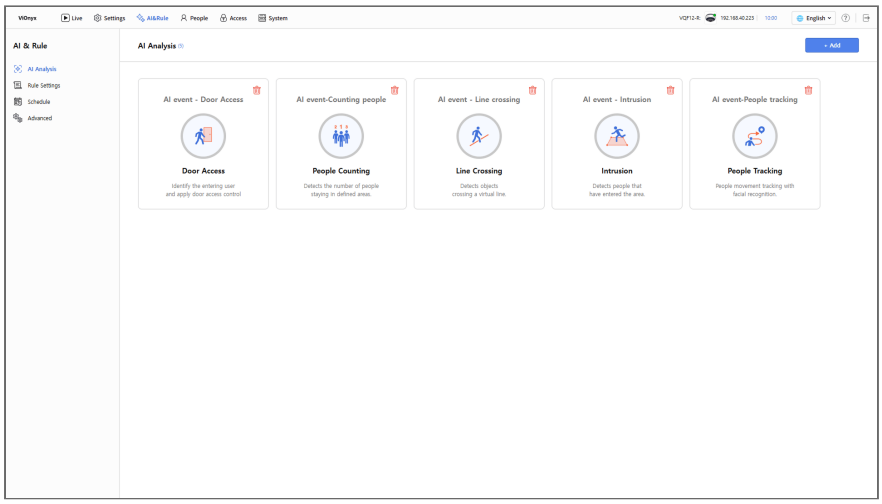
Info

For more information about each event setting, refer to the following document.

- Set Up User Tracking Events
- Set Up Intrusion Detection Events
- Set Up Line-Crossing Detection Event
- Set Up People Counting Event
- Set Up Access Control Events

Delete AI event

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **AI Analysis** on the left sidebar.



3. Click to the right of the AI event to delete.
4. When a warning message appears, review the message and click **OK**.

Info

- Deleted AI events cannot be recovered. If an AI event is linked to rules (Rule), deleting the event also deletes the linked rules.
- Deleting an AI event records the deletion in the system log.

AI Rule Settings

Use AI rules to automatically play audio, send webhooks, or trigger relay actions based on event type and conditions. This document guides the complete procedure for creating and operating rules.

Set AI rules in the following situations.

- Send a webhook to an external server when a specific AI event occurs.

- Play audio on the device when a specific AI event occurs.
- Trigger a relay connected to an access door when a specific AI event occurs
- Automate different follow-up actions by event type.

Before you start

Before starting rule setup, check the following.

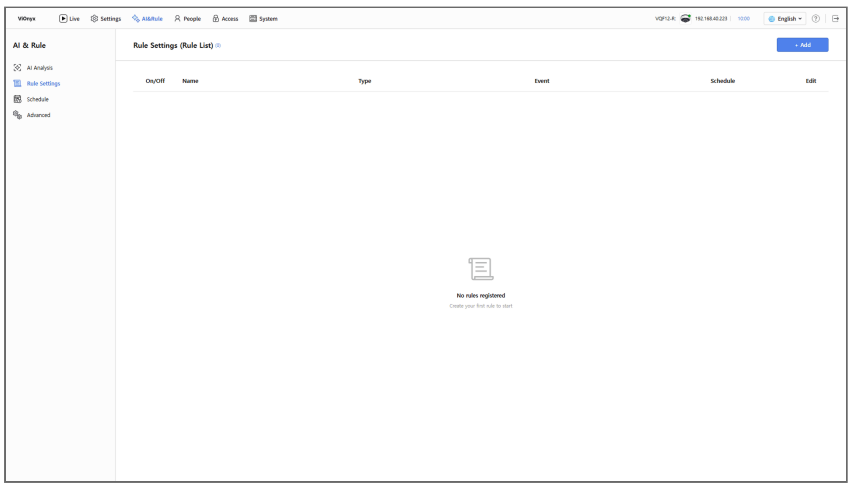
- AI events must already exist. Refer to the following documents to create AI events.
  - Set Up User Tracking Events
  - Set Up Intrusion Detection Events
  - Set Up Line-Crossing Detection Event
  - Set Up People Counting Event
- Prepare the audio clips to play before using audio.
- Prepare the webhook receiver URL beforehand.
- When using relays, verify that the relay port on the device or subdevice is connected.
- Set at least one action: audio, webhook, or relay.

> **Info**
> In AI events, **Door Access** cannot be used as a condition for AI rules.

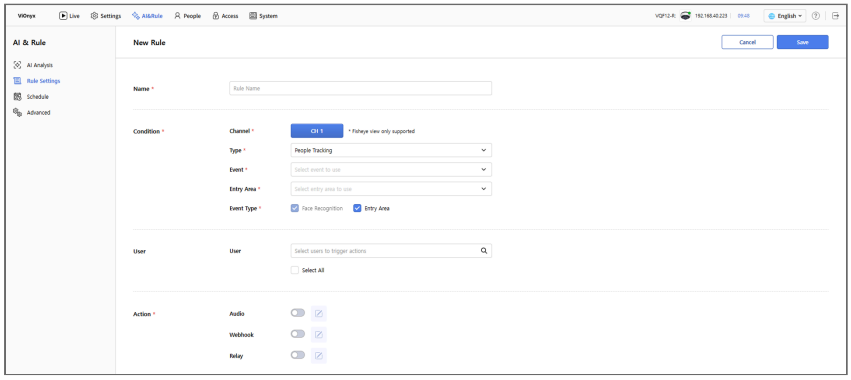
Create AI rule

1 Start creating a rule

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **Rule Settings** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. When the **New Rule** screen appears, enter the rule name and set conditions and actions.



2 Enter rule name

Enter the rule name in the **Name** input field. Rule name is required. Up to 64 characters.

3 Set conditions

Conditions determine whether a rule executes when an AI event occurs. In the **Condition** section, set conditions as instructed below. The **Type** and **Event** options appear based on the settings specified when creating the AI event.

- **Channel**: The channel is fixed to CH 1. Only Fisheye view is supported.
- **Type**: Select the AI event type. Select one of the following.
  - **People Tracking**
  - **Intrusion**
  - **Line Crossing**
  - **People Counting**
- **Event**: Select the AI event that will trigger the rule. The event list shows AI events that match the selected type. Events appear in the format `(ID:N) event_name`.
- **Entry Area** / **Intrusion Area** / **Line** / **Counting Area**: Add conditions for an area based on the selected event type.
- **Event Type**: Select the event type that determines whether the rule executes. The rule executes based on the selected event type.

> You must select at least one event type.

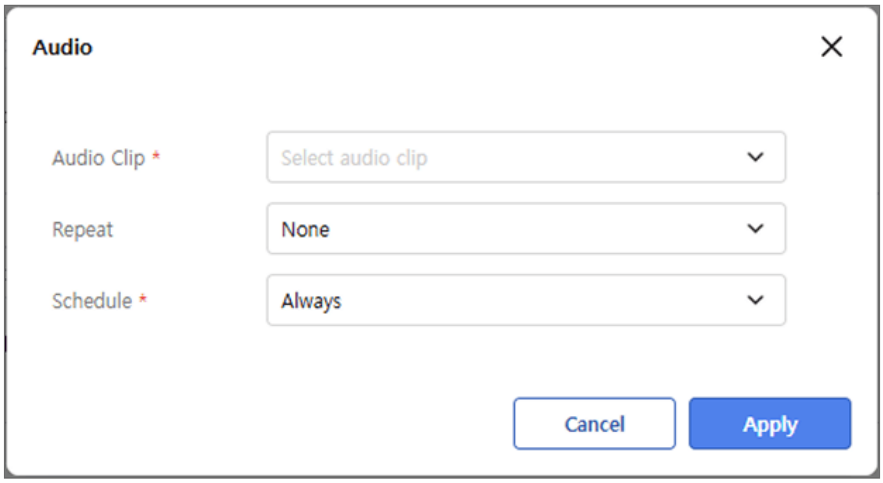
4 User selection

In the **User** section, select the user who determines whether the rule runs. The system runs the rule when it detects the selected user in an AI event.

- Click **Select users to trigger actions** to select specific users. When the user list appears, select the desired users and click the **Save** button.
- Click **Select All** to select all registered users.

5 Audio action settings

Audio action plays audio from the camera when an AI event occurs. In the **Action** section, click the **Audio** toggle to enable the action, and then click . The audio settings pop-up appears.



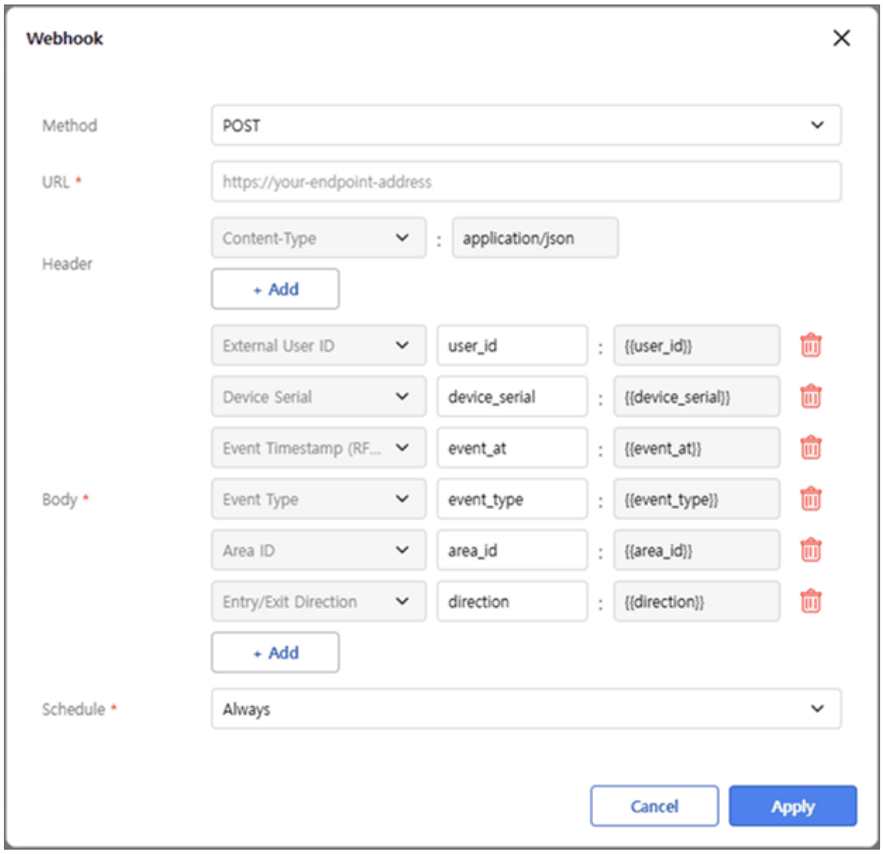
- **Audio Clip**: Select the audio clip to play. Select an audio clip from the list of clips uploaded to the system.
- **Repeat**: Set the number of times to repeat audio playback. Plays the audio clip repeatedly the number of times you set. It can be set to a maximum of 10 times.
- **Schedule**: Select the schedule when the rule runs and plays audio.

Click **Apply** to save the audio action settings.

> **Info**
>
> - Prepare audio clips before configuring audio actions. Upload audio clips in **System** → **Audio**. For more information, refer to Upload Audio Clips.
> - Create, edit, or delete schedules in **AI&Rule** → **Schedule**. For more information on schedule management, see Manage Schedules.

6 Webhook action settings

Webhook action sends a webhook to an external server when an AI event occurs. In the **Action** section, click the **Webhook** toggle to enable the action, and then click . The webhook settings pop-up appears.



- **Method**: The webhook transmission method. Only the `POST` method is supported.
- **URL**: Enter the URL to receive the webhook. The address must be valid and start with `http://` or `https://`.
- **Header**: Set the HTTP headers to include in the webhook. Click **+ Add** to add headers. Enter each header as a key-value pair.
- **Body**: Set the HTTP body to include in the webhook. Click **+ Add** to add body items. Enter each body item as a key-value pair.
- **Schedule**: Select the schedule when the rule runs and sends webhooks.

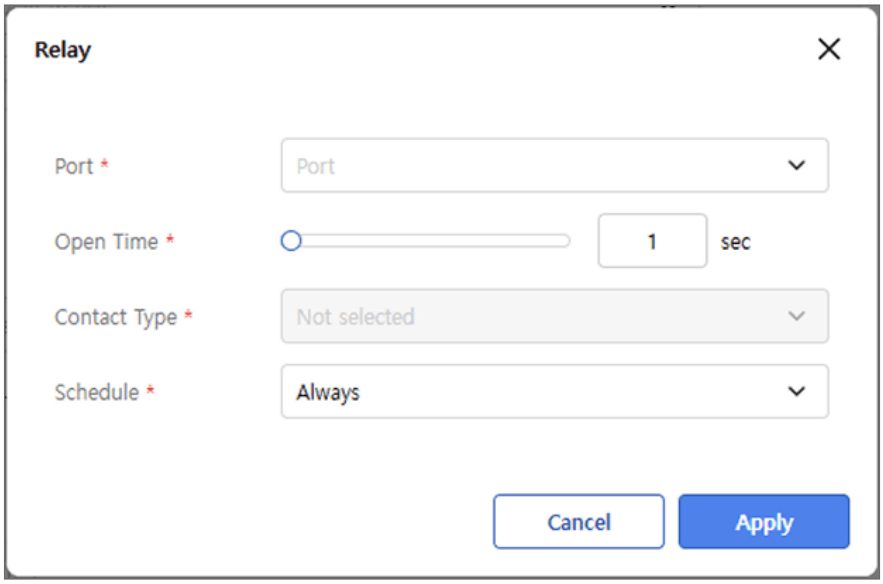
Click the **Apply** button to save the webhook action setting.

> **Info**
>
> - Webhook send logs and response codes can be checked in the system logs for troubleshooting.
> - Create, edit, or delete schedules in **AI&Rule** → **Schedule**. For more information on schedule management, see Manage Schedules.

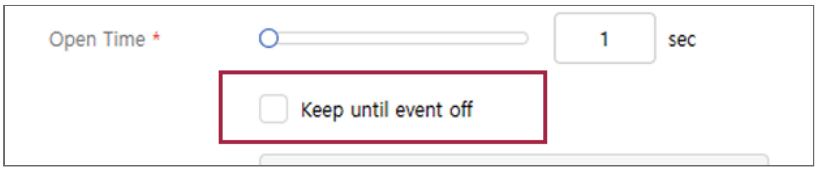
7 Relay action settings

The relay action feature triggers the relay on the device or subdevice when an AI event occurs. For example, trigger the door relay to restrict access when an event involves a blacklisted user.

In the **Action** section, click the **Relay** toggle to enable the action. Then click the button. The relay settings pop-up appears.



- **Port**: Select the relay port to activate. Select the relay port on the device or on a subdevice connected to the device. Ports already used by other rules or doors show "In use" in the list, and the system prevents selection.
- **Open Time**: Set how long the relay remains open. Move the slider or enter a value in the input field. Set it to 1–120 seconds.
  - **Keep until event off**: Set **Type** to **People Counting**, and specify the area set in **Count Limit** as the condition to use the **Keep until event off** option. Selecting this option keeps the relay open until the count limit event clears, regardless of open time.



- **Contact Type**: Select the relay contact type. Select a relay port to set options. The default is **Normal Close**.
  - **Normal Open**: Normally open, and closes when the relay activates.
  - **Normal Close**: Normally closed, and opens when the relay activates.
- **Schedule**: Select the schedule when the rule runs and triggers the relay.

Click **Apply** to save the relay operation settings.

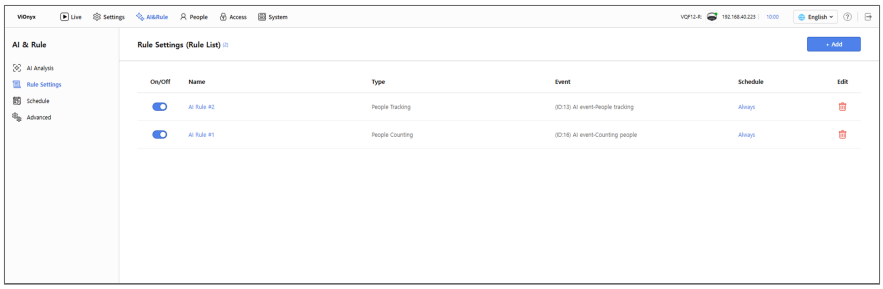
> **Caution**
> **Contact Type** is a setting applied to the relay port, not a rule. Changing **Contact Type** applies immediately to all rules and doors that use the port. When the port is fixed to Lock or Unlock, changing **Contact Type** inverts the output and may open a locked door.

Info

- Firmware version 1.1.0 or later supports this feature.
- Create, edit, or delete schedules in **AI&Rule** → **Schedule**. For more information on schedule management, see Manage Schedules.

8 Save rule

After completing rule setup, click **Save** at the top right to save the rule. Saved rules appear in the rule list. The rule list shows the rule name, type, event, and schedule.



Enable/Disable AI rules

In the rule list, click the leftmost toggle for a rule to enable or disable it. Enabled rules execute the configured actions when an AI event occurs. Disabled rules do not execute actions when AI events occur.

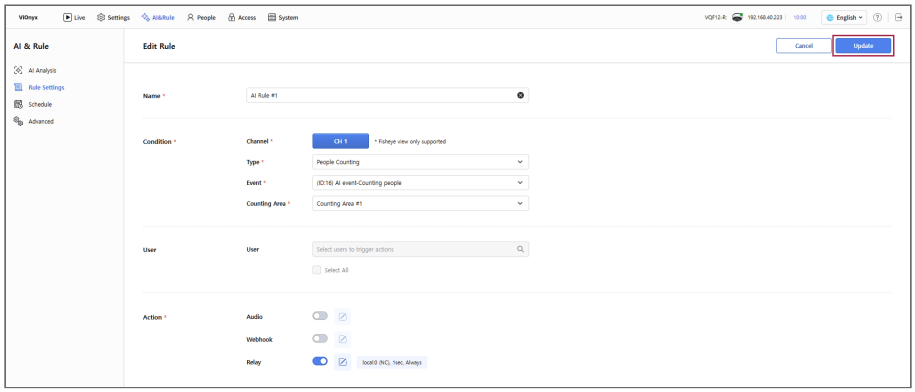


Info

The rule list shows enabled status at a glance. Rules with a blue toggle are enabled; rules with a gray toggle are disabled.

Edit AI rule

Click a rule in the rule list to view or edit its details. On the rule details screen, after modifying conditions and actions, click **Update** to save changes.



Delete AI rule

In the rule list, click on the right of a rule to delete it. Deleted rules cannot be recovered.



Manage Schedules

A schedule is a weekly timetable created by combining days of the week and time slots. When an AI rule action uses a schedule, the action executes only during the time slots in the schedule. A single schedule can be used across multiple AI rules.

Create schedules in the following situations.

- Send webhooks only during weekday business hours
- Play intrusion detection alert audio only at night
- Prevent relays from operating on weekends

> **Info**
>
> The device provides the **Always** schedule by default. The Always schedule runs 24 hours a day and cannot be edited or deleted.

Check the schedule list

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **Schedule** on the left sidebar.



The schedule list shows registered schedules and the AI rules that use each schedule.

- Next to **Schedule**(1) at the top of the screen, the system shows the number of schedules.
- Enter the schedule name or ID in the search field (2) to find a specific schedule.
- Select a value from the Rows per page list (3) to set schedules per page.
- To change the sort order, select a criterion from the **Sort by Name**(4) list.

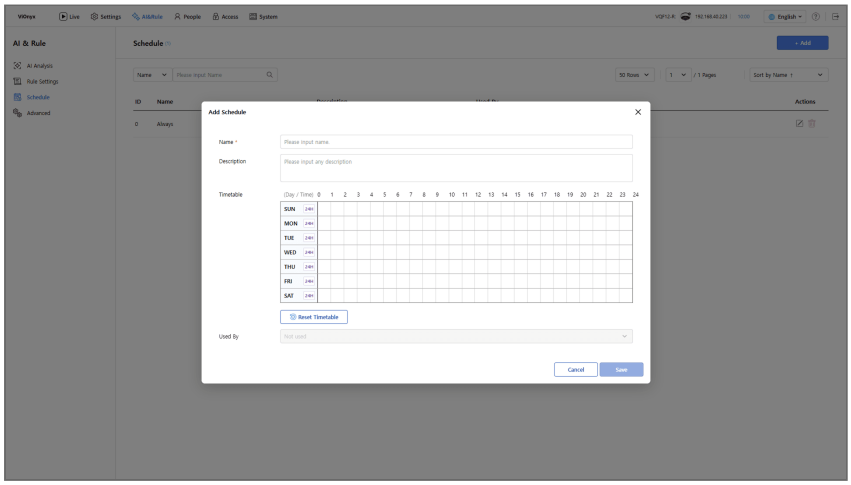
The following items are displayed in the schedule list.

Item	Description
ID	The unique ID of the schedule. Always schedule is `0`.
Name	The name of the schedule.
Description	The description entered when adding or editing the schedule.
Used By	AI rules that use the schedule. When no AI rules use the schedule, **None** appears. When multiple AI rules apply, they appear in the **and {count} more** format.
Actions	This feature enables editing ( ) or deleting ( ) schedules.

Add schedule

1 Start adding a schedule

1. Click **+ Add** in the upper right of the schedule list screen.
2. Enter the schedule information when the **Add Schedule** pop-up appears.

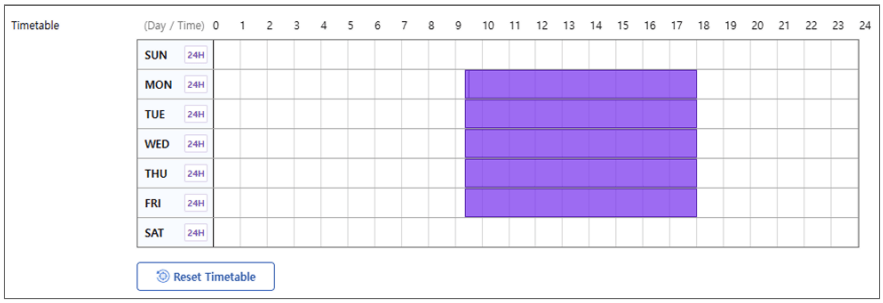


2 Enter a name and description

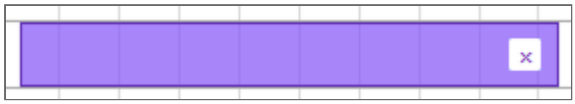
- **Name**: Enter the schedule name. This field is required. Use a unique name for each schedule. You can enter up to 48 characters.
- **Description**: Enter a description for the schedule. For example, add an applied time range like **Mon-Fri 09:00-18:00** to distinguish schedules when selecting them in rules.

3 Set time slots in the timetable

Select the days and time slots when the schedule runs in **Timetable**. The vertical axis shows the day of the week (Sunday~Saturday), and the horizontal axis shows time (0~24). The selected time slots appear as blocks.



- **Select time slots**: Drag from the start time to the end time in the desired day row. Select in 10-minute increments.
- **Move a time slot**: Drag the block left or right to move it to a different time.
- **Select or clear 24 hours**: Click **24H** next to the day name. The timetable selects all 24 hours for that day. Click again to clear all.
- **Delete a block**: Select the block to delete. The ✕ icon appears. Click the Remove block button.



- **Initialize all**: To clear all time slots and set them again, click **Reset Timetable**.

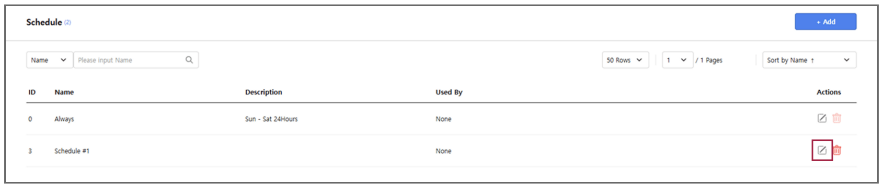
4 Save schedule

After completing all settings, click **Save**. The system adds the saved schedule to the schedule list. Select it in the AI rule operation settings.

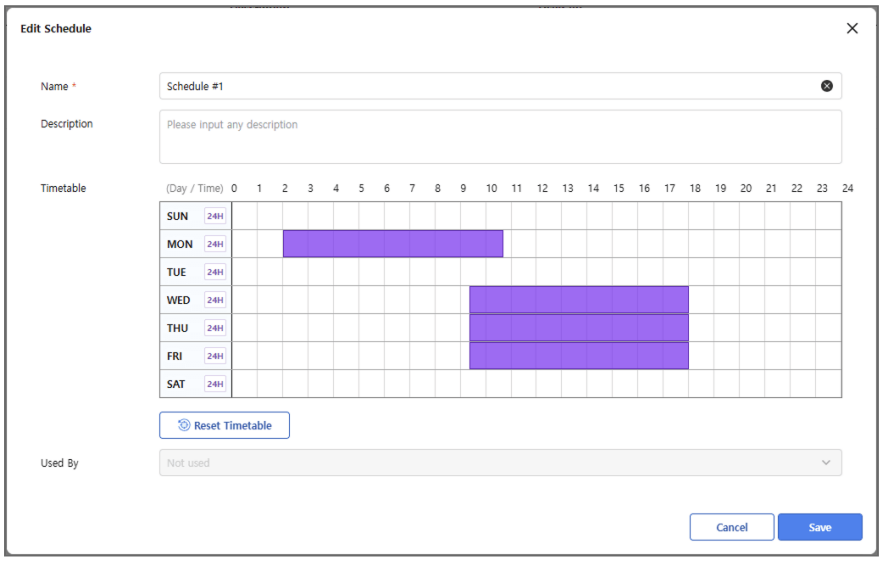
> **Info**
>
> - The **Used By** field is read-only and shows the AI rules that use the schedule. A newly created schedule has no AI rules using it yet, so it appears as **Not used**.
> - To apply a saved schedule to an AI rule, see AI Rule Settings.

Modify schedule

1. In the schedule list, click the ✎ button to the right of the schedule.



2. When the **Edit Schedule** pop-up appears, edit the name, description, and timetable.



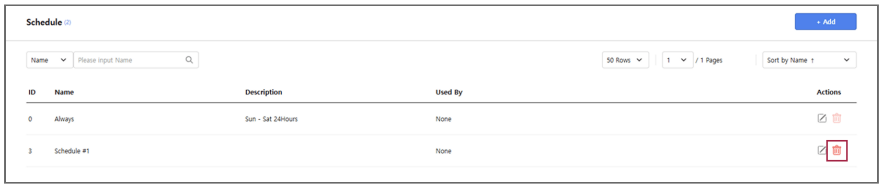
3. Click **Save** to save the changes.

Saving the modified schedule applies it to all AI rules that use it.

> **Info**
>
> - If multiple AI rules share a schedule, check the affected AI rules in the **Used By** column before editing.
> - The Always schedule, the default schedule, cannot be modified.

Delete schedule

1. In the schedule list, click the button to the right of the schedule.



2. If a confirmation message appears, review it and click **OK**.

Deleted schedules cannot be recovered.

Info

- Do not delete schedules that AI rules use. In the AI rules listed in the **Used By** column, select another schedule, then try deleting it again.
- The Always schedule, the default schedule, cannot be deleted.

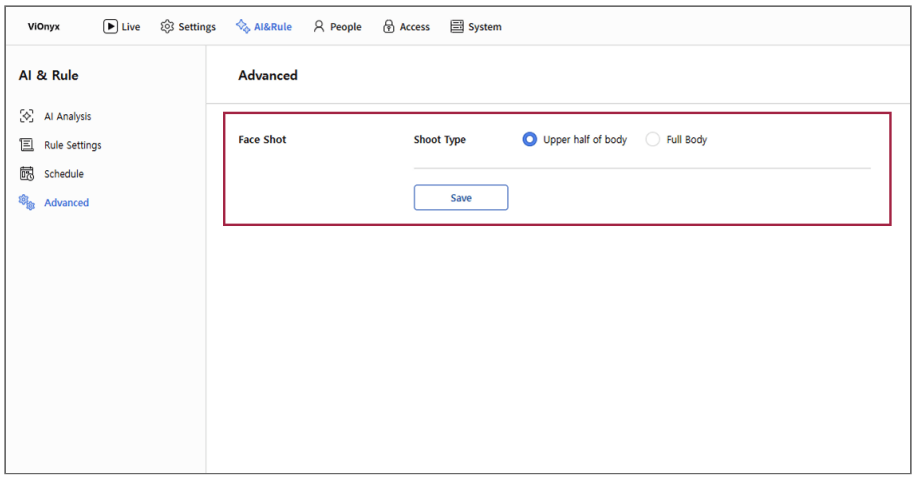
Advanced Settings

In Advanced settings, you can set the face capture type and manage automatic user enrollment and retention policies for enrolled users when facial recognition occurs.

Face capture type setting

Set the face capture type to capture only the upper body or the full body.

1. Click the **AI&Rule** menu in the upper-left corner of the screen.
2. Click **Advanced** on the left sidebar.
3. Select the desired capture type in the **Shoot Type** option, then click **Save**.



Automatic user enrollment setting

Faces detected through AI events can be automatically enrolled as users. This feature is set to Manual Enrollment mode by default, and you can switch to Automatic Enrollment mode as needed.

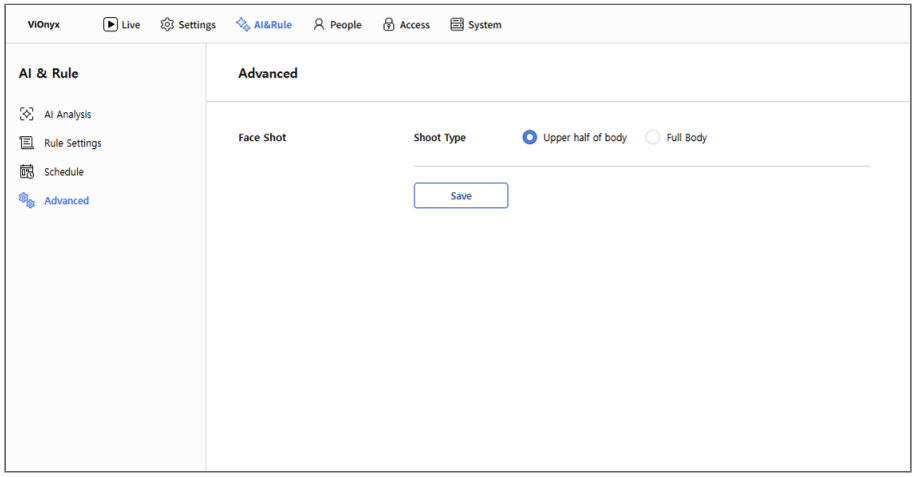
Info

For automatically enrolled users, manually edit information such as user name and description. For more information on editing user information, see Edit and Delete Users.

Enable automatic enrollment mode

1. Click the **AI&Rule** menu in the upper-left corner of the screen.

2. Click **Advanced** on the left sidebar.
3. In the **Auto User Enroll** section, click the toggle button to enable automatic enrollment mode.



Set each option as follows, then click **Save** to save.

> **Info**
> When using **Auto User Enroll** mode, users enrolled with low-quality photos, such as blurry images, masked faces, or side profiles, may experience false authentication.

Automatic enrollment user count setting

In the **# of Auto Enroll User** option, set the number of users that can be automatically enrolled. Drag the slider or enter a number directly in the input field.

- The default value is 50,000 users, and you can set up to 100,000 users.
- When you set the automatic enrollment user count, manually enrolled users can be enrolled only within the configured count. For example, if the configured user count is 50,000, the total of automatic and manual enrollments can reach only 50,000 users.

> **Info**
> - If manually enrolled users already exist, you cannot increase the automatic enrollment user count.
> - When you decrease the automatic enrollment user count, excess users are automatically deleted from the oldest first.

Retention policy setting

In the **Retention Policy** option, set the retention policy for automatically enrolled users. Choose how to delete automatically enrolled users when the user limit is reached.

- **Delete oldest when full**: When the assigned user count is exceeded, automatically delete the oldest enrolled users first.

Retention period setting

In the **Retention Period (Days)** option, set the retention period for automatically enrolled users in days. When the retention period expires, the oldest enrolled users are automatically deleted first.

- **Disabled** (default): When the assigned user count is exceeded, automatically delete the oldest enrolled users first.
- **1 day**, **3 days**, **7 days**, **14 days**, **30 days**, **90 days**, **365 days**: Automatically delete automatically enrolled users after the selected period ends.

> **Info**
> When you set a retention period, once the user limit is reached, older users are deleted immediately instead of waiting for the period to end.

View and manage automatically enrolled users

View in the **People** menu

Automatically enrolled users appear in the user list in the **People** menu.

- User IDs are assigned automatically in sequence based on facial recognition order.
- The **Description** column shows **Auto Enroll**, so you can distinguish these users from manually enrolled users.
- The **Last Updated** column shows the date and time the user was enrolled.

Edit user details

1. Click the **People** menu in the upper-left corner of the screen.
2. Click the automatically enrolled user in the user list.
3. When the user detail popup appears, edit the required information.
4. After editing user information, click **Apply**.

View facial authentication logs and face captures

1. Click the **People** menu in the upper-left corner of the screen.
2. Click the automatically enrolled user in the user list.
3. When the user details popup appears, view facial authentication logs in the **Event Logs** section.

- Select a date to view facial authentication logs for a specific period.
- Click **Face Shot** in the log to display the face photo from that authentication time.

Configure the Camera

After installing the camera, configure it for the installation environment and intended use. This section explains settings for video quality, privacy, time, network, and integration with external devices and systems. Select the required settings below.

Configure Video Profile

Live-view image quality and recorded video quality depend on the video profile settings. In video profile settings, adjust per-channel view modes and stream encoding values. Also provide Mirror (left-right flip) and channel reset features depending on the installation environment.

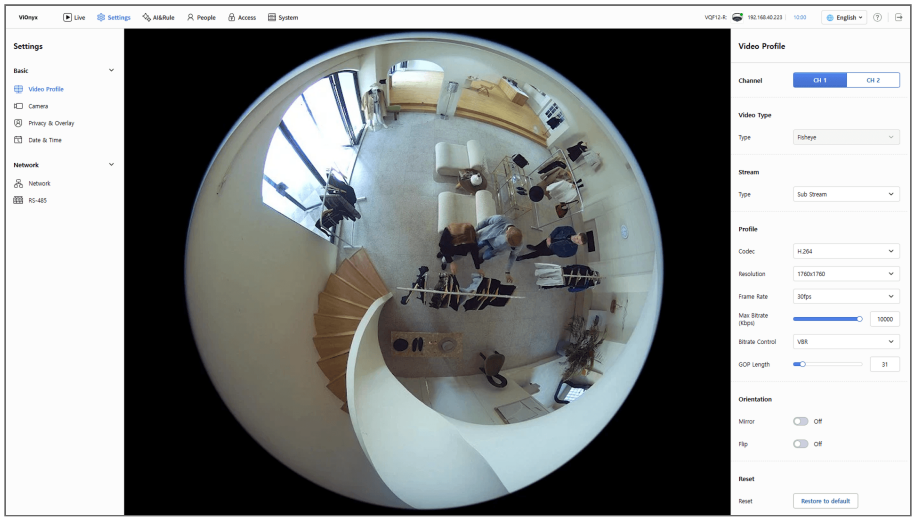
Set the video profile in the following situations to balance image quality, storage, and network bandwidth.

- When balancing storage and image quality
- When separating Main and Sub streams to match network bandwidth
- When using per-channel view modes to match their intended purpose

> **Info**
> If AI events are active, changing the mirror setting or performing a reset may delete AI event settings.

Video profile settings

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Video Profile** on the left sidebar.



> **Info**
> Video profile changes apply to the camera immediately without a separate save button.

Channel selection and view type

The main purpose of each channel is as follows.

- **CH 1**: This channel operates based on the original fisheye view from the physical camera.
- **CH 2**: This channel uses processed views, such as panorama or quad split screens, to improve monitoring efficiency.

Set detailed video profile settings per camera channel.

1. From the right **Video Profile** panel, select **CH 1** or **CH 2** in **Channel**.
2. From **Video Type** → **Type**, select the view type for the selected channel.

Channel view type policies are as follows.

- **CH 1**: Fixed to fisheye and cannot be changed.
- **CH 2**: Select a view mode other than fisheye.
  - **Single Panorama**: This mode corrects video captured by a fisheye camera so you can view a wall-style panorama.
  - **Double Panorama**: This mode corrects distortion in video captured from a 360° area so you can view a panorama split into upper and lower screens.
  - **Quad View**: This mode corrects distortion to suit human vision and lets you view 4 specific screens simultaneously.

Stream type selection

In **Stream**, select the stream to configure. Select the main or sub stream, then adjust the detailed values in the **Profile** section.

- **Main Stream**: Recording and high-quality monitoring
- **Sub Stream**: Low-bandwidth remote monitoring

> **Info**
> The **CH 2** channel supports only **Main Stream**.

Profile detail settings

Adjust codec, resolution, frame rate, and other detailed settings according to the selected stream type.

- **Codec**: Select the codec to apply to the profile. Select one of **H.264**, **H.265**, or **MJPEG**.

  > Selecting H.265 requires Profile T.

- **Resolution**: Resolution to apply to the profile. Supported resolutions vary by channel, video type, and stream type.

Channel	Video Type	Stream Type	Supported Resolution
CH 1	**Fisheye**	**Main Stream**	3520 × 3520
		Sub Stream	1760 × 1760
CH 2	**Single Panorama**	**Main Stream**	2048 × 512, 1920 × 480, 1280 × 320, 704 × 176
	Double Panorama	**Main Stream**	2048 × 2048, 1920 × 1920, 1280 × 1280, 704 × 704
	Quad View	**Main Stream**	2048 × 2048, 1600 × 1600, 1280 × 1280, 1024 × 1024

The **CH 2** channel supports only **Main Stream**.

- **Frame Rate**: Set the number of frames per second. Select one of 30, 25, 20, 15, or 10 frames per second.
- **Max Bitrate**: Set the maximum video bit rate.
- **Bitrate Control**: Select the video bitrate control method.
  - **VBR**: Variable Bitrate adjusts according to scene complexity, providing high quality when the network is stable. Recommended when network bandwidth is sufficient.
  - **CBR**: Fixed bitrate ensures stable streaming but may reduce quality in complex scenes. Recommended when network bandwidth is limited or consistent.
- **GOP Length**: Set the I-frame interval. Select a value between 1 and 300. Longer GOV reduces data size; shorter GOV increases it.

Info

- **Variable Bitrate** (VBR): This method transmits video within the maximum bit rate without fixing the data size of each frame. Bitrate varies according to scene complexity. Generally provides high quality, but may cause video interruptions when network bandwidth is unstable.
- **Constant Bitrate** (CBR): This method transmits video by fixing the data size of each frame. Provides stable streaming in environments with consistent network bandwidth, but quality may degrade depending on scene complexity.
- **GOV** (Group of Video): In H.264/H.265 compression, this refers to the group of frames from an I-frame to the frame immediately before the next I-frame. A GOV contains I-frames (key frames) that hold full image data and P-frames that contain only changes from the previous frame. A longer GOV reduces the number of I-frames, reducing video data. A shorter GOV increases the number of I-frames, increasing video data.

Mirror settings

Depending on the camera installation location, mirror or flip settings may be required.

- **Mirror**: Turn the mirror setting on or off.
- **Flip**: Turn the flip setting on or off.

> **Info**
> Changing Mirror may be restricted when AI events are configured. Follow the popup instructions to delete AI settings and proceed.

Channel settings initialization

Click **Restore to default** in **Reset** to restore the selected channel's view mode and stream settings to factory defaults.

> **Info**
> - Only the selected channel is restored to factory defaults.
> - If an AI event is set in fisheye mode, delete the AI setting before continuing.

Configure Camera Settings

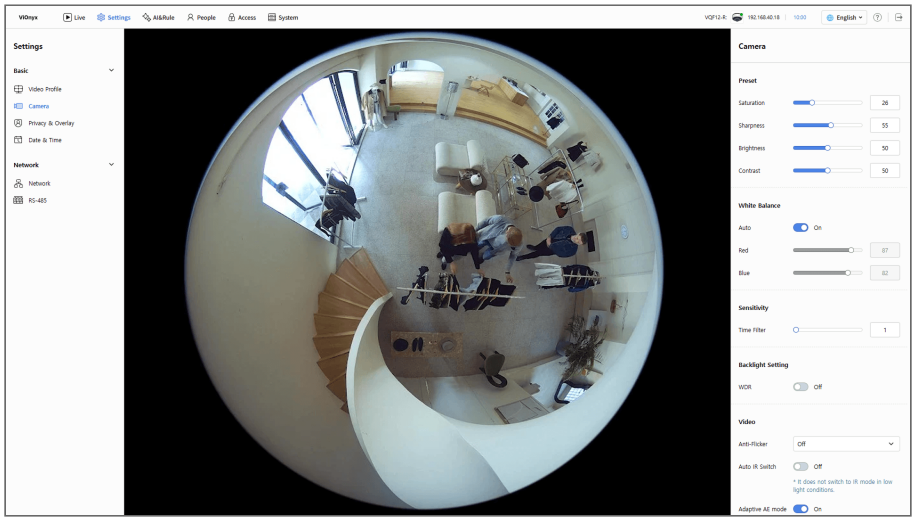
Adjust camera settings to capture optimal footage in the installation environment. Changes appear in Live View immediately, so check results while adjusting image quality, white balance, sensitivity, and backlight compensation. Available AI features vary by mounting type (ceiling or wall).

Adjust camera settings in the following situations.

- To improve image quality to match scene brightness and color.
- To minimize noise in low-light environments while maintaining motion detection.
- When strong backlight from a window or doorway makes the subject look dark
- To reduce flicker from fluorescent or LED lighting.
- When supplemental lighting is available or color video is required, and IR switching at night must stay off
- When ambient light makes a face appear too dark or too bright, face authentication may be difficult
- To optimize the camera and AI features for the installation location.
- When condensation or frost forms on the lens due to cold or humidity, and the image looks blurry

Camera settings

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Camera** on the left sidebar.



Info

Each option change appears in Live View in real time and saves automatically.

Adjust image quality

Adjust image quality to match the shooting environment. Adjust each slider in the **Preset** section to reflect changes in the preview in real time. Set values between 1 and 100.

- **Saturation**: Adjust color saturation. (Default: 26)
- **Sharpness**: Adjust image sharpness. (Default: 55)
- **Brightness**: Adjust overall image brightness. (Default: 50)
- **Contrast**: Adjust contrast between bright and dark areas. (Default: 50)

Info

When moving a slider, each setting updates the preview immediately and saves automatically.

White balance settings

Set white balance so the camera accurately reproduces the scene's lighting color. In the **White Balance** section, enable or disable the **Auto** option.

- **On**(default): The camera automatically detects and adjusts the color temperature.
- **Off**: Set the white balance by manually adjusting the **Red** and **Blue** values.

Sensitivity settings (Time Filter)

Adjust the time filter to balance sensor noise reduction and fast motion detection. Adjust the **Time Filter** slider in the **Sensitivity** section to set noise filtering strength.

- Low (1~30): Weak noise filtering helps detect fast-moving objects, but noise may increase in low-light environments.

- Medium (31~70): Balanced filtering suitable for typical shooting environments.
- High (71~100): Strong noise filtering reduces noise in low-light conditions but may hinder detection of fast-moving objects.

> **Info**
> The default value of **Time Filter** is 1.

Backlight settings

Enable WDR (Wide Dynamic Range) to allow the camera to capture bright and dark areas simultaneously in backlit scenes. In the **Backlight Setting** section, enable the **WDR** option to activate backlight compensation. (Default: **Off**)

> **Info**
> **WDR** (Wide Dynamic Range) mode allows the camera to adjust exposure automatically so both bright and dark areas are represented in backlit scenes. Enabling WDR prevents overexposure of bright areas and improves detail in dark areas. Useful when shooting in heavily backlit environments.

Anti-flicker settings

To reduce screen flicker caused by a mismatch between lighting and frequency, set the **Anti-Flicker** option in the **Video** section.

- **Off** (default): Disable anti-flicker.
- **50HZ**: 50 Hz fluorescent/LED environment
- **60HZ**: 60 Hz fluorescent/LED environment

> **Info**
> Select the option that matches the lighting frequency in the scene. Incorrect settings may cause flicker or banding on the image.

IR auto switch setting

Set whether the camera automatically switches to IR (night) mode when ambient light dims. Disable auto switching in areas with supplemental lighting or where color video is required. In the **Video** section, enable or disable the **Auto IR Switch** option.

- **On** (default): Automatically switches to IR mode when ambient light dims, based on the illuminance sensor and image brightness.
- **Off**: Does not switch to IR mode in low-light environments.

> **Info**
> Firmware version 1.1.0 or later supports the **Auto IR Switch** option.

Adaptive AE mode setting

Near a window or where sunlight changes a lot, Facial Authentication may be difficult. Use Adaptive AE mode in this case. The camera learns where faces often appear and adjusts exposure so faces look properly lit. In the **Video** section, enable or disable the **Adaptive AE mode** option.

- **On** (default): Adjusts exposure based on face area brightness.
  - Keeps face area brightness consistent under strong ambient light or changing sunlight.
  - Image brightness stays stable regardless of clothing colors, whether people pass by or stay.
  - When lighting turns on or off, readjusts exposure to the new brightness.
- **Off**: Does not use Adaptive AE mode correction. When enabled again, correction runs automatically.

> **Info**
>
> - **Adaptive AE mode** operates based on the AI event face area and person detection range. To set the area, see Manage AI Events.
> - Firmware version 1.1.0 or later supports the **Adaptive AE mode** option.

Mounting type settings

Set **Mounting Type** according to the camera's installation location. Supported AI features depend on the mounting type.

- **Ceiling** (default): Select for ceiling installation. All AI features are available.
- **Wall**: Select for wall installation. Only Facial Authentication AI is available; object tracking is not supported.

> **Info**
>
> - **When changing from ceiling to wall**, a confirmation popup appears stating that only Facial Authentication is available and object-tracking AI is unavailable. Review the message before proceeding.
> - **When changing from wall to ceiling**, the change applies immediately and all AI features activate automatically.

Camera heater setting

Low temperatures or high humidity can fog or frost the lens, blur the image, and reduce AI recognition accuracy. Enable the camera heater to keep the lens clear. In the **Heater** section, enable or disable the **Heater** option.

- **On**: The heater operates. The heater turns off automatically after 30 minutes.
- **Off** (default): Stops the heater.

Info

- To prevent overheating and unnecessary power consumption, the heater runs for 30 minutes and then turns off automatically, and the option changes to **Off**. If the lens still has fog or frost after the heater turns off, enable the option again.
- Support for the **Heater** option is included in firmware 1.1.0 or later.

Reset camera settings

To restore all camera settings to factory defaults, click **Restore to default** in the **Reset** section.

Configure Privacy & Overlay Settings

Privacy & Overlay setting lets you mask sensitive areas or automatically blur faces in camera video. Also display date/time and the camera name on video to clearly indicate the source and recording time. All settings take effect immediately in Live View.

Configure Privacy & Overlay in the following situations.

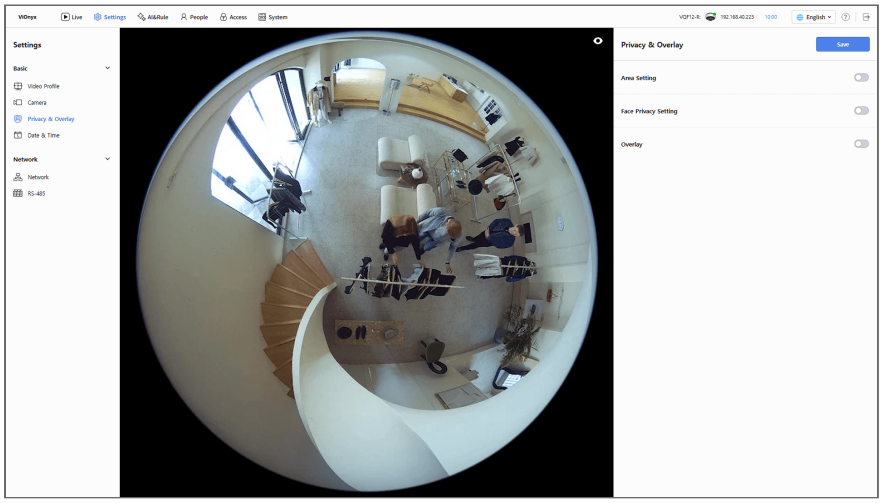
- When you need to mask specific areas that may invade privacy
- When you need to comply with privacy policies by automatically blurring faces
- When you need to ensure traceability of recorded video by displaying date/time
- When operating multiple cameras, display camera names to clarify the video source

Info

Privacy settings (masking, face blur) apply only to video display; AI analysis runs on the original images and does not affect AI performance.

Privacy & Overlay settings

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Privacy & Overlay** on the left sidebar.



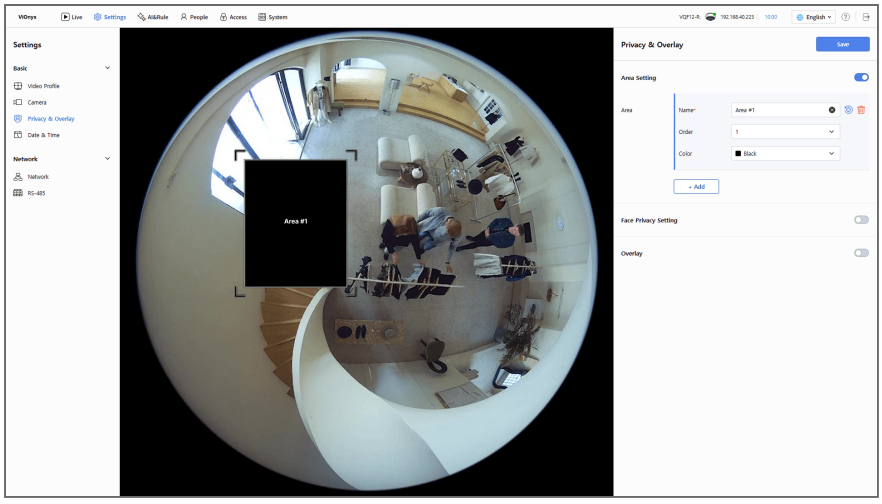
3. To save changes, click **Save** in the upper right corner of the screen.

Saved changes apply to the camera immediately after saving.

Privacy area settings

Mask specific areas in recorded video that should remain private. Set up to 10 areas; each area is fixed and does not move.

1. Click the toggle button in the **Area Setting** section.
2. Click **+ Add**.
3. A masking area is added to Live View. Drag the corners of the area to resize it, or drag the entire area to move it.



4. After you create a masking area, set the area name, order, and color in the right settings panel.
   - **Name**: The masking area name is generated automatically and can be edited if needed.
   - **Order**: Adjust the display order when masking areas overlap. A higher number appears on top.
   - **Color**: Select the masking area color.
5. To save the added masking area, click **Save** in the upper-right corner of the screen.

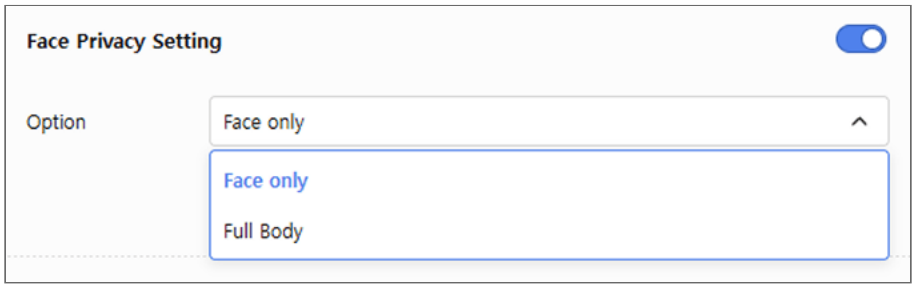
Saved masking areas are applied to Live View and recorded video.

Info

- Masked areas are applied automatically to all view modes (fisheye, single panorama, double panorama, and quad).
- To reset the masking area settings, click .
- To delete a masking area, click .

Face privacy settings

Automatically blur detected faces or full bodies to protect personal information. Enable **Face Privacy Setting** and choose the desired blur scope.



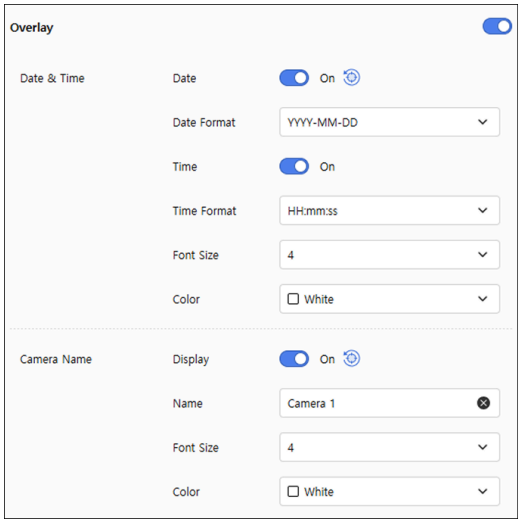
- **Face only**: All detected faces are automatically blurred.
- **Full Body**: The entire detected body is automatically blurred.

Info

Blurring faces or full bodies does not affect AI performance. While the camera displays blurred video, AI analysis runs on the original images, so AI features such as Facial Authentication and object tracking operate normally.

Overlay settings

Display date/time and camera name in Live View. Enable **Overlay** and adjust details in **Date & Time** and **Camera Name**.





> **Info**
> Each setting is saved automatically upon change and immediately applied to Live View.

Date & Time

Set the format, size, and color of the date and time shown in Live View. In Live View, check the date/time position, and drag it with the mouse to adjust its position or size if needed.

- **Date** / **Time**: Click the toggle to turn the date and time overlay on or off.
- **Date Format**: Select the date format.
  - YYYY-MM-DD (default, e.g.: 2026-01-12)
  - MM-DD-YYYY (e.g.: 01-12-2026)
  - DD-MM-YYYY (e.g.: 12-01-2026)
- **Time Format**: Select the time format.
  - HH:MM:SS (default, e.g.: 13:45:56)
  - HH:MM (seconds omitted, e.g.: 13:45)
- **Font Size**: Select the font size shown in Live View. Select from 1 to 20.
- **Color**: Select the text color shown in Live View.

> **Info**
> The date and time overlay appears only in Fisheye View.

Camera Name

Display the camera name in Live View to clarify the video source. In Live View, check the camera name position, and drag it with the mouse to adjust its position or size if needed.

- **Display**: Click the toggle to turn the camera name overlay on or off.
- **Name**: Enter the camera name.
- **Font Size**: Select the font size shown in Live View. Select from 1 to 20.
- **Color**: Select the text color shown in Live View.

Save settings

Verify settings immediately in Live View. To save them, click **Save** in the upper right corner of the screen. Saved settings apply to the camera and appear in Live View and recorded video.

Configure Date and Time

Date and time settings keep the camera's clock accurate. Select a time zone and set the time manually or synchronize automatically with an NTP server. Accurate time ensures the reliability of video timestamps and AI event logs.

Check date and time settings in the following situations.

- After installing the camera, set the time zone to match the operating region.
- To synchronize the camera's clock by entering the exact time manually.
- To maintain accurate time automatically over long periods via an NTP server.
- To unify time across multiple cameras to simplify video analysis and tracking.

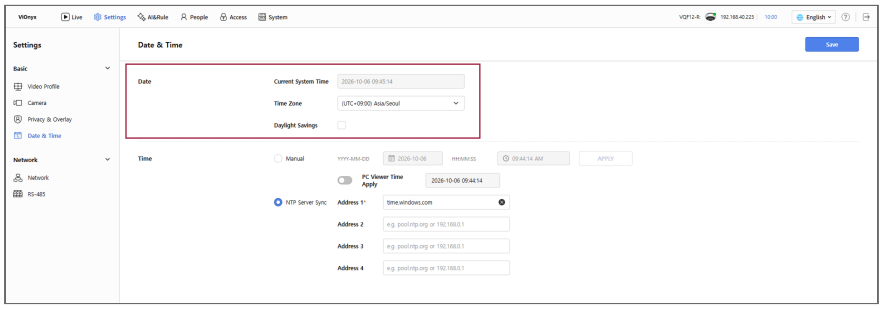
> **Info**
>
> Inaccurate camera time reduces the reliability of AI event logs, video timestamps, and system logs. Check time settings regularly.

Time zone settings

First, set the camera's time zone to the operating region.

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Date & Time** on the left sidebar.
3. In the **Date** section, select the region in **Time Zone**.

   > *Example:* *(UTC+09:00) Asia/Seoul*



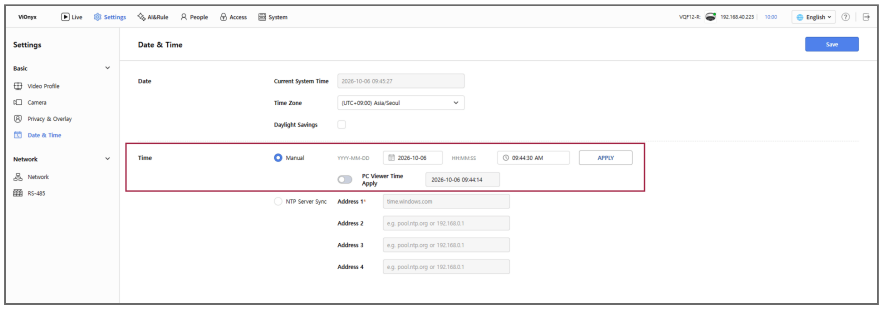
4. To apply daylight savings for the time zone, enable the **Daylight Savings** option by clicking its checkbox.
5. Click **Save** at the top right of the screen to save the selected time zone.

> **Info**
>
> The default is set to (UTC+09:00) Asia/Seoul. If the operating region differs, change the time zone.

Manual time setting

Set the camera's time manually.

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Date & Time** on the left sidebar.
3. In the **Time** section, select **Manual**.



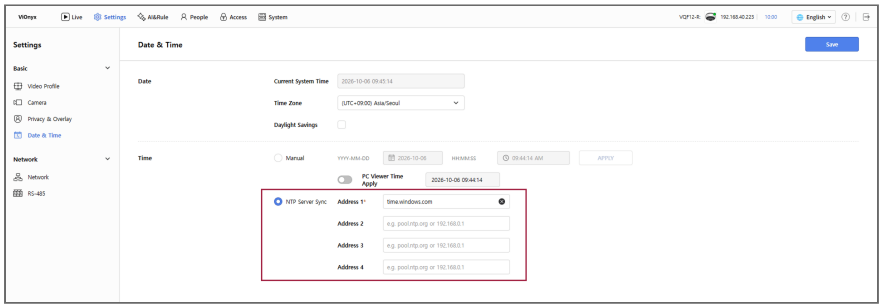
4. Enter the current date in the Date field, or click the calendar icon to select a date.
5. Enter the current time in the Time field, or click the clock icon to select a time.
6. Click **Apply** to apply the manual time setting.
7. Click **Save** at the top right of the screen to save the time settings.

> **Info**
>
> - Enable the **PC Viewer Time Apply** option to apply the PC's time to the camera automatically. The system time in the web browser is applied to the camera.
> - Manual mode and NTP automatic synchronization cannot be active at the same time. Selecting manual mode disables NTP automatic synchronization.

Automatic time synchronization

Use an NTP server to keep the camera's time accurate automatically. Recommended for long-term operation.

1. Click **Settings** in the upper-left of the screen.
2. Click **Basic** → **Date & Time** on the left sidebar.
3. In the **Time** section, select **NTP Server Sync**.



4. Enter the NTP server address in the **Address {n}** (required) field.
   - URL format: time.windows.com, time.nist.gov, etc.
   - IP address: 192.0.2.1, etc.

5. (Optional) Enter additional NTP servers in **Address {n}**, **Address {n}**, and **Address {n}** if needed.
    - Up to 4 servers are supported.
    - If **Address {n}** does not respond, the system automatically switches to the next server.
6. Click **Save** at the top right of the screen to save the time settings.

After setup, the camera automatically synchronizes with the NTP server and periodically updates the time.

> **Info**
>
> **Recommended NTP Servers**
>
> - time.windows.com (Windows public NTP)
> - time.nist.gov (NIST public NTP)
> - pool.ntp.org (NTP Pool project)

Configure Network Settings

Network settings set the device IPv4 address, subnet, gateway, and DNS servers. They set ports for the web UI and live video streaming. Select either automatic assignment (DHCP) or manual (Static) according to your network environment.

Configure the profile that NVR/VMS uses to connect via ONVIF. Connect to the external Suprema CLUe cloud service to synchronize user information. Cloudflare Tunnel enables access to the web UI from outside the network.

Check network settings in the following situations.

- When the network supports DHCP and you need the device to obtain an IP address automatically.
- When you need stable network access using a fixed IP address.
- When the default ports conflict with other devices or you need to change ports for security.
- When connecting via ONVIF to a legacy NVR/VMS that does not support Profile T
- When synchronizing user information with the Suprema CLUe cloud service
- When accessing the device web UI from outside the network without port forwarding or a public IP address

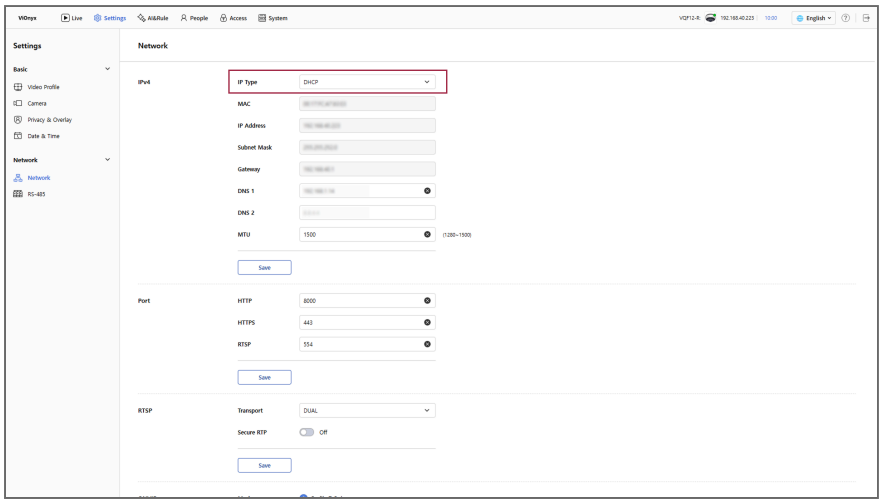
> **Info**
>
> Changing network settings, especially the IP address, may disconnect active connections. Reconnect using the new IP address.

Automatic IP address

DHCP automatically assigns IP addresses on the network. In most typical network environments, it configures automatically without additional settings.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.

3. Select **DHCP** in **IP Type**.



4. If you need **DNS** server addresses, enter them in the **DNS {n}** and **DNS {n}** input fields.

5. Adjust the **MTU** (Maximum Transmission Unit) value as needed in the **MTU** input field.

   - The default is 1500.
   - Set a value between 1280 and 1500.

6. Click **Save** to save the network settings.

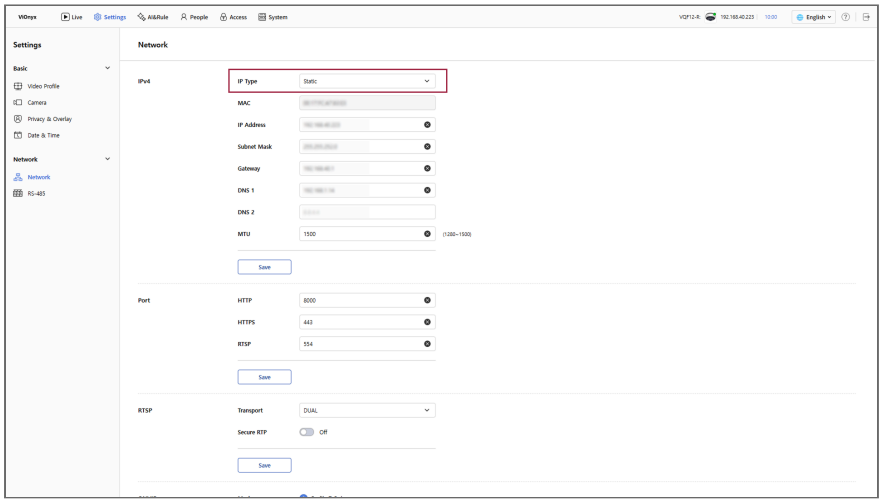
If the settings save successfully, the assigned IP address appears in the **IP Address**, **Subnet Mask**, and **Gateway** input fields.

> **Info**
>
> DHCP mode is set by default and operates automatically in most standard network environments without additional settings.

Static IP address

Set the IP address manually when the network requires a fixed IP for stable access.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. Select **Static** in **IP Type**.



4. Enter the assigned IPv4 address in the **IP Address** input field.

   > *Example: 192.168.111.11*

5. Enter the subnet mask in the **Subnet Mask** input field.

   > *Example: 255.255.255.0*

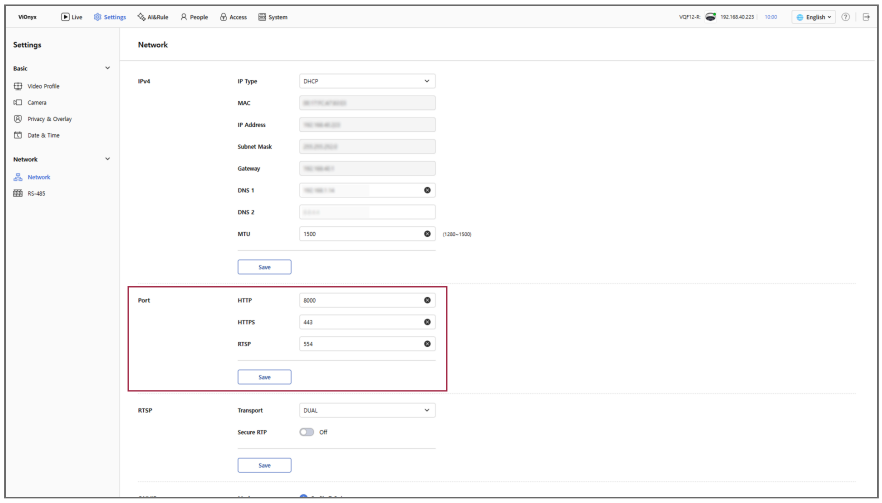
6. Enter the gateway address in the **Gateway** input field.
7. Enter the DNS server address in the **DNS {n}** and **DNS {n}** input fields.
8. Adjust the value in the **MTU** input field as needed.
   - The default is 1500.
   - Set a value between 1280 and 1500.
9. Click **Save** to save the network settings.

> If you do not enter a valid address in each input field, a red border appears around the field and **Save** is disabled. After entering all input fields correctly, try again.

Port settings

In the **Port** section, set port numbers used to access the web UI (HTTP, HTTPS) and for video streaming (RTSP).

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. Set the required ports in the **Port** section.



- **HTTP**: Port for unencrypted access to the web UI (default: 8000)
- **HTTPS**: Port for encrypted access to the web UI (default: 443)
- **RTSP**: Port for streaming video through the RTSP protocol (default: 554)

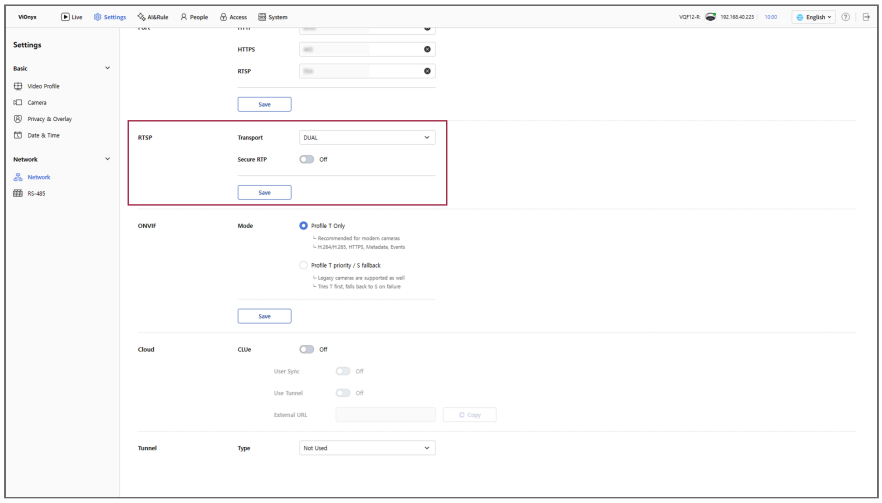
4. Click **Save** to save the port settings.

> **Info**
>
> - Enter a number from 1 to 65535 in each port input field.
> - Do not assign the same port number to multiple services. Each port must have a unique number.
> - If a port differs from the default, include the port number in the web UI URL.
>
> *Example: If the HTTPS port is 4000:* `https://{ip_address}:4000`

Video transmission and encryption settings

In the **RTSP** section, configure video transmission and encryption settings.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. Set the following options in the **RTSP** section.



- **Transport**: Select the transport protocol used for video streaming.
  - **UDP**: Enables faster transmission, but video may stutter depending on network conditions.
  - **TCP**: Provides stable transmission, but latency may occur compared with **UDP** depending on network conditions.
  - **DUAL**: Automatically selects UDP or TCP for streaming based on network conditions. This is the recommended default for general environments.
  - **TLS**: Sends the RTSP stream with TLS encryption. Enhances security, but may increase CPU load. Check whether the connected NVR/VMS supports TLS.
- **Secure RTP**: Enable the RTSP stream encryption option.

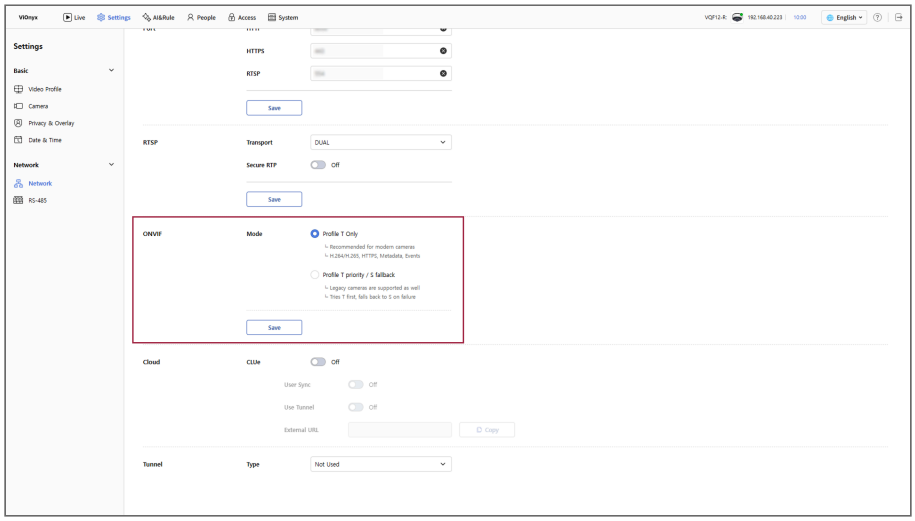
4. Click **Save** to save the settings.

> **Info**
>
> If you need encryption for video and audio data, enable the **Secure RTP** option, and check whether it is compatible with the connected NVR/VMS.

> **Caution**
>
> After changing the **Secure RTP** option, you may need to reconnect the existing RTSP session. Configure the NVR/VMS to be compatible with the selected transport method.

ONVIF settings

In the **ONVIF** section, set the profile that NVR/VMS uses to connect via ONVIF. By default, the device uses only Profile T. Enable Profile S fallback when connecting to legacy NVR/VMS that does not support Profile T.



You can select one of the following two modes.

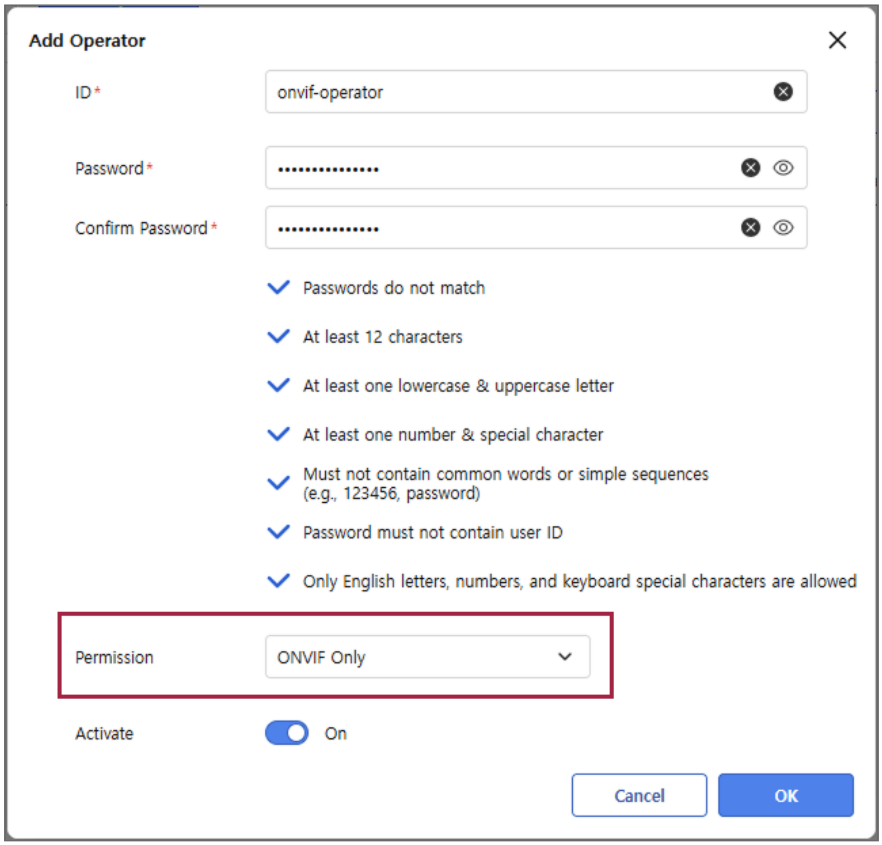
- **Profile T Only**: Connect using only Profile T (Media2). This mode supports H.264/H.265 codecs, HTTPS, metadata, and events, and it is the recommended default for modern NVR/VMS environments.
- **Profile T priority / S fallback**: NVR/VMS first tries to connect using Profile T, then connects using Profile S (Media1) if Profile T is not supported. NVR/VMS that supports Profile T connects using Profile T in this mode.

Item	Profile T (Media2)	Profile S (Media1)
Codec	H.264, H.265	H.264, MJPEG
Encrypted communication	HTTPS support	Not supported (plaintext communication)
Advanced Features	Metadata, events	Basic video streaming
Recommended environment	Latest NVR/VMS	Older NVR/VMS that does not support Profile T

Create an ONVIF-only account

Create an ONVIF-only account for ONVIF and RTSP authentication before enabling Profile S fallback. If you save settings without an account, the **Enabling the Profile S fallback requires an ONVIF-only account** message appears, and the system does not save the settings.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.
3. In the **Operator** section, click **+ Add**.
4. In the **Add Operator** pop-up window, enter the username and password, then select **ONVIF Only** in **Permission**.

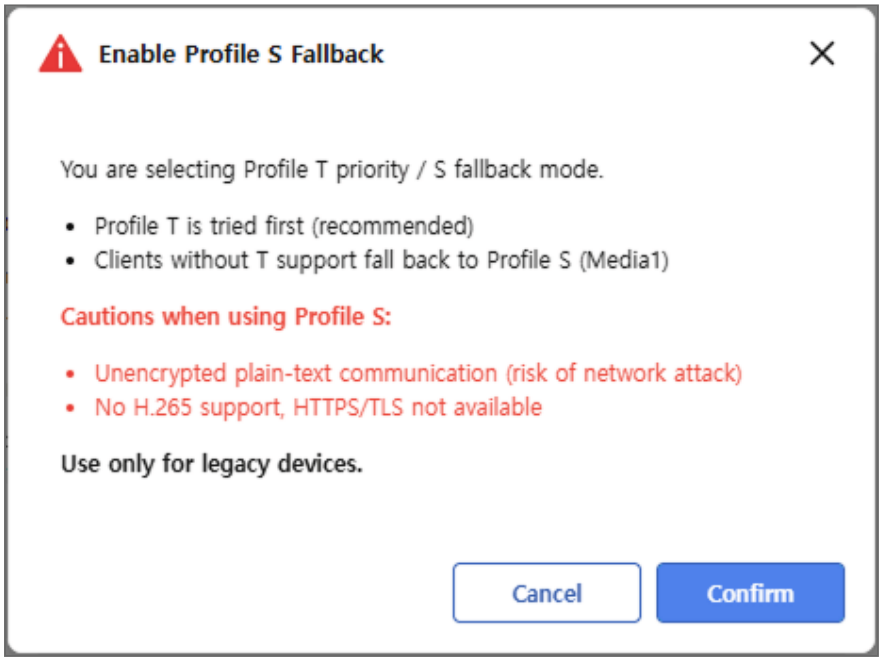


5. Click the **OK** button to create an ONVIF-only account.

Enable Profile S fallback

Enable Profile S fallback.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. In the **ONVIF** section, select **Profile T priority / S fallback** in **Mode**.
4. When the **Enable Profile S Fallback** pop-up window appears, review the precautions for Profile S, then click the **Confirm** button.



5. Click **Save** to save the settings.

When settings save successfully, a success message appears in the upper right corner of the screen. When adding the device to the NVR/VMS, enter the ID and password for the ONVIF-only account.

To disable Profile S fallback, select **Profile T Only**, then click the **Save** button.

> **Caution**
> Profile S sends unencrypted plain-text traffic, which exposes it to network attacks. Profile S also does not support the H.265 codec or HTTPS/TLS. Use it only when connecting to older NVR/VMS that does not support Profile T.

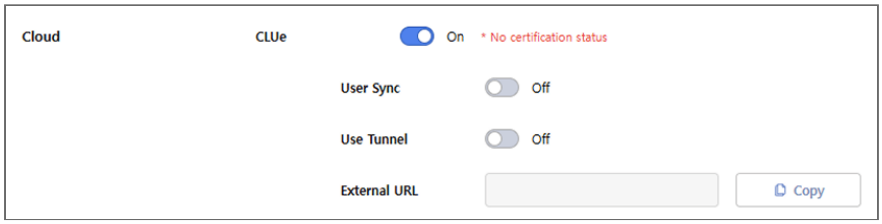
> **Info**
> - Only administrators can change ONVIF settings.
> - Each device allows only one ONVIF-only account. The account cannot log in to the web UI. The system does not allow ID or password changes after creation.
> - Only these actions are available for the ONVIF-only account: enable, disable, or delete. If the account is disabled, the system cannot enable Profile S fallback.
> - To delete the ONVIF-only account, first change to **Profile T Only**.
> - The updated ONVIF settings apply to new connections. Connected streams keep the current connection method until they reconnect.

CLUe cloud connection

Suprema CLUe is a cloud-based access control service. Connect to CLUe to sync user information with the CLUe cloud service.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.

3. Click the **CLUe** toggle in the **Cloud** section to enable it.
4. The system checks the Internet connection and the CLUe server connection. The connection status appears to the right of the **CLUe** toggle.



- *** Connecting...**: Connecting to the CLUe server.
- *** Connected**: Connected to the CLUe server.
- *** Connection failed**: Failed to connect to the CLUe server. Check the Internet connection and try again.
- *** No certification status**: The device is not CLUe-certified.

5. Enable the required options. Enable the **CLUe** toggle to use the following options.
   - **User Sync**: Syncs user information with the CLUe cloud service.
   - **Use Tunnel**: Uses a tunnel for external access to the device through CLUe. When the tunnel connects, the URL appears in the **External URL** field. Click the **Copy** button to copy the URL.

> **Info**
>
> - If the connection succeeds, the **CLUe has been enabled** message appears.
> - If the connection fails, the **CLUe has been disabled** message appears. Check the Internet connection and try again.
> - Disable the **CLUe** toggle to disconnect from the CLUe server. **User Sync** and **Use Tunnel** become unavailable. However, the registration information on the CLUe server is retained.
> - CLUe connection successes and failures are recorded in the system log.

Tunnel settings

In the **Tunnel** section, use Cloudflare Tunnel to create an external URL to access the device web UI from the internet. Use this when remote access is required without router port forwarding or a public IP address.

In **Tunnel** > **Type**, select one of the following.

Type	Description	Required information
Not Used	Do not use Tunnel. This is the default setting.	None
Cloudflare Tunnel (Quick)	Get a temporary external URL without a Cloudflare account. The URL changes when the device restarts.	None
Cloudflare Tunnel (Named)	Create a Tunnel with a Cloudflare API token, and use a fixed external URL with your domain.	Cloudflare account, domain

Type	Description	Required information
Cloudflare Tunnel (Named, Token)	Connect to a Tunnel created in the Cloudflare dashboard using a Connector token.	Cloudflare account, domain, Connector token

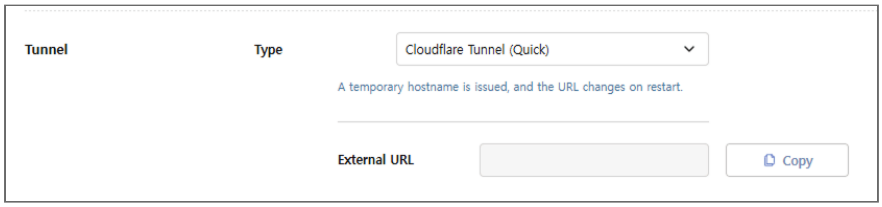
> **Tip**
> Use **Cloudflare Tunnel (Quick)** for testing or temporary remote access. Use **Cloudflare Tunnel (Named)** or **Cloudflare Tunnel (Named, Token)** for continued access with a fixed address.

> **Info**
> - To disable Tunnel, select **Not Used** in **Type**.
> - To use Tunnel, the device must be connected to the internet.
> - Anyone who knows the external URL can access the device login page. Use strong passwords for administrator and operator accounts, and share the external URL only with authorized users.
> - The system log records tunnel mode changes.

Use a temporary external URL

Access the device using a temporary external URL without a Cloudflare account.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. In the **Tunnel** section, select **Cloudflare Tunnel (Quick)** in **Type**.



4. When a temporary external URL is issued, it appears in the **External URL** field. Click the **Copy** button to copy the URL, then open it in a web browser.

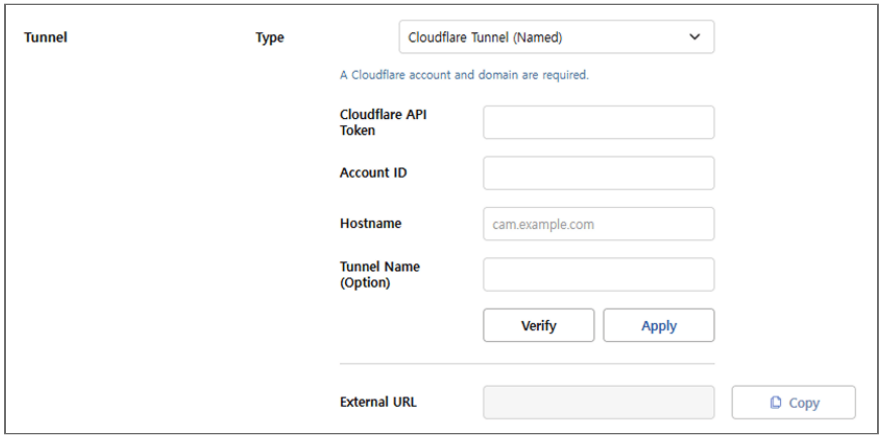
> **Caution**
> The external URL issued with **Cloudflare Tunnel (Quick)** changes when the device restarts. After restarting, check the new URL in the **External URL** field.

Use a fixed external URL (API token)

Enter a Cloudflare API token. The device creates a Tunnel in Cloudflare and links the external URL to the hostname. Before starting, prepare a Cloudflare account and a domain registered in Cloudflare.

1. Click **Settings** in the upper-left of the screen.

2. Click **Network** → **Network** on the left sidebar.
3. In the **Tunnel** section, select **Cloudflare Tunnel (Named)** in **Type**.



4. Enter the following information.
   - **Cloudflare API Token**: Enter the API token issued in the Cloudflare dashboard.
   - **Account ID**: Enter the Cloudflare account ID.
   - **Hostname**: Enter the host name to use for external access.

     > *Example: cam.example.com*

   - **Tunnel Name (Option)**: Enter a name to identify the tunnel in Cloudflare. Optional.
5. Click **Verify** to verify the entered information.
6. Click **Apply** to apply the settings.

When the tunnel connects, the external URL appears in the **External URL** field. Click **Copy** to copy the URL.

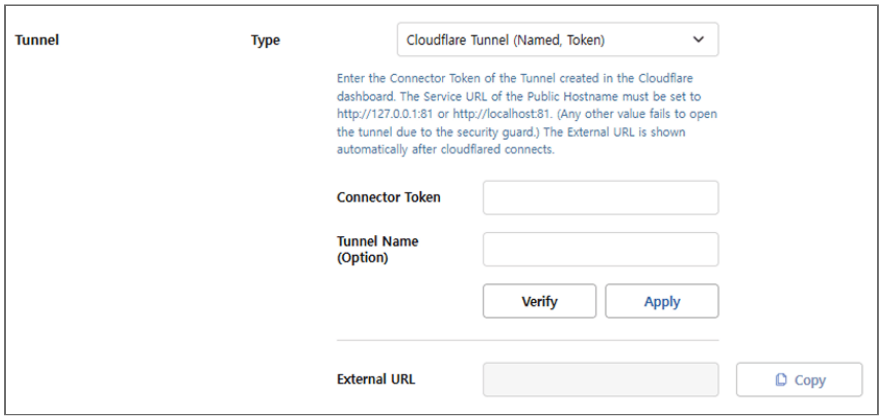
Use a fixed external URL (Connector Token)

This option connects the device to a tunnel created in the Cloudflare dashboard. Before starting, complete the following tasks in the Cloudflare dashboard.

- Create a tunnel, and copy the Connector Token.
- Add the tunnel's Public Hostname and set the Service URL to `http://127.0.0.1:81` or `http://localhost:81`.

After finishing the settings, follow these steps on the device.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **Network** on the left sidebar.
3. In the **Tunnel** section, select **Cloudflare Tunnel (Named, Token)** under **Type**.



4. Enter the following information.
   - **Connector Token**: Enter the Connector Token copied from the Cloudflare dashboard.
   - **Tunnel Name (Option)**: Enter a name to identify the tunnel. Optional.
5. Click **Verify** to verify the entered information.
6. Click **Apply** to apply the settings.

When cloudflared connects, the external URL automatically appears in the **External URL** field.

> **Caution**
> Security policies prevent the tunnel from opening if the Public Hostname Service URL is not `http://127.0.0.1:81` or `http://localhost:81`.

Set Up RS-485

In RS-485 settings, add and manage Suprema I/O devices connected to the camera RS-485 port as slave devices. The camera acts as the master for the RS-485 port. Link registered slave device relays to AI rules to control external devices, such as opening doors or turning on emergency lights.

Check **RS-485** settings in the following situations.

- When adding an I/O device to the camera to increase relay outputs or input ports
- When an AI event occurs and you need to control external devices through a slave device relay
- When checking the slave device connection status or updating firmware
- When removing a slave device that is no longer used

Info

- Firmware version 1.1.0 supports master mode only. The camera does not support slave mode for connecting to another device as a slave.
- Add up to 8 slave devices.
- Suprema I/O devices are the only supported slave devices. Fingerprint authentication devices and facial authentication devices cannot connect as slave devices.
  - Secure I/O 2 (SIO2)
  - Door Module (DM-20)
  - Door Interface (DI-24)
  - Output Module (OM-120)
  - Input Module (IM-120)

Before you start

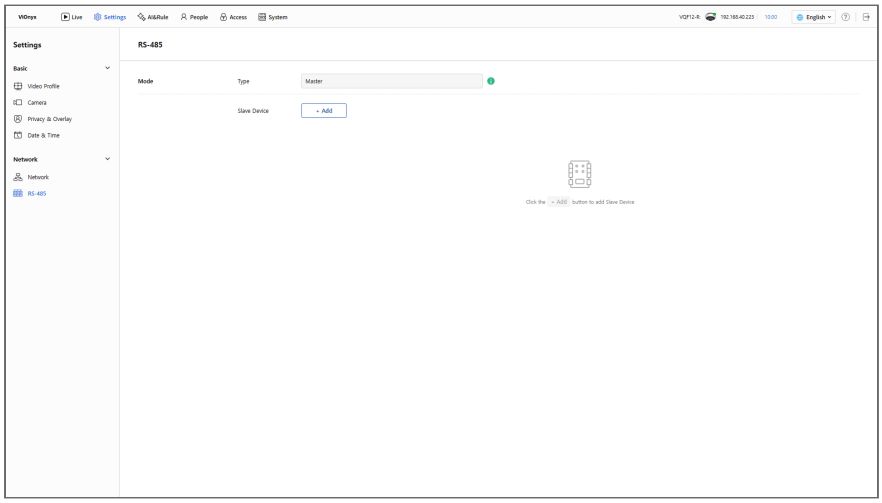
Check the following before adding slave devices.

- Confirm that the slave device is wired correctly to the camera RS-485 port.
- Confirm that an OSDP ID is assigned to the slave device. Devices with an OSDP ID of 0 (unassigned) cannot be added.
- Confirm that devices on the same RS-485 bus have unique OSDP IDs.
- If the slave device was added to another master device, initialize the device.

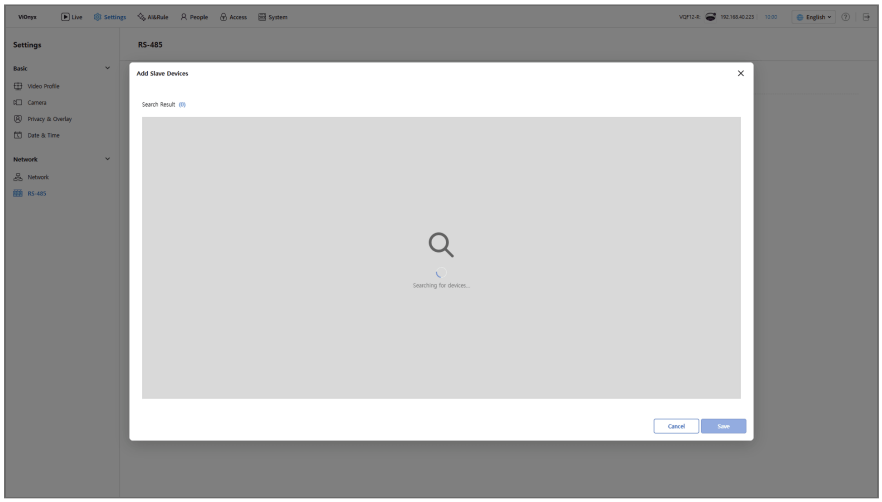
Add slave devices

Search for slave devices connected to the RS-485 port, and add them to the camera.

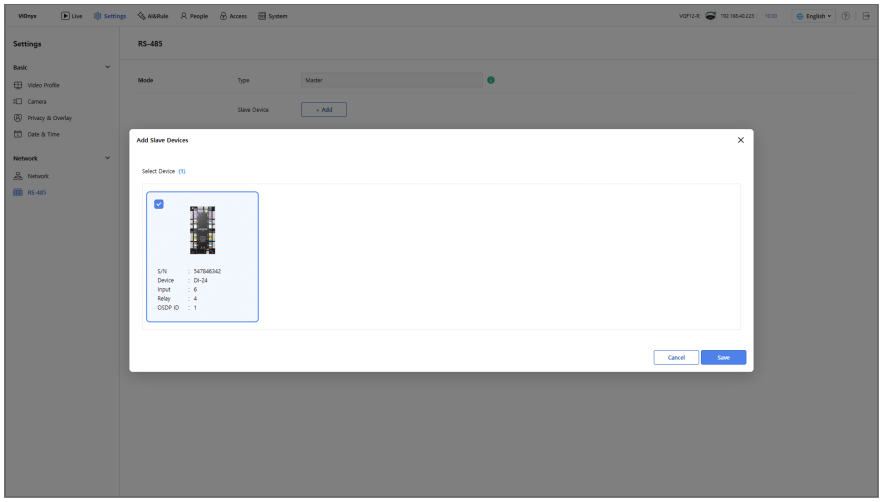
1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **RS-485** on the left sidebar.



3. In **Slave Device**, click **+ Add**.
4. The **Add Slave Devices** pop-up appears, and the device search starts automatically. Wait for the search to complete.



5. Select the checkbox for the device to add in the search results. Select multiple devices.



The discovered devices include the following information.

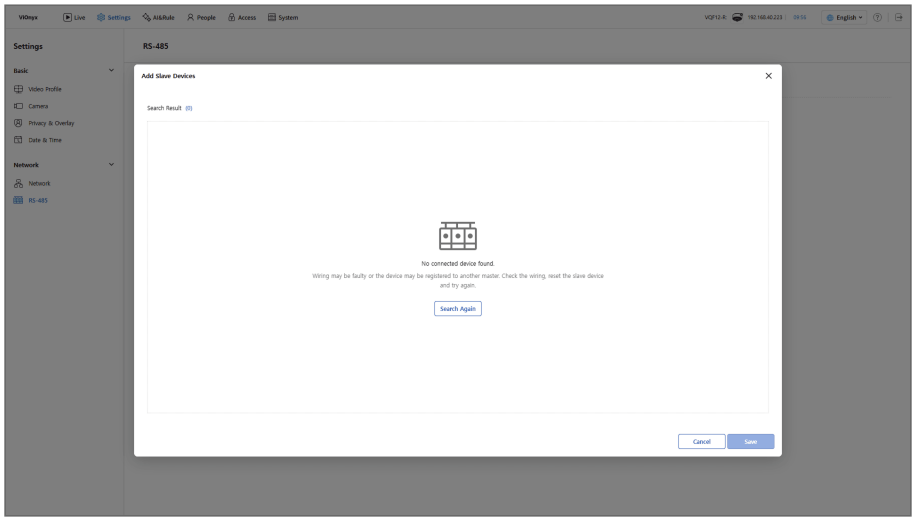
- **S/N**: Device serial number
- **Device**: Device model
- **Input**: Number of input ports
- **Relay**: Number of relay ports
- **OSDP ID**: OSDP ID assigned to the device

6. Click **Save** to add the selected device. Select at least one device to enable the button.

When the device is added successfully, a success message appears in the upper right corner. The **Slave Device** list shows devices in OSDP ID order. The device name defaults to the serial number. Change it in Edit slave device.

When no devices are found

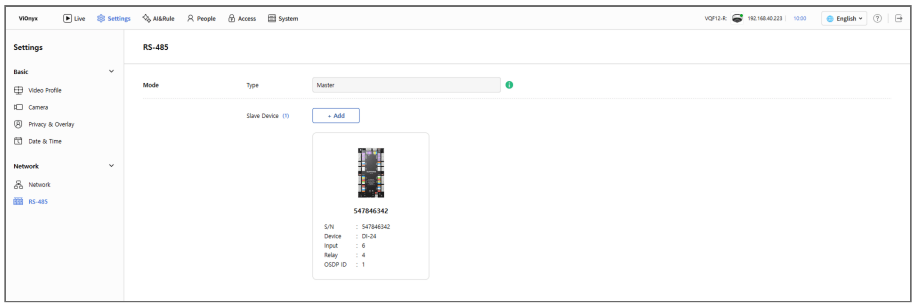
If the **No connected device found.** message appears in the search results, check the following, then click **Search Again**.



- Check that the RS-485 wiring for the slave device is connected correctly.
- If the slave device is added to another master device, initialize it.
- Confirm that an OSDP ID is assigned to the slave device.

Check slave device status

Check the device information and connection status in the **Slave Device** list.



When communication between the device and the camera disconnects, the device card shows **Disconnected** and the disconnection time. Check the device power and RS-485 wiring. The indicator disappears when the device reconnects.



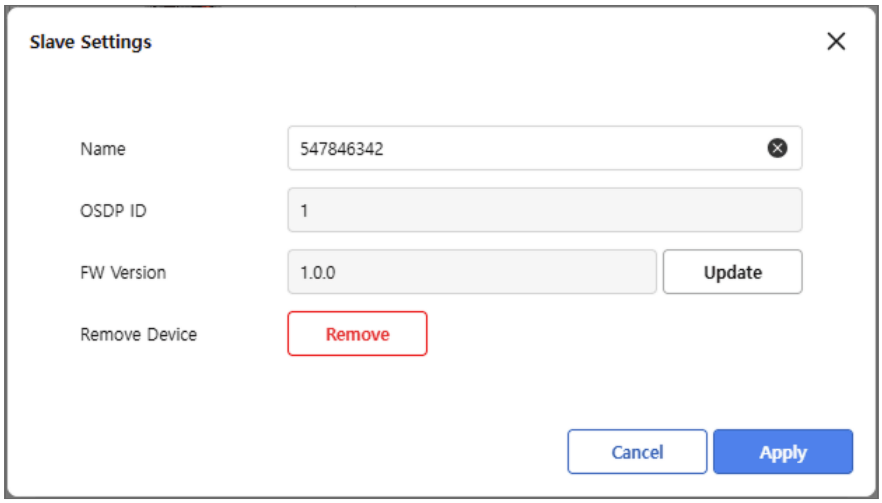
Info

Check slave device connection and disconnection records in the system log. Refer to View system logs for more information.

Edit slave device

Change the name of an added slave device.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **RS-485** on the left sidebar.
3. Hover over the device card to edit, and then click the button at the top right.
4. In the **Slave Settings** pop-up window, enter a new name in the **Name** input field.



5. Click **Apply** to save the changes.

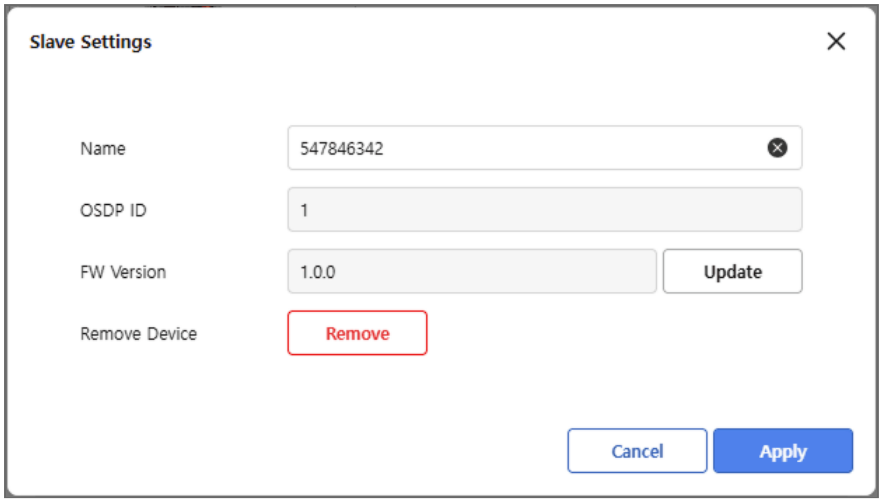
When the changes save successfully, a success message appears in the upper right corner of the screen.

> **Info**
> In the **Slave Settings** pop-up window, view the OSDP ID only. Do not change it.

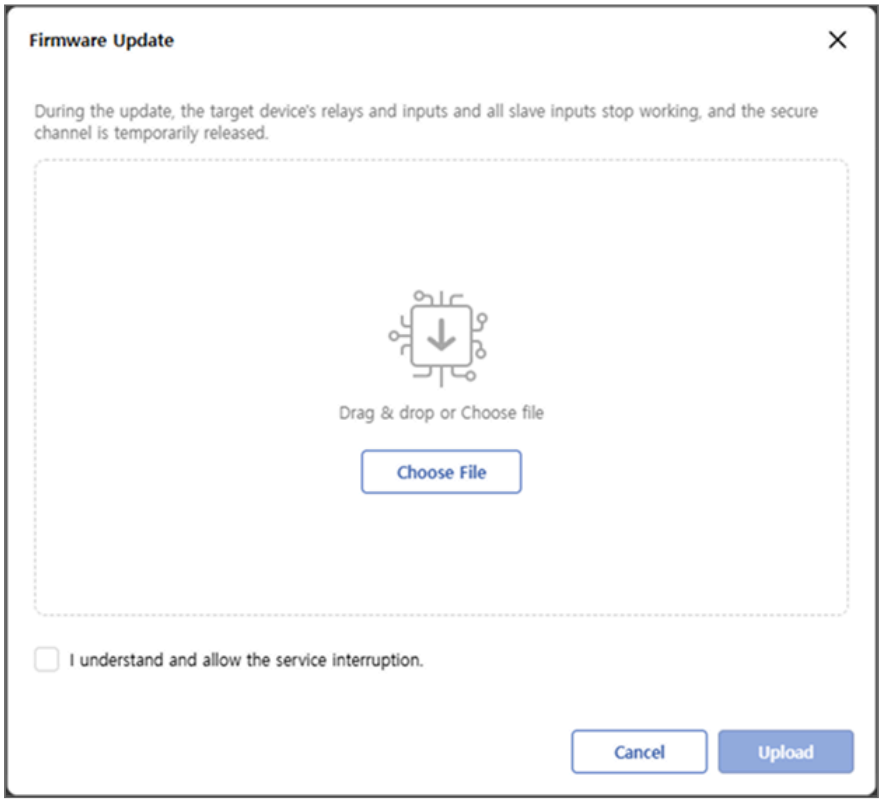
Update slave device firmware

In the **Slave Settings** pop-up window, check the current firmware version and update the slave device.

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **RS-485** on the left sidebar.
3. Hover over the device card to update, and then click the button at the top right.
4. In the **Slave Settings** pop-up window, check the current version in **FW Version**, and then click the **Update** button.



5. Drag and drop the firmware file, or click **Choose File** to select a file.



6. Review the service interruption notice, and then select the **I understand and allow the service interruption.** checkbox.
7. Click **Upload** to start the update.

The status and progress appear during the update. Check the system log for records of successful and failed slave device firmware updates.

> **Caution**
>
> - The update interrupts the target device relay and inputs, interrupts all slave device inputs, and temporarily disables the secure channel. Run the update when the device is not in use.
> - Do not power off the device or disconnect the RS-485 wiring during the update.
> - The system blocks the update while another firmware update is in progress. Try again after the current update finishes.

Remove slave device

Remove slave devices that are no longer in use. Remove devices one at a time, or select multiple devices to remove at once.

> **Caution**
>
> Devices used in AI rules cannot be removed. When you try to delete a device, the rule name that uses it appears. First, remove the device relay setting from the rule, then try again. For rule editing, see AI Rule Settings.

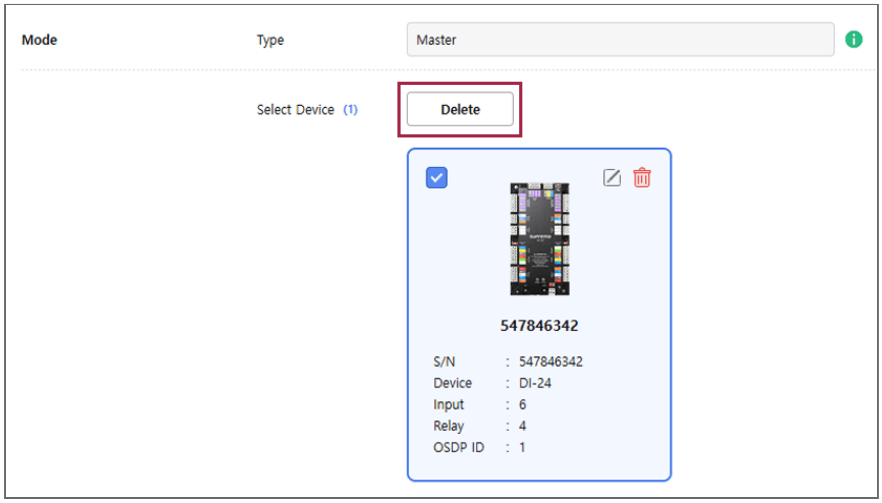
Remove devices one by one

1. Click **Settings** in the upper-left of the screen.

2. Click **Network** → **RS-485** on the left sidebar.
3. Hover over the device card to delete, then click the button at the top right.
   - Alternatively, click the button, then click **Remove** in the **Slave Settings** pop-up window.
4. When the **Remove Device** pop-up appears, click **Apply**.

Remove multiple devices at once

1. Click **Settings** in the upper-left of the screen.
2. Click **Network** → **RS-485** on the left sidebar.
3. Select the checkbox on each device card to delete. The number of selected devices appears next to **Select Device**.



4. Click **Delete**.
5. When the **Remove Device** pop-up appears, click **Apply**.

When deletion succeeds, a success message appears in the upper right corner of the screen.

Troubleshooting

The following error messages may appear when adding, editing, or deleting a slave device.

Message	Cause and solution
Failed to register the slave device. Check the wiring and try again.	Could not communicate with the device. Check the RS-485 wiring and try again.
Up to 8 slave devices can be registered.	8 devices have already been registered. Remove unused devices, and then add the device again.
A device with the same serial number is already registered.	A device with the same serial number is already in the list. Check the list.

Message	Cause and solution
OSDP ID is already in use.	Another device is using the same OSDP ID. Change the OSDP ID on the slave device, and then search again.
The OSDP ID collides with another device on the bus.	The OSDP ID conflicts with another device on the RS-485 bus. Change the OSDP ID on the slave device, and then search again.
OSDP ID 0 (unassigned) cannot be registered. Assign an address on the device and search again.	This device has an OSDP ID of 0 (unassigned). Assign an OSDP ID to the device, then search again.
Device search timed out.	The device did not respond within the search timeout. Check the wiring, then search again.
Slave device is in use by a rule.	An AI rule uses the device. Remove the relay setting for the device from the rule, then try again.
RS-485 is initializing. Please wait.	The camera is initializing the RS-485 port. Try again in a moment.

Integrate RTSP and ONVIF

The camera supports RTSP (Real-Time Streaming Protocol) streaming and the ONVIF (Open Network Video Interface Forum) protocol for standard integration with third-party NVR (Network Video Recorder) and VMS (Video Management Software).

Refer to this guide in the following cases:

- When you want to get camera video through RTSP in a third-party NVR/VMS
- When you want to integrate the camera with an NVR/VMS that supports ONVIF
- When you want to check the account information required for an RTSP access URL or ONVIF integration

RTSP streaming

Port and transport method

Change the RTSP port and transport method in the **Network** setting. For details about port settings, video transmission, and encryption settings, refer to the following document.

- Port settings
- Video transmission and encryption settings

> **Info**
> If you changed the RTSP port from the default value (554), enter the changed port number in the `{port}` part of the **Connection URL** below.

RTSP Connection URL

To get camera video through RTSP in a third-party NVR/VMS, register a Connection URL that matches the channel and resolution.

Channel	Stream	Connection URL
Channel 1 - Fisheye (fisheye video)	Main stream (high resolution)	`rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_primary`
Channel 1 - Fisheye (fisheye video)	Sub stream (low resolution)	`rtsp://{id}:{passwd}@{IP_address}:{port}/fisheye_secondary`
Channel 2 - Dewarp (rectified video)	Main stream (high resolution)	`rtsp://{id}:{passwd}@{IP_address}:{port}/dewarp_primary`

- `{id}`, `{passwd}`: Enter the ID and password for the account used to access the camera.
- `{IP_address}`: Enter the camera's IP address.
- `{port}`: Enter the RTSP port number. The default is 554.

ONVIF integration

Supported specifications

The camera supports ONVIF **Profile S** and **Profile T**.

Prepare a dedicated ONVIF account

According to the security standard specifications, the default administrator (admin) account does not support ONVIF connections. Before integrating with ONVIF, add a dedicated operator account for ONVIF, and use that account information to access the NVR/VMS. See Configure Network Settings for instructions on adding an ONVIF-only operator account.

Integration notes

- **Protecting setting synchronization**

  To keep data consistency with the web settings engine and prevent malfunctions, write operations that change internal camera settings, such as resolution, bitrate, and image sensor properties, through ONVIF are not supported.

- **Disable VMS automatic optimization feature**

  Some VMS products provide a feature that automatically changes camera settings on connection, such as Video Optimization and Auto Configuration. If this feature is enabled, integration errors can occur, so disable the automatic correction/optimization option for camera settings in the VMS.

> **Caution**
> If you change the RTSP transport method, you may need to reconnect the existing RTSP session. Configure the NVR/VMS to be compatible with the selected transport method.

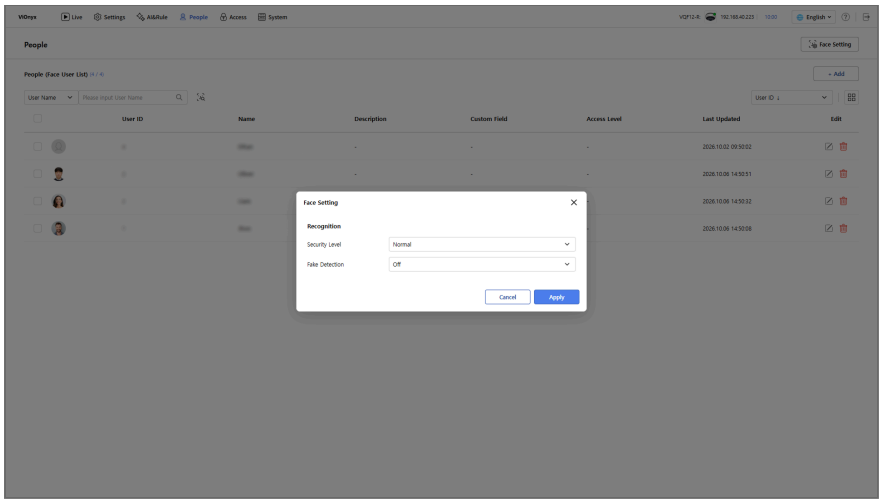
Manage Users

Register users to enable the AI face recognition feature. Efficiently manage the entire user lifecycle, from registering new users to managing and viewing existing user information.

Set Up Facial Authentication

Use Facial Authentication settings to manage authentication efficiency, security level, and spoof detection at once. Adjust values appropriately based on your organization's security policy and operating environment.

1. Click the **People** menu in the upper-left corner of the screen.
2. Click **Face Setting** in the upper right corner of the screen.
3. When the **Face Setting** window appears, set the required options.



   - **Security Level**: Set the security level. The higher the security level, the stricter the authentication becomes.
   - **Fake Detection**: Prevent user authentication with spoofed faces, such as photos.
4. When you finish setting the options, click **Apply**.

> **Tip**
> For areas that require high security, set the **Security Level** option to **Most Secure**.

Add Users

Enroll users for AI Facial Authentication. When adding a user, enter basic information and enroll a face using one of three methods.

Add users in the following situations.

- When enrolling a new employee in the organization

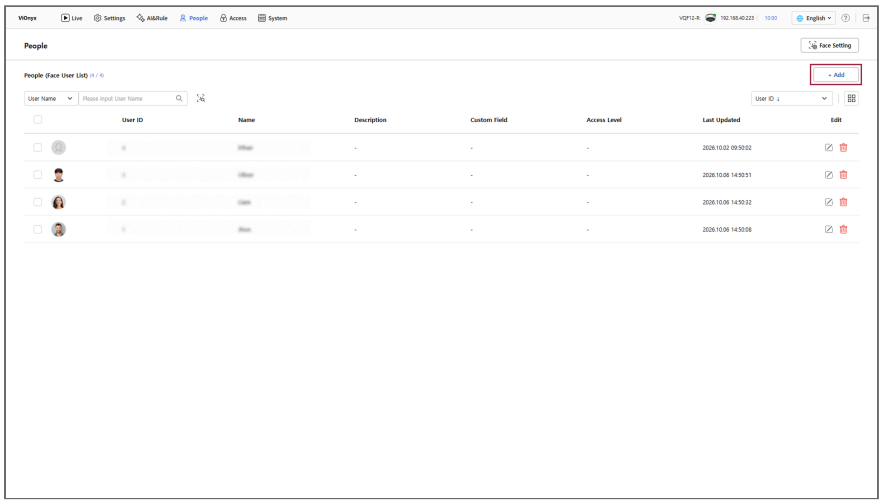
- When enrolling a user's face photo into the Facial Authentication database
- When adding multiple users in bulk
- When enrolling users for integration with external systems (ERP, HR management system)

> **Info**
>
> - To use the Facial Authentication feature, comply with local regulations.
> - When adding the first user, a Facial Authentication consent popup appears. The system log stores consent records; the popup does not reappear after consent.
> - If consent was completed earlier in AI Event settings, no popup appears when adding users.

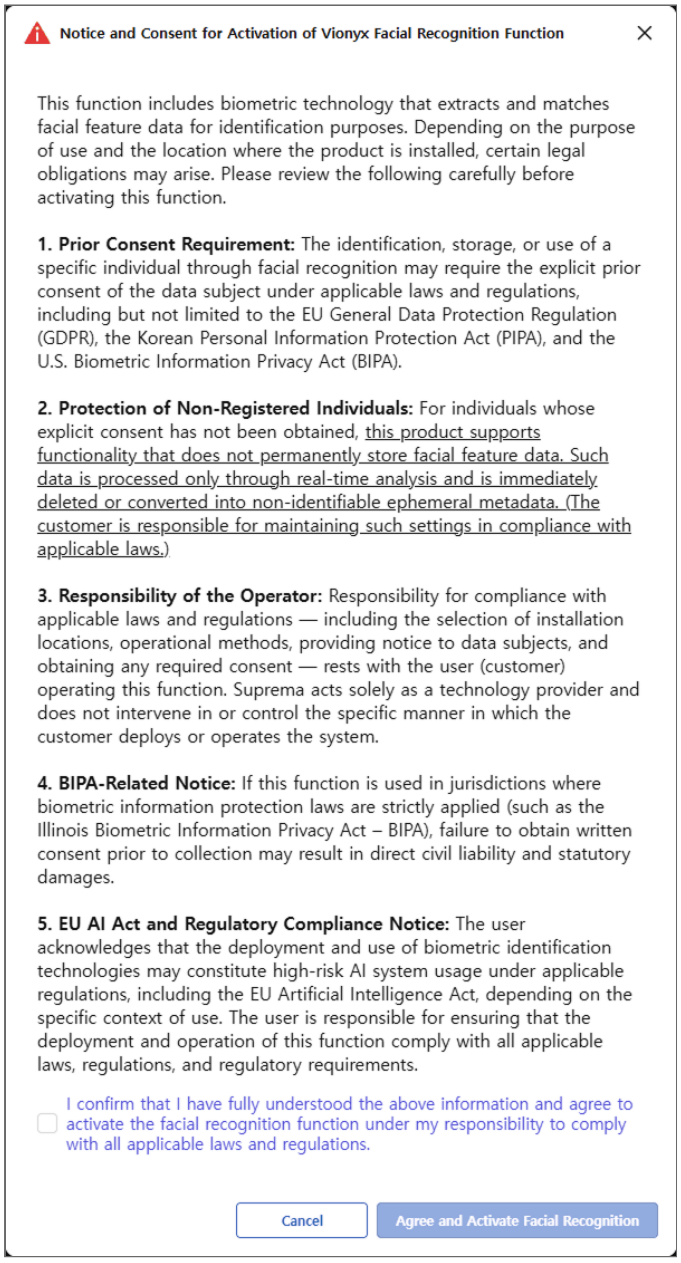
Enter basic user information

If the Facial Authentication consent popup appears when adding the first user, review it and proceed. After giving consent, enter basic information in the Add User dialog.

1. Click the **People** menu in the upper-left corner of the screen.
2. Click **Add** at the top right of the screen.

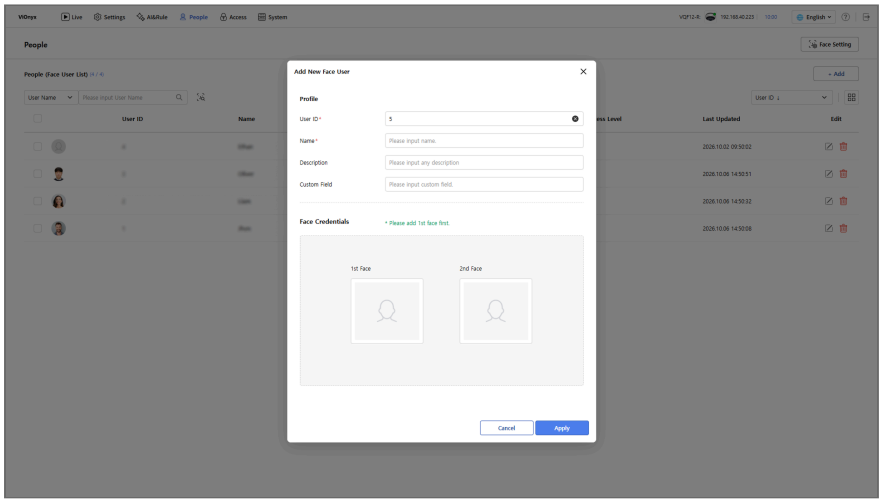


3. When adding the first user, if the **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears, review the content, select the consent checkbox, and click **Agree and Activate Facial Recognition**.



- To use the Facial Authentication feature, comply with local regulations. Cannot proceed without consent.
- The **Notice and Consent for Activation of Vionyx Facial Recognition Function** popup appears only once.

4. When the **Add New Face User** popup appears, enter the user's basic information.



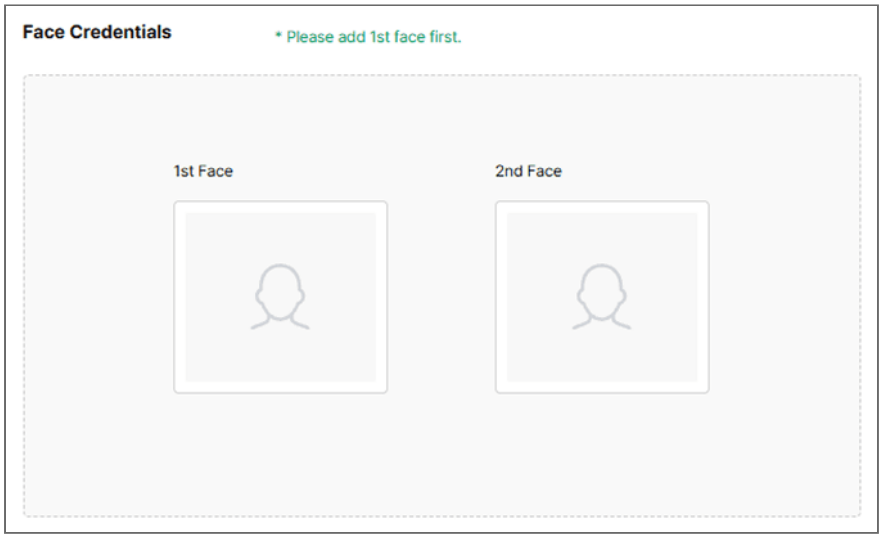
5. Enter the user's unique ID in the **User ID** input field. User ID must be unique.
6. Enter the user's name in the **Name** input field.
   - Up to 64 characters.
   - It can include Korean, Japanese, uppercase and lowercase English letters, numbers, special characters (`#` , `-` , `_` , `.` , `(` , `)`), and spaces within a word.
7. Enter a description of the user in the **Description** input field. Enter up to 256 characters.
8. The **Custom Field** input field lets you enter up to 64 characters of additional user-specific information. For example, enter notes in English such as department, title, or user group.
9. Click **Apply** to save basic user information.

> **Info**
> Create new users without a face photo. Add a face photo later from the user's detail page.

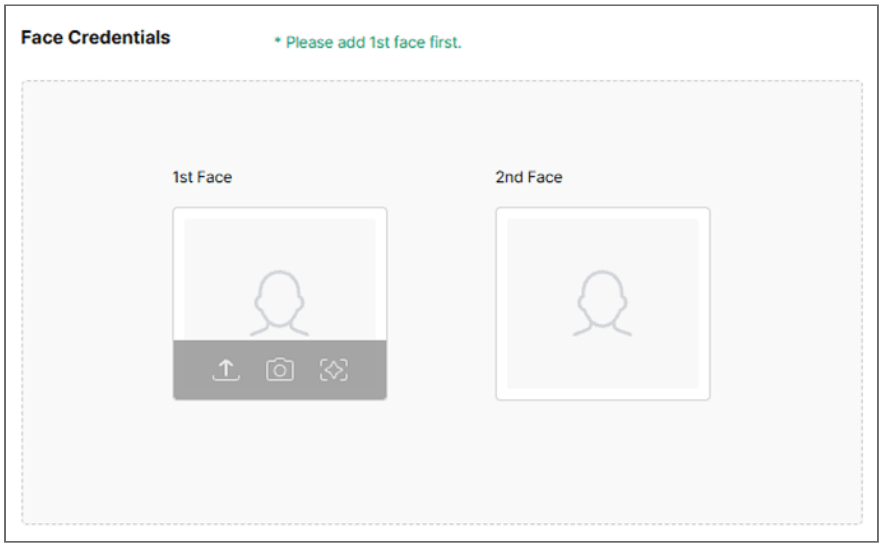
Face enrollment

Enroll a face when adding a new user or from the user's detail page. Three methods are available.

1. Click the **People** menu in the upper-left corner of the screen.
2. Click **Add** at the top right of the screen or click an existing user in the user list to open the detail page.
3. Enroll a face in the **Face Credentials** section of the Add User or User Detail popup.



4. Hover over **1st Face** to show the enrollment options.

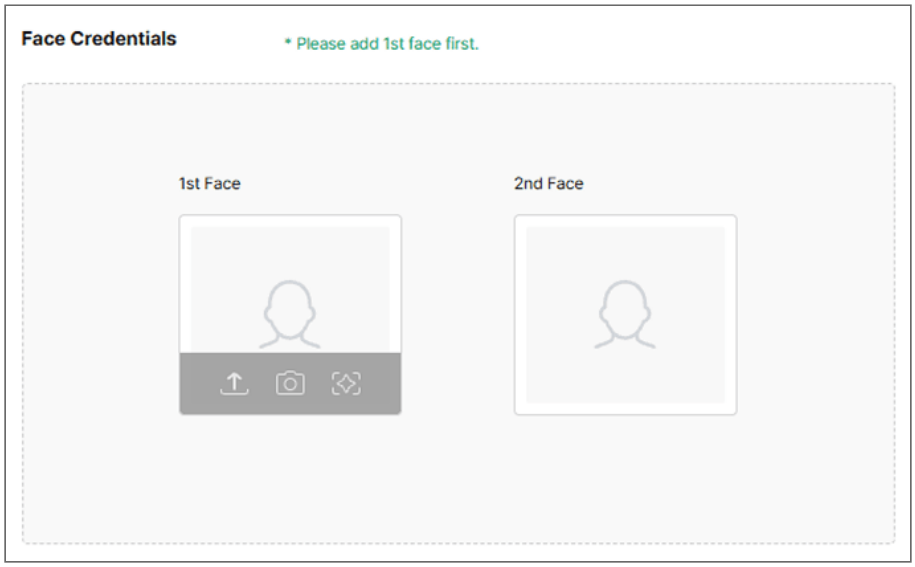


- : Upload a locally saved image file to enroll a face photo.
- : Capture a face photo with a webcam to enroll it.
- : Select a face that matches the user from the list of unrecognized faces detected through AI events, and enroll it.

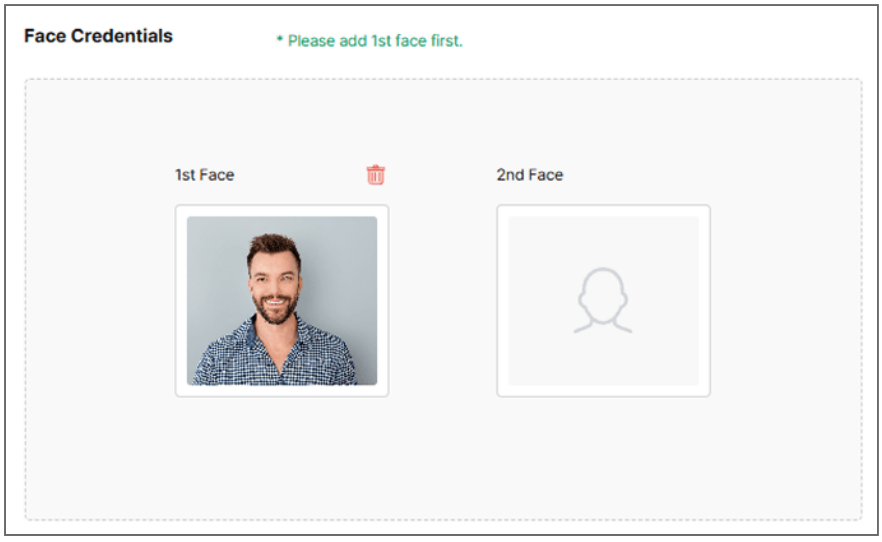
> **Info**
> Select face slot 1 first. Face slot 2 is optional.

Upload face photo

Upload a locally saved image file to enroll a face photo.



1. Upload the face photo using one of the following methods.
   - Drag and drop a locally saved image file onto the face area.
   - To select a locally saved image file, click and choose the image file you want.
2. When the face is detected, the photo appears.



3. To apply the uploaded photo to the user, click **Apply** at the bottom.

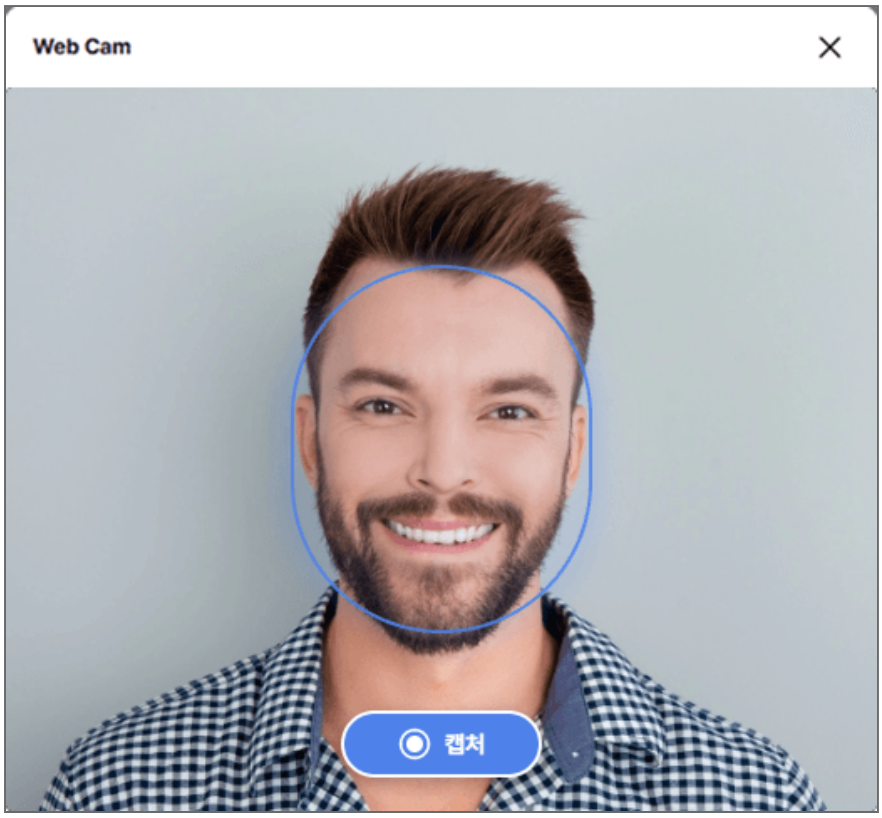
> **Info**
>
> - Supported image formats are PNG, JPEG, and JPG.
> - The maximum size for supported image files is 10MB.

Enroll face with webcam

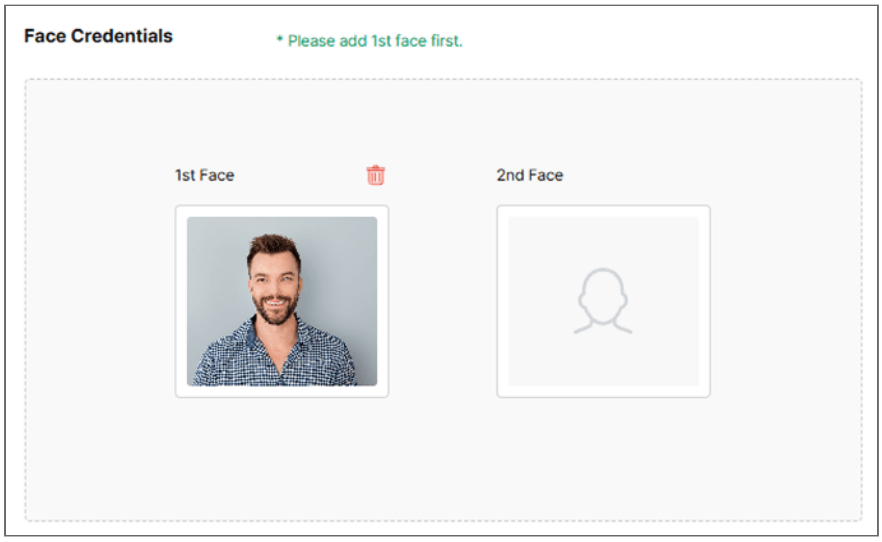
Use a webcam to capture and enroll a face photo.

1. Click .

2. When the webcam capture screen appears, position your face inside the central circle.



3. Click **Capture**.



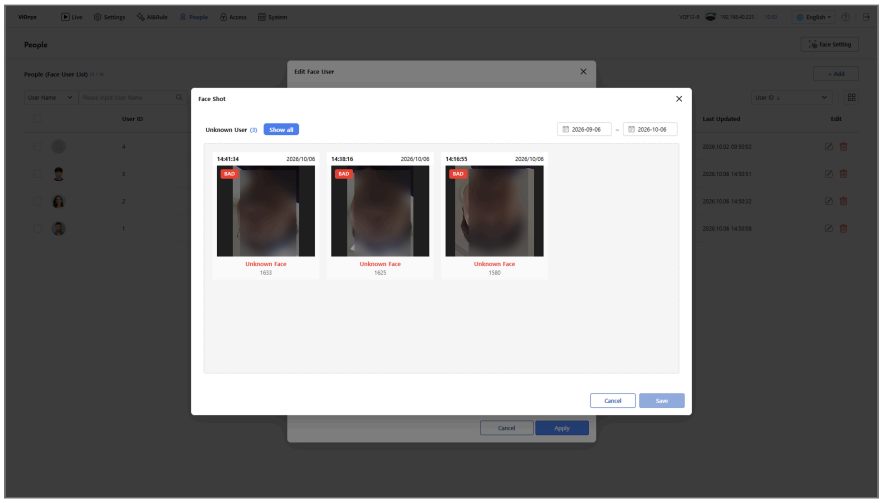
4. To apply the captured photo to the user, click **Apply**.

> **Info**
> To capture again, click the face photo and capture it again.

Enroll AI-recommended face

Select and enroll a face that matches the user from the list of unenrolled faces detected through AI analysis.

1. Click .
2. The **Face Shot** popup shows the list of recently authenticated unenrolled faces.



If the **Enrollable faces** list does not appear, click **Show all**. View all unenrolled faces.

3. Select the face that matches the user. Only one face can be selected at a time.
4. Click **Save**.
5. Click **Apply** to apply the selected face to the user.

Edit and Delete Users

Edit a registered user's information or add/change a face. Delete users who are no longer needed, and view a user's activity history in the event log.

Modify or delete users in the following situations.

- When you need to change a user's name, department, or other information
- When you need to update a user's face photo or add a new face
- When a user leaves or must be removed from the system
- When you need to review a user's authentication records and change history
- When false authentication occurs for a registered user

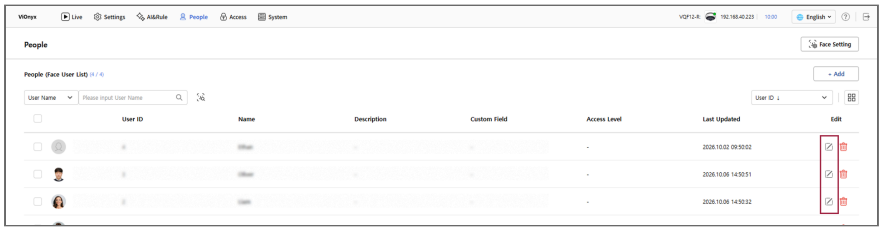
Info

- Even if you upload a high-quality photo when editing user information, previous template data may remain. Delete the user and register again.
- Deletion is irreversible. Back up any required data and verify carefully before deleting a user.

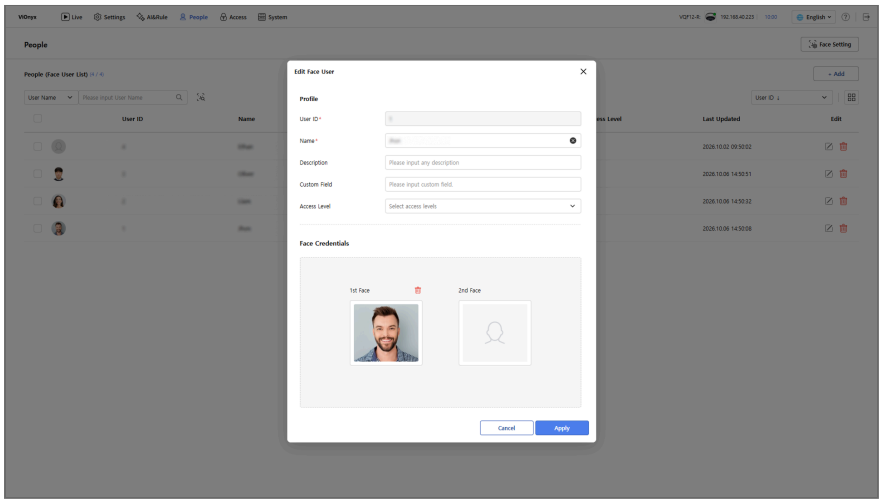
Edit user information

Edit a registered user's information or add/change a face.

1. Click the **People** menu in the upper-left corner of the screen.
2. In the user list, click the button in the **Edit** column for the user you want to edit.



3. When the **Edit Face User** window appears, edit the required information.



4. After editing user information, click **Apply**.

After saving edits, a success message appears in the top-right and the view returns to the user list.

> **Info**
>
> - For more information on user details, see Add Users.
> - The **User ID** cannot be changed.
> - Face photos can be deleted individually. Click in the upper right corner of that face photo.

Delete users

Delete users who are no longer needed.

Delete an individual user

1. Click the **People** menu in the upper-left corner of the screen.
2. In the user list, click at the far right of the user to delete.

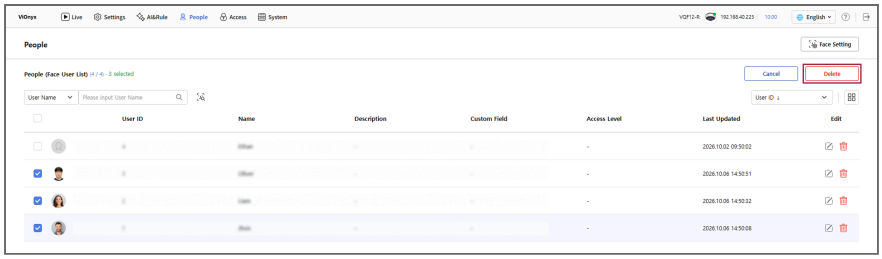


3. When the deletion confirmation message appears, click **OK**.

A deletion confirmation message appears in the top-right and the user is removed from the user list.

Delete multiple users

1. Click the **People** menu in the upper-left corner of the screen.
2. In the user list, click the checkbox at the far left of the user to delete. Select multiple users.



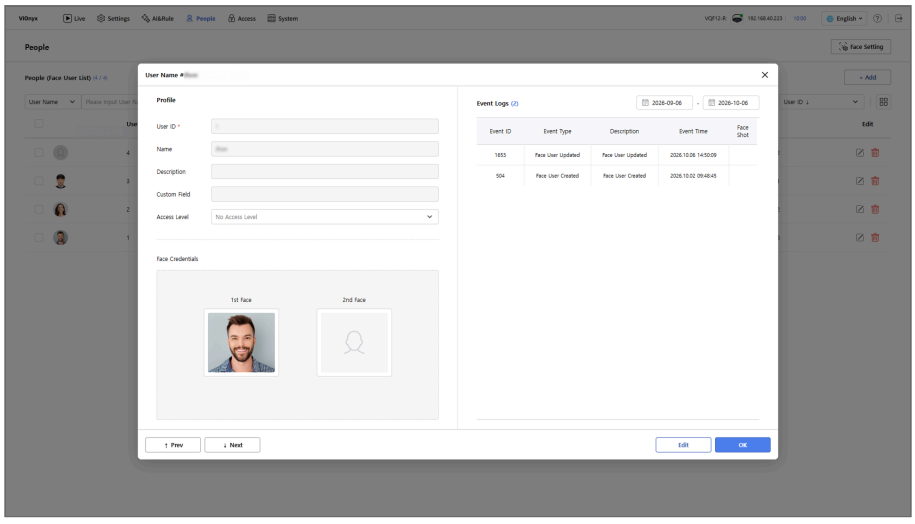
3. When the delete button appears at the top-right of the screen, click **Delete**.
4. When the deletion confirmation message appears, click **OK**.

A deletion confirmation message appears in the top-right and the user is removed from the user list.

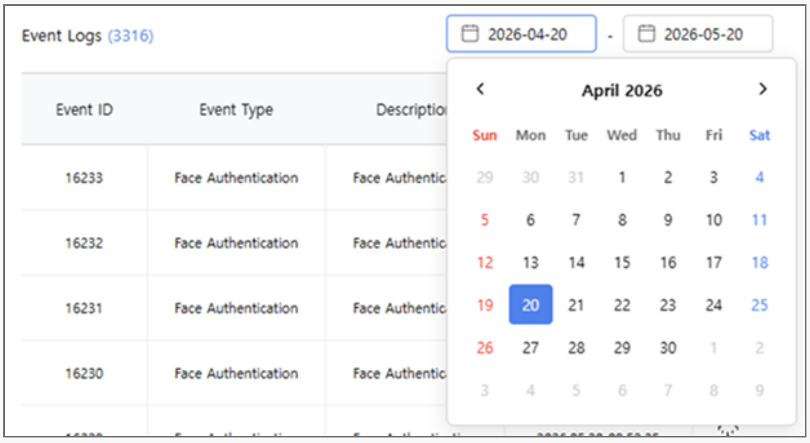
View user event logs

View registered users' activity history in the event log.

1. Click the **People** menu in the upper-left corner of the screen.
2. In the user list, click the user to view the event log.
3. When the user detail popup appears, view the event list on the right under **Event Logs**.



- Use the calendar icon in the top-right to view events for a specific date.



- Event logs are recorded automatically and track all important user activities.

User Search and View

Enter a name or ID in the user list to quickly find a user. Switch between table and card views to show user information as needed.

Use the user search and view feature in the following situations.

- When you must quickly find a specific user among many users
- When you need to view user profiles at a glance in card view
- When you want to sort the user list by name, ID, and last update time

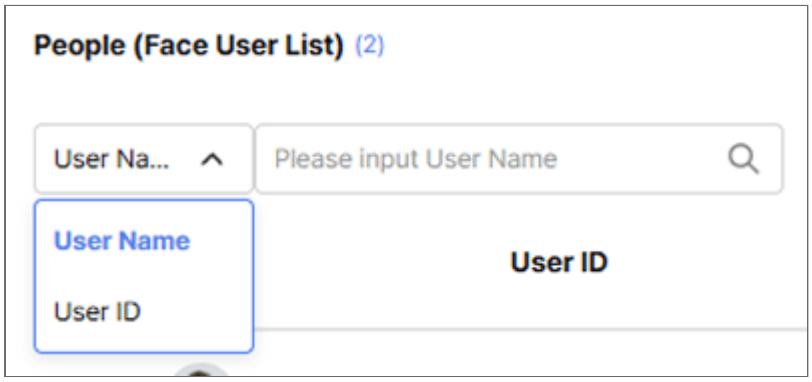
User search

Provides a search feature to find the user you need. Search by user name or ID, or find similar users by facial image.

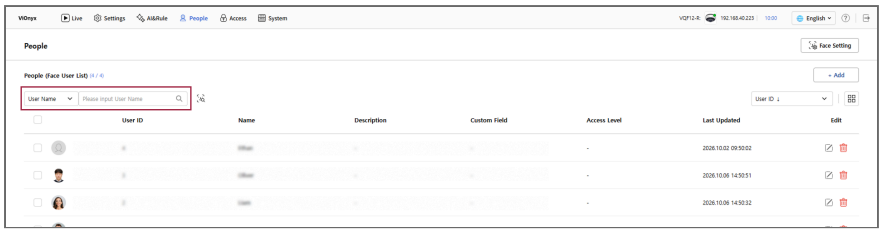
Keyword search

Enter a name or ID in the user list to search for the user you need.

1. Click the **People** menu in the upper-left corner of the screen.
2. Select the search criteria in the search field at the top left of the user list. Select **User Name** or **User ID**.



3. Enter a search term in the search field.



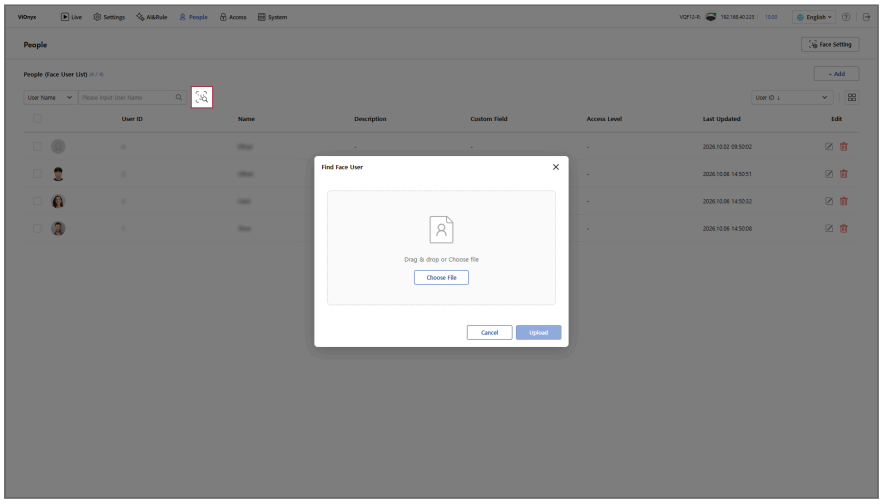
4. Users matching the entered search term appear in the list.

> **Info**
>
> - Supports partial search. For example, entering 'Kim' shows all users whose names include 'Kim'.
> - The currently selected filters determine the search results. Change filters to update the search results accordingly.

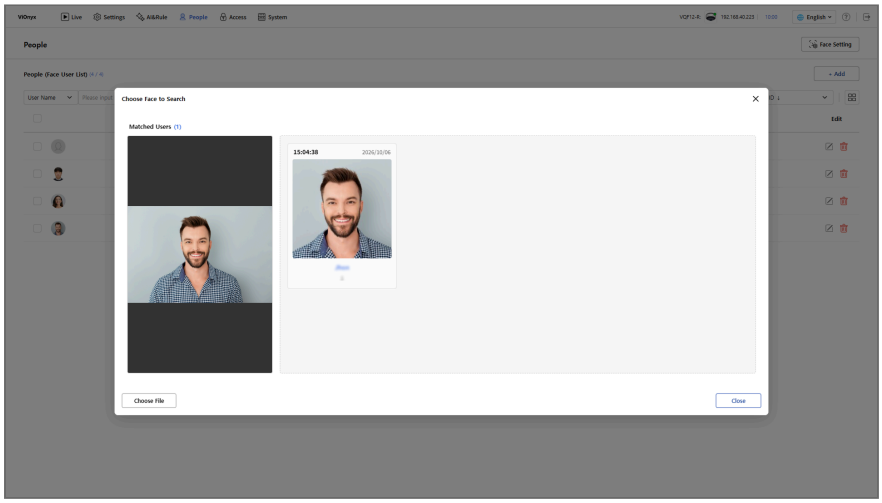
Find by facial image

Upload a facial image to search for users with a similar face.

1. Click the **People** menu in the upper-left corner of the screen.
2. Click to the right of the search field.
3. When the **Find Face User** window appears, drag and drop a facial image or upload it through **Choose File**.



4. After completing the facial image upload, click **Upload**.
5. When the **Choose Face to Search** window appears, a list of users matched to the uploaded facial image appears.



- Select the desired user from the matched users to go to that user's details page.
- To search again with a different facial image, click **Choose File** at the bottom left, and upload a new facial image.

> **Info**
>
> If you upload an image that is not a facial image, a message appears that says it is not a valid facial image. Try again with a facial image.

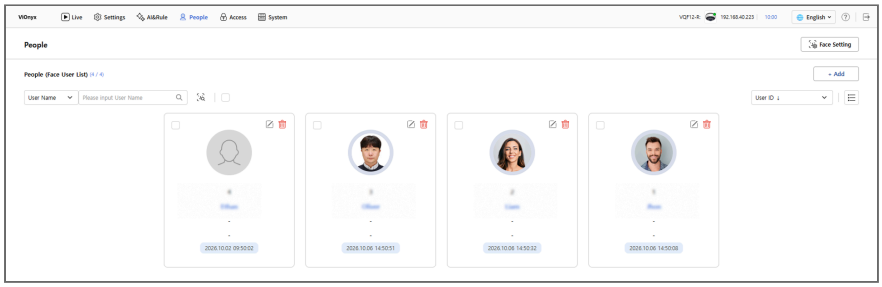
Change view mode

Display the user list in a table or card view. Click ☰ or ⊞ at the top right of the user list to select the view mode you want.

- **Switch to List View**



- **Switch to Grid View**

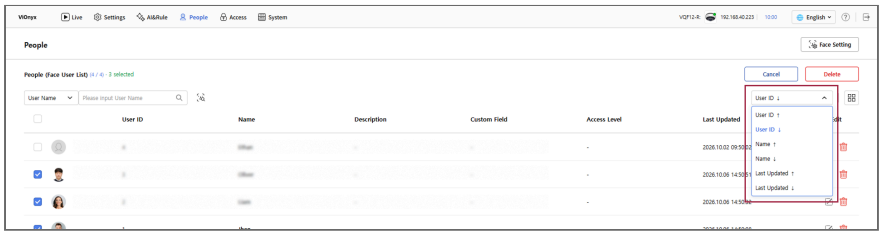


> **Info**
>
> **Switch to List View**, and **Switch to Grid View** both provide the same feature. Only the display differs; search, filter, and sort results are identical.

User list sorting

You can sort the user list in ascending or descending order by user name, user ID, and last update time.

1. Click the sort drop-down option at the top right of the user list.



2. Select the desired sort criteria.

Manage Access Control

In the **Access** menu, add doors connected to the camera. Set access levels to define who can access them and when. When an access control event determines access permission through facial authentication, the camera opens the relay connected to the door to grant access. Check the door status in real time, and open or lock it remotely. Set up voice prompts or webhook notifications based on the access decision. When setting up access control for the first time, create an access control event first, then configure doors, access levels, and door rules in order.

Info

- Support for the **Access** menu is included in firmware version 1.1.0 or later.
- The **Access** menu is in beta. Screen layout and behavior may change in later firmware updates.

Manage Doors

Add doors that the camera unlocks and locks. When adding a door, set the access control event, relay output, and door open time. Add a door before selecting it in access levels and door rules.

Register the door in the following cases.

- Automatically open the door for users authenticated with facial authentication
- Enable users to open the door from inside by pressing the exit button
- Check whether the door is open or closed using a sensor
- Operate the door by time period, such as unlocked during business hours and locked at night

Before you start

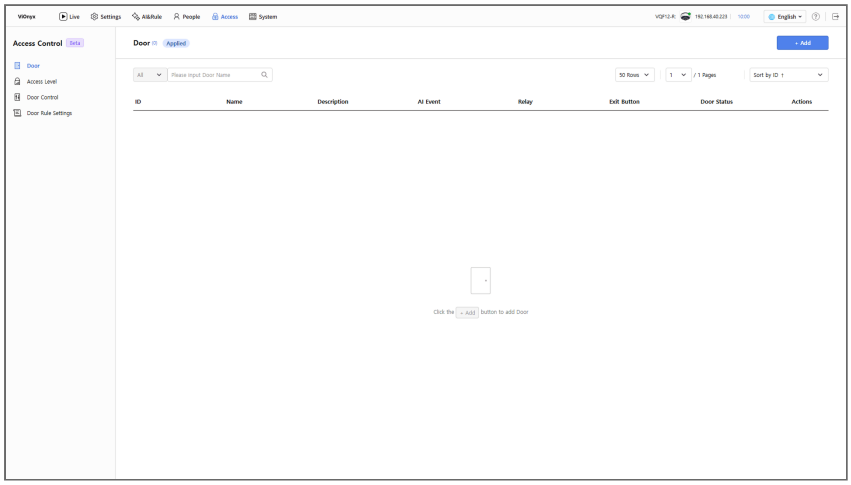
Check the following before adding a door.

- Each camera lets you register up to 10 doors. Check the number of doors the camera will control before setup.
- Create the access control event for access decisions first. For more information, see Set Up Access Control Events.
- Make sure the door lock connects to a relay port on the camera or sub I/O device. To use a sub I/O device, first add it via RS-485. For more information, see Set Up RS-485.
- To use an exit button or door status sensor, make sure the device connects to an input port.
- Create schedules in advance to use unlock and lock schedules. For more information, see Manage Schedules.

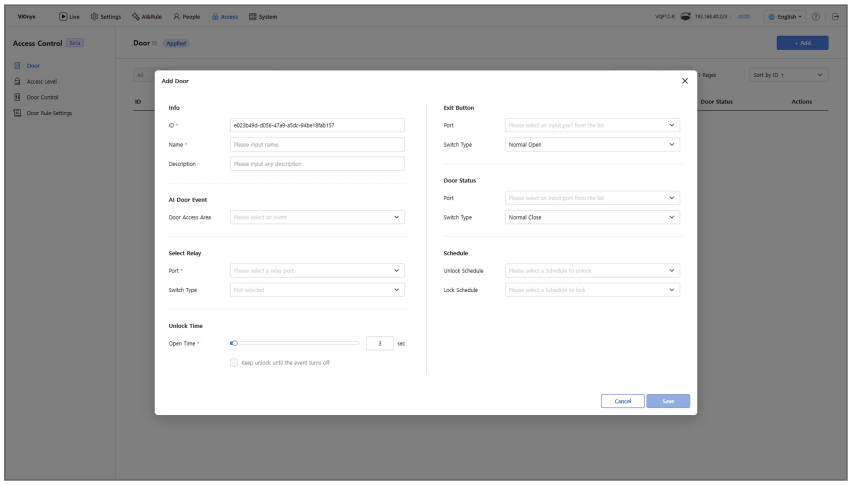
Add doors

1 Start adding doors

1. Click the **Access** menu in the upper-left corner of the screen.
2. Click **Door** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. When the **Add Door** popup appears, enter the door information. Enter all required fields to enable the **Save** button.



2 Enter basic information

In the **Info** section, enter information to identify the door.

- **ID**: The unique ID of the door. The system enters it automatically. Change it if needed. Do not use an ID already assigned to another door. Enter up to 64 characters. Use letters, numbers, hyphens(-), and underscores(_).
- **Name**: Enter the door name. Required. Do not use the same name as another door. Assign a location-based name, such as **Main Entrance** or **2nd Floor Office**, to distinguish doors in access levels and rules.
- **Description**: Enter a description for the door.

Info

- The door ID and name must be unique in the system. Do not use values already in use.
- Once saved, the door ID stays fixed.

3 Link access control events

In the **AI Door Event** section, select an access control area from the **Door Access Area** list to use for this door's access decision. The list shows access control areas set when creating access control events.

Info

- Link each access control area to one door only. Do not select an area already linked to another door.
- The AI Events page blocks deleting or changing the access control area linked to a door. To change the area, unlink it from the door first.
- See Set Up Access Control Events for more information on creating access control events.

4 Set relays

In the **Select Relay** section, set the relay that controls the door lock.

- **Port**: Select the relay port connected to the door lock. Required. Select a relay port on the camera or on a downstream I/O device. Do not select ports used by another door or AI rule.
- **Switch Type**: Select the lock contact type.
  - **Normal Open**: Normally open, and closes when the relay activates.
  - **Normal Close**: Normally closed, and opens when the relay activates.

Caution

- **Switch Type** applies to the relay port, not the door. Saving a door applies the setting to all doors and rules that use the port.
- Check the lock specifications, and select the correct **Switch Type**. An incorrect selection may keep the door unlocked during normal operation.

5 Unlock time setting

In the **Unlock Time** section, set how long to keep the door unlocked after access is granted.

- **Unlock Time**: Move the slider or enter a value in the input field. Set from 1 to 120 seconds. Default: 3 seconds.
- **Keep unlock until the event turns off**: Select this option to keep the door unlocked until the access control event

ends, regardless of unlock time. This option is available only when an access control area is selected.

> **Info**
>
> The access control event **Condition** setting determines when the event ends. For example, to lock the door immediately when someone tailgates, select **Keep until the area is clear or a tailgating violation occurs** in the access control event. For details, see Set Up Access Control Events.

6 Exit button settings (optional)

If an exit button is installed inside the door, set the input port connected to the button in the **Exit Button** section. The exit button opens the door without Facial Authentication.

- **Port**: Select the input port where the exit button is connected.
- **Switch Type**: Select the contact type for the exit button. The default is **Normal Open**.
  - **Normal Open**: Normally open, and closes when the relay activates.
  - **Normal Close**: Normally closed, and opens when the relay activates.

7 Door status settings (optional)

If a door position sensor is installed, set the input port connected to the sensor in the **Door Status** section. After setup, the **Door Control** screen shows whether the door is open or closed.

- **Port**: Select the input port where the door position sensor is connected.
- **Switch Type**: Select the sensor contact type. The default is **Normal Close**.
  - **Normal Open**: Normally open, and closes when the relay activates.
  - **Normal Close**: Normally closed, and opens when the relay activates.

> **Info**
>
> - Connect the exit button and door status sensor to different input ports.
> - Do not select an input port used by another door.

8 Schedule settings (optional)

In the **Schedule** section, set the door to stay unlocked or locked by time period.

- **Unlock Schedule**: Keep the door unlocked during the selected schedule. Use this to keep the lobby door unlocked during busy business hours.
- **Lock Schedule**: Keep the door locked during the selected schedule. During this time slot, enrolled users cannot access the door. However, people inside can exit by pressing the Exit button.

> **Info**
>
> Use different schedules for the open and lock schedules. The system cannot save them if the time zones overlap.

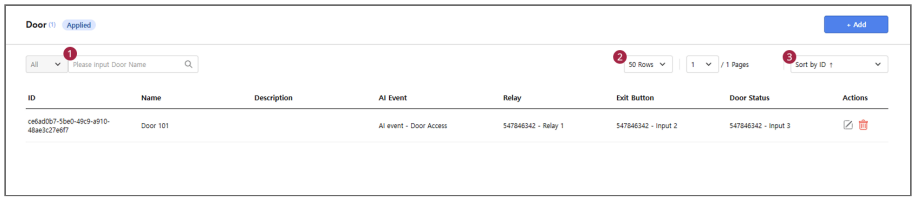
9 Save door

After completing all settings, click **Save**. Saved doors are added to the door list and are available in access levels and door rules.



Check door list

In the door list, check saved doors and the events and ports linked to each door.



- To find a specific door, enter the door name in the search field (1).
- Select a value in the Rows per page list (2) in the upper-right corner. This changes the number of doors per page.
- To change the sort criterion, select one in **Sort by ID**(3).

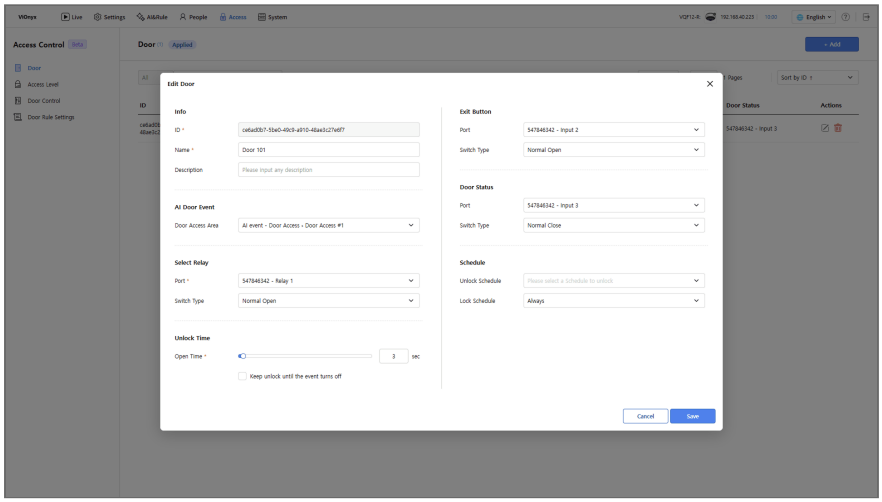
The following items are shown in the door list.

Item	Description
ID	The door's unique ID.
Name	The name of the door.
Description	The description entered when adding or editing the door.
AI Event	The access control area linked to the door.
Relay	Relay port that controls the door lock.
Exit Button	Input port connected to the exit button.

Item	Description
Door Status	Input port connected to the door open/close sensor.
Actions	Edit ( ) or delete ( ) the door.

Edit doors

1. In the door list, click the button at the far right of the door to edit.
2. When the **Edit Door** pop-up appears, edit the fields.



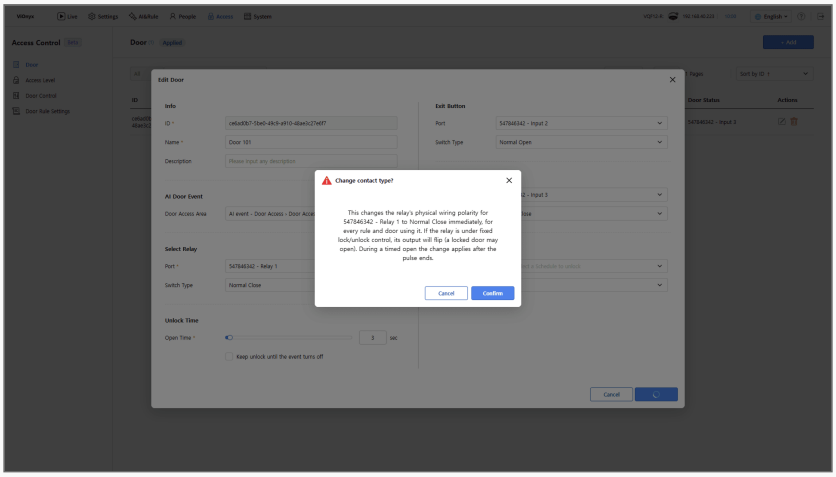
3. Click **Save** to save the changes.

Saving changes applies them immediately to access levels and door rules that use the door.

> **Caution**
>
> If the door is manually locked or unlocked, changing the relay **Switch Type** may invert the output and open a locked door. Manually control it in the **Door Control** menu before changing it.

Info

Change the relay **Switch Type** and click the **Save** button. A confirmation message appears.



- Click **OK** to close the confirmation message and apply the new contact type to the relay port immediately. It also applies to all doors and rules that use the port.
- Click **Cancel** to keep the contact type and save only the other changes.
- Changing it while the door is held open applies after the open time ends.

Delete door

1. In the door list, click  at the far right of the door to delete.
2. If a confirmation message appears, review it and click **OK**.

Deleting the door unlinks it from connected access control events and access levels. The deleted door also disappears from the **Door Control** list and cannot be restored.

Info

- Deleting a door used in an access level or door rule also deletes the related access level and door rule.
- To add, edit, or delete doors, you need **Read Write** permission. If you do not have permission, contact your administrator. For more information on operator roles, see Manage Operators.

Next step

After adding doors, create an access level to set when certain users can enter.

Manage Access Levels

An access level defines **which users** can access **which doors**, and **when**. In access control events, users identified by Facial Authentication cannot enter unless they are assigned to the door's access level and within the access time.

Create an access level in the following situations.

- When you want only certain departments or team members to have access to a door
- When you want to set different access times for each user group, such as allowing access only during weekday business hours
- When you want to grant separate permissions to users who access only during certain time periods, such as night shift workers

Before you start

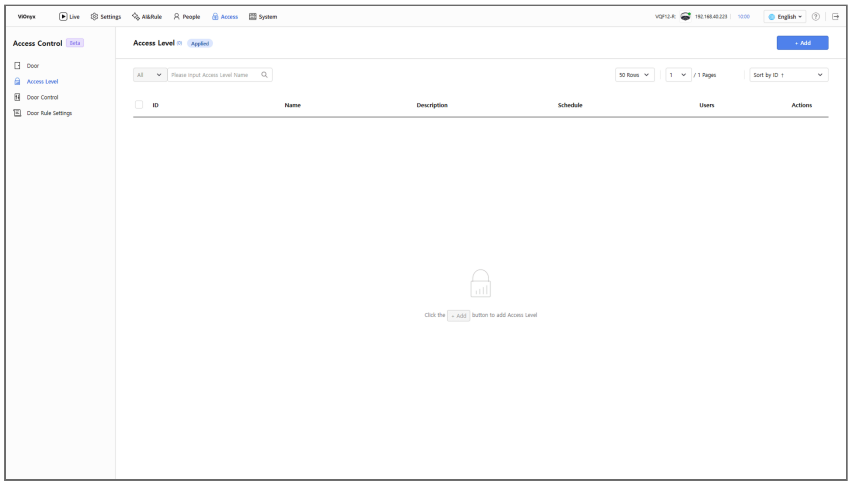
Before creating an access level, check the following.

- Add doors before assigning them to an access level. For more information, see Manage Doors.
- Register users with facial credentials before assigning them to the access level. For more information, see Add Users.
- Create schedules in advance to restrict access times. If no schedule exists, use the default Always schedule. For more information, see Manage Schedules.

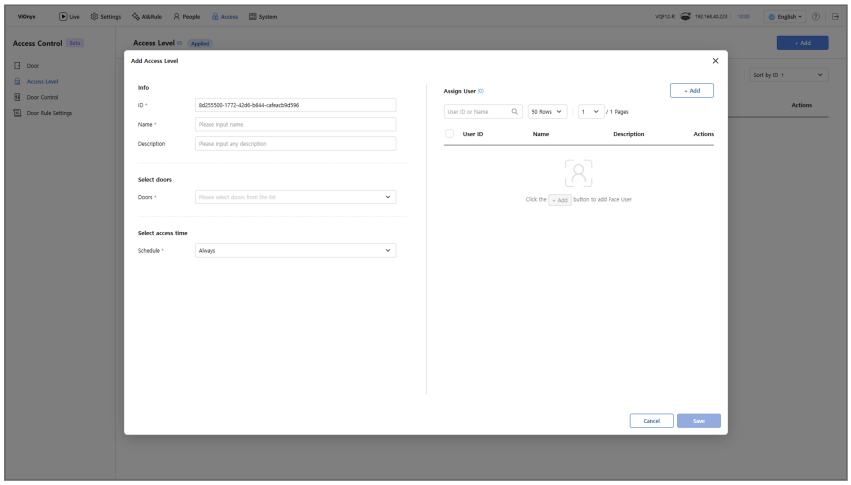
Add an access level

1 Start adding an access level

1. Click the **Access** menu in the upper-left corner of the screen.
2. Click **Access Level** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. When the **Add Access Level** pop-up appears, enter the access level information, then assign users.



2 Enter basic information

In the **Info** section, enter information to identify the access level.

- **ID**: The unique ID of the access level. The system enters it automatically. Change it if needed. Do not use an ID that matches another access level. Enter up to 64 characters. Use letters, numbers, hyphens(`-`), and underscores(`_`).
- **Name**: Enter the access level name. This field is required. Do not use a name that matches another access level. Use a name that indicates who and when, such as **Development team—always access** or **Night shift workers**.
- **Description**: Enter a description for the access level.

3 Select doors

In the **Select doors** section, select the doors to allow access from the **Door** list. Required. More than one door can be selected.

> **Info**
>
> Add at least one door before selecting a door from the list. First, add a door in **Access** → **Door**. For more information on registering doors, see Manage Doors.

4 Select access time

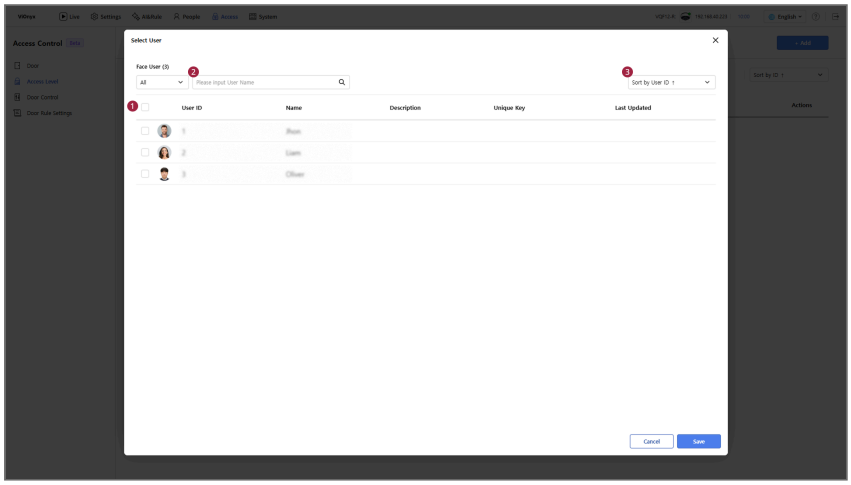
In the **Select access time** section, select a schedule to allow access from the **Schedule** list. This field is required. The default is **Always**. The system allows access only during the selected schedule. It denies access at other times, including for registered users.

> **Info**
>
> For more information on schedule management, see Manage Schedules.

5 Assign users

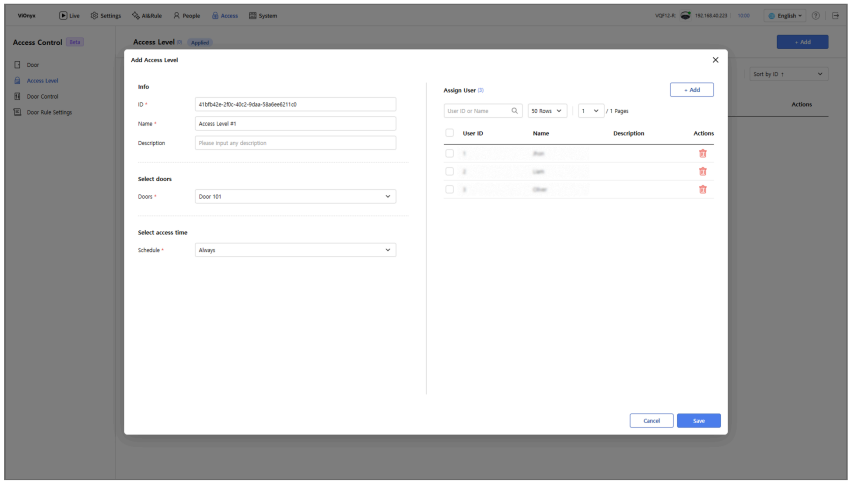
In the **Assign User** section, add users to apply the access level.

1. Click **+ Add** in the upper right corner of the **Assign User** section.
2. When the **Select User** pop-up appears, click the checkbox for each user to assign.



- Select the checkbox (1) in the list header to select all users.
- Enter a user name in the search field (2) to find a specific user.
- Select a criterion in the sort list (3) to change the sort order.

3. Click **Save**. The system adds the selected users to the **Assign User** list.



To remove an assigned user from the access level, in the **Assign User** list, click the button for that user.

Info

- The **Select User** list shows only users registered with facial credentials.
- A user can be assigned to multiple access levels. Each user can be assigned to a limited number of access levels.

6 Save access level

After completing all settings, click **Save**. The system adds the saved access level to the access level list. It applies it immediately to assigned users.



Check the access level list

The access level list shows access levels, access times for each level, and assigned users.



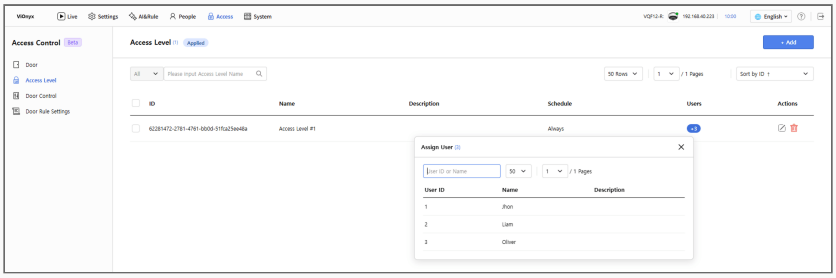
- Enter the access level name in the search field (1) to find a specific access level.
- Select a value from the Rows list (2) at the top right of the screen to change the number of access levels shown per page.
- To change the sort criterion, select one in **Sort by ID**(3).

The following information appears in the access level list.

Item	Description
ID	The unique ID of the access level.
Name	The name of the access level.
Description	The description entered when adding or editing the access level.
Schedule	The schedule that allows access.
User	The number of users assigned to the access level.
Actions	Edit ( ) or delete ( ) access levels.

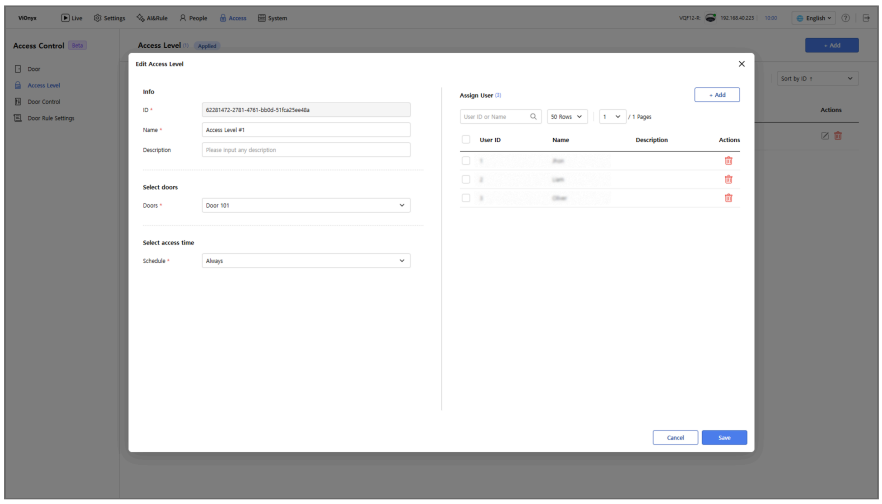
Info

Click the number in **User** to view the assigned user list.



Edit access level

1. In the access level list, click the button to the right of the access level.
2. When the **Edit Access Level** popup appears, edit the doors, access time, and assigned users.



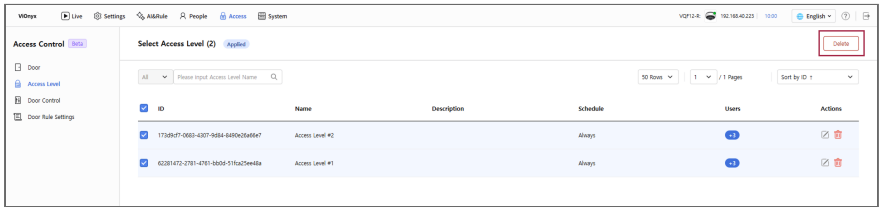
3. Click **Save** to save the changes.

Saving changes applies them immediately to all assigned users.

Delete access level

Delete access levels one at a time, or select multiple access levels to delete at once.

- **Delete one**: In the access level list, click at the far right of the access level to delete.
- **Delete multiple**: In the access level list, select the checkboxes for the access levels to delete, and click **Delete** at the top right of the screen.



If a confirmation message appears, review it and click **OK**. Deleting an access level removes it from all assigned users. Doors and users are not deleted. Deleted access levels cannot be recovered.

> **Caution**
>
> Deleting an access level prevents users assigned only to that level from accessing doors. Check assigned users before deleting.

Next step

Set door rules to execute additional actions, such as voice prompts, webhook notifications, and emergency lights, based on access decisions.

Control Doors

In the **Door Control** menu, check the lock status of registered doors in real time and open or lock doors remotely.

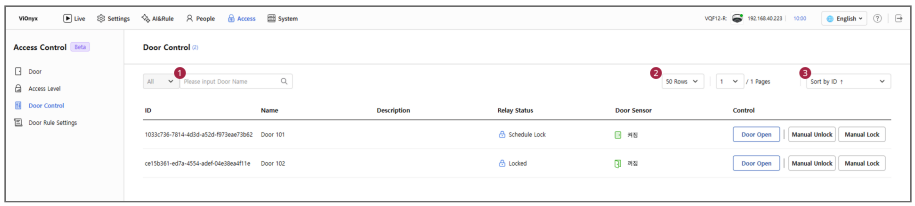
Directly control the door in the following situations.

- Open the door once for visitors or delivery drivers without enrolled facial credentials
- Keep the door open for events or moving day
- Lock the door immediately in an emergency, regardless of the schedule

> **Info**
>
> - An operator account is required to control doors. Without operator permission, the system disables door status checks and door control. For more information on operator roles, see Manage Operators.
> - For more information on adding and managing doors, see Manage Doors.

Check door status

1. Click the **Access** menu in the upper-left corner of the screen.
2. Click **Door Control** on the left sidebar.



The list shows the doors registered in the **Door** menu. When a door is added or deleted, the list updates immediately.

- To find a specific door, enter the door name in the search field (1).

- Select a value in the Rows per page list (2) in the upper-right corner. This changes the number of doors per page.
- To change the sort criterion, select one in **Sort by ID**(3).

The following items are shown in the door list.

Item	Description
ID	The door's unique ID.
Name	The name of the door.
Description	The description entered when adding or editing the door.
Relay Status	The current status of the door lock.
Door Sensor	The current status of the door sensor. This column appears only when you set the **Door Status** input port for the door.
Control	This feature opens the door and manually locks or unlocks it.

Relay status

The **Relay Status** column shows whether the entrance door is locked and what determines that status.

Status	Description
Locked	The entrance door remains locked by default.
Unlocked	The entrance door remains unlocked by default.
Schedule Lock	The entrance door locks according to the lock schedule.
Schedule Unlock	The entrance door unlocks according to the unlock schedule.
Fixed Lock	Locked using **Manual Lock**.
Fixed Unlock	Unlocked using **Manual Unlock**.

Control doors

Click the button in the **Control** column to control the entrance door.

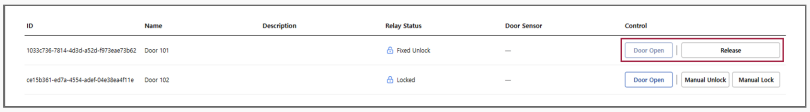
Button	Trigger and Action
Door Open	Open the entrance door once. The entrance door locks again after the configured open time elapses.
Manual Unlock	Unlock the entrance door and keep it open until you execute the **Release** feature.
Manual Lock	Lock the entrance door and keep it locked until you execute the **Release** feature. During this period, registered users cannot enter, and the Exit button cannot open the door.
Release	End **Manual Lock** or **Manual Unlock** and return the entrance door to its previous state.

Caution

- In the **Manual Unlock** state, anyone can access regardless of facial authentication. After completing required tasks, click the **Release** button.
- In **Manual Lock** mode, people inside cannot exit using the Exit button. Before executing **Manual Lock**, confirm that no one remains inside.

Info

- Manual Lock or Manual Unlock disables the **Door Open** button and shows only the **Release** button.



- Manual control takes precedence over the unlock schedule and lock schedule. For example, executing **Manual Lock** during an unlock schedule keeps the entrance door locked.
- Click **Release** to return to the schedule for the current time or the default state.

Set Door Rules

Door rules automatically play audio, send webhooks, or execute relay actions based on access decisions at the door. When access is granted, the door opens automatically based on door settings, so set additional actions in door rules.

Set door rules in the following situations.

- When a welcome message plays on access granted and an instruction message plays on access denied
- When an unauthorized person follows someone in and a beacon light or alarm should activate
- When access logs should be sent to an external access control system or monitoring server

Before you start

Before setting door rules, check the following.

- Add doors before applying rules. For more information, see Manage Doors.
- Upload audio clips before using audio playback. For more information, refer to Upload Audio Clips.
- Prepare the webhook receiver URL before using webhooks.
- Connect beacon lights and alarms to the relay port to use relays. For more information on connecting external devices, see the ViOnyx Installation Guide.

Access decision results

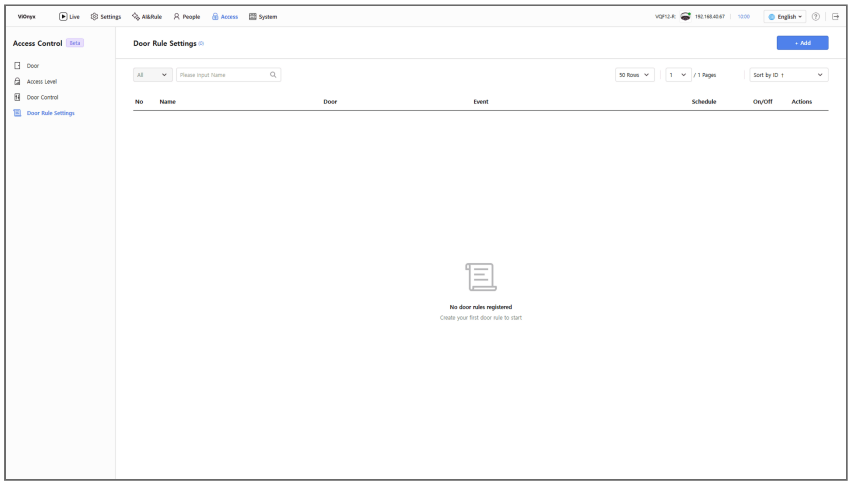
In door rules, set the actions to execute for each access decision result.

Access decision results	Trigger condition
Access Granted	The system identified a user with an access level during access hours and granted access.
Access Denied by Unidentified	Facial Authentication did not authenticate the person, or the person is not registered.
Access Denied by Access Level	The system identified a registered user, but the user lacks the door access level or is outside access hours.
Access Denied by Door Mode (Manual/Schedule Lock)	The system denied access because the door is manually locked or locked by schedule.
Access Denied by Anti-Tailgating	The system denied access because the verification zone did not meet the tailgating condition.
Authenticated Passage (Door Line)	A user granted access crossed the event entry line and entered.
Passage After Denial (Security Event)	A person denied access crossed the event entry line and entered. This security event indicates suspected forced entry.

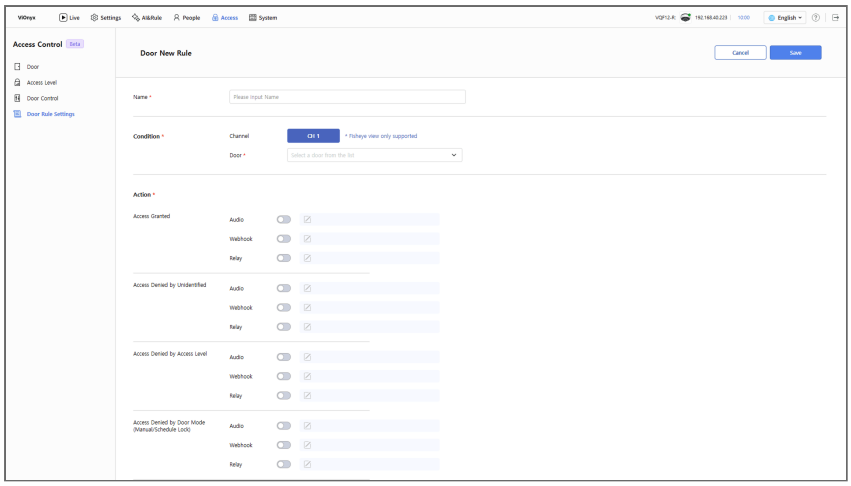
Add a door rule

1 Start creating a rule

1. Click the **Access** menu in the upper-left corner of the screen.
2. Click the **Door Rule Settings** on the left sidebar.



3. Click **+ Add** at the top right of the screen.
4. When the **Add Door Rule** screen appears, enter the rule name and set conditions and actions.



2 Enter rule name

Enter the rule name in the **Name** input field. Required.

3 Set conditions

In the **Condition** section, select the doors to apply the rule to.

- **Channel**: The channel is fixed to CH 1. Support for fisheye view only.
- **Door**: Select the door to apply the rule to. Required.

4 Set actions

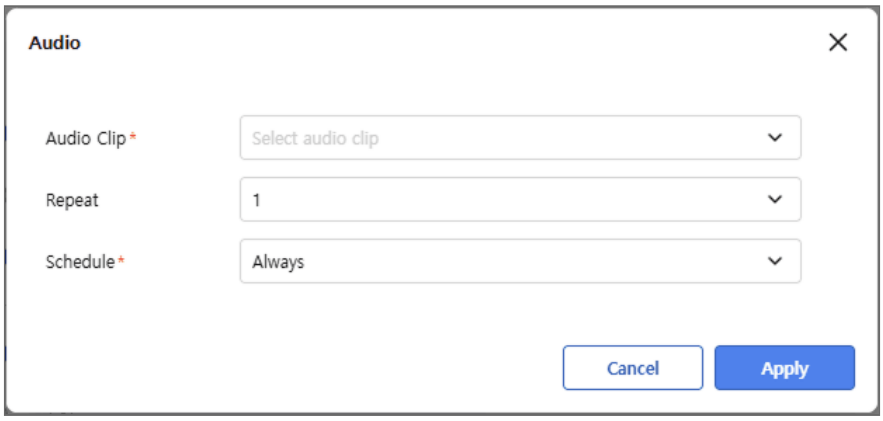
The **Action** section shows **Audio**, **Webhook**, and **Relay** actions for each access decision result. For the access decision result that triggers the action, enable the action toggle, then click . The action settings pop-up appears.

You must enable at least 1 action to save the rule. See below for action-specific settings.

> **Info**
>
> Outside the action schedule, the action does not execute if an access decision result occurs. Manage schedules in **AI&Rule** → **Schedule**. For more information, see Manage Schedules.

5 Audio action settings

When an access decision result occurs, the camera plays an audio clip.



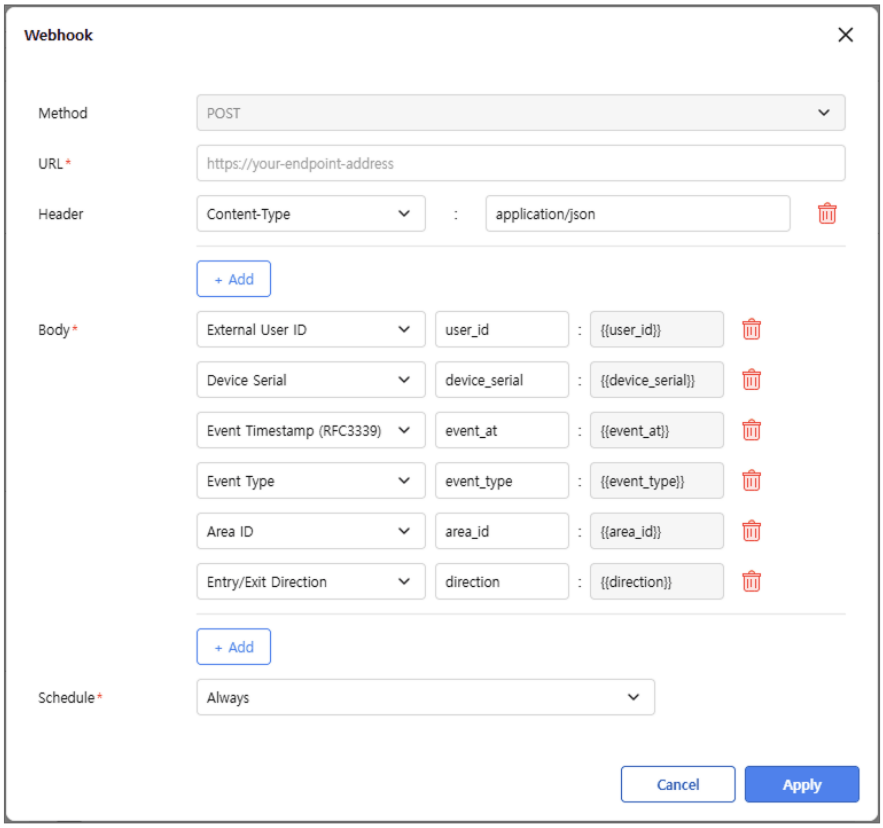
- **Audio Clip**: Select the audio clip to play. Required.
- **Repeat**: Select the number of times to repeat audio playback.
- **Schedule**: Select the schedule for audio playback. Required. The default is **Always**.

Click **Apply** to save the audio action settings.

> **Info**
>
> Prepare audio clips before configuring audio actions. Upload audio clips in **System** → **Audio**. For more information, refer to Upload Audio Clips.

6 Webhook action settings

When an access decision result occurs, the system sends a webhook to an external server.



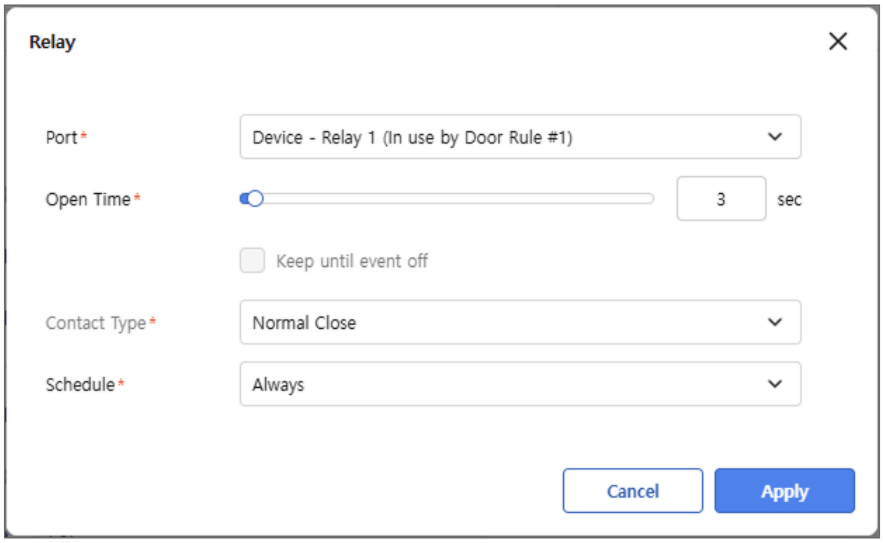
- **Method**: The webhook transmission method. Only the `POST` method is supported.
- **URL**: Enter the URL to receive the webhook. Required.
- **Header**: Set the HTTP headers to include in the webhook. The system adds the `Content-Type: application/json` header by default. Click **+ Add** to add headers. Do not use duplicate header names. Do not use system-reserved header names.
- **Body**: Select the fields to include in the webhook body. Required. In each row, select the data to send on the left, and enter the JSON key in the center field. The right field shows variables that change to actual values when an event occurs. Click **+ Add** to add a custom field, or click to delete it. The maximum body size is 64KB.
- **Schedule**: Select a schedule for sending webhooks. Required. The default is **Always**.

To save the settings, click **Apply**.

> **Info**
>
> - For security, values entered in the header and body do not appear again after saving. When editing a rule, saved values remain. New entries replace existing values.
> - Check webhook delivery results in the system log. For details, see View System Logs.

7 Relay action settings

When an access decision occurs, the system activates the selected relay. Use this to integrate a beacon, a siren, or an auxiliary lock.



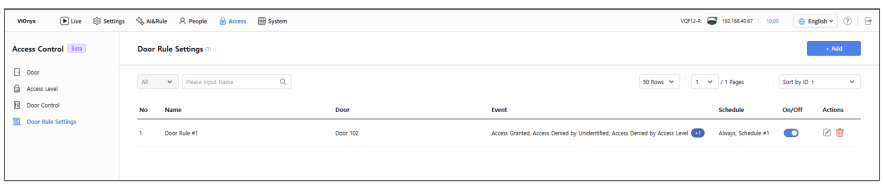
- **Port**: Select the relay port to activate. Required. Relay ports used for door locks cannot be selected.
- **Open Time**: Set how long to keep the relay active. Move the slider or enter a value in the input field. Set from 1 to 120 seconds. Default: 3 seconds.
  - **Keep until event off**: Select this option to keep the relay active until the access control event ends, regardless of open time.
- **Contact Type**: Select the relay contact type. Required. Set this after selecting a port.
  - **Normal Open**: Normally open, and closes when the relay activates.
  - **Normal Close**: Normally closed, and opens when the relay activates.
- **Schedule**: Select a schedule to trigger the relay. Required. The default is **Always**.

To save the settings, click **Apply**.

> **Caution**
>
> **Contact Type** is a setting applied to the relay port, not a rule. Changing **Contact Type** shows a confirmation message. Click **OK** to apply it immediately to all rules and doors that use the port. Changing this while the port is manually locked or unlocked inverts the output. A locked door may open.

8 Save rule

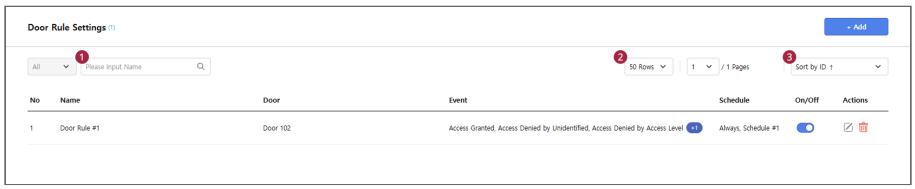
After completing all settings, click **Save** in the upper-right. The system adds saved rules to the door rule list and applies them immediately.



> **Info**
> Create up to 20 door rules.

View the door rule list

The door rule list shows saved rules and each rule's target.



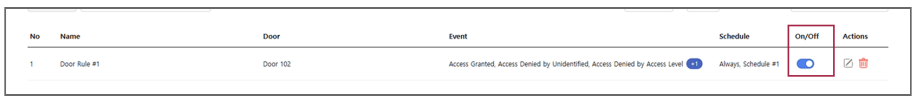
- Enter the door rule name in the search field (1) to find a specific rule.
- Select a value in Rows (2) to change the number of rules per page.
- To change the sort criterion, select one in **Sort by ID**(3).

The following items are displayed in the door rule list.

Item	Description
No	The rule number.
Name	The rule name.
Door	The door the rule applies to.
Event	The access decision result with one or more enabled actions. If multiple results exist, the list shows only part of them.
Schedule	The schedule applied to the rule.
On/Off	Turns the rule on or off.
Actions	Provides controls to edit ( ) or delete ( ) the rule.

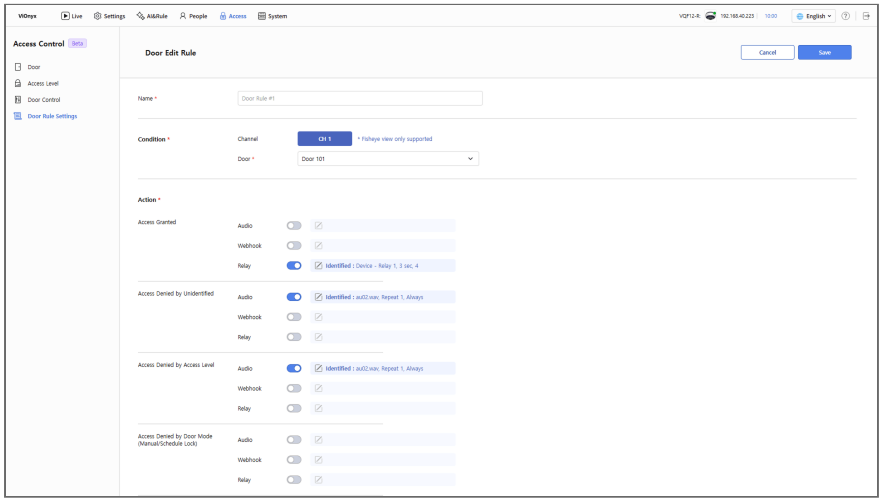
Enable/disable door rules

In the door rule list, click the toggle in the **On/Off** column to enable or disable the rule. Disabled rules do not execute actions when an access decision result occurs. Use this to pause a rule without deleting it.



Edit door rule

1. In the door rule list, click the button at the far right of the rule to edit.
2. When the **Edit Door Rule** screen appears, edit the conditions and actions.



3. To save your changes, click **Save** in the upper right of the screen.

Delete door rule

In the door rule list, click the button at the far right of the rule to delete. When the confirmation message appears, click **OK**. Deleted rules cannot be recovered.

Configure System

Systematically manage device information, firmware, maintenance, accounts, audio, and logs to effectively operate the camera system. Regularly check and update device information, firmware, maintenance, accounts, audio, and logs to ensure stable and secure camera operation.

Update Camera Information

Check basic camera information and enter the device name, description, and location to manage multiple cameras in your organization.

Update camera information in the following situations:

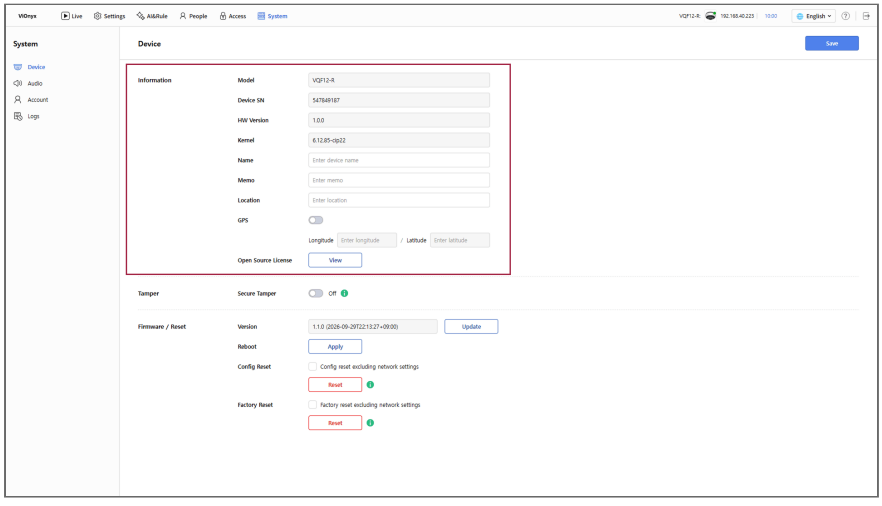
- Rename an installed camera to a distinctive name within your organization.
- Add additional information about the camera's location or installation site.
- Record the camera's precise location by entering GPS coordinates.
- Add specific notes or descriptions for each camera when managing multiple cameras.

> **Info**
>
> - Fields such as model name, serial number, and hardware version are read-only and cannot be edited.
> - Camera name, memo, and location support Unicode and accept Korean, English, numbers, and special characters.

Check basic camera information

Check basic information such as the camera model, serial number, and hardware version.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.



You can check the basic information below in the **Information** section. These fields are read-only and cannot be edited.

- **Model**: Camera model
- **Device SN**: Camera serial number
- **HW Version**: Hardware version
- **Kernel**: Kernel version
- **Open Source License**: Click **View** to view open source license information.

Set camera information

Enter the camera name, memo, and location to manage cameras effectively.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.

Enter name

Enter a custom name to make the camera easy to identify. Enter the camera name in the **Name** input field.

- Up to 64 characters.
- Allows Korean, English, numbers, and special characters (`.`, `-`, `(`, `)`).

> *Example: "Entrance 1", "Conference Room A"*

> **Info**
> The entered camera name appears in the system menu and throughout the web UI, making it easy to identify the camera.

Add memo

Enter additional information or a memo for the camera. Enter a memo or description in the **Memo** input field. Up to 64 characters.

> *Example: installation department, administrator name, installation date*

Enter location information

Enter the camera's installation location as text. Enter the camera's installation location in the **Location** input field. Up to 64 characters.

> *Example: "1st floor lobby entrance", "2nd floor conference room waiting area"*

Save settings

After entering all information, click **Save** in the upper right corner of the screen.

Set GPS coordinates

Enter the camera's exact geographic location as GPS coordinates.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. To enable GPS setting, click the **GPS** toggle in the **Information** section.



4. Enter the longitude and latitude information.

> *Example: Seoul (37.5665, 126.9780)*

5. Click **Save** in the upper right corner of the screen to save the setting.

> **Info**
>
> - Enter GPS coordinates in decimal degrees (DD) format.
> - To disable GPS setting, click the **GPS** toggle again.

Upgrade Firmware

This feature updates the camera firmware to the latest version. Firmware updates apply new features, performance improvements, and security patches.

Update the firmware in the following situations.

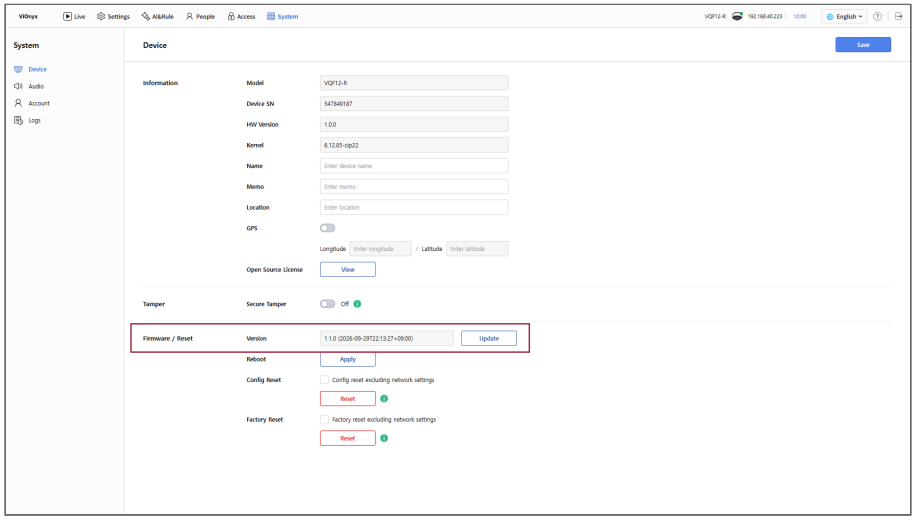
- To use new features
- To apply security patches to protect the camera
- To improve the camera's performance
- When technical support recommends a specific firmware version

> **Info**
>
> - The camera restarts during a firmware update and is unavailable during that time.
> - Ensure the device has sufficient power before starting the firmware update.
> - Use only official firmware files (.bin) provided by Suprema technical support.

Check current firmware version

Check the camera's installed firmware version.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.

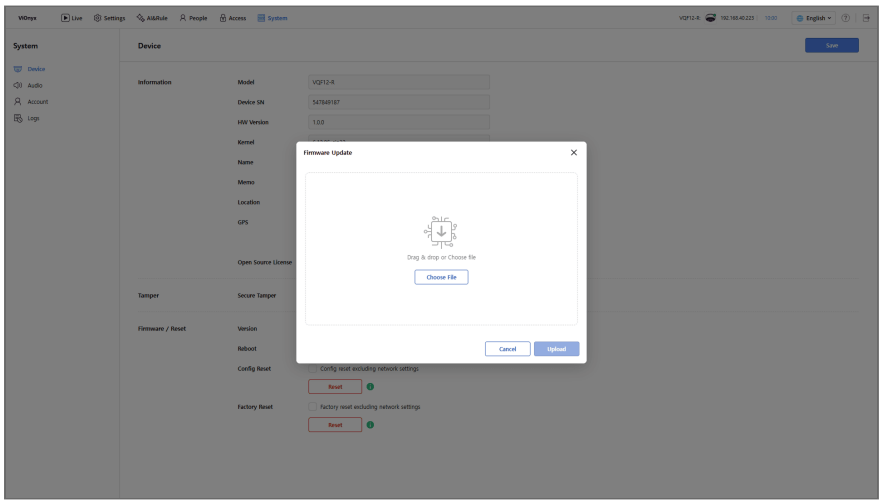


In the **Firmware / Reset** section, check the currently installed firmware version in **Version**.

Upgrade firmware

Select the new firmware file to update the device.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. In the **Firmware / Reset** section, click **Update**.
4. When the **Firmware Update** popup appears, select the firmware file (.bin) provided by Suprema.



   - The file extension must be .bin.
   - Drag the file into the upload area or click **Choose File** to select the file.
5. After selecting a file, **Upload** becomes active.
6. Click **Upload** to start the firmware update.
7. After the upload completes, a reboot confirmation popup appears. Click **OK** to restart the camera and complete the

firmware update.

- Reconnect to the web UI after the camera reboots. To verify the new firmware version, go to **Device**.
- You cannot cancel the firmware update once it has started. Wait until the update completes.

Maintain the Camera

Manage the camera effectively by rebooting it or initializing settings. Covers three methods: reboot, config reset, and factory reset.

Use the camera maintenance feature in the following situations.

- When an external person who is not an administrator tries to remove the camera cover, and you want to apply security measures so the camera stops operating normally.
- After changing network settings, to apply the new settings.
- When the camera responds slowly or its performance degrades.
- When the system is not operating normally.
- When you need to restore all camera settings to defaults.
- Before handing the camera to another user, to remove all information.
- When a system problem requires restoring factory defaults.

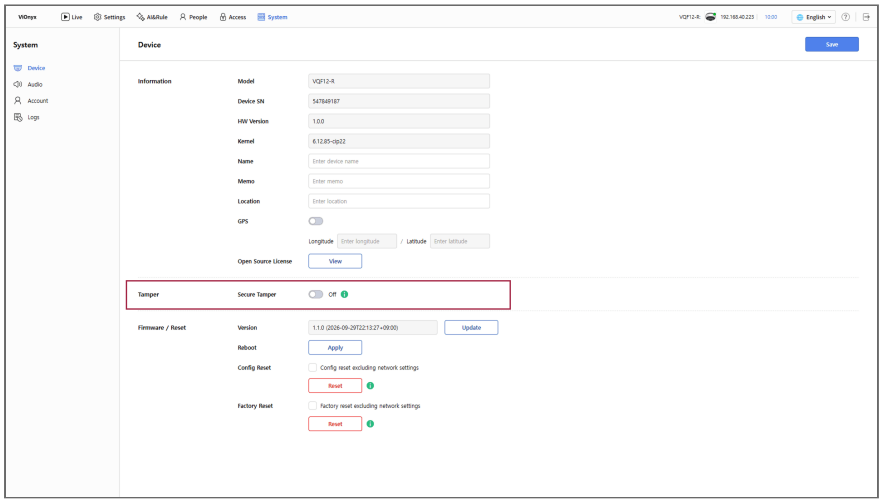
Warning

- Do not power off the camera during reboot or initialization.
- **Factory reset** permanently deletes all user data, event records, and logs. This action is irreversible; proceed with extreme caution.
- Back up necessary data before initializing.

Tamper

Enable the camera's **Tamper** feature to delete the camera's certificates and keys when an external person who is not an administrator tries to remove the camera cover, preventing the camera from operating normally.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. Click the toggle in the **Tamper** section to enable the feature.



4. When the warning message appears, click **OK**.

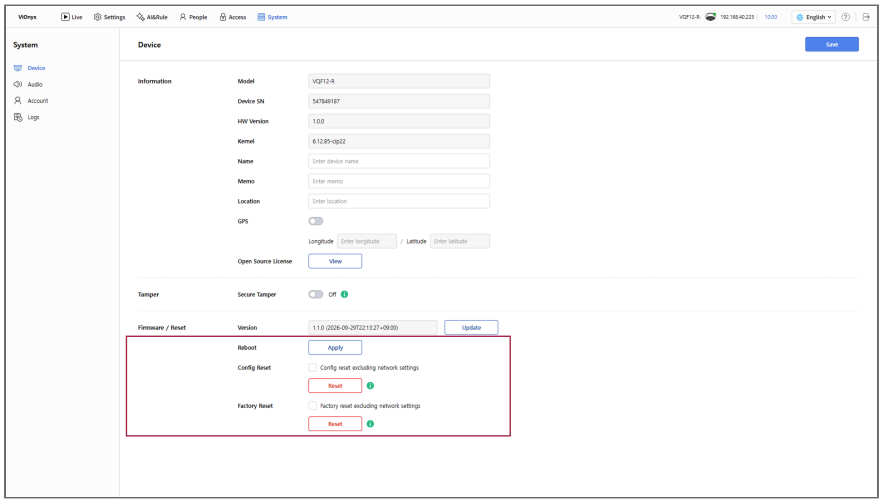
This feature saves changes automatically without clicking **Save**.

> **Caution**
>
> When the **Tamper** feature is enabled and the administrator must remove the camera cover for maintenance, temporarily disable the **Tamper** feature before proceeding. Enable it again after the task is complete to keep security in place.

Reboot the camera

Restart the camera to apply setting changes or restore system performance. Reboot reinitializes the system while keeping current settings.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. In the **Firmware / Reset** section, under **Reboot**, click **Apply**.



4. When the reboot confirmation popup appears, click **OK**.

Info

- While rebooting, the camera is temporarily unavailable. Reboot takes at least 1-2 minutes.
- Do not power off the camera during reboot. System damage may occur.
- If the camera's IP address changes after reboot, connect using the new IP address.
- When reboot starts, the web UI connection disconnects automatically. This is normal behavior.

Reset

Initialize the camera's settings or fully restore it to factory defaults. Two initialization methods are available; they delete different data, so choose carefully.

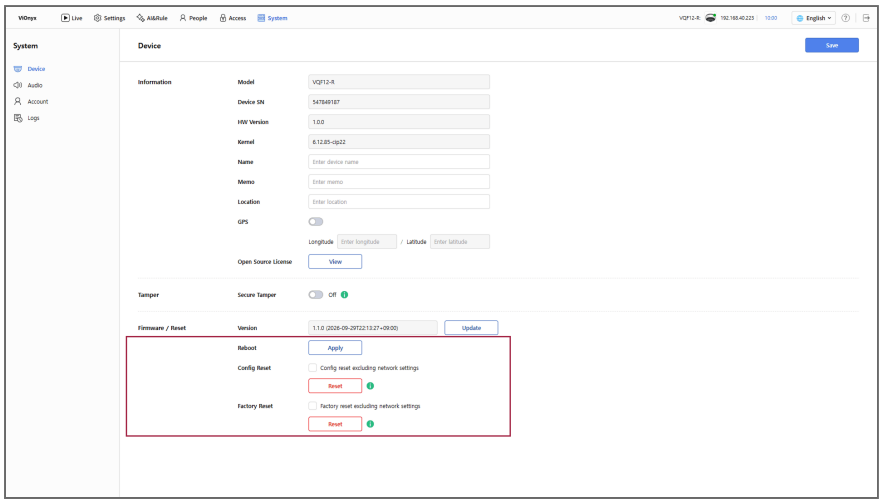
Initialization method comparison

Method	Description	Data deleted	Data retained
Config Reset	Initialize settings only	Camera settings, network settings (optional), video profiles, rules, accounts	User information, face data, events/logs
Factory Reset	Delete all data and restore factory defaults	All settings, user information, events, logs, accounts	-

Config Reset

Initialize only settings; retain user information and log data.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. In the **Firmware / Reset** section, under **Config Reset**, click **Reset**.



To exclude network settings from the initialization, click the checkbox for the **Config reset excluding network settings** option.

4. When the settings reset confirmation popup appears, click **OK**.

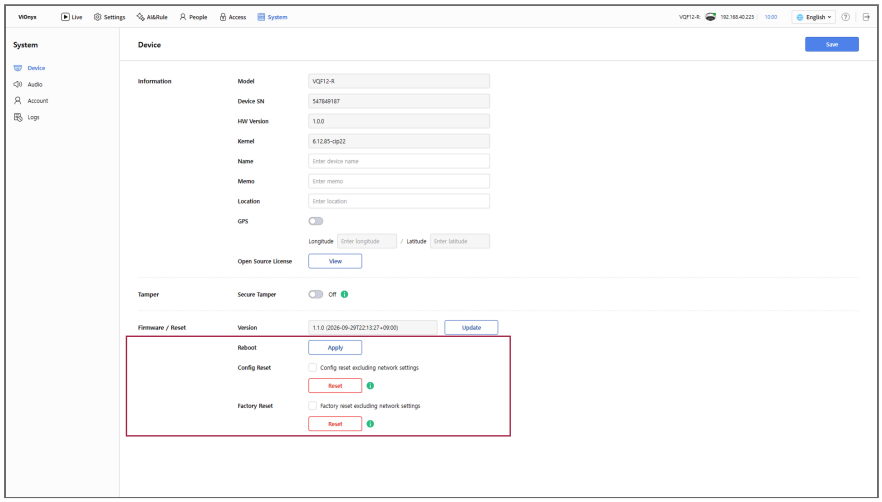
The settings reset proceeds, and the camera restarts automatically.

Factory Reset

Fully initialize the camera to restore it to factory defaults. This action cannot be undone.

> **Warning**
> Factory reset completely deletes all data. This action is irreversible; proceed with extreme caution.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Device** on the left sidebar.
3. In the **Firmware / Reset** section, under **Factory Reset**, click **Reset**.



To exclude network settings from the initialization, click the checkbox for the **Config reset excluding network settings** option.

4. When the factory reset confirmation popup appears, click **OK**.
5. When the final confirmation popup appears, enter the administrator password.
6. Click **OK**.

> **Info**
>
> - After factory reset completes, the following items are restored to their defaults.
>   - Admin ID: **admin**
>   - Network settings: DHCP
>   - All user data, events, and logs: deleted
> - After factory reset, set a new default password when accessing the web UI.

Upload Audio Clips

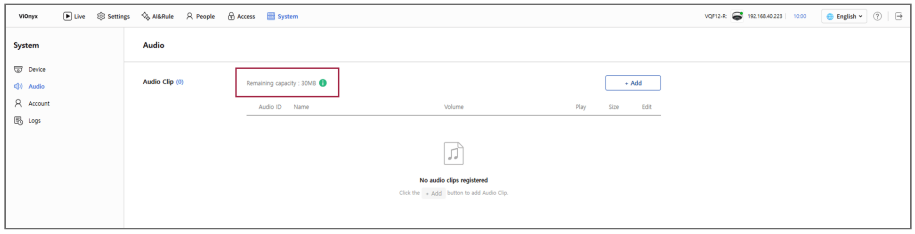
Upload audio clips for the camera and apply them as alarm tones or voice prompts. Upload and manage audio files in WAV format.

Upload audio clips in the following situations.

- When you need to upload alarm tones to play when an event occurs
- When you need to add multilingual voice prompts
- When you need to add voice messages for specific situations

Check audio storage capacity

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Audio** on the left sidebar.
3. You can check the remaining capacity of the audio storage in the **Audio Clip** section.



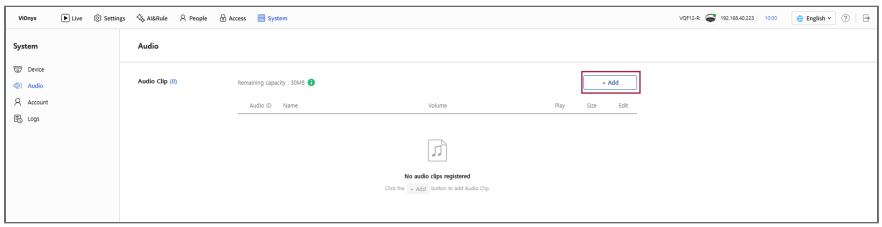
Prepare audio files

Before uploading audio clips, check the following.

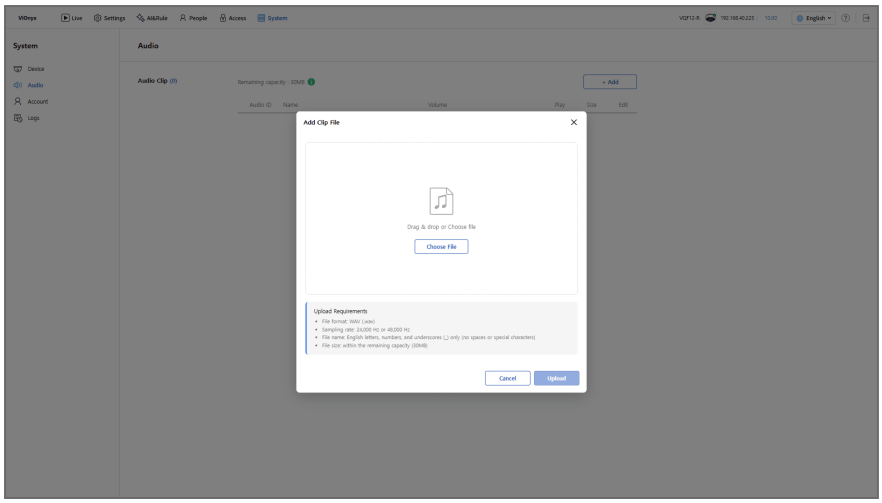
- **File format**: Only the `.wav` extension is supported.
- **Sample rate**: Use a sample rate of 48 kHz or higher.
- **File name**: Use only English letters, numbers, and underscores (`_`), up to 64 characters. Spaces and special characters are not allowed.
- **File size**: You can upload files within the remaining capacity.

Upload audio clips

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Audio** on the left sidebar.
3. Click **+ Add** at the top right of the screen.

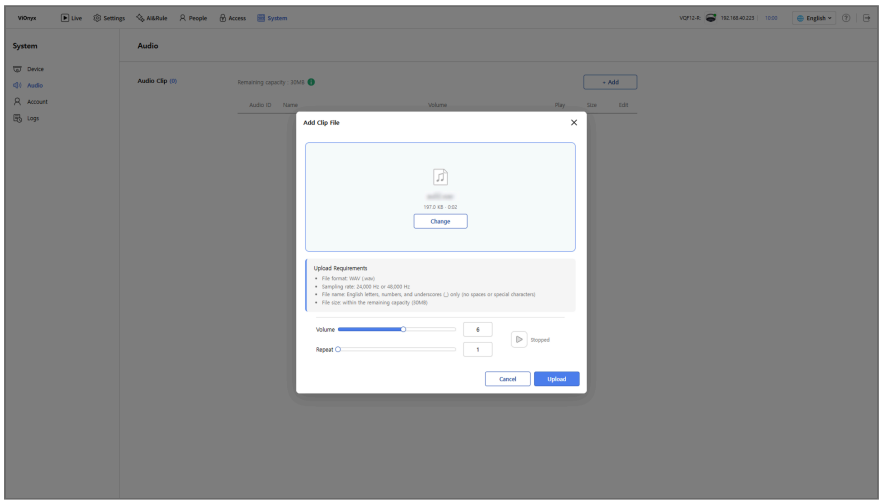


4. The **Add Clip File** popup appears.



5. Drag and drop a WAV file into the upload area, or click **Choose File** and select a WAV file stored locally.

6. After the upload completes, adjust the volume and repeat settings options.



7. Click **Upload** to upload the audio clip.

View uploaded audio clips in the list.



Info

- Adjust the volume slider to set the playback volume for the audio clip.
- To play the audio clip, click ▶.

Delete audio clip

Click to the right of the audio clip you want to delete.



> **Info**
>
> - If the audio clip you want to delete is applied to an AI rule, it is automatically excluded from the AI rule settings.
> - For more information on AI rule settings, see AI Rule Settings.

Update Administrator Account Password

Change the administrator account password to enhance camera access security. Change the password regularly as a security best practice.

Change the password in the following situations.

- When setting up the administrator account for the first time to enhance security
- When renewing the password to comply with routine security policy
- If the password is compromised and requires immediate change
- When replacing the administrator, set a new password

Check password rules

Check the following rules before setting the password. All rules must be met.

- The password must be at least 12 characters long. Maximum length: 64 characters.
- Include at least one lowercase letter (`a-z`) and one uppercase letter (`A-Z`).
- Include at least one digit (`0-9`) and one special character.

  > *Example special characters:* `"` `!` `@` `#` `$` `%` `^` `&` `*` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}`

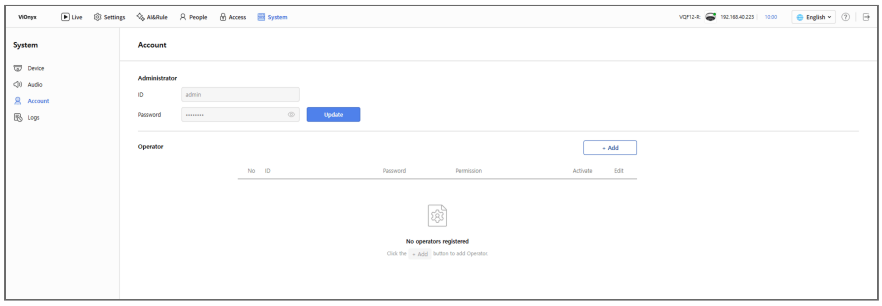
- Do not include sequences of 4 or more consecutive characters (e.g., `1234` , `abcd`) or 4 or more identical characters.
- The username (case-insensitive) must not be included in the password.

  > *admin, Admin, ADMIN, Admin123! etc.*

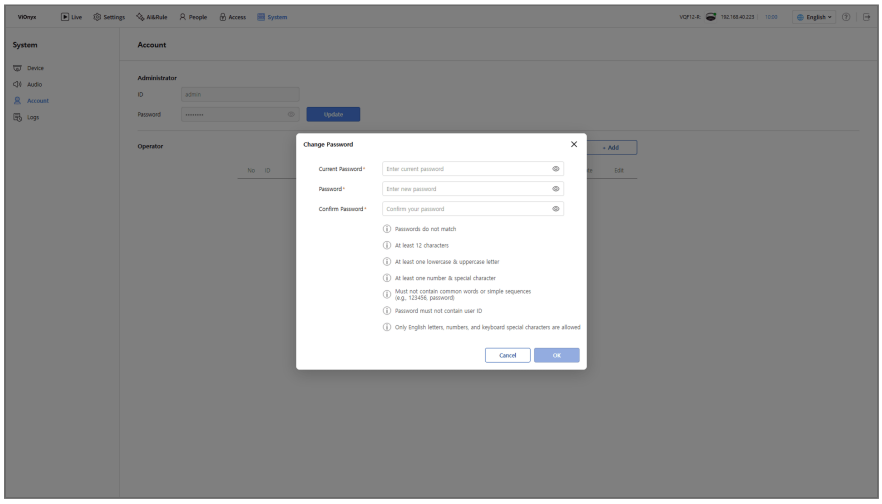
- Common weak passwords such as `password` , `qwerty` , `123456` are not allowed.
- Use only English letters, numbers, and special characters from an English keyboard.

Change administrator password

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.



3. In the **Administrator** section, click **Update**.
4. When the **Change Password** window appears, enter the current administrator password in the **Current Password** input field.



5. Enter the new password in the **Password** and **Confirm Password** input fields, in that order.
6. Click **OK** to change the new password.

When a success message appears, the password change is complete.

> **Info**
>
> - After changing the password, you may need to log in again.
> - Password change events are recorded in the system log.

If you forget the password

Recover a lost administrator password using the following methods.

- **Factory reset**: Running a factory reset restores the administrator account to the default values. Warning: Factory Reset deletes all data. For more information on factory initialization, see the ViOnyx Installation Guide.
- **Contact technical support**: Contact Suprema Global Technical Support Team for help.

Manage Operators

In addition to administrators, add, edit, or delete operator accounts with limited permissions. Operators can manage certain camera features on behalf of administrators.

Also add an ONVIF-only account that the NVR/VMS uses for ONVIF and RTSP authentication. An ONVIF-only account is required to enable ONVIF Profile S fallback.

Add operators in the following situations.

- Assign additional staff for camera operation.
- Grant only specific permissions.
- When multiple people must collaborate to manage the camera.
- Grant team members read-only or edit permissions.

Info

- Add up to 10 operators.
- Operators cannot add other operators. Only administrators can add operators.
- Operator passwords follow the same rules as administrator passwords. For more information, refer to Update Administrator Account Password.
- Each operator can change only their own account information.

Operator permission types

Select one of the following 3 permissions when adding an operator.

- **Read Only**: View all camera settings and logs; cannot change settings.
- **Read Write**: Access all menus except the Administrator menu and change camera settings. Operators can change their own password but not other operators' or administrators' passwords.
- **ONVIF Only**: A device-only account that the NVR/VMS uses for ONVIF and RTSP authentication. Cannot log in to the web UI. Required when enabling ONVIF Profile S fallback. For more information, see Configure Network Settings.

Limitations of ONVIF-only accounts

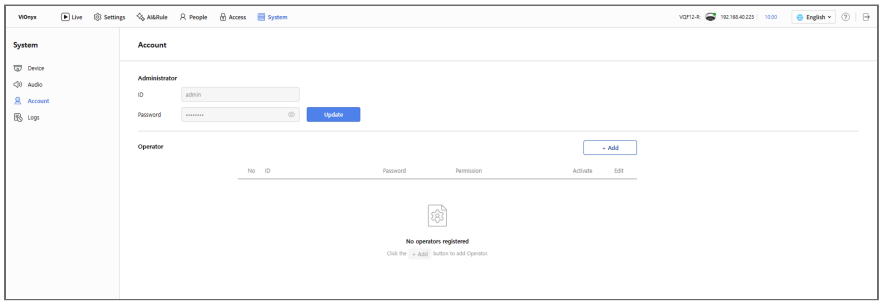
ONVIF-only accounts have the following limitations, unlike standard operator accounts.

- Create only one per device.
- After creating the account, the system blocks changes to the ID, password, and permissions. Only enable, disable, or delete the account.
- Disabling the account prevents Profile S fallback.
- When Profile S fallback is enabled, the system blocks account deletion. First, change the ONVIF mode to **Profile T Only**.

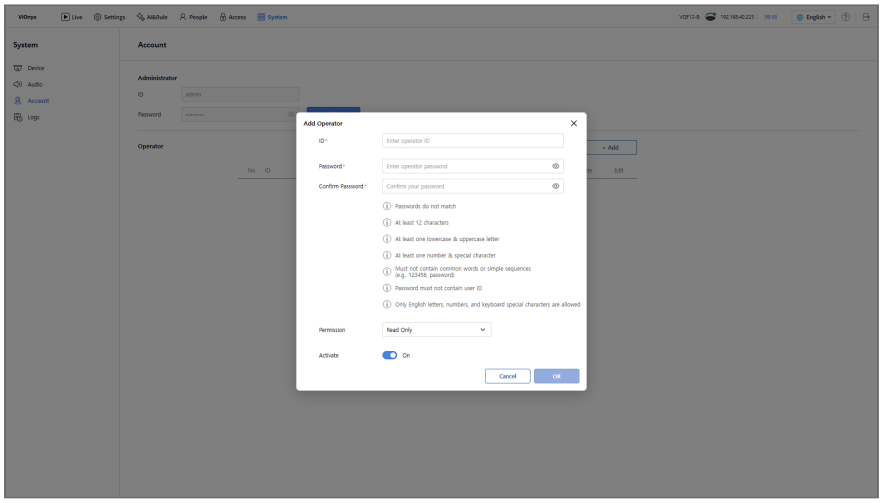
> **Caution**
>
> ONVIF-only accounts do not allow ID or password changes after creation. Decide in advance what to enter on the NVR/VMS, and store the account information securely. To change the password, delete the account, then create it again.

Add operator

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.



3. In the **Operator** section, click **+ Add**.
4. When the **Add Operator** popup appears, enter the required information.



- **ID**: Enter the operator's unique ID.
  - Up to 64 characters.
  - Can include Korean, English letters, and numbers.
  - Allowed special characters: `_`, `.`, `-`, `(`, `)`.
  - Must be unique and not duplicate another operator.
- **Password**: Enter the operator's password. Follows the same rules as the administrator password. For more information, refer to Update Administrator Account Password.
- **Confirm Password**: Re-enter the password.
- **Permission**: Select the operator's permission. Select **ONVIF Only** to create an ONVIF-only account.

- **Enabled**: Enable or disable the operator's account.

5. After entering all information, click **OK**.

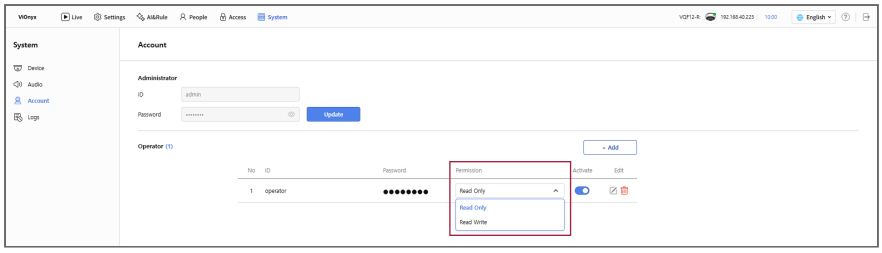
After adding a new operator, the new account appears in the list.

> **Info**
>
> - After adding an operator, log in with that account to verify permissions are applied correctly.
> - Deliver the operator's ID and password to the operator securely.

Change operator permissions

Change an operator's permissions.

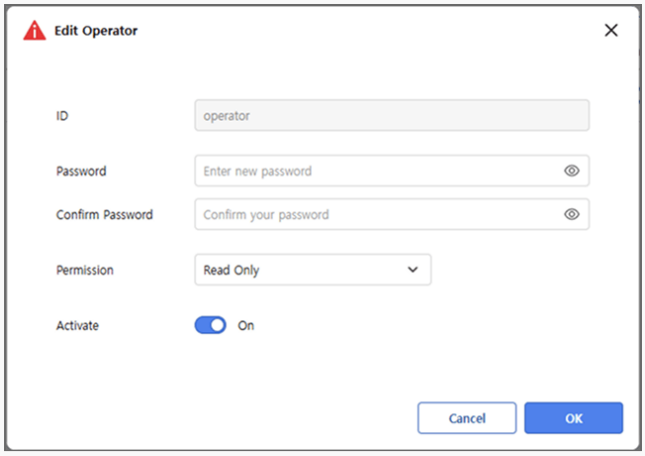
1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.
3. In the **Operator** section, click the **Permission** field for the operator whose permissions you want to change.



4. Select the desired permissions from the list.

When the permission change succeeds, a success message appears in the upper right corner of the screen.

> **Tip**
>
> Click to open the **Edit Operator** window. In the **Permission** field, change to the desired permissions, and then click **OK**.



Info

ONVIF-only accounts do not allow permission changes. If another permission is required, add a new operator account.

Disable operator

Temporarily disable an operator's account. Blocks access without deleting the account.

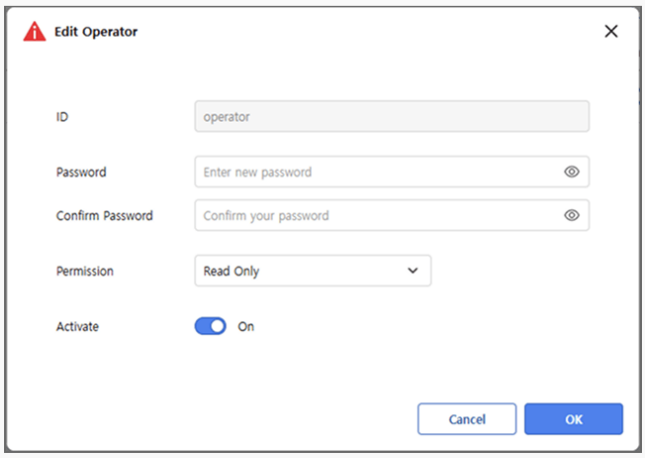
1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.
3. In the **Operator** section, click the toggle in the **Enabled** field for the operator you want to deactivate.



When deactivation succeeds, a success message appears in the upper right corner of the screen. Disabled operator accounts cannot log in.

Tip

Click to open the **Edit Operator** window. Click the toggle in the **Enabled** field to deactivate the account. Click **OK** to save the changes.



Info

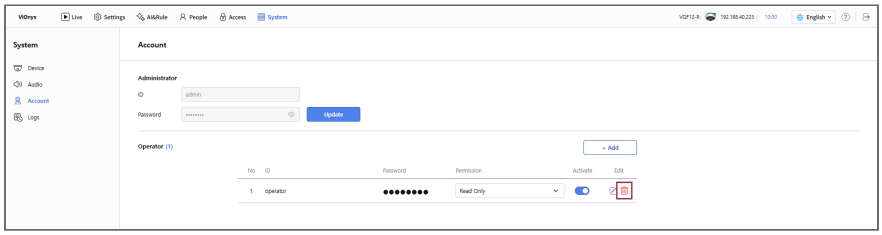
Disabled accounts can be reactivated later.

> **Caution**
> If an operator is already logged in, they will be denied access on their next login attempt.

Delete operator

You can permanently delete operator accounts. Deleted accounts cannot be recovered.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Account** on the left sidebar.
3. In the **Operator** section, click for the operator you want to delete.



4. When the warning message appears, click **OK**.

When deletion succeeds, a success message appears in the upper right corner of the screen. The operator account is removed from the list.

> **Info**
> If **Profile T priority / S fallback** is enabled, the system blocks deletion of the ONVIF-only account. Go to **Settings** → **Network** → **Network**, change the ONVIF mode to **Profile T Only**, then try again. For more information, see Configure Network Settings.

View System Logs

View and manage logs for camera user access, event occurrences, AI analysis, and system operations. In the web interface, filter logs by category, level, and actor. Export logs as CSV or download encrypted device logs for detailed analysis.

Check logs in the following situations.

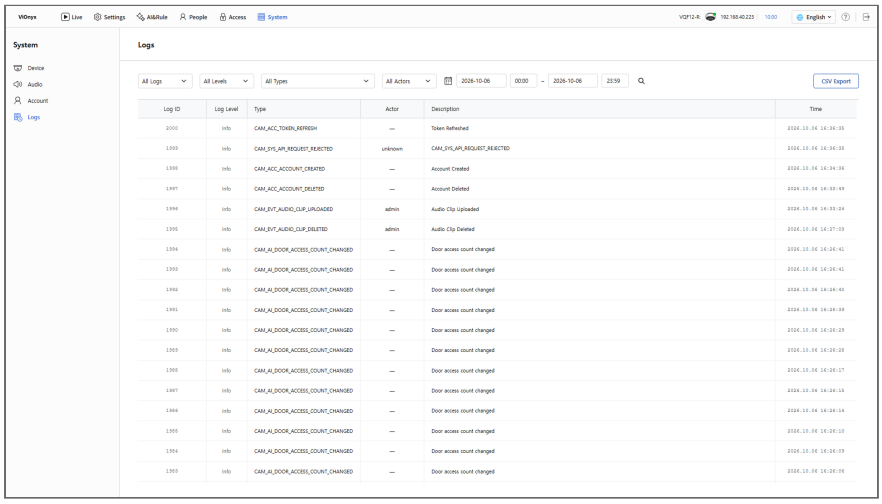
- To check who accessed the camera and when
- To track when a specific event occurred
- To check major system operations such as boot and reboot
- To review access records for security monitoring
- To collect system logs for troubleshooting
- When you need to distinguish actions executed by an administrator or operator from actions executed automatically by the camera

Info

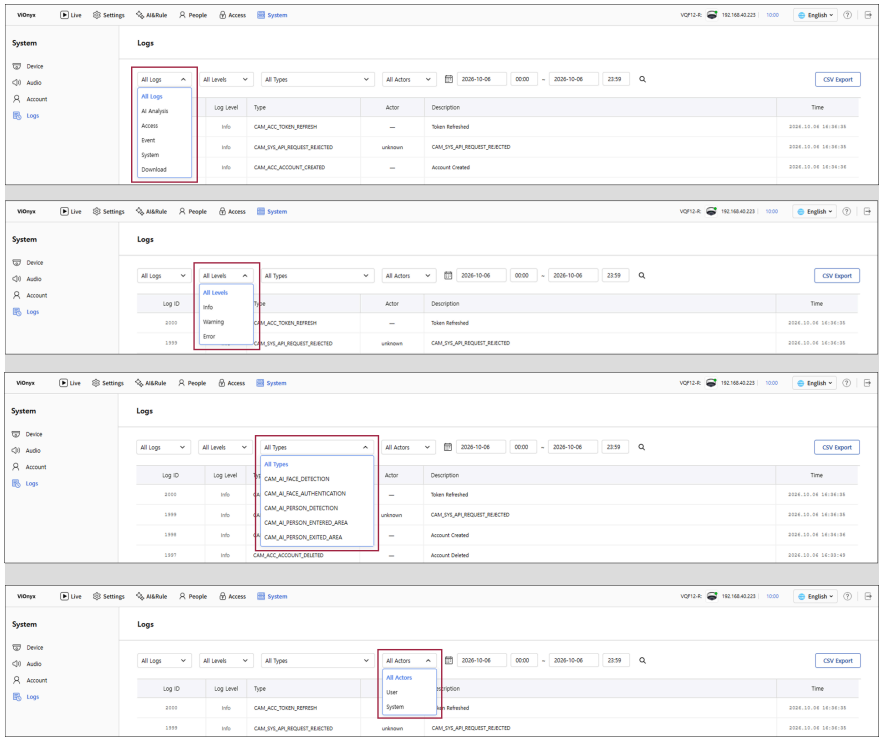
- Logs are retained automatically according to the device's memory size.
- Each log type is retained for approximately 1 month.
- When memory is full, the oldest logs are deleted automatically.
- Only administrators and operators with read/write permission can use the **Logs** menu. However, only administrators can view **System** logs.

View logs

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Logs** on the left sidebar. View all logs.



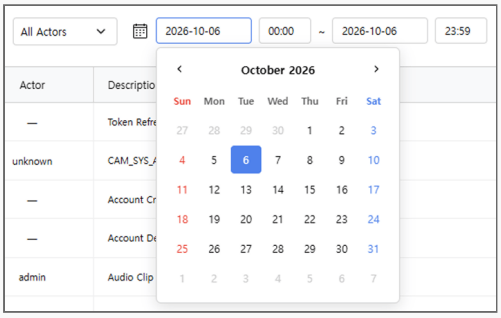
3. Select criteria in **All Logs**, **All Levels**, **All Types**, and **All Actors** at the upper left of the log list. Use them to filter logs by category, level, type, and actor.



4. Click Q at the top of the log list to filter logs based on the selected criteria.

Info

- To view logs for a specific period, click the date and time input fields. When the calendar and time picker appear, select the desired start date and time. Set the end date and time the same way.



- Scroll down the list to refresh it and keep viewing older logs.
- For more information about log types, see System Log Types.

Log types

Logs are categorized as follows.

- **AI Analysis**: View event records related to AI analysis.
- **Access**: View records related to user access and accounts, such as login, logout, and account creation.
- **Event**: Records of event occurrences, Webhook sends, and rule executions.
- **System**: Records of system operations such as boot, reboot, and initialization. This log is **viewable by administrators only**.

Info

Select **Download** to download the device's encrypted log file. For more information, see Device log download.

Log levels

Logs are categorized by the following levels.

- **Info**: View general informational message logs.
- **Warning**: View warning message logs.
- **Error**: View error message logs.

Actors

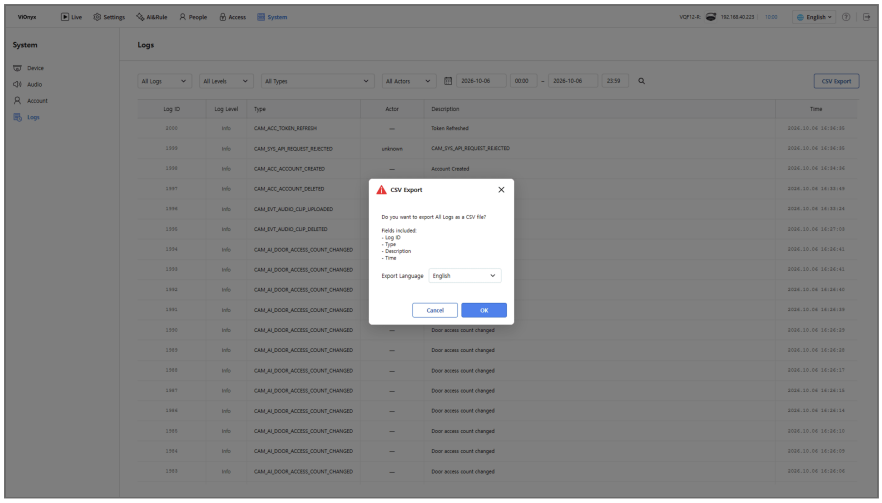
The entity that generates a log is called an actor. Actors are categorized as follows.

- **User**: An administrator or operator who executes tasks directly in the web interface.
- **System**: A camera that executes tasks automatically based on AI rules and schedules.

Export logs

Download logs in CSV format for external analysis or archiving.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Logs** on the left sidebar.
3. Select criteria for the logs to export in **All Logs**, **All Levels**, **All Types**, and **All Actors** at the upper left of the log list. Set a search period to export logs for a specific time range. The CSV file reflects the selected criteria and period.
4. Click **CSV Export** at the top right of the screen.
5. When the **CSV Export** popup appears, select the language to export.



6. Click **OK**.

Download the log list as a CSV file.

> **Info**
>
> - CSV filename format: `system-logs-YYYYMMDD_HHMMSS.csv`.
>
> *Example: system-logs-20240326_153000.csv*
>
> - The file is saved to the browser's default download folder or to a user-selected location.

Log retention and management

Automatic log deletion

When the camera's memory is full, the oldest logs are deleted automatically.

Log category	Retention period
AI Analysis	Approximately one month
Access	Approximately one month

Log category	Retention period
Event	Approximately one month
System	Approximately one month

How to retain important logs

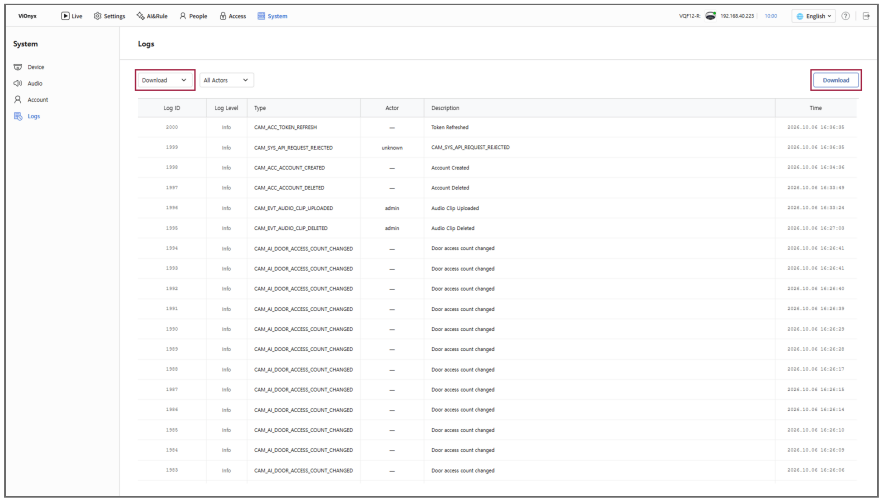
To retain important logs long-term, follow these steps:

- Export logs to CSV regularly.
- Store exported files on external storage (NAS, cloud storage, etc.).
- Include the export date and log period in the file.

Device log download

Download log files stored on the device in encrypted form. Device logs are detailed log files that include all events and operational records generated by the camera system. The file is encrypted to keep it secure, and provide it to Suprema Global Technical Support Team when needed for troubleshooting.

1. Click the **System** menu in the upper-left corner of the screen.
2. Click **Logs** on the left sidebar.
3. Select **Download** in **All Logs** at the upper left of the log list.



4. To download logs for a specific actor, select an actor in **All Actors**. If no actor is selected, the system downloads logs for all actors. For more information on actors, see Actors.
5. Click **Download** at the upper right of the log list.

Download the device log file locally. The file name uses the format `device_logs_{device-serial-number}_YYYYMMDDTHHMMSS.zip.enc`.

> *Example: device_logs_1234567890_20240326T153000.zip.enc*

System Log Types

Provides information about the log types available in system logs.

Log types	Description
CAM_AI_FACE_DETECTION	**Face Detection**
CAM_AI_FACE_AUTHENTICATION	**Face Authentication**
CAM_AI_PERSON_DETECTION	**Person Detection**
CAM_AI_PERSON_ENTERED_AREA	**Person Entered Area**
CAM_AI_PERSON_EXITED_AREA	**Person Exited Area**
CAM_AI_INTRUSION_ENTRY_AREA_APPEARED	**Intrusion Detected (Entry Area)**
CAM_AI_INTRUSION_EXIT_AREA_APPEARED	**Intrusion Detected (Exit Area)**
CAM_AI_PEOPLE_COUNT_CHANGED	**People Count Changed**
CAM_AI_PEOPLE_COUNT_LIMIT_REACHED	**People Count Limit Reached**
CAM_AI_LINE_CROSSED	**Line Crossed**
CAM_AI_FACE_AUTHENTICATION_FAILED	**Face Authentication Failed**
CAM_AI_DOOR_ACCESS_EVENT_OFF	**Door access event off**
CAM_AI_DOOR_ACCESS_SOURCE	**Door access source signal**
CAM_AI_DOOR_ACCESS_AREA_ENTERED	**Door access area entered**
CAM_AI_DOOR_ACCESS_AREA_EXITED	**Door access area exited**
CAM_AI_DOOR_ACCESS_LINE_CROSSED	**Door line crossed**
CAM_AI_DOOR_ACCESS_COUNT_CHANGED	**Door access count changed**
CAM_EVT_RULE_TRIGGERED	**Rule Triggered**
CAM_EVT_RULE_CREATED	**Rule Created**
CAM_EVT_RULE_UPDATED	**Rule Updated**
CAM_EVT_RULE_DELETED	**Rule Deleted**

Log types	Description
CAM_EVT_RULE_ENABLED	**Rule Enabled**
CAM_EVT_RULE_DISABLED	**Rule Disabled**
CAM_EVT_RULE_USERS_ADDED	**Rule users added**
CAM_EVT_RULE_USERS_REMOVED	**Rule users removed**
CAM_EVT_RULE_RELAY_SCHEDULE_BLOCKED	**Relay denied — outside scheduled hours**
CAM_EVT_WEBHOOK_SEND	**Webhook Send Attempt**
CAM_EVT_WEBHOOK_SENT	**Webhook Sent**
CAM_EVT_WEBHOOK_FAILED	**Webhook Failed**
CAM_EVT_WEBHOOK_CREATED	**Webhook Created**
CAM_EVT_WEBHOOK_UPDATED	**Webhook Updated**
CAM_EVT_WEBHOOK_DELETED	**Webhook Deleted**
CAM_EVT_FACE_USER_CREATED	**Face User Created**
CAM_EVT_FACE_USER_UPDATED	**Face User Updated**
CAM_EVT_FACE_USER_DELETED	**Face User Deleted**
CAM_EVT_FACE_USER_CREATE_FAILED	**Face User Create Failed**
CAM_EVT_FACE_USER_UPDATE_FAILED	**Face User Update Failed**
CAM_EVT_FACE_USER_DELETE_FAILED	**Face User Delete Failed**
CAM_EVT_AI_ANALYSIS_CREATED	**AI Analysis Created**
CAM_EVT_AI_ANALYSIS_UPDATED	**AI Analysis Updated**
CAM_EVT_AI_ANALYSIS_DELETED	**AI Analysis Deleted**
CAM_EVT_AI_ANALYSIS_DELETE_STARTED	**AI Analysis Delete Started**
CAM_EVT_AI_EVENT_SETTINGS_UPDATED	**AI Event Settings Updated**
CAM_EVT_PEOPLE_COUNT_RESET_ALL	**People Count Reset All**

Log types	Description
CAM_EVT_PEOPLE_COUNT_RESET	**People Count Reset**
CAM_EVT_PEOPLE_COUNT_AUTO_RESET	**People Count Auto Reset**
CAM_EVT_AUDIO_CLIP_UPLOADED	**Audio Clip Uploaded**
CAM_EVT_AUDIO_CLIP_DELETED	**Audio Clip Deleted**
CAM_EVT_AUDIO_CLIP_PLAY	**Audio Clip Play**
CAM_EVT_AUDIO_CLIP_PLAYED	**Audio Clip Played**
CAM_EVT_AUDIO_CLIP_PLAY_FAILED	**Audio Clip Play Failed**
CAM_EVT_AUDIO_CLIP_API_PLAY	**Audio Clip API Play**
CAM_EVT_AUDIO_CLIP_API_STOP	**Audio Clip API Stop**
CAM_EVT_RELAY_SENT	**Relay command sent**
CAM_EVT_RELAY_FAILED	**Relay communication failed**
CAM_EVT_RELAY_KEEP_STARTED	**Relay keep started**
CAM_EVT_RELAY_KEEP_ENDED	**Relay keep ended**
CAM_EVT_RELAY_KEEP_REARM_FAILED	**Relay keep re-arm failed**
CAM_EVT_RELAY_OPENED	**Relay opened**
CAM_EVT_RELAY_LOCKED	**Relay locked**
CAM_EVT_RELAY_RELEASED	**Relay released**
CAM_EVT_RELAY_OPEN_REJECTED	**Relay open rejected**
CAM_EVT_RELAY_AUTO_CLOSED	**Relay auto-closed**
CAM_EVT_RELAY_STATE_RESTORED	**Relay state restored**
CAM_EVT_RELAY_UNLOCKED	**Relay unlocked**
CAM_EVT_RELAY_IDLE_STATE_CHANGED	**Relay idle state changed**
CAM_EVT_RELAY_IDLE_STATE_APPLIED	**Relay idle state applied**

Log types	Description
CAM_EVT_RELAY_OPEN_FAILED	**Relay open failed**
CAM_EVT_RELAY_LOCK_FAILED	**Relay lock failed**
CAM_EVT_RELAY_RELEASE_FAILED	**Relay release failed**
CAM_EVT_RELAY_AUTO_CLOSE_FAILED	**Relay auto-close failed**
CAM_EVT_RELAY_STATE_RESTORE_FAILED	**Relay state restore failed**
CAM_EVT_RELAY_UNLOCK_FAILED	**Relay unlock failed**
CAM_EVT_RELAY_IDLE_STATE_CHANGE_FAILED	**Relay idle state change failed**
CAM_EVT_RELAY_IDLE_STATE_APPLY_FAILED	**Relay idle state apply failed**
CAM_EVT_RELAY_TOKEN_MIGRATED	**Relay token migrated**
CAM_EVT_SCHEDULE_CREATED	**Schedule created**
CAM_EVT_SCHEDULE_UPDATED	**Schedule updated**
CAM_EVT_SCHEDULE_DELETED	**Schedule deleted**
CAM_EVT_SCHEDULE_LEGACY_MIGRATED	**Schedule data migrated**
CAM_EVT_ACCESS_DOOR_CREATED	**Door created**
CAM_EVT_ACCESS_DOOR_UPDATED	**Door updated**
CAM_EVT_ACCESS_DOOR_DELETED	**Door deleted**
CAM_EVT_ACCESS_DOOR_DELETE_STARTED	**Door delete started**
CAM_EVT_ACCESS_DOOR_DELETE_FAILED	**Door delete failed**
CAM_EVT_ACCESS_LEVEL_CREATED	**Access level created**
CAM_EVT_ACCESS_LEVEL_UPDATED	**Access level updated**
CAM_EVT_ACCESS_LEVEL_DELETED	**Access level deleted**
CAM_EVT_ACCESS_MEMBERSHIP_UPDATED	**Access level membership updated**
CAM_EVT_ACCESS_POLICY_APPLY_STARTED	**Access policy apply started**

Log types	Description
CAM_EVT_ACCESS_POLICY_APPLIED	**Access policy applied**
CAM_EVT_ACCESS_POLICY_APPLY_FAILED	**Access policy apply failed**
CAM_EVT_ACCESS_RUNTIME_RECOVERED	**Access runtime recovered**
CAM_EVT_ACCESS_RUNTIME_RECOVER_FAILED	**Access runtime recovery failed**
CAM_EVT_ACCESS_POLICY_REBUILT_ON_BOOT	**Access policy rebuilt on boot**
CAM_EVT_ACCESS_RUNTIME_DEGRADED	**Access runtime degraded**
CAM_EVT_ACCESS_DOOR_TRIGGER_CREATED	**Door trigger binding created**
CAM_EVT_ACCESS_DOOR_TRIGGER_UPDATED	**Door trigger binding updated**
CAM_EVT_ACCESS_DOOR_TRIGGER_DELETED	**Door trigger binding deleted**
CAM_EVT_ACCESS_DOOR_PASSED_UNIDENTIFIED	**Passage (unidentified)**
CAM_EVT_ACCESS_DOOR_UNLOCK_REQUESTED	**Door unlock requested**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_DOOR_MODE	**Door access denied (door mode)**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_UNIDENTIFIED	**Door access denied (unidentified)**
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED	**Door access granted**
CAM_EVT_ACCESS_DOOR_ACCESS_GRANTED_ALREADY_UNLOCKED	**Door access granted (already unlocked)**
CAM_EVT_ACCESS_DUAL_AUTH_PENDING	**Dual authentication pending**
CAM_EVT_ACCESS_DUAL_AUTH_TIMEOUT	**Dual authentication timed out**
CAM_EVT_ACCESS_DOOR_SCHEDULE_UNLOCKED	**Schedule unlock started**
CAM_EVT_ACCESS_DOOR_SCHEDULE_LOCKED	**Schedule lock started**
CAM_EVT_ACCESS_DOOR_SCHEDULE_RELEASED	**Schedule window released**
CAM_EVT_ACCESS_DOOR_HOLD_RELEASED	**Keep-unlock released**
CAM_EVT_ACCESS_DOOR_RULE_ACTION_SUCCEEDED	**Door rule action succeeded**
CAM_EVT_ACCESS_DOOR_RULE_ACTION_FAILED	**Door rule action failed**

Log types	Description
CAM_EVT_ACCESS_DOOR_RULE_CREATED	**Door rule created**
CAM_EVT_ACCESS_DOOR_RULE_UPDATED	**Door rule updated**
CAM_EVT_ACCESS_DOOR_RULE_DELETED	**Door rule deleted**
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCKED	**Exit button unlocked**
CAM_EVT_ACCESS_DOOR_EARLY_RELOCKED	**Door early relocked**
CAM_EVT_ACCESS_EXIT_BUTTON_UNLOCK_FAILED	**Exit button unlock failed**
CAM_EVT_ACCESS_DOOR_PASSED	**Authenticated passage**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_ACCESS_LEVEL	**Door access denied (access level)**
CAM_EVT_ACCESS_DOOR_ACCESS_DENIED_TAILGATING	**Door access denied (tailgating)**
CAM_EVT_ACCESS_DOOR_UNLOCK_FAILED	**Door unlock failed**
CAM_EVT_ACCESS_DOOR_PASSED_AFTER_DENIED	**Passage after denial**
CAM_EVT_ACCESS_DOOR_RULE_ACTION_RETRYING	**Door rule action retrying**
CAM_EVT_ACCESS_DOOR_RULE_MUTATION_REJECTED	**Door rule change rejected**
CAM_EVT_HEATER_CONTROL_REQUESTED	**Heater control requested**
CAM_EVT_HEATER_ENABLED	**Heater enabled**
CAM_EVT_HEATER_DISABLED	**Heater disabled**
CAM_EVT_HEATER_AUTO_DISABLED	**Heater auto-disabled**
CAM_EVT_HEATER_CONTROL_FAILED	**Heater control failed**
CAM_EVT_HEATER_STATE_RECONCILED	**Heater state reconciled**
CAM_EVT_HEATER_BOOT_RECOVERED	**Heater boot recovered**
CAM_EVT_HEATER_BOOT_RECOVERY_FAILED	**Heater boot recovery failed**
CAM_EVT_HEATER_FAULT_DISABLED	**Heater disabled by fault**
CAM_EVT_INPUT_IDLE_STATE_CHANGED	**Input idle state changed**

Log types	Description
CAM_EVT_INPUT_IDLE_STATE_CHANGE_FAILED	**Input idle state change failed**
CAM_SYS_NETWORK_CHANGE	**Network Settings Changed**
CAM_SYS_NETWORK_DHCP_FALLBACK	**DHCP Fallback to Link-local**
CAM_SYS_DATETIME_CHANGE	**Date/Time Settings Changed**
CAM_SYS_NTP_SYNC_FAILED	**NTP Sync Failed**
CAM_SYS_FIRMWARE_UPGRADE	**Firmware Upgrade**
CAM_SYS_SYSTEM_STARTED	**Web Server Started**
CAM_SYS_FACTORY_RESET	**Factory Reset**
CAM_SYS_CONFIG_RESET	**Config Reset**
CAM_SYS_SYSTEM_REBOOT	**System Reboot**
CAM_SYS_CLUE_ENABLED	**CLUe Enabled**
CAM_SYS_CLUE_DISABLED	**CLUe Disabled**
CAM_SYS_CLUE_ENABLE_FAILED	**CLUe Enable Failed**
CAM_SYS_CLUE_USER_SYNC_CHANGED	**CLUe user sync changed**
CAM_SYS_CLUE_TUNNEL_CHANGED	**CLUe tunnel changed**
CAM_SYS_CONSENT_ENROLLMENT_CHANGED	**Consent Enrollment Changed**
CAM_SYS_CONSENT_ANALYTICS_CHANGED	**Consent Analytics Changed**
CAM_SYS_AI_SETTINGS_CHANGED	**AI Settings Changed**
CAM_SYS_AI_LOAD_FAILED	**AI Load Failed**
CAM_SYS_SECURE_TAMPER_CHANGED	**Secure Tamper Settings Changed**
CAM_SYS_TUNNEL_MODE_CHANGED	**Tunnel mode changed**
CAM_SYS_TUNNEL_SETTING_UPDATED	**Tunnel setting updated**
CAM_SYS_WEBRTC_SESSION_START	**WebRTC session started**

Log types	Description
CAM_SYS_WEBRTC_SESSION_END	**WebRTC session ended**
CAM_SYS_CRYPTO_KEYGEN_FAILED	**Crypto key generation failed**
CAM_SYS_CRYPTO_OP_FAILED	**Crypto operation failed**
CAM_SYS_SLAVE_CONNECTED	**RS485 slave connected**
CAM_SYS_SLAVE_DISCONNECTED	**RS485 slave disconnected**
CAM_SYS_RS485_SLAVE_FW_UPDATE_SUCCEEDED	**Slave firmware update succeeded**
CAM_SYS_RS485_SLAVE_FW_UPDATE_FAILED	**Slave firmware update failed**
CAM_SYS_ONVIF_MODE_CHANGED	**ONVIF mode changed**
CAM_SYS_ONVIF_HTTP_PROXY_FAILED	**ONVIF HTTP proxy failed**
CAM_SYS_API_OPERATION_FAILED	**API operation failed**
CAM_SYS_API_COMPLETION_UNCONFIRMED	**API completion unconfirmed**
CAM_SYS_API_REQUEST_REJECTED	**API request rejected**
CAM_ACC_LOGIN	**Login**
CAM_ACC_LOGOUT	**Logout**
CAM_ACC_TOKEN_REFRESH	**Token Refreshed**
CAM_ACC_PASSWORD_CHANGE	**Password Changed**
CAM_ACC_AUTH_FAILURE	**Authentication Failure**
CAM_ACC_REFRESH_TOKEN_REUSE	**Refresh Token Reuse Detected**
CAM_ACC_SESSION_INVALIDATED	**Session Invalidated**
CAM_ACC_RATE_LIMIT_EXCEEDED	**Rate Limit Exceeded**
CAM_ACC_FORBIDDEN_ACCESS	**Forbidden Access**
CAM_ACC_PASSWORD_SETUP	**Password Setup**
CAM_ACC_ACCOUNT_LOCKED	**Account Locked**

Log types	Description
CAM_ACC_SESSION_EXPIRED	**Session Expired**
CAM_ACC_ACCOUNT_CREATED	**Account Created**
CAM_ACC_ACCOUNT_UPDATED	**Account Updated**
CAM_ACC_ACCOUNT_DELETED	**Account Deleted**
CAM_ACC_ACCOUNT_DISABLED	**Account Disabled**
CAM_ACC_SESSION_KICKED	**Session Force Terminated**
CAM_ACC_LOGIN_FAILED	**Login Failed**
CAM_ACC_PERMISSION_DENIED	**Permission denied**
CAM_ACC_SESSION_LIMIT_REJECTED	**Session limit rejected**
CAM_ACC_ACCOUNT_CREATE_FAILED	**Account create failed**

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this web site.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema’s products that are not within Suprema’s direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.