OCTAVUE SIMBIOS KLAVYS FENNEC SERIES

GSD GROUP

SECURING YOUR WORLD

USER MANUAL

ACCESS DOORBELL

Contents

PART I

Getting Started

Connection, IP addressing, and web login

Chapter 1 Overview & Product Description

The OCTAVUE access control camera by GSD Group combines identity verification with high-definition video monitoring in a single intelligent device, delivering integrated security and entrance management for a wide range of environments.

1.1 Scope of Application

The access control camera integrates identity verification and video surveillance into a unified intelligent platform. Its core value is to improve the efficiency, convenience, and security of entrance management. Typical deployment scenarios span commercial, residential, office, and public-service environments.

In commercial premises and offices, where the flow of personnel is high and mixed (employees, visitors, and contractors), the camera balances throughput efficiency against security control: its core function is to distinguish personnel authority and maintain a verifiable record of every entry and exit.

In residential scenarios, the primary objective is to protect the privacy of residents and prevent unauthorized access by strangers while preserving day-to-day convenience. Card-free face recognition is especially valuable for elderly residents and children, eliminating the familiar pain point of forgotten or lost access cards.

> **NOTE** Throughout this manual, the terms **IP camera** and **network camera** are used interchangeably to refer to the OCTAVUE access control camera.

1.2 Product Description

Compared with traditional access control equipment, the OCTAVUE visual access control camera offers three principal advantages:

- **Enhanced security:** AI algorithms defeat identity spoofing and tailgating, while high-definition video and early-warning functions deliver prevention beforehand and traceability after an event.
- **Improved efficiency:** Hierarchical permissions and remote management reduce manual intervention and simplify the linkage between control devices.
- **Optimized experience:** Card-free face recognition and a lightweight operation platform accommodate the needs of diverse user groups.

Together, these capabilities raise safety, lower management costs, and provide a one-stop entrance and exit management solution.

The camera also packs advanced audio and video technology into a single, compact device, using modern video compression to keep footage sharp and high-quality without saturating available network bandwidth. Monitoring is straightforward: enter the camera's web address in any supported browser to view the live stream in real time. Administrators can create multiple user accounts with distinct permission levels for full control over who may

view or manage the camera. When motion is detected, the camera can immediately send an email alert with captured images or video clips, and it automatically saves an event backup to the local memory card.

1.2.1 Appearance

The exterior of the visual access control camera is shown below.

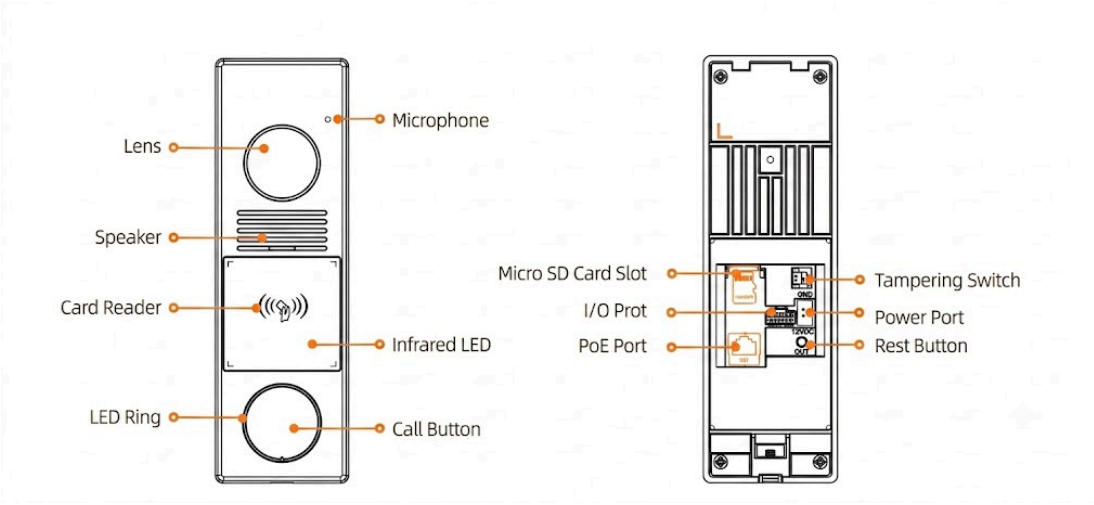

Figure 1-1. Appearance of the access control camera

1.2.2 I/O Ports and Tail-Line Definitions

The I/O port supports connection to a Wiegand card reader, an RS-485 card reader, alarm devices, and related peripherals. The individual tail lines are described in the following figure and table.

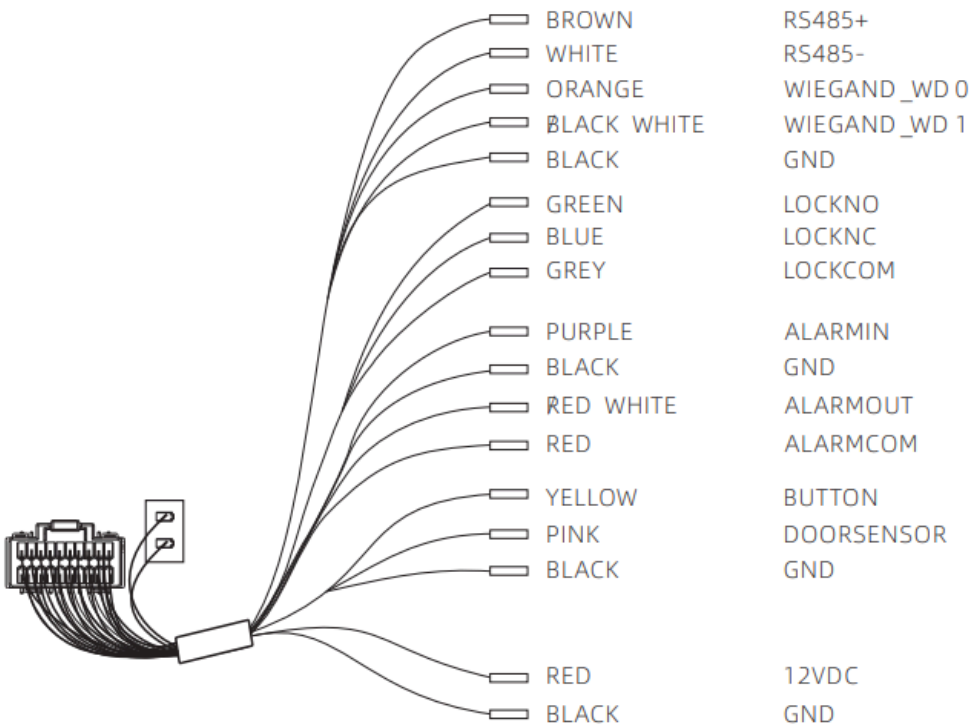

Figure 1-2. I/O port tail-line layout

Tail Line Name	Wire Color	Port	Description
RS-485	Brown	RS-485+	External RS-485 card reader

	White	RS-485-	
Wiegand	Orange	WIEGAND_WD0	External Wiegand card reader
	Black/White	WIEGAND_WD1	
	Black	GND	
Door lock	Green	LOCKNO	External door lock
	Blue	LOCKNC	
	Grey	LOCKCOM	
Alarm input/output	Purple	ALARMIN	Alarm input
	Black	GND	
	Red/White	ALARMOUT	External alarm
	Red	ALARMCOM	
Exit button and door sensor	Yellow	BUTTON	External exit button and door sensor
	Pink	DOORSENSOR	
	Black	GND	
Power supply	Red	12VDC	12 VDC power supply connection
	Black	GND	

1.2.3 Wiring Diagrams

Refer to the following diagrams when connecting card readers, door locks, exit buttons, door sensors, and alarm devices to the camera.

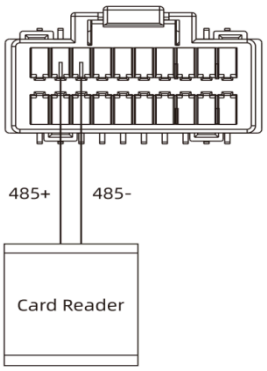

Figure 1-3. RS-485 card reader wiring diagram

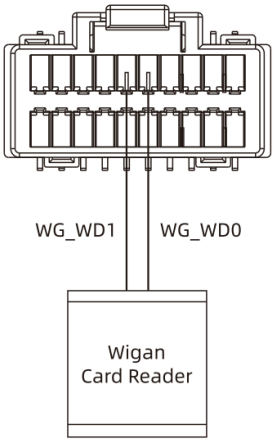

Figure 1-4. Wiegand card reader wiring diagram

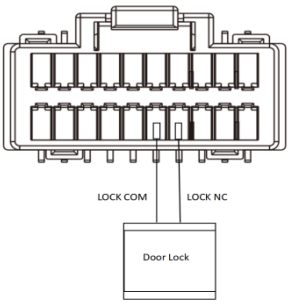

Figure 1-5. Normally closed (NC) door lock wiring diagram

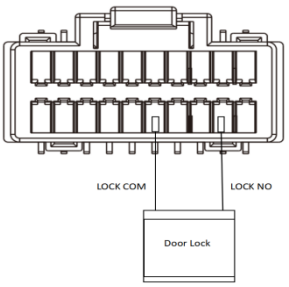

Figure 1-6. Normally open (NO) door lock wiring diagram

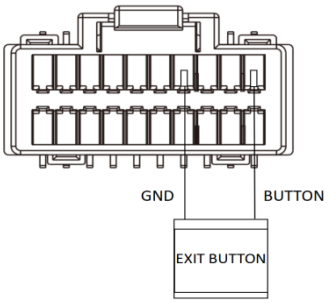

Figure 1-7. Exit button wiring diagram

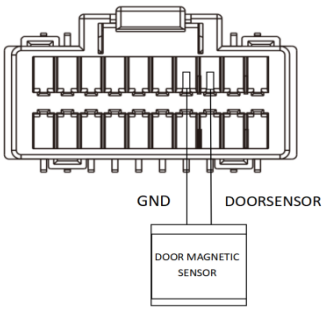

Figure 1-8. Door sensor (magnetic contact) wiring diagram

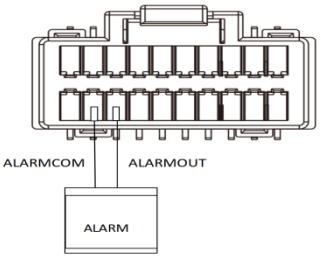

Figure 1-9. Alarm wiring diagram

1.3 Installation Environment

The access control camera can be installed indoors or outdoors. When installing the device outdoors, do not position it in direct sunlight. When installing it indoors, maintain an appropriate distance from lights and windows, as shown in the figure below.

CAUTION Prolonged exposure to direct sunlight or strong backlighting can degrade image quality and shorten the service life of the device. Choose a mounting location that avoids these conditions.

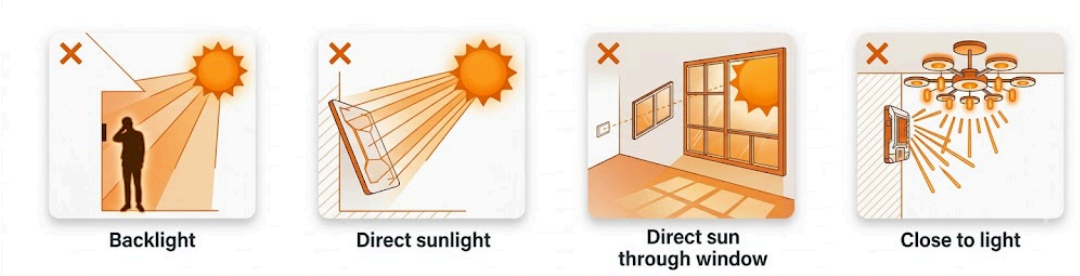

Figure 1-10. Recommended installation positioning

1.4 Operating Environment

To access and manage the camera through a web browser, the client computer should meet the following minimum requirements.

- **Operating system:** Windows XP / Windows 7 / Windows 8 / Windows 10 / Windows 11, or MacOS 10 or above.
- **CPU:** Intel i3 or higher.
- **Memory:** 2 GB or more.
- **Video memory:** 1 GB or higher.
- **Display:** 1024×768 resolution or higher.
- **Browser:** IE 10 and above, Chrome 57 and above, Firefox 52 and above, Edge 41 and above, or Safari 12 and above.

1.5 Default Configuration and Initial Login

Before installation, review the following default network settings, credentials, and connectivity options.

1.5.1 Network Settings

By default, the camera automatically obtains an IP address from a DHCP server. If no DHCP server is active on the network, the camera falls back to the static IP address **10.0.0.6**.

NOTE The default web port is **80**. ONVIF is enabled by default to allow immediate integration with third-party systems, and the default ONVIF port is synchronized with the web port.

1.5.2 Initial Login and Security

The default administrator user name is **admin** (case-sensitive, all lowercase). For security, the camera ships with no default password.

CAUTION On first-time login you must create a strong password by following the on-screen prompts. Store this password securely; it is required for all subsequent access. See Section 4.2 for details.

TIP If the administrator password is later lost, **Super Code** is the recommended password-recovery method. Enabled by default in recent firmware, it restores access with the assistance of technical support.

Chapter 2 Device Connection

The OCTAVUE access control camera supports two physical connection methods. Select the method that matches your deployment: a direct connection to a single computer for initial configuration and bench testing, or a connection through a router, switch, or NVR for everyday operation and remote access.

NOTE Before connecting the camera, note its default IP address, subnet mask, and login credentials as printed on the device label or in the accompanying quick-start documentation. These values are required to reach the camera for the first time.

2.1 Direct Connection to a PC

This method links the camera directly to a computer without a router or internet connection. It is best suited to initial setup, firmware maintenance, and on-site diagnostics.

1. Connect one end of an Ethernet cable to the camera's network port and the other end directly to the network port on your computer.
2. Connect the camera to power using the supplied **12V power adapter**.
3. Adjust your computer's network settings so that its IP address is on the same subnet as the camera's default IP address.
4. Wait approximately one minute. Once the camera completes its startup sequence, it will begin communicating with your computer automatically.

TIP If your computer and the camera are on different subnets, the camera will not respond. Set the computer to a static IP address within the same range as the camera before attempting to connect.

2.2 Connection via Router, Switch, or NVR

This method connects the camera to your local home or business network, allowing access from other devices on the network and, when configured, over the internet. It is the recommended method for everyday use and remote viewing.

1. Connect both the camera and your computer to the **LAN** ports of your router, network switch, or NVR.
2. Connect the camera to its power adapter.
3. Configure the camera's **Gateway** setting to match your router's IP address. This allows the camera to route its video stream through the router and, where permitted, out to the internet.

NOTE When the camera is powered through a PoE switch or NVR, a separate power adapter is not required. Verify that the switch or NVR provides sufficient PoE output for the camera before relying on it as the sole power source.

Chapter 3 Setting the IP Address

Before the OCTAVUE access control camera can be reached from a web browser or added to an NVR, it must hold an IP address that is valid for your local network. The bundled Discovery Tool locates every camera on the same subnet and lets you assign or correct its network settings without prior access to the web interface.

3.1 Using the Discovery Tool

Install and launch the **Discovery Tool** on a computer connected to the same local area network as the camera. When the application opens, it displays the device list and the search controls used to scan the network.

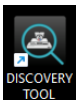

Figure 3-1. Discovery Tool main window

Click **Search** to refresh the list of cameras detected on the local area network. Each device that responds is shown with its identifying details, so you can locate the target camera by its P2P ID or MAC address.

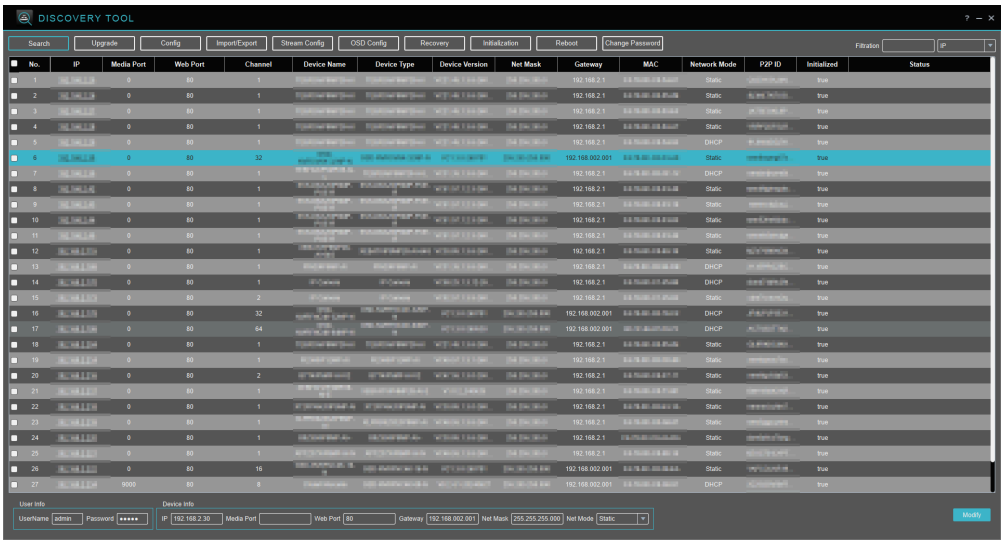

Figure 3-2. Cameras detected on the local area network

1. Click **Search** to scan the local area network for connected OCTAVUE cameras.
2. Identify the target camera in the results by matching its P2P ID or MAC address to the label on the device.
3. Select the camera to display its current network configuration, then enter the required IP address, subnet mask, and gateway.
4. Apply the changes to write the new IP address to the camera.

TIP If the camera does not appear after the first scan, click **Search** again to refresh the list. A newly powered device may take a few moments to respond on the network.

NOTE The assigned IP address must belong to the same subnet as the computer running the Discovery Tool; otherwise the camera will not be reachable from a web browser.

Chapter 4 Web Login

The OCTAVUE access control camera provides a browser-based web client for configuration and daily operation. This chapter describes how to reach the web client, activate the camera on first use, sign in, and recover the administrator password if it is lost.

4.1 Accessing the Web Client

There are two ways to open the web client of the camera.

Run the **Device Config Tool** to search for cameras on the current network. Once the search completes, click the IP address of the target camera in the results list to open its web client directly.

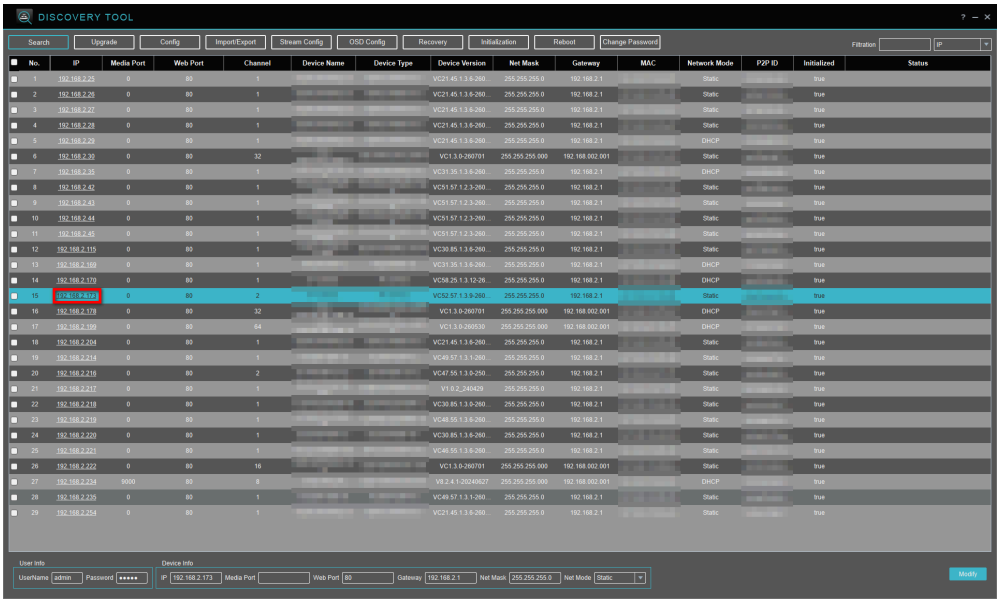

Figure 4-1. Searching for cameras with the Device Config Tool

Alternatively, enter **http://<IP>:<web port>** in the address bar of your browser. For example, if the camera IP address is 192.168.2.173 and the web port is 80, enter **http://192.168.2.173:80** to reach the device. In normal use, HTTP access defaults to port 80.

> **NOTE** Before connecting, make sure that the camera and the PC are on the same network segment; otherwise the web client cannot be reached.

4.2 First-Time Login

When you access the web client for the first time, you must set a password to complete activation of the camera. The default user name is **admin**, which can be changed after you log in.

> **CAUTION** To protect the device, the password must be 8 to 16 characters long and combine at least two of the following character types: uppercase letters, lowercase letters, numbers, and special characters. The password must not be identical to the user name.

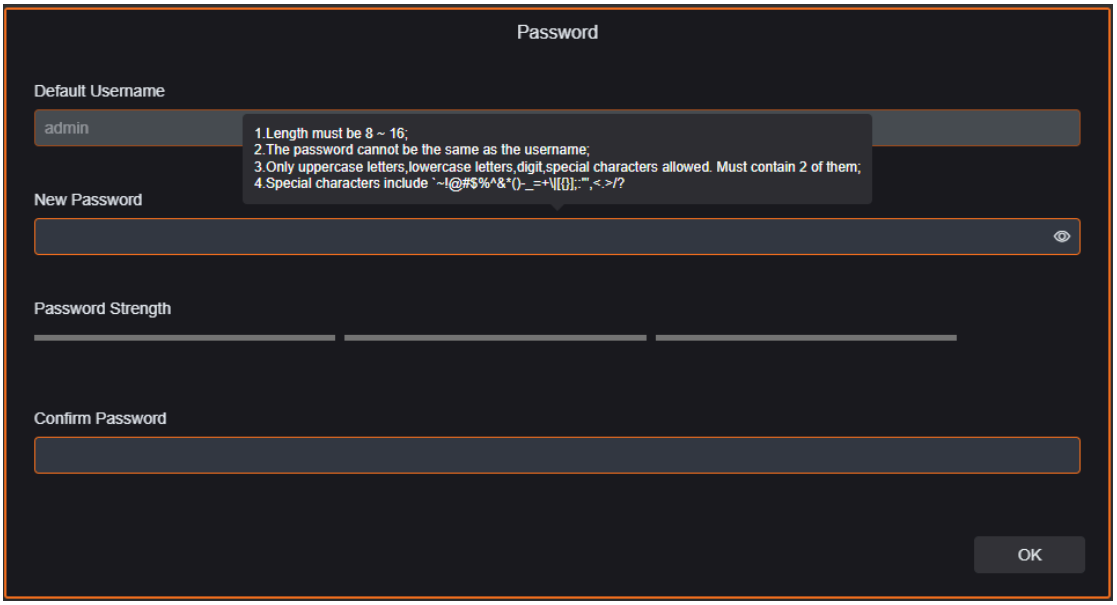

Figure 4-2. Setting the password to activate the camera

After entering a new password, click **OK** to save it. The web client then displays the password recovery configuration screen shown below, where you can set up one or more recovery methods in advance so that the administrator password can be reset if it is ever forgotten.

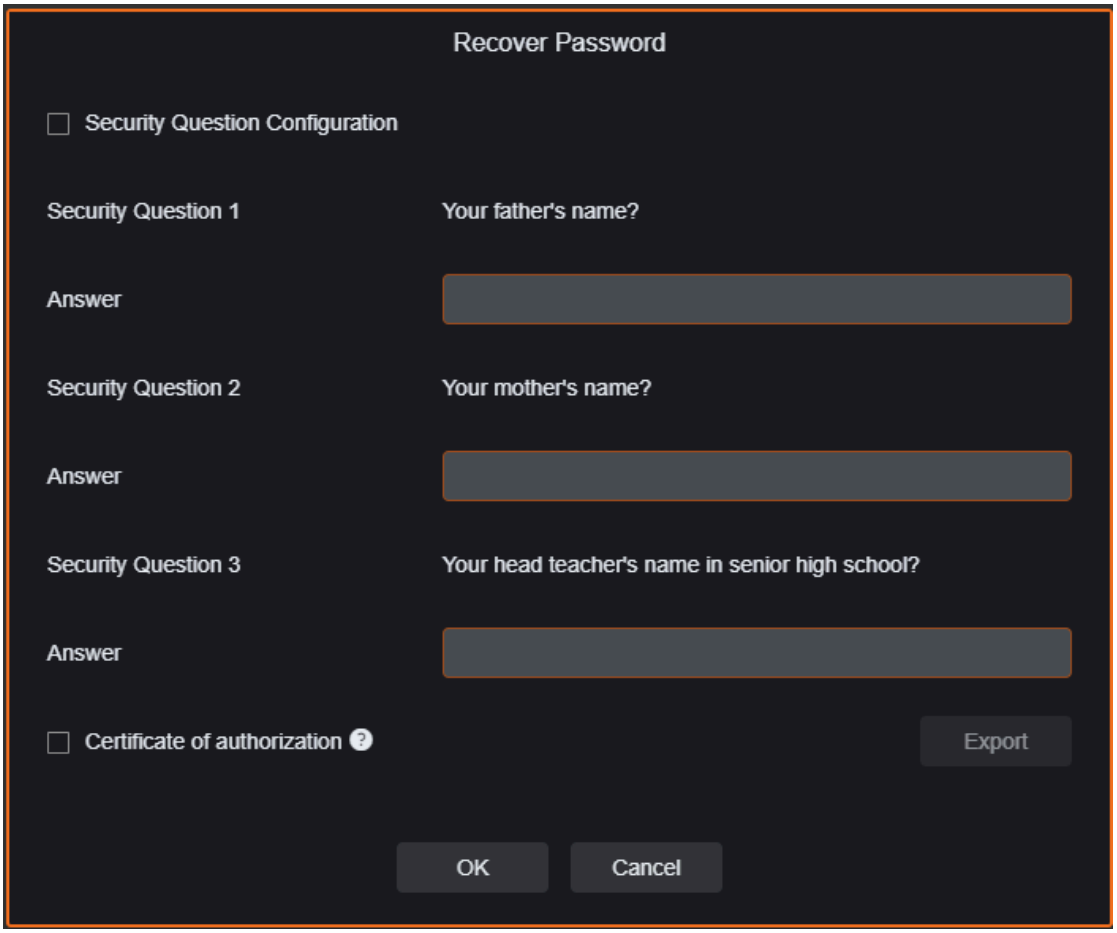

Figure 4-3. Password recovery configuration on first login

Three recovery methods are available:

- **Security Question Configuration** — Used to reset the administrator password by answering preset questions. Choose 3 of the 15 available questions and provide an answer for each. Each answer may be up to 64 characters long.
- **Certificate of Authorization** — Used to reset the administrator password with a key file. When this method is enabled, click **Export** to download the key file, certificate.txt, and store it in a safe location.
- **Super Code** — The recommended recovery method, enabled by default in recent firmware. A one-time super code is derived from the camera MAC address and the camera system time and, once verified, allows the administrator password to be reset. Because the super code is generated by GSD Group technical support, this method provides a reliable way to regain access when the other methods are unavailable.

> **NOTE** When you enable any password recovery method, keep the associated verification information safe and up to date.

4.3 General Login

On subsequent visits to the web client, the login screen shown below is displayed. Enter the account name and password, then click **Login** to open the operation interface of the camera. You can also select the interface language on the login screen.

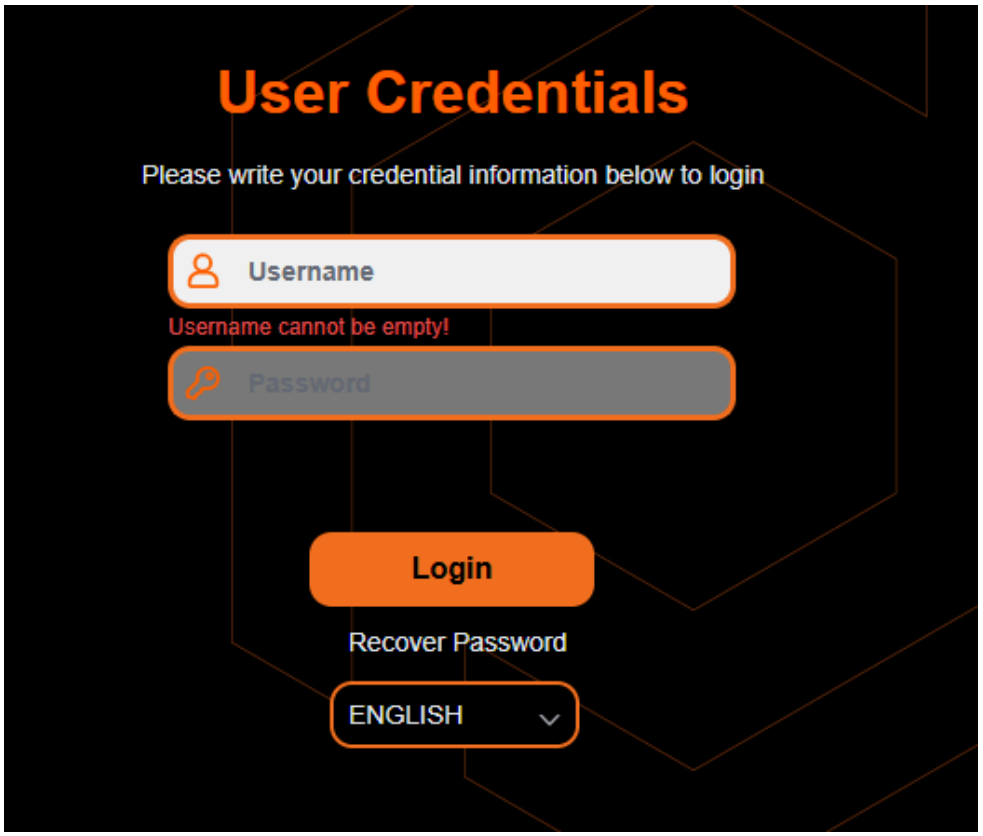

Figure 4-4. Web client login screen

4.4 Recovering a Password

When password recovery has been enabled, you can regain access if you forget the login credentials. On the login screen, click **Recover Password** to open the recovery screen, then use the security question, certificate of authorization, or super code method that you configured at first login.

4.4.1 Security Question

On the **Recover Password** screen, answer the security questions that you configured previously. Once the answers are verified, you can set a new administrator password directly.

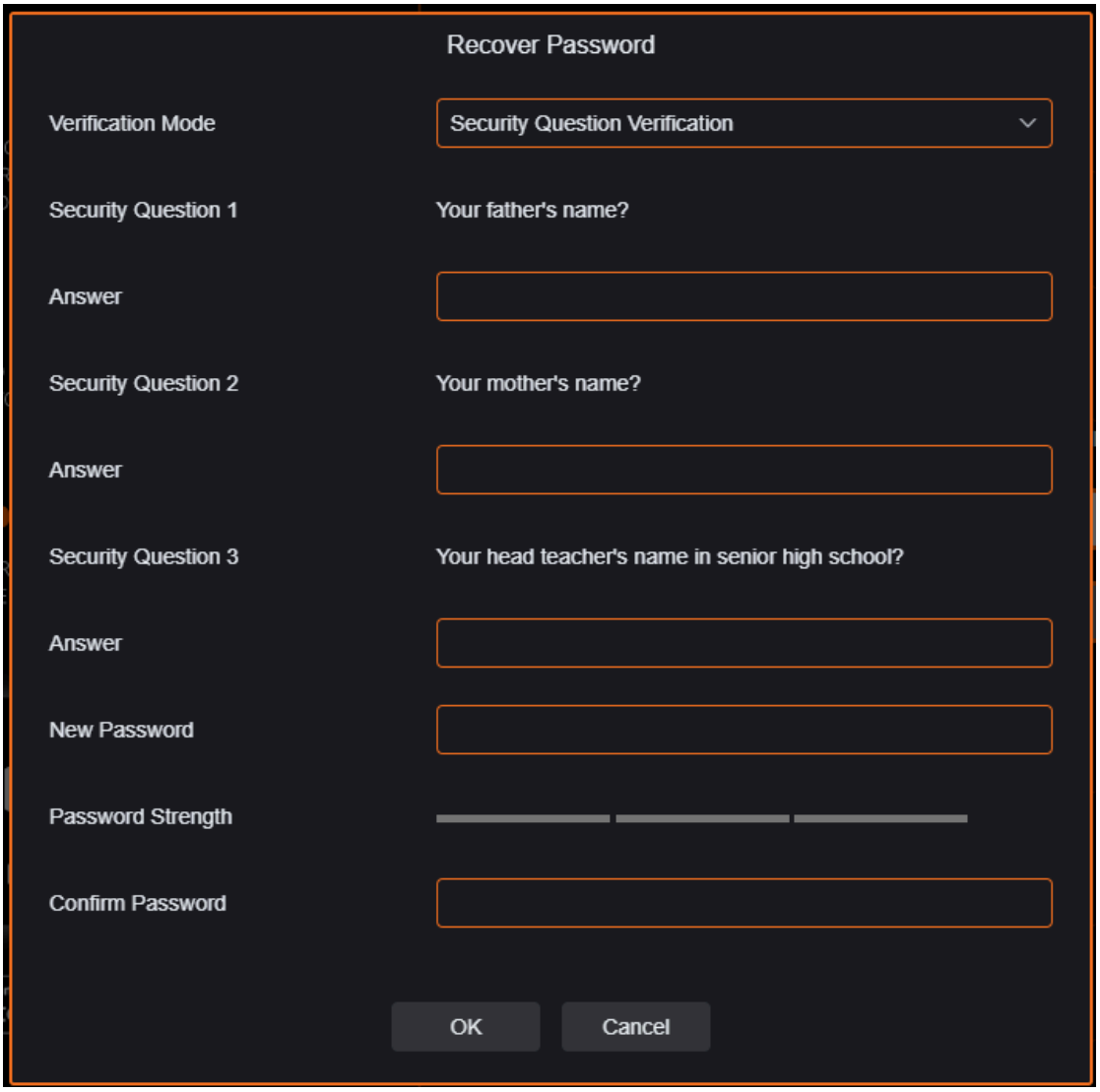

Figure 4-5. Recovering the password with security questions

4.4.2 Certificate of Authorization

On the login screen, click **Recover Password** and switch to the **Certificate of Authorization** method. Load the key file (certificate.txt) that you exported previously to verify your identity, then set a new administrator password.

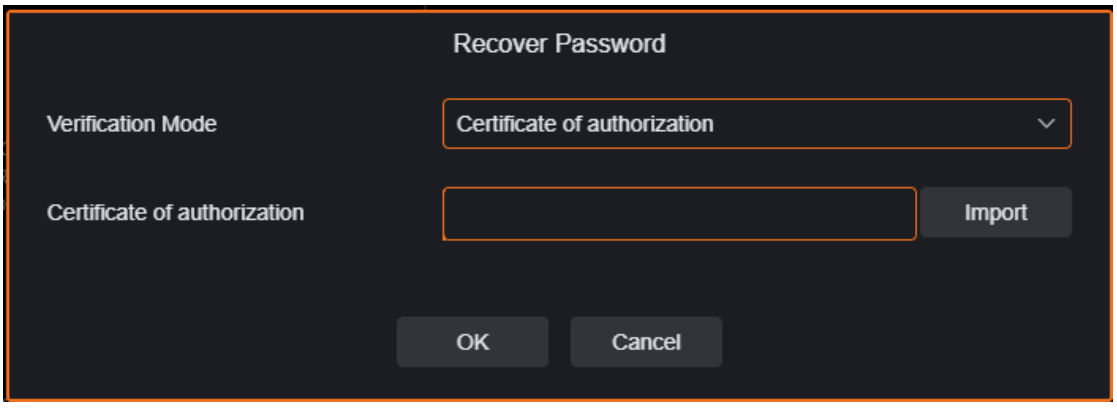

Figure 4-6. Recovering the password with the certificate of authorization

NOTE After the password is reset with this method, the existing key file becomes invalid. Log in again and export a new key file when prompted.

4.4.3 Super Code

On the login screen, click **Recover Password** and switch to the **Super Code** method. The screen changes as shown below. Enter the correct verification code to reset the administrator password. The verification code is calculated by GSD Group technical support using a dedicated tool, based on the camera MAC address and the camera system time.

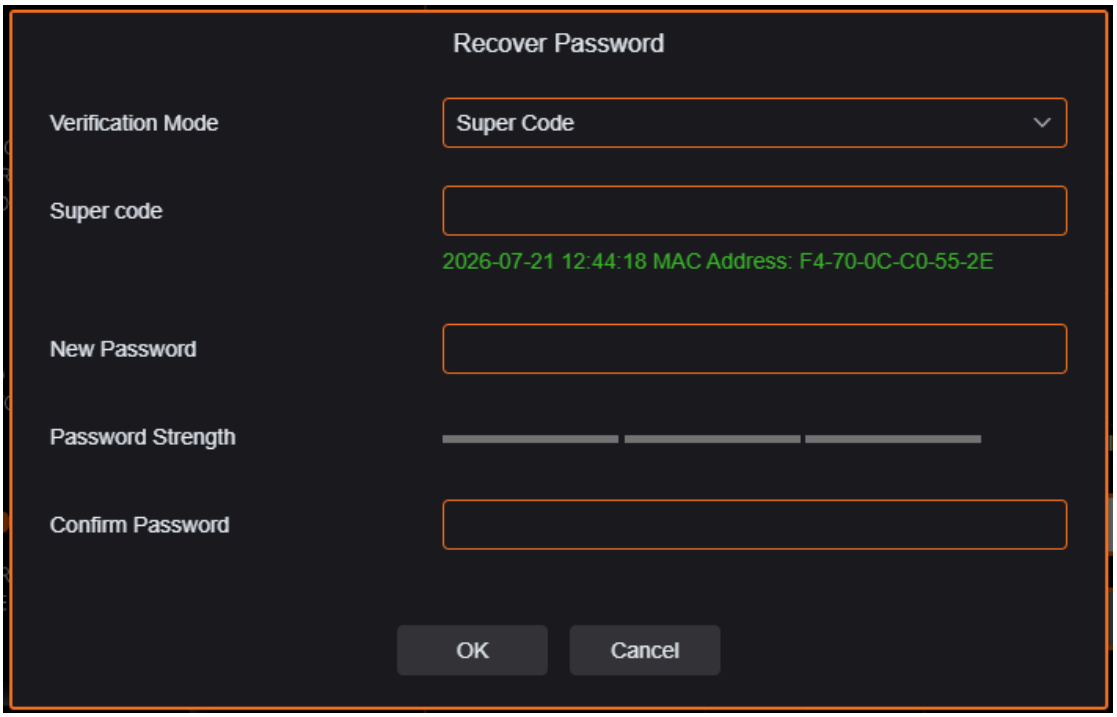

Figure 4-7. Recovering the password with a super code

TIP Super Code is the recommended recovery method and is enabled by default in recent firmware. To obtain a verification code, contact GSD Group technical support with the camera MAC address and system time.

PART II

Live View, Playback & Events

Live preview, recorded video, and event search

Chapter 5 Preview Screen

5.1 Live Menu

After you log in successfully, the OCTAVUE by GSD Group web client opens the live preview interface, shown below. The live view is the default workspace for monitoring the camera and operating its access-control functions.

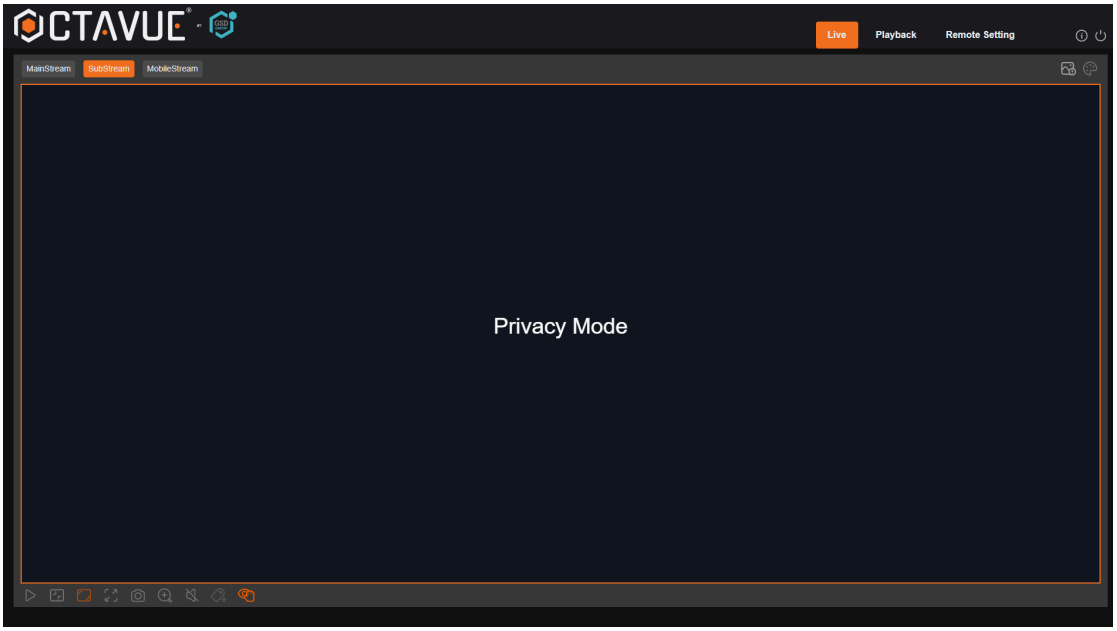

Figure 5-1. Web client live preview interface

NOTE Available functions vary by camera model. The controls described here may differ from those shown on your device; always refer to the actual interface.

The upper-left corner of the window provides the stream and navigation controls:

- **Stream switch menu** — Selects the stream used for the current live view, letting you balance image quality against network and PC load.
- **Main stream** — Delivers a high-definition image, but places higher demands on bandwidth and PC performance.
- **Sub stream** — Places moderate demands on bandwidth and PC performance, with lower image quality than the main stream.
- **Main switch bar** — Switches between the web client function screens. The web client provides four menus: Live, Playback, Remote Setting, and Local Settings.

The live toolbar provides the following controls:

Info — Displays the current logged-in user, the web client version, and the plug-in version.

AI Alarm — Opens the alarm push bar on the right side of the window, which displays the captured images pushed by functions such as face, human-shape, and vehicle detection.

Color — Adjusts image settings such as saturation and sharpness.

- **Exit** — Logs out of the current session.
- **Video Alarm Status** — Indicates the alarm and recording status of the current camera. For details, see Video Status, later in this chapter.

Stop / Play — Starts or stops the preview of the current stream.

Original Proportions — Displays the current preview at its original aspect ratio.

Stretch — Scales the current preview to fill the entire display area.

Full Screen — Displays the current preview in full screen. Double-click the image to toggle full screen, and press Esc to exit.

Record — Manually records the current preview stream.

Capture — Manually captures a still image from the current stream.

Digital Zoom — Electronically magnifies a selected area of the display.

Audio — Turns the preview audio on or off and adjusts its volume.

Voice Intercom — Establishes two-way audio with the camera.

Siren — Manually turns the siren on or off.

Pixel Counter — Draws a selection box to report the pixel dimensions of the selected area within the stream.

- **Pop-up box information** — When certain alarms are triggered, a prompt describing the current alarm appears in the lower-right corner of the window.

Privacy Mode — Turns privacy mode on or off.

Door — Opens and closes the door-control menu.

Unlock / Lock — In the door menu, click Unlock to release the door lock or Lock to secure it.

5.2 Video Status

The video status indicators are on-screen notifications that report the current alert and recording state of the camera. Several alarms can be active at the same time, so more than one indicator may appear together.

Indicator	Meaning
(none)	The SD card is normal, but no recording is in progress.
R	The camera is recording normally.
H	The SD card is in an abnormal state. Check and confirm the SD card.
M	A motion alarm is active, but motion-alarm recording is not enabled.
M	A motion alarm is active and motion-alarm recording is in progress.

I	An I/O alarm is active, but I/O-alarm recording is not enabled.
I	An I/O alarm is active and I/O-alarm recording is in progress.
S	An intelligent alarm is active, but intelligent-alarm recording is not enabled.
S	An intelligent alarm is active and intelligent-alarm recording is in progress.
D	An access alarm (authentication failures reaching the set count, door-open timeout, or a tampering alarm) is active, but alarm recording is not enabled.
D	An access alarm is active and alarm recording is in progress.

NOTE Intelligent alarms include face detection, human-shape detection, and other AI-based detections.

Chapter 6 Playback

Live monitoring alone is not sufficient for an access-control deployment: recorded video must be retained so that events can be reviewed after the fact. The OCTAVUE by GSD Group access control camera stores video to its SD/TF card and provides two complementary retrieval modes — general playback for browsing continuous and event recordings, and smart playback for locating clips in which a person was detected.

6.1 General Playback

General playback combines a conventional video search with AI-assisted image search. Open the playback page and use the video search view shown below to locate and review footage stored on the SD/TF card.

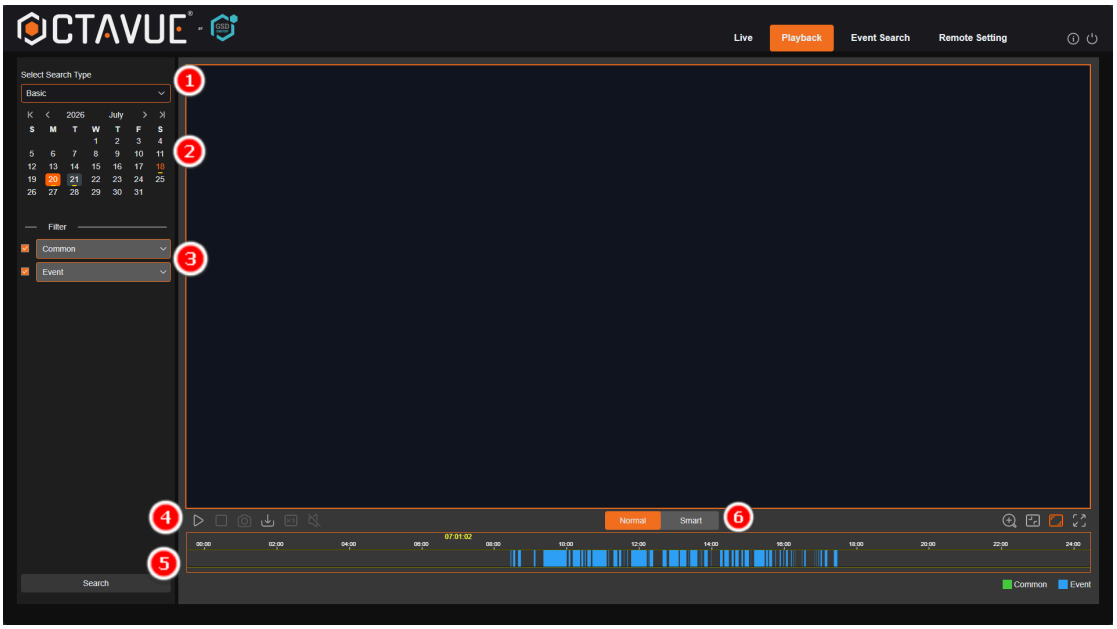

Figure 6-1. General video search interface

The search view exposes the following controls:

- **Search mode switch** — Switches the active search function. The default is General search, which retrieves standard video files. Toggle this control to change to AI image search, described later in this section.
- **Search date** — Sets the date to be searched. Click **Search** to query the SD/TF card; dates that contain recordings are indicated on the calendar.
- **Search type** — Lists the recording types supported by the camera so that only the required footage is displayed. On the timeline, general (continuous) recordings appear in green and event recordings appear in blue.
- **Playback progress bar zoom** — The progress bar shows a 24-hour span by default. Zoom the bar in or out to jump more precisely to a playback position. The mouse wheel performs the same zoom action.
- **Search** — Displays the video stored on the SD/TF card according to the current search settings.
- **Normal / Smart Search** — Switches between normal and smart search. After selecting Smart Search, click the person-type and vehicle-type buttons in the lower-left corner; the recording bar then marks the alarm video triggered by the selected type for that day in blue. This alarm video includes footage that triggered pedestrian detection and motion detection.

6.1.1 Playback Control Toolbar

The toolbar beneath the video window controls the active playback stream.

Pause / Play — Pauses or resumes the playback stream.

Stop — Closes the playback stream.

Forward by One Frame — Advances the playback one frame with each click.

Record — Manually records the current playback stream.

Capture — Manually captures a still image from the current stream.

Download — Downloads the video returned by the current search.

NOTE When a video is downloaded in AVF format, the camera prompts whether the file should be encrypted, as shown below. The AVI and MP4 formats do not display this prompt.

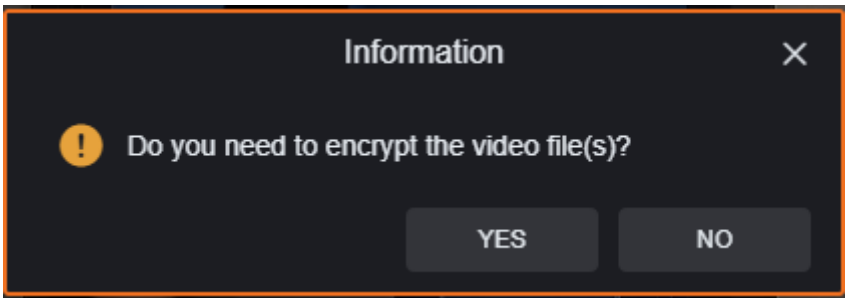

Figure 6-2. Encryption prompt shown when downloading AVF-format video

Speed — Changes the playback speed. Supported rates are 1/8, 1/4, 1/2, 1, X2, X4, X8, and X16.

Audio — Turns the sound of the playback stream on or off and adjusts its volume.

Digital Zoom — Enlarges a selected area of the playback stream.

Original Size — Displays the playback image at its original scale.

Stretch — Scales the playback image to fill the available display area.

Full Screen — Double-click the window to enter or leave full-screen mode. Press Esc to exit full screen.

6.2 Smart Playback

Smart playback is available when you log in through the plug-in-free browser view. It identifies whether an alarm was triggered by a person and marks those periods in blue on the timeline below, allowing you to skip directly to the relevant footage.

Figure 6-3. Smart playback interface

The smart search view exposes the following controls:

- **Search mode switch** — Switches the active search function; here it is set to Smart.
- **Search date** — Sets the date of the smart event to search. Click **Search** to query the card; dates that contain recordings are indicated.
- **Search time** — Sets the time span of the events to search, making it easier to locate a specific period.
- **Search type** — Lists the search types supported by the camera so that only the required footage is displayed.
- **Search** — Click to start the search.
- **Search results display area** — Displays the footage returned by the search.

6.2.1 Playback Control Toolbar

The toolbar beneath the video window controls the active playback stream and the smart detection area.

Pause / Play — Pauses or resumes the playback stream.

Stop — Closes the playback stream.

Capture — Manually captures a still image from the current stream.

Speed — Changes the playback speed. Supported rates are 1/8, 1/4, 1/2, 1, X2, X4, X8, and X16.

Audio — Turns the sound of the playback stream on or off and adjusts its volume.

Smart — Opens the smart-area configuration screen.

All — Sets the entire camera view as the smart detection area.

Delete — Clears the entire smart detection area.

Digital Zoom — Enlarges a selected area of the playback stream.

Original Size — Displays the playback image at its original scale.

Stretch — Scales the playback image to fill the available display area.

- **Full Screen** — Double-click the window to enter or leave full-screen mode. Press Esc to exit full screen.

Chapter 7 Event Search

The OCTAVUE by GSD Group access control camera records every authentication event, captured picture, and AI detection snapshot to the installed SD/TF card together with the associated video. The Event Search interface lets you retrieve these records against precise criteria and play back the recording linked to any result.

Search functions are grouped by type. Use the **text**search mode switch at the top of the interface to move between Access Control Event, Picture, and AI search without leaving the page. Each mode presents the filter fields relevant to that record type; set the fields, click **Search**, and matching results appear in the display area on the right.

7.1 Access Control Event

This interface lists every access authentication event and lets you play back the recording associated with each one.

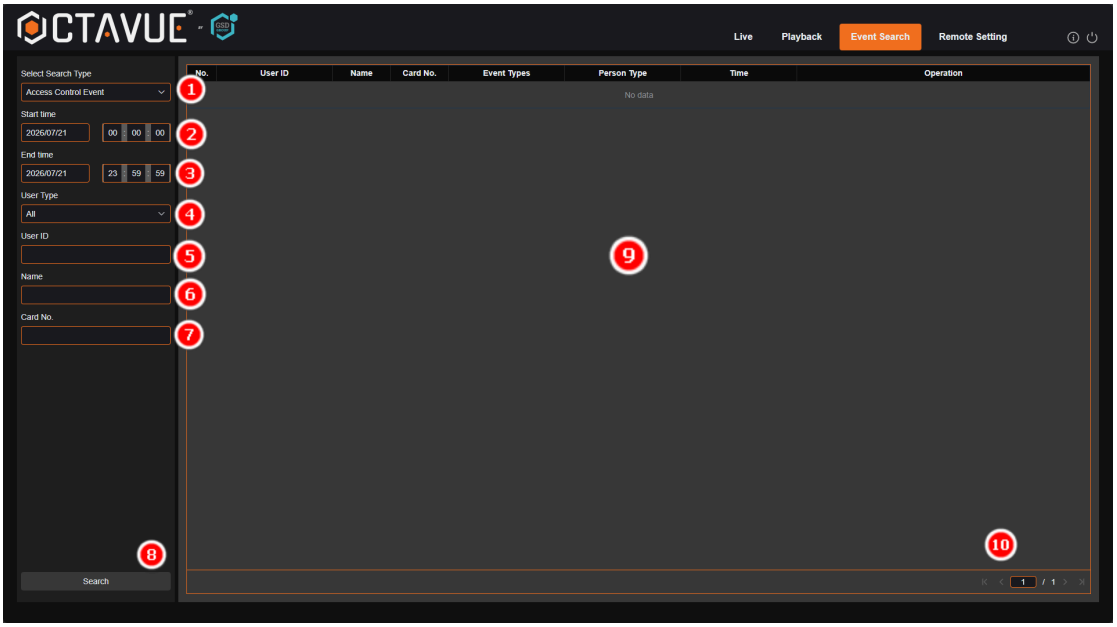

Figure 7-1. Access Control Event search interface

Configure the following fields, then click **Search** to run the query:

- **Search mode switch** — selects the active search function. Access Control Event is the default; in this mode the query returns the video files linked to access authentication events.
- **Start Time** — sets the beginning of the search period.
- **End Time** — sets the end of the search period.
- **User Type** — restricts results to one or more user types. All types are selected by default: administrator, ordinary, guest, and custom users.
- **Name** — enter a user name keyword to filter the results.

- **Card No.** — enter an access card number keyword to filter the results.
- **Search** — starts the query using the criteria above.
- **Search results display area** — lists the events that match the criteria. Each row corresponds to one authentication event and its recording.

Within a result row, click the playback button to open the recording for that event:

Play back the recording associated with the selected event.

- **Search results page** — the pager in the lower-right corner lets you move through multiple pages of results.

7.2 Picture

Use this interface to search captured pictures and play back the video surrounding them.

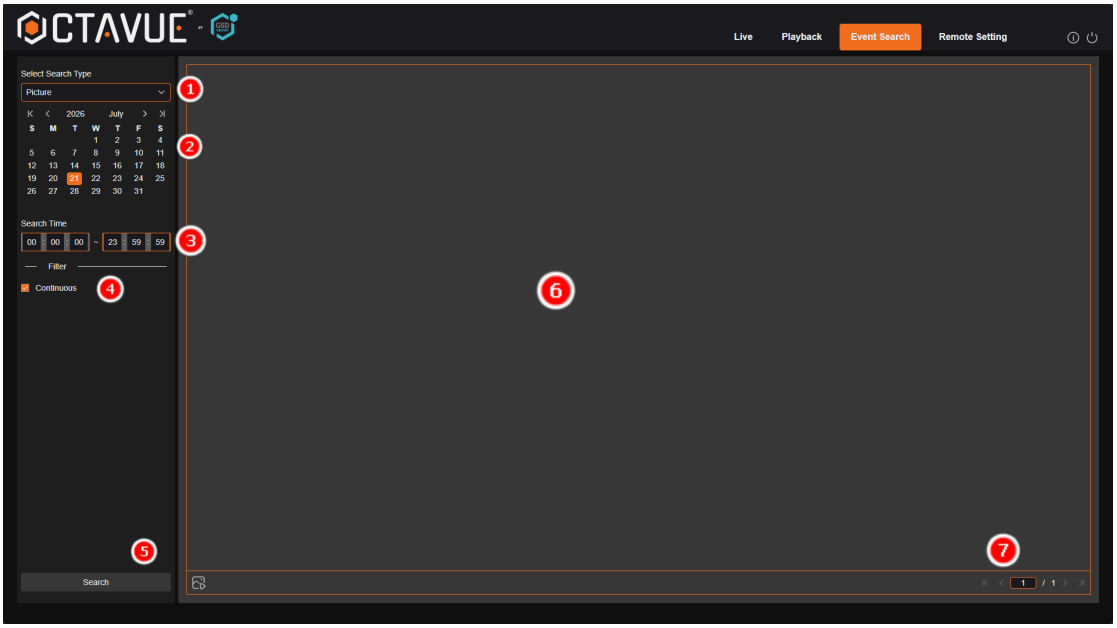

Figure 7-2. Picture search interface

Set the following fields, then click **Search**:

- **Search mode switch** — set to Picture to search captured images.
- **Search date** — sets the date to search. After you click Search, the dates that contain captured files are indicated.
- **Search time** — sets the time range so you can retrieve pictures from a specific period.
- **Search type** — selects the type of image capture to search. All types are selected by default.
- **Search** — starts the picture search.
- **Search results display area** — displays the pictures that match the criteria. Double-click a picture to play the video from the period immediately before and after it.
- **Search results page** — the pager in the lower-right corner lets you move through the results.

7.3 AI

AI search retrieves the face and pedestrian snapshots produced by the camera's recognition functions, letting you locate the corresponding recording from a snapshot.

7.3.1 Face Detection

When the camera performs face recognition, it stores each captured face and its related image information on the SD/TF card. During a search you can quickly retrieve a face snapshot that meets your criteria and jump to the recording associated with it. The Face Detection playback interface is shown below.

Figure 7-3. Face Detection search interface

Configure the search and comparison controls as needed:

- **Search mode switch** — set to Face Detection.
- **Start Time** — sets the start of the period to search for captured faces.
- **End Time** — sets the end of the period to search for captured faces.
- **Face Attribute** — cleared by default. When enabled, the search returns only faces captured while face feature detection was active. The firmware recognizes five face attributes: gender, age, mask, glasses, and expression.
- **Search** — searches for face data according to the current settings.
- **Add** — adds a reference image to the comparison area. You can add both local images and captured images.
- **Delete** — removes the currently added images.
- **Similarity** — sets the minimum feature-value similarity a face must reach to be treated as a match when using the Compare function.
- **Compare** — searches for captured faces using the selected search time, the group in which the captured images reside, and the selected reference face image.
- **Add image display area** — shows the reference images currently added and available for comparison.
- **Search result display area** — on the right, displays the images returned by Search and Compare. Double-click a picture to play the video from before and after it.

> **NOTE** Compare matches captured faces against your reference images by feature-value similarity. Lowering the **Similarity** threshold returns more candidate matches but increases the chance of false results; raise it to prioritize precision.

7.3.2 Pedestrian

When the camera performs pedestrian recognition, it stores each captured pedestrian and its related image information on the SD/TF card. During a search you can quickly retrieve a pedestrian snapshot that meets your criteria and jump to the recording associated with it. The pedestrian search playback interface is shown below.

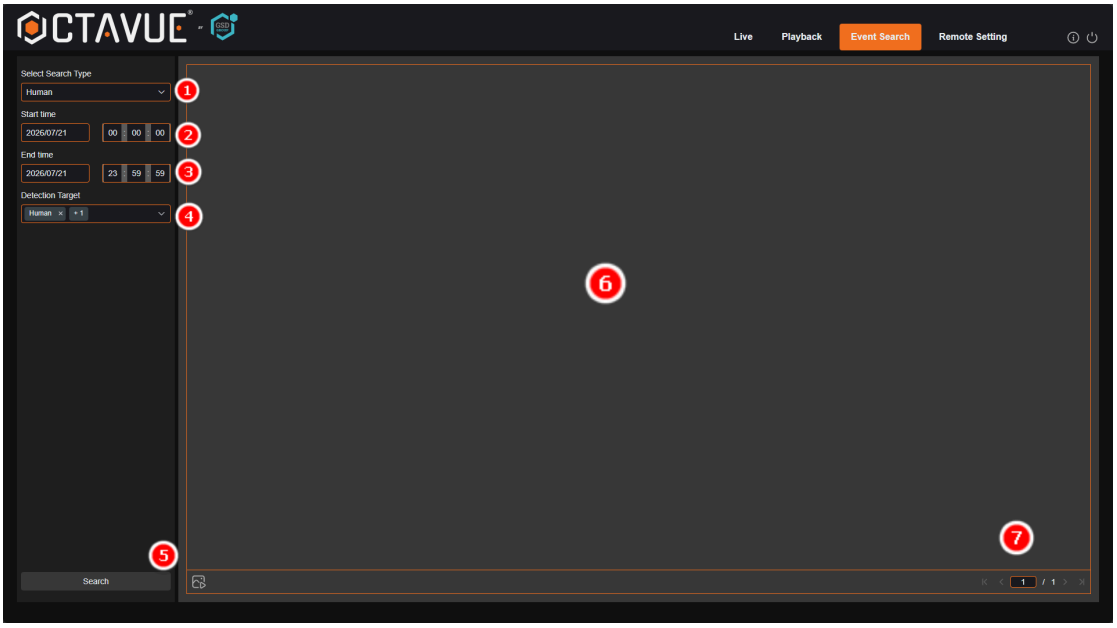

Figure 7-4. Pedestrian search interface

Set the following fields, then click **Search**:

- **Search mode switch** — set to Pedestrian.
- **Start Time** — sets the start of the period to search for pedestrian images.
- **End Time** — sets the end of the period to search for pedestrian images.
- **Detection Target** — selects the human images to include as needed.
- **Search** — searches for pedestrian images according to the current settings.
- **Search results display area** — displays the matching results. Double-click a picture to play the video from before and after it.
- **Search results page** — the pager in the lower-right corner lets you scroll through the results.

PART III

Camera Configuration

Image, recording, alarms, events, and network settings

Chapter 8 Image & Encoding

This chapter describes the image and encoding settings available under the remote configuration menu of the OCTAVUE access control camera. From these pages you can adjust the live preview overlay, tune the image processing pipeline, define the recording and encoding streams, manage audio, and configure automatic image capture.

8.1 Preview

The Live page configures the channel name and the on-screen display (OSD) position for the camera, as shown below.

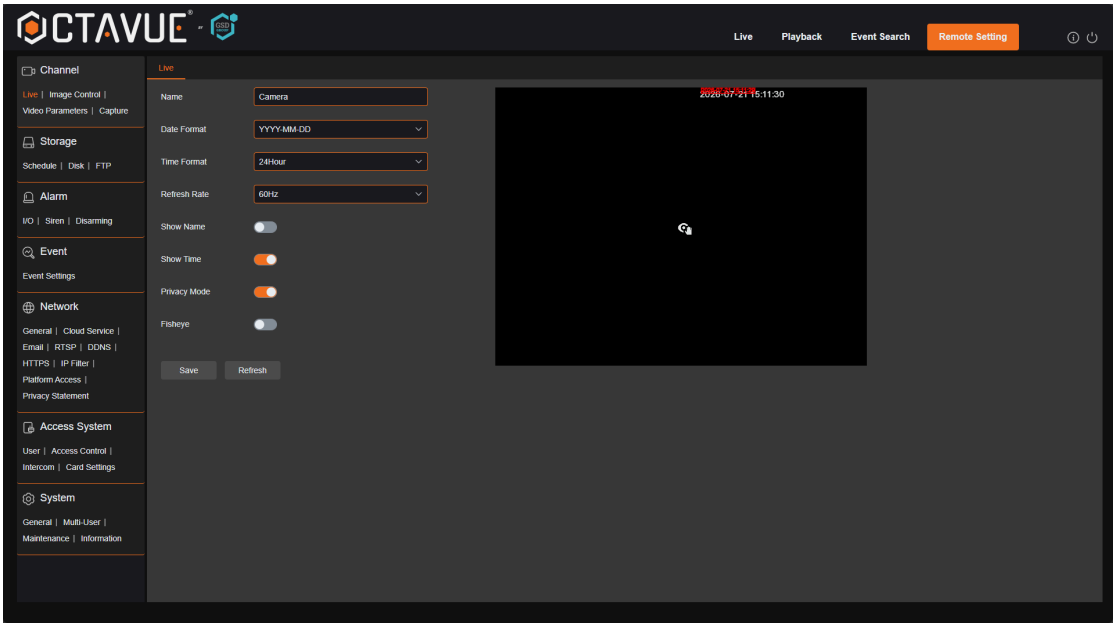

Figure 8-1. Live preview and OSD configuration

Configure the following parameters:

- **Channel Name**: Sets the name of the camera channel.
- **Date Format**: Sets the date format shown in the camera OSD. Available options are MM/DD/YYYY, YYYY-MM-DD, and DD/MM/YYYY.
- **Time Format**: Sets the time format shown in the camera OSD, either 12-hour or 24-hour.
- **Refresh Rate**: Sets the camera refresh rate. Two options are available, 60Hz and 50Hz, corresponding to N and P modes respectively.
- **Show Name**: Displays the camera channel name in the preview. Disabled by default.
- **Show Time**: Displays the camera time in the preview.

- **Privacy Mode**: When enabled, no images are shown in preview or playback, and the settings pages do not display a preview image.
- **Lens Distortion**: When enabled, the image is displayed in fisheye preview mode. When disabled, distortion is corrected and the image fills the entire display area. Disabled by default.
- **Display Channel Name Position**: Sets where the channel name appears by dragging its position on the image.
- **Show Time Position**: Sets where the time appears by dragging its position on the image.
- **Save**: Saves the current changes.
- **Refresh**: Reloads the current page parameters.

CAUTION Enabling **Privacy Mode** suppresses all live and recorded video, including on the configuration pages. Use it only when you intend to disable image capture entirely.

8.2 Image Controls

The Image Controls page modifies image-processing parameters directly, including the color-to-black-and-white mode, wide dynamic range, and backlight compensation, as shown below.

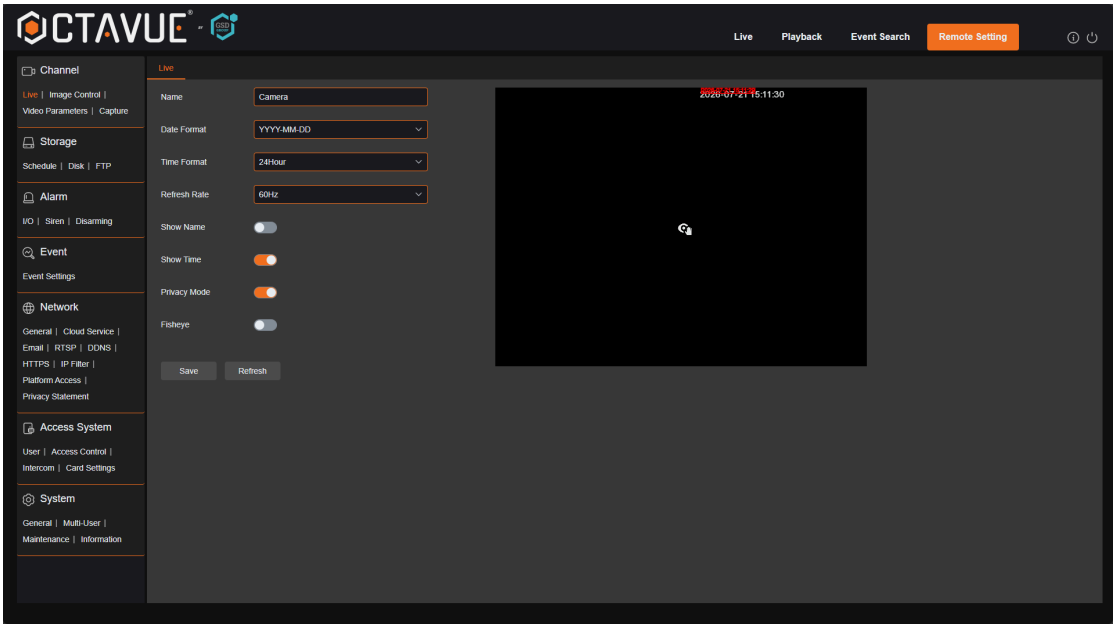

Figure 8-2. Image control parameters

- **IR-CUT Mode**: Sets the camera image mode. Four modes are available:
- **Color Mode**: The image remains in color and does not switch to black and white.
- **Black White Mode**: The image remains in black and white and does not switch to color.
- **Image Mode**: Switches between color and black and white based on the image itself.
- **Schedule**: Switches between color and black and white on a schedule. To use this mode, set the start and end times for entering night vision.
- **IR LED Control**: Sets the night-vision behavior of the camera's infrared fill light. Three modes are available:
- **Smart IR**: Dynamically adjusts the infrared illumination intensity based on factors such as focal length and whether the image is overexposed.
- **Manual**: Sets the infrared fill-light brightness manually.
- **Low Beam Light**: Manually adjusts the infrared lamp brightness (0 to 100). A value of 0 turns the lamp off, and 100 sets maximum brightness.
- **Anti-Overexposure**: When enabled, prevents overexposure of the image in high-brightness environments across all image modes.

- **Exposure Compensation**: Sets how the camera behaves in backlit conditions. Four modes are available:
- **WDR**: Wide Dynamic Range balances the image uniformly according to the setting so that both bright and dark areas remain clearly distinguishable. Referred to as DWDR on some models.
- **HLC**: Highlight compensation makes objects in high-light areas clearer according to the configured HLC Level. Not supported on some models.
- **Back Light**: Makes dark areas of the image clearer according to the configured BLC Level and BLC Area.
- **Disable**: No exposure compensation is applied to the image.
- **White Balance**: Sets white balance. Two modes are available. **Automatic** adjusts white light using default parameters, while **Manual** lets you set the combined red, green, and blue gain directly.
- **Shutter**: Sets the shutter exposure length. On models that support aperture control, **Automatic** selects an appropriate exposure time and aperture value within the configured Time Exposure and Iris ranges, while **Manual** uses the configured values directly. **Shutter First** derives the aperture value from a manually defined shutter, and **Iris First** derives the shutter value from a manually defined aperture. Models without aperture support offer only automatic and manual modes.

> **NOTE** In shutter manual mode the exposure time removes the flickerless option, whereas in shutter automatic mode the flickerless option is enabled. If you switch back to manual mode, the exposure time is automatically set to 1/100 or 1/120.

- **Exposure Time**: Sets the camera exposure time, used together with **Shutter**. A long exposure time overexposes the image, while a short exposure time darkens it.
- **Defog Mode**: When enabled, makes the image clearer in rainy or foggy conditions.
- **3D Noise Reduction**: Reduces image noise for a clearer picture. Three modes are available: **Automatic** selects the noise-reduction level algorithmically, **OFF** disables noise reduction, and **Manual** applies a manually set noise-reduction coefficient.
- **Save**: Saves the image control parameters.
- **Default**: Restores the image control parameters to their defaults.
- **Refresh**: Reloads the image parameters.

8.3 Video Parameters

This menu configures the parameters used for screen preview and recording.

8.3.1 Record Parameters

This section configures parameters related to system recording.

- **Stream Mode**: Selects the stream that is recorded to the SD card. Defaults to the main stream.
- **Record**: Select to enable recording.
- **PreRecord**: When enabled, the camera begins recording a few seconds before an alarm event. This option is recommended when recording is primarily triggered by motion detection or I/O alarms.
- **Netbreak**: When enabled, events continue to be recorded even when the network is down or the connection fails.

8.3.2 Encoding Parameters

This section configures the image-quality parameters for recorded video and network transmission. The Main Stream typically defines the quality of the video recorded to the HDD. The Sub Stream defines the quality of the preview video accessed remotely, for example by web clients and VMS. The Mobile Stream, which can optionally be disabled, defines the quality of the preview viewed remotely from a mobile device.

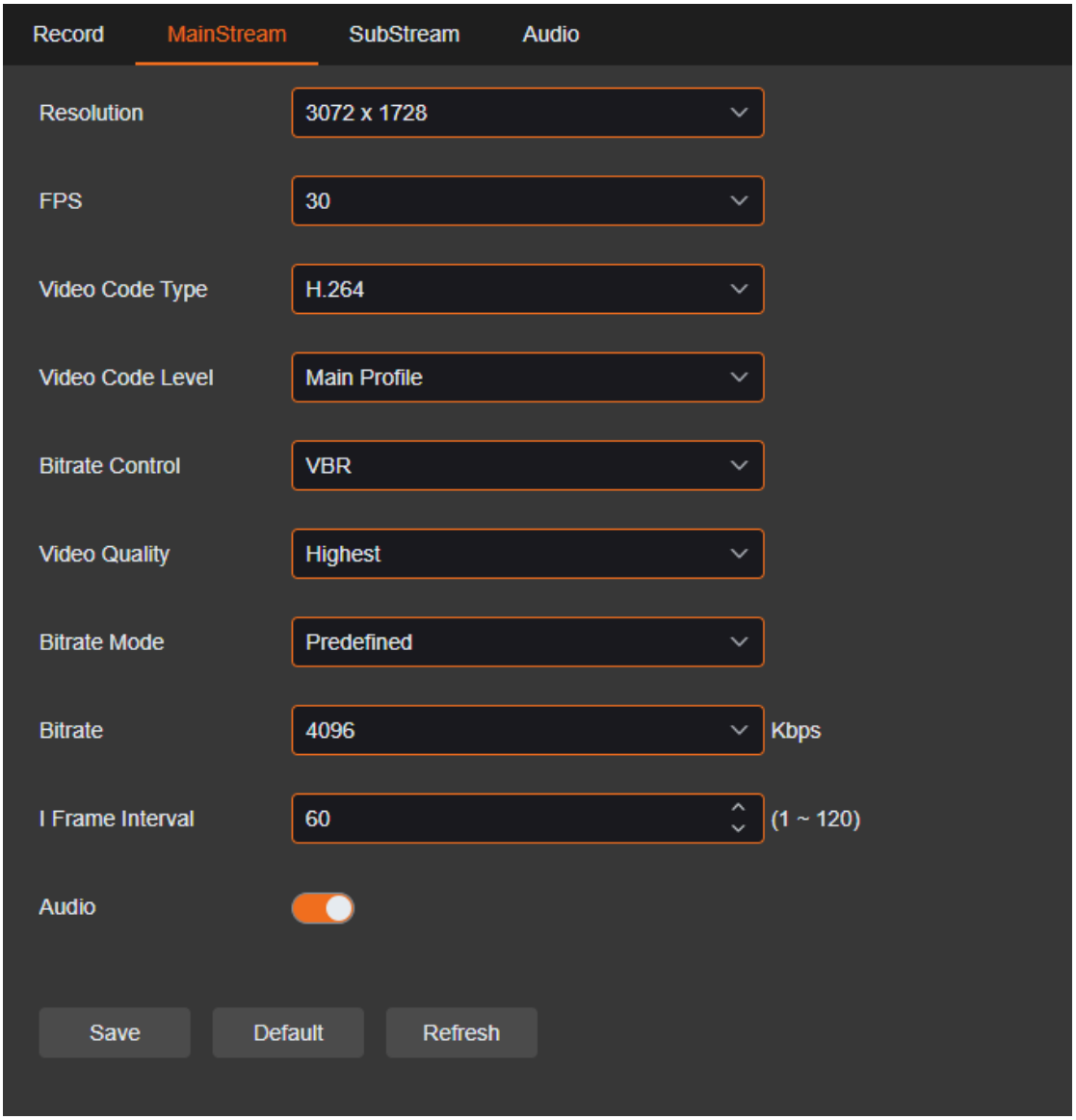

Figure 8-3. Encoding parameters for the main, sub, and mobile streams

- **Resolution**: Indicates the resolution of the recorded image.
- **Frame Rate**: Indicates the number of frames per second recorded by the camera.
- **Encoding Format**: Sets the channel encoding type. Options are H.264, H.265, H.264+, H.265+, and MJPEG. MJPEG is available only in sub-stream mode.
- **Video Code Level**: Sets the video quality level: Baseline, Main Profile, or High Profile. Main Profile is available only with H.265.
- **Encoding Mode**: Selects the bitrate control method. Constant Bit Rate (CBR) is suitable for simple scenes such as a plain wall, while Variable Bit Rate (VBR) is suitable for more complex scenes such as busy streets.
- **Config Mode**: Select **User Defined** to set the bitrate manually, or **Preset Mode** to choose a preset bitrate.
- **Bitrate**: Corresponds to the data transfer rate the camera uses to record video. A higher bitrate yields better video quality.
- **I Frame Interval**: Sets the camera's I-frame interval.
- **Audio**: Enable this option to record audio and video simultaneously. It requires a microphone connected to the camera or a camera with built-in audio.
- **Save**: Saves the encoding parameters.
- **Default**: Restores the encoding parameters to their defaults.
- **Refresh**: Reloads the encoding parameters.

8.3.3 Audio Management

This section configures the camera's audio input and output.

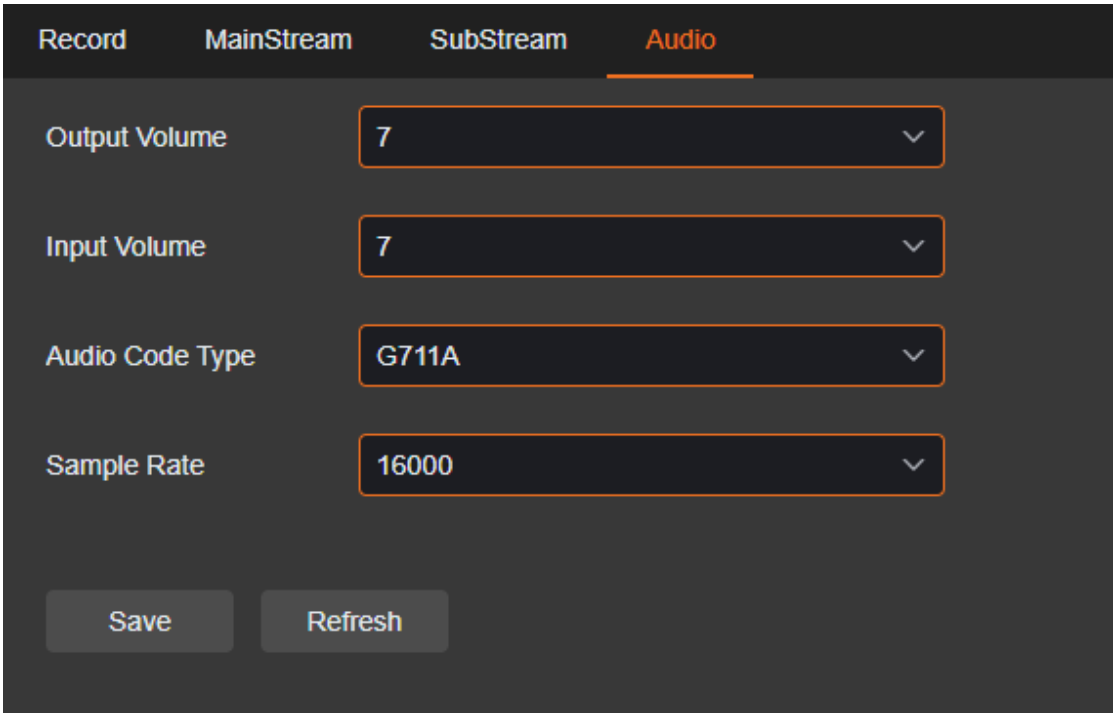

Figure 8-4. Audio management settings

- **Output Volume**: Sets the volume of the audio output.
- **Input Volume**: Sets the volume of the audio input.
- **Audio Code Type**: Sets the audio encoding type. G.711A and G.711U are supported.
- **Sample Rate**: Sets the audio sampling rate. 8000 and 16000 are supported.

8.4 Capture Settings

This menu configures the parameters for the automatic image capture function.

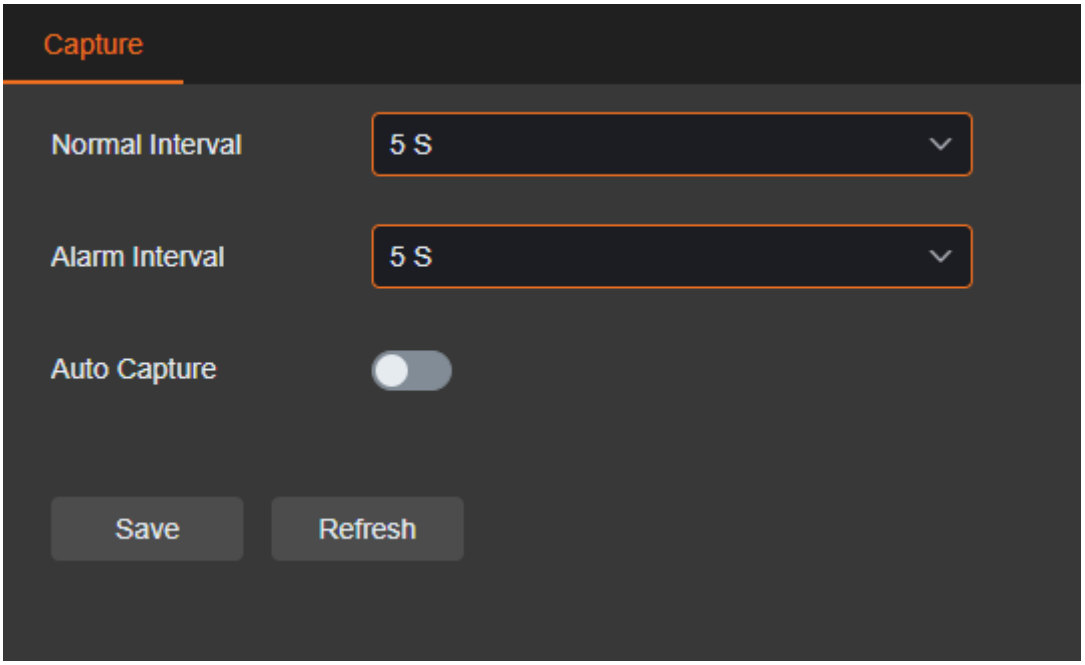

Figure 8-5. Automatic capture settings

- **Normal Interval**: The interval between captures during normal recording.
- **Alarm Interval**: The interval between captures when a motion detection or I/O alarm is triggered.
- **Auto Capture**: Enables or disables automatic capture.

Chapter 9 Recording, Storage & FTP

This chapter explains how to control when the OCTAVUE access control camera records video and captures still images, how to manage the storage media that hold those files, and how to forward alarm media to an external FTP server. Together these settings determine what the camera saves, where it is saved, and how it is delivered.

9.1 Schedule Settings

Schedules define the periods during which the camera performs continuous, motion-triggered, or I/O-triggered actions. Both recording and image capture are governed by their own independent schedules.

9.1.1 Record Schedule

Use the record schedule to configure regular and alarm recording over a defined weekly period. Recording is disabled by default; a schedule must be enabled before the camera will store video.

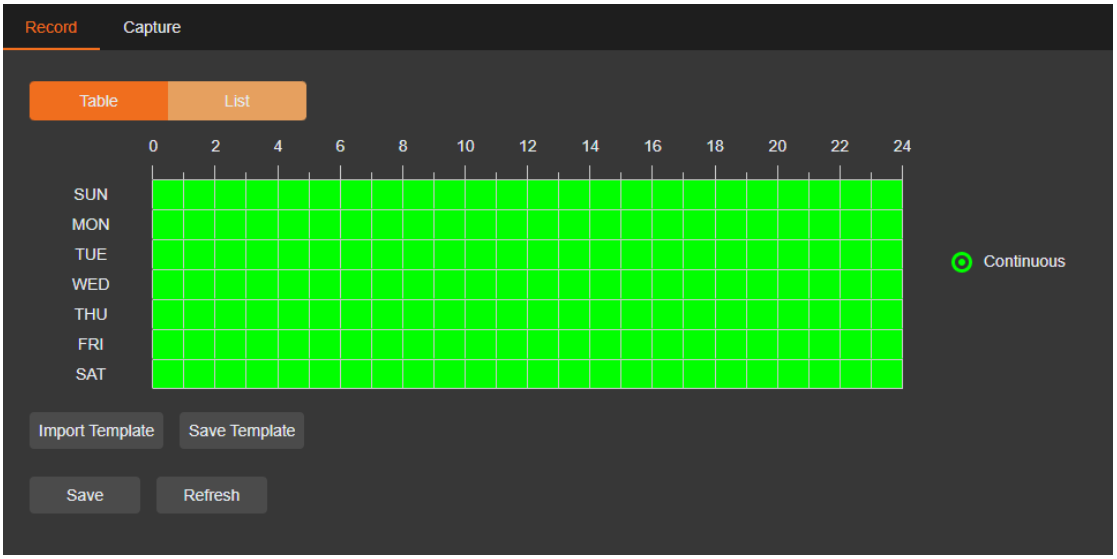

Figure 9-1. Record schedule shown in table view

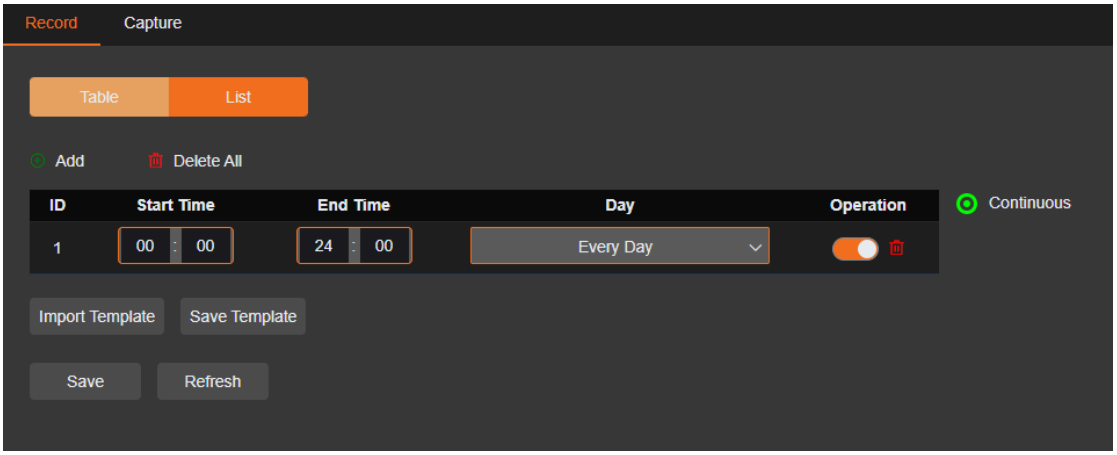

Figure 9-2. Record schedule shown in list view

The schedule can be defined in either **Table** or **List** view. Use the selector at the right of the **Normal**, **Motion**, and **I/O** entries to switch the video type whose schedule you are editing.

- **Table view**: drag across the grid, or select the individual time cells, to mark the periods when the chosen recording type is active.
- **List view**: add rules manually and enter a start and end time for each, defining the active period explicitly.

The following controls are available when building a schedule:

- **Add**: create a new schedule rule.
- **Delete All**: remove every schedule rule.
- **Start Time**: set the time at which the rule takes effect.
- **End Time**: set the time at which the rule ends.
- **Day**: select the day or days on which the rule applies.
- **Import Template**: apply a custom or system-default schedule template to the current settings.

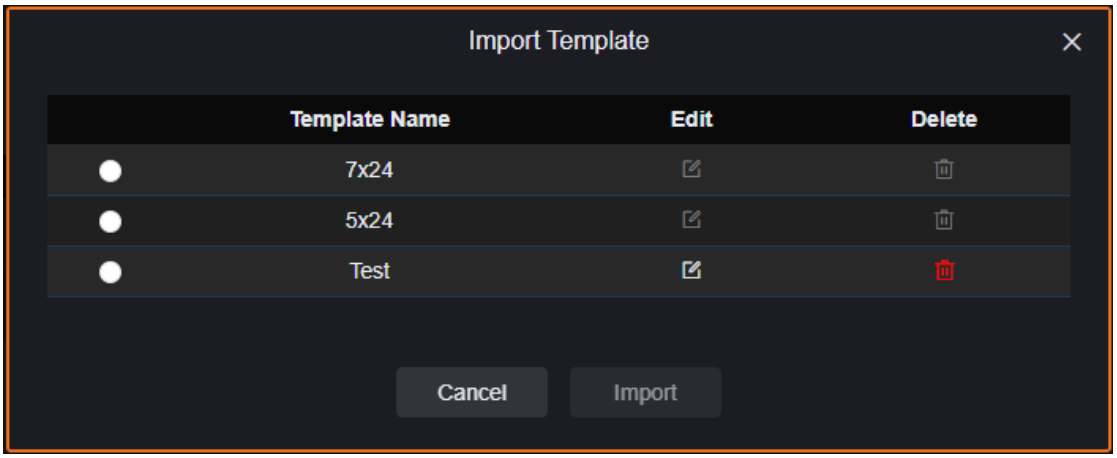

Figure 9-3. Importing a schedule template

Templates let you reuse a schedule across pages and channels. The following template controls are available:

- **Edit**: modify a template, including its name and its individual rules.
- **Delete**: remove a template.

> **NOTE** The system provides two built-in templates, **7×24** and **5×24**. These default templates can be edited but not deleted.

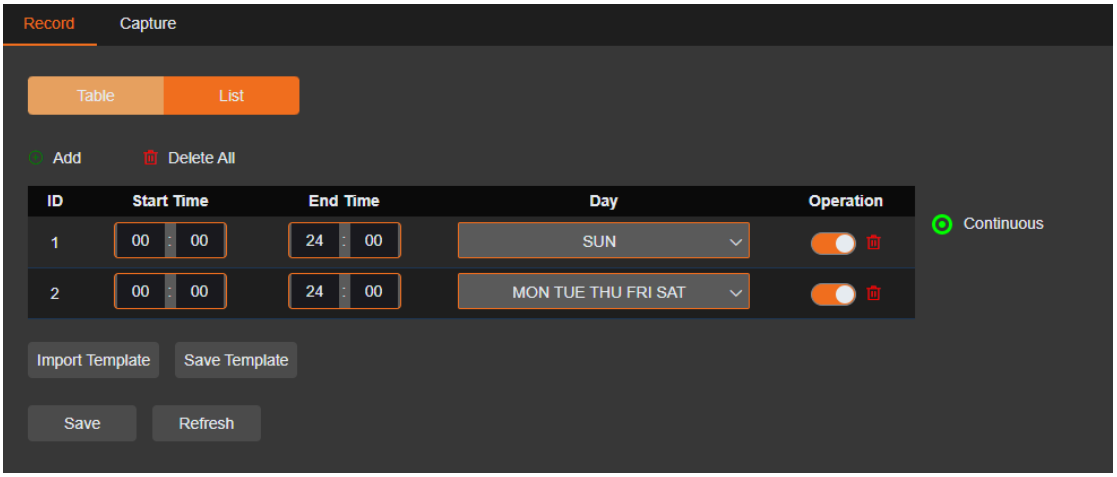

Figure 9-4. Selecting a built-in schedule template

Use **Save the Template** to store the current set of rules as a custom template. Once saved, the template can be imported on other settings pages, such as the capture schedule.

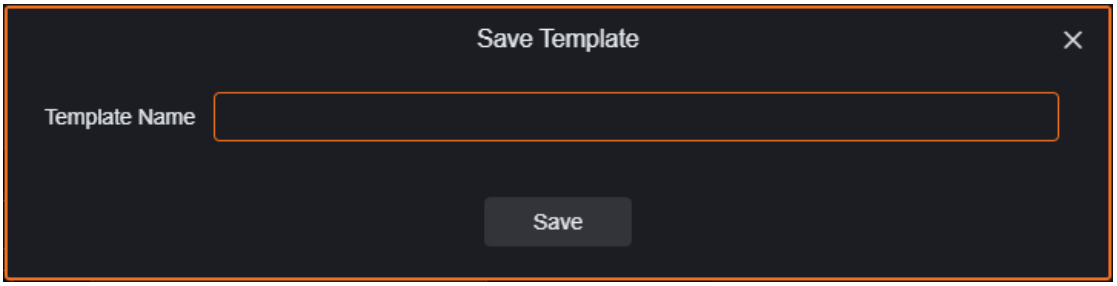

Figure 9-5. Saving a custom schedule template

When the schedule is complete, use the following controls to store and distribute it:

- **Save**: save the edited parameters.
- **Copy**: copy the parameters to one or more other channels.
- **Refresh**: reload the current parameters from the camera.

9.1.2 Capture Schedule

The capture schedule controls when the camera records still images. Set up regular and alarm capture periods so that the camera performs capture actions only during the times you define. The capture schedule is configured in the same way as the record schedule described above, using the same table and list views, templates, and controls.

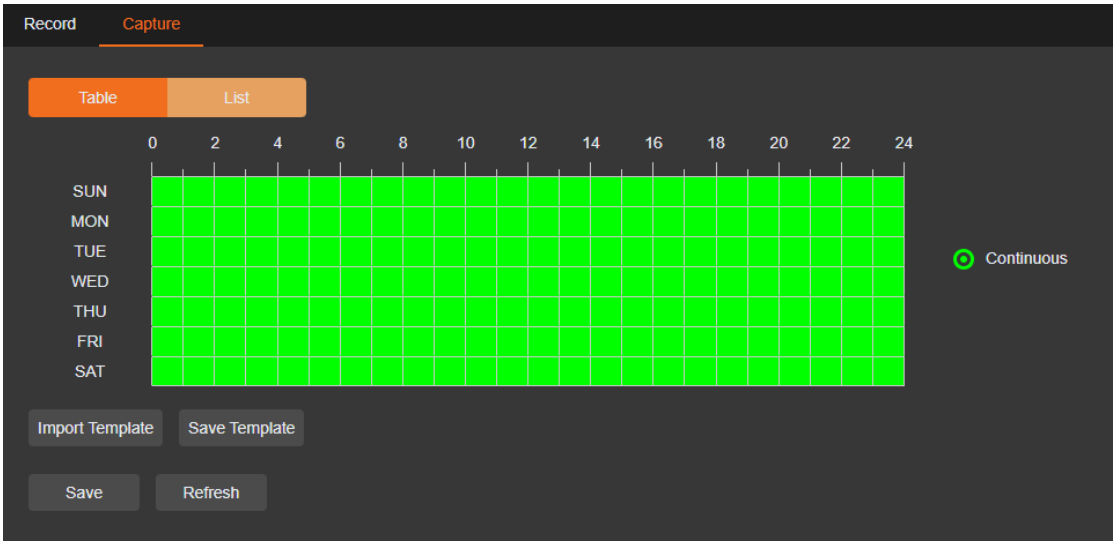

Figure 9-6. Capture schedule shown in table view

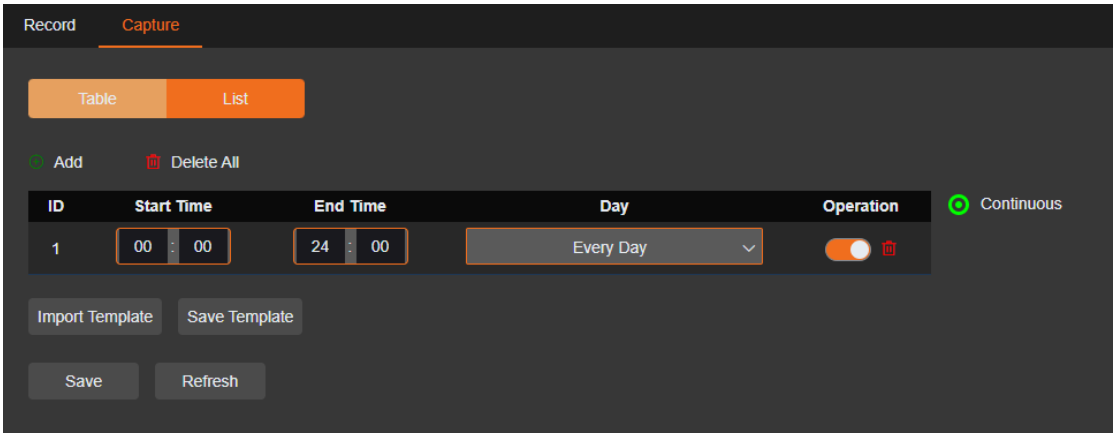

Figure 9-7. Capture schedule shown in list view

9.2 Disk Management

Disk management lets you inspect and configure the storage that holds recorded video and captured images, including the internal TF card and an optional network hard disk.

The internal TF card must be formatted before first use and again whenever it is replaced with a new card. From this menu you can review the status of the card and format it as required.

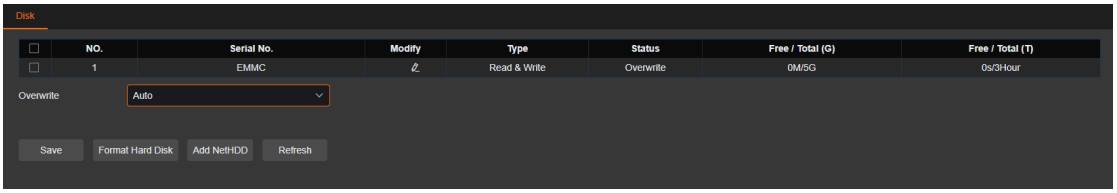

Figure 9-8. Disk management page

Select **Format Hard Disk** to format the TF card. A window appears prompting you to choose which partition or partitions to format; make your selection, enter your user name and password, and confirm to begin.

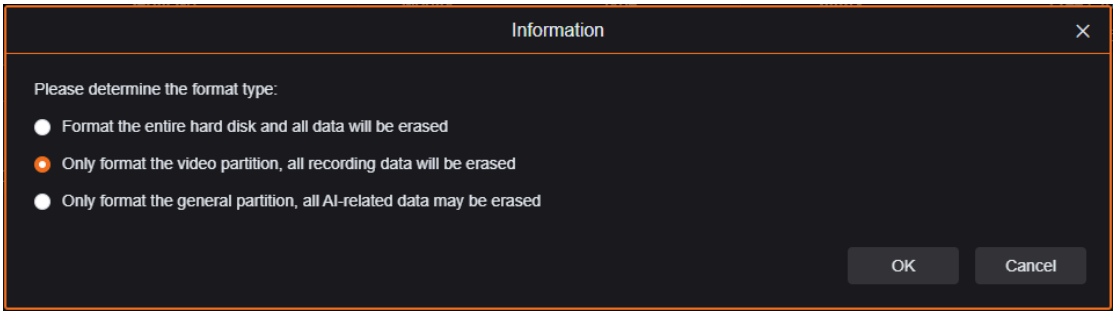

Figure 9-9. Selecting the partition to format

CAUTION Formatting permanently erases data and cannot be undone. Formatting the entire disk removes all partitions and clears all video and database content, including the AI face database; formatting only the video partition erases all recording data. Back up any files you need before you format.

The following formatting options are available:

- **Format the hard disk and all data will be erased**: formats every partition, including the video partition and the general partition, clearing all video and all database content.
- **Only format the video partition**: erases all recording data while leaving the general partition intact.
- **Only format the general partition**: formats the general partition and clears the database, leaving recorded video intact.

The **Overwrite** setting controls what happens when the TF card becomes full. When set to **Auto**, the oldest data is overwritten automatically as space is needed. When set to **Off**, no existing video is overwritten; in this case, check the card status periodically to ensure it does not fill up.

Use **Add NetHDD** to add a network hard disk (NAS). Once a NAS is configured and connected to the network, the camera can record channel video and capture images to it. The AI face database can be stored only on a hard disk.

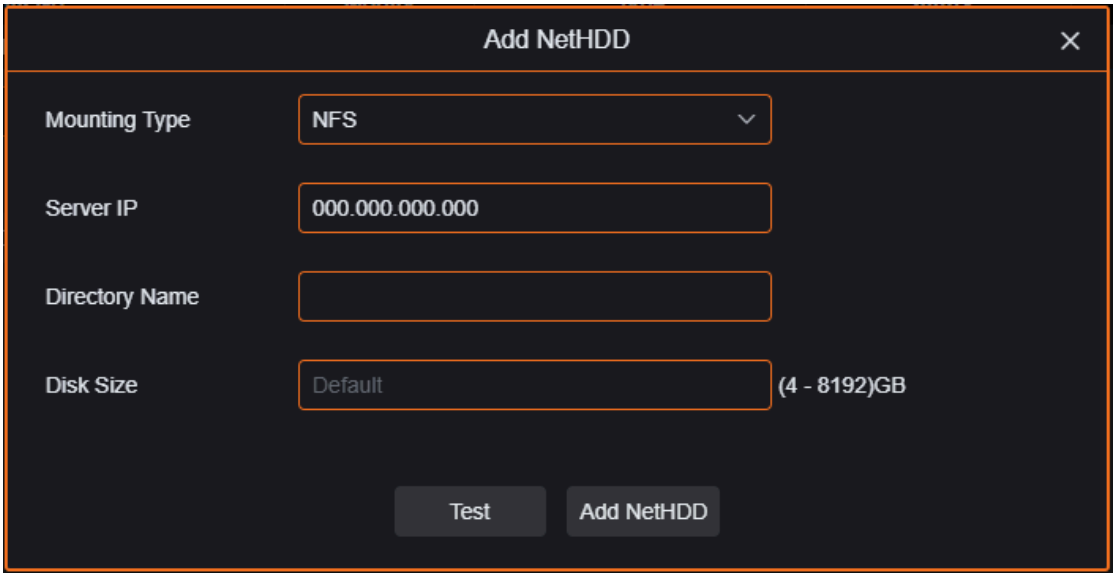

Figure 9-10. Adding a network hard disk (NAS)

Configure the network hard disk using the following fields:

- **Mounting type**: select the protocol, either **NFS** or **SMB/CIFS**. NFS does not require a user name and password; SMB/CIFS does.
- **User Name**: the NAS user name (not used in NFS mode).
- **Password**: the NAS password (not used in NFS mode).

- **Server IP**: the IP address of the NAS.
- **Directory Name**: the folder on the NAS in which data is stored.
- **Disk Size**: the size of the network hard disk.
- **Test**: verify connectivity to the NAS.
- **Add NetHDD**: add the NAS to the camera.

9.3 FTP Server Settings

Enable the FTP function to upload pictures and videos from the camera to an FTP server, where they can be viewed and archived.

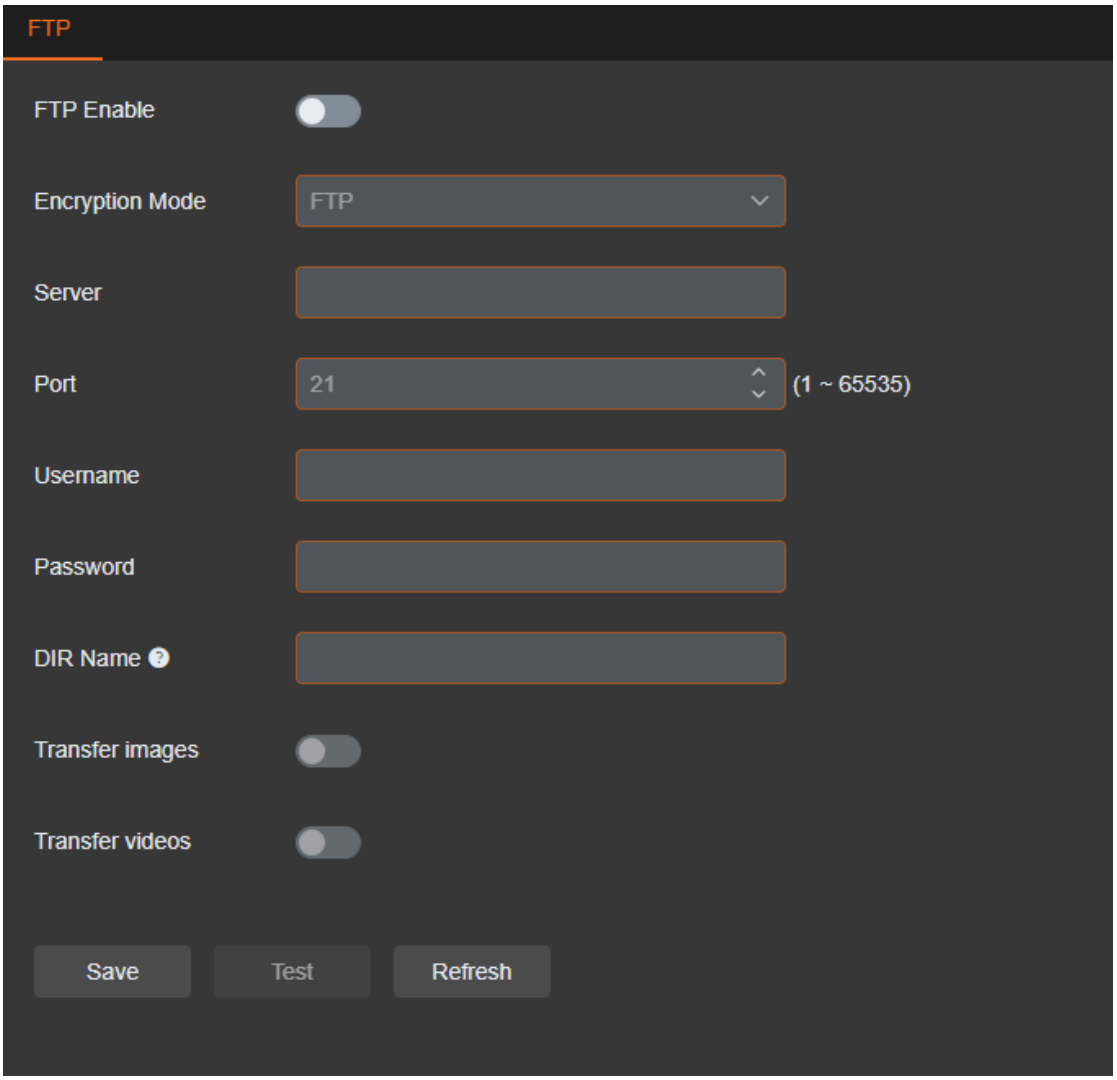

Figure 9-11. FTP server settings page

Configure FTP uploads using the following fields:

- **FTP Enable**: turn the FTP function on.
- **FTP Protocol**: select the transfer protocol, either **FTP** or **SFTP**.
- **Server**: enter the IP address or domain name of your FTP server.
- **Port**: enter the FTP port.
- **Username / Password**: enter the credentials for your FTP server.
- **Transfer images**: upload alarm images to the FTP server.
- **Transfer Videos**: upload alarm video to the FTP server.

TIP Use **SFTP** where your server supports it. SFTP encrypts the connection, protecting your credentials and uploaded media in transit.

Chapter 10 Alarms, I/O & Deterrence

The OCTAVUE access control camera pairs its physical alarm terminals with an on-board deterrence siren and a configurable disarming schedule. This chapter explains how to wire and configure I/O alarm inputs, define linkage responses, tune the built-in siren, and temporarily suspend alarm actions with the disarming function.

10.1 I/O Settings

The I/O menu configures the camera's physical alarm terminals. An external detector connected to the alarm input can trigger a coordinated set of responses, while the alarm output relay can drive an external device such as a strobe, lock, or auxiliary siren.

10.1.1 Alarm Input Settings

Click **Settings** → **Event** → **I/O Settings** and open the **Alarm Input** tab. The list shows each available input channel together with its alarm type and enabled state.

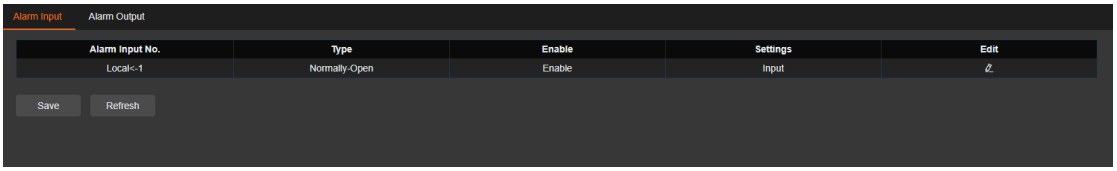

Figure 10-1. Alarm input channel list

Click the **Edit** icon in the row of the channel you want to modify to open the **Advance** configuration dialog, then set the following parameters.

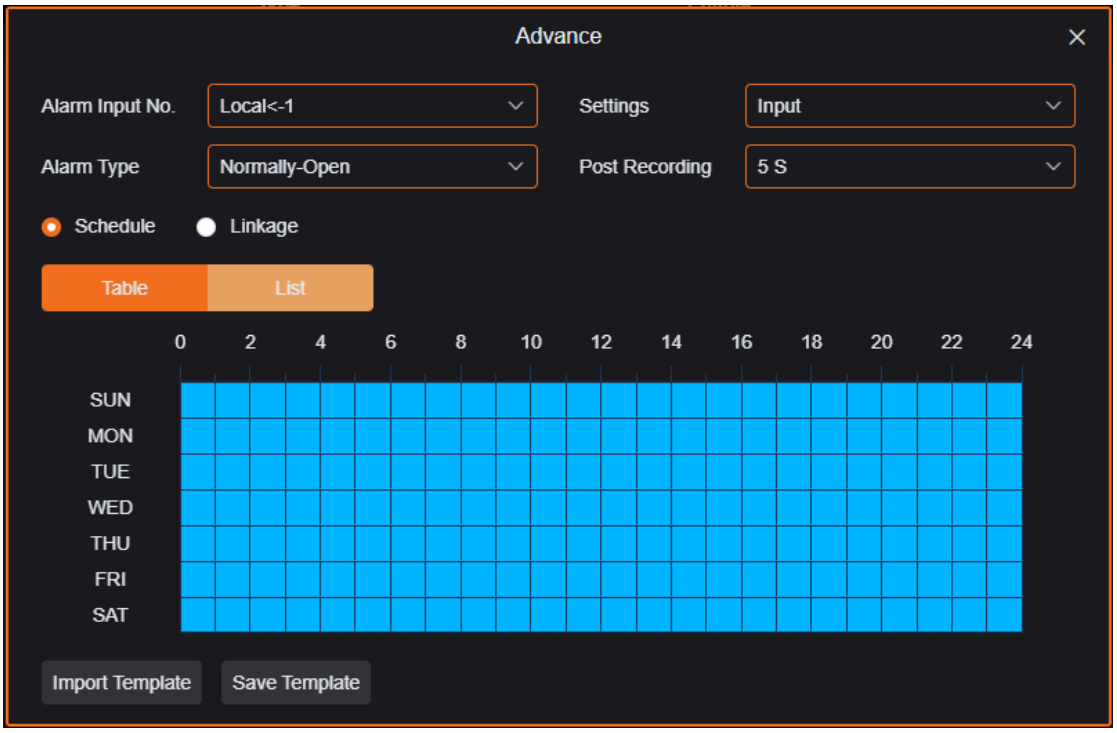

Figure 10-2. Alarm input parameters and effective schedule

- **Alarm Input No.** — Select the input source for the I/O alarm.
- **Settings** — Enable or disable the I/O alarm input function for the selected channel.
- **Alarm Type** — Select the input contact type to match the connected detector: Normally-Open or Normally-Closed.
- **Post Recording** — Continue recording for the defined interval after the triggering condition clears. The default is 5 seconds.
- **Schedule** — Define the arming period during which the I/O input alarm is active. Refer to the Schedule Settings section for details on editing the weekly time grid.

10.1.1.1 Alarm Linkage

Select the **Linkage** option in the **Advance** dialog to define the actions the camera performs when this input is triggered.

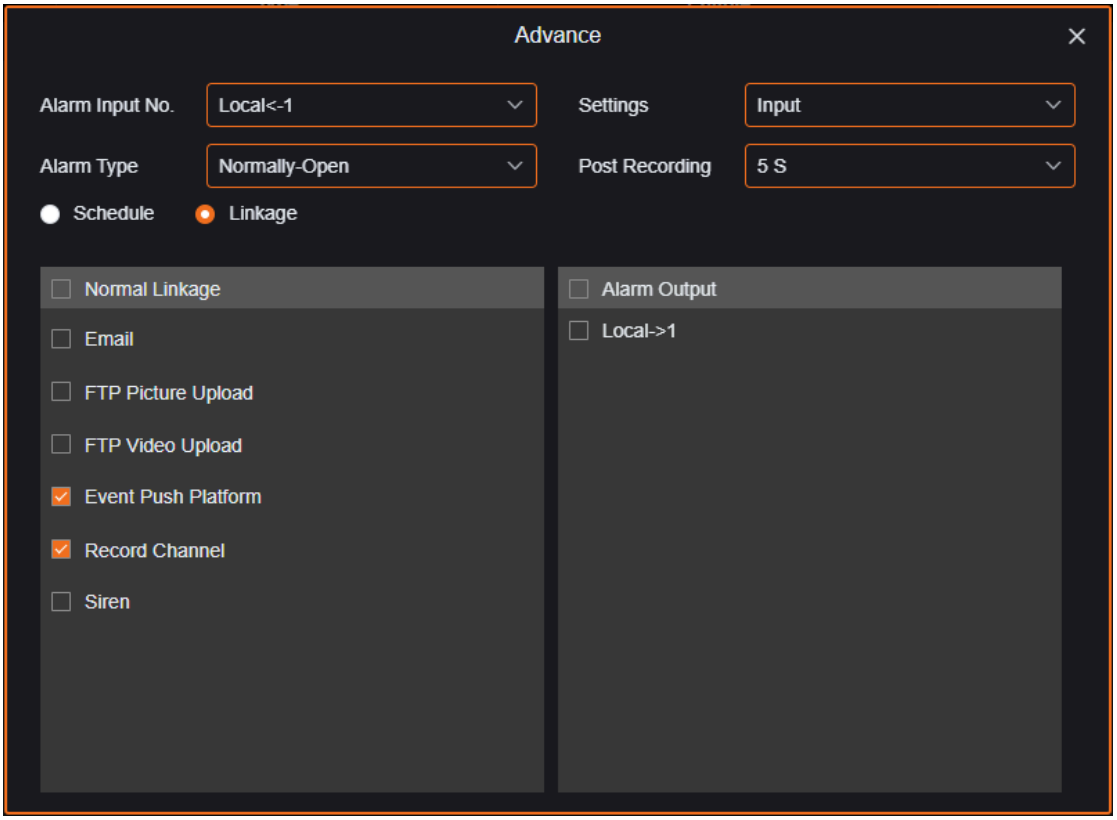

Figure 10-3. Alarm input linkage actions

- **Email** — Send a notification email to the configured mailbox when the alarm is triggered.
- **FTP Picture Upload** — Upload a snapshot of the alarm event to the FTP server.
- **FTP Video Upload** — Upload a video clip of the alarm event to the FTP server.
- **Siren** — Sound the built-in siren for deterrence when the alarm is triggered.

> **NOTE** Email and FTP linkages act only after the corresponding Email and FTP servers have been configured in the network menus. Use the **Settings** button beside the FTP options to confirm which server receives the uploaded pictures and video.

10.2 Siren Settings

On models equipped with a siren, this menu configures the audible deterrent that sounds when an alarm linkage calls for it. When triggered, the siren activates automatically to deter intruders.

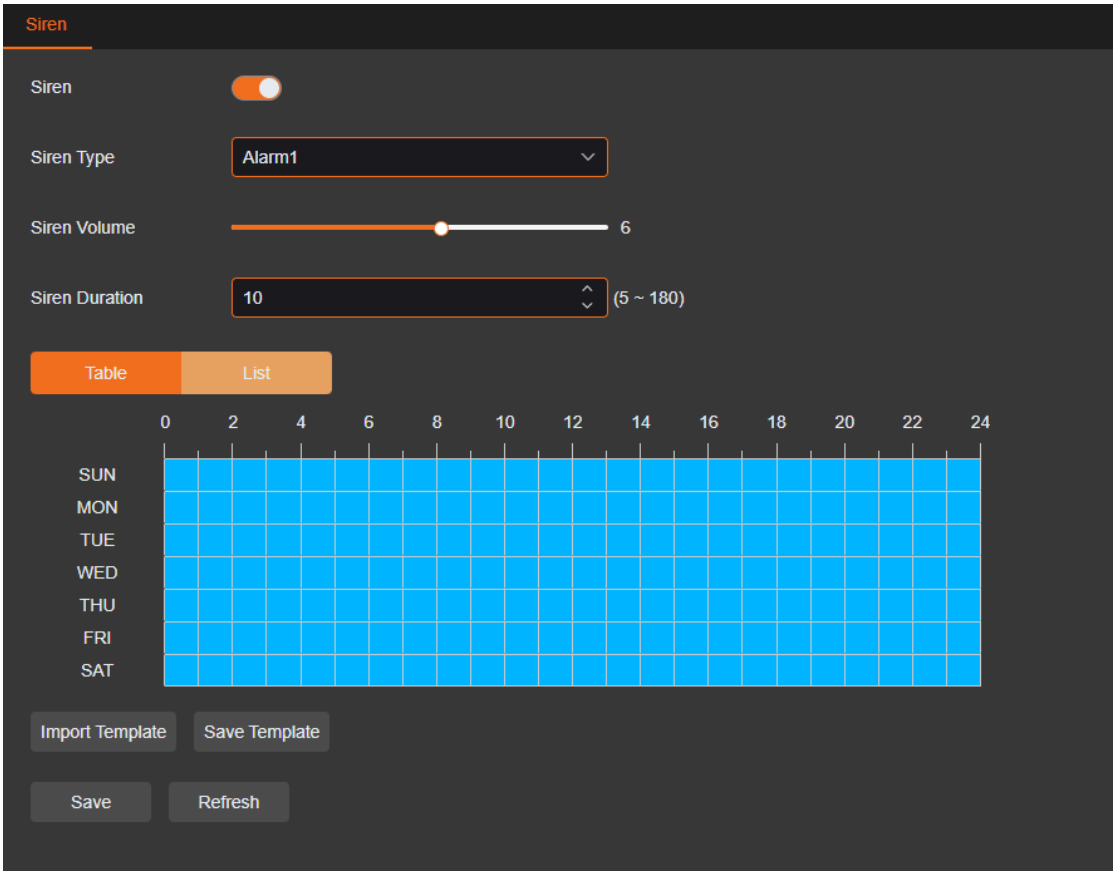

Figure 10-4. Siren configuration page

- **Siren** — Enable or disable the siren.
- **Siren Type** — Select the audio file the siren plays. Two built-in tones are provided.
- **Siren Volume** — Set the output level, adjustable from 1 to 10.
- **Siren Duration(s)** — Set how long the siren sounds per trigger, adjustable from 5 to 180 seconds.
- **Schedule** — Define the period during which the siren is permitted to sound. Refer to the Schedule Settings section.

TIP In addition to the built-in tones, some models support importing up to three custom siren files in PCM or WAV format. Each imported file must use a sampling rate no higher than 8000 Hz and must not exceed 256 KB. To remove a custom tone, select it and click the **Delete** button beside it.

10.3 Disarming

Disarming temporarily suspends the camera's response to alarm linkages, which is useful during maintenance or authorized activity that would otherwise trigger alerts. This menu sets the disarming switch, the linkage types to suppress, and the schedule during which suppression applies.

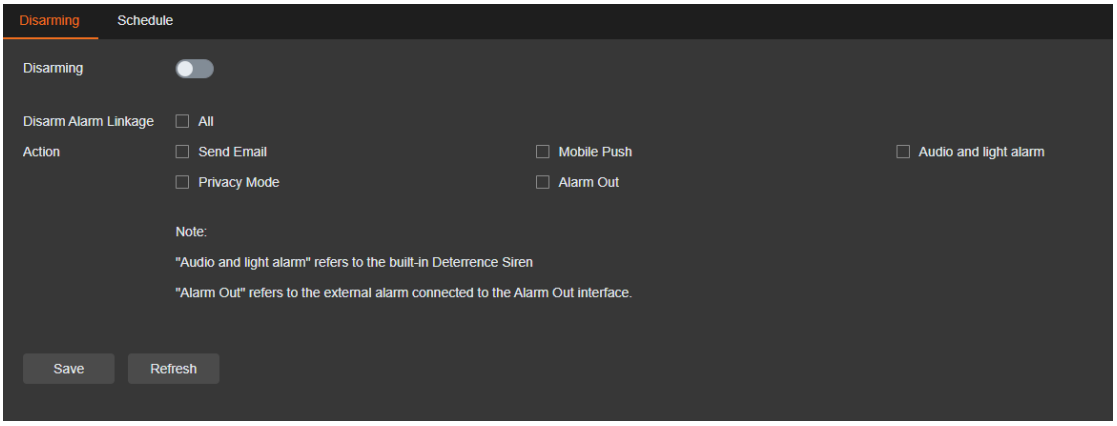

Figure 10-5. Disarming configuration page

- **Disarming** — Enable or disable the disarming function.
- **Action** — Select which local alarm linkage responses are suppressed while disarming is active. Use **All** to select or clear every type at once.
- **Send Email** — When selected, triggered alarms do not send notification emails.
- **Mobile Push** — When selected, the camera does not push alarm messages to the RXCam View and CybVu mobile apps.
- **Audio and light alarm** — When selected, the built-in deterrence siren does not respond to triggered alarms.
- **Alarm Out** — When selected, the external device connected to the Alarm Out interface does not respond to triggered alarms.
- **Privacy Mode** — When selected, the visual access control unit enters privacy mode once the one-click disarming switch is turned on.
- **Schedule** — Define the period during which disarming is in effect. Refer to the Schedule Settings section.

CAUTION While disarming is active, the selected alarm linkages are fully suppressed and the camera will not notify you of events they would normally report. Confirm that disarming is disabled, or that its schedule has ended, before relying on the camera for security monitoring.

Chapter 11 Events & AI Detection

The OCTAVUE access control camera uses AI-based intelligent alarms to recognize faces, pedestrians, and motion in the monitored scene and to trigger the linked responses you configure. Each detection type must first be enabled from the **Event** settings before its alarms take effect.

Every AI detection function consumes camera processing power. Because on-device performance is limited, some AI functions cannot run at the same time. The combinations available on a given device depend on the model; always follow the on-screen prompts and the specifications for your specific camera model.

NOTE Enabling additional AI functions increases the processing load on the camera. If a function cannot be enabled together with another, the interface indicates which detection types are mutually exclusive on your model.

11.1 Face Detection

Face detection first locates a face target in the camera view and captures an image that meets the configured requirements. The face model algorithm then computes the facial feature data from the

captured image and compares it against the face database to raise an alarm. The face detection function must be enabled before any of these steps can occur.

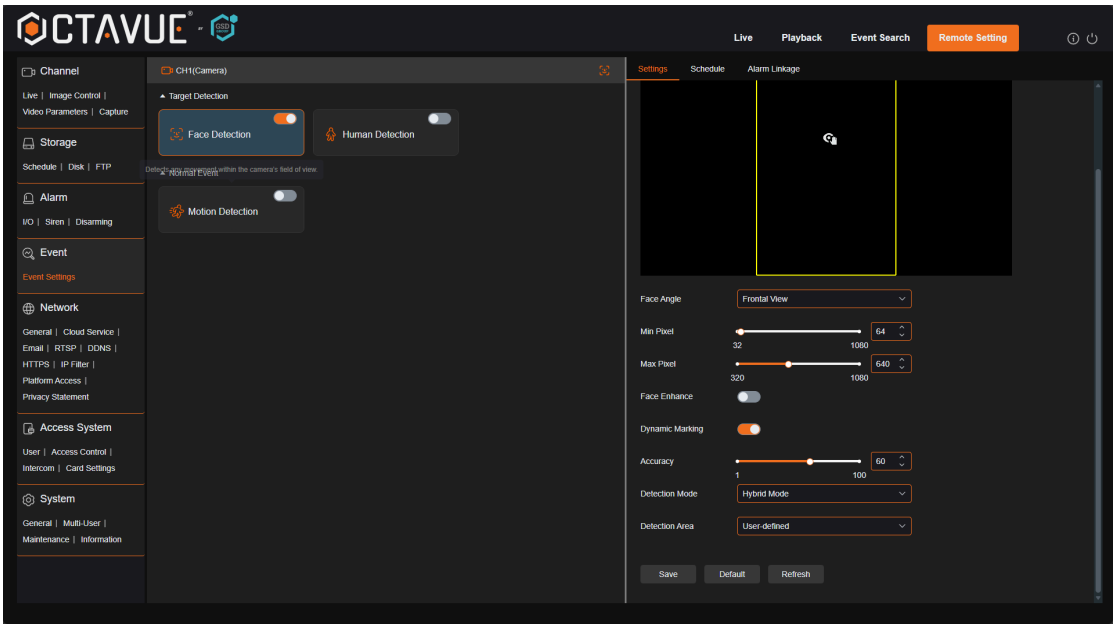

Figure 11-1. Face detection settings

Configure the following parameters to control how faces are captured, filtered, and detected:

- **Face Detection** — Enables or disables the face detection function.
- **Face Angle** — Filters the captured images so that only images matching the selected angle setting are pushed. Three modes are available.
- **Frontal View** — Pushes only frontal views of the subject.
- **Multi Angle** — Pushes images that contain side (profile) faces.
- **User-defined** — Customizes the range of angles for which images may be pushed. When enabled, the **Roll Range**, **Pitch Range**, **Yaw Range**, and **Picture Quality** options, along with the **Frontal Default** and **Multi Default** buttons, become available.
- **Roll Range** — Sets the permitted roll of the captured face in the 3D model. When the angle falls outside the limit, face detection still occurs but the image is not pushed.
- **Pitch Range** — Sets the permitted pitch of the captured face in the 3D model. When the angle falls outside the limit, face detection still occurs but the image is not pushed.
- **Yaw Range** — Sets the permitted yaw of the captured face in the 3D model. When the angle falls outside the limit, face detection still occurs but the image is not pushed.
- **Picture Quality** — Sets the minimum image quality. Higher quality helps filter out detected images that are not usable faces.
- **Frontal Default** — When the apply mode is set to **User-defined**, applies frontal capture defaults: Roll Range 30, Pitch Range 30, Yaw Range 45, and Picture Quality 100.
- **Multi Default** — When the apply mode is set to **User-defined**, applies multi-angle capture defaults: Roll Range 180, Pitch Range 180, Yaw Range 180, and Picture Quality 100.
- **Min Pixels** — Sets the minimum recognition pixel frame; a face must be larger than this value to be recognized. Hovering over the slider shows the actual pixel frame in the preview at right, and dragging the frame adjusts the value directly. The frame disappears from the preview five seconds after the mouse moves away.
- **Max Pixels** — Sets the maximum recognition pixel frame; a face must be smaller than this value to be recognized. Hovering over the slider shows the actual pixel frame in the preview at right, and dragging the frame adjusts the value directly. The frame disappears from the preview five seconds after the mouse moves away.

- **Face Enhance** — Improves capture of moving targets and adjusts brightness according to the face closest to the camera to optimize the capture result (supported by some models).
- **Bounding Box** — Displays the face detection box and the detection rule line (supported by some models).
- **Sensitivity** — Higher sensitivity reduces missed alarms but increases the likelihood of false alarms.
- **Detection Mode** — Filters which objects the camera evaluates. Two modes are available.
- **Always** — Performs face detection on all objects in the view.
- **Motion Only** — Filters out motionless faces, such as portraits and statues in the scene.
- **Detection Area** — Defines the area used to recognize objects. Two modes are available.
- **Full Screen** — Detects across the entire area the camera can monitor.
- **User-defined** — Detects only within the areas you box off manually.

11.2 Pedestrian Detection

Pedestrian detection identifies the human shape in the scene according to your settings, raises an alarm, and records the corresponding capture.

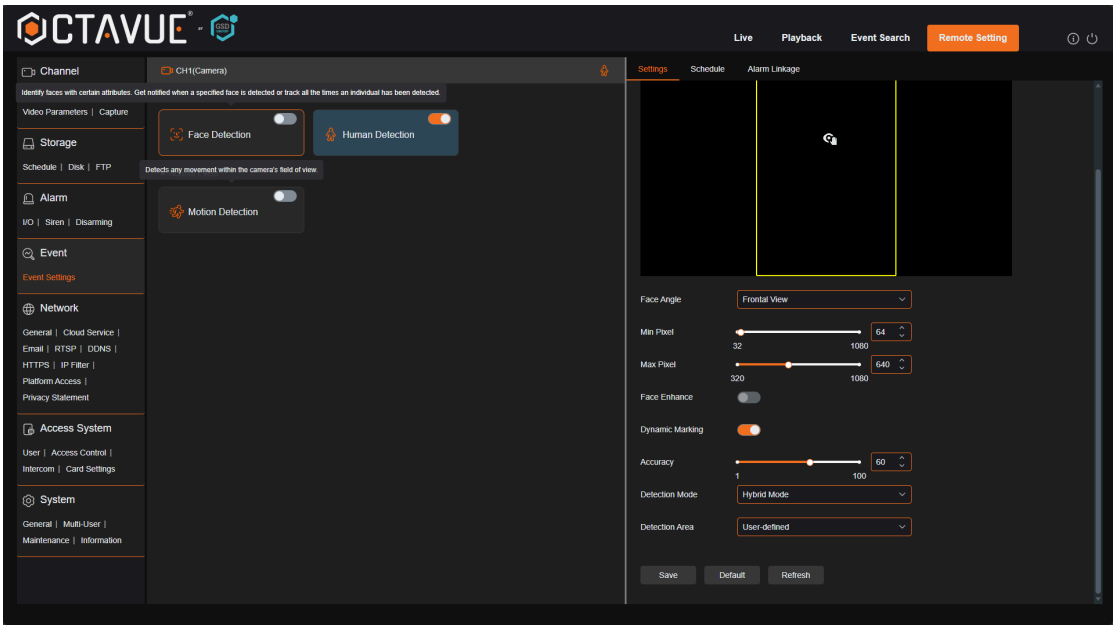

Figure 11-2. Pedestrian detection settings

- **Enable** — Enables or disables pedestrian shape detection.
- **Capture Mode** — Sets the snapshot behavior. Captured images can be received as push notifications in live view or reviewed through a connected NVR. Three capture modes are supported.
- **Default** — The camera pushes a single image of the detected pedestrian or vehicle, from the moment the object is detected until it disappears.
- **RealTime Mode** — On detecting an object, the camera immediately pushes one image, then pushes another image when the object disappears.
- **Interval Mode** — Pushes images a set number of times according to the configured interval. This mode exposes the **Snapshot Qty** and **Capture Interval** settings.
- **Snapshot Qty** — Sets how many times an image is pushed for what the camera considers the same target: 1, 2, 3, or unlimited, at the interval defined by **Capture Interval**.
- **Capture Interval** — Sets the time between pushes, measured from the target's appearance or from the previous push.
- **Min Pixel** — Sets the minimum recognition pixel frame; the pedestrian or vehicle must be larger than this value to be recognized. Hovering over the slider shows the actual pixel frame in the preview at right, and

dragging the frame adjusts the value directly. The frame disappears from the preview five seconds after the mouse moves away.

- **Max Pixel** — Sets the maximum recognition pixel frame; the pedestrian or vehicle must be smaller than this value to be recognized. Hovering over the slider shows the actual pixel frame in the preview at right, and dragging the frame adjusts the value directly. The frame disappears from the preview five seconds after the mouse moves away.
- **Bounding Box** — Displays the pedestrian or vehicle detection box and the detection rule line.
- **Detection Area** — Defines the detection area. Two modes are available.
- **Full Screen** — Detects across the entire area the camera can monitor.
- **User-defined** — Detects only within the area you box off manually.
- **Sensitivity** — Higher sensitivity makes pedestrian or vehicle objects easier to detect but may generate more false alarms.
- **Detection Mode** — Filters object behavior within the detection area. Two modes are available.
- **Always** — Detects all pedestrians in the view.
- **Moving Only** — Filters out motionless pedestrians.

11.3 Motion Detection

On this page you configure the motion detection parameters. When the camera detects movement of a target within the picture, it triggers a series of alarm responses.

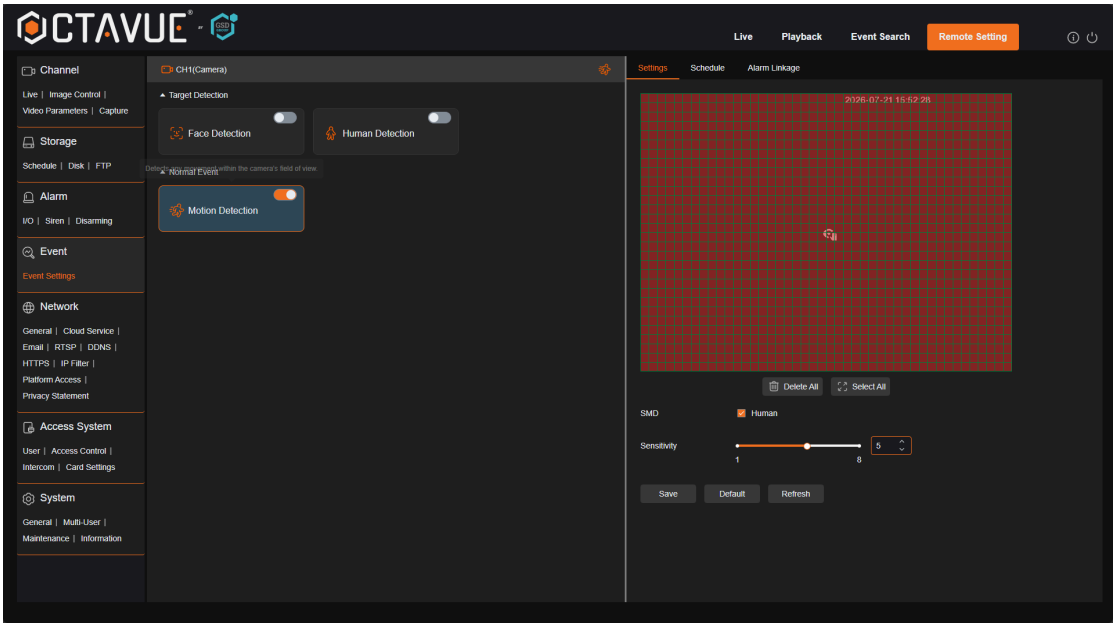

Figure 11-3. Motion detection settings

For example, a triggered motion alarm can send an email to a user-specified address with an image from the camera attached (when that option is enabled), or deliver a push notification through the mobile app.

Drag the left mouse button across the right-hand window to define the detection area. Only motion within this area triggers an alarm.

- **Motion Detection** — Enables or disables motion detection.
- **SMD** — Configures the detection targets for motion detection.
- **Pedestrian** — Detects and alerts only for human-shaped targets.
- **Sensitivity** — Adjusts the motion detection sensitivity; higher values increase sensitivity.

11.4 Alarm Linkage Settings

Alarm linkage defines the actions the camera performs when an event triggers an alarm. Configure each linkage so that the appropriate responses run automatically.

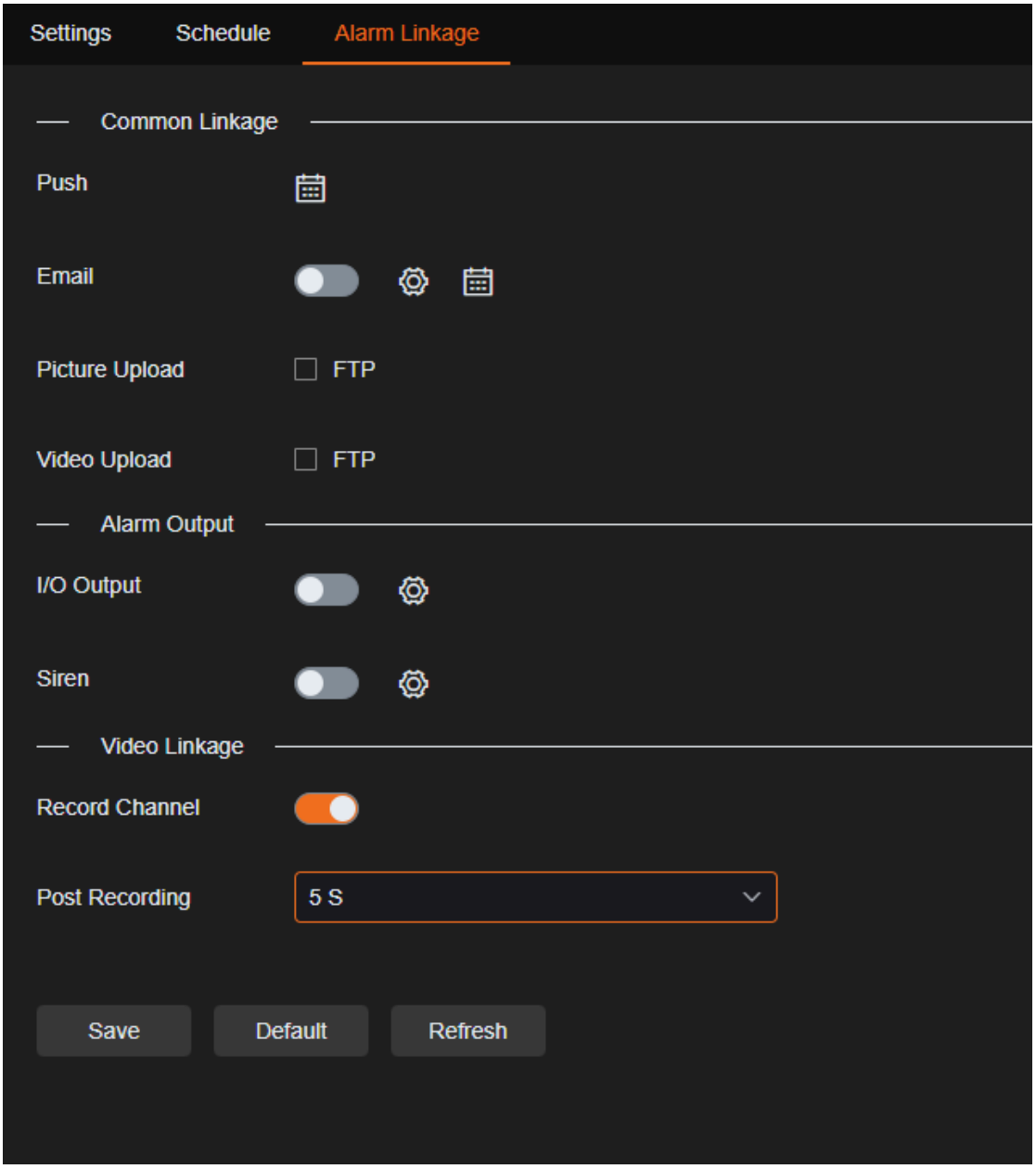

Figure 11-4. Alarm linkage settings

- **Event Push Platform** — Pushes events to third-party service platforms after an I/O alarm occurs. This option is selected by default.
- **Email** — Determines whether the camera sends an email when an event alarm is triggered. Click **Setup** or **Schedule** at the right to configure the email parameters.
- **Picture Upload** — When **FTP** is selected, the camera sends a picture to the associated FTP server when an event alarm is triggered. The FTP server must be associated first; refer to the FTP Server Settings section. Click **Setup** at the right to select which channel's alarm pictures are uploaded to the FTP server.
- **Video Upload** — When **FTP** is selected, the camera sends a video to the associated FTP server when an event alarm is triggered. The FTP server must be associated with the camera first. Click **Setup** at the right to select which channel is uploaded to the FTP server.

- **Siren** — A deterrent switch. When an alarm is triggered, the camera responds according to the parameters on the Siren Deterrent settings page. Click **Setup** at the right to set those parameters directly.
- **Recording Channel** — A recording channel linkage switch. Click **Setup** at the right to select the linked channels. When an alarm is triggered, the selected channels record the corresponding alarm type.
- **Recording Delay** — The length of time the camera continues recording after the alarm ends.

11.4.1 Custom Alarm Push (Notification)

Custom alarm push delivers device-side alarm information to one or more specified servers. This function requires that each server has completed integration and debugging with the camera.

Figure 11-5. Alarm linkage with custom notification

To configure custom alarm push on the device side, click **Notification** (custom alarm push settings) to open the settings page.

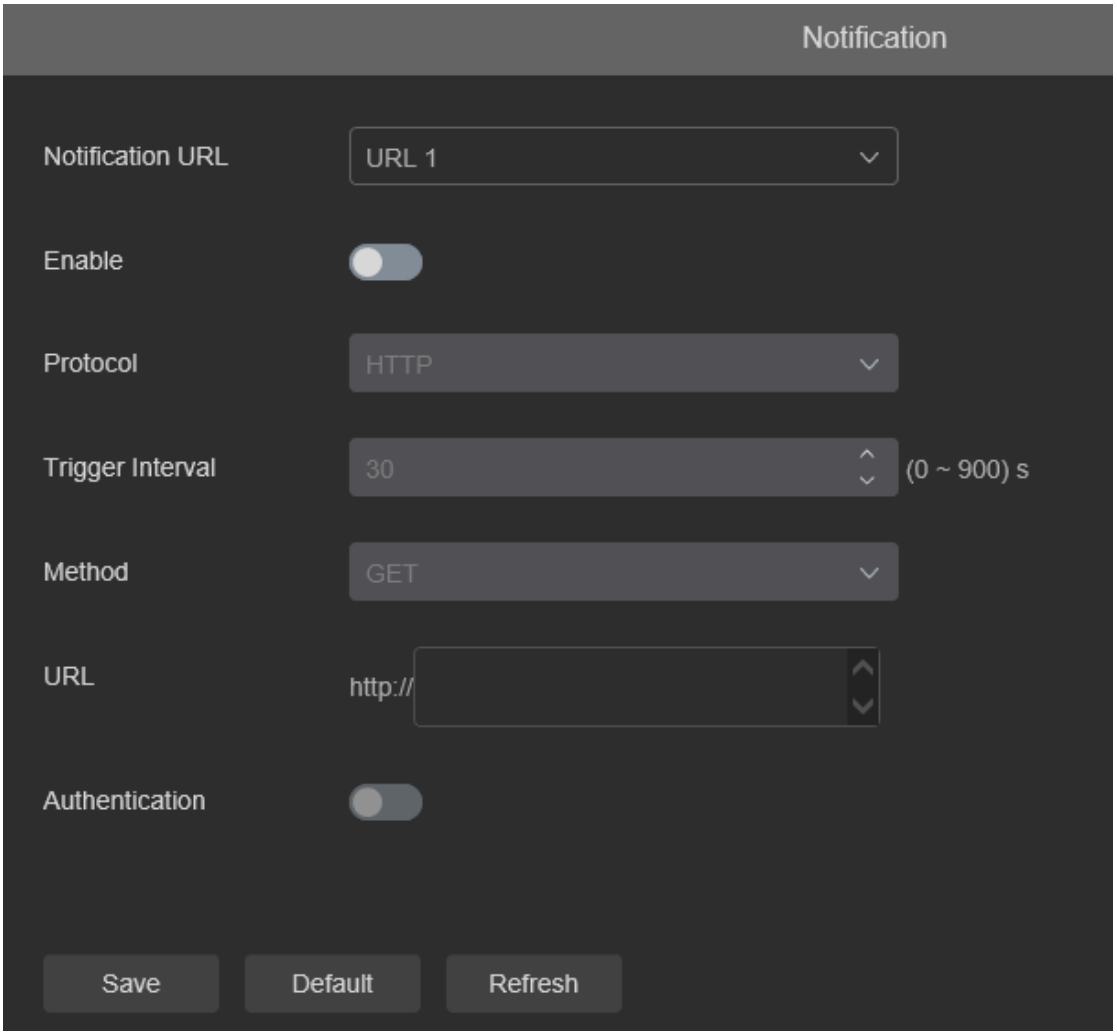

Figure 11-6. Custom alarm push settings

- **Notification URL** — Selects the target server. Up to three servers are supported, which may be identical or different.
- **Enable** — Turns the selected server's push on.
- **Protocol** — Sets the protocol mode. HTTP and HTTPS are supported for pushing alarm information to the server.
- **Trigger Interval** — The push interval, from 0 to 900 s; the default is 30 s.

- **Method** — The push method. POST and GET are supported; the POST method supports pushing an image.
- **URL** — The custom push URL.
- **Authentication** — When disabled, no authentication is required to accept the push notifications.
- **Username** — The server authentication user name.
- **Password** — The server authentication password.

> **CAUTION** Send alarm notifications only to servers you control and trust. When using the HTTP protocol or disabling authentication, alarm data and credentials are transmitted without protection; use HTTPS with authentication enabled wherever possible.

Chapter 12 Network & Services

This chapter describes the network configuration and connected-service options available on the OCTAVUE access control camera. From these menus you define how the camera obtains its address, which protocols and ports it uses, and how it reaches cloud, e-mail, streaming, and third-party management platforms.

12.1 Network Settings

The Network Settings menu is where you configure the camera's core network parameters, including the addressing method (DHCP or static), PPPoE dial-up, and SNMP. For most installations, DHCP is the recommended and most common option; use a static IP address only when your deployment requires fixed addressing. If your Internet connection requires an authentication user name and password, select PPPoE.

12.1.1 General Settings

Open **Settings** → **Network** → **General** to configure the camera's IP addressing. If the camera is connected to a router that supports DHCP, enable the **DHCP** option and the router will automatically assign all network parameters to the device. Disable DHCP to enter the parameters manually.

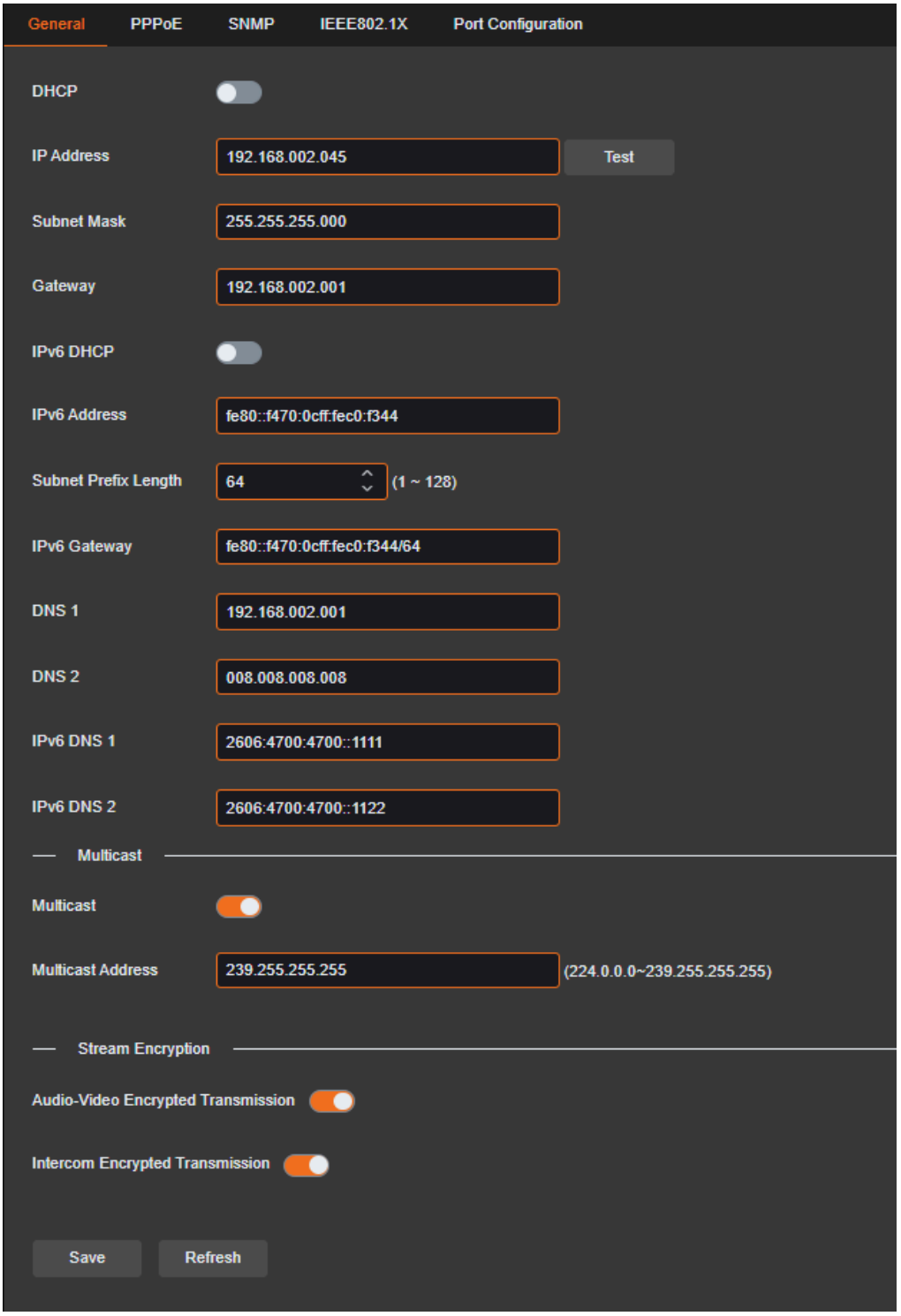

Figure 12-1. General network settings

When addressing is configured manually, set the following parameters:

- **IP Address** — the identifier of the camera on the network. It consists of four numbers between 0 and 255 separated by periods, for example “192.168.001.100”.
- **Subnet Mask** — a network parameter that defines the range of IP addresses that can be used on the network. If the IP address is likened to the street you live on, the subnet mask represents the surrounding community. It also consists of four numbers separated by periods, for example “255.255.000.000”.
- **Gateway** — the address that allows the camera to reach other networks. Its format is the same as an IP address, for example “192.168.001.100”.

- **IPv6 Address** — the IPv6 identifier of the camera on the network. It consists of eight groups of hexadecimal values between 0 and FFFF, separated by colons, for example “ABCD:EF01:2345:6789:ABCD:EF01:2345:6789”.
- **DNS1 / DNS2** — DNS1 is the active DNS server and DNS2 is the standby DNS server. In most cases, only the DNS1 address needs to be entered.
- **Multicast** — when enabled, the main stream can be delivered by multicast.
- **Multicast Address** — specifies the multicast address. A third-party player can request a multicast media stream from the camera over the RTSP protocol.
- **Audio-Video Encrypted Transmission** — enables encrypted transmission of the audio and video streams.

Figure 12-2. Manual IP address parameters

The camera can detect duplicate IP addresses within the same network segment. If the address you apply is already in use, a warning message is displayed so that you can assign a different address before saving.

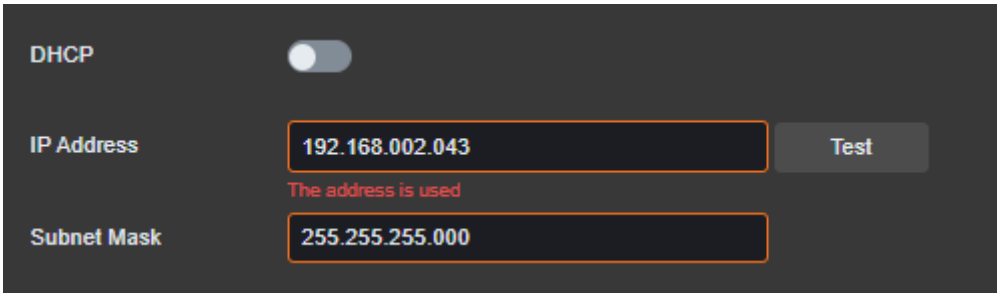

Figure 12-3. Duplicate IP address warning message

12.1.2 PPPoE

The camera supports dial-up networking through PPPoE. Open **Settings** → **Network** → **PPPoE** to configure it.

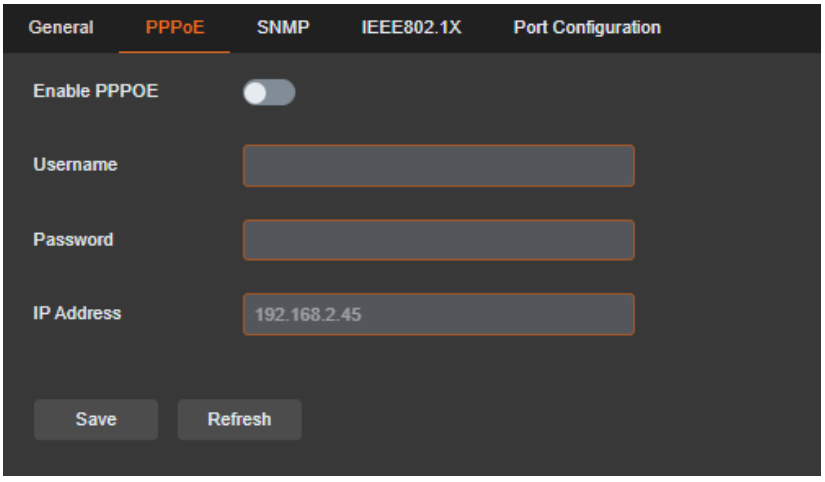

Figure 12-4. PPPoE settings

1. Select the **Enable PPPoE** check box.
2. Enter the PPPoE user name and password provided by your service provider.
3. Click **Save** to apply the settings.

NOTE After the PPPoE settings are saved, the camera restarts to activate the connection.

12.1.3 SNMP

Simple Network Management Protocol (SNMP) enables remote monitoring of the camera over the network. Open **Settings** → **Network** → **SNMP** to configure the following parameters.

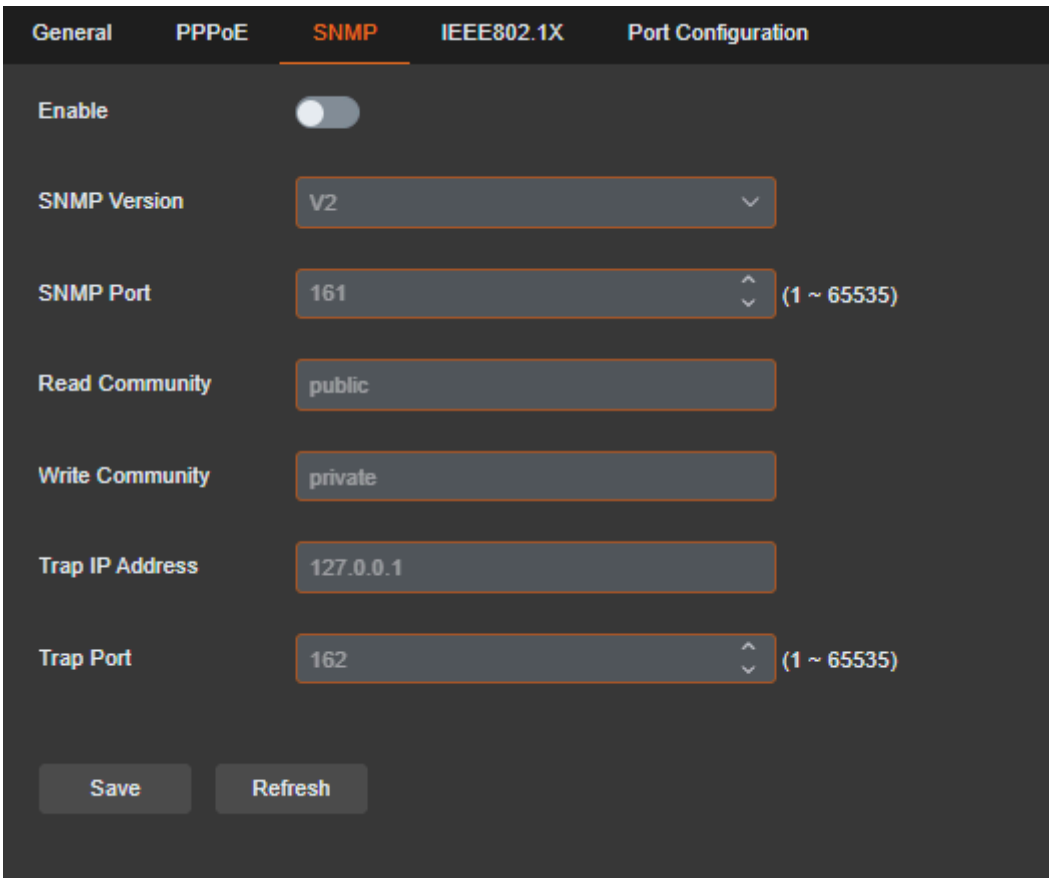

Figure 12-5. SNMP settings

- **Enable** — turns SNMP on or off.
- **SNMP Version** — sets the version of the SNMP server. V1, V2, and V3 are available.
- **SNMP Port** — sets the port used by the SNMP server.
- **Read Community** — sets the SNMP server read community string.
- **Write Community** — sets the SNMP server write community string.
- **Trap IP Address** — sets the destination IP address for SNMP traps.
- **Trap Port** — sets the destination port for SNMP traps.

12.1.4 IEEE 802.1X

IEEE 802.1X is a port-based network access control protocol used primarily in local area network environments to strengthen network security by verifying user identity and controlling access permissions at the port level. A network device connected to a switch port can access resources on the local area network only after it passes authentication; if authentication fails, access to those resources is denied.

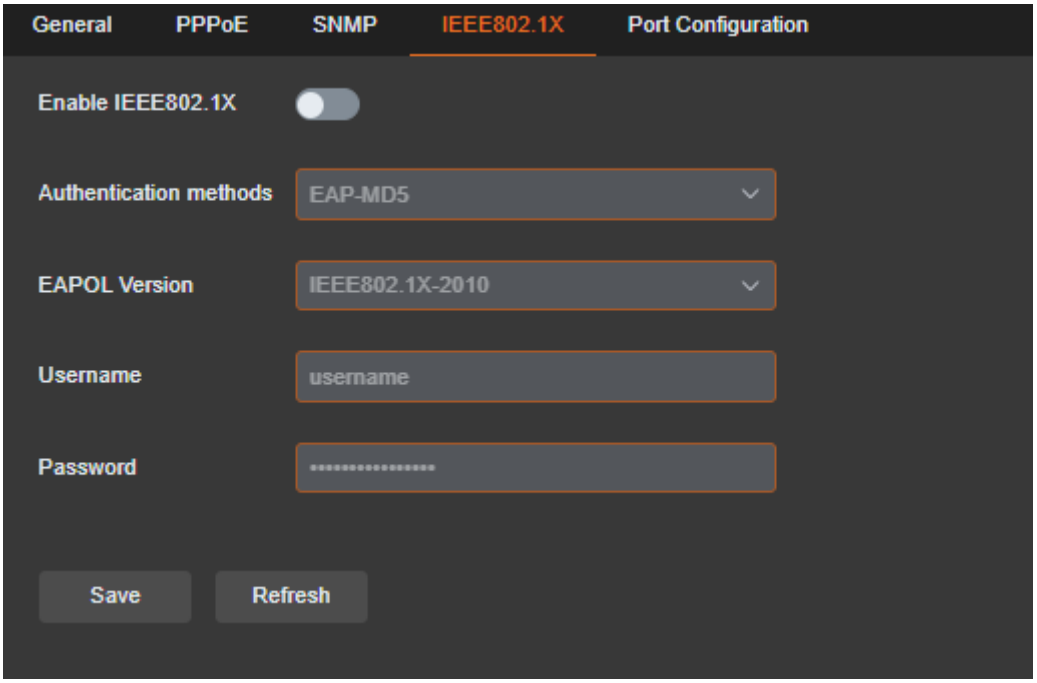

Figure 12-6. IEEE 802.1X settings

- **Enable IEEE 802.1X** — turns IEEE 802.1X authentication on or off.
- **Authentication Method** — sets the IEEE 802.1X authentication mode.
- **EAPOL Version** — selects the EAPOL protocol version.
- **Username** — sets the IEEE 802.1X authentication user name.
- **Password** — sets the IEEE 802.1X authentication password.
- **CA Cert** — imports the CA certificate.
- **Client Cert** — imports the client certificate.
- **Client Private Key** — imports the client private key.
- **Client Private Key Password** — enters the password for the client private key.
- **Install** — the import button. After selecting a certificate or key file, click this button to save it to the camera.

12.1.5 Port Settings

Open **Settings** → **Network** → **Port** to configure the protocol ports and related network services.

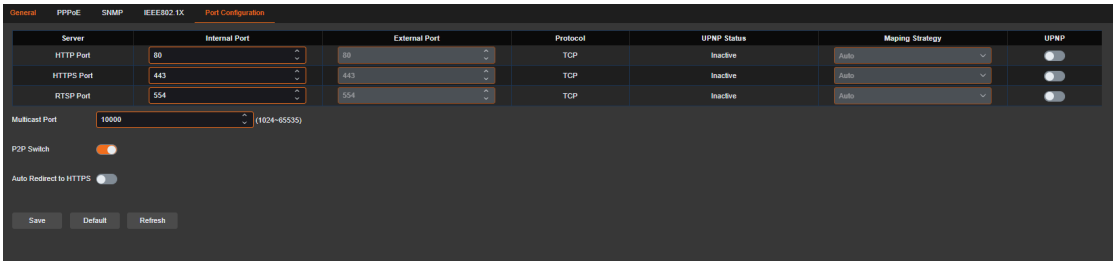

Figure 12-7. Port settings

- **HTTP Port** — the port used to access the camera from a web browser over the HTTP protocol. Default: 80.
- **HTTPS Port** — the port used to access the camera from a web browser over the HTTPS protocol. Default: 443.
- **RTSP Port** — the port used to access the camera over the RTSP protocol. Default: 554.
- **UPnP** — to log in to the camera remotely with the Web Client, port forwarding must be configured on the router. If your router supports UPnP, enable this option and the required ports are mapped automatically; you do not need to configure port forwarding manually. If your router does not support UPnP, configure port forwarding manually.

- **Multicast Port** — sets the multicast port.
- **P2P Switch** — enables or disables P2P. When it is turned off, P2P connectivity does not take effect.

12.2 Cloud Service

Enabling the cloud service generates a dynamic QR code for the selected region. Scanning this code with the mobile app adds the camera to the app for remote management. When a Cloud ID is pre-programmed with a fixed region, only the binding information is shown; the cloud service switch and dynamic code are not displayed.

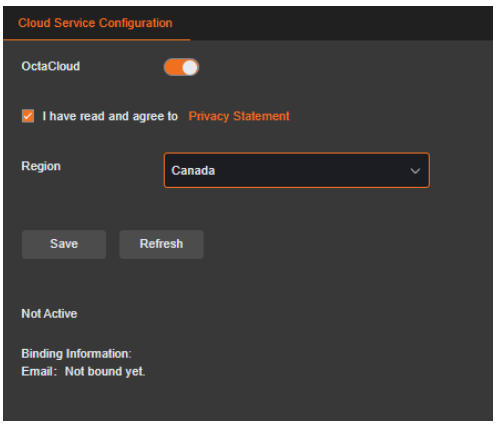

Figure 12-8. Cloud service settings

- **Cloud Service** — enables or disables the cloud service.
- **Privacy Statement** — before the cloud service can be enabled, you must read and agree to the privacy statement.
- **Region** — selects the cloud service region. This must match the region used when registering the app account.
- **QR Code Display** — once the cloud service is enabled and a region is set, a dynamic QR code is generated automatically. The code is valid for 300 s, after which it expires and must be refreshed. Scan the code with the app to add the camera.
- **Unbind** — removes the binding between the camera and the app account. After unbinding, the device appears offline in the app and can no longer be accessed there.

> **NOTE** The cloud service communicates with the cloud server, so the camera must have Internet access for this feature to work.

12.3 Email

Configure the e-mail settings so that the camera can send system notifications — for example, when an alarm is triggered or the storage is full — to one or more recipients.

12.3.1 Parameter Settings

Open **Settings** → **Network** → **Email** to configure the mail server and recipients.

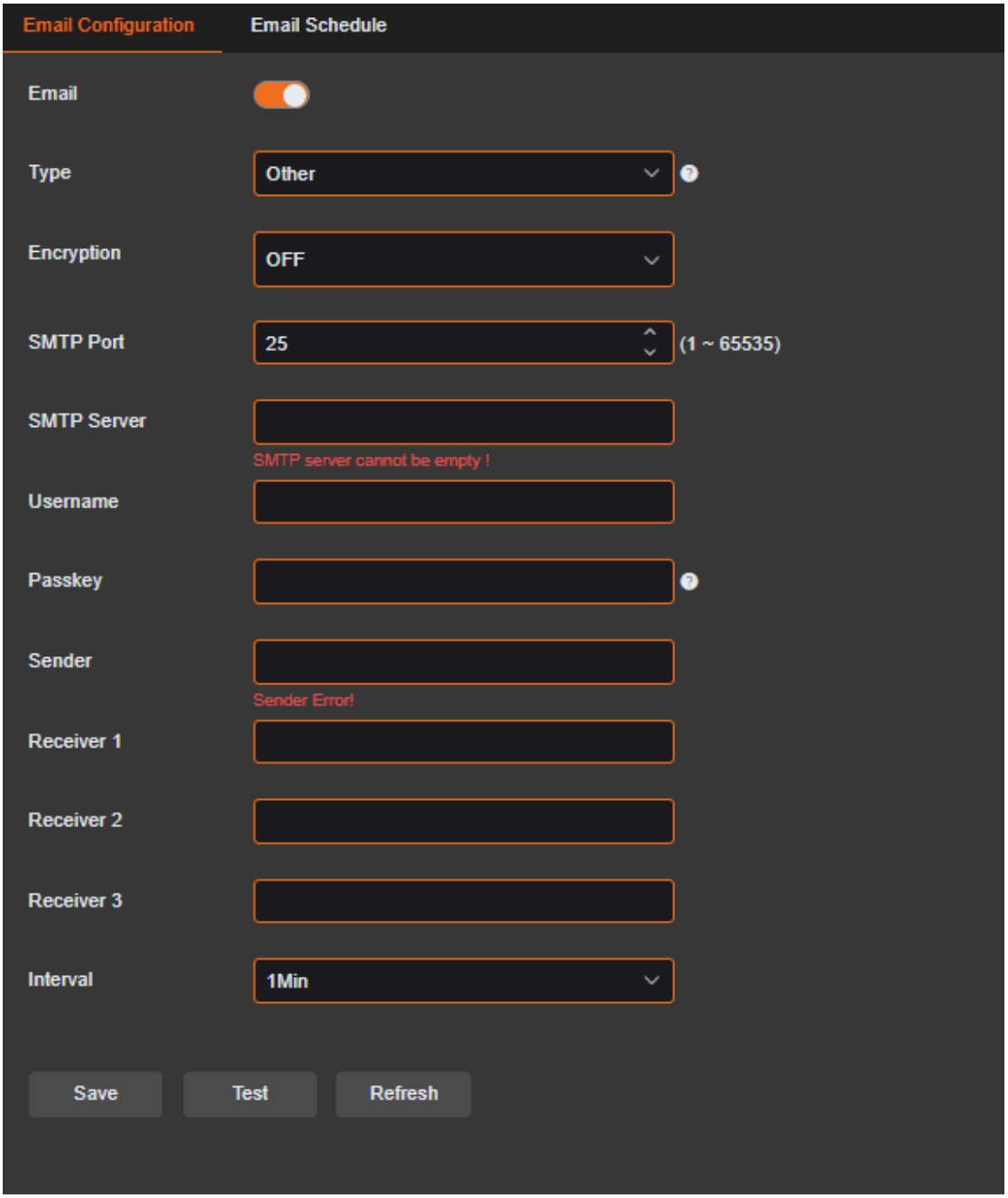

Figure 12-9. E-mail parameter settings

- **Email** — select the check box to enable e-mail notifications.
- **Type** — the mailbox type. Two types are available: Outlook and Other.
- **Encryption** — enable this if your mail server requires SSL or TLS authentication. If you are unsure, set it to Automatic.
- **SMTP Port** — the SMTP port of the mail server.
- **SMTP Server** — the address of the SMTP server.
- **Username** — the sender's e-mail address.
- **Password** — the password for the sender's e-mail account.
- **Receiver 1 to 3** — the e-mail addresses that will receive event notifications from the camera.
- **Interval** — the minimum time interval between notification e-mails.

TIP To confirm that all settings are correct, click **Test Email**. A test message is sent to the recipient address; if it arrives, the configuration is correct.

12.3.2 Schedule Settings

Define a schedule during which the e-mail feature is active. Notifications are sent only within the scheduled time periods. For details on defining a schedule, refer to the schedule configuration section.

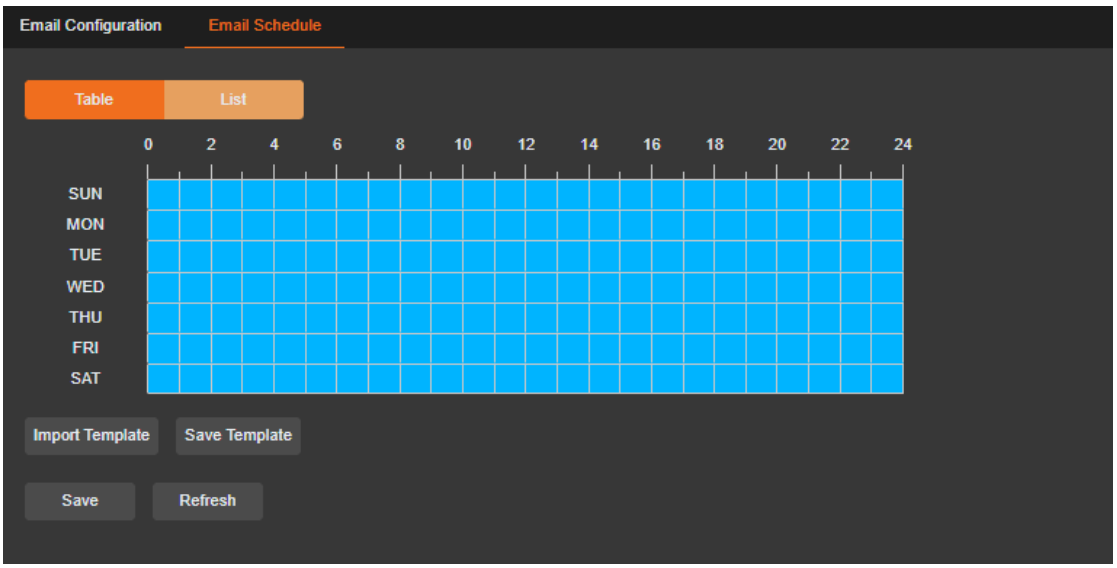

Figure 12-10. E-mail schedule settings

12.4 RTSP

RTSP (Real Time Streaming Protocol) controls the transmission of the media stream. Open **Settings** → **Network** → **RTSP** to configure the following parameters.

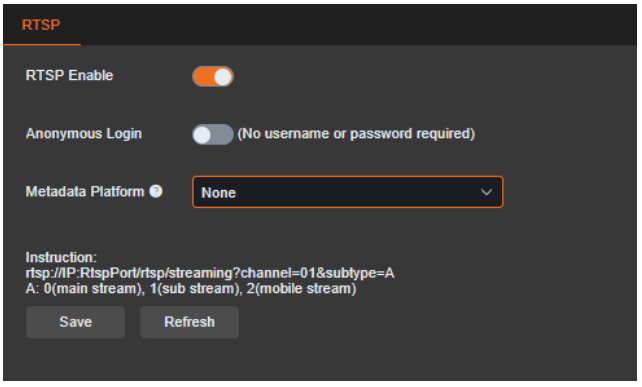

Figure 12-11. RTSP settings

- **RTSP Enable** — turns RTSP on or off. The protocol is available only when this option is enabled.
- **Anonymous Login** — when enabled, the RTSP stream can be accessed without authentication.
- **Metadata Platform** — when the camera is connected to a third-party monitoring platform through the ONVIF protocol, this setting controls the format of event and alarm metadata pushed to that platform:
- **None** — no metadata is pushed.
- **General** — pushes metadata in a common format suitable for third-party platforms with no special requirements.
- **Milestone** — pushes metadata formatted for the Milestone platform.

12.5 DDNS

Dynamic Domain Name Service (DDNS) lets you reach the camera through a domain name instead of a changing IP address. Open **Settings** → **Network** → **DDNS** to configure it.

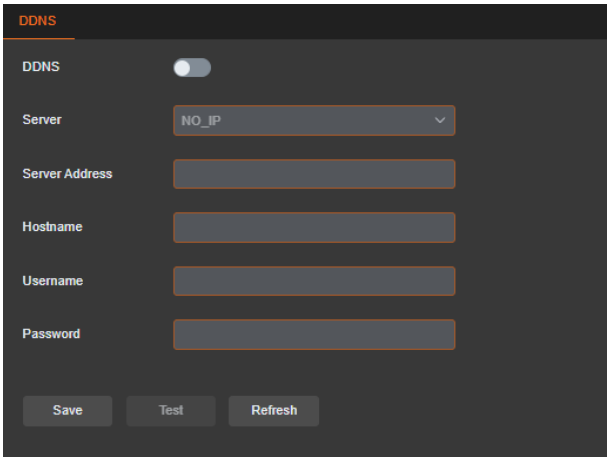

Figure 12-12. DDNS settings

- **DDNS** — select the check box to enable DDNS.
- **Server** — selects the preferred DDNS server. DYNDNS and NO_IP are supported, with partial support for CHANGEIP and DNSEXIT.
- **Hostname** — the domain name you created on the DDNS provider's web page. This is the address entered in the browser to connect to the camera remotely from a PC.
- **User / Password** — the user name and password obtained when creating an account with the DDNS provider.

NOTE After entering all parameters, click **Test** to verify the DDNS settings. If the result is “Network unreachable or DNS error”, confirm that the network connection is working and that the DDNS information is correct.

12.6 HTTPS

This menu configures secure access to the camera over the HTTPS protocol. Open **Settings** → **Network** → **HTTPS** to select the certificate.

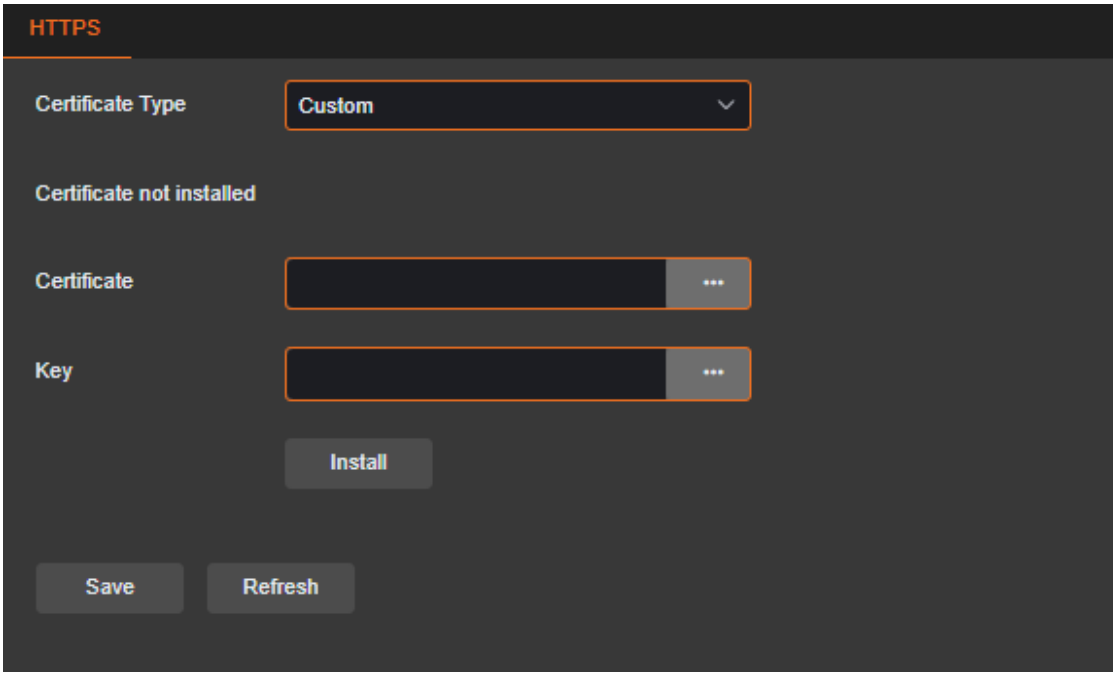

Figure 12-13. HTTPS settings

- **Certificate Type** — the authentication type. Default and Custom are available. Select Custom to connect using your own certificate.
- **Certificate** — under the Custom type, select the custom certificate file.
- **Key** — under the Custom type, select the custom key file.

12.7 IP Filter

The IP Filter function lets you define a blacklist or whitelist of addresses allowed to connect to the camera. Open **Settings** → **Network** → **IP Filter** to configure it.

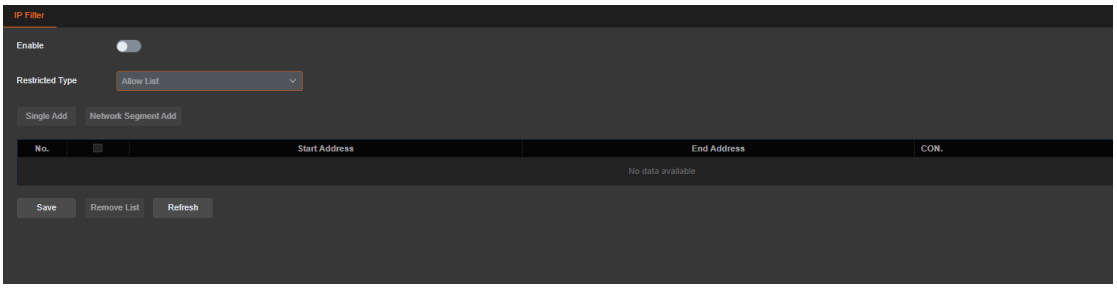

Figure 12-14. IP filter settings

- **Enable** — enables or disables the filtering function. When enabled, you can choose to apply a blacklist or a whitelist.
- **Edit Filtering List** — selects the list to configure (blacklist or whitelist).
- **Single Add** — adds a single IP address.
- **Network Segment Add** — adds a range of addresses.
- **Start Address** — the starting address of the range.
- **End Address** — the ending address of the range.
- **Delete** — removes an added IP address from the blacklist or whitelist.

> **CAUTION** Take care when applying a whitelist. If your own address is not included, you may lock yourself out of the camera and require a local connection to regain access.

12.8 Platform Access

The camera can push its audio and video streams and event notifications to external platforms, either through RTMP live streaming or through the event push platform.

12.8.1 RTMP

On the RTMP page, enable the function and enter a valid server address to push the camera's audio and video stream to a live-streaming server, such as YouTube.

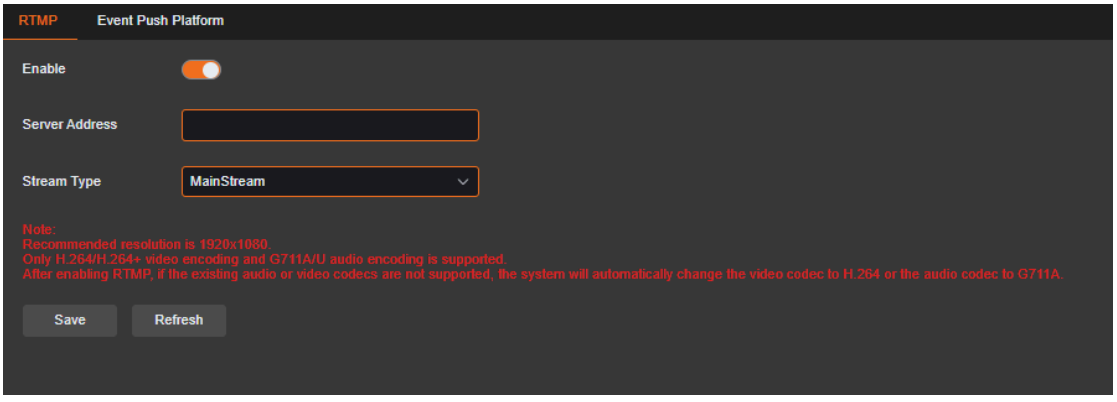

Figure 12-15. RTMP settings

- **Enable** — turns the RTMP function on or off.
- **Server Address** — the address of the server to which the stream is pushed.
- **Stream Type** — selects which audio and video stream is pushed to the server.

12.8.2 Event Push Platform

Event push delivers alarm notifications to an external platform using the HTTP, HTTPS, or UDP method. The HTTP/HTTPS method supports both POST and GET requests; the UDP method supports unicast, multicast, and broadcast.

> **NOTE** The event push function is supported on select models only.

12.8.2.1 HTTP/HTTPS Push

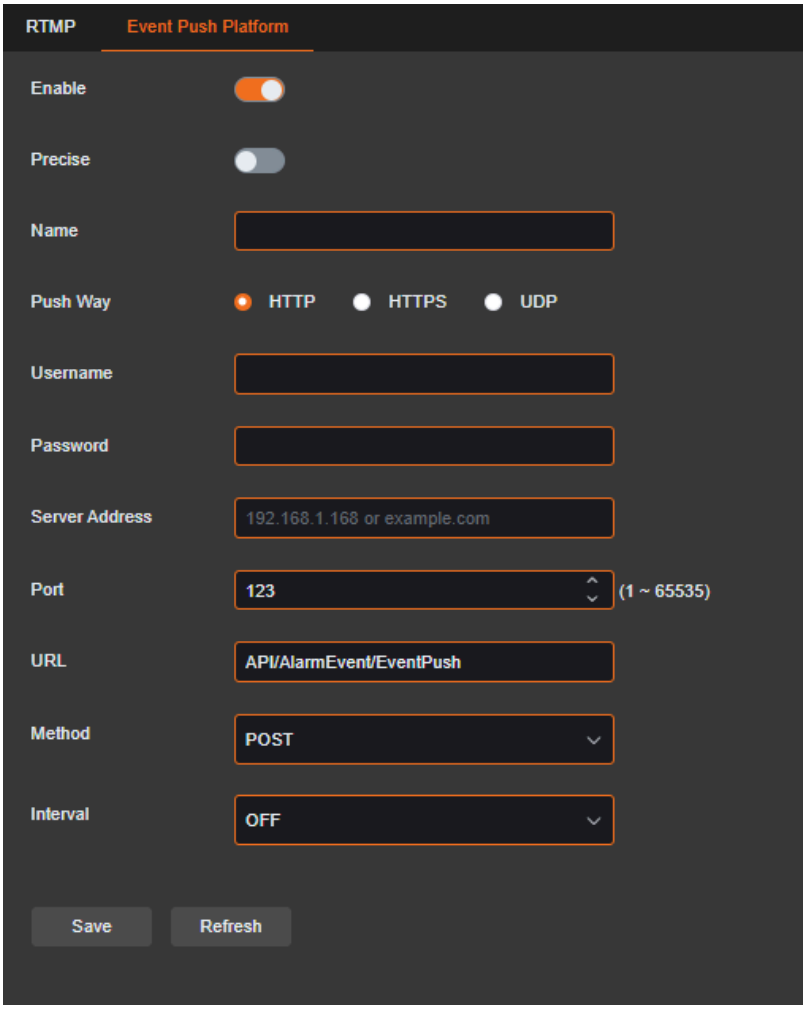

Figure 12-16. HTTP/HTTPS event push settings

- **Enable** — enables or disables the event push function.
- **Precise** — enables or disables precise push. When on, the camera pushes once when an alarm is triggered and again when the alarm ends. When off, it pushes only once, at the start of the alarm.
- **Name** — sets the channel name. Chinese characters are not supported.
- **Push Method** — selects HTTP push, HTTPS push, or UDP push.
- **Username** — sets the user name. It can be left as NULL if not required.
- **Password** — sets the password. It can be left as NULL if not required.
- **Server Address** — sets the server address.

- **Port** — sets the server port. Range: 1–65535.
- **URL** — sets the server API path. It can be left as NULL if not required.
- **Method** — the HTTP/HTTPS request type. POST and GET are supported. Only the HTTP/HTTPS POST method can push images; the other methods push messages only, without an accompanying image. The alarm type of a pushed image must match the preview alarm bar on the web interface.
- **Interval** — sets the keep-alive interval. The keep-alive mechanism periodically pushes a notification to the client at the preset interval without affecting normal alarm push. UDP mode has no keep-alive mechanism.

12.8.2.2 UDP Push

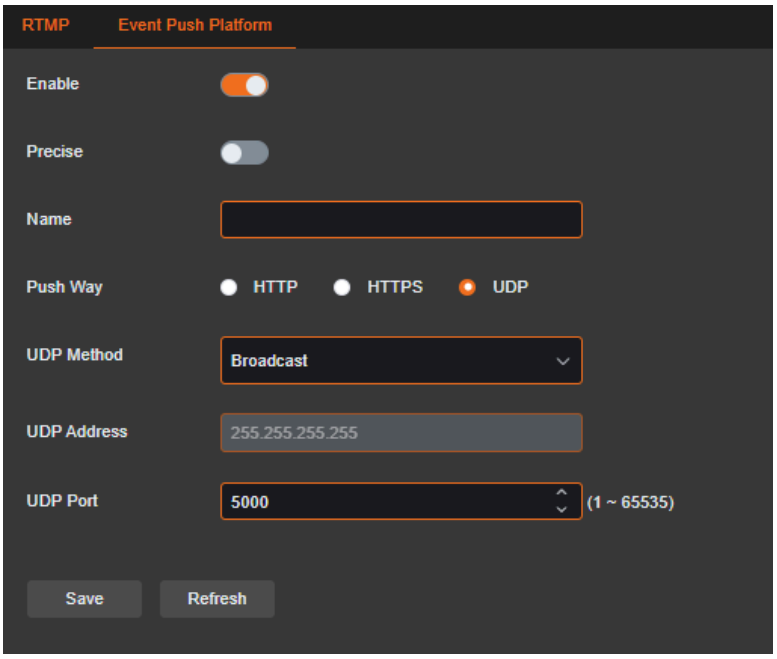

Figure 12-17. UDP event push settings

- **Enable** — enables or disables the event push function.
- **Precise** — enables or disables precise push. When on, the camera pushes once when an alarm is triggered and again when the alarm ends. When off, it pushes only once, at the start of the alarm.
- **Name** — the channel name. Chinese characters are not supported.
- **Push Method** — selects the push method. Select HTTP for HTTP push or UDP for UDP push.
- **UDP Method** — the UDP push type. Unicast, Multicast, and Broadcast are supported:
- **Unicast** — enter the IP address and port of the client's UDP server. Only that address receives the pushed messages.
- **Multicast** — client UDP servers on the same network segment that share the same UDP address and port all receive the message; other addresses do not.
- **Broadcast** — all UDP servers on the same network segment receive the message.
- **UDP Address** — the UDP server address.
- **UDP Port** — the UDP server port. Range: 1–65535.

PART IV

Access Control & System

Users, doors, cards, intercom, and system administration

Chapter 13 Access Control System

The Access Control System is the core of the OCTAVUE by GSD Group access control camera. It brings together everything required to manage who may open a door and how: user enrolment with face and access-card credentials, authentication and door-hardware parameters, third-party reader integration over RS-485 and Wiegand, alarm linkage, an integrated SIP intercom, and card-format settings. This chapter describes each area in turn.

All of the settings below are reached from the web interface of the camera. The access control features are grouped under **Settings** → **Access System**; for example, user records are managed at **Settings** → **Access System** → **User**.

13.1 User

The **User** area is where operators review enrolment status at a glance and create, edit, filter, import, and export the people who are permitted to use the door. The camera supports up to **3,000 users**, **3,000 faces**, and **30,000 access cards**.

13.1.1 User Information

The **User Information** page is a dashboard that summarizes the current enrolment state of the system. It reports the total number of enrolled users, how many have face and access-card credentials, and how much of the device capacity for users, faces, cards, and events has been consumed.

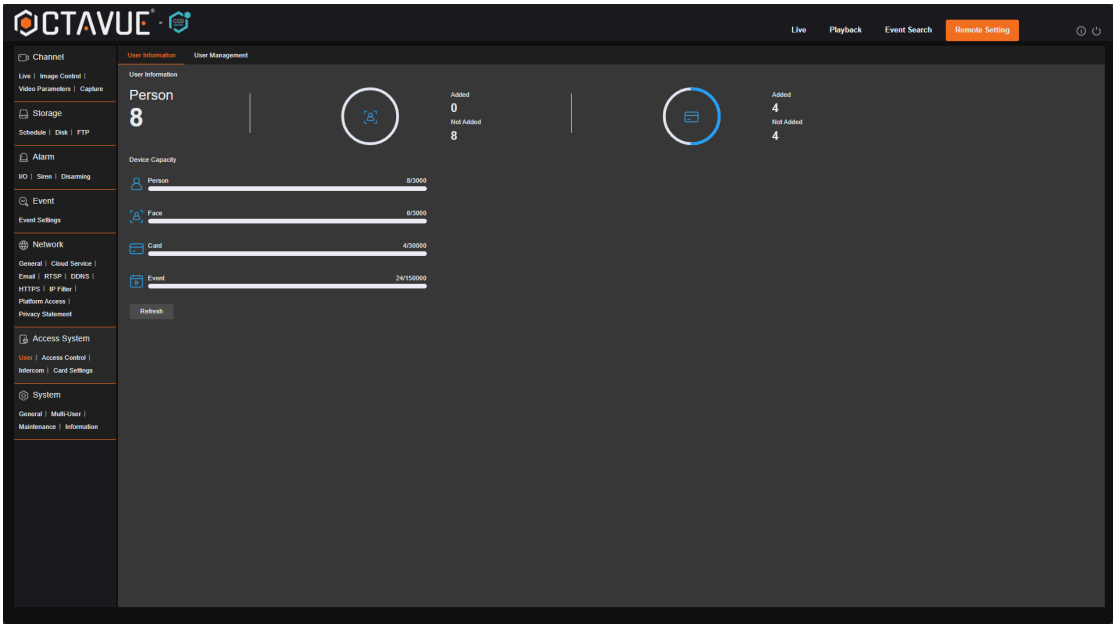

Figure 13-1. User Information dashboard

The dashboard presents the following counters:

- **Total Users** — the total number of users that have been added.
- **Added / Not Added Facial Recognition** — the number of users with, and without, an enrolled face. Click either figure to jump to the User Management page filtered to the matching users.
- **Added / Not Added Access Cards** — the number of users with, and without, an enrolled access card. Click either figure to open the User Management page filtered accordingly.
- **Person** — the number of users currently enrolled against the maximum number of users that can be added.
- **Face** — the number of faces enrolled against the maximum number of faces that can be added.
- **Card** — the number of access cards enrolled against the maximum number of cards that can be added.
- **Event** — the number of access events recorded against the maximum number of events that can be stored.

13.1.2 User Management

The **User Management** page is used to add and modify user records and to locate individual users quickly. Users can be filtered by user ID, user name, or access-card number, and further narrowed by credential status and user type. The entire user database can also be imported and exported for backup or bulk provisioning.

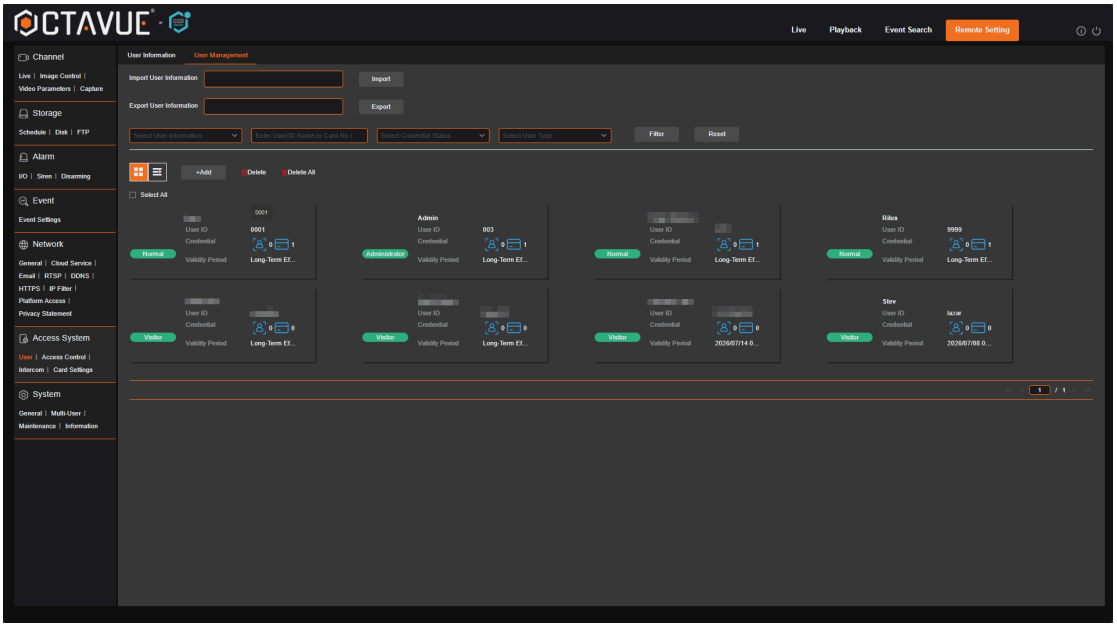

Figure 13-2. User Management page

The following controls manage the user database as a whole:

- **Import User Information** — click the field to open the file-selection dialog, choose the parameter file, then click **Import** to load the user database.
- **Export User Information** — enter a file name for the exported parameters and click **Export** to save the current user database.

Use the filter bar to locate specific users:

- **Select User Information** — choose whether to filter by user ID, user name, or card number.
- **Enter User (ID, Name, or Card No.)** — type the keyword that corresponds to the field selected above.
- **Select Credential Status** — filter by credential state: all, no credential added, face added, face not added, card added, or card not added.
- **Select User Type** — filter by role: administrator, regular user, visitor, or custom user.
- **Filter** — apply the selected filter conditions to the user list.
- **Reset** — clear all filter conditions.

User records can be viewed in two layouts. Use the display-mode icons to switch between them:

Business Card mode — displays users as visual cards.

List mode — displays users in a compact list.

The remaining controls act on individual or selected users:

- **Add** — create a new user record.
- **Delete** — select a user and click to remove that user record.
- **Delete All** — remove every user record. A confirmation prompt must be accepted before the operation proceeds.
- **Select All** — select every user on the current page so that the same operation can be applied to all of them.
- **User information display area** — shows each enrolled user, including face, user ID, user name, credential, expiration date, and user type.
- **Edit** — hover over a user card to reveal the edit button, then click it to open the user details page.
- **Pagination** — the controls in the lower-right corner page through the user list.

> CAUTION **Delete All** erases the entire user database and cannot be undone. Export the user information first so that enrolment can be restored if required.

13.1.2.1 Adding and Editing a User

Click **Add** or the **Edit** button on a user card to open the user details page, where the user's information and credentials are entered or modified.

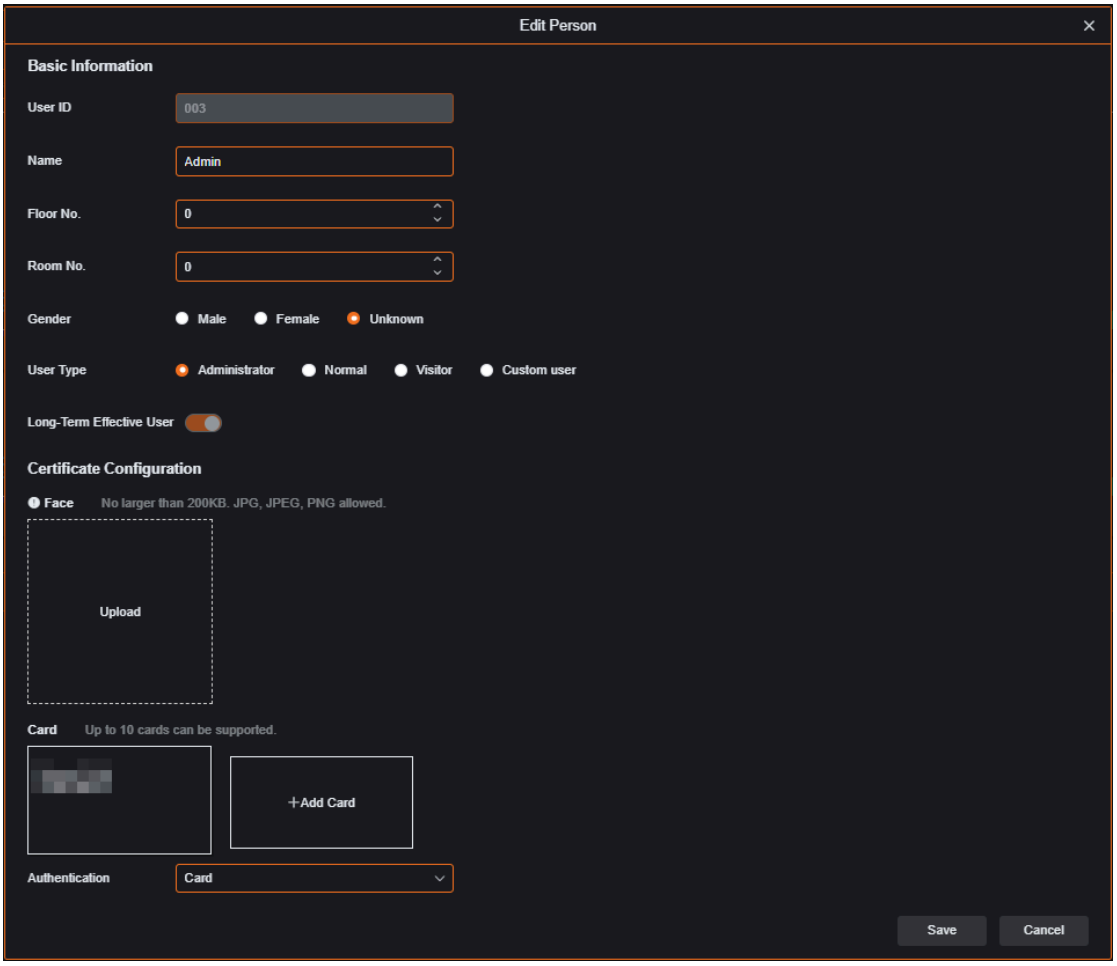

Figure 13-3. User details page

Enter the identity and access rules for the user:

- **User ID** — a customizable identifier. This field is required when adding a user.
- **Name** — the user name. Optional and editable.
- **Floor No.** — the floor number. Optional and editable.
- **Room No.** — the room number. Optional and editable.
- **Gender** — Male, Female, or Unknown. The default is Male.
- **User Type** — administrator, regular user, guest, or custom user. The default is regular user.
- **Long-Term Effective User** — when enabled, the user has no expiry. Administrator users have this enabled permanently and cannot change it; guest users do not have this switch.
- **Validity Period** — the active date range for the user. Regular and custom users can set this once **Long-Term Effective User** is turned off.
- **Unlimited Times** — when enabled, the user may authenticate to open the door an unlimited number of times. This switch is available to guest and custom users.
- **Visit Times** — the permitted number of entries. Each successful authentication decrements the count by one; when it reaches 0 the user can no longer open the door. This value can be set once **Unlimited Times** is turned off.

NOTE The user ID can be assigned only when a user is first created. It cannot be changed after the record is saved.

Under **Certificate Configuration**, assign the user's credentials:

- **Face** — the enrolled reference face. During authentication, the detected face is compared with this image; a similarity of 70% or higher passes. Uploaded face images must not exceed 200 KB and must be in JPG, JPEG, or PNG format.
- **Card** — enter the card number manually or present the access card to the reader area to capture it automatically. Each user may hold up to 10 access cards, and each card can be designated as a normal card, duress card, patrol card, or a disabled (accessibility) card.
- **QR Code** — for guest users, a QR code can be generated for authentication. The generated code can be exported as an image and given a validity period.
- **Authentication** — the accepted authentication method for the user. Options include face or card or QR code, card, card and face, face, and QR code. The default is face or card or QR code.

TIP A duress card lets a user open the door under coercion while silently triggering an alarm. Reserve at least one duress card for high-risk locations and keep its assignment confidential.

13.2 Access Control

The **Access Control** area governs how authentication behaves, how the door hardware is driven, how external readers are connected over RS-485 and Wiegand, and which actions are linked to access-control alarms.

13.2.1 Authentication Settings

This page sets the authentication interval for a single user and configures the authentication-failure and tamper alarms. Within the configured interval, a given user can authenticate successfully only once; if repeated attempts are made in quick succession, only the first succeeds. A maximum-failure threshold can be defined so that, once the number of failed attempts reaches it, an authentication-failure alarm is raised and its configured linkage actions are triggered.

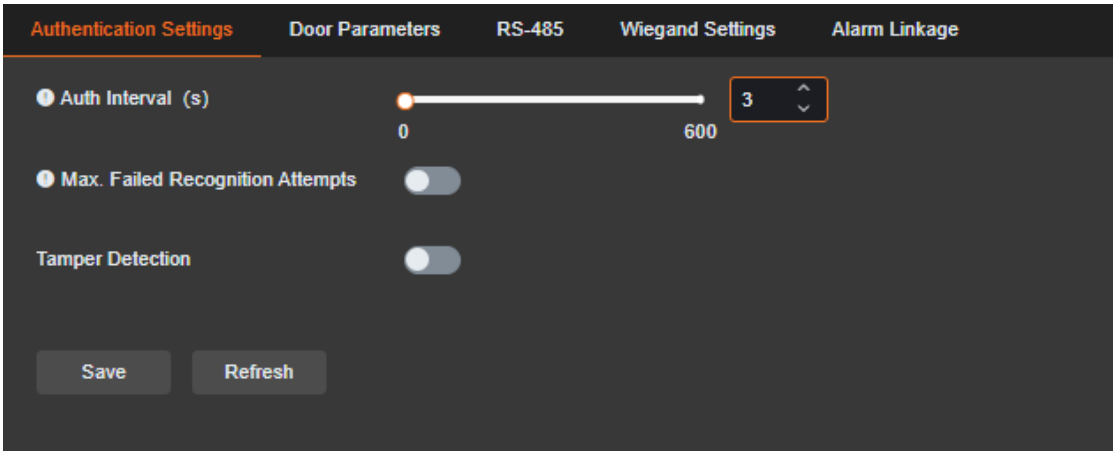

Figure 13-4. Authentication Settings

- **Auth Interval** — the minimum time that must elapse between two successful authentications by the same user. Range 0 to 600 s; default 3 s.
- **Max. Failed Recognition Attempts** — the switch that enables the maximum-failure alarm.
- **Max. Failed Authentication Attempts** — the number of consecutive failures that triggers the alarm. Range 1 to 10.
- **Tamper Detection** — the tamper-alarm switch. When enabled, a tamper alarm is raised if the camera is forcibly removed after installation, and the configured linkage actions are initiated.

CAUTION Enable **Tamper Detection** on any door where the camera is physically accessible. Without it, removal of the device from its mount will not generate an alarm.

13.2.2 Door Parameters

This page defines how long the door stays unlocked, the door-open timeout, and the electrical characteristics of the connected door hardware. A separate, longer open duration can be granted to accessibility users. When a door-magnetic (door contact) sensor is used, the camera raises a door-open timeout alarm if the door is not closed within the configured time, and initiates the linked actions.

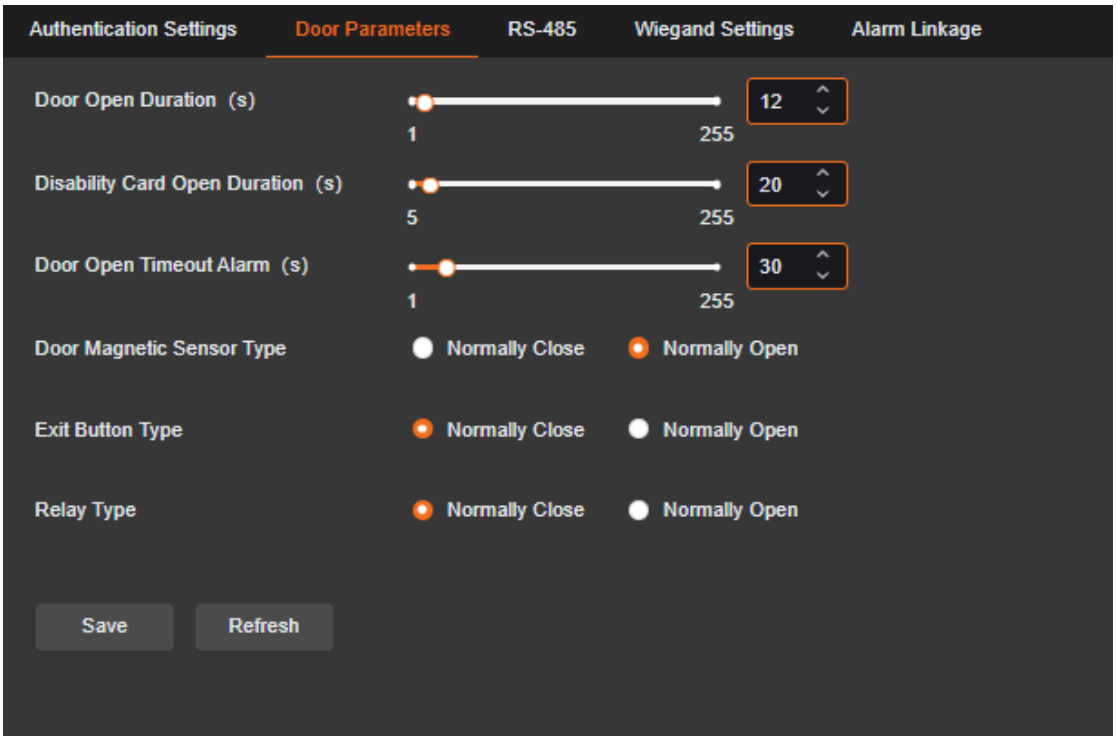

Figure 13-5. Door Parameters

- **Door Open Duration** — how long the door remains unlocked after a successful authentication or a manual open. Range 0 to 255 s; default 5 s.
- **Disability Card Open Duration** — the open duration granted when an accessibility card is used, giving the user more time to pass through. Range 5 to 255 s; default 20 s.
- **Door Open Timeout Alarm** — the time after which an alarm is raised if the door has not been closed. Used together with the door-magnetic sensor. Range 1 to 255 s; default 30 s.
- **Door Magnetic Sensor Type** — set to normally open or normally closed to match the installed door contact. If this does not match the actual sensor type, the reported door state will be inverted.
- **Exit Button Type** — set to normally open or normally closed to match the installed exit (request-to-exit) button. Pressing the exit button opens the door directly, without authentication.
- **Door Lock Status** — set to normally open or normally closed to match the installed lock. If this does not match the actual lock type, the lock behavior will be inverted. After a successful authentication, a manual unlock, or a manual lock, the connected lock responds accordingly.

> **WARNING** The **Door Magnetic Sensor Type**, **Exit Button Type**, and **Door Lock Status** settings must match the wiring of the installed hardware. A mismatch inverts the behavior of the door and can leave it unlocked when it should be secured.

13.2.3 RS-485

An external RS-485 card reader can read access-card information so that an enrolled card can be swiped at that reader to open the door.

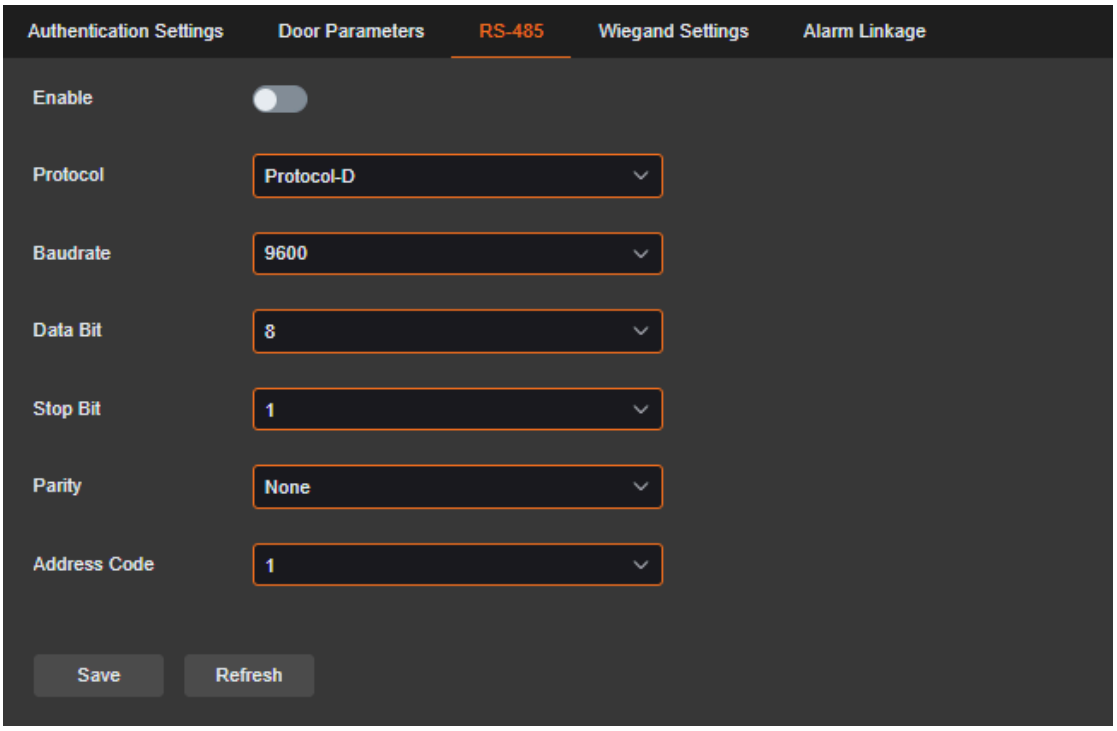

Figure 13-6. RS-485 settings

- **Enable** — the RS-485 enable switch.
- **Protocol** — Pelco-D or Pelco-P over RS-485. The access control camera is fixed to Pelco-D.
- **Baudrate** — the signaling rate of the RS-485 link. The access control camera is fixed to 9600.
- **Data Bit / Stop Bit** — the number of data bits per character and the number of stop bits that mark the end of a packet. Data Bit options are 8, 7, 6, or 5; Stop Bit options are 1 or 2. The access control camera is fixed to 8 data bits and 1 stop bit.

- **Address Code** — the command-receiving address. This is obtained automatically by the access control camera and is not editable.

> **NOTE** On the OCTAVUE access control camera the RS-485 protocol, baud rate, data/stop bits, and address are preset; only the **Enable** switch is configurable. These fixed values are shown for reference when wiring a compatible reader.

13.2.4 Wiegand Settings

Enable this switch to connect a Wiegand card reader and open the door by swiping a card. The access control camera supports Wiegand 26 and Wiegand 34 protocol readers.

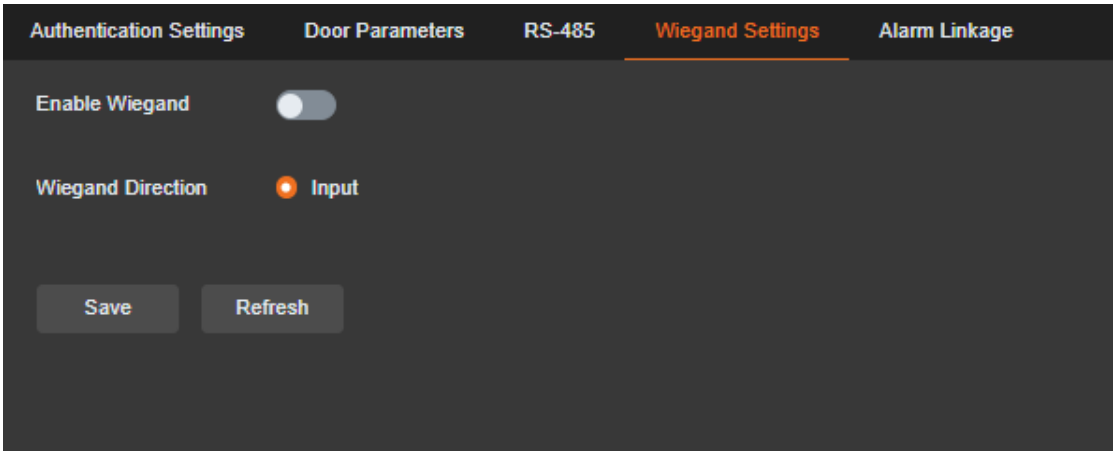

Figure 13-7. Wiegand Settings

- **Enable Wiegand** — the Wiegand card-reader enable switch.

13.2.5 Alarm Linkage

Access-control alarms can trigger a set of linked responses. Three alarm sources are available: authentication failure, door-open timeout, and tamper. Each source has its own linkage configuration, and the available actions are the same across all three.

The linkage actions are:

- **Event Push Platform** — pushes the event to the configured management platform.
- **Email** — sends an email when the event is triggered. Click the settings or schedule button to configure the email parameters and the active time period.
- **Picture Upload** — uploads alarm snapshots to the linked FTP server. The FTP server must be configured first; click the settings button to select the channels whose snapshots are uploaded.
- **Video Upload** — uploads alarm video to the linked FTP server. The FTP server must be configured first; click the settings button to select the channels whose video is uploaded.
- **Siren** — the deterrence-siren linkage switch. When the alarm is triggered, the siren responds according to the parameters on the deterrence settings page. Click the settings button to configure them directly.
- **Recording Channel** — the recording-linkage switch. Click the settings button to select the channels that record the corresponding alarm type when the alarm is triggered.
- **Recording Delay** — how long recording continues after the alarm ends.
- **Notification** — the custom-push switch. Click the settings button to open the custom notification page, where a custom push URL and related options are defined.

13.2.5.1 Authentication Failure

Raised when face authentication fails. Available links are Event Push Platform, Email, Picture Upload, Video Upload, Siren, Recording Channel, Recording Delay, and Notification.

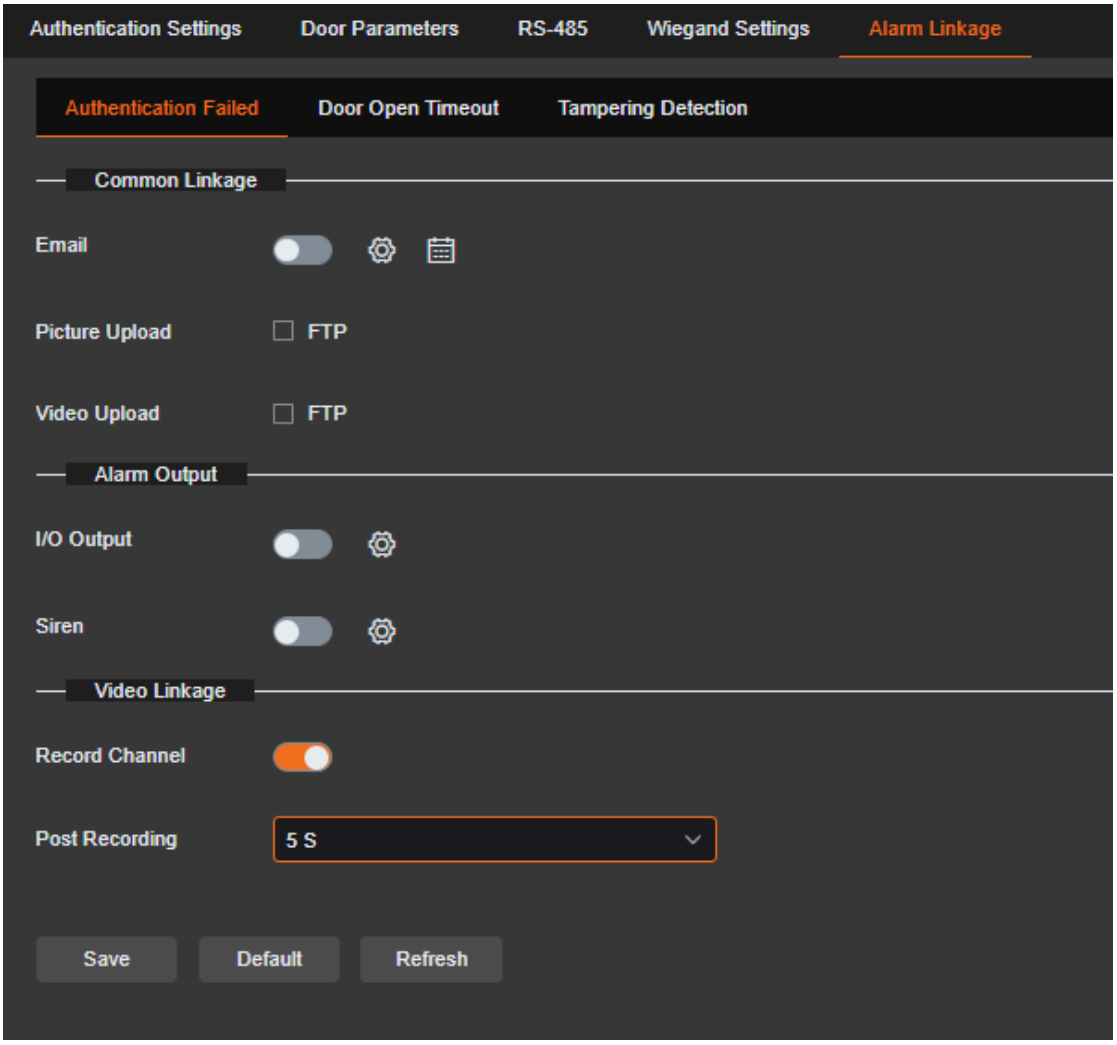

Figure 13-8. Authentication-failure alarm linkage

13.2.5.2 Door Open Timeout

Raised when the door is not closed within the configured timeout. Available links are Event Push Platform, Email, Picture Upload, Video Upload, Siren, Recording Channel, Recording Delay, and Notification.

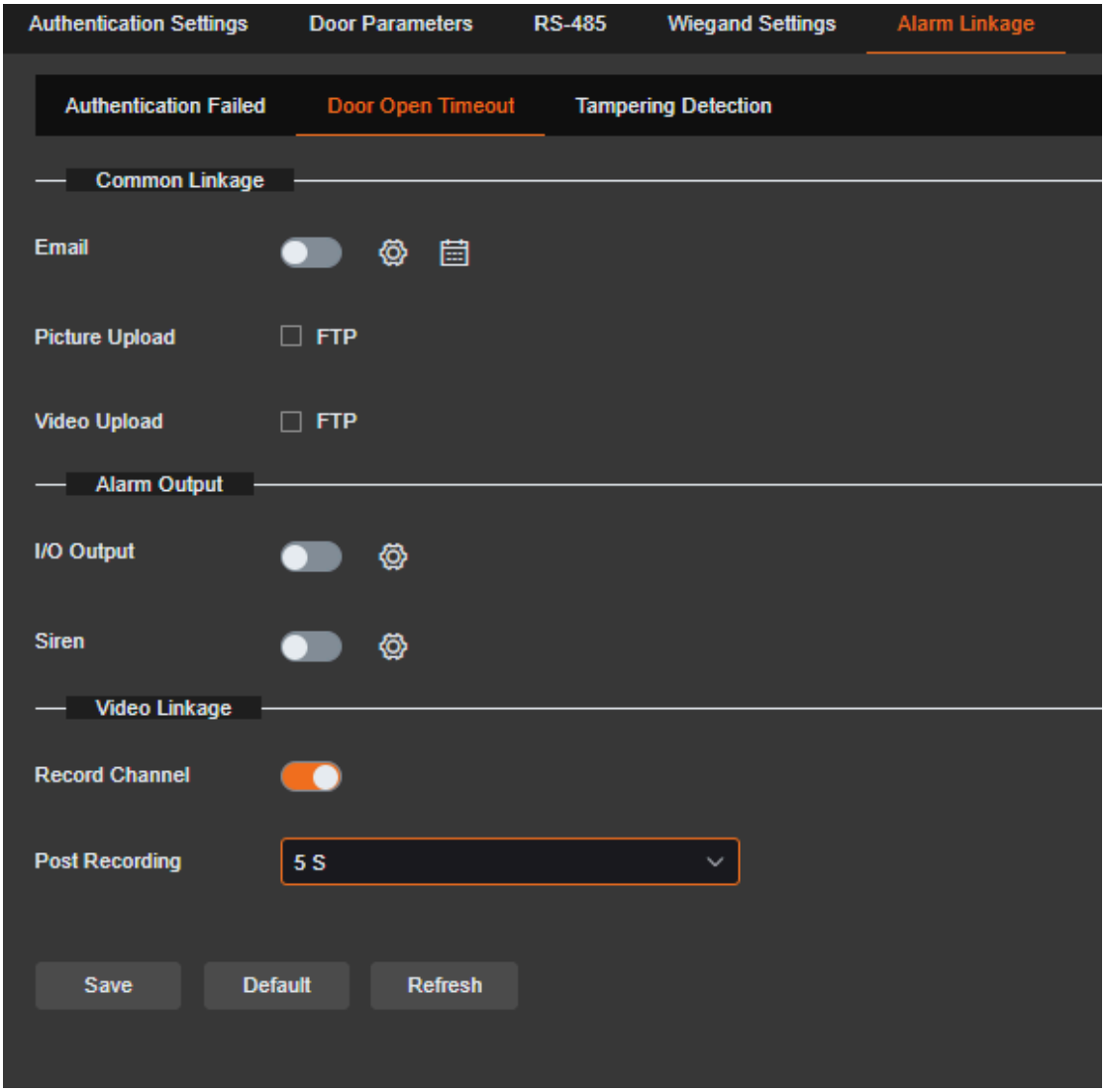

Figure 13-9. Door-open timeout alarm linkage

13.2.5.3 Tamper

Raised when the camera is tampered with or removed. Available links are Event Push Platform, Email, Picture Upload, Video Upload, Siren, Recording Channel, Recording Delay, and Notification.

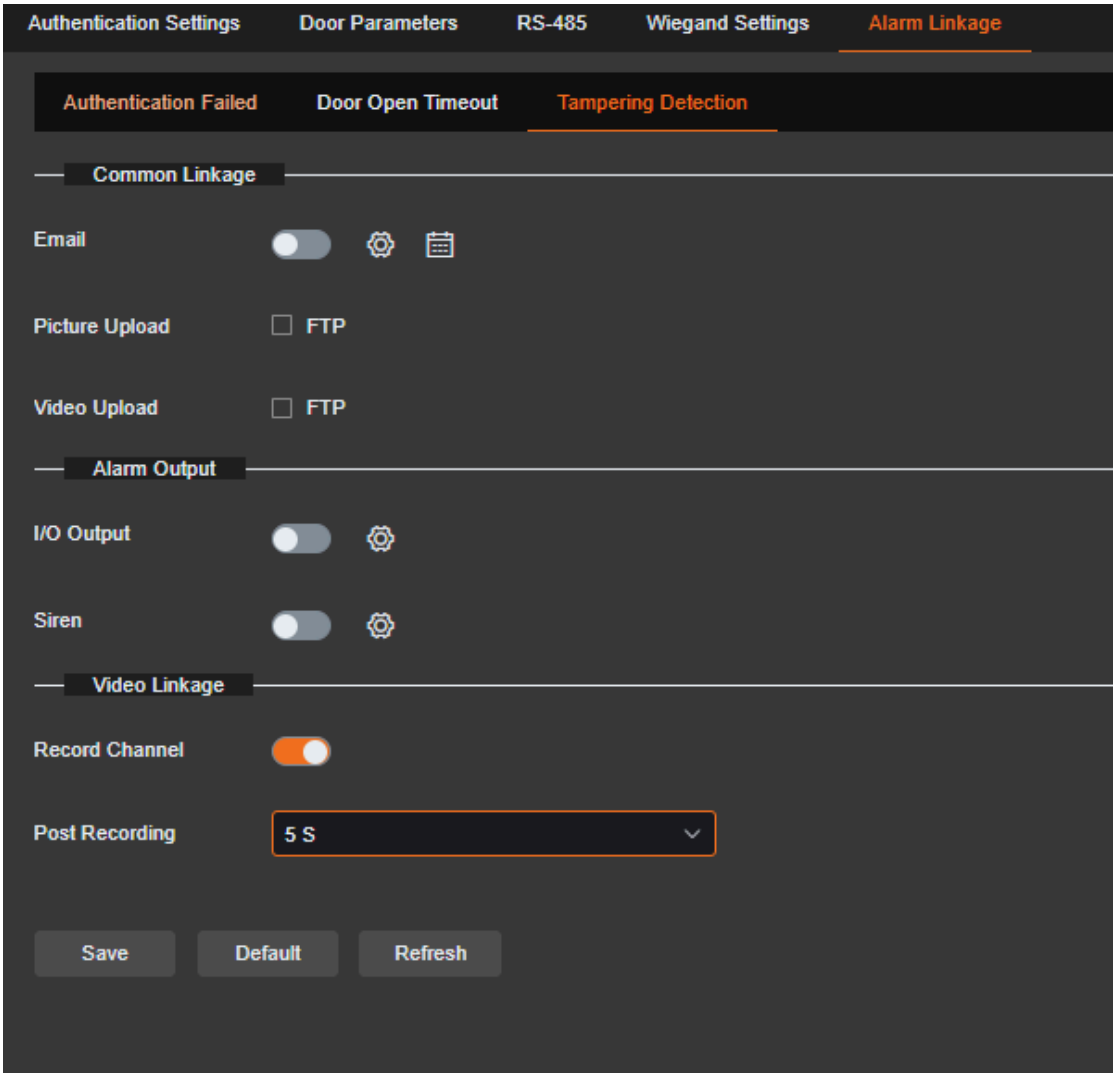

Figure 13-10. Tamper alarm linkage

13.3 Intercom

The integrated intercom lets the access control camera place and receive audio and video calls, either directly between devices (Peer to Peer) or through a SIP server. This area covers call behavior, SIP account and recipient setup, and DTMF rules for remote door control during a call.

13.3.1 Call Setup

This page controls general call behavior. An unanswered call is automatically ended once the call timeout is reached. To make SIP calls, enable the SIP switch, then configure a SIP server account on the SIP Account Setup page and a recipient on the SIP Recipient page. With incoming SIP calls allowed, a SIP phone can call the access control camera; with automatic answering enabled, the camera answers those calls automatically. Video calls can be started when the SIP client supports them.

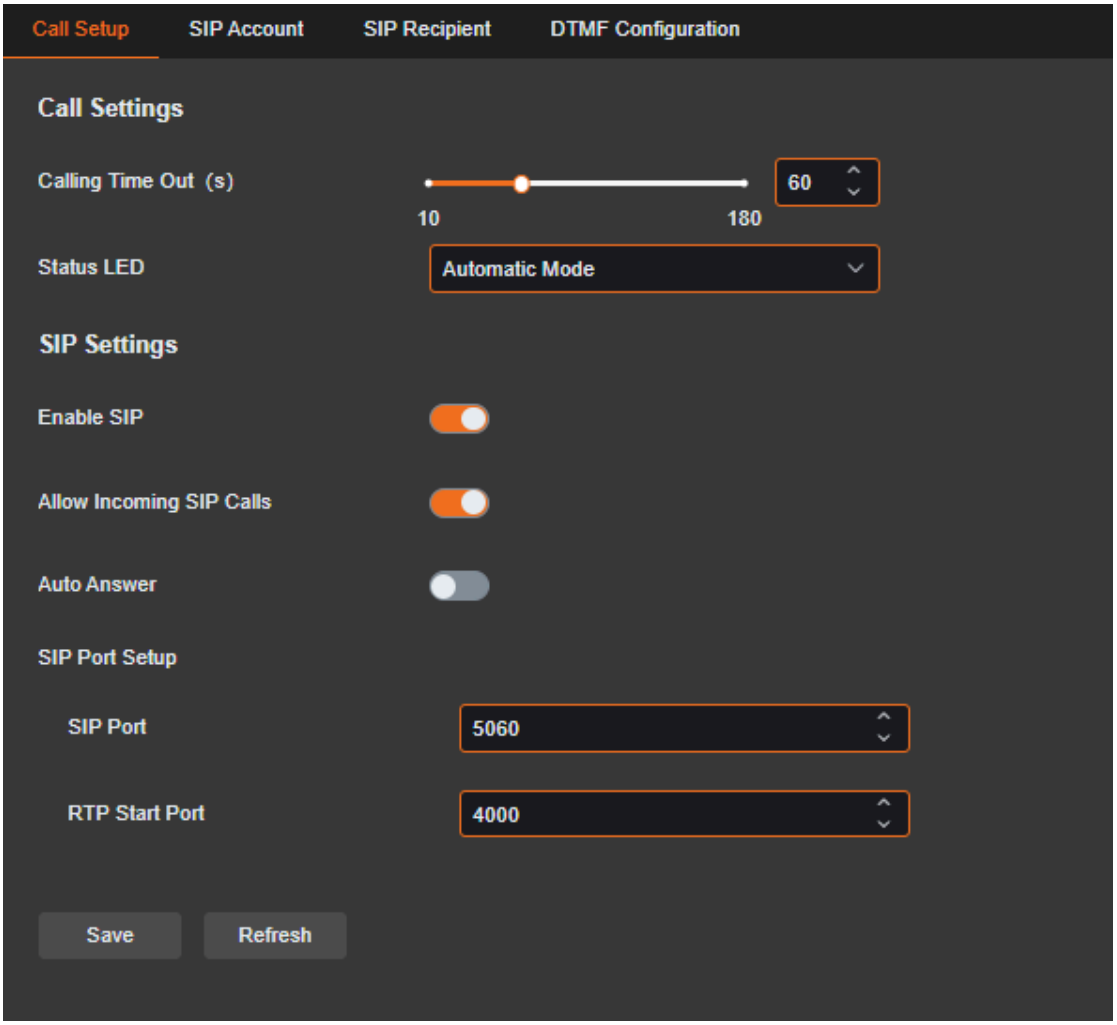

Figure 13-11. Call Setup

- **Calling Time Out** — how long the device rings before an unanswered call is automatically ended. Range 10 to 180 s; default 60 s.
- **Status LED** — the indicator-light mode: automatic, constant on, or off.
- **Enable SIP** — enables outgoing SIP calls.
- **Allow Incoming SIP Calls** — allows the camera to receive SIP calls.
- **Auto Answer** — automatically answers an incoming SIP call.
- **SIP Port** — the SIP signaling port.
- **RTP Start Port** — the starting port for the RTP media stream.

> **NOTE** When a video call is established, the encoding format is forced to H.264 for compatibility with the calling client.

13.3.2 SIP Account Setup

This page defines the SIP call account. By default the camera uses a Peer to Peer account, for which only the name can be changed. Up to 7 SIP server accounts can be added, but only one account can be enabled at a time; the enabled account shows as available and the remaining accounts show as unavailable.

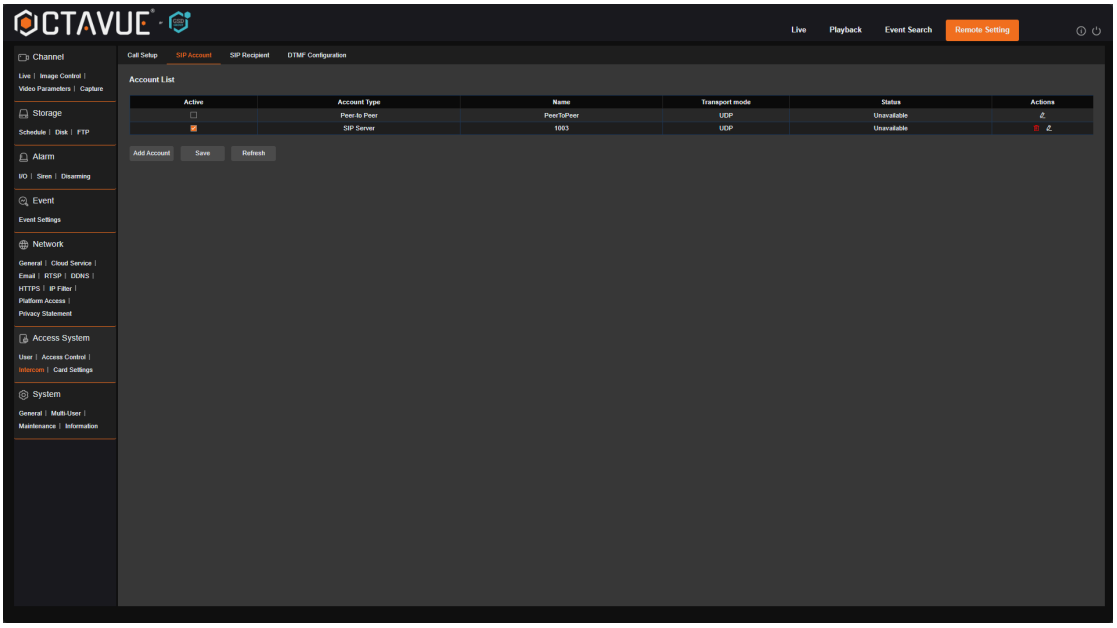

Figure 13-12. SIP Account Setup

Click add to create a SIP server account and enter its parameters:

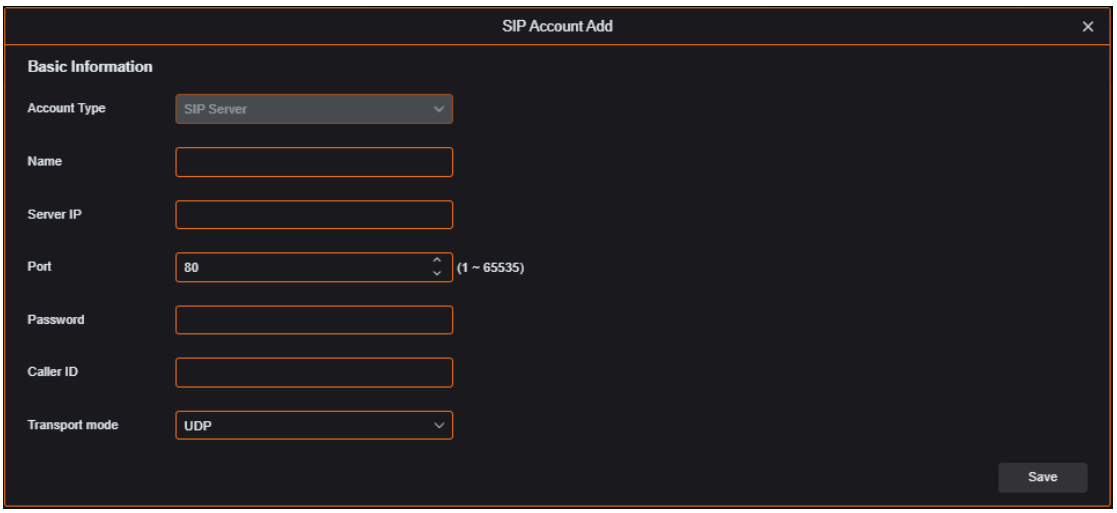

Figure 13-13. Adding a SIP server account

- **Account Type** — set to the SIP Server type.
- **Name** — the account name.
- **Server IP** — the IP address of the SIP server.
- **Port** — the SIP server port.
- **Password** — the account password.
- **Caller ID** — the caller identification presented for the account.
- **Transport Mode** — the transport protocol: UDP, TCP, or TLS.

> **TIP** Use **TLS** as the transport mode where the SIP server supports it, so that signaling between the camera and the server is encrypted.

13.3.3 SIP Recipient

This page manages the contacts the camera can call. Both Peer to Peer and SIP Server recipient types can be added, up to a maximum of 16 recipients in the contact list.

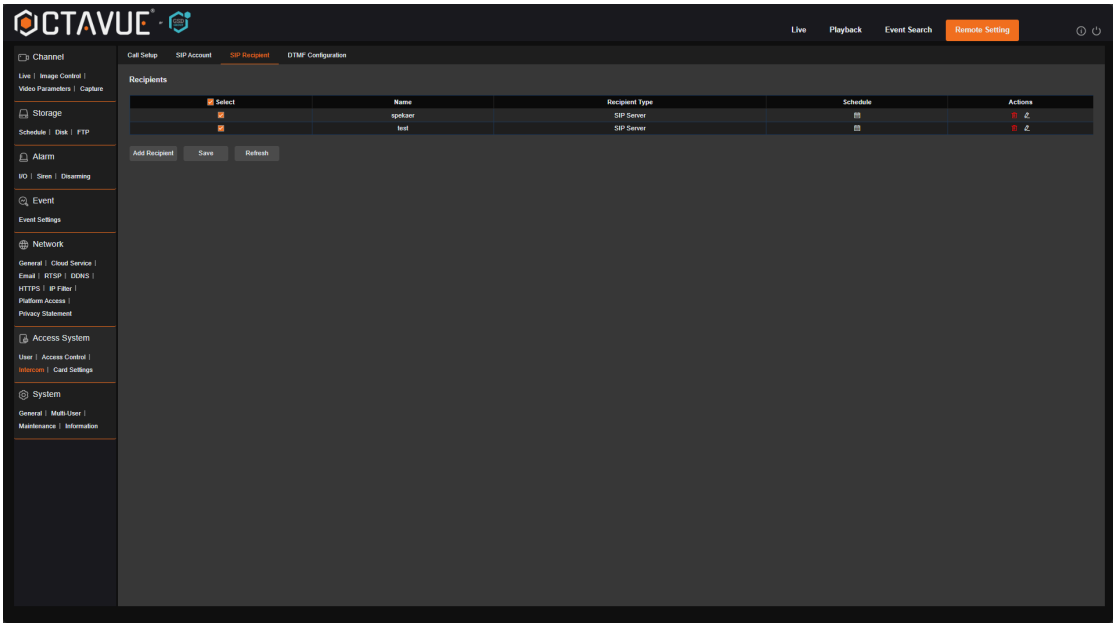

Figure 13-14. SIP Recipient list

For a **SIP Server** recipient, enter:

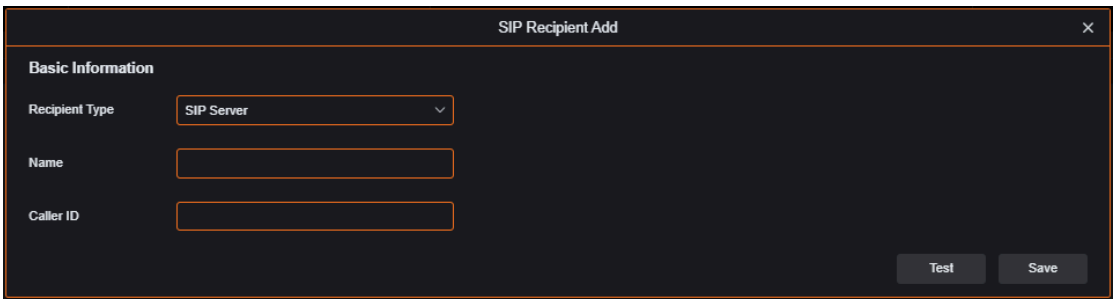

Figure 13-15. Adding a SIP server recipient

- **Recipient Type** — set to SIP Server.
- **Name** — the recipient account name.
- **Caller ID** — the caller identification for the recipient.

For a **Peer to Peer** recipient, enter:

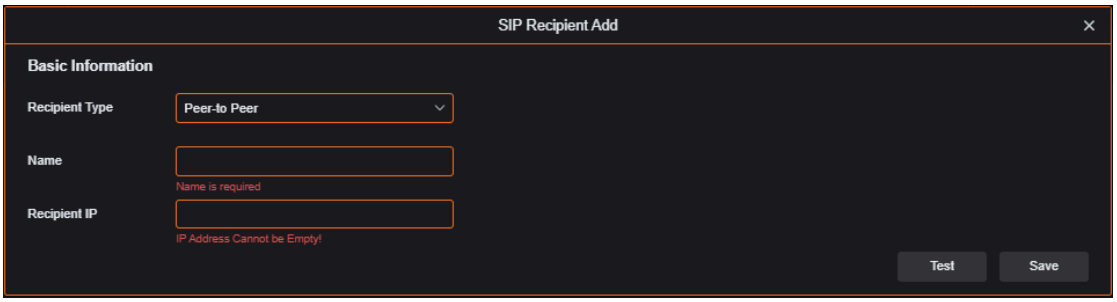

Figure 13-16. Adding a Peer to Peer recipient

- **Recipient Type** — set to Peer to Peer.
- **Name** — the recipient account name.
- **Recipient IP** — the IP address of the recipient device.

13.3.4 DTMF Configuration

DTMF rules let the person on a SIP call operate the door remotely from the call keypad. Once a rule is enabled, entering the corresponding keypad code followed by # during a SIP call performs the mapped action, such as opening or closing the door. Up to 16 rules can be added, and no two rules may share the same keypad code.

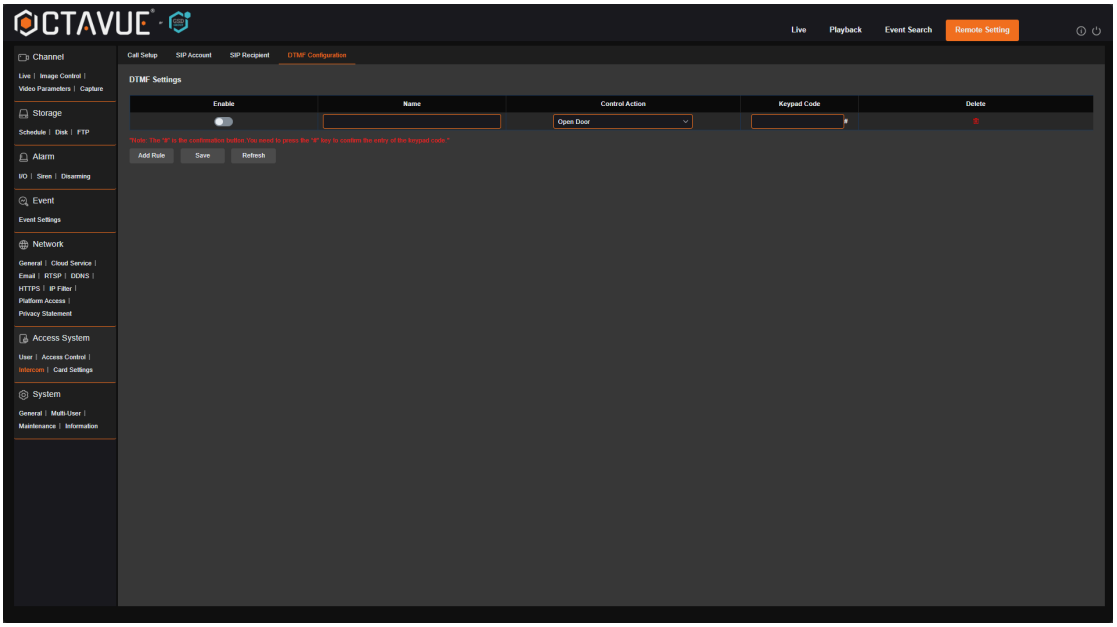

Figure 13-17. DTMF Configuration

- **Enable** — the switch that activates the rule.
- **Name** — the rule name.
- **Control Action** — the action performed by the rule: open or close.
- **Keypad Code** — the keypad command that invokes the rule.
- **Delete** — removes the corresponding rule.
- **Add Rule** — creates a new rule.

CAUTION A DTMF rule allows the door to be opened remotely from a call keypad. Restrict which recipients can reach the camera and keep keypad codes confidential to prevent unauthorized entry.

13.4 Card Settings

The **Card Settings** area selects which contactless card technologies the camera reads and how card numbers are interpreted when a third-party reader is used.

13.4.1 Card Type

Select which card technologies are enabled. NFC, Mifare, and Desfire are supported. The three types are controlled independently and are not mutually exclusive, so any combination can be enabled at once.

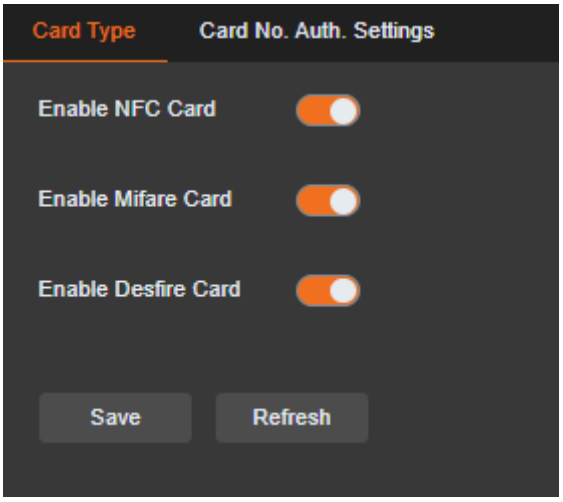

Figure 13-18. Card Type

- **Enable NFC Card** — enables or disables NFC cards.
- **Enable Mifare Card** — enables or disables Mifare cards.
- **Enable Desfire Card** — enables or disables Desfire cards.

13.4.2 Card Number Authentication

Select how card numbers are read: the Full Card Number protocol, the Wiegand 26 protocol, or the Wiegand 34 protocol. As long as the access controller supports the Full Card Number protocol and can automatically detect the Wiegand format, it is compatible with both Wiegand 26 and Wiegand 34 readers. When Full Card Number is selected, readers using either the Wiegand 26 or the Wiegand 34 protocol are recognized normally.

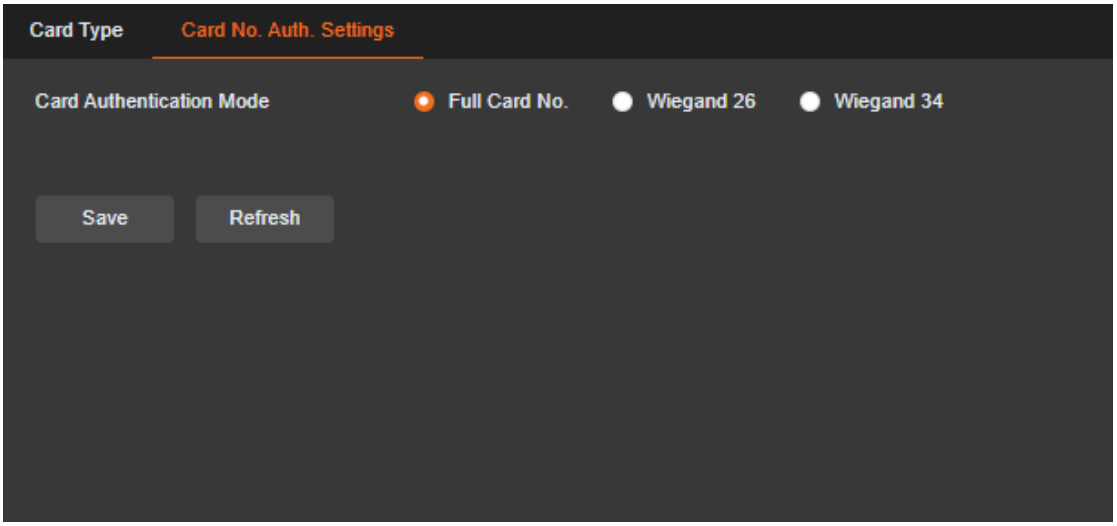

Figure 13-19. Card Number Authentication

- **Full Card No.** — the full card-number protocol. When selected, full-card-number readers and compatible readers are supported.
- **Wiegand 26** — when selected, only Wiegand 26 protocol readers are supported.
- **Wiegand 34** — when selected, only Wiegand 34 protocol readers are supported.

> **NOTE** These options apply only to third-party card readers. The card reader built into the access control camera is unaffected by this setting.

Chapter 14 System, Users & Maintenance

This chapter covers the administrative settings that keep the OCTAVUE access control camera accurate, secure, and up to date: the system clock and daylight saving time, multi-user accounts and permissions, routine maintenance tasks such as log review, firmware upgrade and parameter backup, and the read-only pages that report device and privacy information.

14.1 General System Setup

The general system settings define how the camera keeps time. An accurate clock is essential for meaningful log entries, scheduled recordings, and access events, so configure the time source, time zone, and daylight saving rules before placing the camera into service.

14.1.1 Date and Time

Open the date and time page to set how the camera obtains and displays the current time.

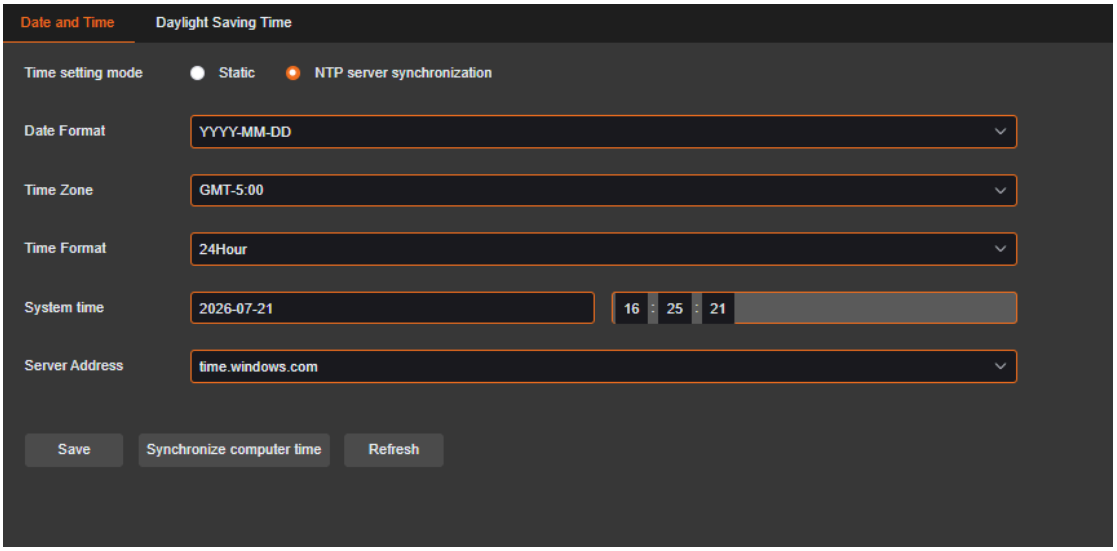

Figure 14-1. Date and time settings

Configure the following options:

- **Time Settings Mode** — choose **Manual** or **NTP**. In manual mode you enter the time yourself; in NTP mode the camera synchronizes automatically with a network time server.
- **Date Format** — select the preferred order for day, month, and year.
- **Time Zone** — select the time zone that matches the camera's region or city.
- **Time Format** — choose between the 24-hour and 12-hour clock.
- **System Time** — click the field to set the current date and time manually.
- **Synchronize with Computer Time** — apply the clock of the computer you are using to the camera.
- **Server Address** — in NTP mode, select the time server used for synchronization.

> **NOTE** When **NTP** synchronization is selected, the system time cannot be set manually; the camera obtains the time from the configured server.

14.1.2 Daylight Saving Time

Daylight saving time (DST) advances the clock by a fixed offset during part of the year. Enable this function if the camera's time zone or region observes daylight saving time.

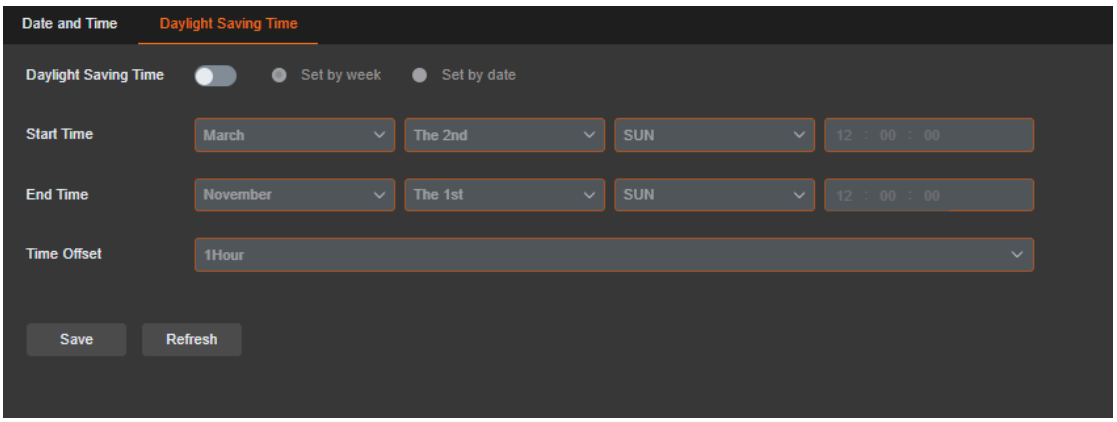

Figure 14-2. Daylight saving time settings

- **Daylight Saving Time** — enable this option if the camera's time zone observes daylight saving time.
- **Set by Week** — define the start and end of the DST period by month, week, and time of day (for example, the first Sunday of the month at 2:00 a.m.).
- **Set by Date** — define the exact calendar dates and times on which daylight saving time begins and ends.
- **Start Time / End Time** — set the moments at which daylight saving time begins and ends.
- **Time Offset** — select the amount of time added during the daylight saving period. This is the difference between Coordinated Universal Time (UTC) and the local time.

14.2 Multi-User Management

This menu lets the administrator create and configure additional accounts, each with its own user name, password, and access rights.

The system supports the following user types:

- **Administrator (ADMIN)** — the system administrator has full control over the configuration and can change both the administrator and user passwords, as well as enable or disable password protection.
- **Normal User (USER)** — a standard account limited to functions such as preview, search, and playback. The administrator can create multiple users, each granted different access rights.

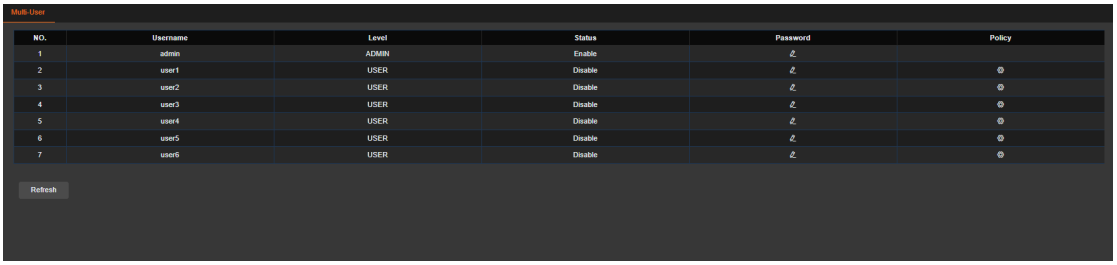

Figure 14-3. User account list

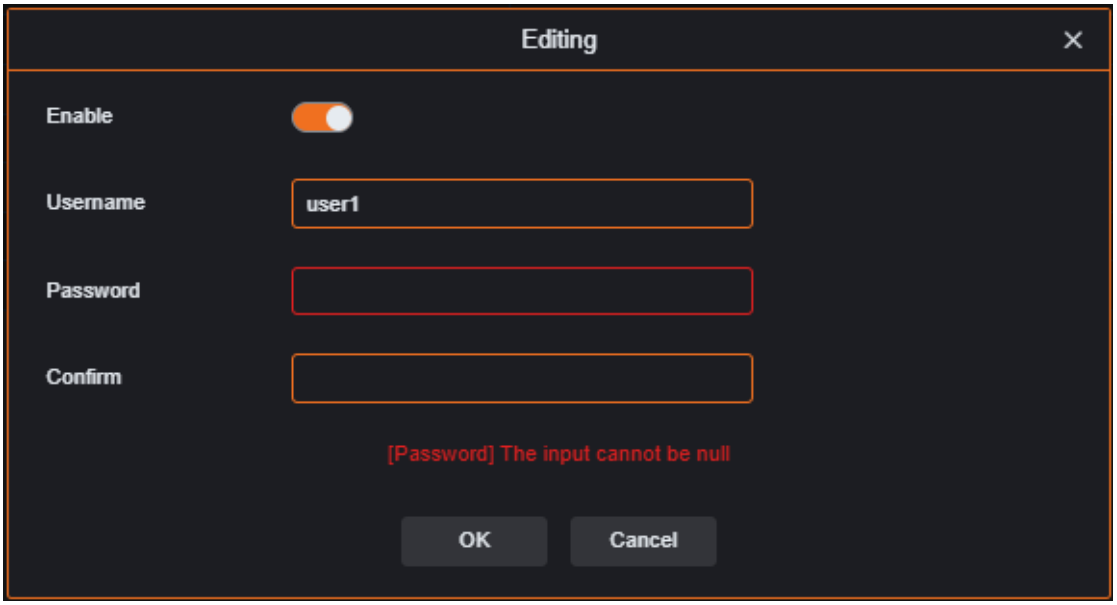

Figure 14-4. Editing a user account

To create or enable a user account:

1. Select one of the currently inactive users and click the **Edit Password** icon.
2. Select **Enable** to activate the account.
3. Click **User Name** to edit the account name.
4. Click the field next to **Password** and enter the desired password.
5. Click the field next to **Confirm** and re-enter the same password.
6. Click **OK**. You will be prompted to enter the administrator password for authentication.

Figure 14-5. Password authentication prompt

To set the permissions for a sub-user, click the account to open the **Policy** page, then select the checkbox beside each function you want to grant. Click **All** to select every permission or **Clear** to remove all selections.

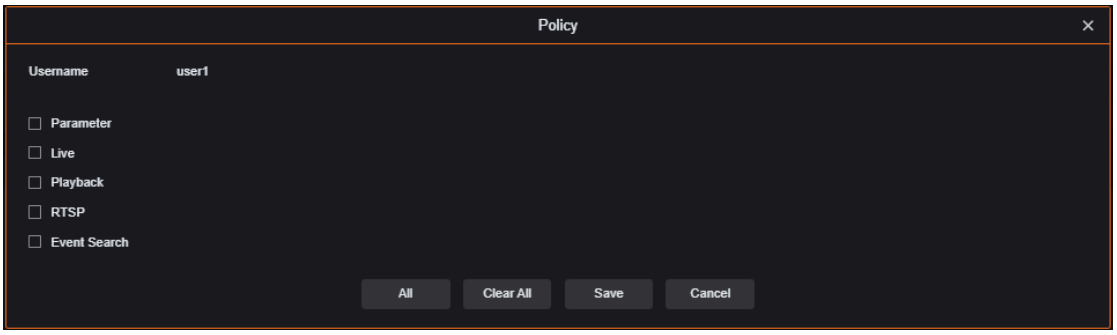

Figure 14-6. Sub-user permission policy page

14.3 System Maintenance

From the system maintenance menu you can search and review system logs, restore factory settings, upgrade the firmware, export and import configuration parameters, schedule automatic reboots, and enable developer mode.

14.3.1 Log Management

The system log records important events such as motion alerts and system warnings. You can search the log by type and time period and export a backup file to your computer.

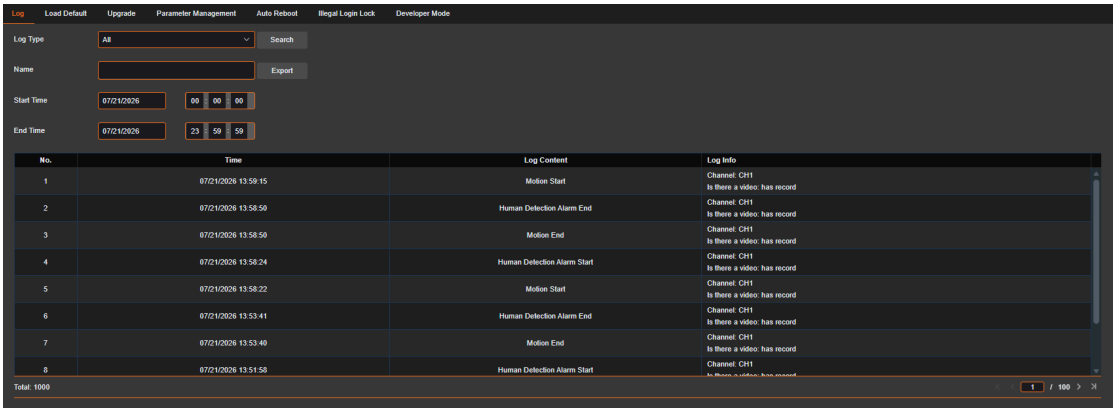

Figure 14-7. Log search and backup

Select a category from the **Log Type** list, or choose **All** to view every event in the selected time period. The available categories are:

- **System** — system settings, reboot, auto reboot, upgrade, time settings, and NTP calibration.
- **Configuration** — changes to live control, privacy masking, recording mode and schedule, main and sub stream, network, email, color, motion detection, storage, multi-user, NTP, image control, mobile stream, RTSP, IP filter, restore factory settings, sound detection, import and export, event push, capture, deterrent, AI, FTP, DDNS, HTTPS, audio, siren, system maintenance, video masking, I/O alarm, and cloud service settings.
- **Alarm** — start and end of motion detection, I/O alarm, pedestrian detection, face detection, authentication failure, and door open timeout, as well as tampering detection events.
- **Account** — login, logout, account lock, and user changes.
- **Recording** — search, playback, and backup.
- **Storage** — disk format, disk full, and disk error.
- **Network** — network disconnected, network online, network errors, and network mode changes.

To search and export the log:

1. From the **Minor Type** list, select the specific event type to search for. (This list is unavailable when the log type is set to **All**.)
2. In the **Name** field, enter a file name for the exported log. Click **Export** to create a system log backup.
3. Click the **Start Time** field and select the start date and time from the on-screen calendar.
4. Click the **End Time** field and select the end date and time from the calendar.
5. Click **Search** to run the query.
6. Review the log entries for the selected time period.

Figure 14-8. System log entries

Figure 14-9. Alarm log entries

Figure 14-10. Account log entries

Figure 14-11. Network log entries

Use the navigation buttons in the lower-right corner of the menu to move between pages of log events.

14.3.2 Load Default Settings

This page offers several reset methods that restore the camera's configuration parameters to their factory values. Restoring factory settings does not format the data stored on the TF card.

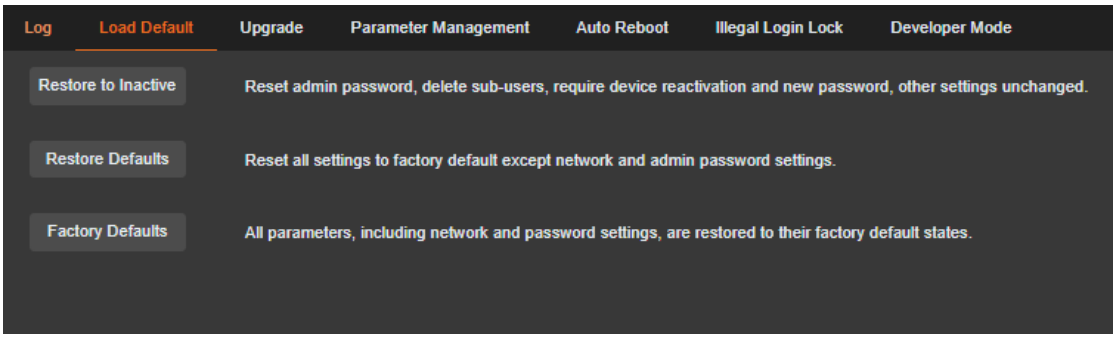

Figure 14-12. Load default settings

- **Restore to Inactive** — resets the administrator password and deletes all sub-users. The camera must be reactivated, but all other page parameters remain unchanged.
- **Restore Defaults** — restores all page parameters to factory values except the network settings and the administrator password.
- **Factory Defaults** — restores every camera parameter to its factory value.

> **CAUTION** Restoring default settings is irreversible and clears your configuration. Depending on the method selected, sub-users, the administrator password, and network settings may be removed, requiring the camera to be reactivated and reconfigured. Export a parameter backup before proceeding.

14.3.3 System Upgrade

This menu lets you upgrade the camera's firmware, either from a file on your computer or by detecting an online upgrade.

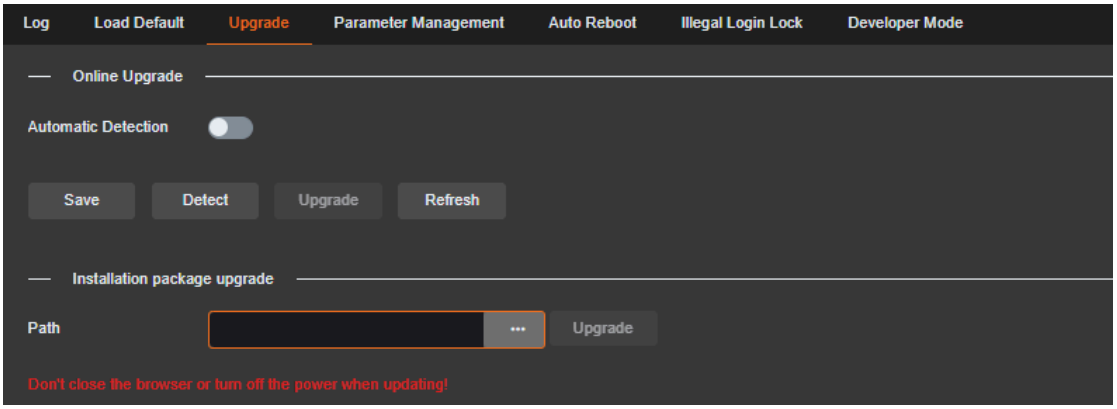

Figure 14-13. System upgrade

- **Automatic Detection** — enable this option to check automatically for online upgrade files.
- **Save** — save the current settings.
- **Detect** — after setting the upgrade path, click to check manually for an online upgrade file. A prompt appears when a new version is available.

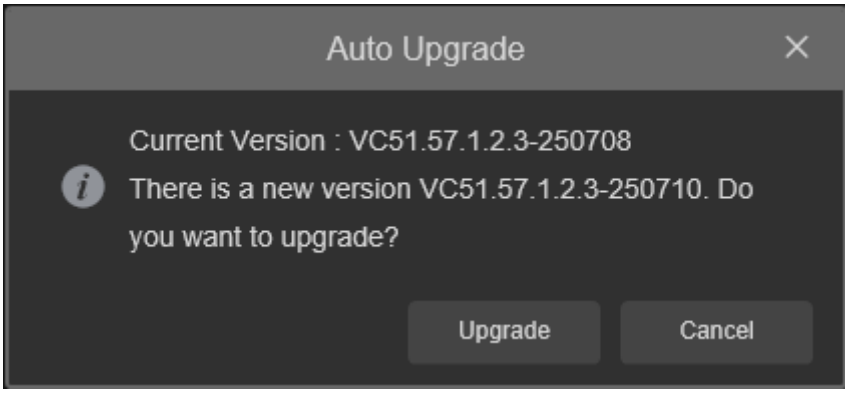

Figure 14-14. New firmware version detected

To upgrade the firmware from a local file:

1. Save the firmware file (a **.bin** file) to your computer's hard drive.
2. Click **...** next to **Path** and select the firmware file on your computer.
3. Click **Upgrade** to begin. The upgrade takes approximately 3 to 4 minutes.

CAUTION Do not turn off the camera's power or close the web interface at any point during the firmware upgrade. Interrupting the process can leave the device inoperable.

NOTE If the camera should check the cloud server for the latest firmware version, enable the cloud service switch to bind the app and clear the online upgrade configuration parameters on this page.

14.3.4 Parameter Management

Parameter management lets you export the configured main-menu settings to a computer, or import a previously saved configuration file back onto the camera.

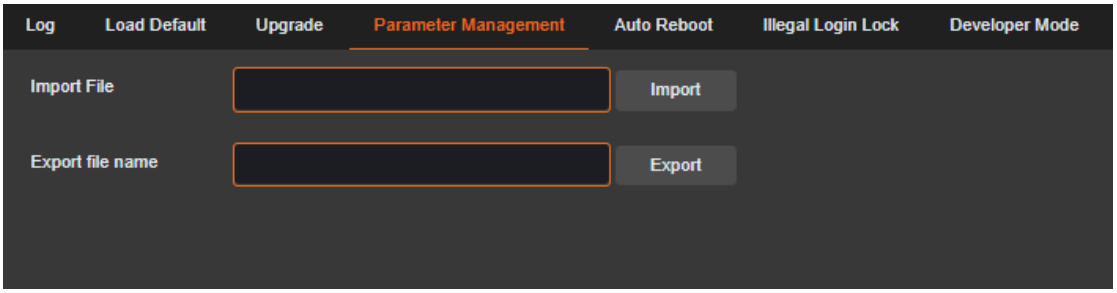

Figure 14-15. Parameter import and export

- **Import File** — click the field to open the path window, select the parameter file, and click **Import** to begin importing.
- **Export File Name** — click the field to enter a name for the exported file, then click **Export** to save the parameters.

14.3.5 Auto Reboot

Automatic reboot lets the camera restart itself on a regular schedule, which helps maintain long-term stability. Keeping this function enabled is recommended.

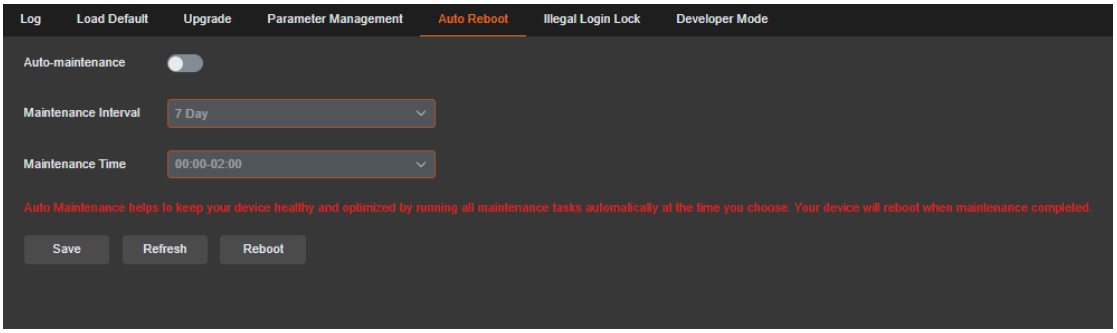

Figure 14-16. Auto reboot settings

- **Auto Maintenance** — enable or disable the automatic maintenance feature.
- **Maintenance Interval** — set how often the camera performs automatic maintenance.
- **Maintenance Time** — set the period during which automatic maintenance occurs. The camera reboots at a random moment within this window.

14.3.6 Developer Mode

Developer mode allows technical staff to collect and record log information for device debugging.

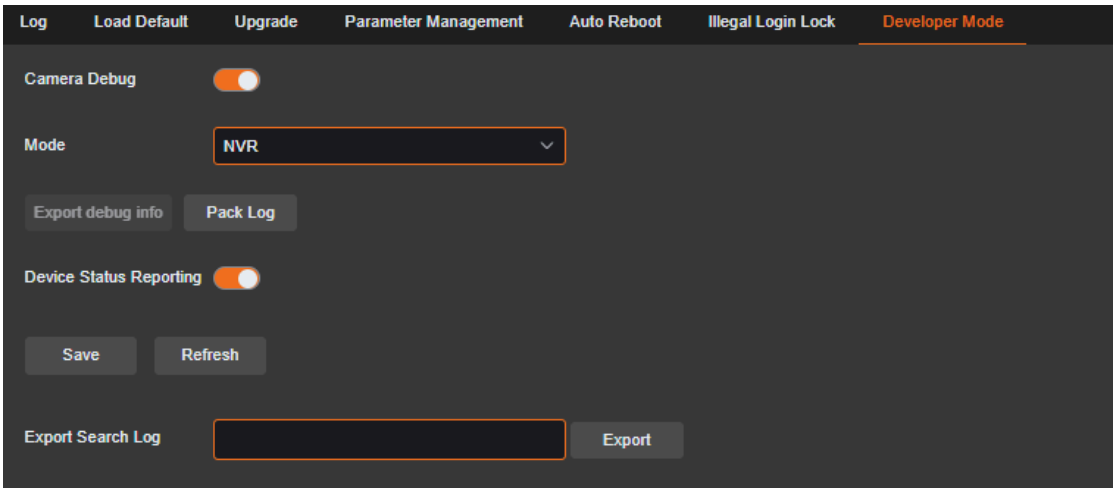

Figure 14-17. Developer mode settings

- **Camera Debug** — select to enable developer mode.
- **Mode** — select the method for collecting and recording debugging information: **NVR**, **SD_Card**, or **FTP**.
- **Download Debug Logs** — in **SD_Card** mode, click this button and enter the correct password to export the debug information to your computer.
- **Pack Log** — in **NVR** or **FTP** mode, click this button to upload the packed log information to the FTP server.
- **Device Status Reporting** — enable to upload storage status, channel status, and device information to the P2P server.
- **Export Search Log** — enter a file name and click **Export** to export all log files stored on the device to your computer.

14.3.7 Illegal Login Lock

The illegal login lock protects the camera against repeated password-guessing attempts by temporarily blocking access after too many consecutive failures.

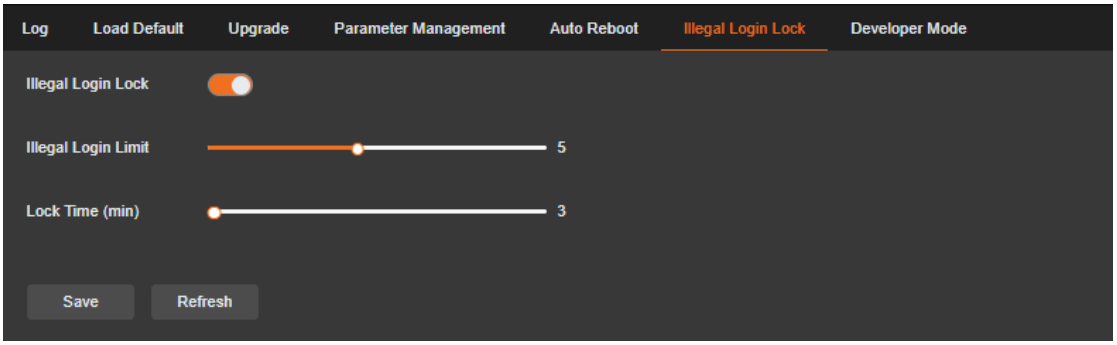

Figure 14-18. Illegal login lock settings

- **Illegal Login Lock** — select to enable the feature.
- **Illegal Login Limit** — set the number of consecutive failed login attempts allowed before the account is locked. Drag the slider to adjust the value.
- **Lock Time (min)** — set how long, in minutes, login is blocked once the limit is reached. Login attempts are allowed again after this period expires. Drag the slider to adjust the value.

14.4 System Information

The system information pages present read-only details about the camera and its privacy agreement.

14.4.1 Device Information

This page displays system information such as the device ID, model name, MAC address, and firmware version.

Figure 14-19. Device information

14.4.2 Privacy Statement

This page presents the full text of the device's privacy agreement for your review.

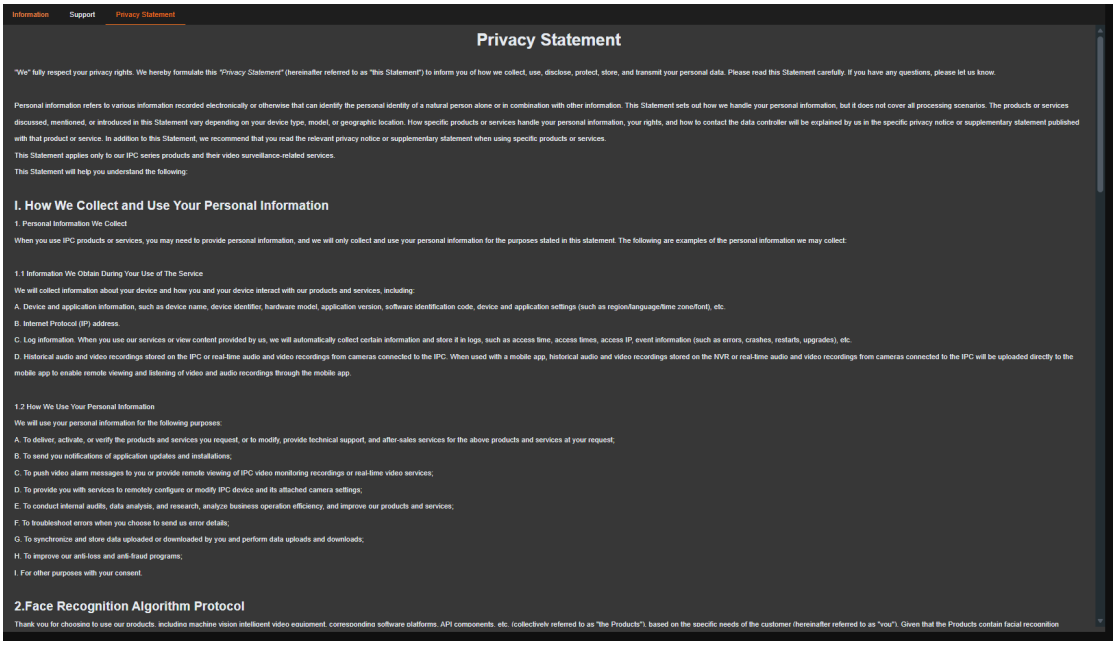

Figure 14-20. Privacy statement