



User Manual

# **Viasecurity Control Center**

## **V1.2.0**



# Contents

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Chapter 1 Introduction to Viasecurity Control Center.....          | 7  |
| 1.1 Recommended Running Environment.....                           | 8  |
| 1.2 Feature and Capability Differences: Free vs. Full Version..... | 10 |
| 1.3 Hardware Specifications and Peak Performance Metrics.....      | 16 |
| 1.4 Decoding Capabilities.....                                     | 20 |
| Chapter 2 Get Started.....                                         | 23 |
| 2.1 Activate License.....                                          | 23 |
| 2.1.1 Online Activation Method.....                                | 23 |
| 2.1.2 Offline Activation Method.....                               | 24 |
| 2.2 Adding Devices.....                                            | 26 |
| 2.2.1 Server Adding and Details Management.....                    | 29 |
| 2.3 Configuring Local Settings.....                                | 31 |
| 2.3.1 Event and Alarm.....                                         | 31 |
| 2.3.2 Advanced System Parameters.....                              | 32 |
| 2.3.3 Video Display Settings.....                                  | 33 |
| Chapter 3 Video Monitoring.....                                    | 35 |
| 3.1 System Setup and Preparations.....                             | 35 |
| 3.1.1 Encoding device integration.....                             | 35 |
| 3.1.2 Managing Hardware Settings.....                              | 36 |
| 3.2 Core Surveillance Tools.....                                   | 39 |
| 3.2.1 Live Video and Playback Operations.....                      | 39 |



|                                                                        |    |
|------------------------------------------------------------------------|----|
| 3.2.2 Real-time PTZ control.....                                       | 43 |
| 3.2.3 Monitor via Cameras on the Map.....                              | 43 |
| 3.3 Face Picture Comparison and Human Body Detection.....              | 47 |
| 3.3.1 Add Face Picture Libraries and Face Pictures.....                | 47 |
| 3.3.2 View Videos Related to Face and Human Body Recognition.....      | 49 |
| 3.3.3 Search for Recognized Face Pictures and Human Body Pictures..... | 51 |
| 3.3.4 Search Targets by a Picture.....                                 | 53 |
| 3.4 Vehicle Operations.....                                            | 54 |
| 3.4.1 Add Vehicle Lists and Vehicles.....                              | 54 |
| 3.4.2 View Video Related to Vehicle Monitoring.....                    | 55 |
| 3.4.3 Search and Export ANPR Events.....                               | 56 |
| 3.5 Smart Search Capabilities.....                                     | 58 |
| 3.5.1 Smart Search / VCA.....                                          | 58 |
| 3.5.2 TargetTrace and Object Search.....                               | 61 |
| 3.5.3 People Counting Analytics and Reports.....                       | 62 |
| Chapter 4 Access Control and Video Intercom.....                       | 65 |
| 4.1 Preparations.....                                                  | 66 |
| 4.1.1 Add Devices.....                                                 | 66 |
| 4.1.2 View Details of a Device.....                                    | 67 |
| 4.1.3 View Details of a Door.....                                      | 68 |
| 4.2 Add Departments and Persons.....                                   | 69 |
| 4.2.1 Credential Configuration.....                                    | 72 |
| 4.2.2 Protect Profile Pictures.....                                    | 73 |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| 4.3 Managing Access Levels.....                                   | 74  |
| 4.4 Add an Alarm.....                                             | 75  |
| 4.5 Real-Time Monitoring of Doors.....                            | 78  |
| 4.5.1 Monitor Doors and Control Door Status.....                  | 80  |
| 4.5.2 Display and Control Doors on the Map.....                   | 82  |
| 4.6 Video Intercom Setup and Operations.....                      | 83  |
| 4.7 Event Management, Search, and Analytics.....                  | 85  |
| 4.7.1 Searching and Exporting Event Logs.....                     | 85  |
| 4.7.2 Importing Missing Authentication Logs.....                  | 87  |
| 4.7.3 Data Statistics and Dashboards.....                         | 88  |
| Chapter 5 Storage Management.....                                 | 90  |
| 5.1 Preparations.....                                             | 91  |
| 5.2 Storage Location and Capacity Allocation.....                 | 91  |
| 5.3 Storage Schedule Configuration.....                           | 92  |
| 5.4 Video Playback and VCA Search.....                            | 94  |
| 5.5 Data Retention Lifecycle.....                                 | 95  |
| 5.6 Advanced Storage Management.....                              | 96  |
| 5.6.1 Network Interface Controller (NIC) Assignment.....          | 96  |
| 5.6.2 Rebuild Index.....                                          | 96  |
| 5.6.3 Maintenance.....                                            | 96  |
| Chapter 6 Viasecurity Control Center Monitoring Interface.....    | 98  |
| Chapter 7 Search.....                                             | 102 |
| 7.1 Search for Detected Vehicles or Persons by Cameras/Doors..... | 102 |

|                                                               |     |
|---------------------------------------------------------------|-----|
| 7.2 Search for Detected Persons or Vehicles in VCA Areas..... | 105 |
| 7.3 Search for Detected Persons/Vehicles by Features.....     | 106 |
| Chapter 8 Event and Alarm Management.....                     | 107 |
| 8.1 Supported Triggering Events.....                          | 107 |
| 8.3 Add an Alarm.....                                         | 123 |
| 8.4 Supported Linkage Actions.....                            | 124 |
| 8.5 Managing Configured Alarms.....                           | 126 |
| 8.6 Monitoring, Searching, and Exporting Alarms.....          | 126 |
| Chapter 9 System Access and Account Administration.....       | 129 |
| 9.1 User and System Role Administration.....                  | 129 |
| 9.1.1 Add a User.....                                         | 129 |
| 9.1.2 Managing and Maintaining the User List.....             | 130 |
| 9.1.3 Configuring System Roles.....                           | 130 |
| 9.2 Account Security and Credential Recovery.....             | 137 |
| 9.2.1 Account Security Configurations.....                    | 137 |
| 9.2.2 Reset Login Password.....                               | 137 |
| Chapter 10 System Configuration.....                          | 139 |
| 10.1 Configure Email Parameters.....                          | 139 |
| 10.2 Managing Holiday Schedules.....                          | 140 |
| 10.3 Managing Network and Communication Interfaces.....       | 140 |
| 10.3.1 Configure Internet Time Sync.....                      | 141 |
| 10.3.2 Configure Device Access Protocol.....                  | 141 |
| 10.3.3 Configure WAN Access.....                              | 141 |

|                                                                |     |
|----------------------------------------------------------------|-----|
| 10.3.4 Configure NIC Settings.....                             | 142 |
| 10.3.5 Network Reset Information.....                          | 142 |
| 10.4 Securing HTTPS Connections with SSL/TLS Certificates..... | 142 |
| 10.4.1 Certificate Management.....                             | 143 |
| 10.4.2. Get Your SSL/TLS Certificate.....                      | 143 |
| 10.5 Configure Service Component Certificate.....              | 145 |
| 10.6 Privacy and Security.....                                 | 146 |
| Chapter 11 Maintenance.....                                    | 147 |
| 11.1 Generate and Display Maintenance Report.....              | 147 |
| 11.2 Search for Notifications.....                             | 151 |
| 11.3 Search for System Logs.....                               | 152 |
| A. Product Usage Restrictions: Scenarios & Guidelines.....     | 155 |



# Chapter 1 Introduction to Viasecurity Control Center

## Center

Engineered to consume minimal system resources, Viasecurity Control Center is a streamlined Video Management Software solution designed to deliver an optimized user experience. This platform centralizes application and configuration features across multiple domains, including video surveillance, Automatic Number Plate Recognition (ANPR), video intercom, and access control.

Thanks to its highly intuitive user interface and clear built-in guidance, operators can rapidly deploy and navigate the system with minimal training. Furthermore, the software offers broad interoperability with a variety of third-party hardware. A mobile client provides features such as alarm monitoring, video playback, and real-time viewing.

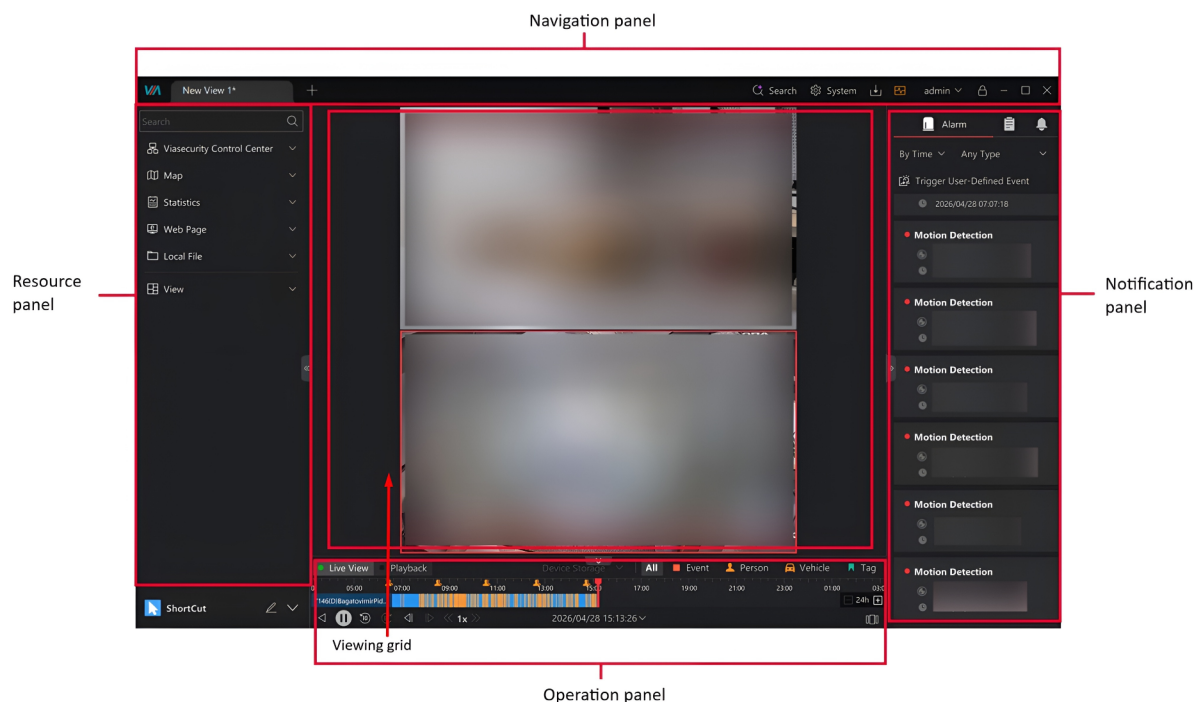


Figure 1.1 Main Page

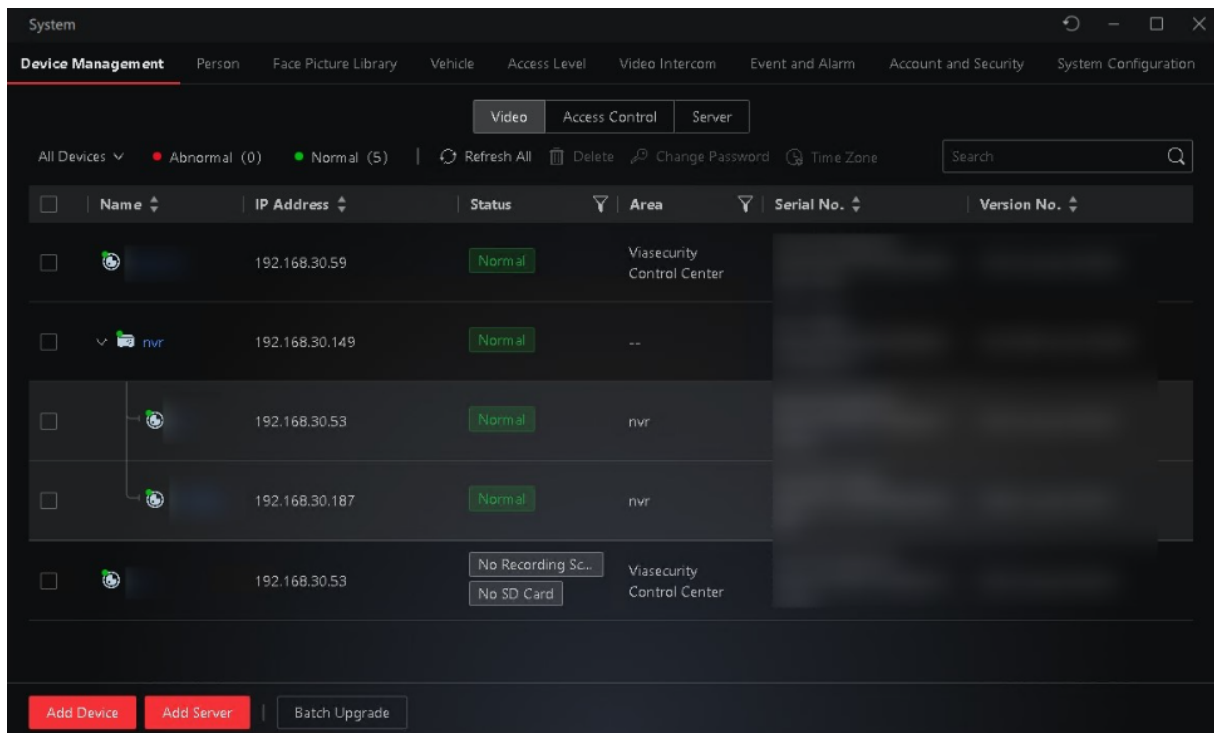


Figure 1.2 System Window

## 1.1 Recommended Running Environment

Table 1.1 Recommended Running Environment

| Platform      | OS                                                                                                                                                                                                                                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server        | <ul style="list-style-type: none"> <li>● Microsoft® Windows Server 2025</li> <li>● Microsoft® Windows Server 2022</li> <li>● Microsoft® Windows Server 2019 64-bit</li> <li>● Microsoft® Windows Server 2016 64-bit</li> <li>● Microsoft® Windows 11 64-bit</li> <li>● Microsoft® Windows 10 64-bit</li> </ul> |
| Desktop       | <ul style="list-style-type: none"> <li>● Microsoft® Windows Server 2025</li> <li>● Microsoft® Windows Server 2022</li> <li>● Microsoft® Windows Server 2019 64-bit</li> <li>● Microsoft® Windows Server 2016 64-bit</li> <li>● Microsoft® Windows 11 64-bit</li> <li>● Microsoft® Windows 10 64-bit</li> </ul> |
| Mobile Client | <ul style="list-style-type: none"> <li>● iOS 14.0+</li> <li>● Android 8.0+</li> </ul>                                                                                                                                                                                                                          |

## 1.2 Feature and Capability Differences: Free vs. Full Version

This section outlines the core functional distinctions and maximum performance capacities between the Free version and the Full version of Viasecurity Control Center.

### Maximum Performance

**Table 1.2 Manageable Resources**

| Performance                                              | Full Version                                                                                                                                                            | Free Version |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Total Camera Channels                                    | 128<br>*Includes numbers of TargetTrace cameras, ANPR cameras, people counting cameras, cameras for face picture comparison & body recognition, and third-party cameras | 16           |
| People Counting Cameras                                  | 128                                                                                                                                                                     | 0            |
| TargetTrace Cameras                                      | 128                                                                                                                                                                     | 0            |
| ANPR Cameras                                             | 8                                                                                                                                                                       | 0            |
| Cameras for Face Picture Comparison and Body Recognition | 16                                                                                                                                                                      | 0            |
| Third-Party Cameras                                      | 128                                                                                                                                                                     | 0            |
| Doors                                                    | 32                                                                                                                                                                      | 2            |
| External Streaming Servers                               | 64                                                                                                                                                                      | 64           |

**Table 1.3 Others**

| Performance | Full Version | Free Version |
|-------------|--------------|--------------|
| Vehicles    | 2,000        | 0            |

**Table 1.4 Access Control**

| <b>Performance</b> | <b>Full Version</b>                                       | <b>Free Version</b>                                       |
|--------------------|-----------------------------------------------------------|-----------------------------------------------------------|
| Persons            | 500                                                       | 500                                                       |
| Credentials        | Cards: 1,000<br>Face Pictures: 500<br>Fingerprints: 1,000 | Cards: 1,000<br>Face Pictures: 500<br>Fingerprints: 1,000 |

**Table 1.5 Users**

| <b>Performance</b>                               | <b>Full Version</b> | <b>Free Version</b> |
|--------------------------------------------------|---------------------|---------------------|
| Local Users                                      | 128                 | 128                 |
| Roles                                            | 64                  | 64                  |
| Users Logged in Simultaneously via Desktop       | 64                  | 3                   |
| Users Logged in Simultaneously via Mobile Client | 64                  | 3                   |

## Core Features

The following features are **available only in the full version**.

### People Counting Report

- Access to comprehensive people counting reports

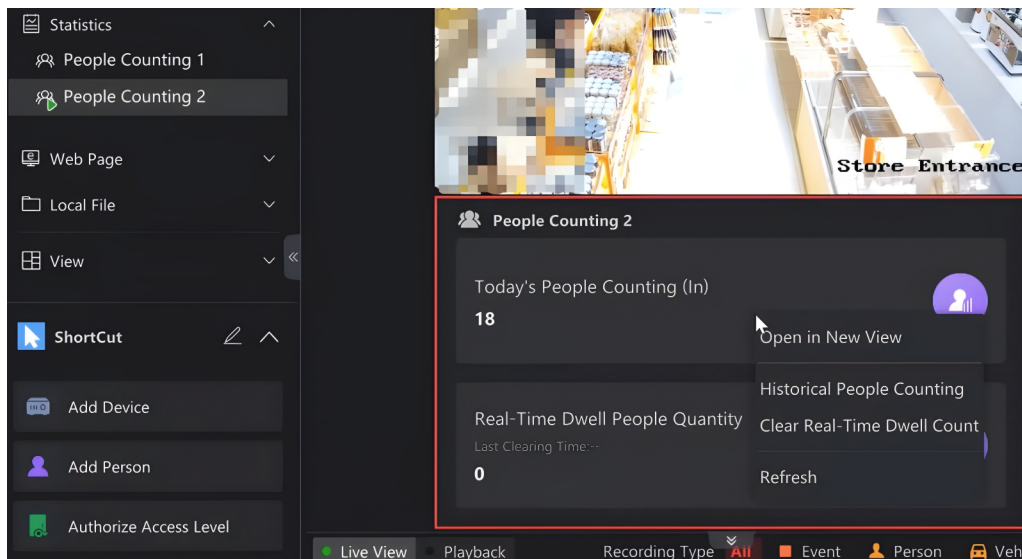


Figure 1.4 People Counting Report

### Vehicle Search

- Users can filter and search for specific vehicles based on identifiable characteristics by navigating to **Search → Vehicle Passing Event**

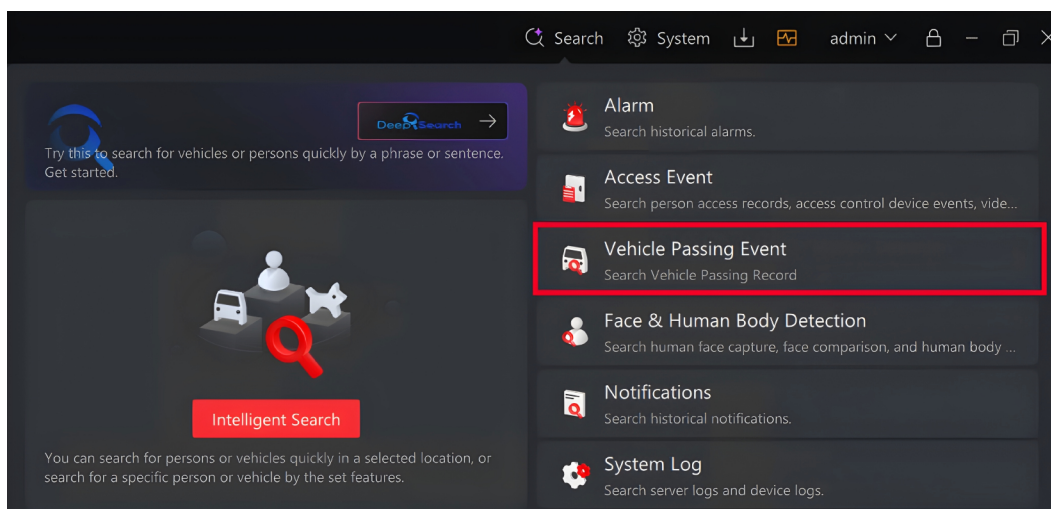


Figure 1.5 Vehicle Passing Event

- or **Search** → **Intelligent Search**

Target

Person

Vehicle

If you select Person in System, searching by vehicle features will be not allowed.

Country/Region

Please enter country/region name to search.

License Plate No.

☐ With License Plate

☐ No License Plate

Vehicle Owner

Please enter vehicle owner name.

Type

Please enter vehicle type to search.

Brand

Please enter brand name to search.

Color

OK

Cancel

Figure 1.6 Search for Vehicles by Features

- Furthermore, the system enables license plate and vehicle list management when integrated with ANPR cameras.

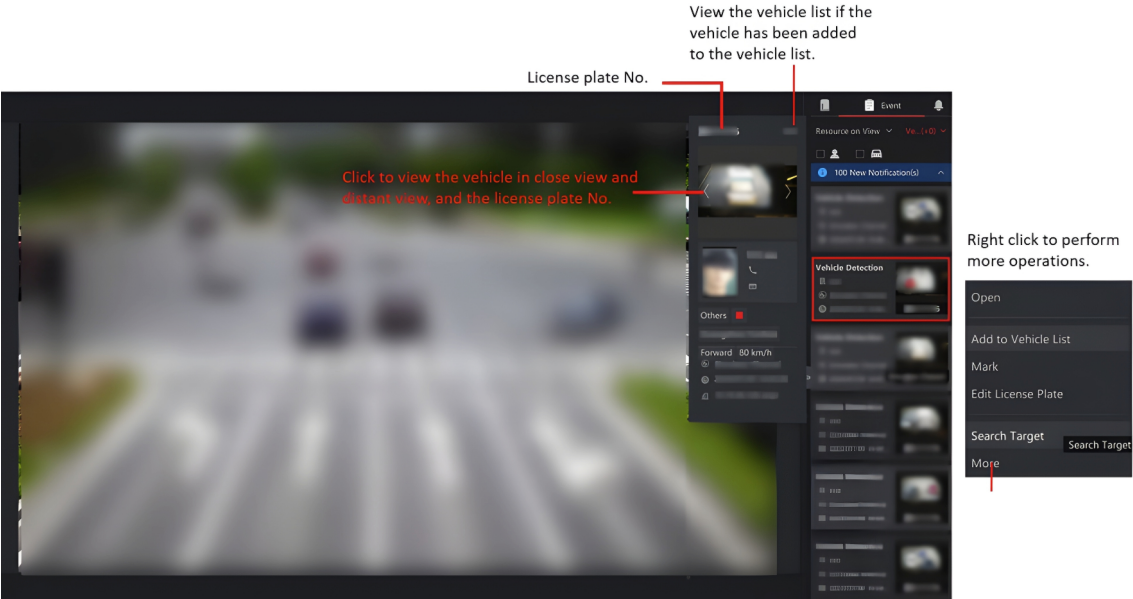


Figure 1.7 ANPR Camera

## Face Picture Comparison

- The software allows personnel searches via specific traits through **Search → Face & Human Body Detection**

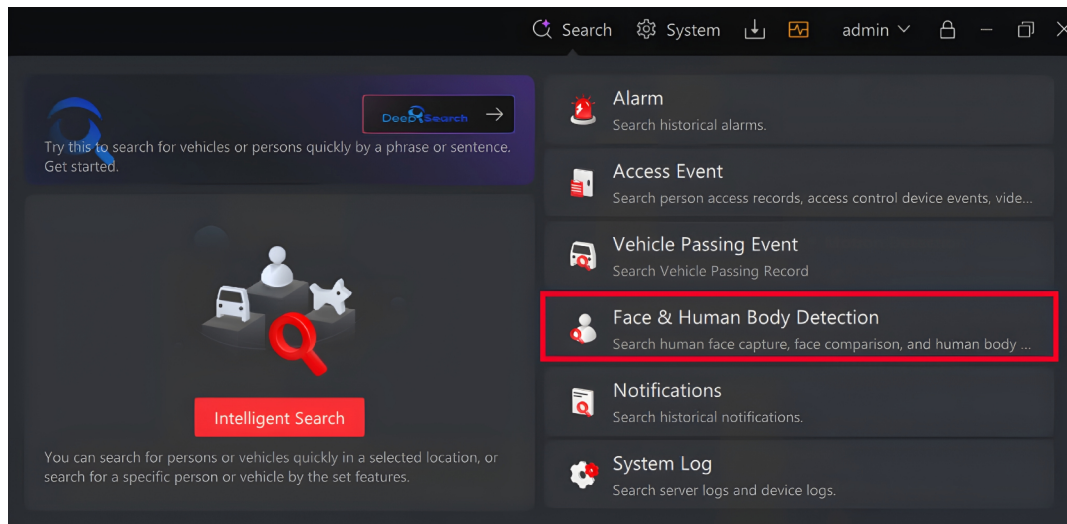


Figure 1.8 Face & Human Body Detection

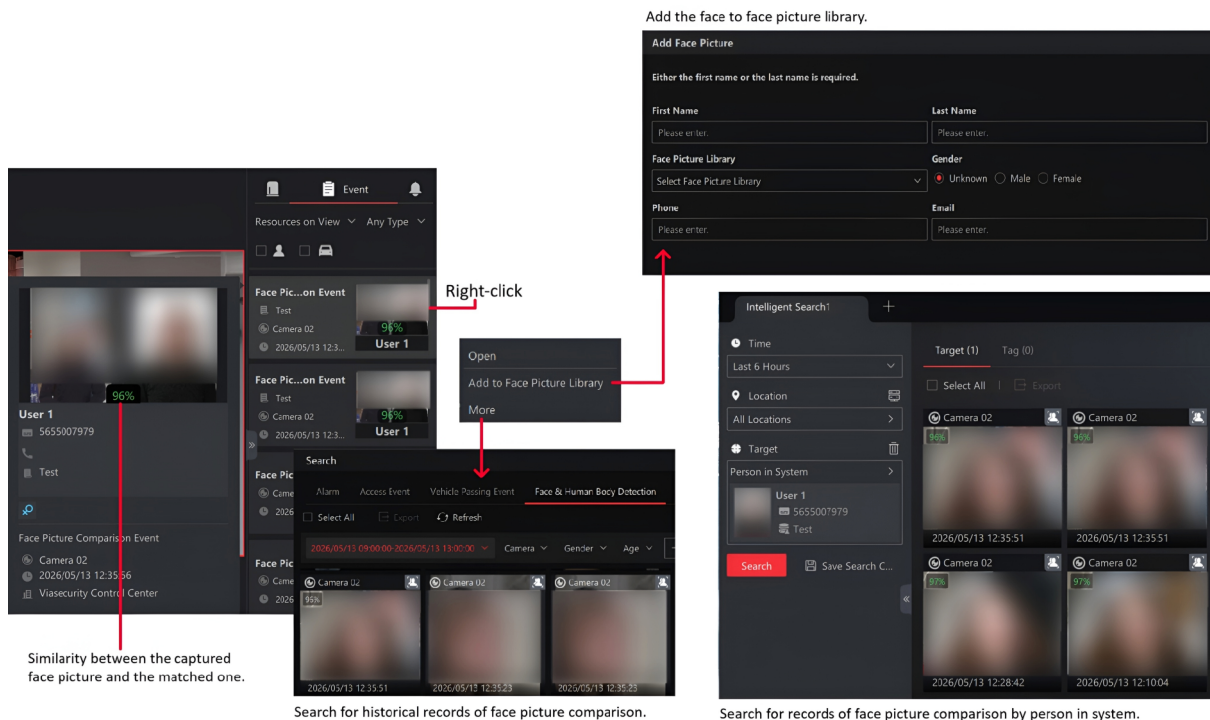
- and **Search → Intelligent Search**

A screenshot of a software application window titled 'Intelligent Search'. The window is divided into two main sections. On the left, there is a 'Target' section with two options: 'Person' (selected and highlighted with a red border) and 'Vehicle'. Below these options, there is a text box that says 'If you select Person in System, searching by vehicle features will be not allowed.' On the right, there is a 'Person Feature' section with a 'Person in System' tab. This section contains several categories of search criteria: 'Gender' (Male, Female), 'Age Group' (Teenage, Youth, Middle Age, Elderly, Infant, Child, Adolescent, Adult, Middle Age and Elderly), 'Accessories' (Wearing Glasses, No Glasses, Wearing Sunglasses, Wearing Mask, No Mask, Carrying Backpack, No Backpack), 'Hair Style' (Long Hair, Short Hair), and 'Tops Type' (Short Sleeves, Long Sleeves). At the bottom right of the window, there are two buttons: 'OK' (highlighted in red) and 'Cancel'.

Figure 1.9 Search for Persons by Features



- Face picture comparison is fully supported when utilizing TargetTrace and dedicated facial recognition cameras



**Figure 1.10 Camera for Face Picture Comparison**

### Search by Face/Body Pictures

Operators can upload reference images and define specific parameters to locate matching face or body pictures. Right-clicking on any search result also allows for rapid retrieval of visually similar images.

### Server Disk Storage

- The Full Edition permits direct video recording to server disk storage.

*(Note: The Free Edition is restricted to storing only files and static pictures.)*

### Extended Third-Party Integration

- Broad compatibility is unlocked for cameras utilizing ONVIF protocols, as well as devices from Hikvision, Dahua, Axis, and Hanwha.

### Mobile Client / Desktop

- Concurrent connectivity is scaled up to 64 simultaneous logins across Desktop and Mobile Clients.

*(Note: The Free version caps this at 3 concurrent logins. Mobile access is automatically granted once a base license is activated, eliminating the need for a separate mobile license.)*

## 1.3 Hardware Specifications and Peak Performance Metrics

The operational limits of the Viasecurity Control Center have been benchmarked using specific hardware environments. Table 1.6 details the two primary setups utilized to determine these baseline capabilities.

### System Configurations

**Table 1.6 Hardware Environments**

| Feature                   | Configuration 1                                                                                        | Configuration 2                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| CPU                       | Intel® Core™ i5-12500                                                                                  | Intel® Core™ i7-12700                                                                                  |
| RAM                       | 2*8 GB                                                                                                 | 2*8 GB                                                                                                 |
| NIC                       | 1 GbE Network Interface Card                                                                           | 1 GbE Network Interface Card                                                                           |
| SSD for OS                | Enterprise Class SSD                                                                                   | Enterprise Class SSD                                                                                   |
| HDD for Video Storage     | Enterprise-class HDD or high-performance network HDD. It should support writing or reading of 10 MB/s. | Enterprise-class HDD or high-performance network HDD. It should support writing or reading of 20 MB/s. |
| SSD Capacity for Database | At least 500 GB                                                                                        | At least 500 GB                                                                                        |
| OS                        | Microsoft® Windows 10 64-bit or later                                                                  | Microsoft® Windows 10 64-bit or later                                                                  |

The following subsections document the absolute maximum system of capacities achievable under these validated conditions.

## Resource Capacities

**Table 1.7 Resource Capacities**

| Resource Type                                                                     | Configuration 1                                                                              | Configuration 2                                                                              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Cameras<br>(Including cameras accessed by ONVIF protocol and third-party cameras) | 128<br>(No more than 8 ANPR cameras and 16 cameras for face picture comparison are allowed.) | 128<br>(No more than 8 ANPR cameras and 16 cameras for face picture comparison are allowed.) |
| Doors                                                                             | 32                                                                                           | 32                                                                                           |
| External Streaming Servers                                                        | 64                                                                                           |                                                                                              |

## Video Processing Constraints

The system's built-in streaming server is restricted to processing a maximum of 200 internal channels, capped at a combined input/output bandwidth of 400 Mbps.

## Access Control

**Table 1.8 Access Control Parameters**

| Parameter        | Configuration 1 | Configuration 2 |
|------------------|-----------------|-----------------|
| Persons          | 500             | 500             |
| Cards            | 1,500           | 1,500           |
| Profile Pictures | 500             | 500             |

## Monitoring and Control Panel Thresholds

Table 1.9 defines the rendering and management of ceilings within the primary monitoring interface.

**Table 1.9 Main Monitoring Interface Capacities**

| Parameter                   | Configuration 1                                                                                  | Configuration 2                                                                                  |
|-----------------------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Resources in One View       | 64                                                                                               | 64                                                                                               |
| Resources in Multiple Views | 256                                                                                              | 256                                                                                              |
| Areas                       | 256                                                                                              | 256                                                                                              |
| Map                         | <ul style="list-style-type: none"><li>• Total E-Maps: 16</li><li>• Maps in One View: 4</li></ul> | <ul style="list-style-type: none"><li>• Total E-Maps: 16</li><li>• Maps in One View: 4</li></ul> |

**Table 1.10 Hardware-Independent UI Parameters**

| Parameter                          | Performance |
|------------------------------------|-------------|
| New Windows                        | 4           |
| Views                              | 64          |
| Area Levels                        | 5           |
| Resources on GIS Map or Each E-Map | 256         |

## Users, Roles, and Permissions

**Table 1.11 User and Role Metrics**

| Parameter                      | Configuration 1 | Configuration 2 |
|--------------------------------|-----------------|-----------------|
| Local Users                    | 128             | 128             |
| Roles                          | 64              | 64              |
| Online Users on Desktop        | 64              | 64              |
| Online Users on Mobile Clients | 64              | 64              |

## Event and Alarm

**Table 1.12 Performance of Event and Alarm**

| Parameter                                                              | Configuration 1 | Configuration 2 |
|------------------------------------------------------------------------|-----------------|-----------------|
| Events Receiving                                                       | 20/s            | 20/s            |
| Number of Alarm Rules                                                  | 1000            | 1000            |
| Speed of Pushing Alarms/Events/Notifications from Server to One Client | 20/s            | 20/s            |

## Data Archiving and Storage Limits

**Table 1.13 Storage Performance Parameters**

| Parameter                                                                                                                     | Configuration 1 | Configuration 2 |
|-------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------------|
| Video Storage Throughput                                                                                                      | 480 Mbps        | 600 Mbps        |
| Retention Period of Captured Faces, ANPR Records, Events, Intelligent Analysis Data, Access Records, and System Logs          | 3 Years         | 3 Years         |
| Storage Capacity (including captured faces, ANPR records, events, intelligent analysis data, access records, and system logs) | 10 million      | 10 million      |

## 1.4 Decoding Capabilities

The client decoding capabilities detailed in this section were evaluated within a dedicated client hardware setup. Table 1.14 defines the specific testing configuration used to establish these limits.

**Table 1.14 Client Decoding Hardware Configuration**

| Feature       | Configuration                           |
|---------------|-----------------------------------------|
| CPU           | Intel® Core™ i5-12500 3.0.0 GHz         |
| RAM           | 16 (8+8) GB                             |
| NIC           | Intel® Ethernet Connection (17) I219-LM |
| Graphics Card | Intel® UHD Graphics 770                 |
| OS            | Microsoft® Windows 10 (64-bit)          |

The matrices below break down the maximum number of simultaneous live view streams achievable via hardware-accelerated and software-based decoding, categorized by H.264 and H.265 compression formats.

### H.264

**Table 1.15 Hardware Decoding Benchmarks for H.264**

| Frame Rate (fps) | Bit Rate (Mbps) | Resolution | Max. Live View Channels |
|------------------|-----------------|------------|-------------------------|
| 30               | 6               | 1080p      | 35                      |
| 30               | 12              | 8 MP       | 10                      |
| 25               | 6               | 1080p      | 42                      |
| 25               | 12              | 8 MP       | 12                      |

**Table 1.16 Software Decoding Benchmarks for H.264**

| Frame Rate (fps) | Bit Rate (Mbps) | Resolution | Max. Live View Channels |
|------------------|-----------------|------------|-------------------------|
| 30               | 6               | 1080p      | 15                      |
| 30               | 12              | 8 MP       | 5                       |
| 25               | 6               | 1080p      | 17                      |
| 25               | 12              | 8 MP       | 6                       |

## H.265

**Table 1.17 Hardware Decoding Benchmarks for H.265**

| Frame Rate (fps) | Bit Rate (Mbps) | Resolution | Max. Live View Channels |
|------------------|-----------------|------------|-------------------------|
| 30               | 3               | 1080p      | 41                      |
| 30               | 6               | 8 MP       | 11                      |
| 25               | 3               | 1080p      | 45                      |
| 25               | 6               | 8 MP       | 15                      |

**Table 1.18 Software Decoding Benchmarks for H.265**

| Frame Rate (fps) | Bit Rate (Mbps) | Resolution | Max. Live View Channels |
|------------------|-----------------|------------|-------------------------|
| 30               | 3               | 1080p      | 13                      |
| 30               | 6               | 8 MP       | 4                       |
| 25               | 3               | 1080p      | 15                      |
| 25               | 6               | 8 MP       | 5                       |





# Chapter 2 Get Started

This section serves as your foundational guide for deploying and configuring the software. It provides essential instructions to help you swiftly establish your initial setup and familiarize yourself with core operations.

## 2.1 Activate License

Upon initial installation, the client software operates under a temporary license, which restricts the total number of manageable devices and limits certain system features. To unlock the platform's full potential—including expanded device capacities and advanced functionalities—you must register for your Server.

*(Note: Activation is optional at this stage and can be postponed to a later time if desired).*

### Important Considerations:

- System activation, license updates, and deactivations are strictly restricted to accounts with Administrator rights.
- Should you experience any errors during the licensing lifecycle, please export the server logs and forward them to our technical support team for assistance.
- Navigate to the *License Overview* menu to assign available license resources specifically for ANPR, Facial Recognition, or Human Body Recognition cameras.

### To begin the activation procedure:

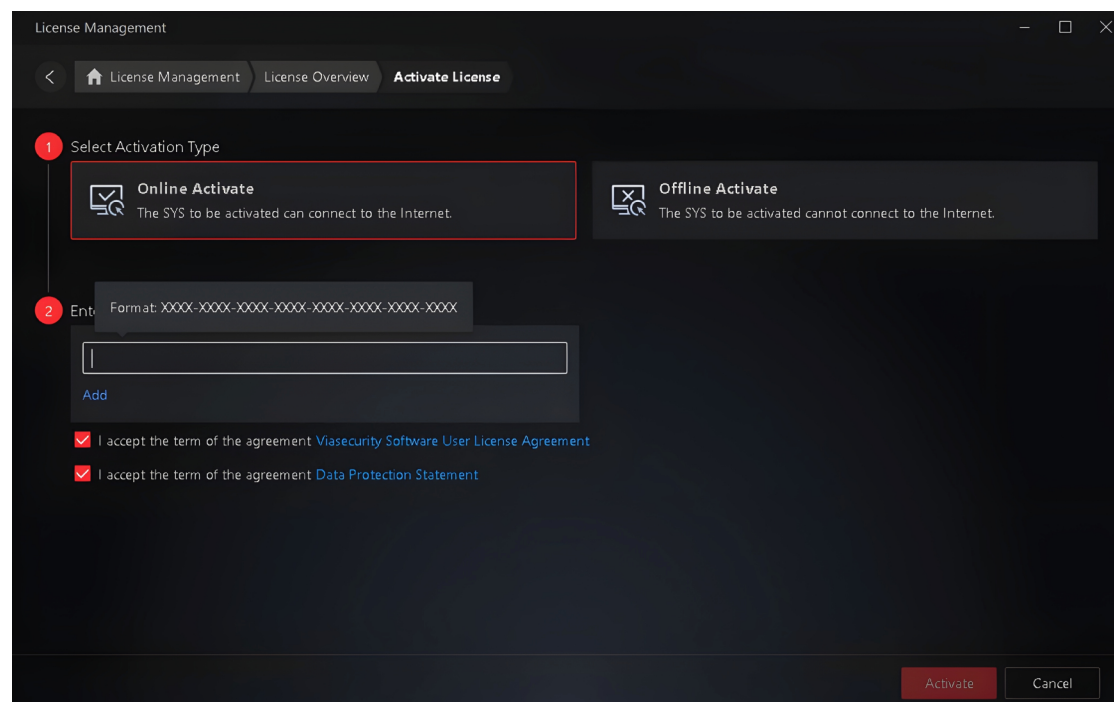
1. From the primary Dashboard (Home page), click on your profile/username located in the upper-right corner.
2. Choose **License Management** from the dropdown menu to launch the dedicated panel.
3. Click the **Activate License** button situated at the bottom left of the interface.

### 2.1.1 Online Activation Method

If your host machine maintains an active internet connection, registering over the network is the most streamlined method.

**Procedure:**

1. Choose **Online Activate** as your preferred method from the activation prompt.
2. Input the unique activation key provided at the time of your software purchase. If you possess multiple keys, use the **Add** button to input supplementary codes.
  - a. Ensure the activation key consists exactly of 32 alphanumeric characters (except dashes), format at: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX
3. Review the mandatory legal documents. You must mark the checkboxes acknowledging your acceptance of both the *Viasecurity Software User License Agreement* and the *Data Protection Statement*. Click **OK** to proceed.
4. Finalize the process by clicking **Activate**.



**Figure 2.1 Activate the License Online**

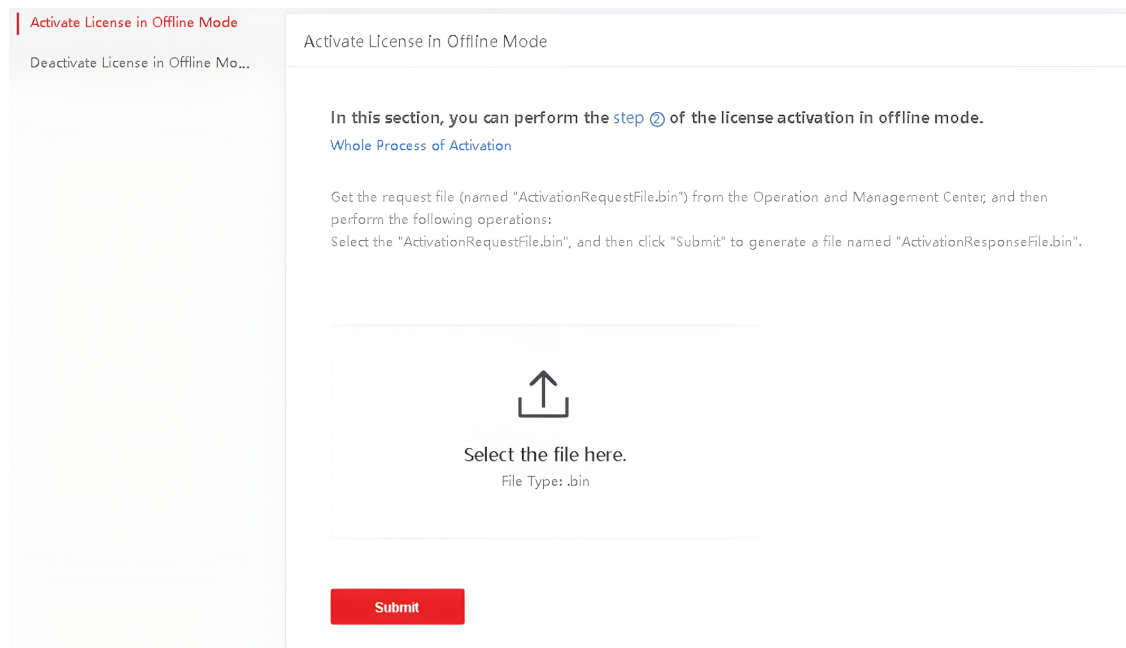
## 2.1.2 Offline Activation Method

For secure environments without direct web access, the system supports a localized offline licensing procedure requiring the use of a separate, internet-connected device.

**Procedure:**

1. From the activation menu, designate **Offline Activate** as your method.

2. Provide your purchased activation key. Multiple keys can be appended by clicking the **Add** button.
  - a. Ensure the activation key consists exactly of 32 alphanumeric characters (except dashes), format at: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX.
3. Agree to the required terms by checking the boxes for the *Viasecurity Software User License Agreement* and the *Data Protection Statement*, then confirm by clicking **OK**.
4. Click **Generate Request File**. This action creates a file named `ActivationRequestFile.bin`. Select **View File** to specify a save destination (such as a portable USB drive) or check your downloading records from the home page.
5. Transfer this generated file to a secondary workstation that has active internet access.
6. On the connected workstation, navigate to the official licensing portal via your web browser: <https://kms.fc-solution.com/active#/active>



**Figure 2.2 Activate the License Offline**

7. Upload your downloaded `ActivationRequestFile.bin` into the web portal and click **Submit**.
8. The portal will generate an `ActivationResponseFile.bin`. Download and securely save this file back to your portable USB drive.
9. Return to your offline Viasecurity Control Center workstation. On the *Activate License* screen, either click to browse the `ActivationResponseFile.bin` or drag and drop the file directly into the designated area.

10. Conclude the setup by clicking **Activate**.

## 2.2 Adding Devices

The system allows you to integrate various hardware, including video intercoms, and encoding equipment. You can incorporate these using three primary methods: automated discovery, bulk import, or manual entry.

### Add Device

Navigate from the main Dashboard to **System → Device Management → Add Device**. From here, choose your preferred integration method (Auto Detect, Batch Import, or Manually Add). Alternatively, you can introduce new equipment by utilizing a designated shortcut or by right-clicking directly within a specific area on the interface.

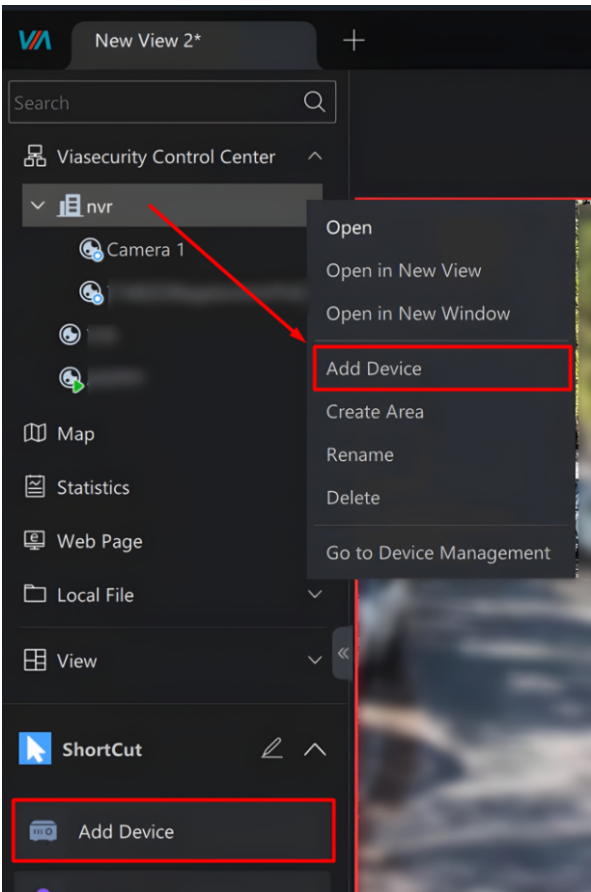


Figure 2.3 Other Entries for Adding Devices

Table 2.1 Add Device

| Mode         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Detect  | <p>Choose this option to locate equipment sharing the local area network (LAN) with your client or server.</p> <p><b>Available Actions:</b></p> <ul style="list-style-type: none"> <li>• Use the "Specify IP Address Range" feature to scan all networks that the client can reach, even across different subnets. (Note: Requires ONVIF compatibility to work.)</li> <li>• Click  to edit Device IP Address and Port number.</li> <li>• Click  to reset the password.</li> <li>• Click  to filter by <b>Activated</b> or <b>Unactivated</b>, as well as device type.</li> <li>• If hardware displays an unactivated status, click Activate to initialize it prior to system adding it.</li> <li>• Configure the Device Time Zone. By default, it mirrors the server's local time. Aligning the device and server time zones enables video recording on both the hardware and the recording server; mismatched time zones restrict storage solely to the device itself.</li> </ul> <p>Manual time zone configurations are automatically synchronized to connected devices every 24 hours (excluding ONVIF-connected hardware).</p> |
| Batch Import | <p>Utilize this method to efficiently register multiple units at once when their network details (IP address, port number, ID, and secret key) are already known, allowing you to add them rapidly without immediate validity verification.</p> <ul style="list-style-type: none"> <li>• This approach is recommended for hardware that is currently offline or situated on a separate network from the server or client.</li> <li>• Set the <b>Device Time Zone</b>, which defaults to the server's configuration. Synchronized time zones permit dual storage (server and device), whereas disparate settings limit recordings to local device storage.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <ul style="list-style-type: none"> <li>• Custom time zone configurations are refreshed across hardware every 24 hours (excluding units utilizing ONVIF or third-party SDK protocols).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Manually Add | <p>Select this to individually register a single piece of equipment using its specific credentials (IP address, port, ID, and password).</p> <ul style="list-style-type: none"> <li>• You must specify the appropriate communication protocol and provide the necessary hardware details. Supported base protocols include: <b>VIA Security Protocol</b>, <b>Hikvision Private Protocol</b>, and <b>ONVIF Protocol</b>. Additional protocol options may be available depending on your installed addons.</li> </ul> <p><i>(Note: For security purposes, you must manually enable the ONVIF feature before utilizing that protocol. Additionally, equipment integrated via ONVIF, or third-party SDKs requires strict manual time zone configuration.</i></p> |

Once your hardware is successfully added, right-clicking on any entry in the device list will reveal additional management options. The system also supports displaying firmware versions and serial numbers for cameras connected via NVRs.

### **Configuring Time Zones**

Highlight the desired device(s) and click **Time Zone** to modify their temporal settings. Check the manual configuration option if you wish to define the time zone yourself; if left unchecked, the software will automatically synchronize with the hardware's existing time zone.

*(Note: Time zone adjustments can solely be applied to devices that are currently online.)*

### **Remote Device Setup**

To remotely adjust a device's parameters, hover over its listing, right-click, and choose **Device Remote Configuration**.

### **Manually synchronizing settings for access control equipment**

When hardware is offline, configuration changes are cached within the platform. Once connectivity is restored, these queued parameters must be manually synchronized to the unit. Furthermore, a manual push of platform access control rules (such as first-person-in, multi-door interlocking, multi-factor authentication, or permanent lock/unlock states) is required whenever you factory reset a device, restore the system database, or set doors to remain locked/unlocked. To execute this, navigate to the **Access Control** interface and select **Apply Manually**.

*(Note: If devices are set up to capture images as a linkage response, these visual assets might be transmitted to the Server via HTTP.)*

## **2.2.1 Server Adding and Details Management**

To effectively distribute real-time media across various devices and clients, you can connect an external streaming server to your infrastructure. Implementing this architecture optimizes video data handling, guaranteeing prompt access to media streams whenever required.

### **Add a Server**

On the Home page, go to **System** → **Device Management** → **Add Server**.

The server is for the live view, playback, video intercom, etc. **Max. Streaming Channel** refers to the max. channel of streams that the streaming server can support.

After adding servers, you can perform further operations on the server list.

### View Alarm Configuration

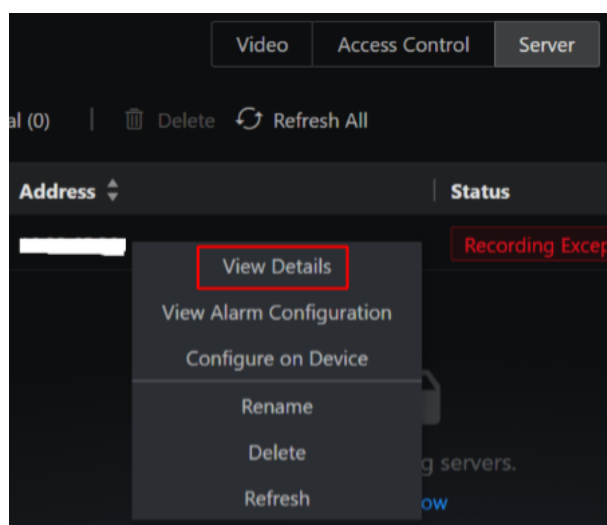
Hover on one server, then right-click and select **View Alarm Configuration** to view and edit the alarm configurations of the corresponding server.

### Remote Configuration

Hover on one server, then right-click and select **Configure on Device** to open the device's web configuration page.

### Inspecting Server Information

For granular insights into a server's operational metrics, hover on the server, right-click, and click **View Details**.



**Figure 2.4 View Server Details**

Within this view, the following actions are available:

- Monitor the operational health (both normal and abnormal states) directly beneath the server's name. The interface prioritizes displaying abnormal statuses by default. Expand the view by clicking **More** to assess the comprehensive status log.
- Modify the server's **Basic Configuration** parameters.



## 2.3 Configuring Local Settings

This section describes how to customize client-specific settings, including video playback parameters, notification alerts, and general application behavior.

To modify these settings, click your **User Name** in the upper-right corner of the interface and navigate to **Local Configuration**.

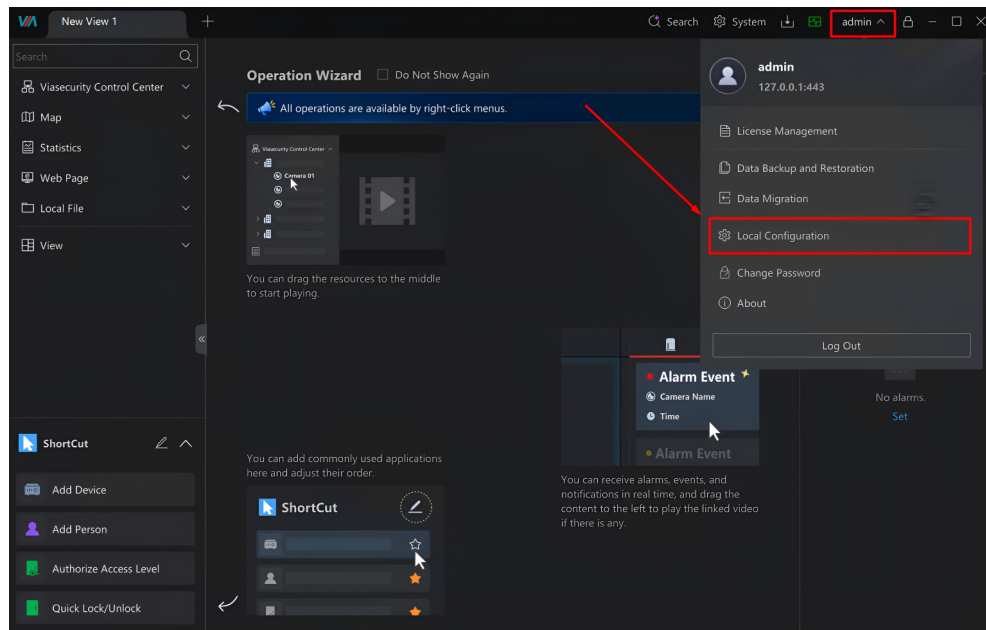


Figure 2.5 Local Configuration

### 2.3.1 Event and Alarm

#### Display

- **Audio Alerts:** Toggle all sound-based notifications (such as sirens or audible alarms) for the current client.
- **Pop-Up Window:** Enable or disable visual alert windows. These windows appear in the center of the screen by default, but the system will save any manual adjustments made to their position for future sessions.

*(Note: If audio or pop-ups are disabled, associated linkage actions will still be triggered but will not be perceptible to the user.)*

#### Alarm Sound

- **Voice Engine (Requires the Operating System's Support):** Utilizes the operating system's text-to-speech capabilities to read out alert descriptions.
- **Local Audio Files:** Triggers the playback of custom uploaded files. The configured voice text will be irrelevant.

### Audio Loop Settings

- **Play the Audio Repeatedly:** Toggle this switch if you want the selected alarm sound to be played repeatedly rather than just once.
- **Times of Playing:** If the repeat playback function is enabled, use this drop-down list to set the exact number of times the system should play the audio file.

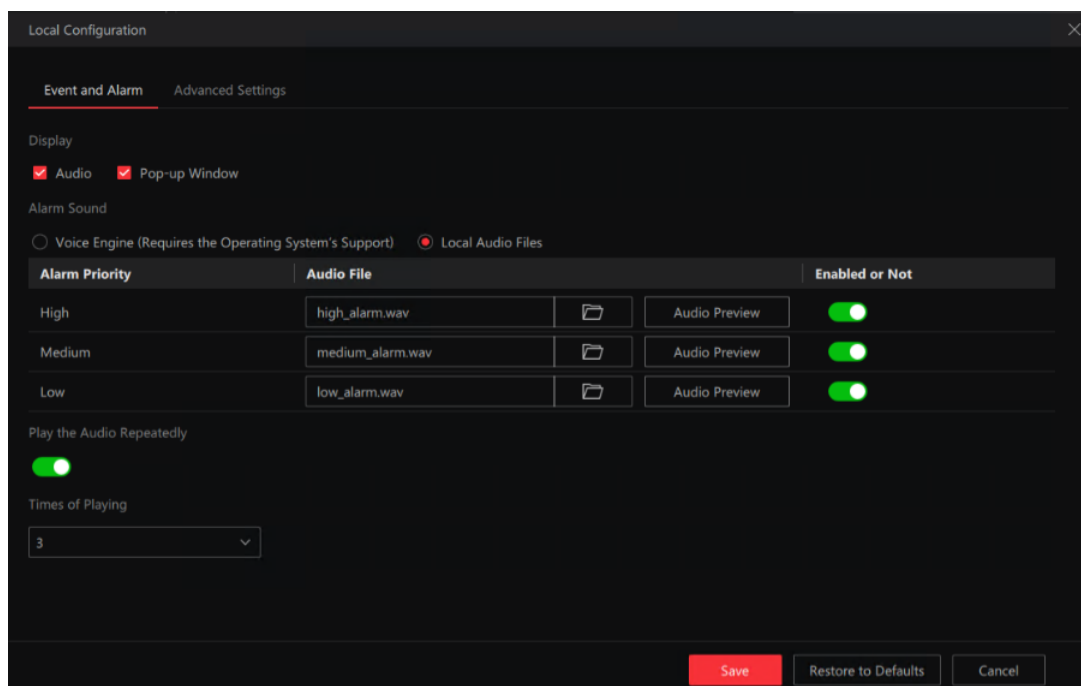


Figure 2.6 Event and Alarm Configuration

## 2.3.2 Advanced System Parameters

### File Saving Path

- Select a destination folder for exported media, including images, video downloads, and manual recordings.

### Streaming Access Mode

Define how to access all the added encoding devices and decoding devices.

- **Automatically Judge:** The system chooses the most efficient path based on network domains. Direct streams are used if the client and device share a domain; otherwise, data is routed through a streaming server.
- **Direct Access:** When this option is selected, the client software establishes a connection and receives the video stream directly from the end device, completely bypassing the intermediate streaming server. Using this mode is advisable when it is necessary to reduce the load on the central server, provided that the client workstation has stable direct network access to the device.
- **Via Streaming Server:** All data is accessed via a streaming server to minimize hardware overhead, especially in environments with multiple active clients.

### 2.3.3 Video Display Settings

To access these preferences, right-click on any unoccupied area of the main control panel.

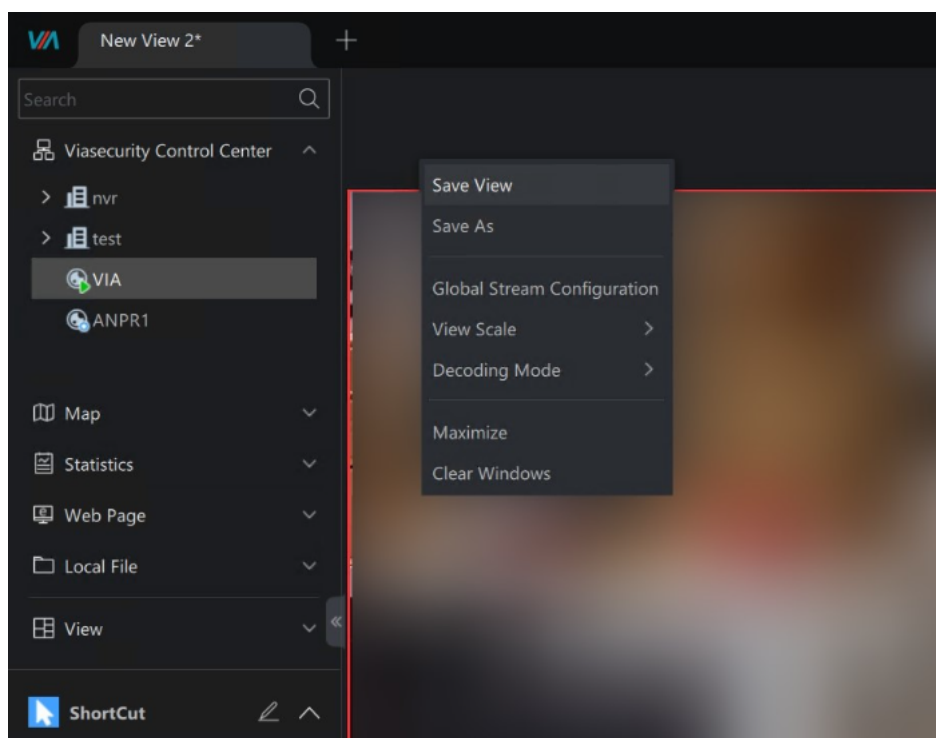


Figure 2.7 Access to Basic Video Preference

#### Global Stream Configuration

- If you check **Stream Adaption**, the software automatically toggles between Main and Sub-streams based on the resolution of the viewing window.
- **Manual Resolution:** You can select a preferred resolution (Extra Large to Small) to balance video quality and network load.

- **Fixed Mode:** If adaptation is disabled, the software uses the specific Main or Sub-stream selected, reverting to a compatible mode if necessary.

#### **View Scale**

- **Original Resolution:** Displays video in its actual dimensions (which may result in black borders).
- **Windowed Fullscreen:** Expands the video to fill the entire viewing area.

#### **Decoding Mode**

- Hardware decoding is to be decoded based on GPU, while software decoding is on CPU. Choose the decoding mode according to your GPU/CPU performance.

# Chapter 3 Video Monitoring

Video Monitoring is the foundational security component of the Viasecurity Control Center. This module empowers operators with real-time visual oversight of protected environments, instant notifications for triggered alarms or events, and comprehensive tracking of various target trends across the facility.

- **System Setup and Preparations**
  - Encoding device integration
  - Managing Hardware Settings
- **Core Surveillance Tools**
  - Live Video and Playback Operations
  - Real-time PTZ control
  - Monitor via Cameras on the Map
- **Face Picture Comparison and Human Body Detection**
  - Add Face Picture Libraries and Face Pictures
  - View Videos Related to Face and Human Body Recognition
  - Search for Recognized Face Pictures and Human Body Pictures
  - Search Targets by a Picture
- **Vehicle Operations**
  - Add Vehicle Lists and Vehicles
  - View Video Related to Vehicle Monitoring
  - Search and Export ANPR Events
- **Smart Search capabilities**
  - Smart Search / VCA
  - TargetTrace and Object Search
  - People Counting Analytics and Reports

## 3.1 System Setup and Preparations

### 3.1.1 Encoding device integration

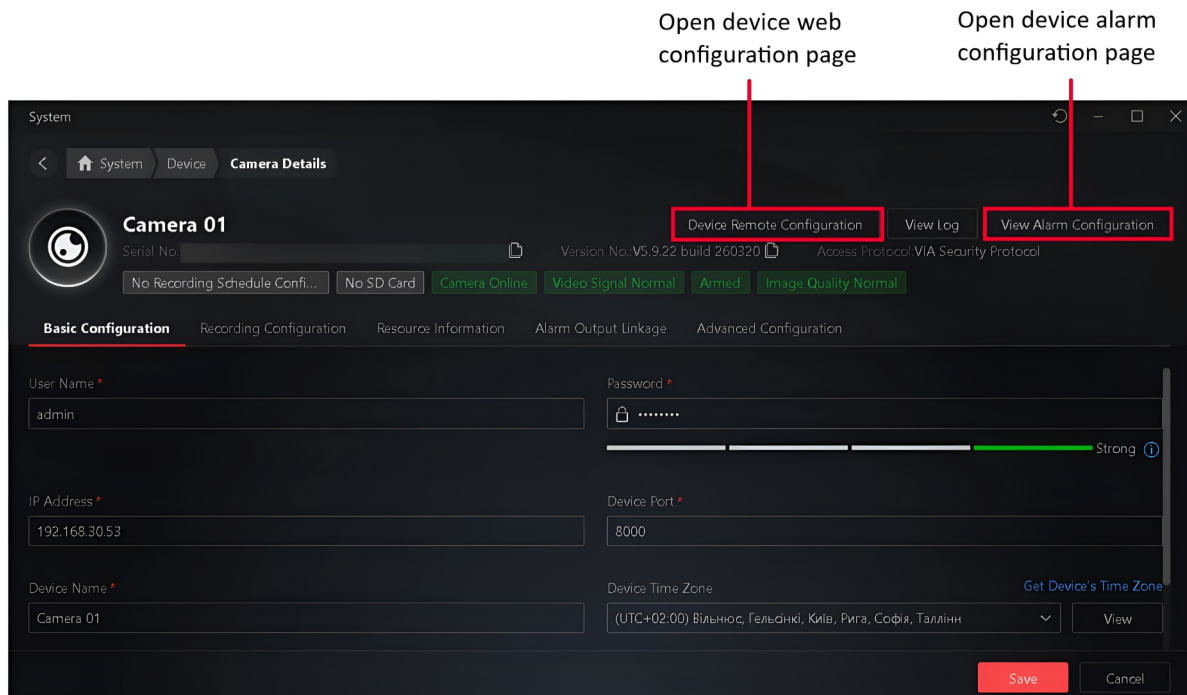
Before using basic features such as live streaming, video storage, or event triggers, operators must first connect all physical encoding equipment, including IP cameras and network video recorders (NVRs), to the platform.

- From the main workspace interface, navigate to **System** → **Device Management** → **Add Device** to register new hardware. (See the "Adding Devices" section for comprehensive pairing instructions.)

### 3.1.2 Managing Hardware Settings

Once equipment is linked, administrators can fine-tune operational parameters. The available interface options—such as recording timetables, I/O resources, AI capabilities, and advanced network or PTZ settings—will dynamically adjust based on the specific model, its connection protocol, and the integration method used.

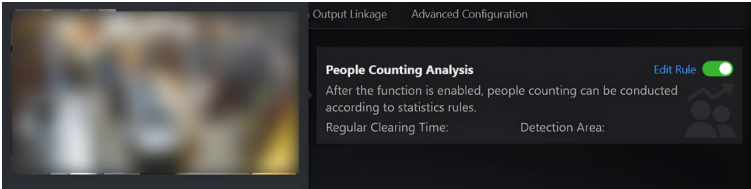
- Go to **System** → **Device Management** to view your hardware inventory. Click directly on a designated hardware name to access its dedicated configuration panel.



**Figure 3.1 Camera Details**

*(Note: The device details vary according to the device type, access protocol, and device adding method. Configurations should be subject to the actual situation.)*

**Table 3.1 Device Details Tab Page Introduction**

| Tab Name                | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recording Configuration | Exclusively for camera hardware, used to define storage rules.                                                                                                                                                                                                                                                                                                                                |
| Resource Information    | Displays all peripheral components linked to the hardware, such as alarm inputs/outputs and subordinate cameras. Operators can right-click any listed resource to execute specific commands, such as launching the hardware native web portal, querying logs, managing alarms, or deleting the item.                                                                                          |
| Intelligent Capability  | <p>Highlights the available Intelligent functions tools (e.g., TargetTrace, ANPR, facial recognition) tied to the hardware's processing power and active licensing. Operators must toggle these features before they can be deployed globally. Rule cloning and editing are also managed in this tab.</p>  |
| Alarm Output Linkage    | Exclusively for cameras, allowing users to map physical alarm outputs directly onto the live feed layout.                                                                                                                                                                                                                                                                                     |
| Advanced Configuration  | Used for assigning network transfer protocols and dictating media profiles (main/sub-streams). If the system fails to recognize a camera Pan-Tilt-Zoom (PTZ) functions automatically, administrators can manually force the PTZ classification here to enable direct interface controls.                                                                                                      |

## Defining Storage and Recording Parameters

When a new camera is integrated, the Viasecurity Control Center automatically imports its pre-existing recording timetable. By default, the system will capture a dual-stream format if the hardware allows it, giving operators the flexibility toggle video quality during historical playback. Toggle the **Recording** switch to the "on" position to access the following parameters:

The screenshot displays the 'Recording Configuration' window. At the top, there are tabs for 'Basic Configuration', 'Recording Configuration' (selected), 'Intelligent Capability', 'Alarm Output Linkage', and 'Advanced Configuration'. Below the tabs, a 'Recording' toggle switch is turned on. To the right is a 'Copy To' button. The main area is divided into two sections: 'Video Parameter Settings' and 'Recording Schedule'. In 'Video Parameter Settings', 'Video Storage Location' is set to 'System Storage', 'Stream Type' is 'Main Stream (Estimated HDD Cons...)', and the 'Overwrite After Retention Time' checkbox is checked. The 'Recording Schedule' section shows a 'Custom' schedule with 'Scheduled Recording' and 'Event-Based Recording' tabs. A grid shows the recording schedule for the week of Monday to Saturday, with blue blocks indicating recording times from 00:00 to 06:00 and 18:00 to 22:00, and orange blocks indicating recording times from 06:00 to 18:00. The 'Save' button is highlighted in red.

Figure 3.2 Recording Configuration

### Video Storage Location

- Determine whether archived footage resides on the central system servers or local device drives.

(Note: If you utilize System Storage alongside Stream Encryption, you must strictly manage your encryption keys. Updating an encryption key without safeguarding the previous one will render all historical footage encrypted under the old key permanently unreadable.)

### Stream Type

Select Main Stream, Sub-Stream, or Dual-Stream based on your network bandwidth and desired playback resolution.

### Data Retention



Activate the **Overwrite After Retention Time** feature to automatically purge footage once it exceeds a defined age limit. If left disabled, the system will simply overwrite the oldest available video blocks whenever storage capacity maxes out.

### **Auto Copy-Back**

A failover mechanism that stores video locally on the device during a network failure. Once the connection is restored, recordings are transferred to the primary storage drive. *(Note: This feature only works when the stream type is set to "Main stream" and requires compatible cameras manufactured by Viasecurity or Hikvision.)*

### **Recording Schedule**

Dictate when the camera records. Operators can assign pre-built templates or draft custom windows, distinguishing between continuous 24/7 recording and event-triggered captures.

### **Back up Video**

Enable redundant storage. This creates a secondary archive on a backup device, ensuring footage is accessible even if the primary storage suffers corruption or data loss.

### **Copy To**

Use this action to rapidly push your customized recording setup to other compatible cameras in your network.

## **3.2 Core Surveillance Tools**

The Viasecurity Control Center equips operators with fundamental capabilities for active facility observation. These foundational features encompass real-time video streaming, historical footage retrieval, precise pan-tilt-zoom (PTZ) maneuvering, and spatial tracking through interactive floor plans and maps.

### **3.2.1 Live Video and Playback Operations**

Operators can seamlessly initiate and manage video feeds for individual or clustered hardware units.

#### **Single Device Monitoring**

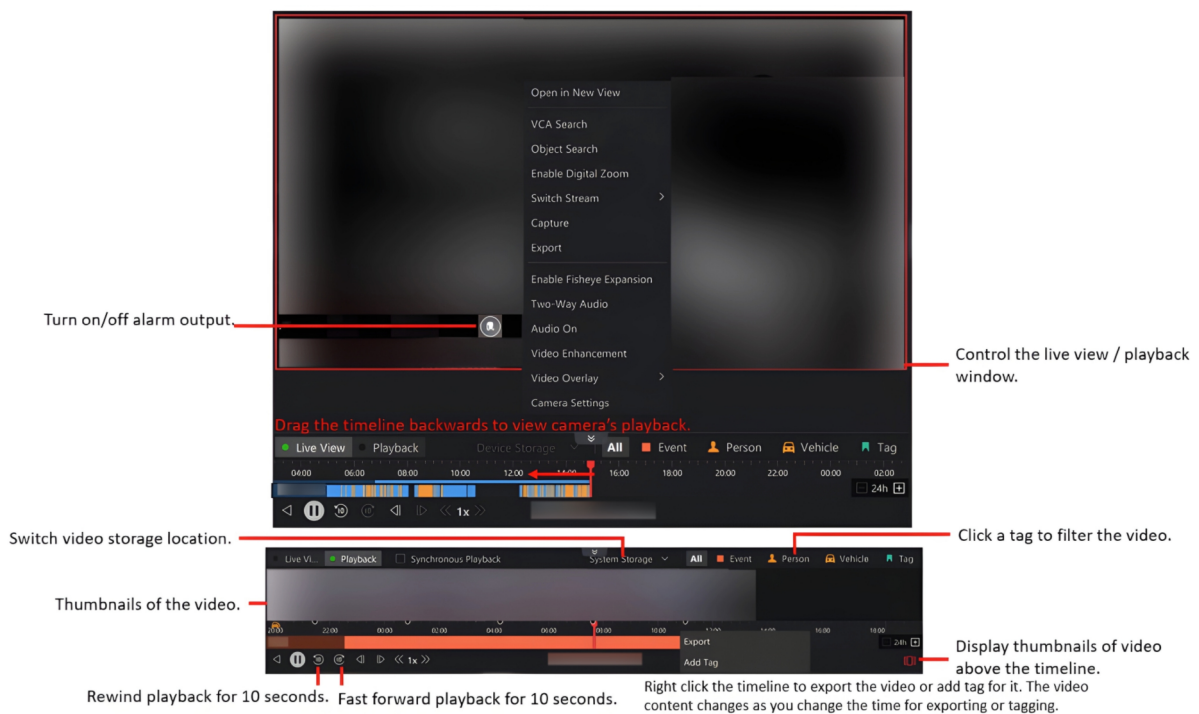
- To launch a real-time stream, simply double-click the desired device in the hardware roster, drag its icon onto the viewing matrix, or right-click the item and select Open.

## Reviewing Historical Footage

- While actively monitoring a stream, operators can transition to archived video by dragging the chronological timeline in reverse or by pressing the Playback icon located at the bottom-left of the viewing pane.

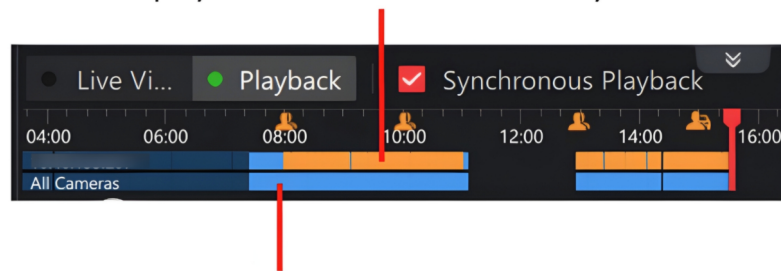
## Multi-Device Monitoring

- To observe multiple feeds simultaneously, hold the Ctrl key while clicking to select several cameras. These can then be dragged onto the viewing matrix together or opened via the right-click menu.



**Figure 3.4 Start Live View / Playback of One Camera**

The playback timeline of the currently selected camera.



The playback timeline of all cameras in the viewing grid.

**Figure 3.5 Synchronous Playback**

### In-Stream Capabilities

Right-clicking the viewing pane or utilizing the control icons at the bottom-right exposes a suite of operational tools for both live and archived streams:

- **Workspace Management:** Spawn the current feed into an independent viewing window.
- **Smart Search / VCA Search:** Draw custom bounding boxes directly on the footage to trigger detection for humans, vehicles, or anomalous motion within that zone. Results populate on the side panel for quick review or deep-dive analysis.
- **TargetTrace / Object Search:** Isolate specific human or vehicle profiles to sweep captured imagery for matching targets.
- **Enable Digital Zoom:** Zoom into specific quadrants by clicking on the magnifying icon, drawing a defined frame over the area of interest, or scrolling the mouse wheel.
- **Stream Quality Adjustment:** Toggle between Main, Sub, Fourth, or Smooth streaming profiles depending on network bandwidth availability.
- **Media Extraction:** Capture immediate snapshot images from the feed, or export specific video segments during playback.
- **Manual Recording:** Force the system to capture a localized recording block during active live observation.
- **Lens & View Modifications:** Activate Fisheye for expansion to correct ultra-wide perspective distortions, tweak visual parameters like brightness and saturation, or overlay vital metadata directly onto the feed.
- **Active Deterrence & Audio:** Initiate two-way voice communication, toggle audio listening, or manually trigger the camera's physical warning lights.

*(Note: Hardware must support these features.)*

- **Automated Tracking & Linkage:** Engage continuously track the selected target (person/vehicle) in the video or trigger smart linkage to pinpoint targets.

### Tags person/vehicle

For the system to successfully label historical video blocks with "Person" or "Vehicle" indicators, several prerequisites must be met:

- The connected hardware must have VCA rules (e.g., line crossing, intrusion) actively configured.
- Human and/or vehicle target detection must be enabled.
- The corresponding event subscription must be active within the Viasecurity Control Center.
- Videos recorded before the device is added to the platform will not be tagged

### Playback Keyboard Shortcuts

Operators can accelerate footage review using standard keyboard shortcuts

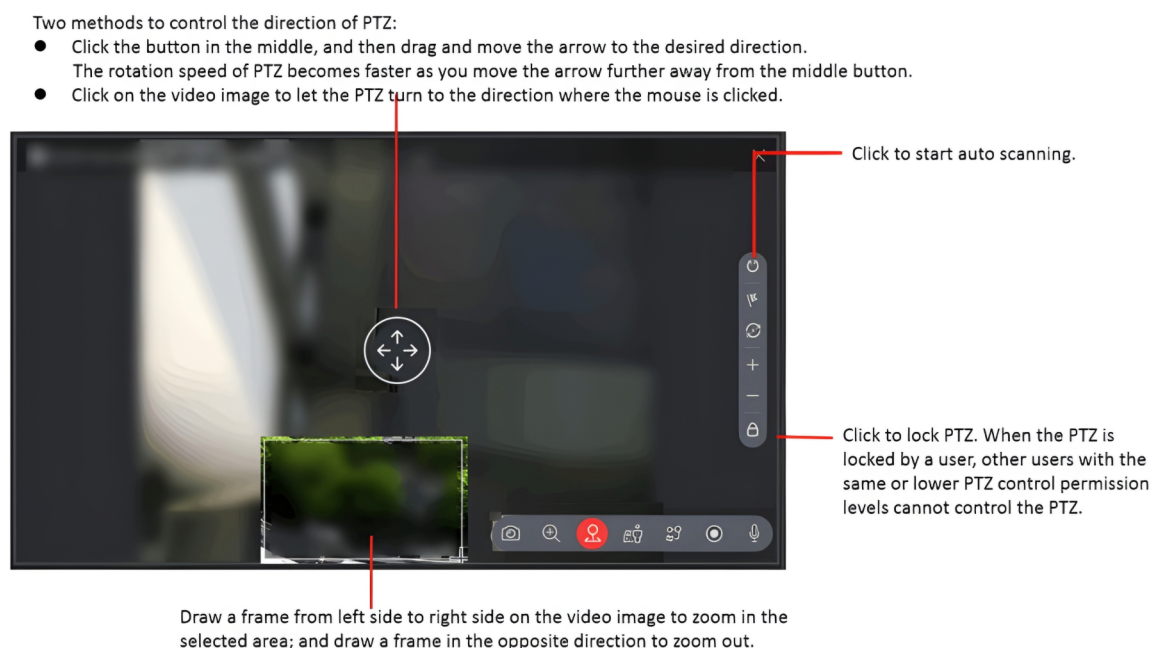
**Table 3.2 Shortcuts**

| Key      | Function                      |
|----------|-------------------------------|
| Spacebar | Play / Pause                  |
| ↑        | Fast Forward                  |
| ↓        | Fast Rewind                   |
| ←        | Single-Frame Reverse Playback |
| →        | Single-Frame Fast Forward     |
| [        | Reverse Playback              |
| ]        | Normal Playback               |

### 3.2.2 Real-time PTZ control

You can control cameras with pan/tilt/zoom functionality during live view.

After launching a PTZ-capable camera into the viewing grid (via double-click, drag-and-drop, or right-click) , locate and click the designated PTZ icon  in the bottom-right corner of the pane. This action deploys a dedicated control overlay on the right side of the screen, allowing security personnel to manually steer the lens, adjust optical zoom levels, and configure automated patrol routes or fixed preset viewing angles.



**Figure 3.6 PTZ Control**

### 3.2.3 Monitor via Cameras on the Map

The platform's mapping integration provides a spatial context to the surveillance network, allowing operators to monitor activity and device statuses based on physical locations.

To access a site map, navigate to the Map module and open the desired schematic by double-clicking, dragging it to the right window, or using the right-click menu. The interface operates under two distinct environments:

#### 1. Configuration Mode

Utilized by administrators to plot camera coordinates, define geographical hot regions, and customize the types of resource markers visible on the map.

## 2. Monitoring Mode

Designed for active surveillance. Operators can click on any camera icon pinned to the map to instantly generate a pop-up live view of that device.

### Add Map

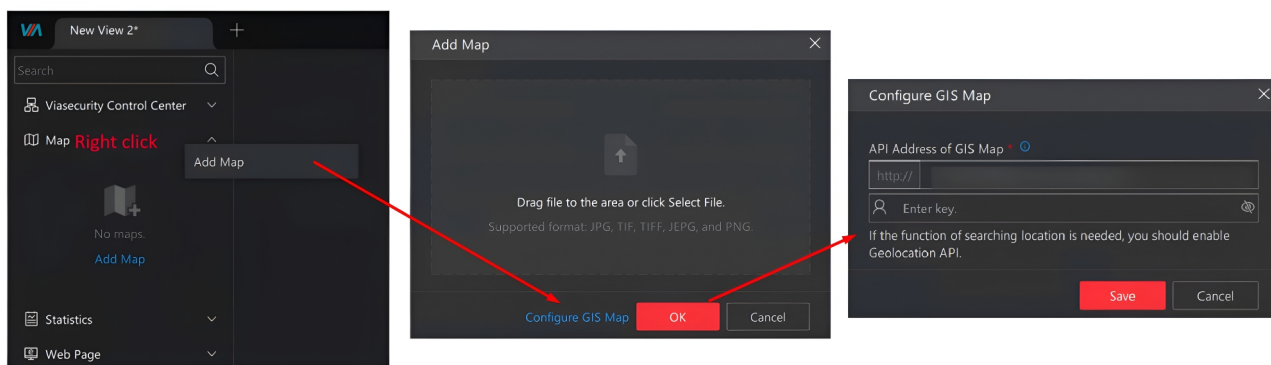


Figure 3.7 Add GIS Map

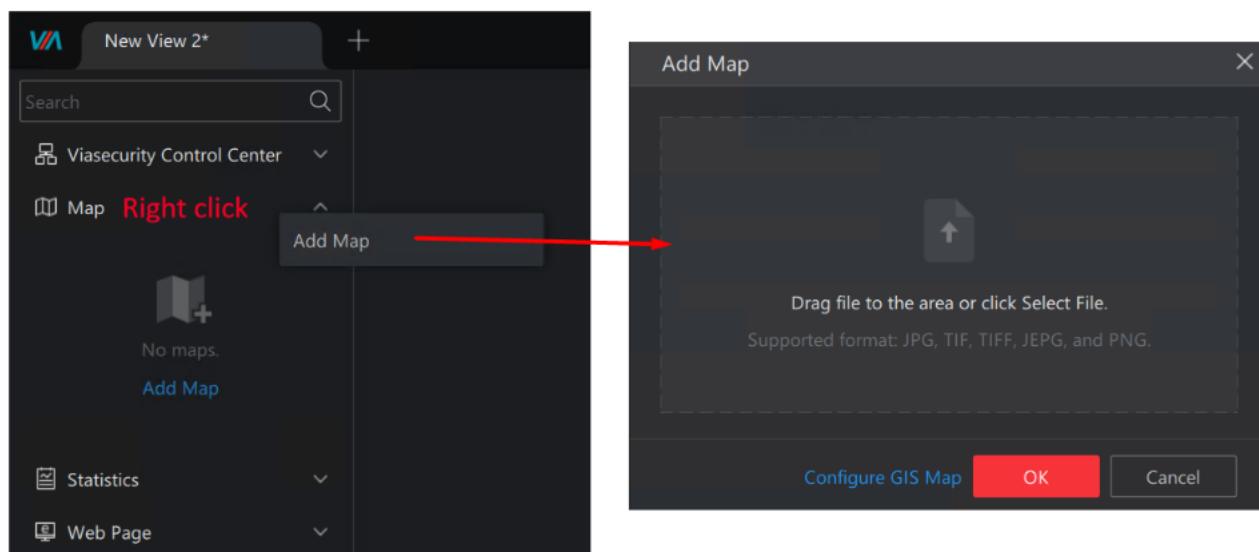
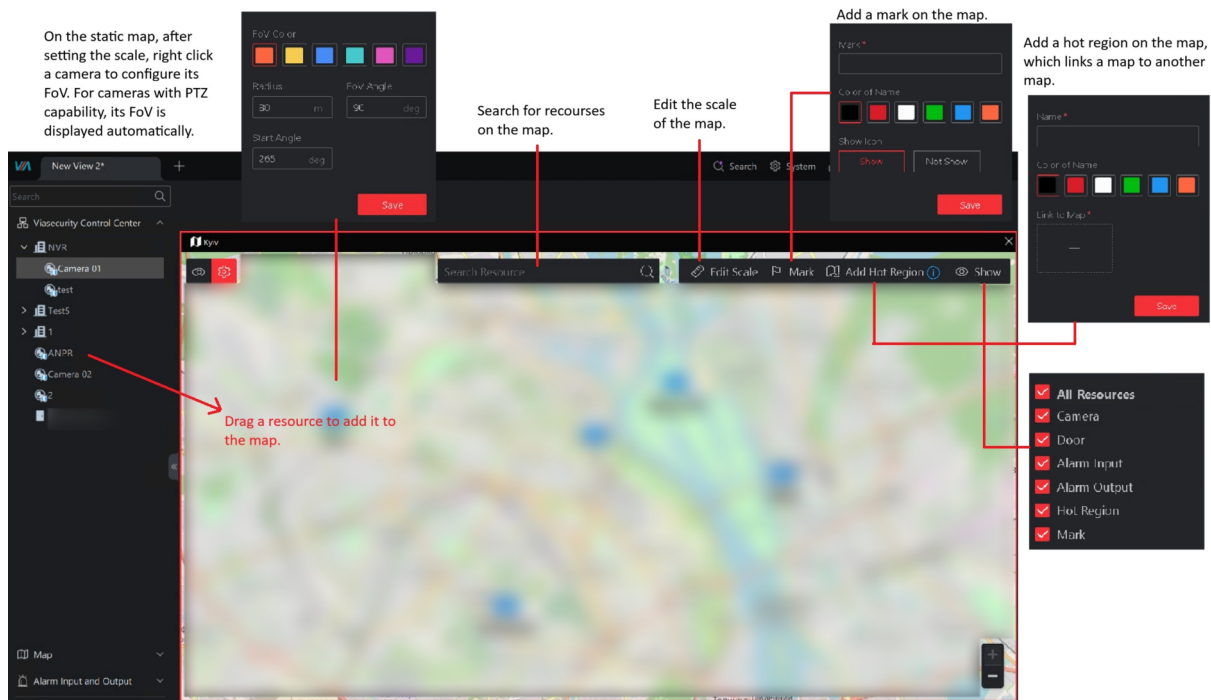


Figure 3.8 Add E-Map

### Configuration Mode

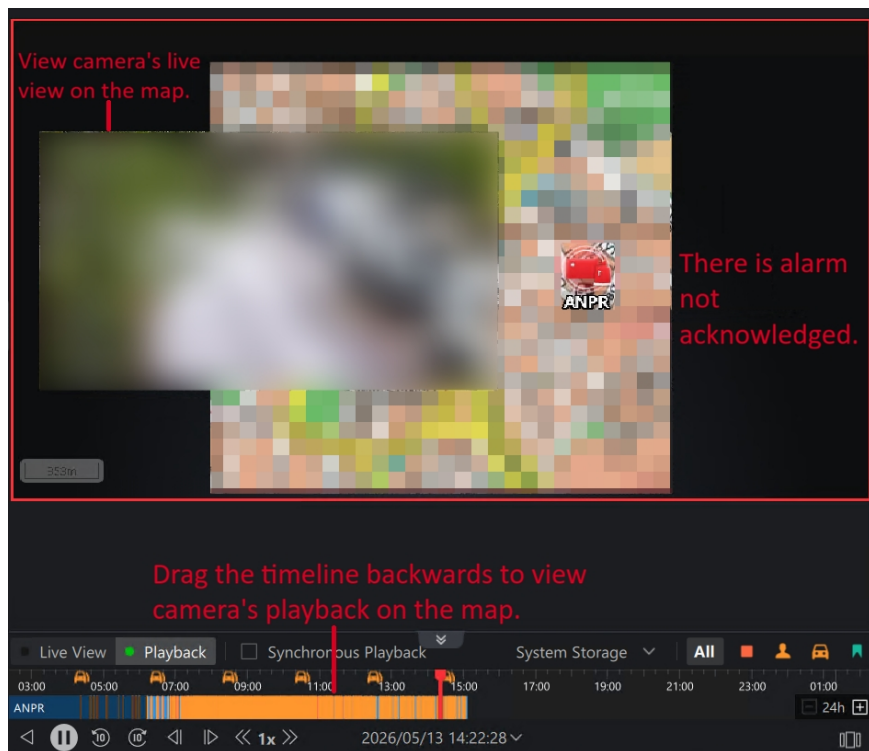


**Figure 3.9 Supported Operations in Configuration Mode**

## Monitoring Mode

You can monitor via cameras on the map.

- Click on a camera to view the live view of the camera on the map.



**Figure 3.10 View Camera's Live View and Playback on the Map**

To efficiently survey an entire sector, use the **Batch Select** tool to draw a perimeter around a cluster of mapped cameras, then click **Batch Play** to simultaneously stream all selected devices. Alternatively, operators can hold the **Ctrl** key to select multiple map icons and drag them into the standard viewing windows outside the map area for persistent observation.



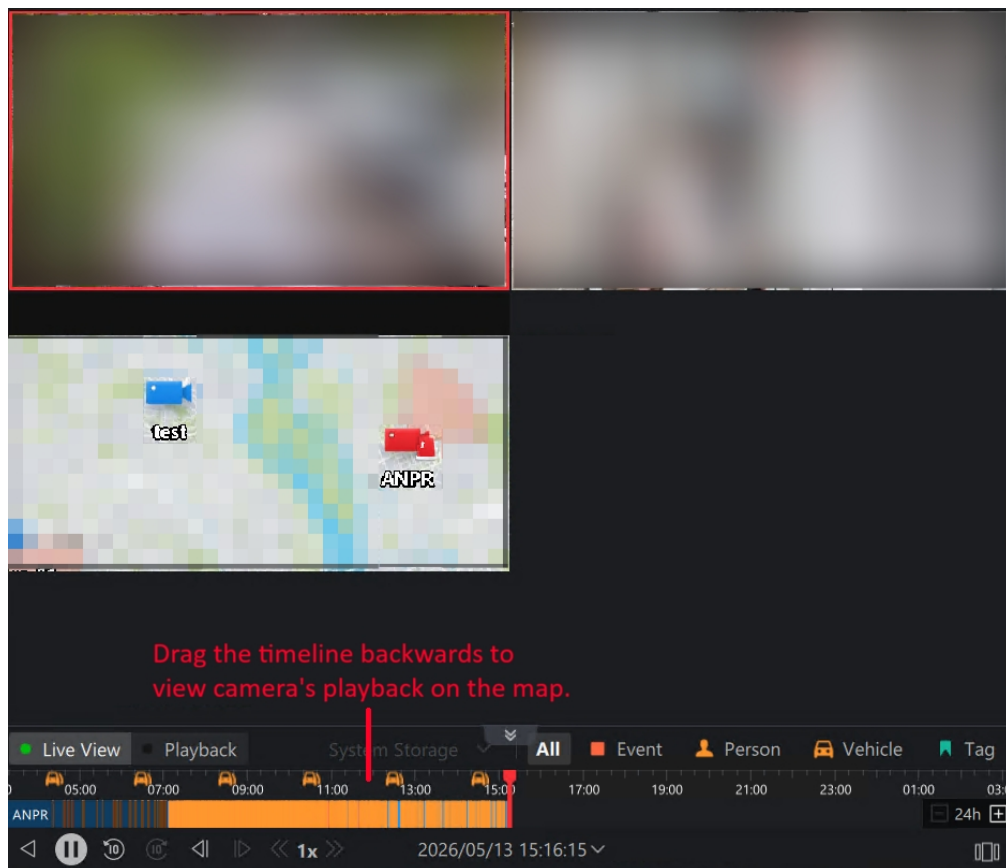


Figure 3.11 Batch View Cameras' Live View and Playback

### 3.3 Face Picture Comparison and Human Body Detection

Facial comparison evaluates a captured subject against established profiles to confirm identity matches, while human shape detection identifies individuals across varied physical environments. These tools are foundational for proactive security measures and are widely deployed across retail and enterprise environments.

#### Hardware Requirement

- To use these biometric features, operators must employ compatible facial recognition cameras or DeepCore Series Network Video Recorders (NVRs). Please consult the technical support team for an exhaustive list of supported hardware models.

#### 3.3.1 Add Face Picture Libraries and Face Pictures

To effectively use face matching, administrators must create databases known as Face Image Libraries that contain the base images used to match against actively captured facial images. These repositories allow security services to group facial data (for example, creating a special catalog for “Blacklist”).

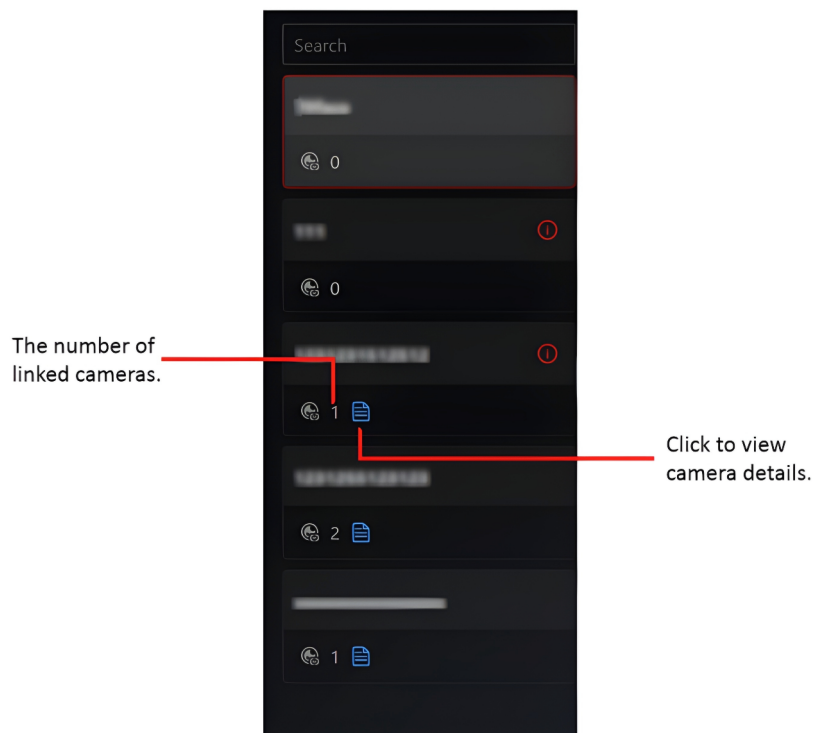
Navigate to **System → Face Picture Library** to access the facial data management dashboard.

#### **Creating a Face Library:**

- Locate and click the **Add Face Picture Library** button situated in the bottom-left corner of the interface.
- Once a library is created and linked to specific recording hardware, the interface will display the total count and corresponding names of the associated cameras directly beneath the library title.

#### **Adding Face Picture:**

- Click **Add Face Picture** in the bottom-left corner to manually register a single identity profile.
- For bulk operations or alternative data import methods, use the **Import** menu, which offers the following functions:
  - **Add from Existing Person:** Pull reference images from user profiles already registered within the system.
  - **Import Face Picture Information via Excel:** Use a standardized spreadsheet template to ingest a high volume of facial data simultaneously.
  - **Import Face Pictures:** Upload a manually packaged batch of image files.
  - **Import Device Face Picture Library:** Synchronize and extract existing facial databases stored locally on connected edge devices.



**Figure 3.12 Cameras Linked with Face Picture Libraries**

### 3.3.2 View Videos Related to Face and Human Body Recognition

#### Reviewing Biometric Video Captures

Once facial and human body recognition cameras are configured, operators can monitor live streams enhanced with biometric analytics. The system continuously displays associated detection events in real-time alongside the active video feed.

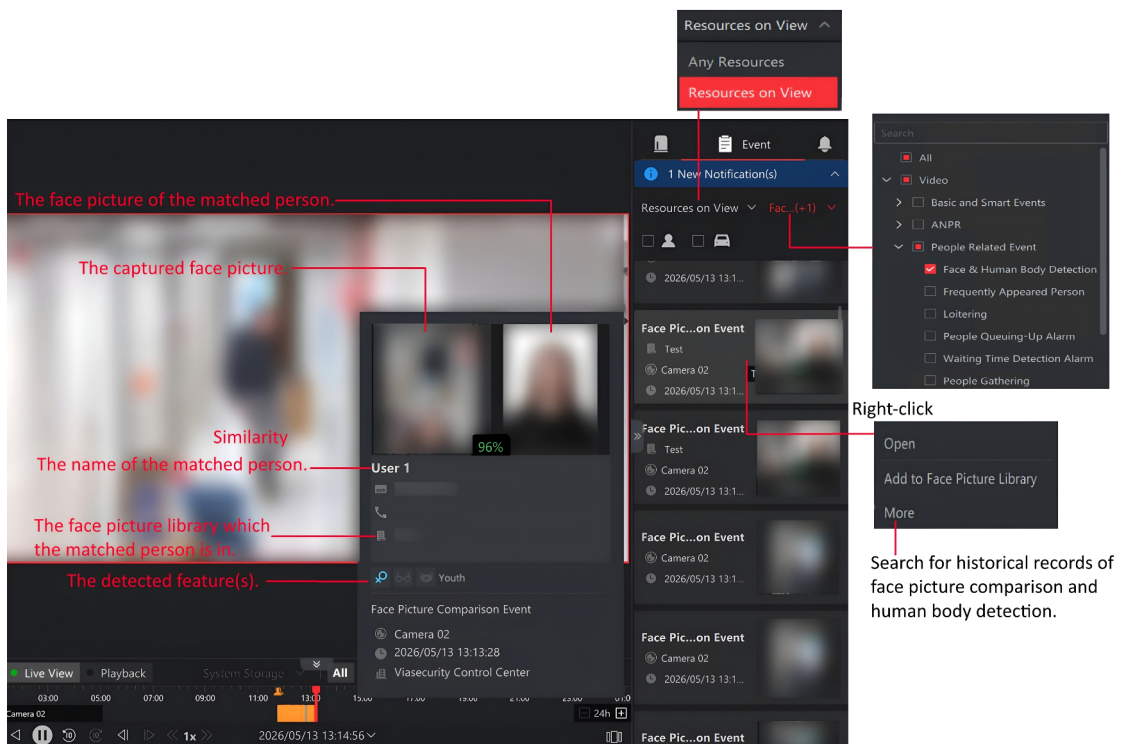
*(Note: Ensure compatible recognition cameras are integrated, and their respective channel licenses are actively allocated by navigating to License Management → License Overview.)*

#### Live Match Analytics

Instantly view match similarity percentages and identify the specific face repository associated with the captured subject.

#### Quick Interactions

Hover over any active event to reveal a quick data summary, or right-click the event to access additional actions, such as initiating targeted searches for related captures.



**Figure 3.13 Face Picture Comparison Details**

## Visual Verification

Open the **Alarm Details** window during a matched event to enlarge both the live captured snapshot and the database reference image for precise visual comparison.

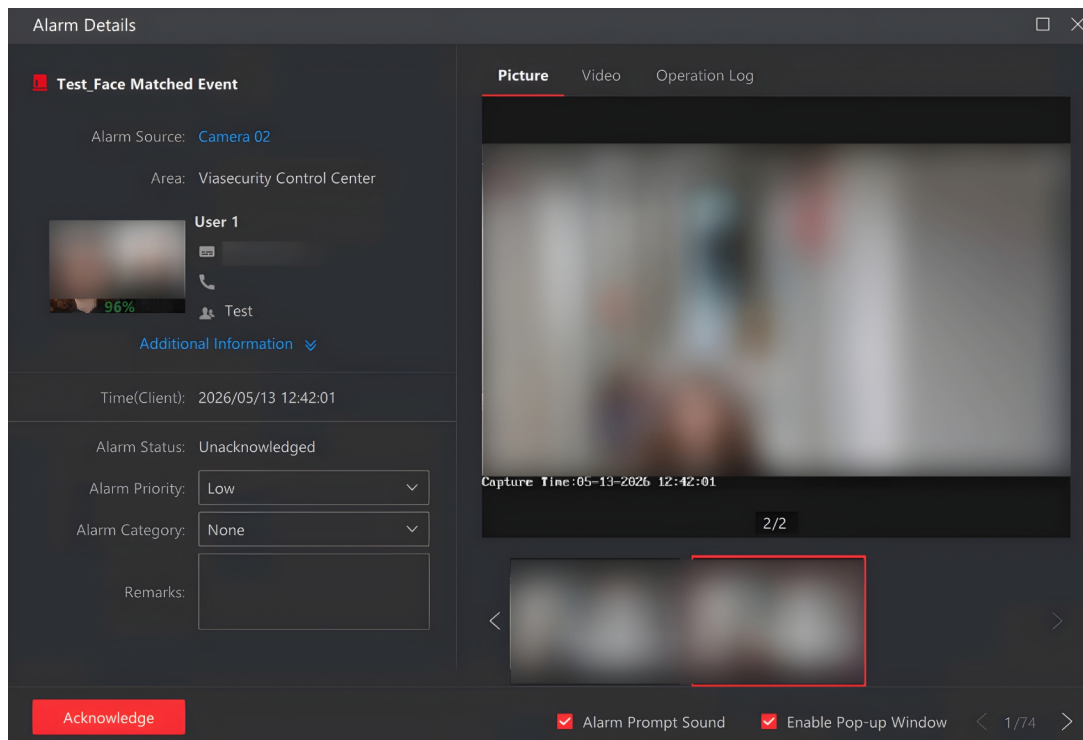


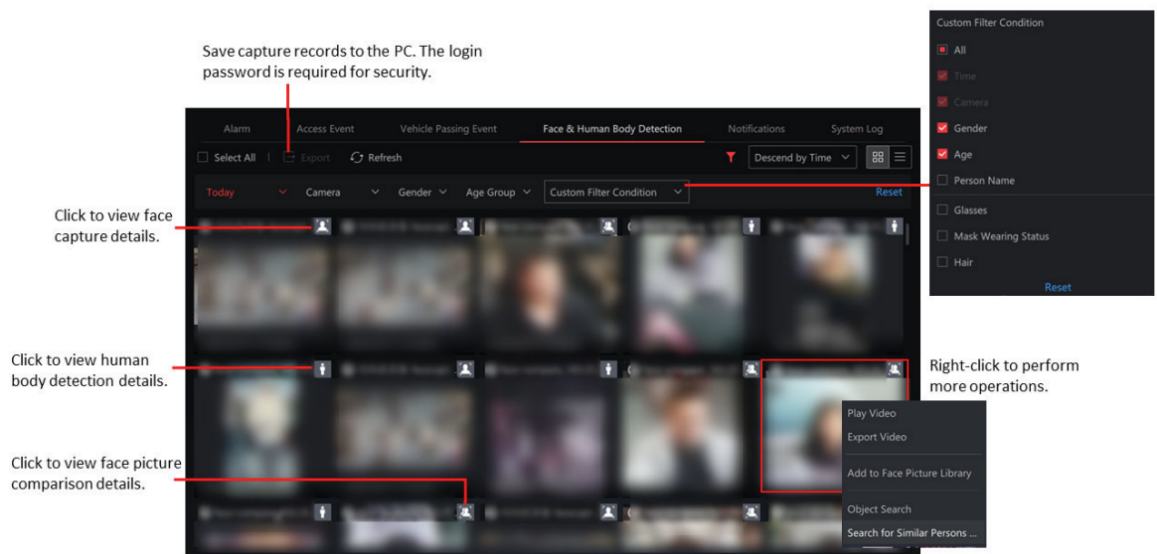
Figure 3.14 Alarm Details

### 3.3.3 Search for Recognized Face Pictures and Human Body Pictures

Operators can efficiently retrieve historical biometric logs by applying specific search filters. This query engine covers standard face captures, matched comparison records, and human shape detection events.

#### Search for Recognized Face Pictures and Human Body Pictures:

1. Navigate to **Search → Face & Human Body Detection** to access the query dashboard.
2. Define your search parameters to filter and locate the required biometric capture records.



Fig

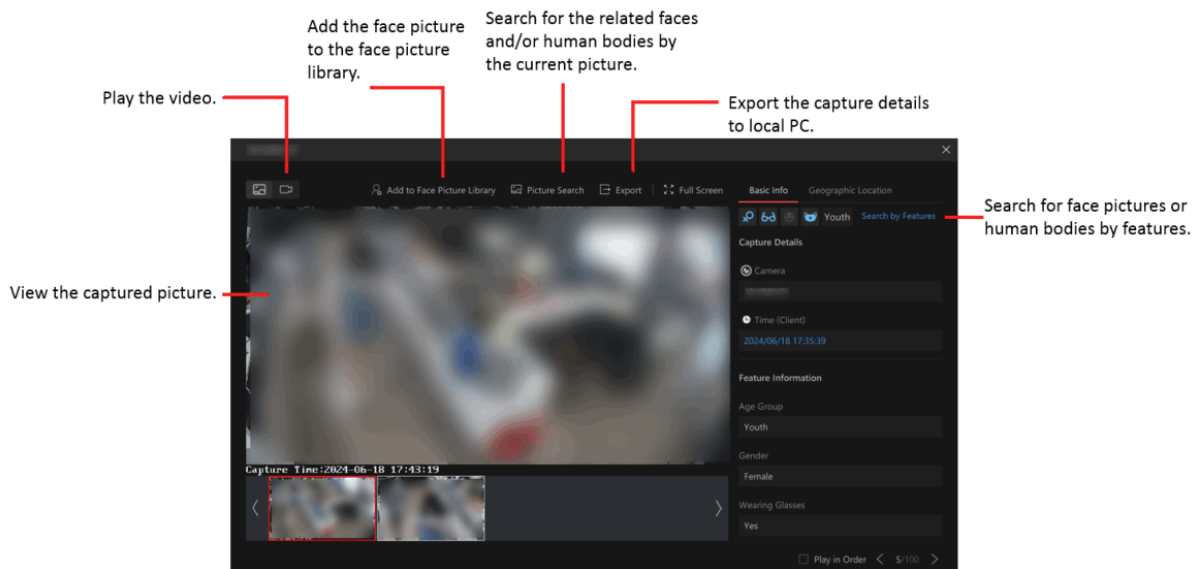
Figure 3.15 Face & Human Body Detection

3. Select any individual record from the generated results to examine its comprehensive details.
4. Use the export feature to store target capture logs locally for external reporting or evidence management.

| Basic Information                    |                         |            |            |            |                                |            |                |            |         | Face Human Body Detection |         |            |              |
|--------------------------------------|-------------------------|------------|------------|------------|--------------------------------|------------|----------------|------------|---------|---------------------------|---------|------------|--------------|
| Export Time: [redacted]              |                         |            |            |            |                                |            |                |            |         |                           |         |            |              |
| Operator: [redacted]                 |                         |            |            |            |                                |            |                |            |         |                           |         |            |              |
| Export Content: Data, Capture, Video |                         |            |            |            |                                |            |                |            |         |                           |         |            |              |
| Report Time: 2                       |                         |            |            |            |                                |            |                |            |         |                           |         |            |              |
| Total Number: 7                      |                         |            |            |            |                                |            |                |            |         |                           |         |            |              |
| No                                   | Capture Type            | Time       | Camera     | Capture    | Partial View with Key Informat | Video      | Similarity     | Age Group  | Gender  | Wearing Mask              | Glasses | Hair       | Tops Type    |
| 1                                    | Face Capture            | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Unknown    | Unknown | Unknown                   | Unknown | Unknown    | Unknown      |
| 2                                    | Human Body Detection    | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Unknown    | Male    | No Mask                   | Unknown | Short Hair | Long Sleeves |
| 3                                    | Face Picture Comparison | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Middle Age | Female  | Wearing Mask              | No      | Unknown    | Unknown      |
| 4                                    | Human Body Detection    | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Unknown    | Female  | Wearing Mask              | Unknown | Long Hair  | Long Sleeves |
| 5                                    | Human Body Detection    | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Unknown    | Male    | No Mask                   | Unknown | Short Hair | Long Sleeves |
| 6                                    | Face Picture Comparison | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Adult      | Male    | No Mask                   | Yes     | Unknown    | Unknown      |
| 7                                    | Face Picture Comparison | [redacted] | [redacted] | [redacted] | [redacted]                     | [redacted] | Not supported. | Adult      | Female  | Wearing Mask              | No      | Unknown    | Unknown      |

Figure 3.16 Export Capture Records

(Note: This historical search capability is hardware-dependent and must be natively supported by the connected devices.)



**Figure 3.17 Supported Operations on Face Capture Details Page**

### 3.3.4 Search Targets by a Picture

Operators can perform reverse-image searches by uploading a reference photo to quickly locate matching facial profiles, human shapes, or vehicles across recorded video archives.

**Hardware Requirement:** This advanced search functionality is strictly supported by DeepCore series NVRs.

#### Instructions:

1. Navigate to **Search → Intelligent Search → Upload Picture**.
2. Import a reference image from your local workstation by selecting it via the file browser or dragging it directly into the interface.
3. If the uploaded image contains only one recognizable subject, the system will automatically execute the query and display the results.
4. If the image contains a crowd or multiple elements, manually click to select the specific face, human body, or vehicle you wish to isolate and search.

From the generated results dashboard, operators can review precise capture details and initiate playback of the associated video footage.

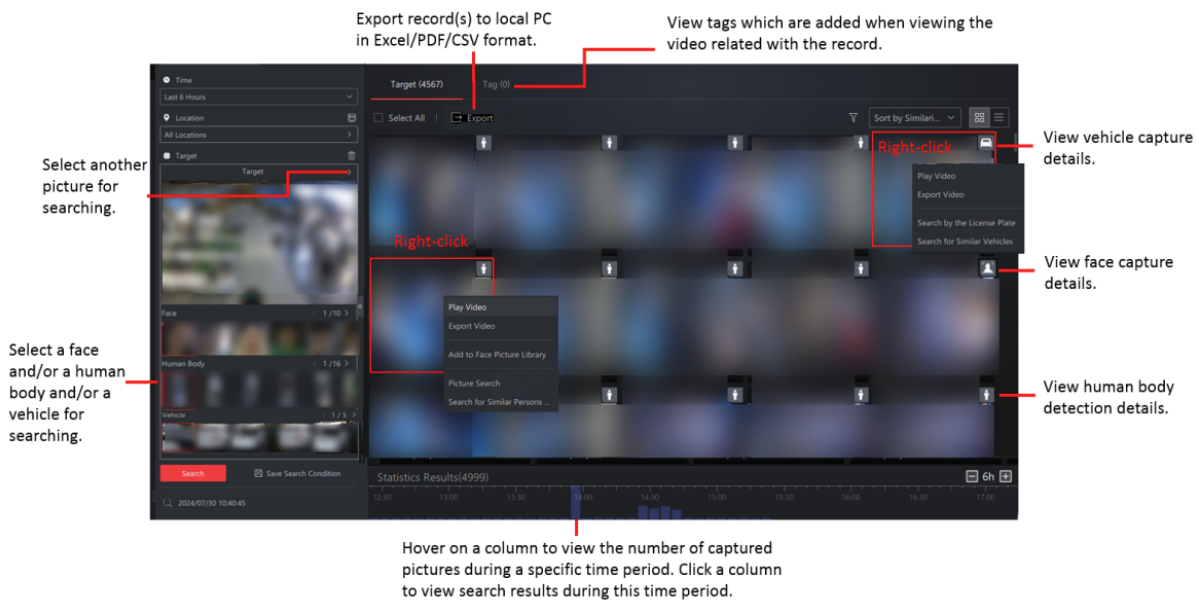


Figure 3.18 Search Conditions and Supported Operations on Search Results Page

## 3.4 Vehicle Operations

The Viasecurity Control Center facilitates comprehensive vehicle tracking, allowing operators to oversee live traffic feeds, manage categorized vehicle registries, and search historical passing events.

*(Note: Vehicle monitoring relies exclusively on devices with **ANPR** compatibility. Please consult the technical support team for a verified list of supported camera models.)*

### 3.4.1 Add Vehicle Lists and Vehicles

To effectively categorize and monitor vehicular traffic, administrators must build and maintain dedicated vehicle lists. This module allows for bulk management, cross-list transfers, and data extraction.

#### Vehicle Lists:

1. Navigate to **System** → **Vehicle** to access the centralized vehicle management dashboard.
2. Use this interface to create new vehicle categories (lists), add individual vehicle profiles, or transfer existing vehicles between different lists.



3. To extract data for external reporting, select the desired registry and utilize the export function to download the vehicle information.

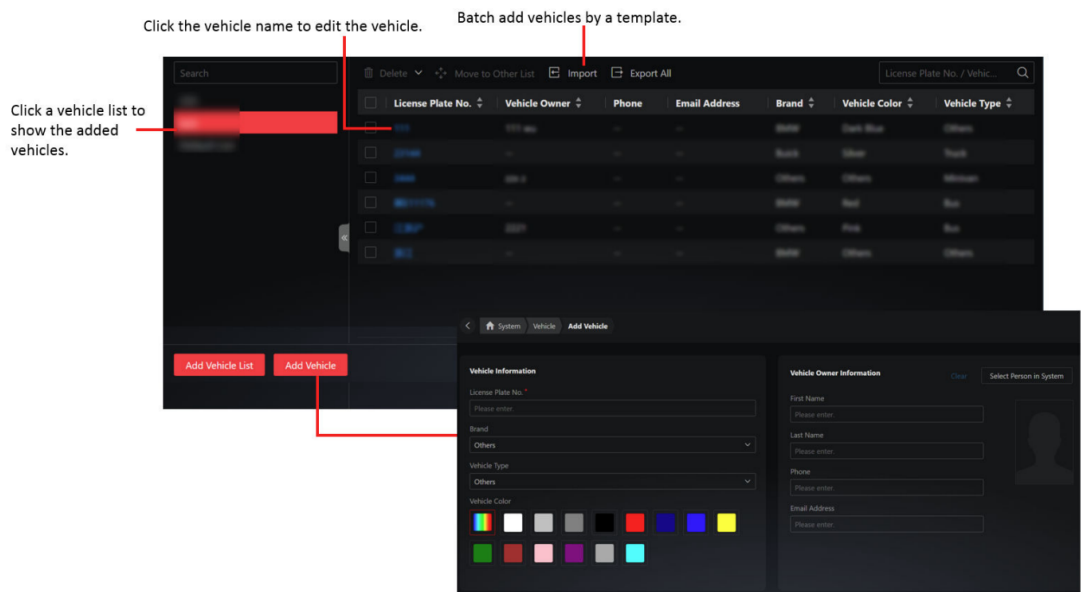


Figure 3.19 Vehicle Page

| Basic Information                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               |       |               |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------|---------------|-------|---------------|
| Time                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               |       |               |
| Operator                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               |       |               |
| Total Records                                                             | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |       |               |       |               |
| Rule (Enter corresponding vehicle information according to following No.) |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               |       |               |
| Brand                                                                     | 0=Others 1=Volkswagen 2=Buick 3=BMW 4=Honda 5=Peugeot 6=Toyota 7=Ford 8=Nissan 9=Audi 10=Mazda 11=Chevrolet 12=Citroen 13=Hyundai 14=Chery 15=KIA 25=Dongfeng 26=BYD 27=Suzuki 28=Jinbei 29=Haima 30=SGMW 31=JAC 32=Subaru 33=Englon 34=GWM 35= Hafei 36=Qingling/Isuzu 37=SOUEAST 38=Changan 39=50=Kama 51=Zotye 52=Changhe 53=Xiamen King Long (Golden Dragon) 54=Shanghai Huizhong 55=Suzhou Jinglong 56=Higer 57=Yutong 58=CNHTC 59=Beiben Heavy 100=BMW MINI 101=Toyota MARKX 102=HAVAL 103=Acura 104=Venucia 105=BYD Style 2 106=Benz SMART 107=BAW 108=Luxgen 109=Mustang 110=Zhongxing 111=121=Foday 122=Lotus 123=Nanjun 124=Shuanghuan Motor 125=Hafei Saibao 126=Huatai 127=Yongyuan Feidie 128=Yongyuan Motor 129=Fu Long Ma 130=Hyundai 1 150=GMC 151=SAIC Maxus 152=Beiqi Yinxiang 153=New Qirui 154=Mudan 155=Dayun Motor 156=Dongwo Motor 157=Union Motor 158=Chunzhou Bus 159=Sany Hea 200=Maserati 201=Shuchi Bus 202=Shili Bus 203=Zhongke Huabei 204=SAIC Yizheng 205=Chunlian Motor 206=Dafa Motor 207=Sheny Motor 208=Ferrari 209=Fuxing 81=1025=AC Schnitzer 1026=Alfa Romeo 1027=ASTON MARTIN 1029=LA JOYA 1041=BRABUS 1042=BUGATTI 1047=Changfeng Liebao 1049=Changan Saloon 1055=DETRC 90=KANDI 1092=KOENIGSEGG 1095=Rolls-Royce 1096=LINCOLN 1099=LANCIA 1100=LOTUS NYO 1109=Meiya 1110=McLaren 1111=MAYBACH 1113=MORGAN 111 1681=Wanda Bus 1682=Changan Suzuki 1683=Gullin 1684=Sichuan Hyundai 1685=Aochi 1686=Denway Bus 1687=FAW-Liut 1688=Wanxiang 1690=Sojen 1692=Zoomliao 1776=Rohens 1783=Proton 1786=Emgrand 1787=HINO 1792=Alfa 1793=Equus 1794=Renault Samsung 1796=Oushang 1797=BONLUCK 1798=Qiling 1799=Wanxiang 1 0=Others 1=Bus 2=Truck 3=Sedan 4=Minivan 5=Light Truck 6=Pedestrian 7=Two-Wheeler 8=Tricycle 9=SUV/MPV 10=Medium-Sized Bus 11=Motor Vehicle 12=Non-Mo 13=Vehicle Color 0=Other 1=White 2=Silver 3=Gray 4=Black 5=Red 6=Dark Blue 7=Blue 8=Yellow 9=Green 10=Brown 11=Pink 12=Purple 13=Dark-Grey 14=Cyan. |                  |       |               |       |               |
| Vehicle Information                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               |       |               |
| *License plate No.                                                        | Vehicle Owner                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Vehicle Owner ID | Phone | Email Address | Brand | Vehicle Color |
|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               | 6     | 3             |
|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               | 31    | 9             |
|                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |       |               | 22    | 1             |

Figure 3.20 Export Vehicle Information

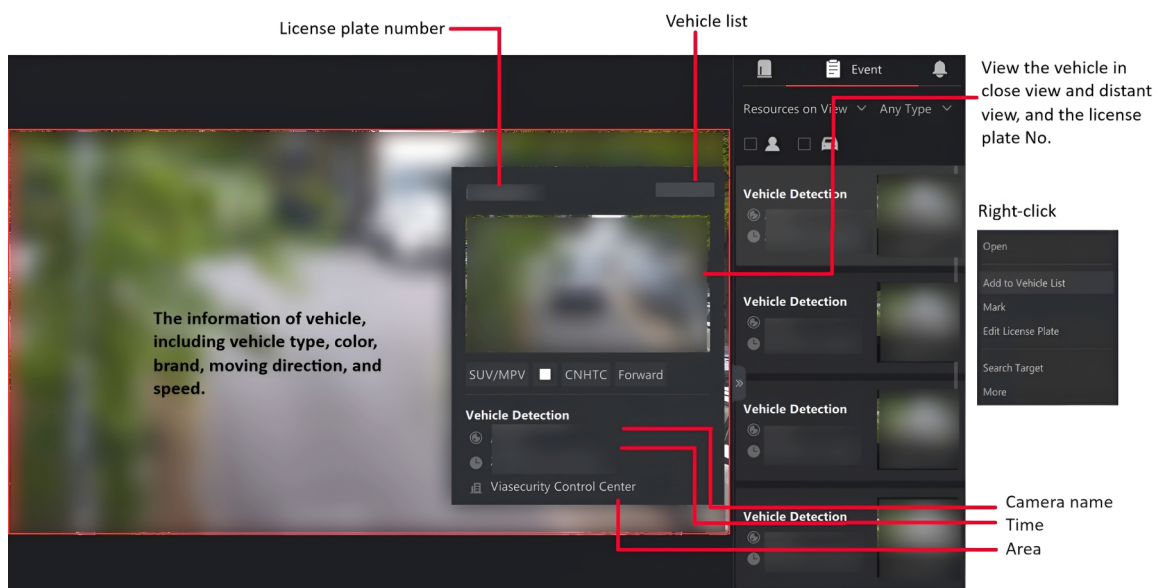
### 3.4.2 View Video Related to Vehicle Monitoring

Operators can oversee live traffic and monitor real-time vehicle passing events through connected ANPR camera streams. As vehicles are detected, the system instantly cross-references the captures against active vehicle list, displaying recognized owner details and list matches directly alongside the video feed.

**Key Interactions:**

- Hover over any active vehicle event to instantly view a summary of the detection.
- Right-click an event to perform immediate administrative actions, such as manually correcting a misread license plate or directly assigning the recognized vehicle to a specific registry list.

**Prerequisite:** Before utilizing live ANPR monitoring, verify that all necessary recognition cameras are fully integrated and that their respective channels are licensed. Allocate these licenses by navigating to **License Management → License Overview**.



**Figure 3.21 ANPR Event Details**

### 3.4.3 Search and Export ANPR Events

The Viasecurity Control Center maintains a comprehensive, searchable archive of all vehicle passing events, enabling security personnel to efficiently retrieve and extract historical traffic data.

#### Instructions:

- Navigate to **Search → Vehicle Passing Event** to access the historical ANPR query interface.
- Apply precise search filters—including date and time ranges, specific camera sources, target vehicle lists, or exact license plate strings—to isolate the required records.
- To examine an individual's detection in depth, click directly on the text within the **License Plate No.** column to open its full capture details.

- To extract these logs for external auditing or reporting, click the **Export** button to download the filtered results locally in Excel, PDF, or CSV format.

|    |                        |      |        |              |       |           |                |              |       |       |               |                   |
|----|------------------------|------|--------|--------------|-------|-----------|----------------|--------------|-------|-------|---------------|-------------------|
| 1  | ANPR Retrieval Records |      |        |              |       |           |                |              |       |       |               |                   |
| 2  | SYS:                   |      |        |              |       |           |                |              |       |       |               |                   |
| 3  | Export Time:           |      |        |              |       |           |                |              |       |       |               |                   |
| 4  | Total Number: 17353    |      |        |              |       |           |                |              |       |       |               |                   |
| 5  |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 6  | License Plate No.      | Time | Camera | Vehicle List | Owner | Phone No. | Country/Region | Vehicle Type | Brand | Color | Driving Speed | Driving Direction |
| 7  |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 8  |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 9  |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 10 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 11 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 12 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 13 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 14 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 15 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 16 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 17 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 18 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 19 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 20 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 21 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 22 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 23 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 24 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 25 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 26 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 27 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 28 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 29 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 30 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 31 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 32 |                        |      |        |              |       |           |                |              |       |       |               |                   |
| 33 |                        |      |        |              |       |           |                |              |       |       |               |                   |

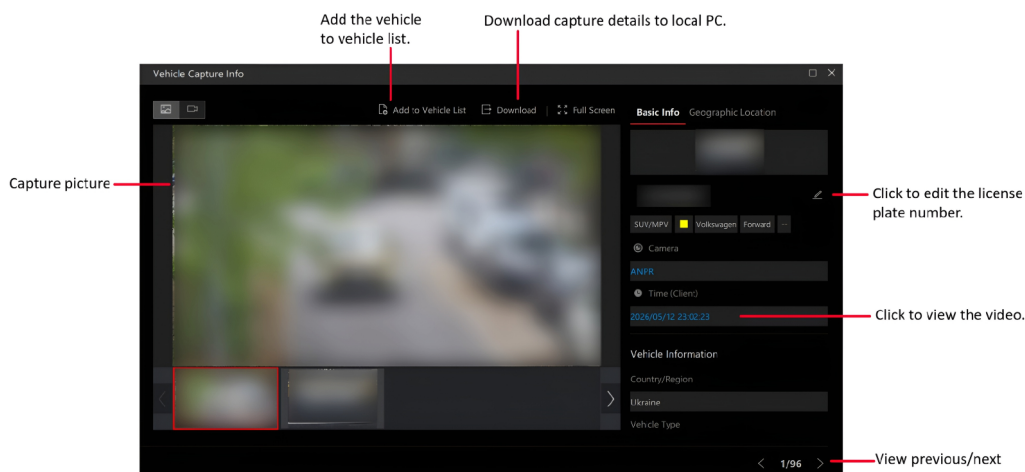
Figure 3.22 Export Vehicle Passing Events in Excel Format

Vehicle Pass Information

Basic Info  
Search Time: 2026/05/12 17:03:31  
Search by: admin  
Time: 2026/05/12 00:00:00 - 2026/05/12 23:59:59  
Total Number: 96

| License Plate | Capture Details             | Vehicle Information                                   | Owner Information | Thumbnails |
|---------------|-----------------------------|-------------------------------------------------------|-------------------|------------|
|               | ANPR<br>2026/05/12 23:02:23 | Ukraine<br>SUV/MPV<br>Volkswagen<br>Yellow<br>Forward | --                |            |
|               | ANPR<br>2026/05/12 23:02:07 | Ukraine<br>SUV/MPV<br>Ford<br>Black<br>Reverse        | --                |            |
|               | ANPR<br>2026/05/12 23:00:06 | Ukraine<br>Sedan<br>Changan DS<br>Black<br>Reverse    | --                |            |
|               | ANPR<br>2026/05/12 22:59:52 | Ukraine<br>SUV/MPV<br>Citroen<br>Black<br>Forward     | --                |            |
|               | ANPR<br>2026/05/12 22:58:11 | Ukraine<br>SUV/MPV<br>Nissan<br>Black<br>Forward      | --                |            |
|               | ANPR<br>2026/05/12 22:58:01 | Ukraine<br>Sedan<br>Toyota<br>Black<br>Forward        | --                |            |

Figure 3.23 Export Vehicle Passing Events in PDF Format



**Figure 3.24 Vehicle Capture Details**

## 3.5 Smart Search Capabilities

The Smart Search / VCA module provides advanced tools to efficiently locate specific targets and analyze recorded video footage. You can use the smart search or VCA search function depending on whether your connected devices support the corresponding features. Before using either the smart search or VCA search functions, make sure that recording schedules have been properly configured for the relevant network cameras

### 3.5.1 Smart Search / VCA

#### Configuration for NVR and Network Camera

To leverage the Smart Search or VCA features, ensure your network cameras are configured with active recording schedules and that your NVR hardware supports these functions. Configuration procedures vary depending on your specific hardware deployment:

- **For NVRs running Firmware V5.01 or higher:** Access the NVR web interface. Navigate to **Storage Management** → **Advanced Configuration** and enable the **Camera Intelligence Data Storage**.

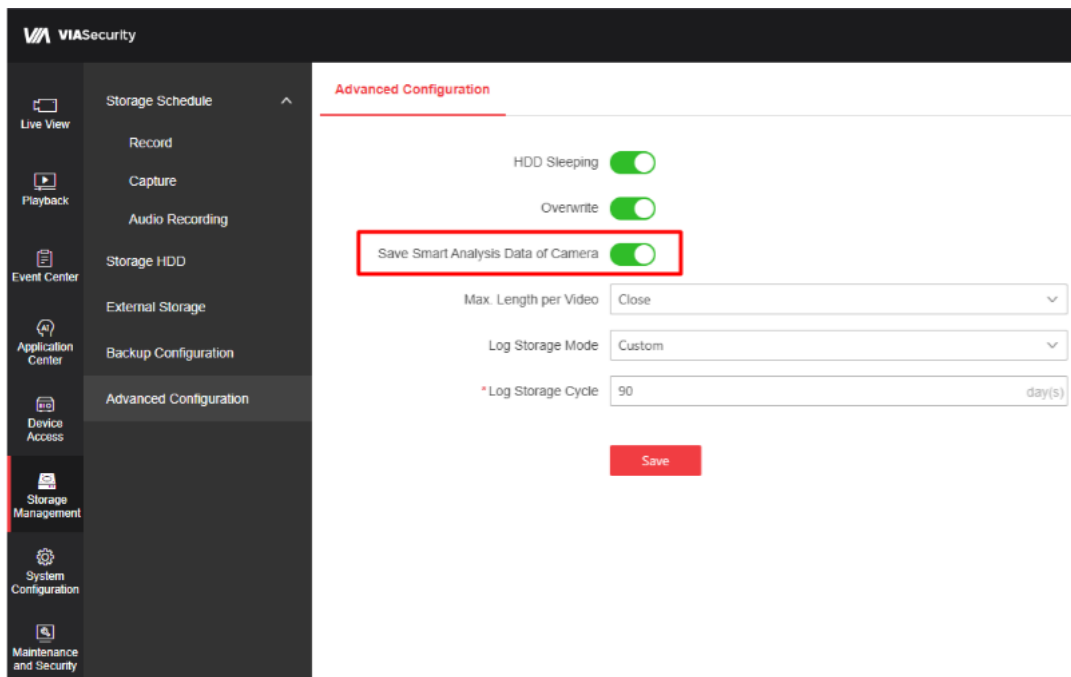


Figure 3.24 Save Smart Analysis Data of Camera

- **For NVRs running Firmware below V5.01:** Log into the NVR web interface and enable **Dual-VCA** for the target network camera. Ensure both **Enable Line Crossing Detection** and **Enable Intrusion** are checked. And select **Save Camera VCA Data** to apply the settings.

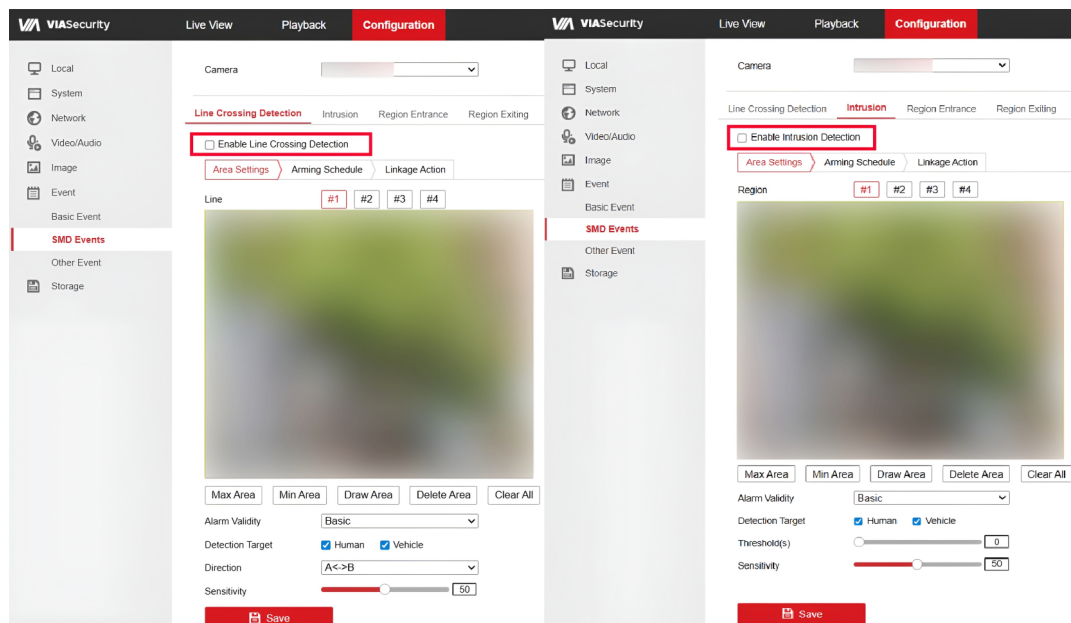


Figure 3.25 Enable Line Crossing Detection & Enable Intrusion Detection

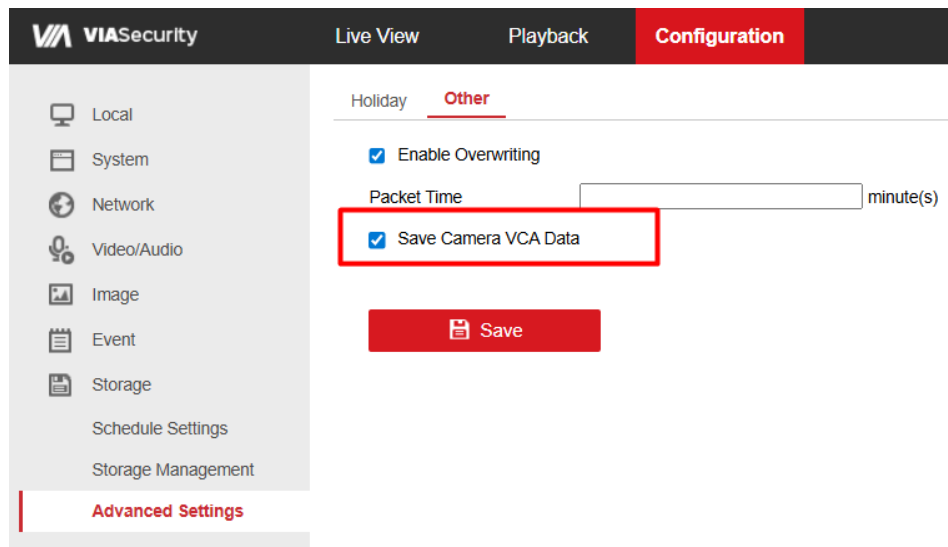


Figure 3.26 Save Camera VCA Data

- **For cameras added independently to Viasecurity Control Center or via NVR without VCA support:** Access the standalone web interface of the camera and enable **Dual-VCA**. Afterward, navigate to the Camera Details page within the system and set the video storage location to **System Storage**.

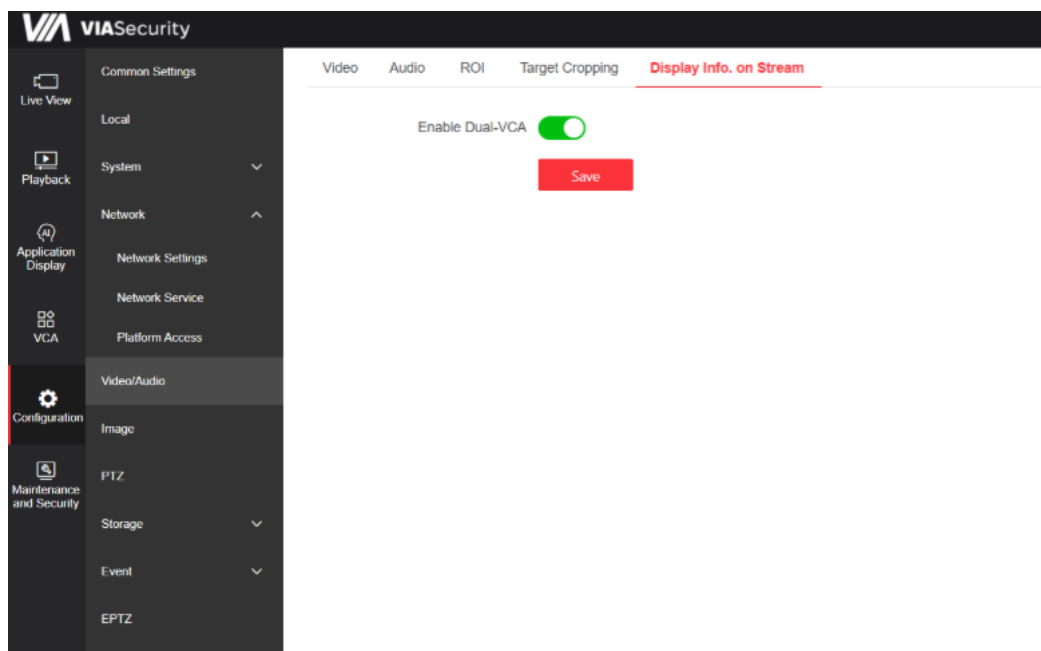
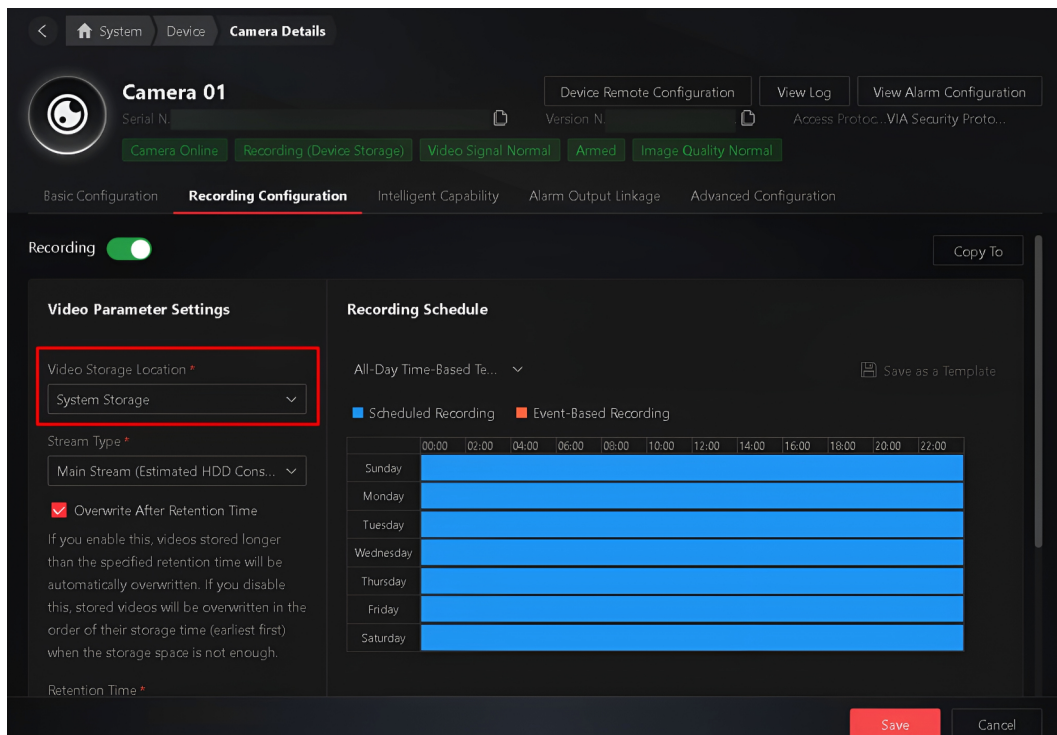


Figure 3.27 Enable Dual-VCA





**Figure 3.28 Configure Video Storage Location**

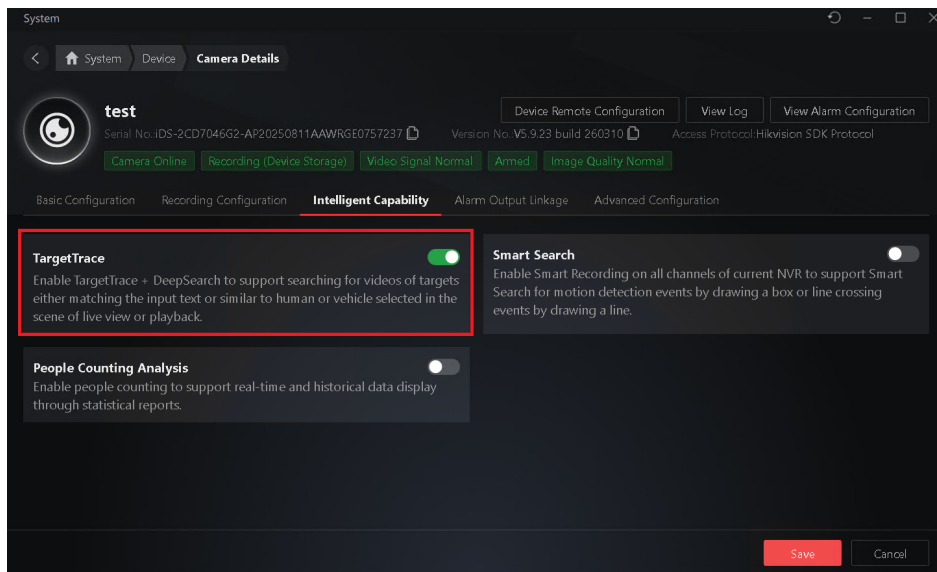
## 3.5.2 TargetTrace and Object Search

This feature automates the extraction and comparison of human or vehicle imagery from live feeds and recorded playback, allowing operators to rapidly track specific targets across the surveillance network. The interface dynamically labels the activation button as either "TargetTrace" or "Object Search," depending on whether the connected hardware explicitly supports advanced object searching. The feature must be toggled on within the Camera Details menu.

We highly recommend updating all system devices to their latest firmware versions to ensure full compatibility.

### Before You Start

Before using this function, make sure you have enabled it on the Camera Details page.



**Figure 3.29 Camera Details**

### Execution via Intelligent Search

While viewing search results, right-click a video thumbnail and choose the TargetTrace / Object Search option to initiate a system-wide scan for similar targets in recorded footage.

### Execution via Live View or Playback

Click the designated TargetTrace / Object Search icon directly on the viewing window. Corresponding matches will automatically populate in the right-hand panel.

## 3.5.3 People Counting Analytics and Reports

Generate comprehensive visual reports detailing real-time entries, current location occupancy (dwell quantity), and historical foot traffic metrics.

*(Note: A dedicated License for people counting must be acquired and activated prior to report generation.)*

### Usage

The Real-Time People Counting pane monitors today's specific entry events and current dwell quantities, whereas the Historical People Counting pane tracks overall entry and exit visits. All historical data reports can be downloaded directly to a local PC for external review.



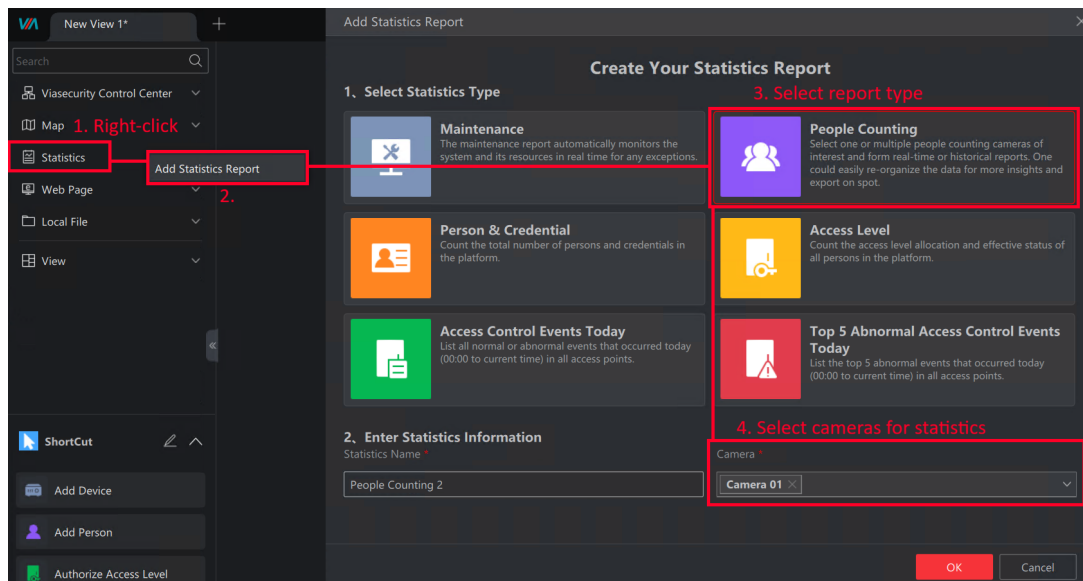


Figure 3.39 Generate People Counting Report

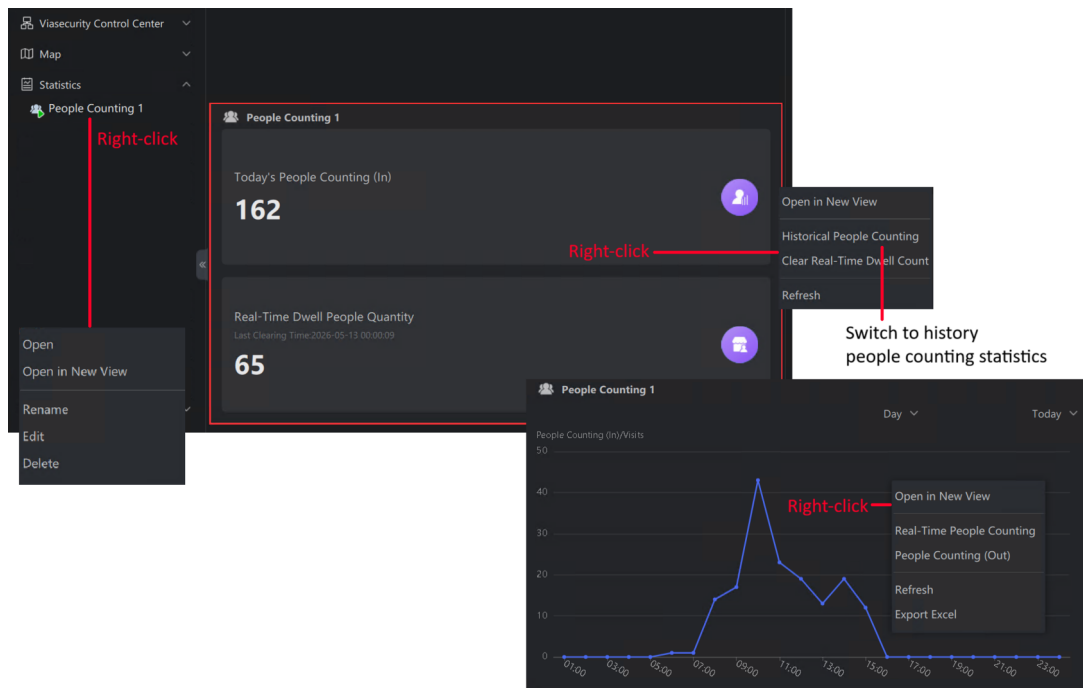


Figure 3.40 View Generated People Counting Report

| Historical People Counting   |                                                               |             |                                    |                     |                                     |                     |
|------------------------------|---------------------------------------------------------------|-------------|------------------------------------|---------------------|-------------------------------------|---------------------|
| Basic Information            |                                                               |             |                                    |                     |                                     |                     |
| Export Time                  | 2024-11-01 10:31:55                                           |             |                                    |                     |                                     |                     |
| Operator                     | admin                                                         |             |                                    |                     |                                     |                     |
| Statistics Name              | People Counting                                               |             |                                    |                     |                                     |                     |
| Data Source                  | Total Cameras: 5(camera1; camera2; camera3; camera4; camera5) |             |                                    |                     |                                     |                     |
| Data Type                    | People Counting (In)&People Counting (Out)                    |             |                                    |                     |                                     |                     |
| Data Time Period             | 2024-11-01 00:00:00 - 2024-11-01 23:59:59                     |             |                                    |                     |                                     |                     |
| Total People Count 6(Visits) |                                                               |             |                                    |                     |                                     |                     |
| Total People Counting        |                                                               |             |                                    |                     |                                     |                     |
| No.                          | Date                                                          | Time        | Total People Counting (In)(Visits) |                     | Total People Counting (Out)(Visits) |                     |
| 1                            | 2024-11-01                                                    | 00:00-00:59 | 0                                  |                     | 0                                   |                     |
| 2                            | 2024-11-01                                                    | 01:00-01:59 | 0                                  |                     | 0                                   |                     |
| 3                            | 2024-11-01                                                    | 02:00-02:59 | 0                                  |                     | 0                                   |                     |
| 4                            | 2024-11-01                                                    | 03:00-03:59 | 0                                  |                     | 0                                   |                     |
| 5                            | 2024-11-01                                                    | 04:00-04:59 | 0                                  |                     | 0                                   |                     |
| 6                            | 2024-11-01                                                    | 05:00-05:59 | 0                                  |                     | 0                                   |                     |
| 7                            | 2024-11-01                                                    | 06:00-06:59 | 0                                  |                     | 0                                   |                     |
| 8                            | 2024-11-01                                                    | 07:00-07:59 | 0                                  |                     | 0                                   |                     |
| Details                      |                                                               |             |                                    |                     |                                     |                     |
| No.                          | Date                                                          | Time        | camera1                            | camera2             | camera3                             | camera4             |
| 1                            | 2024-11-01                                                    | 00:00-00:59 | People Counting (0)                | People Counting (0) | People Counting (0)                 | People Counting (0) |
| 2                            | 2024-11-01                                                    | 01:00-01:59 | 0                                  | 0                   | 0                                   | 0                   |
| 3                            | 2024-11-01                                                    | 02:00-02:59 | 0                                  | 0                   | 0                                   | 0                   |
| 4                            | 2024-11-01                                                    | 03:00-03:59 | 0                                  | 0                   | 0                                   | 0                   |
| 5                            | 2024-11-01                                                    | 04:00-04:59 | 0                                  | 0                   | 0                                   | 0                   |
| 6                            | 2024-11-01                                                    | 05:00-05:59 | 0                                  | 0                   | 0                                   | 0                   |
| 7                            | 2024-11-01                                                    | 06:00-06:59 | 0                                  | 0                   | 0                                   | 0                   |
| 8                            | 2024-11-01                                                    | 07:00-07:59 | 0                                  | 0                   | 0                                   | 0                   |
| 9                            | 2024-11-01                                                    | 08:00-08:59 | 0                                  | 0                   | 0                                   | 0                   |

Figure 3.41 Downloaded Reports

# Chapter 4 Access Control and Video Intercom

This section outlines the system's capabilities for managing access devices, personnel data, and communication features, enabling comprehensive facility monitoring. The software offers multiple tools to track credentials, review event statistics, and maintain real-time physical security.

## Access Control Overview

The access control functionalities provide a streamlined approach to managing your facility's physical security infrastructure. Administrators can easily integrate access hardware into the system, configure core network parameters, and view detailed operational statuses for devices. To maintain an organized database, the software allows operators to structure users into departments, manage individual profiles, and set up the necessary credential collection of devices.

To regulate facility entry, security operators can define specific authorization schedules. These access levels can be assigned to either entire departments or individual users, dictating exactly who can unlock specific doors and at what times. During daily operations, the system offers robust real-time monitoring capabilities. Operators can watch live camera feeds linked to specific doors, dynamically alter door lock statuses on the fly, and visually monitor multiple entry points using interactive system maps.

Additionally, the system ensures comprehensive data tracking and reporting. Operators can search through historical access events or generate detailed statistical overviews covering personnel and system activities. To guarantee data integrity, the software also supports the manual importation of offline person authentication logs directly from the hardware.

## Video Intercom Capabilities

The Video Intercom module facilitates comprehensive communication between devices and the central client software, giving operators detailed control over visitor interactions. Through the notification panel, operators can easily monitor missed calls from hardware devices and seamlessly initiate callbacks directly from the interface. Additionally, security personnel have the ability to manually start a live, two-way audio stream with any connected device at any time.

To streamline operational workflows, administrators can configure specific audio and call routing rules for the current client. The software allows you to define precise time limits, such as an Automatic Call End Time After No Answer, which automatically terminates unanswered device calls after a specified timeout duration. You can also establish a Maximum Call Duration to cap the length of any active, ongoing conversation. Furthermore, the system supports custom call routing, enabling you to link specific hardware devices to designated client users. This ensures that intercom requests from various locations are always directed to the appropriate personnel.

## 4.1 Preparations

### 4.1.1 Add Devices

The system supports adding access control devices, door stations, and barrier gates.

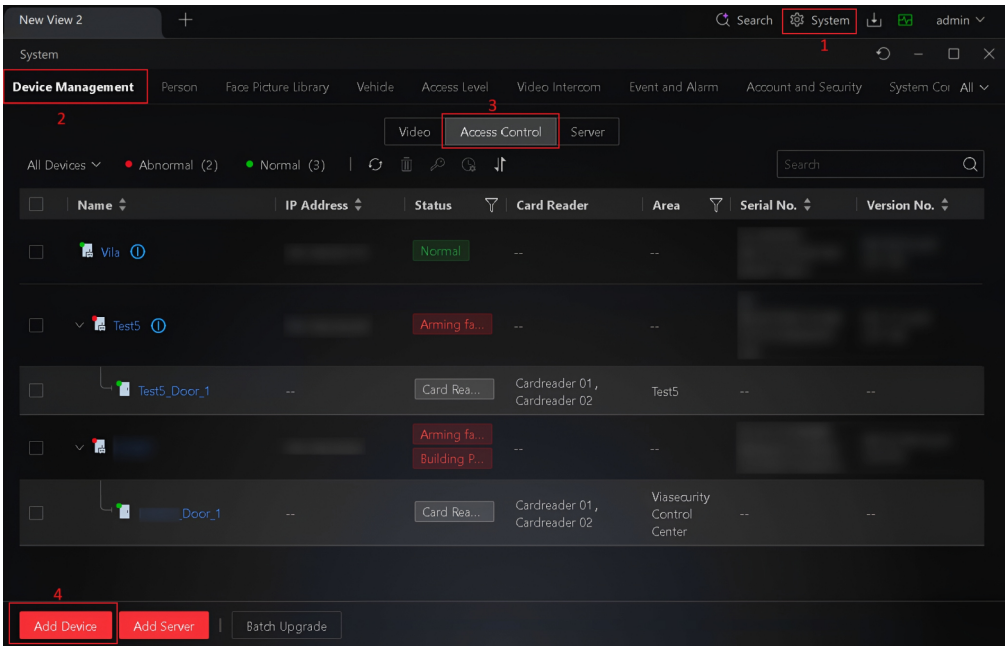
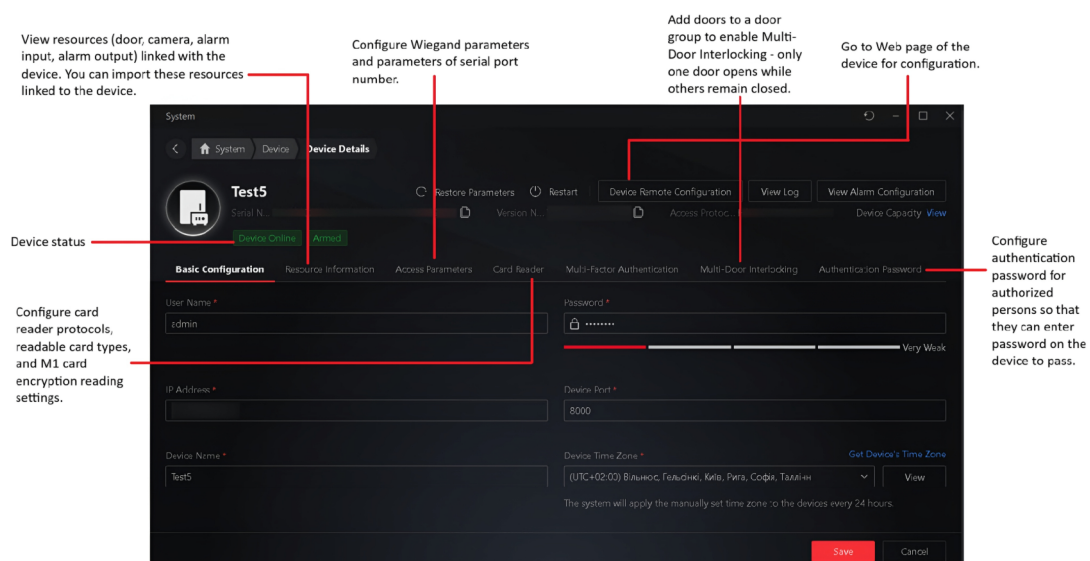


Figure 4.1 Device List

See [2.2 Adding Device](#) for details.

## 4.1.2 View Details of a Device

To check the current status or modify settings for specific hardware, navigate to the device list. Access the configuration interface by clicking the device's name directly, or by right clicking the device or door and selecting **View Details**.



**Figure 4.2 Details of an Access Control Device**

Within the details page, operators can manage the following key features:

### Resource Management

View and configure linked hardware resources. For added convenience, alarm inputs and outputs can also be imported in bulk directly via the main device list.

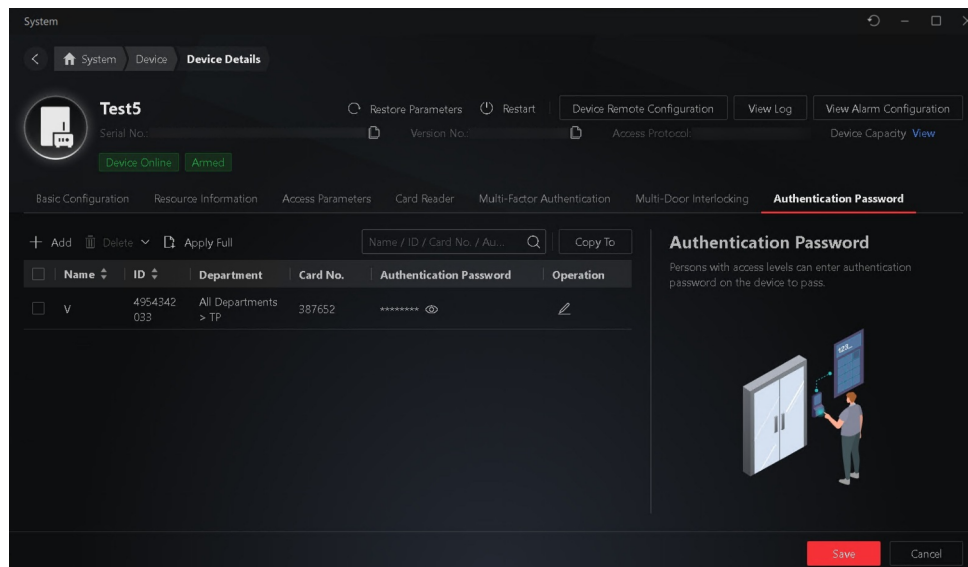


Figure 4.3 Device List

### Multi-Factor Authentication Interval

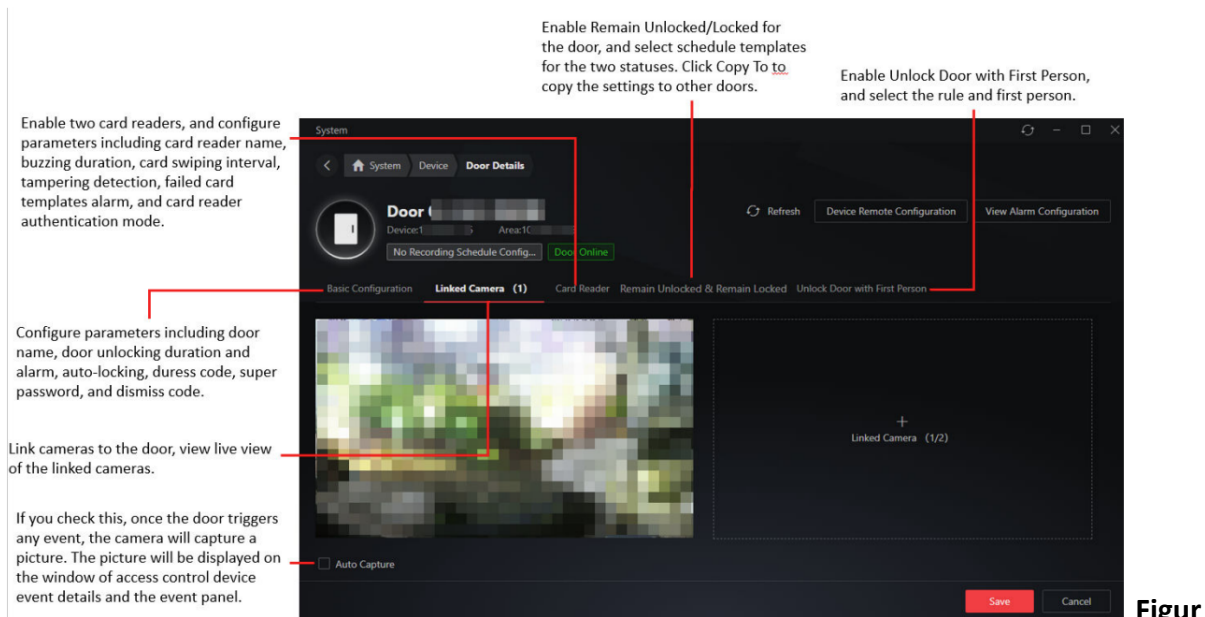
Set the maximum allowed time limit between each verification step. If this timeframe (for example, 5 seconds) expires before the next credential is presented, the attempt is invalidated, and the user must restart the entire authentication sequence.

### Authentication Password

Enable supplementary password verification. Please note that this feature requires compatible hardware. Additionally, the administrator or operator configuring this setting must have the **Authentication Code Configuration** permission assigned to their user role.

## 4.1.3 View Details of a Door

In the device list, click the name of a door, or right-click a door, and then select **View Details**.



## 4.2 Add Departments and Persons

The **Person** page allows operators to manage user profiles, organize organizational structures, and export personnel data to a local PC.

### Add Departments

To build your organizational hierarchy, right-click the root node or any existing folder to add a **Sub-Department** or **Same-Level Department**. You can easily adjust a department's level by dragging and dropping it within the department tree.

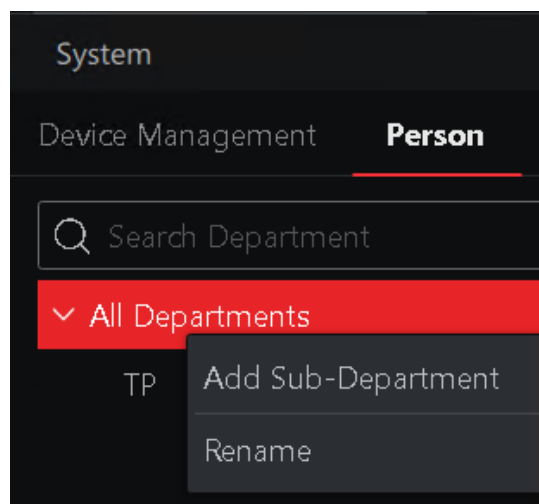


Figure 4.5 Department Tree

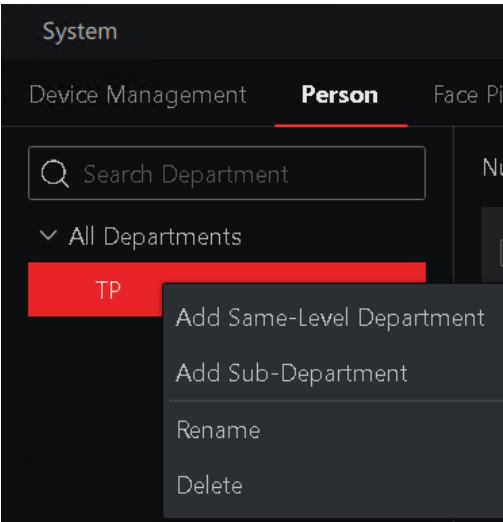


Figure 4.6 Department Tree

Add Persons

Import person information via an excel file, import person information saved in devices, and import person profile pictures to the client.

Save person information or profile pictures to the PC. The login password is required for security.

Right-click a profile picture to show the following list:

- Identity Access Search
- Edit Person
- Replace Profile Picture
- Delete Person
- Delete Profile Picture

Click a person's name to enter the profile page.

Adjust Department  
Adjust Effective Period  
Batch Issue Cards  
Batch Report Card Loss  
Batch Cancel Card Loss  
Forbid Passing  
Allow Passing  
Configure Additional Information

Configure Credentials  
No Credential Configured  
Loss Reported  
Reset

Expired  
Forbid Passing  
Normal  
Reset

Add and configure cards for the person.  
Add or edit the PIN.  
Collects fingerprints or irises.

A screenshot of the 'Person' tab in the 'System' interface. The top navigation bar includes 'Device Management', 'Person', 'Face Picture Library', 'Vehicle', 'Access Level', 'Video Inspection', 'Event and Alarm', 'Account Security', and 'System Configuration'. Below the navigation bar is a search bar and a table of people. The table has columns: 'Profile Picture', 'ID', 'Given Name', 'Surname', 'Department', 'Access Level', 'Status', and 'Credential'. The first row shows a person with a profile picture, ID, and 'New Organization' in the department. A context menu is open over the first row, showing options: 'Delete All', 'Delete Profile Picture Only', 'Identity Access Search', 'Edit Person', 'Replace Profile Picture', 'Delete Person', and 'Delete Profile Picture'. Another context menu is open over the 'Credential' column of the first row, showing options: 'Adjust Department', 'Adjust Effective Period', 'Batch Issue Cards', 'Batch Report Card Loss', 'Batch Cancel Card Loss', 'Forbid Passing', 'Allow Passing', 'Configure Additional Information', 'Configure Credentials', 'No Credential Configured', 'Loss Reported', 'Reset', 'Expired', 'Forbid Passing', 'Normal', and 'Reset'. A third context menu is open over the 'Profile Picture' column of the first row, showing options: 'Show Sub-Department Persons' and 'Show Person Profile Picture'. At the bottom of the page, there are buttons for 'Add Department', 'Add Person', and 'Credential Configuration'.

Figure 4.7 Person List



<

System

Person

Add Person

Basic Information

Credential

Access Level

Assign New Access Level

No assigned access levels.

Assign Now

☐ Super Access Permission

If you enable this, the person will not be subject to such access rules as remaining locked and first person authorization. The function is exclusive from the extended access function.

☐ Extended Access

If you enable this, the door unlocking duration will be extended and can be configured in door details page in Device Management > Access Control. The function and the access permission function cannot be enabled concurrently.

☐ Device Administrator

If you enable this, the person can log in to the device-related platform for operation.

Add

Add and Continue

Cancel

**Fig**

### Figure 4.8 Add Person Page

[illegible]

**Figu**

## re 4.9 Template for Importing Persons

| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | B          | C         | D               | E                              | F                            | G    | H      | I     | J     | K         | L               | M                    | N            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------|-----------------|--------------------------------|------------------------------|------|--------|-------|-------|-----------|-----------------|----------------------|--------------|
| Person Information_2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |           |                 |                                |                              |      |        |       |       |           |                 |                      |              |
| <b>Rule</b><br>Either first name or last name is required.<br>Once configured, the ID cannot be edited. Confirm the ID rule before setting an ID.<br>Do NOT change the layout or column heading in this template file. Otherwise, importing may fail.<br>You can add persons to existing departments. The department name should be separated by /. For example, to import persons to Department A under All Departments, please enter All Departments/Department A.<br>Start Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.<br>End Time of Effective Period: The effective period of the person for access control and access time. Format: yyyy/mm/dd HH:MM:SS.<br>No more than 3 cards can be applied to each person. Use semicolon (;) to separate if there is more than one card No., e.g. 01;02;03.<br>Extended Access and Super User: cannot be enabled at the same time. |            |           |                 |                                |                              |      |        |       |       |           |                 |                      |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           |                 |                                |                              |      |        |       |       |           |                 |                      |              |
| ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | First Name | Last Name | Department      | Start Time of Effective Period | End Time of Effective Period | Card | Gender | Email | Phone | Superuser | Extended Access | Device Administrator | Access Level |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           | All Departments |                                |                              |      |        |       |       | Disable   | Disable         | Disable              |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           | All Departments |                                |                              |      |        |       |       | Disable   | Disable         | Disable              |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           | All Departments |                                |                              |      |        |       |       | Disable   | Disable         | Disable              |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           | All Departments |                                |                              |      |        |       |       | Enable    | Disable         | Disable              |              |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |           | All Departments |                                |                              |      |        |       |       | Disable   | Disable         | Disable              |              |

### Figure 4.10 Exported Person Information

## Managing and Exporting Personnel

You can add new personnel profiles using various methods. When downloading templates for importing users, any supplementary system fields will be automatically included. If you need to export user profile pictures to your PC, you must first enable the permission by navigating **System → System Configuration → Security → Profile Picture**.

## Deleted User Data Retention

When a person is removed from the system, their core details (including name, ID, validity period, and credentials) are temporarily archived rather than immediately erased. To configure exactly how long this information is preserved before permanent deletion, navigate to **System → Storage → Data Retention Time → Deleted Person Data**.

## 4.2.1 Credential Configuration

Make sure you select the right collecting mode and configure the collecting device properly.

On the Person page, click **Credential Configuration**. Select a collection mode according to the following table.

**Table 4.1 Scenarios Applicable for Different Collection Mode**

| Collection Device                                                                                                             | Scenario                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Card Enrollment Station</li><li>• Fingerprint Recorder</li><li>• USB Camera</li></ul> | Ideal for mobile enrollment operations where administrators must travel to various locations to physically capture cards, face pictures, and fingerprints locally.                                                                                                                                    |
| Access Control Device                                                                                                         | Designed for remote credential collection using permanently installed hardware. The device must support this feature and be added to the system beforehand.<br><i>(Note: If the system fails to read a card number, access the Door Details page to ensure the specific door is currently armed.)</i> |
| Enrollment Station                                                                                                            | Versatile, portable units that connect via USB or network to capture face pictures, cards, and fingerprints. These stations allow collected credentials to be stored locally directly on the device itself.                                                                                           |

## 4.2.2 Protect Profile Pictures

Read this topic if you have a requirement for protecting profile pictures.

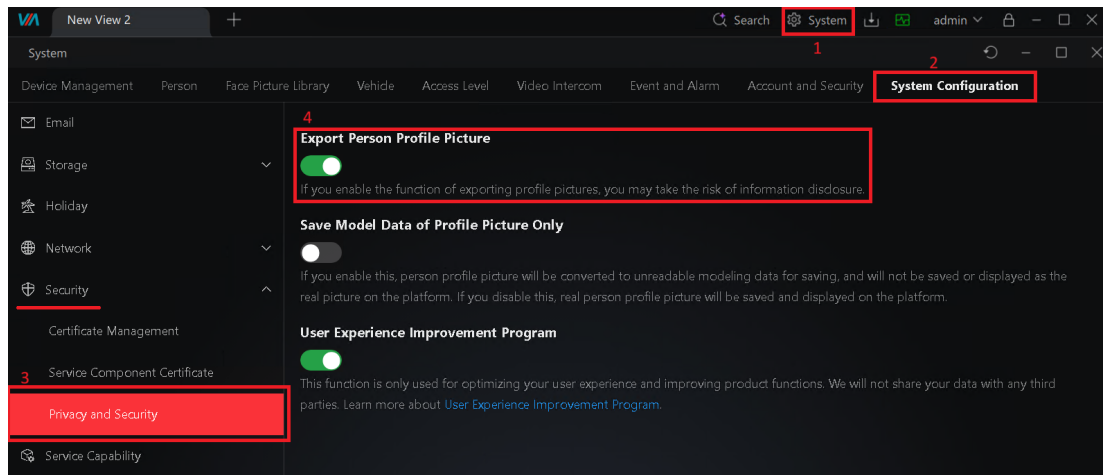


Figure 4.11 Entry of Protect Profile Pictures

### Export Person Profile Picture

If you enable this function, you will be able to export persons' profile pictures to the PC.

*(Note: Only the admin user can enable this function.)*

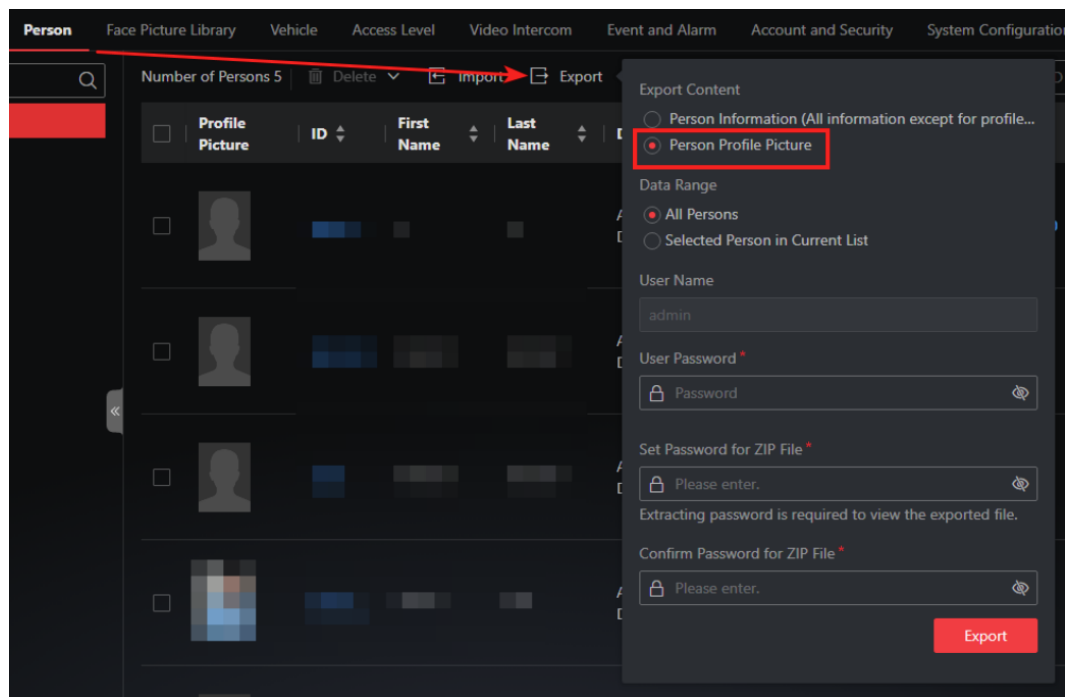


Figure 4.12 Entry of Exporting Profile Pictures

## 4.3 Managing Access Levels

An access level groups on specific doors with a designated time schedule, determining exactly who can unlock which doors and when. You can streamline security management by assigning these rules to either individual personnel or entire departments.

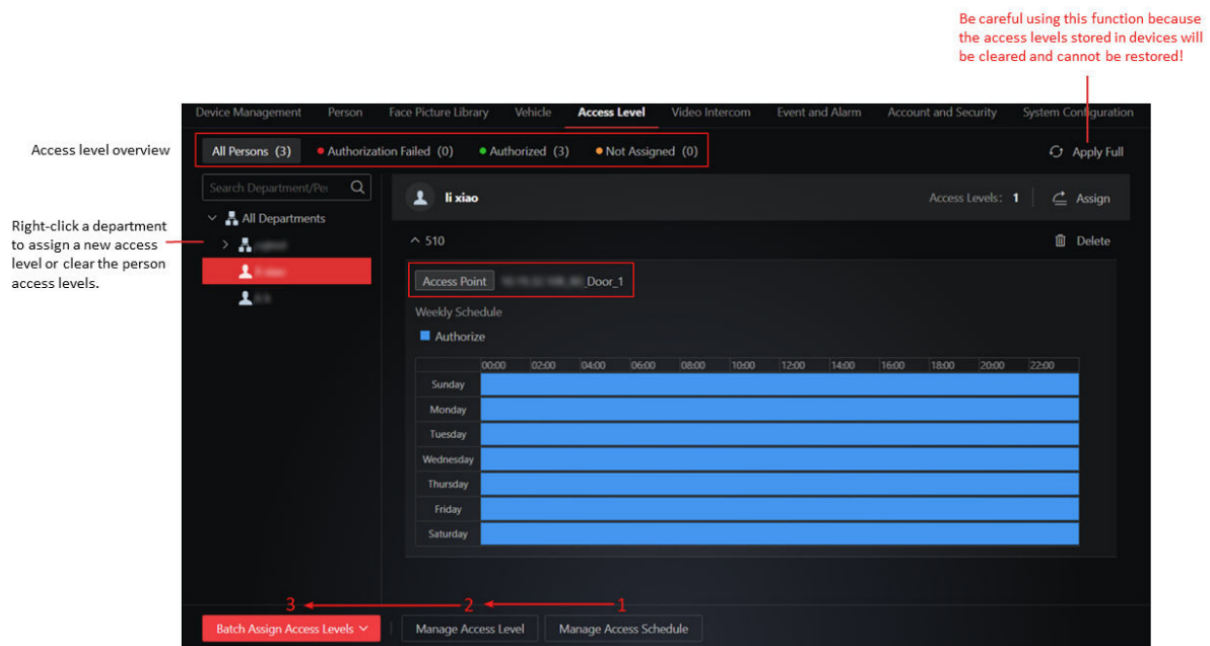


Figure 4.13 Access Level Page

### Add an Access Schedule

Schedules dictate when entry is permitted. You can utilize the three provided templates (all-day, workday, and weekend) or create custom parameters. Click **Authorize** and drag across the timeline to draw valid time periods. For precise adjustments, hover your cursor over the blue authorized block to manually type or tweak the exact times.



**Figure 4.14 Add an Access Schedule**

### Add an Access Level

Once a schedule is set, select the relevant doors to finalize the access level. Please note that a single door can be included in multiple different access levels simultaneously.

### Assigning Permissions:

- **By Department:** Recommended for granting standard entry to fixed locations, such as general office areas. Any new personnel added to that department will automatically inherit its associated access levels.
- **By Person:** Ideal for granting an individual user temporary permissions or highly specialized access to a restricted door.

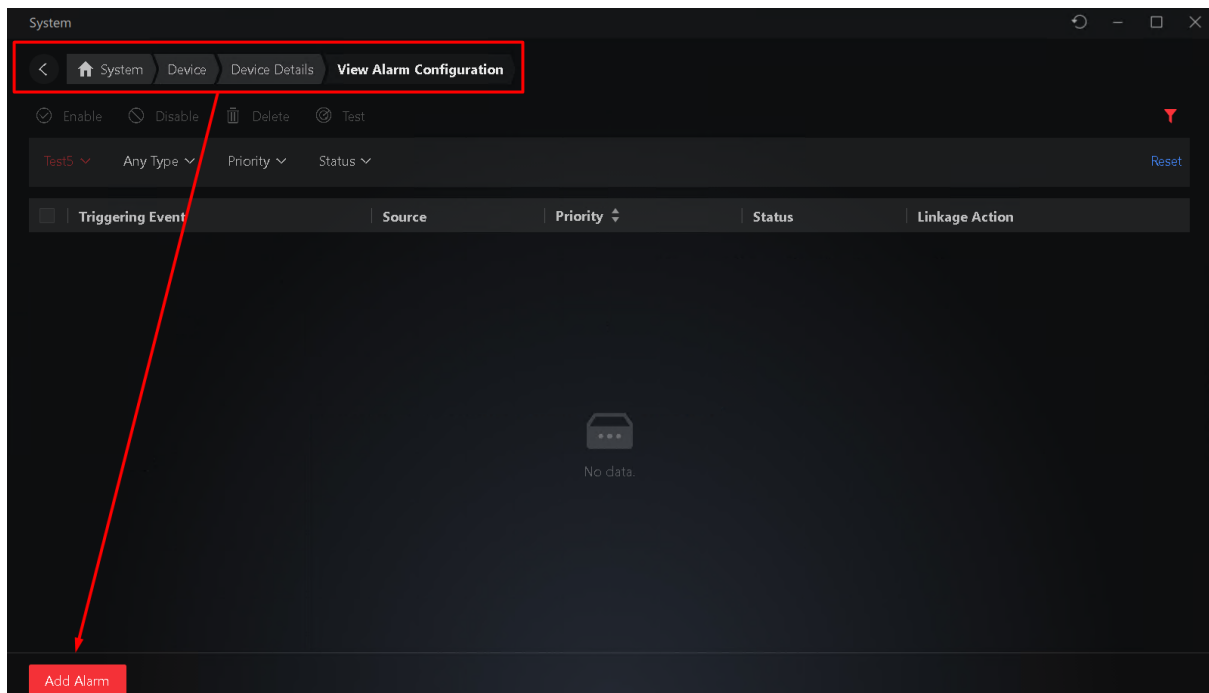
### Hardware Synchronization

Access levels assigned via the client software are automatically pushed to the physical hardware. If an assignment fails to apply, verify that the target device is not offline and that the network connection remains stable.

## 4.4 Add an Alarm

You can add an alarm for a specified device, or all resources in the system.

Both doors and access control / video intercom devices can trigger alarms. You can go to the Add Alarm page from the device details page, or the Event and Alarm module.



**Figure 4.15 Alarm Configuration Page**

| Resources that Can Trigger Alarms      | Alarm Category                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Door                                   | <ul style="list-style-type: none"> <li>• Normal Card Swiping</li> <li>• Abnormal Card Swiping</li> <li>• Other Door Events</li> </ul>                                                                                                                                                                        |
| Access Control / Video Intercom Device | <ul style="list-style-type: none"> <li>• Device Security</li> <li>• Device Network</li> <li>• Device Battery</li> <li>• Device Record Reporting</li> <li>• Device Disk/HDD</li> <li>• Device Component Communication</li> <li>• Local Operation on Device</li> <li>• Remote Operation on Platform</li> </ul> |
| Alarm Input                            | <ul style="list-style-type: none"> <li>• Alarm Input Triggered</li> <li>• Alarm Input Restored</li> </ul>                                                                                                                                                                                                    |
| Person                                 | <ul style="list-style-type: none"> <li>• Person Matched Event</li> <li>• Card Number Matched Event</li> </ul>                                                                                                                                                                                                |

## 4.5 Real-Time Monitoring of Doors

You can monitor doors and control door status in real time. Refer to the following table for the explanations.

**Table 4.2 Explanations of Door Status, Door Contact Status, Door Lock Status, and Door Status Control**



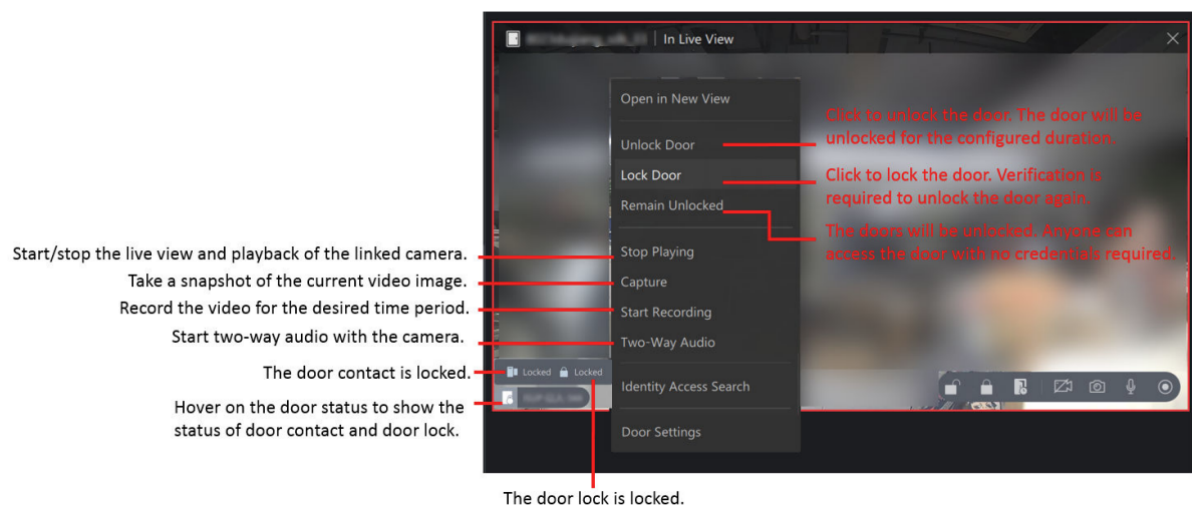
| Status              | Icon                                                                                | Explanation                                |
|---------------------|-------------------------------------------------------------------------------------|--------------------------------------------|
| Door Status         |    | Door Locked<br>Door Lock Locked            |
|                     |    | Door Locked<br>Door Lock Remain Locked     |
|                     |    | Door Locked<br>Door Lock Unlocked          |
|                     |    | Door Locked<br>Door Lock Remain Unlocked   |
|                     |    | Door Unlocked<br>Door Lock Locked          |
|                     |    | Door Unlocked<br>Door Lock Remain Locked   |
|                     |  | Door Unlocked<br>Door Lock Unlocked        |
|                     |  | Door Unlocked<br>Door Lock Remain Unlocked |
|                     |  | Unknown                                    |
| Door Contact Status |  | Door Contact Unlocked                      |
|                     |  | Door Contact Locked                        |
| Door Lock Status    |  | Door Lock Unlocked                         |
|                     |  | Door Lock Locked                           |
| Door Status Control |  | Close Door                                 |
|                     |  | Open Door                                  |
|                     |  | Set to Door Remain Locked                  |
|                     |  | Set to Door Remain Unlocked                |

## 4.5.1 Monitor Doors and Control Door Status

Once doors are configured, operators can manage their lock status and view live feeds (if equipped with or linked to a camera).

### Controlling Individual Doors

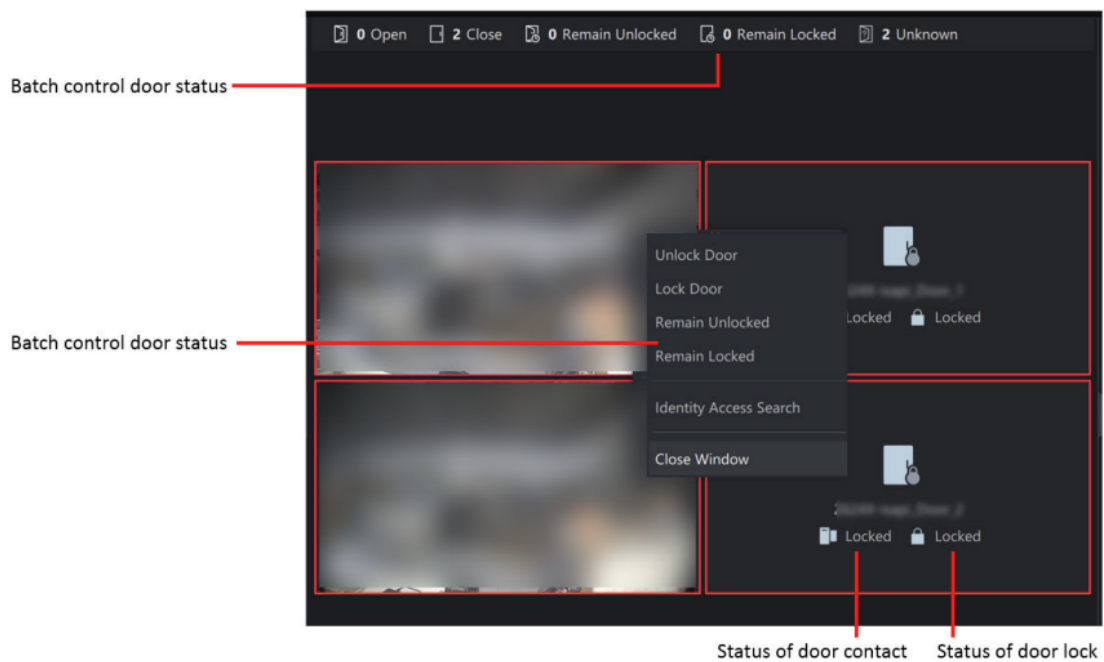
Double-click a door or drag it into the viewing grid. Right-click the item or use the icons in the lower-right corner to change the lock status.



**Figure 4.16 Supported Operations to Control One Door**

### Camera Features

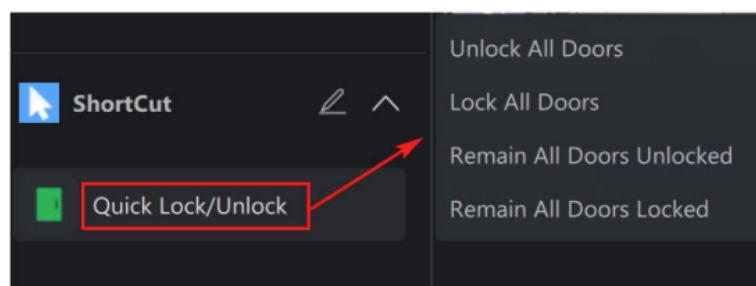
For doors with linked video, additional options are available directly from the view: Play/Stop Live Video, Image Capture, Video Recording, and Two-Way Audio.



**Figure 4.17 Select a Way to Control Doors on The Current View**

### Controlling Multiple Doors

- **Current View:** Draw a selection box over multiple doors in your grid, then right-click to apply bulk commands. Alternatively, use the top status icons to batch-control all currently visible doors.
- **Global Control:** Navigate to the **Shortcut** area and use the **Quick Lock/Unlock** function to globally lock, unlock, or secure all system doors instantly.



**Figure 4.18 The Entry to Control All Doors**

### Troubleshooting Status Exceptions

If the system reports a mismatch between a door's magnetic contact and its lock status, this typically indicates a physical obstruction preventing proper closure. The hardware should be physically inspected immediately

## 4.5.2 Display and Control Doors on the Map

The Map module provides a geographical interface for managing entry points and live camera feeds, including face recognition terminals and doors linked with cameras,

### Accessing Maps

Navigate to the **Map** module. Open a map by double-clicking it, dragging it to the main viewing window, or right-clicking and selecting **Open**.

### Add Map

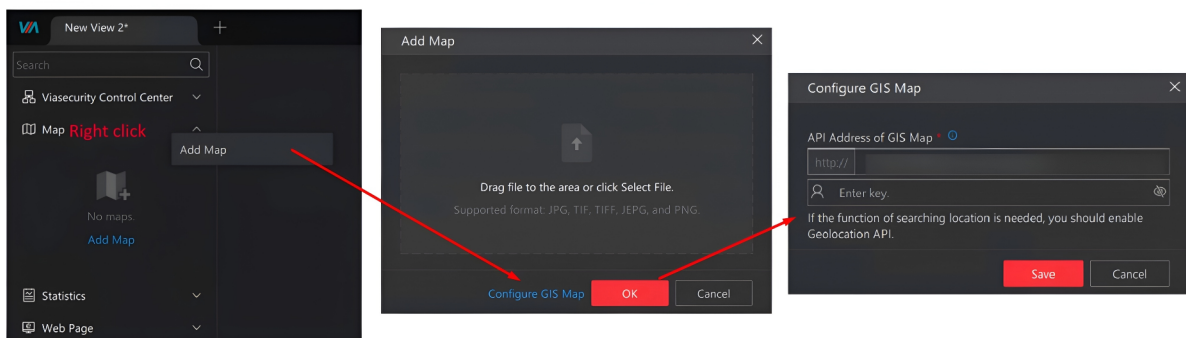


Figure 4.19 Add GIS Map

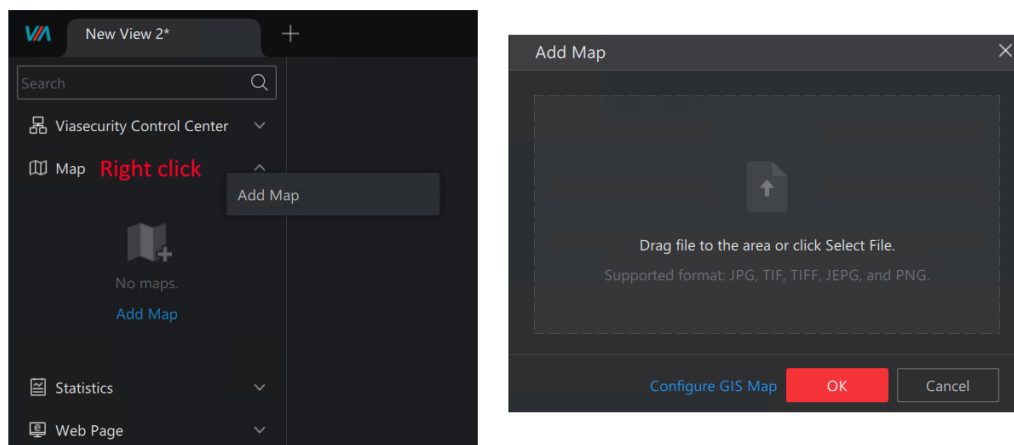


Figure 4.20 Add E-Map

### Operational Modes

The map interface uses two separate modes to separate setup from daily operations:

#### Configuration Mode

Use this mode to build your layout. You can add doors, place markers, define hot regions, and select which resources are displayed on the map.

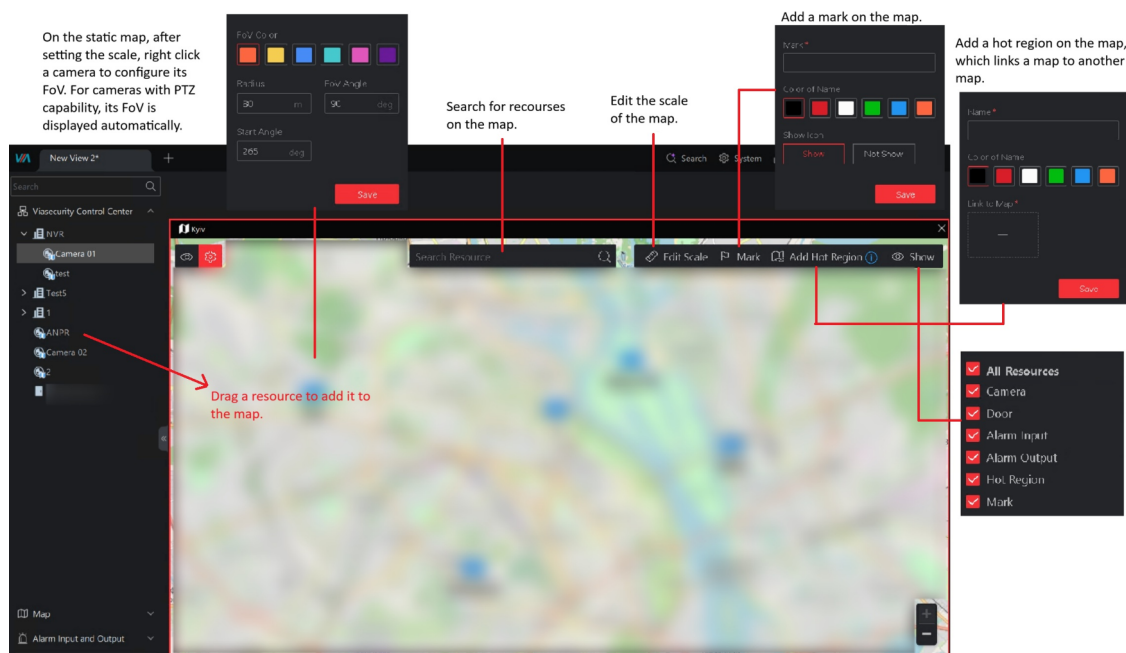


Figure 4.21 Supported Operations in Configuration Mode

## Monitor Mode

Use this mode for active security operations, live viewing, and door control.

### Actions in Monitor Mode

- **Single Door Operations:** Click on a door icon to immediately launch the live video feed from its linked camera. To alter the lock status, simply right-click the door.
- **Batch Operations:** To view multiple feeds simultaneously, click **Batch Select**, draw a highlighted area around the target doors on the map, and click **Batch Play** to open all linked live views at once.

## 4.6 Video Intercom Setup and Operations

People can call the system users via access control devices and video intercom devices, and users can also call the device via the client.

## Configuration Parameters

Before using the intercom, administrators must define call routing rules and time limits:

- **Call Recipients:** You can assign specific hardware devices to ring designated client operators, ensuring calls reach the appropriate personnel.
- **Automatic Call End Time After No Answer:** Establish an automated hang-up duration; if an operator fails to answer an incoming device call within this window, the system automatically terminates it.
- **Max. Call Duration:** Enforce a strict maximum time limit for any active, ongoing conversation between a field device and the client software.

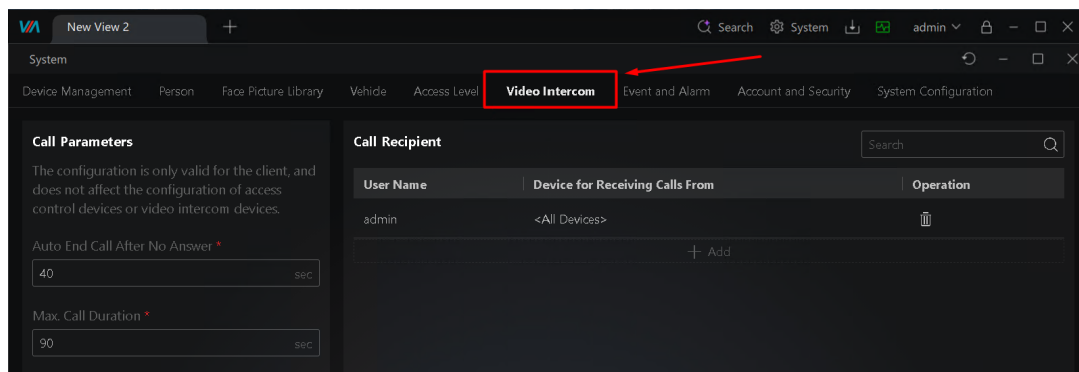


Figure 4.22 Entry of Video Intercom

## Video Intercom Call

Client operators can initiate communication with hardware devices using two primary methods:

- **Via Missed Call Notifications:** If a visitor attempts to call the client and the operator misses it, an alert populates in the notification panel. Right-click this alert, navigate to **View Details**, and select **Call Again** to instantly dial the device.

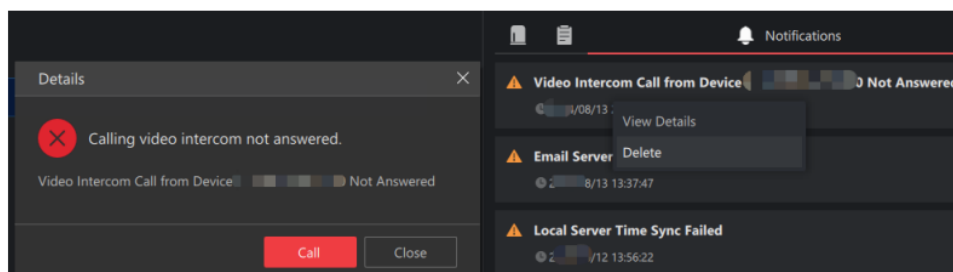


Figure 4.23 Call Device

- **Via Live View:** While actively monitoring the live video feed of a door's associated camera, click the designated intercom icon on the interface to open a two-way audio channel.

## 4.7 Event Management, Search, and Analytics

This section consolidates all tools required to track facility activity, recover offline logs, and visualize system data.

### 4.7.1 Searching and Exporting Event Logs

Operators can investigate historical system activity by navigating to **System → Access Event**. You can filter your search across three primary categories:

- **Person Authentication Event:** Review a history of both successful (normal) and failed (abnormal) credential scans.

The screenshot displays the 'Person Authentication Event' search interface. At the top, there are tabs for 'Person Authentication Event', 'Access Control Device Event', and 'Video Intercom Call Record'. Below these, there are buttons for 'Import Events', 'Import via File', and 'Export'. A red box highlights the 'Filtering conditions' section, which includes dropdown menus for 'Today', 'Access Points', 'Card No. Does Not Exist', 'Authentication Result', and 'Person'. Below the filters, a table lists event details with columns: Profile, First Name, Last Name, ID, Card No., Department, Time (Client), Access Points, Card Reader, Authentication Result, and Event Type. A red box highlights the 'Export' button. To the left, a text box says 'Select device(s) from which the person authentication events need to be imported to the client.' and another says 'Export person authentication events in in other client, and then import the file here.' Below this, a 'Details' panel shows 'Access Information' and 'Geographic Location'. At the bottom, a 'Total: 1' and '100' are displayed.

Exported person authentication events in Excel format

Select device(s) from which the person authentication events need to be imported to the client.

Export person authentication events in in other client, and then import the file here.

Filtering conditions

Profile First Name Last Name ID Card No. Department Time (Client) Access Points Card Reader Authentication Result Event Type

Total: 1 100

Figure 4.24 Person Authentication Event

- **Access Control Device Event:** Track hardware-level occurrences, such as unlocked door states, or general device triggers.

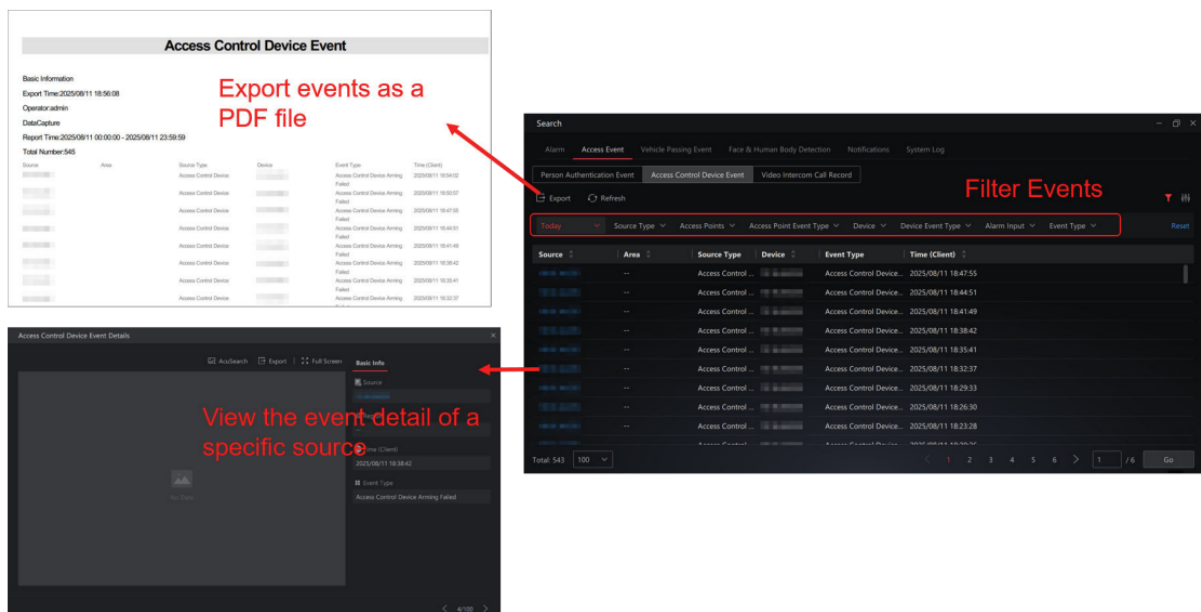


Figure 4.26 Access Control Device Event

- **Video Intercom Call Record:** Access to a complete historical record of all calls initiated from field devices to the client.

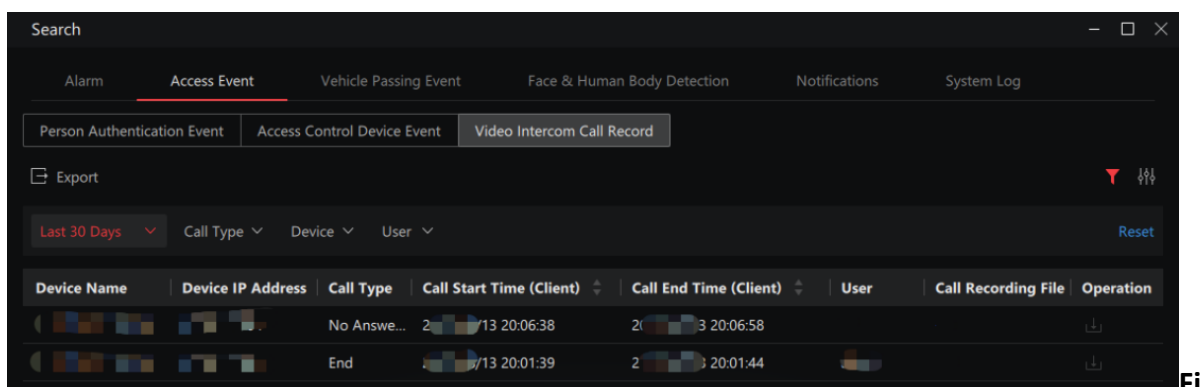


Figure 4.27 Video Intercom Call Records

|    | A                                   | B                 | C           | D                | E                | F    | G                       |
|----|-------------------------------------|-------------------|-------------|------------------|------------------|------|-------------------------|
| 1  | Video Intercom Call Record          |                   |             |                  |                  |      |                         |
| 2  | Basic Information                   |                   |             |                  |                  |      |                         |
| 3  | Export Time: 2025/08/11 20:02       |                   |             |                  |                  |      |                         |
| 4  | Operator: Data                      |                   |             |                  |                  |      |                         |
| 5  | Export Content: 2025/08/11 00:00:00 |                   |             |                  |                  |      |                         |
| 6  | Report Time: 2025/08/11 23:59:59    |                   |             |                  |                  |      |                         |
| 7  | Total Number: 84                    |                   |             |                  |                  |      |                         |
| 8  | Device Name                         | Device IP Address | Call Type   | Call Start Time  | Call End Time    | User | Call Recording File     |
| 9  |                                     |                   | No Answered | 2025/08/11 19:18 | 2025/08/11 19:18 |      | 10.18.36.101_2024073118 |
| 10 |                                     |                   | Answered    | 2025/08/11 19:17 | 2025/08/11 19:17 |      | 10.18.36.101_2024073118 |
| 11 |                                     |                   | No Answered | 2025/08/11 19:15 | 2025/08/11 19:15 |      | k                       |
| 12 |                                     |                   | End         |                  |                  |      |                         |

Figure 4.28 Exported Video Intercom Call Records



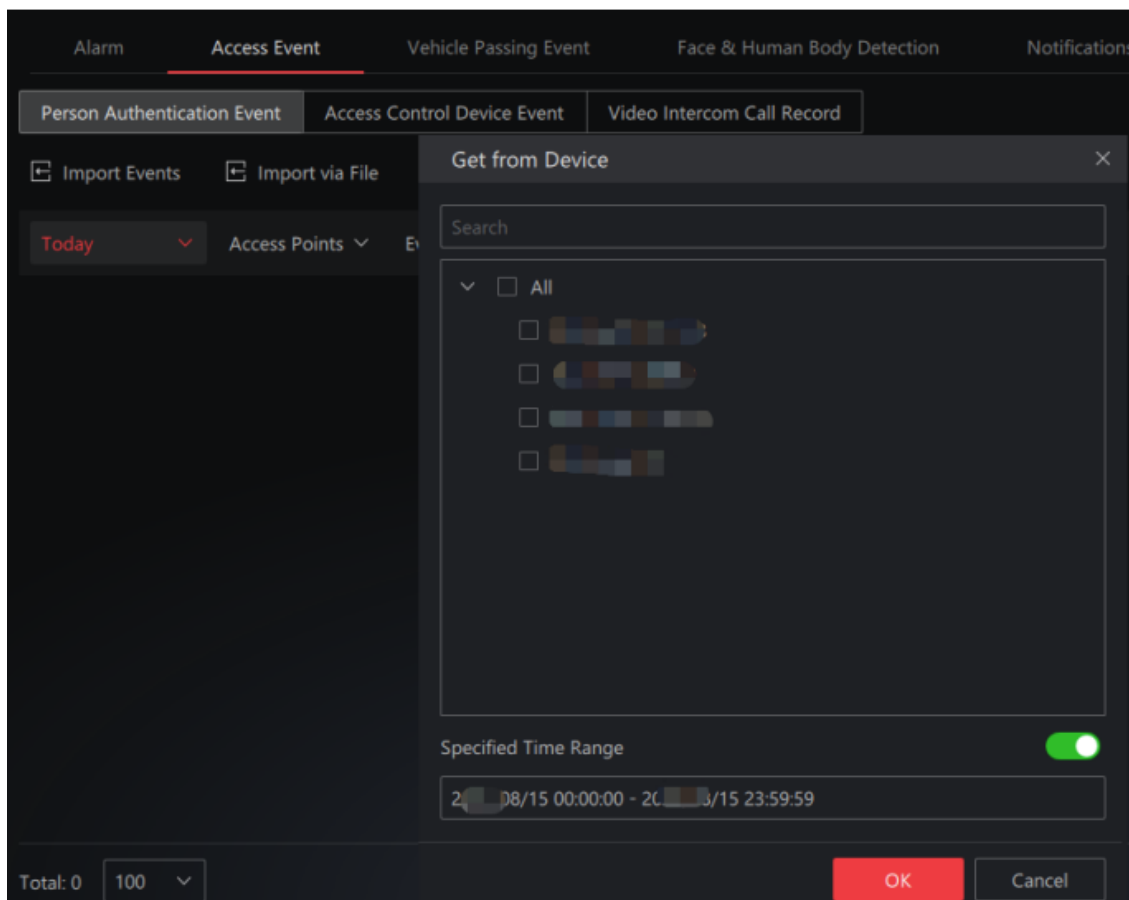


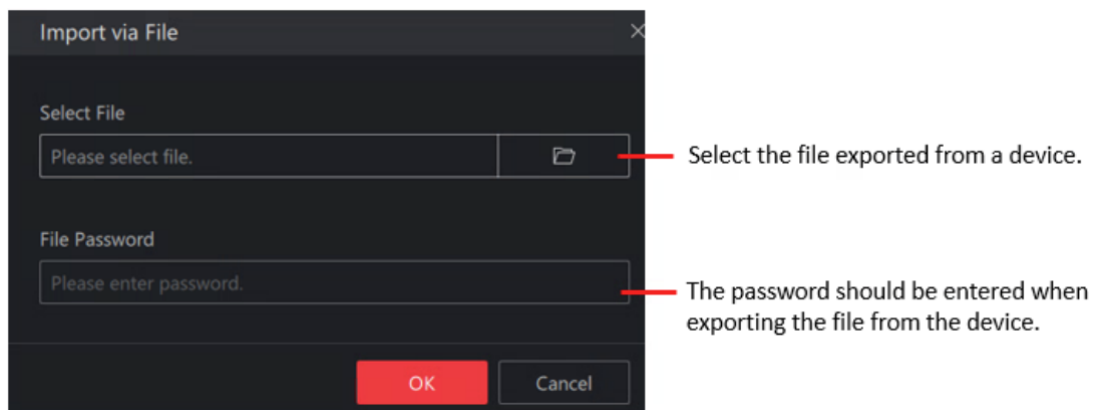
Figure 4.29 Get Events from Device

### 4.7.2 Importing Missing Authentication Logs

If network disruptions cause the client to miss real-time access events, you can manually sync these records from the hardware. Navigate to **System → Access Event → Person Authentication Event**.

- **Network Sync (Online Devices):** Select the target hardware, specify the relevant time frame, and pull the stored events directly over the network.
- **USB Sync (Offline Devices):** For hardware completely disconnected from the network, insert a USB flash drive directly into the device and export the records. Transfer the drive to the client's PC and import the CSV file.

*(Note: The system will only accept encrypted files. Additionally, the imported file must adhere to the strict naming convention: recordlist\_ [Device Serial No.] (e.g., recordlist\_FC2922753).)*



**Figure 4.30 Import Events via File**

### 4.7.3 Data Statistics and Dashboards

The software provides a comprehensive visual overview of your physical security environment, detailing active personnel, registered credentials, configured access levels, and daily event volumes.

#### Daily Analytics

Quickly review today's access metrics, including total successful entries ("Normal Access by Authentication") and rejected attempts ("Access Denied").

#### Interactive Management

The dashboard is fully actionable. Clicking on a statistical metric will route you directly to the corresponding configuration page to make real-time adjustments.

#### Reporting

Right-click on any statistical widget to open it in a dedicated viewing window, refresh the data feed, or export the visual report as a PDF document.

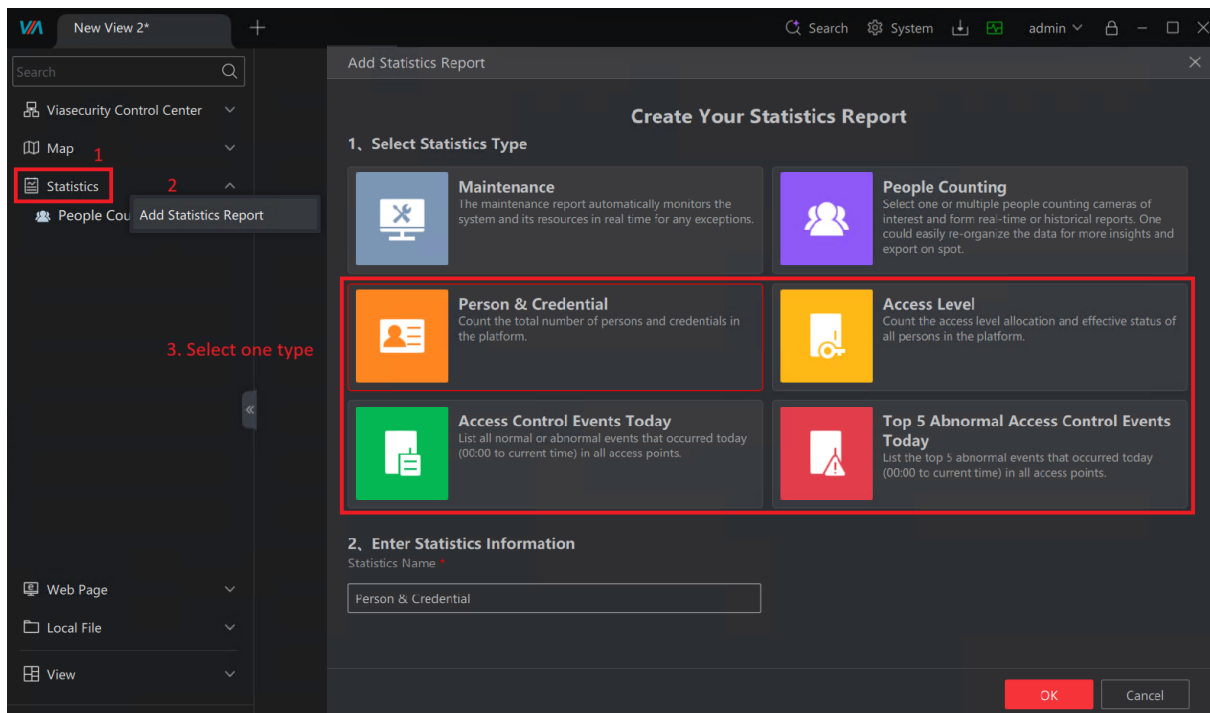


Figure 4.31 Add Statistics Report

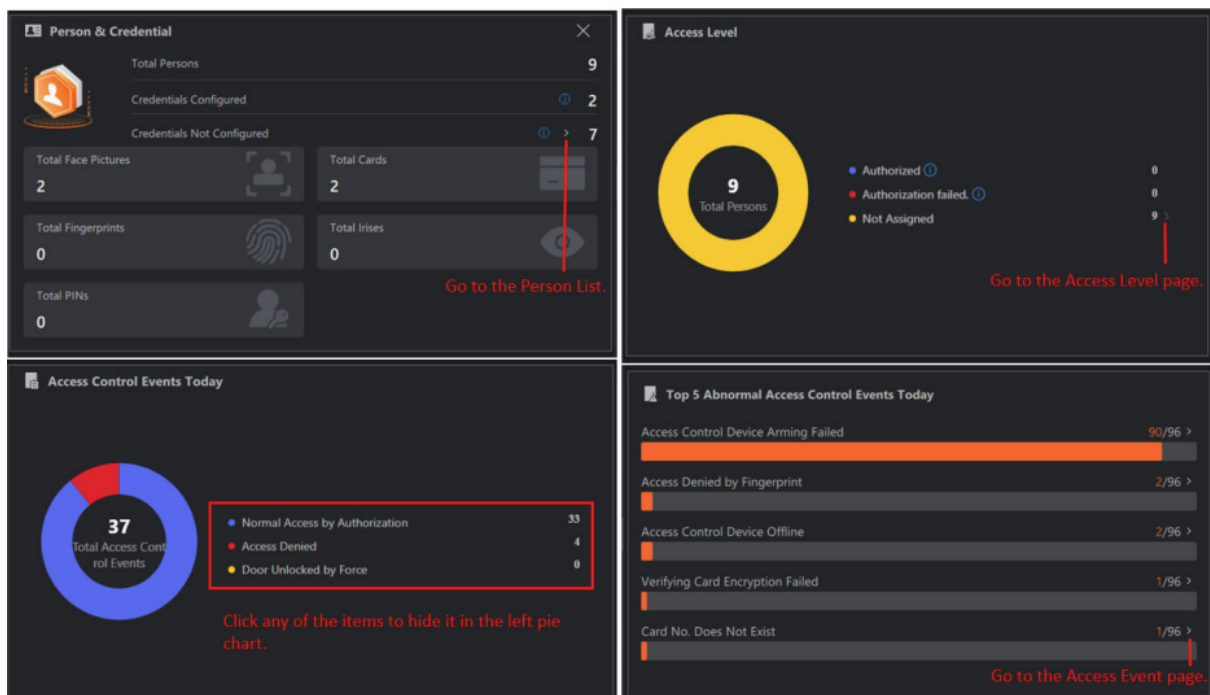


Figure 4.32 Statistics

# Chapter 5 Storage Management

The Viasecurity Control Center provides a centralized server-based storage mechanism for archiving video streams, captured images, and related files. This module allows administrators to allocate specific disk capacities, establish camera recording schedules, and define strict retention periods for system data, including logs and events.

## Video

Archives continuous time-based and event-triggered camera footage according to the assigned schedules.

## Picture and Files

Stores manual snapshots, alarm-linked pictures, and audio files generated by video intercoms

To configure these parameters, click **System → System Configuration → Storage → System Storage / Data Retention Time** in the upper-right corner of the Desktop.

*(Note: First-time users can activate a 30-day trial license that supports video storage for up to 4 channels. If you apply for a formal license while a trial is active, the system will retain the trial features until the original 30-day period expires.)*

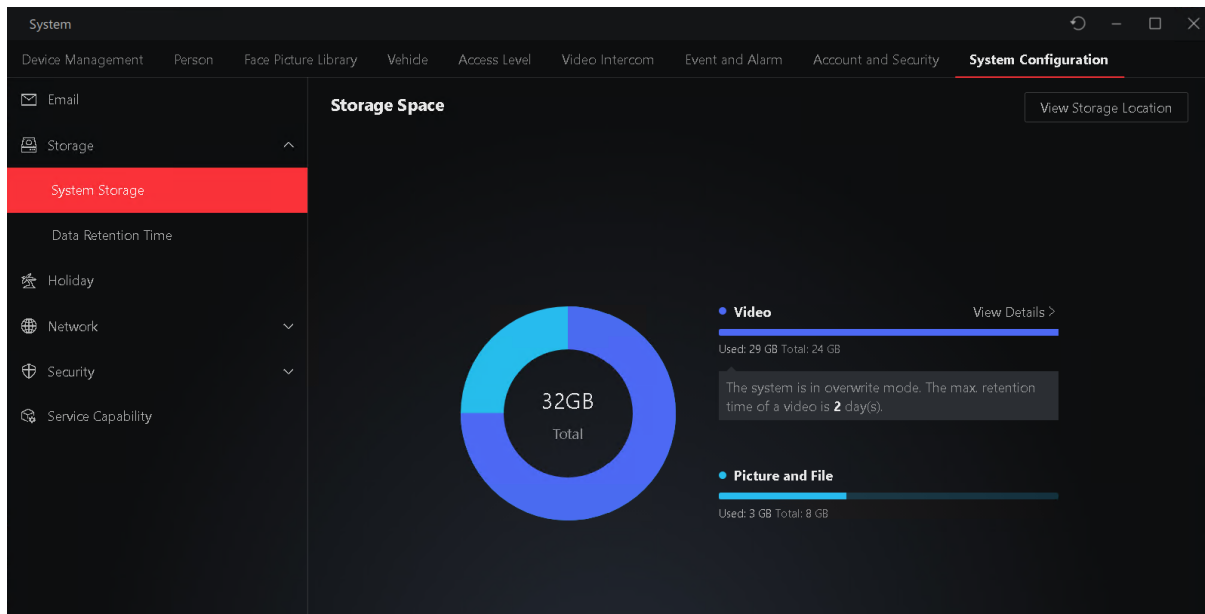


Figure 5.1 Storage Configuration

## 5.1 Preparations

Before initializing storage locations, ensure the following system prerequisites are met:

- The video storage functionality is only accessible after activating either a trial license or a formal purchased license.
- You must add the system storage process to your server's firewall allowlist. Failing to whitelist this process will block required network ports and cause connection timeouts or rejections. If the firewall blocks the storage service, an exception warning will appear in the Notifications pane on the Main Panel.

## 5.2 Storage Location and Capacity Allocation

This section outlines how to define where your data is saved and how to partition the available disk space between video archives and static media (pictures and files).

### Defining the Storage Path

To manage your storage drives, click **View Storage Location** in the top-right corner of the interface.

- The system automatically prioritizes the disk with the highest available capacity. Circulars overwrite is enabled by default, ensuring continuous operation by automatically replacing the oldest files when the drive becomes full.
- Click the add icon to initialize additional storage disks. Note that dynamic disks and non-NTFS formatted drives are strictly prohibited.

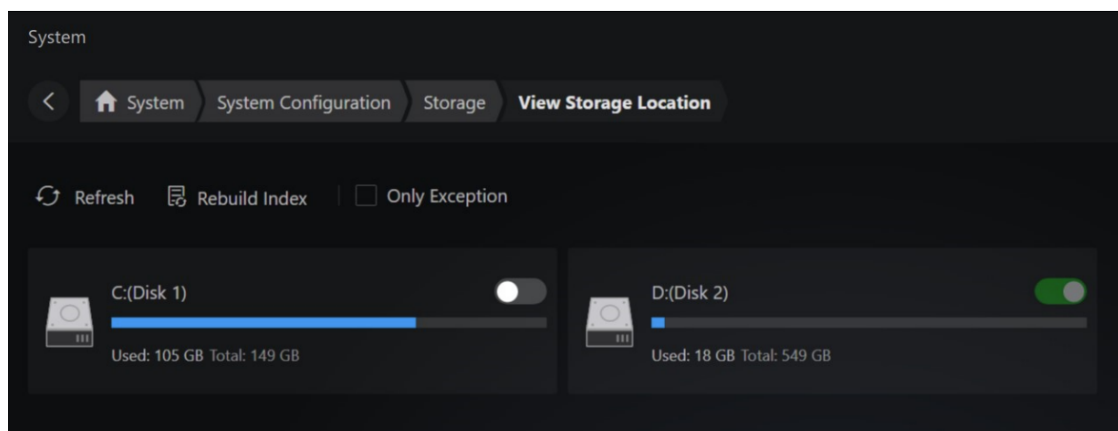


Figure 5.2 Storage Location

## Disk Maintenance & Replacement Guidelines

Manually deleting files directly from the disk or taking the drive offline will permanently destroy critical recordings. The system will generate an alert if this occurs.

When swapping a drive, always back up your existing data first. Ensure the replacement drive capacity is equal to or greater than the old one.

**Replacement Steps:** First, disable the active logical disk and clear its associated files. Next, create a new drive letter specifically for the storage location and verify its operational status. Do not modify the drive letter in the operating system, as it may cause anomalies.

## Configure Storage Space

You must divide your total storage pool between video streams and other media formats (like pictures and audio).

- Click **Configure Storage Space** in the top-right menu.
- Drag  on the pie chart to define the distribution ratio. Or manually enter a numerical value for one category, and the system will automatically calculate the balance for the other.

## 5.3 Storage Schedule Configuration

You can establish recording schedules for individual cameras or apply settings to multiple devices simultaneously. Navigate to the setup by clicking **View Details** to access the **Video Storage Details** page. Click **Add** to create a new recording schedule. Existing schedules can be modified directly within the camera list. Before proceeding, always verify that your system has adequate storage space available.

### Recording Modes and Stream Configuration

#### Schedule Type

Choose to apply a predefined schedule template or construct a custom timeline. You must decide between continuous scheduled recording over a set time duration or event-triggered recording that activates only during an alarm.

## Stream Selection

Select Main Stream, Sub-Stream, or Dual-Stream based on your requirements for playback clarity and power consumption. When utilizing the Sub-Stream, you can enable **Use Main Stream to Record Event Triggered Video**. This automatically captures high-resolution video when an event occurs, and the system will prioritize this main stream footage during event playback.

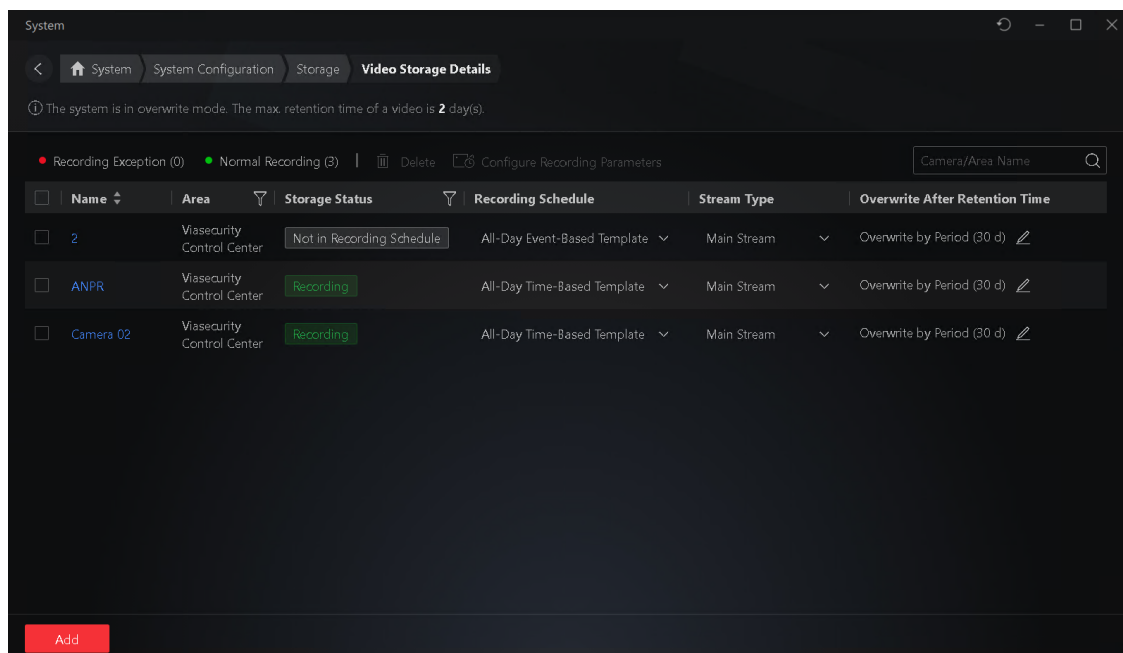


Figure 5.3 Storage Schedule

## Data Retention and Overwrite Policies

### Retention Time

Enable **Overwrite After Retention Time** to ensure videos are automatically deleted once they exceed your defined retention period. If you leave this disabled, the system falls back to a standard first-in, first-out method, overwriting the oldest stored videos only when disk space is depleted.

### Local Device Migration

If you migrate a camera from an active local schedule (where the storage location was set to Local Device) over to System Storage, the system automatically enables the retention overwrite feature and applies for a default 30-day retention period.

## Capacity Planning

The system analyzes global storage space during configuration; ensures you set appropriate retention times. Defining excessively long retention periods for one camera may compromise the storage capacity needed by other devices on the network.

## Network and Security Enhancements

### Auto Copy-Back

Enable this fail-safe to temporarily cache video data on the device if the network connection drops. Once connectivity is restored, the cached video is automatically transported to the primary storage device.

### Streaming Server Routing

Selecting a designated streaming server optimizes and saves network bandwidth.

### Batch Configuration Instructions

To edit parameters for multiple cameras at once, select the populated cameras from the list and click **Configure Recording Parameters**.

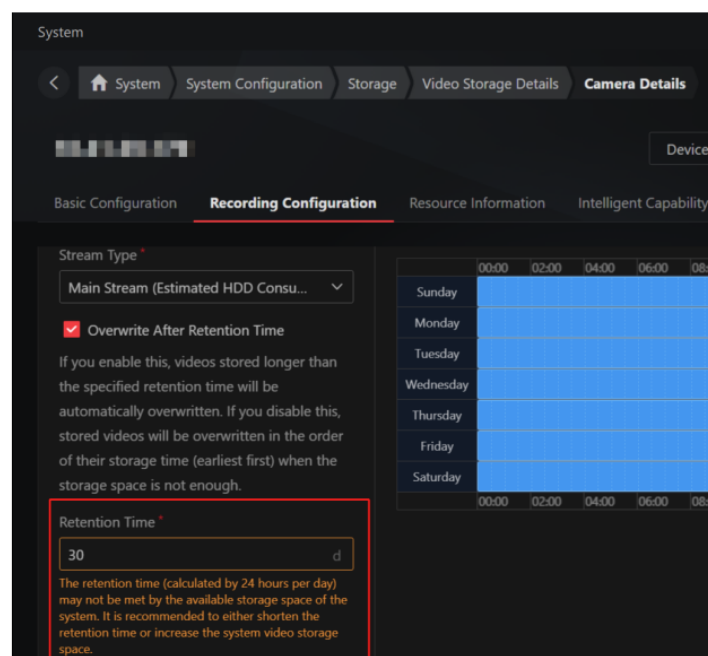


Figure 5.4 Recording Configuration for a Camera

## 5.4 Video Playback and VCA Search



The Viasecurity Control Center facilitates seamless playback of all footage housed within the system of storage. Furthermore, operators can utilize the Video Content Analysis (VCA) functionality to efficiently locate specific events. The system permits targeted filtering by isolating human subjects, vehicular traffic, or a combination of both.

For comprehensive instructions, kindly refer to the chapter "Smart Search / VCA".

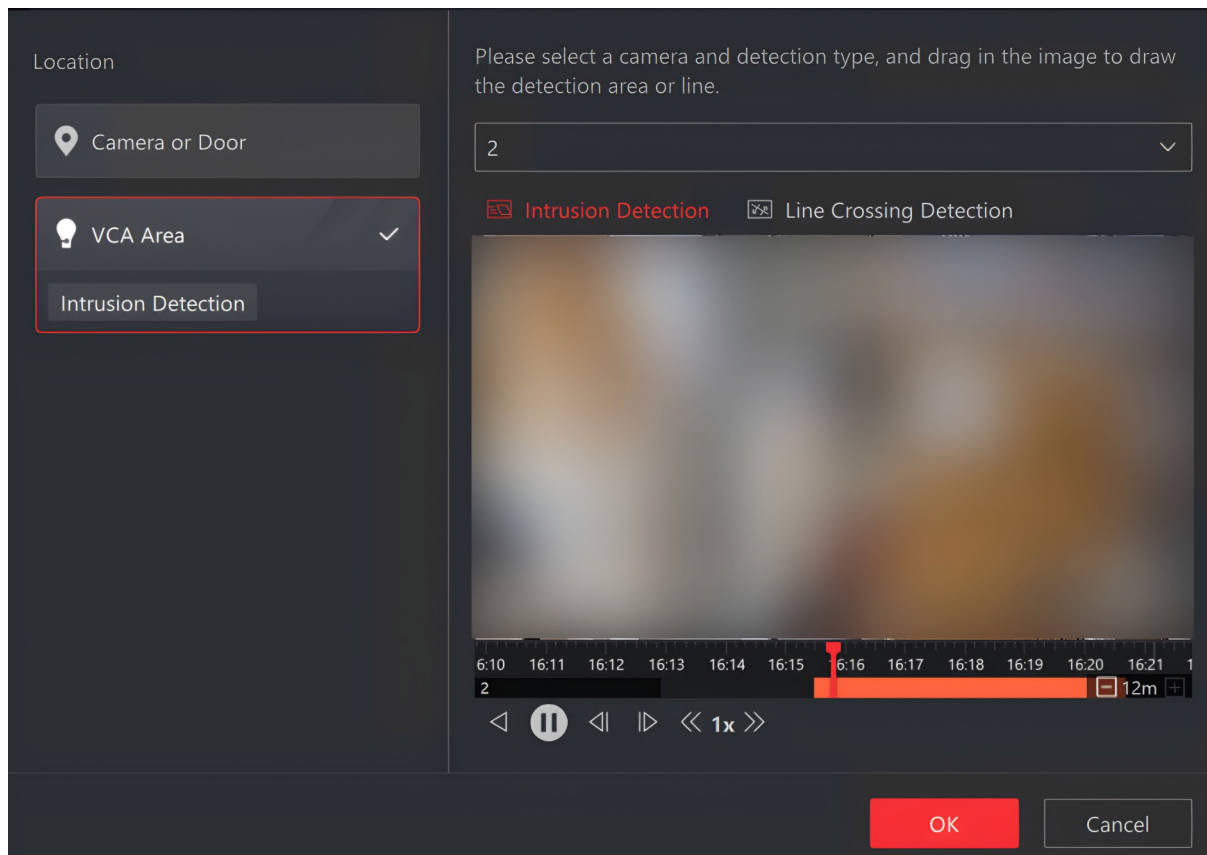


Figure 5.6 VCA Search

## 5.5 Data Retention Lifecycle

To optimize server capacity, administrators are encouraged to establish automated deletion schedules for historical records. Once a designated retention limit is reached, the system will permanently purge the corresponding video footage, access control logs, and general system data.

### Configuration Steps:

1. Navigate to **Storage** → **Data Retention Time**.
2. Specify the desired storage duration for each respective data category

## 5.6 Advanced Storage Management

This section outlines specialized administrative tools designed to configure network interfaces, resolve database anomalies, and monitor overall system health.

### 5.6.1 Network Interface Controller (NIC) Assignment

To ensure optimal data flow, the system storage service may be bound to a dedicated NIC. Administrators possess the flexibility to assign a discrete network interface exclusively for system storage or share a single NIC with the central SYS service. During WAN deployments, the storage and SYS services can either share an identical IP address or operate on distinct IP addresses.

### 5.6.2 Rebuild Index

In the event of database corruption, storage exceptions, or diminished search responsiveness, rebuilding the system index is highly recommended to restore optimal query performance.

- **Crucial Warning:** Kindly ensure the system is not shut down and remains fully operational throughout this procedure to prevent further anomalies.

#### Configuration Steps:

1. Navigate to **System Storage → View Storage Location**.
2. Select **Rebuild Index**.

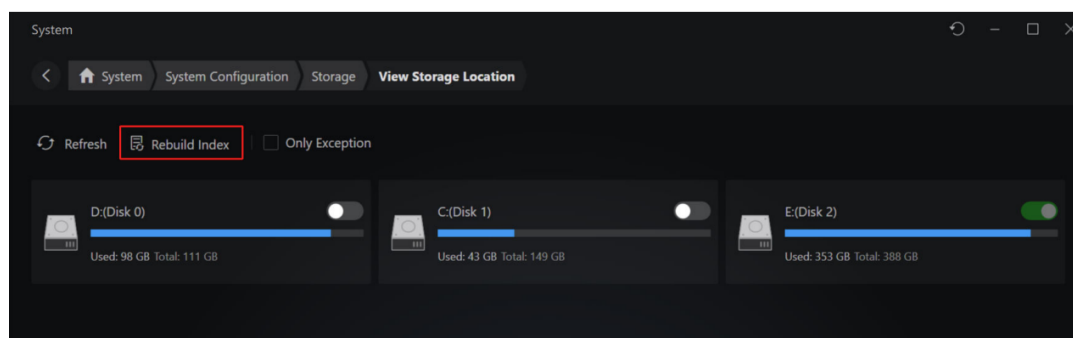


Figure 5.7 Rebuild Index

### 5.6.3 Maintenance

The Viasecurity Control Center offers comprehensive diagnostic oversight for storage infrastructure. By accessing the Maintenance Report interface, administrators can review real-time statistical data regarding the Recording Server NIC throughput, physical disk health, active storage paths, and the overall video repository status.

*(Note: For detailed reporting capabilities, please review the [11.1 Generate and Display Maintenance Report section](#).)*

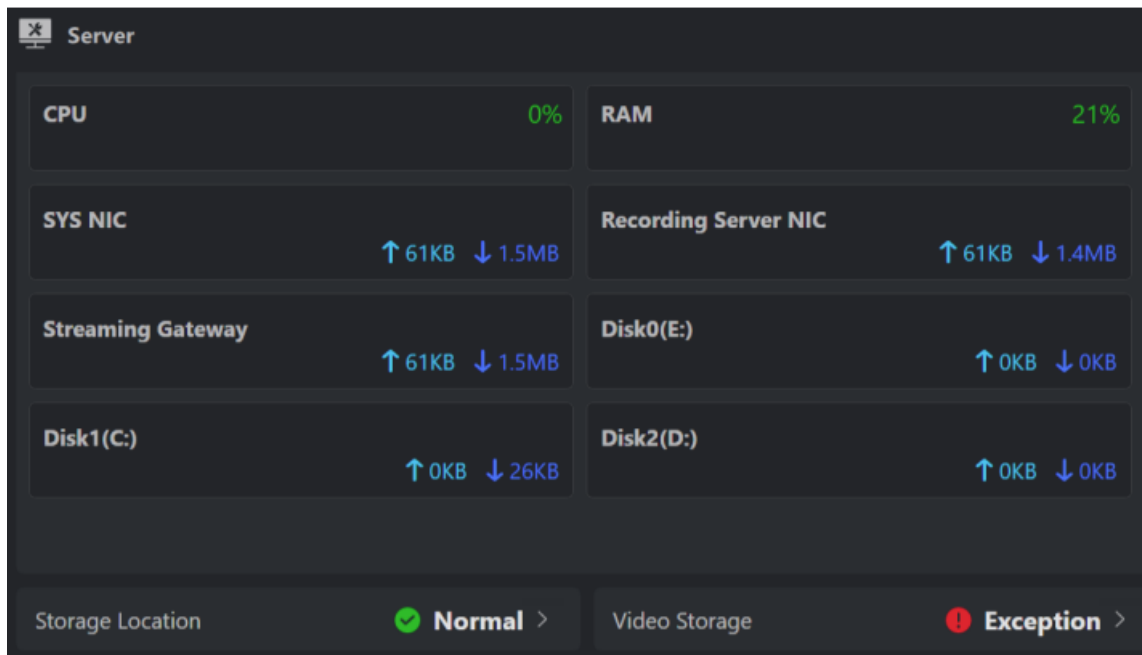


Figure 5.8 Server Statistics

# Chapter 6 Viasecurity Control Center Monitoring Interface

This chapter provides a comprehensive overview of the main monitoring and control panel, detailing how to navigate the interface, manage video layouts, and utilize real-time analytics.

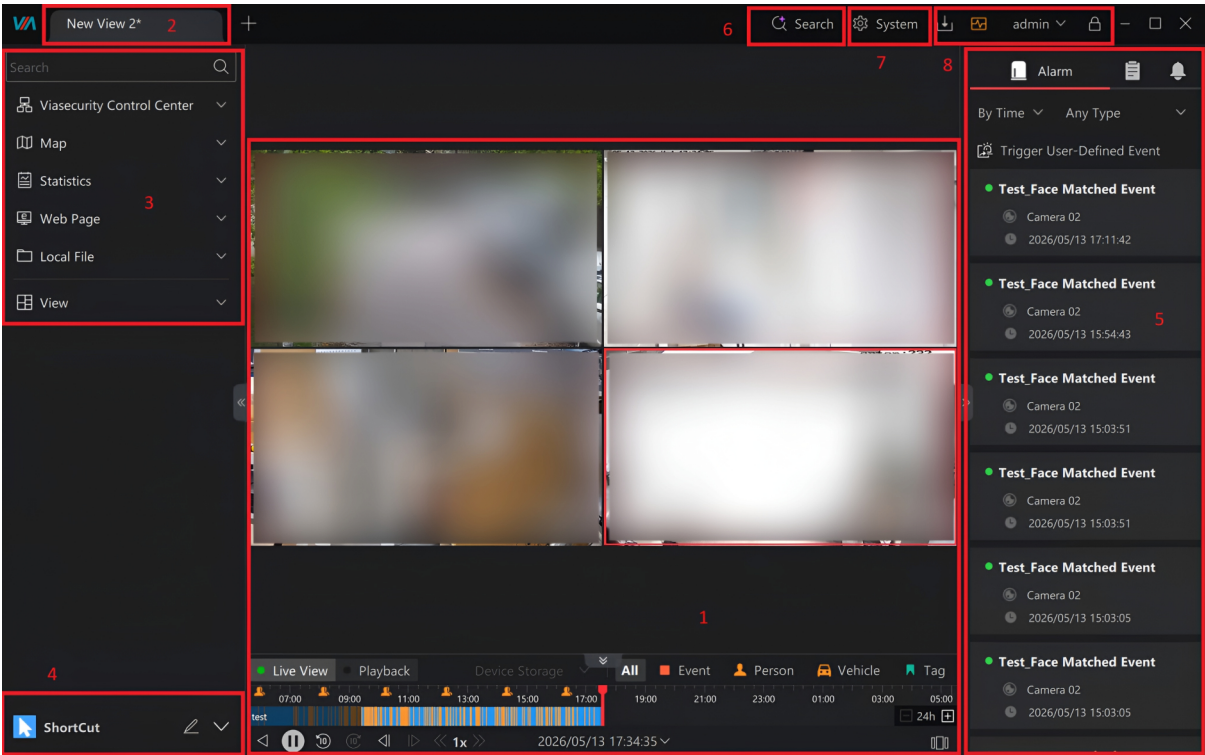


Figure 6.1 Main Panel for Monitoring and Control

Table 6.1 Main Panel Introduction

| No. | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | <p>The Viewing Grid is the central workspace for rendering live video, maps, local media, web pages, and statistical reports.</p> <p><b>Populating the Grid</b><br/> Drag and drop resources directly from your local PC or the Resource Browser into the grid cells. Local media includes recorded videos and captured images.</p> <p><b>Window Management</b><br/> Rearrange your workspace by dragging views up or down. To detach a view, right-click it and select <b>Open in New Window</b>.</p> <p><b>Grid Context Menu</b><br/> Right-click any blank area within the grid to access advanced display controls:</p> <ul style="list-style-type: none"> <li>• <b>Layout Management:</b> Save the current layout as a new view, clear all active windows, or maximize the currently selected image.</li> <li>• <b>Stream Configuration:</b> Apply global stream settings across the grid.</li> <li>• <b>View Scale:</b> Determine how video fits within the cell. Select <b>Full Screen</b> to stretch the image to fill the window, or <b>Original Resolution</b> to maintain the true video size (which may result in black borders if it does not match the window dimensions).</li> <li>• <b>Decoding Mode:</b> Optimize playback performance. Select <b>Hardware</b> decoding to utilize your system's GPU, or <b>Software</b> decoding to rely on the CPU, depending on your workstation's hardware capabilities.</li> </ul> |
| 2   | <p>Drag a view upwards or downwards, or right-click a view and click <b>Open in New Window</b> to open the current view in a new window.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 3   | <p>Located on the left panel, this directory organizes your system's hierarchy, including cameras, areas, web pages, and saved views.</p> <p><b>Navigation</b><br/> Double-click any resource to instantly display it in the Viewing Grid.</p> <p><b>Management</b><br/> Right-click within the directory to add new resources, maps, or view groups.</p> <p><b>Quick Filtering</b><br/> To isolate specific hardware, right-click an area and select <b>Go to Device Management</b>. This will automatically filter the device list to show only the hardware assigned to that location.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 4   | <p>Customize your navigation for maximum efficiency.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"><li>• Click the  main menu icon to reveal all client modules.</li><li>• Click the add icon  next to frequently used modules to pin them to your <b>Shortcut</b> bar.</li><li>• Drag and drop the pinned shortcut icons to rearrange their sequence.</li></ul> |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5 | <p>The right-side panel provides immediate visibility into system activity, automated tracking, and active alarms.</p> <p><b>Alarm Tab</b><br/>Monitors up to 100 live alarms. You can sort the list by priority or timestamp, and filter by event type. Hover over an alarm for text details or drag it into the Viewing Grid to play the associated video. Right-click an alarm to acknowledge it, export data, or adjust settings. Use the <b>Configure</b> button to establish new alarm rules.</p> <p><b>Event Tab</b><br/>Displays configured system events for either the "current view" or "all resources." Similar to alarms, you can hover for details or drag for video playback. Right-click options vary depending on the specific event type.</p> <p><b>Notification Tab</b><br/>Logs general system operational statuses and software notifications.</p> <p><b>VCA / Smart Search</b><br/>Displays results from Video Content Analysis. Filter results by time and click on any thumbnail to review the exact moment in the video.</p> <p><b>Object Search / TargetTrace</b><br/>Tracks specific subjects across the network. Filter by time and similarity percentage to cross-reference detected objects with captured database pictures.</p> |
| 6 | <p>The dedicated portal for querying historical data, such as past alarms, person access logs, and vehicle transit records.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 7 | <p>The central hub for software administration. Use this section to add devices, manage user access levels, build face picture libraries, and establish global security parameters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 8 | <ul style="list-style-type: none"> <li>● : Enter the Download Center.</li> <li>● : View the performance of the PC on which the client is installed.</li> <li>● : View the information of the login user, manage Licenses, back up data, change password, etc.</li> <li>● : Lock the client.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

# Chapter 7 Search

The Viasecurity Control Center features a comprehensive investigation module designed to retrieve a wide array of system records and events. By navigating to the top of the desktop interface and clicking **Search**, administrators can easily locate critical data, including alarms, access control logs, ANPR (Automatic Number Plate Recognition) records, facial and human body captures, system notifications, and operational logs. Furthermore, the platform incorporates advanced Smart Query capabilities to precisely cross-reference video feeds with specific person, vehicle, and Video Content Analysis (VCA) parameters.

## 7.1 Search for Detected Vehicles or Persons by Cameras/Doors

This module facilitates the retrieval of video archives and event data associated with specific system endpoints, such as cameras or access-controlled doors.

### Cameras

Access standard video recordings, vehicle transit logs, captured facial snapshots, and metadata tags generated during playback or via alarm linkages.

### Doors

Retrieve synchronized video feeds, facial detection assets, and comprehensive credential/card authentication records.

### Search for Vehicles by Cameras



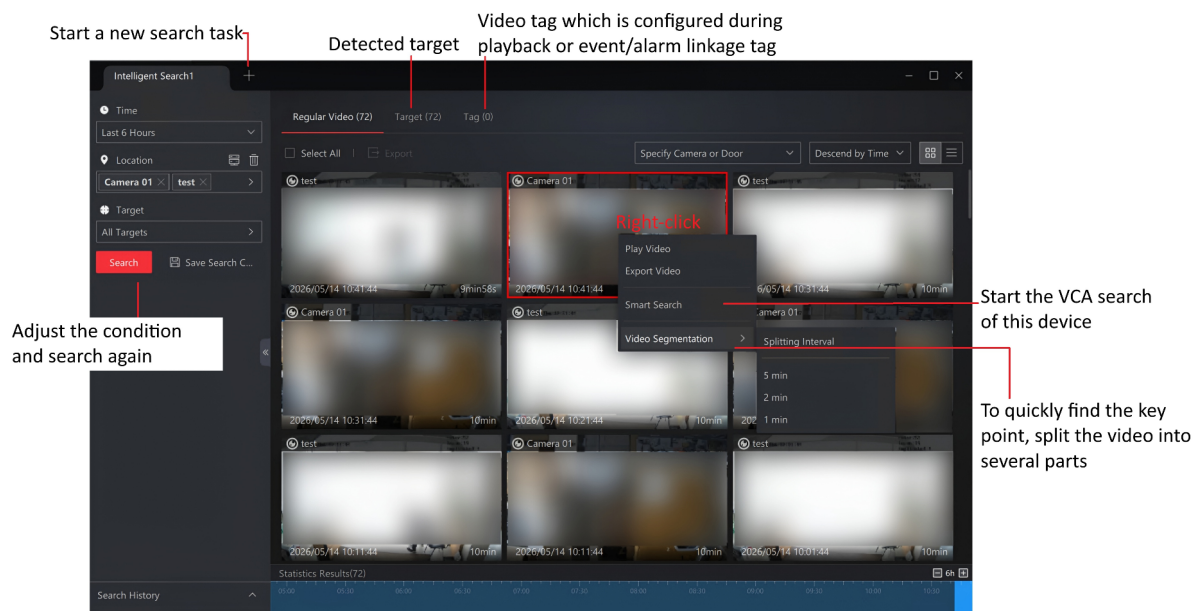


Figure 7.1 Result of Searched Videos

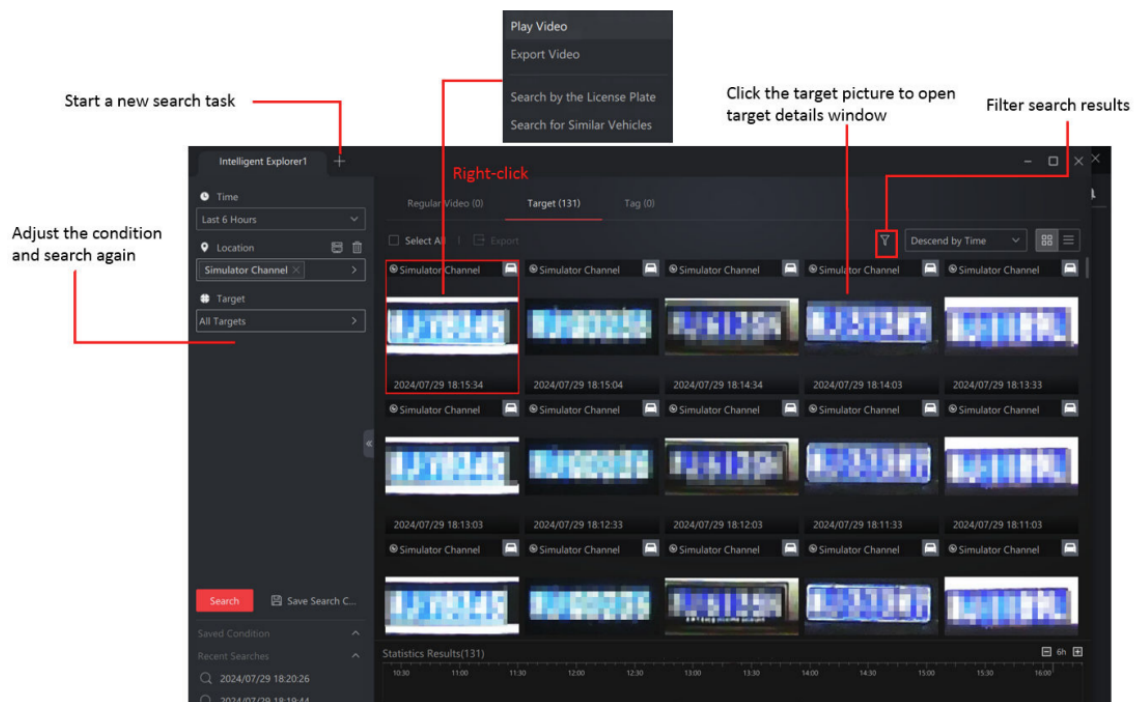


Figure 7.2 Result of Searched Vehicles

Figure

## Search for Persons by Cameras

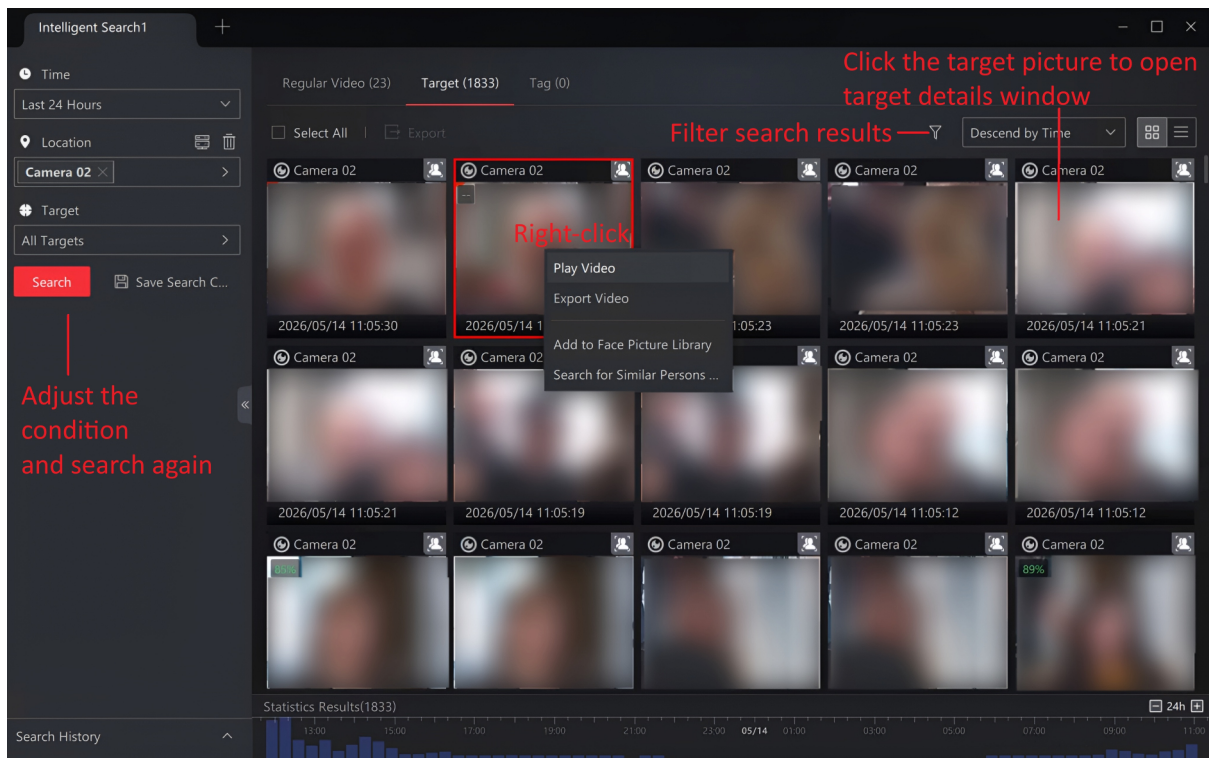


Figure 7.3 Search for Persons by Cameras

## Search for Persons by Doors

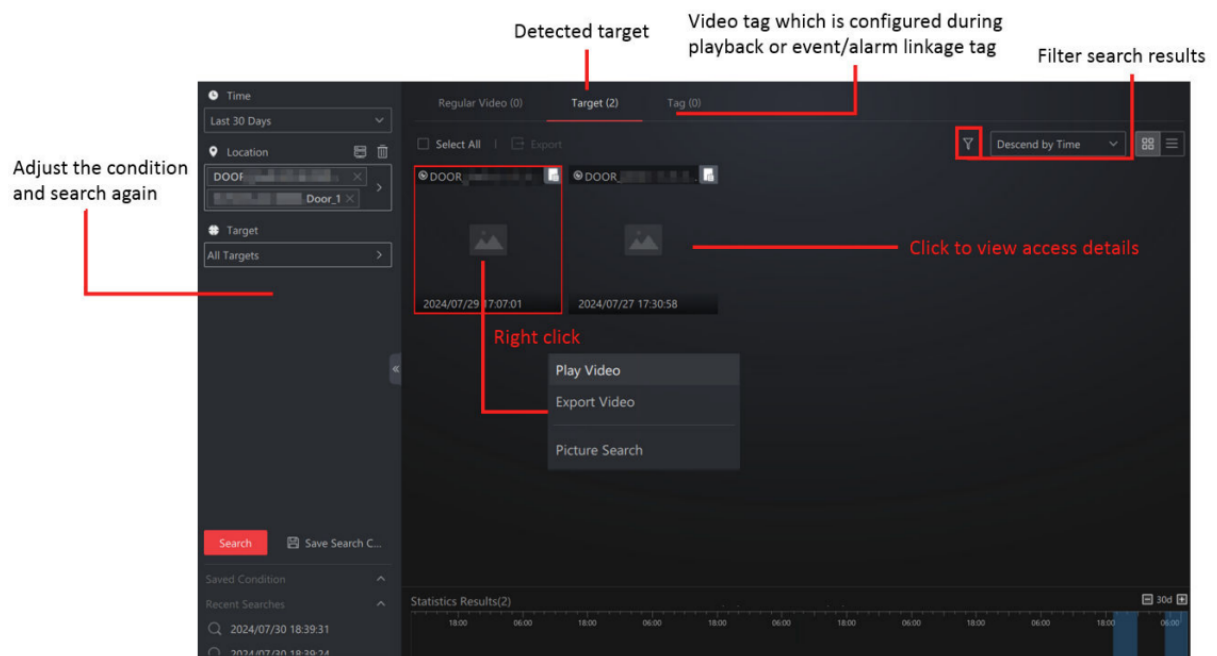


Figure 7.4 Search for Persons by Doors

## Reviewing Results

To examine a specific record, double-click or right-click the file to initiate the playback interface. Operators can adjust playback velocity or navigate directly to the detailed resource page for further analysis.

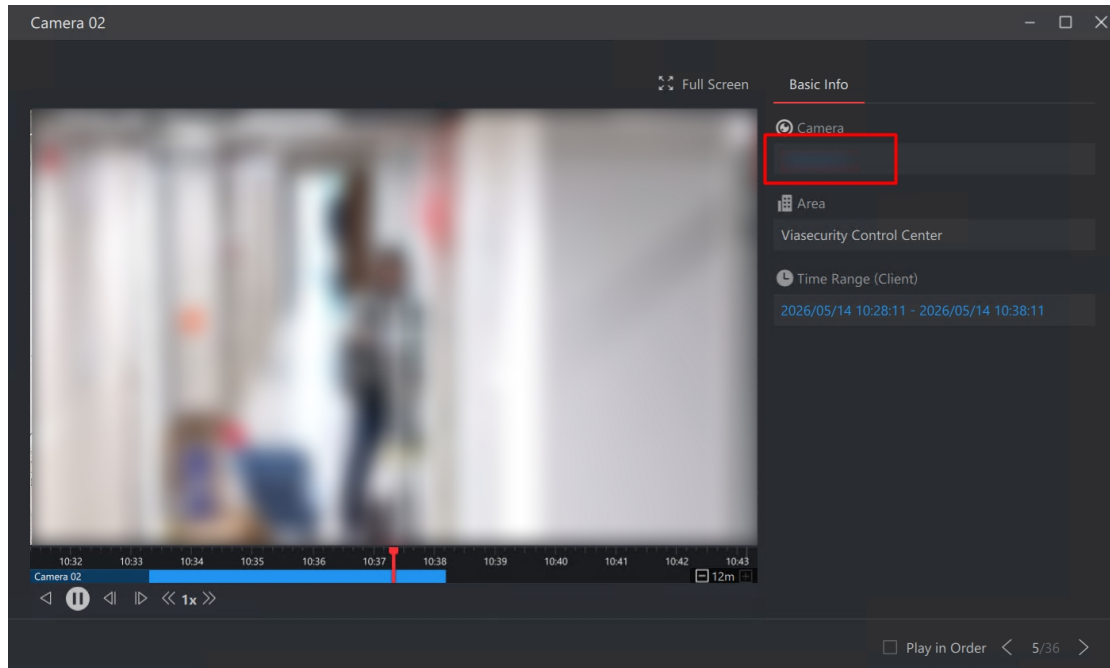


Figure 7.5 Video Playback

## 7.2 Search for Detected Persons or Vehicles in VCA Areas

Use this feature to isolate targets (persons or vehicles) that have triggered certain video content analysis (VCA) rules. The system specifically filters for **Intrusion Detection** and **Line Crossing Detection** events.

*(Note: Ensure that VCA functions are enabled on the relevant hardware prior to initiating a search.)*

### Operational Steps:

1. Navigate to the **Intelligent Search** interface and define the investigation timeframe.
2. Set the **Location** parameter to **the VCA Area**.
3. Designate the target **Camera** for the query.
4. Select the desired behavior (**Intrusion Detection** or **Line Crossing Detection**) and interactively draw the detection zone or line directly on the video preview.
5. Execute the **Search** command.

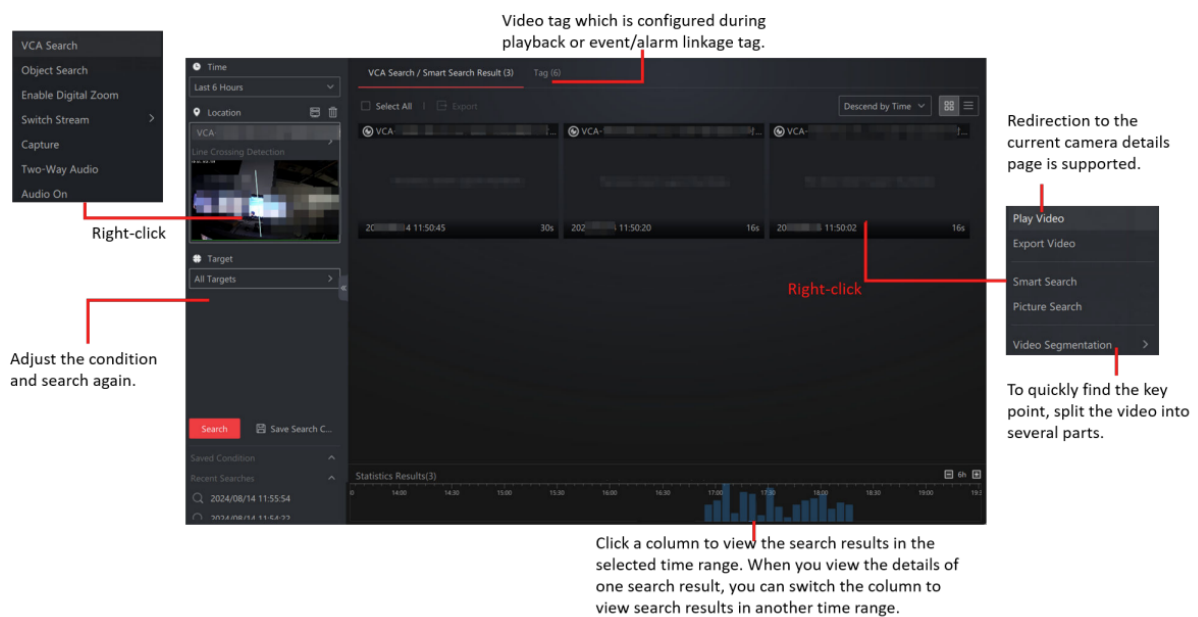


Figure 7.6 VCA Search

## 7.3 Search for Detected Persons/Vehicles by Features

On the Intelligent Search page, set the time and target features for search.

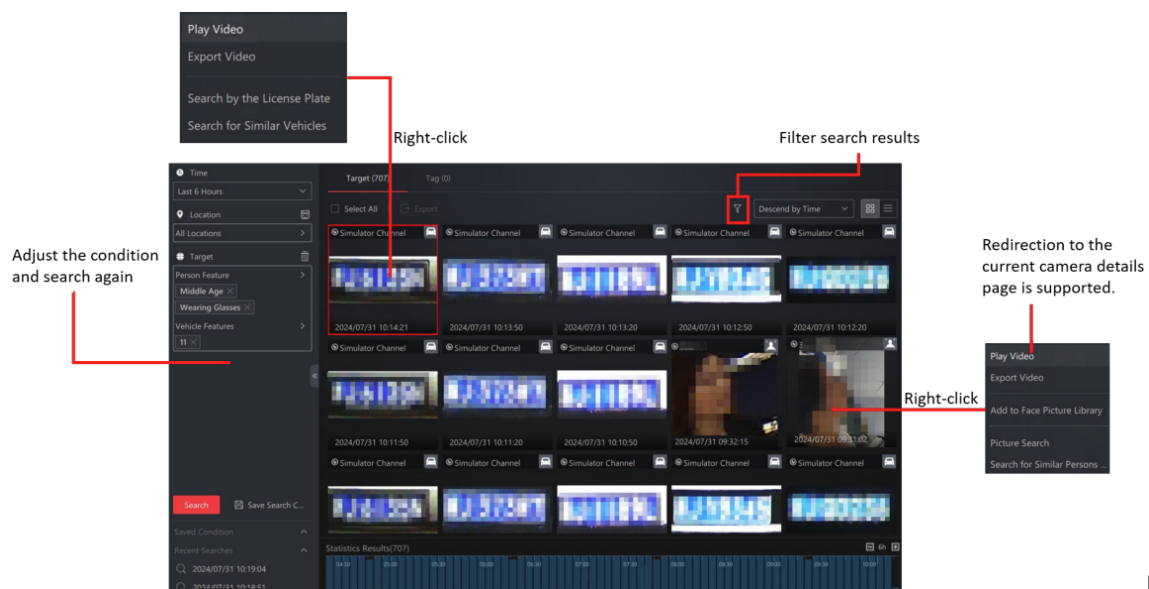


Figure 7.7 Search for Persons/Vehicles by Features

# Chapter 8 Event and Alarm Management

The **Event and Alarm Management** module serves as the centralized interface for administering system triggers, monitoring real-time notifications, and performing forensic data exports. Within this section, operators can define sophisticated alarm protocols, manage event subscriptions, and review historical incident logs.

Access these settings via: **System** → **Event and Alarm**.

## 8.1 Supported Triggering Events

To identify the specific triggers available for alert configuration, follow these steps:

1. Navigate to **Alarm Configuration** and select **Add Alarm**.
2. Consult the **Triggering Event** dropdown menu to view the full catalog of compatible system signals.

### Alarms of Video

Table 8.1 Video

| Category             | Specific Event               |
|----------------------|------------------------------|
| VCA Event            | Fast Moving                  |
|                      | Intrusion                    |
|                      | Line Crossing                |
|                      | Motion Detection             |
|                      | Object Removal               |
|                      | Object Thrown from building  |
|                      | Region Entrance              |
|                      | Region Exiting               |
|                      | Reverse Entering Alarm       |
|                      | Unattended Baggage           |
| ANPR                 | Vehicle Type Matched Event   |
|                      | Vehicle Matched Event        |
|                      | Vehicle Mismatched Event     |
|                      | No License Plate             |
| People Related Event | Face Matched Event           |
|                      | Face Mismatched Event        |
|                      | Multi-Target-Type Detection  |
|                      | Frequently Appeared Person   |
|                      | Loitering                    |
|                      | Face Detection               |
|                      | Face Capture                 |
|                      | People Queuing-Up Alarm      |
|                      | Waiting Time Detection Alarm |
|                      | People Gathering             |
|                      | People Density               |
| Alarm Input          | Alarm Input Triggered        |

## Alarms of Access Control

Table 8.2 Door

| Category              | Specific Event                                      |
|-----------------------|-----------------------------------------------------|
| Normal Card Swiping   | Access Granted by Card and Fingerprint              |
|                       | Access Granted by Card, Fingerprint, and PIN        |
|                       | Access Granted by Valid Card                        |
|                       | Access Granted by Card and PIN                      |
|                       | Access Granted by Fingerprint                       |
|                       | Access Granted by Fingerprint and PIN               |
|                       | Duress Alarm                                        |
|                       | Access Granted by Face and Fingerprint              |
|                       | Access Granted by Face and PIN                      |
|                       | Access Granted by Face and Card                     |
|                       | Access Granted by Face, PIN, and Fingerprint        |
|                       | Access Granted by Face, Card, and Fingerprint       |
|                       | Access Granted by Face                              |
|                       | Access Granted by Employee ID and Fingerprint       |
|                       | Access Granted by Employee ID, Fingerprint, and PIN |
|                       | Access Granted by Employee ID and Face              |
|                       | Access Granted by Employee ID and PIN               |
|                       | Access Granted via Combined Authentication Modes    |
|                       | Access Granted by PIN                               |
| Abnormal Card Swiping | Verifying Card Encryption Failed                    |

|  |                                                        |
|--|--------------------------------------------------------|
|  | Max. Card Access Failed Attempts                       |
|  | Card No. Expired                                       |
|  | Authentication via Card + PIN Timed Out                |
|  | Access Denied (Door Remained Locked or Inactive)       |
|  | Access Denied (First Person Not Authorized)            |
|  | Access Denied by Card and PIN                          |
|  | Authentication via Card + Fingerprint + PIN Timed Out  |
|  | Access Denied by Card, Fingerprint, and PIN            |
|  | Access Denied by Card and Fingerprint                  |
|  | Authentication via Card + Fingerprint Timed Out        |
|  | No Access Level Assigned                               |
|  | Card No. Does Not Exist                                |
|  | Invalid Time Period                                    |
|  | Fingerprint Does Not Exist                             |
|  | Access Denied by Fingerprint                           |
|  | Access Denied by Fingerprint and PIN                   |
|  | Authentication via Fingerprint + PIN Timed Out         |
|  | Access Denied by Face and Fingerprint                  |
|  | Authentication via Face + Fingerprint Timed Out        |
|  | Access Denied by Face and PIN                          |
|  | Authentication via Face + PIN Timed Out                |
|  | Access Denied by Face and Card                         |
|  | Authentication via Face + Card Timed Out               |
|  | Access Denied by Face, PIN, and Fingerprint            |
|  | Authentication via Face + PIN + Fingerprint Timed Out  |
|  | Access Denied by Face, Card, and Fingerprint           |
|  | Authentication via Face + Card + Fingerprint Timed Out |
|  | Access Denied by Face                                  |



|                                                              |
|--------------------------------------------------------------|
| Face Capture Failed                                          |
| Interlocking Door Not Closed                                 |
| Access Denied by Employee ID and Fingerprint                 |
| Authentication via Employee ID + Fingerprint Timed Out       |
| Access Denied by Employee ID, Fingerprint, and PIN           |
| Authentication via Employee ID + Fingerprint + PIN Timed Out |
| Access Denied by Employee ID and Face                        |
| Authentication via Employee ID + Face Timed Out              |
| Access Denied by Employee ID and PIN                         |
| Authentication via Employee ID + PIN Timed Out               |
| Person Not in Multi-Factor Authentication Group              |
| Person Not in Multi-Factor Authentication Time Period        |
| Combined Authentication Timed Out                            |
| Access Denied by Invalid M1 card                             |
| Verifying CPU Card Encryption Failed                         |
| Access Denied (NFC Card Reading Disabled)                    |
| EM Card Reading Not Enabled                                  |
| M1 Card Reading Not Enabled                                  |
| CPU Card Reading Disabled                                    |
| Authentication Mode Mismatch                                 |
| Lost Card Authenticated                                      |
| Authentication Attempts via Card + PIN Exceeded Limit        |
| Password Mismatch                                            |
| Employee ID Does Not Exist                                   |
| Failed Password Attempts Alarm                               |
| Verifying DESFire Card Encryption Failed                     |
| DESFire Card Recognition Disabled                            |
| Authentication Failed Due to Abnormal Features               |

|                   |                                     |
|-------------------|-------------------------------------|
|                   | Iris Anti-Spoofing Detection Failed |
| Other Door Events | Door Unlocked (Door Lock)           |

|  |                                             |
|--|---------------------------------------------|
|  | Door Locked (Door Lock)                     |
|  | Exit Button Pressed                         |
|  | Exit Button Released                        |
|  | Card Reader Tampering Alarm                 |
|  | Door Abnormally Open (Door Contact)         |
|  | Remote: Unlocked Door                       |
|  | Remote: Locked Door                         |
|  | Doorbell Rang                               |
|  | Remote: Remained Unlocked (Free Access)     |
|  | Remote: Remained Locked (Credential Failed) |
|  | Remaining Unlocked Status Started           |
|  | Remaining Unlocked Status Ended             |
|  | Remaining Locked Status Started             |
|  | Remaining Locked Status Ended               |
|  | First Person in Started                     |
|  | First Person in Ended                       |
|  | First Person Authorization Started          |
|  | First Person Authorization Stopped          |
|  | Door Open (Door Contact)                    |
|  | Door Closed (Door Contact)                  |
|  | Unlocking Timed Out                         |
|  | Face Recognition Terminal Online            |
|  | Face Recognition Terminal Offline           |
|  | Tailgating                                  |
|  | Reverse Passing                             |
|  | Force Access                                |
|  | Climbing Over Barrier                       |
|  | Passing Timed Out                           |

|                                                                                 |
|---------------------------------------------------------------------------------|
| Intrusion                                                                       |
| Access Denied When Free Passing                                                 |
| Barrier Blocked                                                                 |
| Barrier Restored                                                                |
| Multi-Factor Authentication: Access Denied by Super Password                    |
| Multi-Factor Authentication: Access Denied by Remote Authentication             |
| Multi-Factor Authentication: Access Granted                                     |
| Multi-Factor Authentication: Remotely Open Door                                 |
| Multi-Factor Authentication: Super Password Access Granted                      |
| Multi-Factor Authentication: Repeated Authentication                            |
| Multi-Factor Authentication: Timed Out                                          |
| Card Reader Lid Closed                                                          |
| Secure Door Control Unit Lid Opened                                             |
| Enter Dismiss Code                                                              |
| Fire Alarm Relay Triggers Door Remain Open                                      |
| Fire Alarm Relay Recovered and Door Recovered                                   |
| Blocklist Event                                                                 |
| Opening Door via Exit Button Failed When Door Remaining Closed or in Sleep Mode |
| Opening Door by Linkage Failed When Door Remaining Closed or in Sleep Mode      |
| Overstay                                                                        |
| Unlock by Center                                                                |
| Door Not Open                                                                   |
| Door Not Closed                                                                 |
| Secure Door Control Unit Disconnected                                           |
| Secure Door Control Unit Connected                                              |

|  |                  |
|--|------------------|
|  | Motion Detection |
|--|------------------|

**Table 8.3 Access Control Device**

| Category                  | Specific Event                                     |
|---------------------------|----------------------------------------------------|
| Device Security           | Device Tampering Alarm Restored                    |
|                           | Secure Door Control Unit Tampering Alarm           |
| Local Operation on Device | Local: Login Locked                                |
|                           | Local: Login Unlocked                              |
|                           | Local: Login                                       |
|                           | Local: Logout                                      |
|                           | Local: Upgrade                                     |
|                           | NTP Auto Time Synchronization                      |
|                           | Local: Restored Default Parameters                 |
|                           | Edit Network Center Configuration                  |
|                           | Edit GPRS Parameters                               |
|                           | Edit Central Group Configuration                   |
|                           | Import Normal Configuration File                   |
|                           | Export Normal Configuration File                   |
|                           | Import Card Permission Parameters                  |
|                           | Export Card Permission Parameters                  |
|                           | Local: Upgrade Device Firmware via USB Flash Drive |
|                           | Local: Upgrading Failed                            |
| Device Component          | Lane Controller Fire Input Alarm                   |

|                              |                                                    |
|------------------------------|----------------------------------------------------|
| Communication                | Pedestal Temperature Too High                      |
|                              | Communication with Light Board Exception           |
|                              | Indicator Turned Off                               |
|                              | Lane Controller Disconnected                       |
|                              | Lane Controller Connected                          |
|                              | CAN BUS Recovered                                  |
|                              | Lane Controller Fire Input Recovered               |
|                              | Communication with IR Adaptor Recovered            |
|                              | Active Infrared Intrusion Detector Recovered       |
|                              | Extension Module Offline                           |
| Device Disk/HDD              | No Memory Alarm for Unreported Events              |
|                              | No Memory for Unreported and Access Granted Events |
| Device Battery               | AC Power On                                        |
|                              | Battery Voltage Recovered                          |
|                              | Battery Voltage Restored                           |
|                              | Device Power On                                    |
| Device Record Reporting      | Access Control Device Armed                        |
|                              | Video Intercom Device Armed                        |
| Device Network               | Access Control Device Online                       |
|                              | Video Intercom Device Online                       |
| Remote Operation on Platform | Remote: Login                                      |

|  |                                             |
|--|---------------------------------------------|
|  | Remote: Logout                              |
|  | Remote: Arming                              |
|  | Remote: Disarming                           |
|  | Remote: Restart                             |
|  | Remote: Upgrade                             |
|  | Remote: Export Configuration File           |
|  | Remote: Import Configuration File           |
|  | Alarm Output On                             |
|  | Alarm Output Off                            |
|  | Remote: Manual Time Synchronization         |
|  | Remote: Clear Card No.                      |
|  | Remote: Restored Default Parameters         |
|  | Remote: Capture                             |
|  | Remote: Upgrading Failed                    |
|  | Remote: Extension Module Upgraded           |
|  | Remote: Extension Module Upgrading Failed   |
|  | Remote: Fingerprint Module Upgraded         |
|  | Remote: Fingerprint Module Upgrading Failed |
|  | SOS                                         |

**Table 8.4 Alarm Input**

| Specific Event        | Description                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarm Input Triggered | Occurs when an abnormal signal is detected at the device's alarm input (e.g., smoke detector measuring concentration beyond the threshold), activating the alarm. This event indicates the beginning of an alarm condition. |
| Alarm Input Restored  | Occurs when the abnormal signal ceases, and the alarm state returns to normal. This event signifies the end of an alarm condition.                                                                                          |

**Table 8.5 Person**

| Specific Event      |
|---------------------|
| Person Matched      |
| Card Number Matched |

## **Alarms of Maintenance**

**Table 8.6 Service**

| Category                  | Specific Event           |
|---------------------------|--------------------------|
| Streaming Server          | Streaming Server Offline |
| Storage Server            | Storage Exception        |
| System Management Service | CPU Exception            |



|  |                                   |
|--|-----------------------------------|
|  | CPU Warning                       |
|  | RAM Exception                     |
|  | RAM Warning                       |
|  | System Service Abnormally Stopped |

**Table 8.7 Access Control Device**

| Specific Event                               |
|----------------------------------------------|
| Device Tampered                              |
| Lane Controller Tampering Alarm              |
| Secure Door Control Unit Tampering Alarm     |
| Access Control Device Offline                |
| Video Intercom Device Offline                |
| AC Power Off                                 |
| Device Power Off                             |
| Low Storage Battery Voltage                  |
| Battery Voltage Restored                     |
| Low Battery Voltage                          |
| Arming Device failed                         |
| Video Intercom Device Arming Failed          |
| Memory Card Full                             |
| Flash Writing/Reading Exception              |
| Motor or Sensor Exception                    |
| CAN BUS Exception                            |
| Active Infrared Intrusion Detector Exception |
| Communication with IR Adaptor Exception      |
| Indicator Turned On                          |
| Lane Controller Disconnected                 |
| Lane Controller Connected                    |
| Extension Module Offline                     |
| Access Control Device Call Center            |
| Video Intercom Device Call Center            |

**Table 8.8 Camera**

| Specific Event                     |
|------------------------------------|
| Camera Online                      |
| Camera Offline                     |
| Channel Armed                      |
| Channel Arming Failed              |
| Defocus Detection                  |
| Video Loss                         |
| Camera Recording Exception         |
| Camera Recording Recovered         |
| Image Exception Event              |
| Video Tampering Detection          |
| Scene Change Detection             |
| Vibration Detection Alarm          |
| Audio Exception Detection          |
| Video Stream Transcoding Exception |

**Table 8.9 Encoding Device**

| Specific Event       |
|----------------------|
| Device Reconnected   |
| Device Offline       |
| HDD Full             |
| HDD High Temperature |
| HDD Impact Detection |
| HDD Server Failure   |
| R/W HDD Failure      |
| Array Exception      |
| Illegal Login        |
| Device Armed         |
| Arming Device Failed |

## **Alarms of Custom Event**

**Table 8.10 Custom Event**

| Category           | Specific Event     |
|--------------------|--------------------|
| User-Defined Event | User-Defined Event |
| Generic Event      | Generic Event      |

## 8.2 Event Subscription

In the Viasecurity Control Center, subscribing to events ensures that they are actively logged, searchable within the system, and visible on the main monitoring panel.

### Key Considerations:

- You will still receive triggered alarms even if you are not subscribed to the underlying event.
- If an event is unsubscribed, it will not appear in the Search module and will not be pushed to the main monitoring panel.

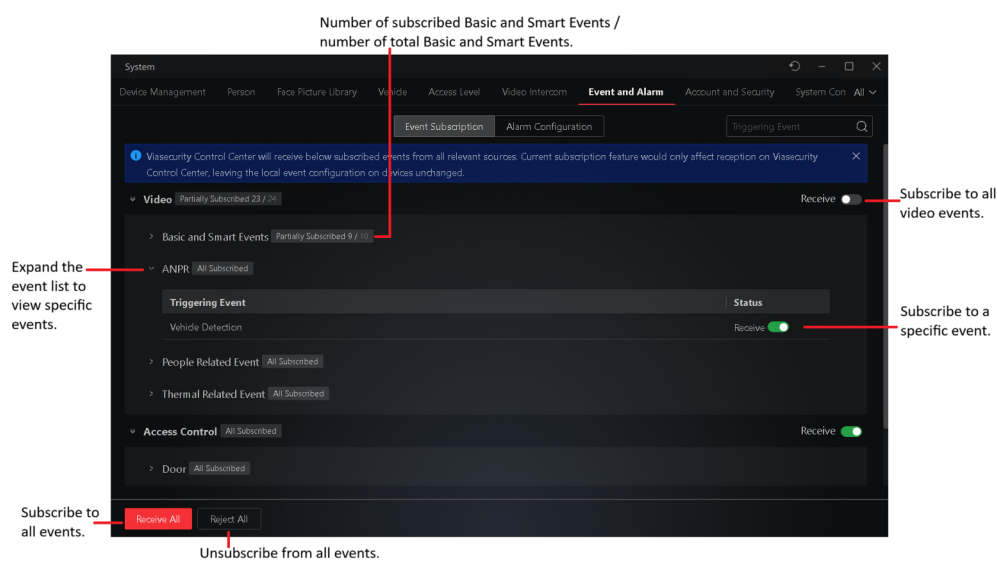


Figure 8.1 Event Subscription

### Subscription Management:

- **Targeted Selection:** Expand the event categories to manually toggle subscriptions for specific events.
- **Category Selection:** You can subscribe to entire groups of events at once (e.g., enabling all video-related events).

## 8.3 Add an Alarm

The platform allows you to create customized alarm rules, linking specific system detections to automated responses and notifications.

### Configuration Steps:

1. Navigate to the **Event and Alarm** module.
2. Go to **Alarm Configuration** and click the **Add Alarm** button.
3. Choose your desired triggering event and select the specific hardware source(s) that will monitor it.
4. Assign an alarm priority level, then click **Next**.
5. Define the active receiving schedule for this alarm, then click **Next**. *(Note: If you need to account for holidays, configure those under the Holiday settings).*
6. Select the system for users or groups who should receive this alarm notification, then click **Next**.
7. Assign automatic system responses (e.g., start recording, capture image, pop-up window) to be executed when an alarm is triggered.
8. Click **Complete** to save and activate the alarm rule.

## 8.4 Supported Linkage Actions

The Viasecurity Control Center platform allows you to configure automated system responses, known as linkage actions, that execute immediately when a specific alarm triggers.

*(Note: If you apply visual actions (Recording, Capture Picture, or Create Tag) to an access control door, the door must have a linked camera. If no camera is linked, the system will allow the configuration, but the action will fail to execute.)*

### Video & Image Linkage

#### Trigger Video Recording

Command cameras to record the alarm event. You can utilize the **Source Camera** (the camera that detected the event) and define its storage location (Main Storage, Auxiliary Storage, or Not Store), or choose a **Specified Camera** to record from secondary angles.

- Footage begins 3 seconds prior to the event and ends 15 seconds after.
- Files are stored for a minimum of 7 days before adhering to the device's standard overwrite cycle.

#### Capture Picture

Instructs the Source Camera or manually Specified Cameras to take a single snapshot during the event. Only one image is captured per camera.

## Create Tag

Adds searchable bookmarks to the alarm footage.

- "Trigger Recording" must be enabled to use this feature.
- Tags are applied to the 3-second pre-alarm and 15-second post-alarm timeframe. You can write custom text or use system variables (\$Event Name, \$Event Time, or \$Event Source).

## Trigger PTZ Control

Forces selected PTZ cameras to instantly move to a specific Preset, Patrol, or Pattern.

## Hardware & Access Control Linkage

### Link Access Point

Automatically change the physical status of selected doors (e.g., Lock, Unlock, Remain Locked, or Remain Unlocked) to secure an area during an alarm.

### Link Alarm Output

Activate connected physical peripherals, such as external warning speakers.

*(Note: These output devices must be imported into the system before they can be selected here.)*

## System & Operator Notification Linkage

### Trigger Pop-up Window

Pushes an immediate on-screen interface to the operator, displaying critical alarm details alongside live video feeds and instant playback options.

### Trigger Audible Alarm

Broadcasts a synthesized voice alert from the operator's PC to catch their attention.

*Prerequisite: System audio must be active, and the voice engine must be designated as the alarm sound.*

### Send Email

Dispatches an automated email alert detailing the event to specified recipients.

Trigger User-Defined Event

Before adding this linkage action, you should configure alarm(s) for user-defined event(s) first. As the user-defined event(s) cannot be automatically detected, it needs to be manually triggered by clicking **Trigger User-Defined Event** on the notification panel of the main page or added as a linkage action for another alarm.

8.5 Managing Configured Alarms

Once created, alarm rules are activated automatically. You can manage your configured alarms directly from the main list:

- Manually enable or disable alarms. Disabling an alarm prevents it from triggering and halts all associated linkage actions.
- Click directly on an event name to modify its existing parameters.
- Select specific alarms and use the test-trigger function to verify your configuration.

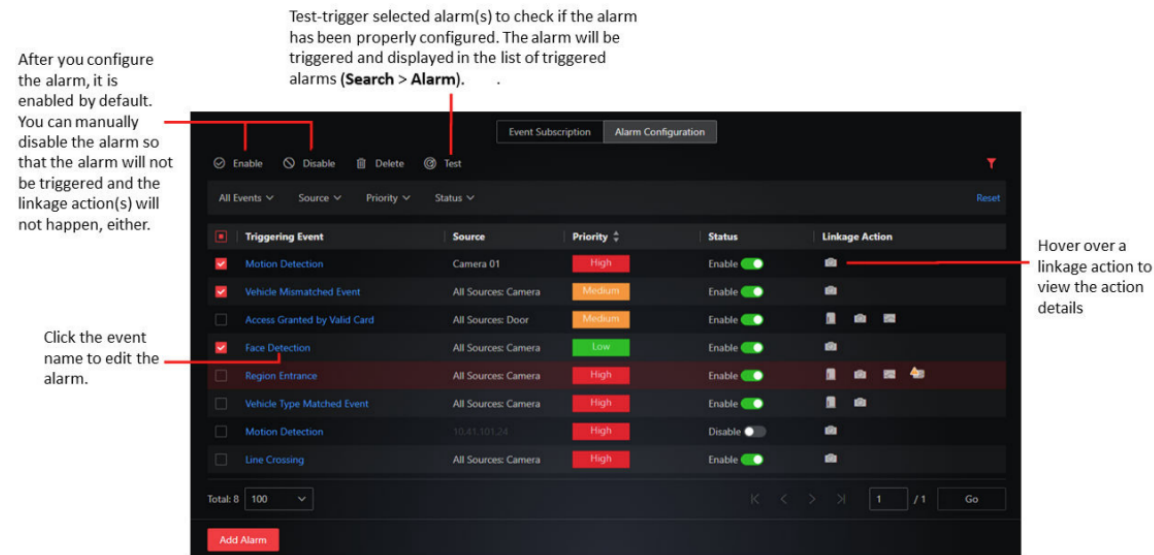


Figure 8.2 List of Configured Alarms

Fig

8.6 Monitoring, Searching, and Exporting Alarms



Access the complete history of triggered events by navigating to **Search → Alarm**. This module allows operators to review, manage, and extract event data.

**Event Details & Bookmarking**

Click on any specific alarm to view comprehensive details, including the trigger source, linked video, and operational records. You can also manually mark critical alarms as important for quick reference.

**List Customization**

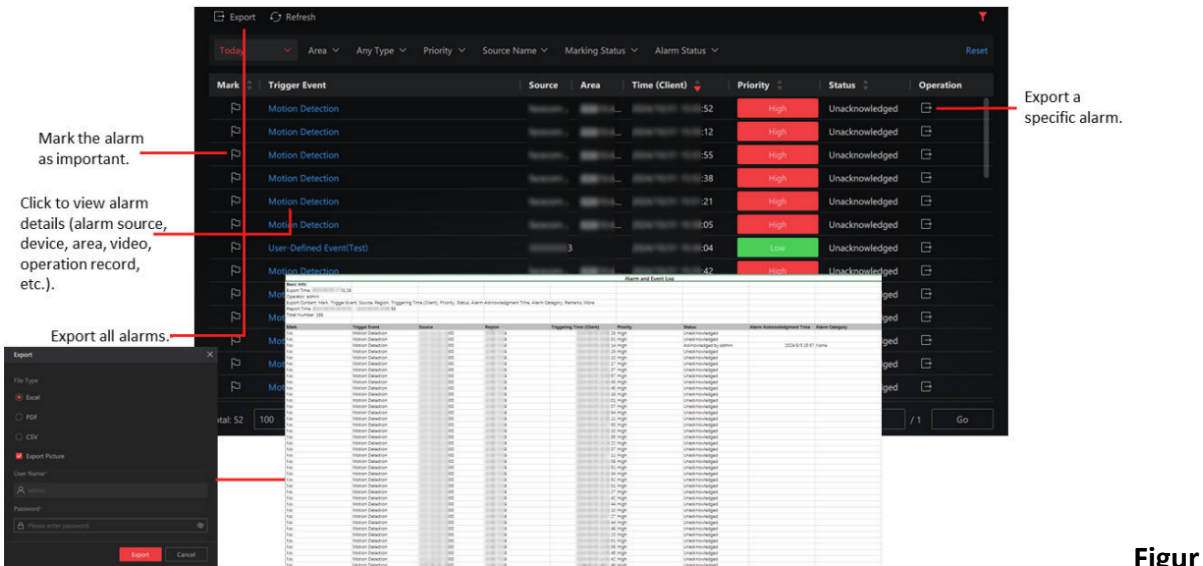
Optimize your view by setting the list to always display the latest events or the highest-priority alarms at the top.

**Export Capabilities**

Operators can export a single specific alarm record or perform a batch of export of all logged alarms for external reporting.

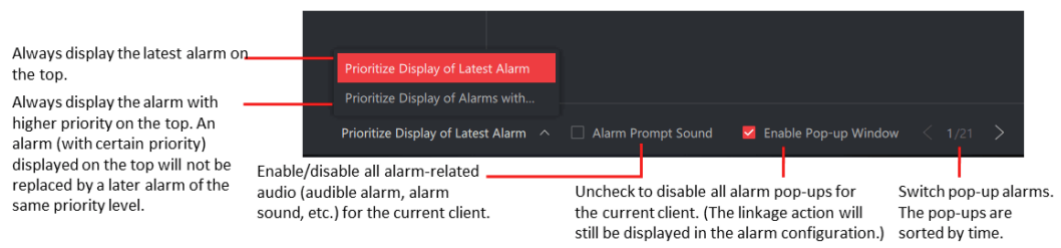
**Pop-up Notifications**

Real-time pop-up windows display critical alerts chronologically. You can switch between active pop-ups or disable them entirely for the local client.



**e 8.3 Triggered Alarm List**

**Figur**



**Figure 8.4 Alarm Pop-up Window**

# Chapter 9 System Access and Account Administration

The Account and Security module provides the necessary tools to configure user credentials, define permission groups, and enforce overarching authentication protocols. To access and manage these settings, navigate to **System** → **Account and Security**.

## 9.1 User and System Role Administration

The User and System Role Administration section provides the tools necessary to manage platform access and security. This module allows administrators to create and configure local user accounts, manage the existing user database, and define specific permission sets through the creation and assignment of system roles. By effectively utilizing these features, you can ensure that each user has the appropriate level of authority required for their specific operational tasks.

### 9.1.1 Add a User

You can add regular users and assign roles to them for accessing the system. Regular users refer to all users except the super.

**To generate and configure a new profile:**

- Access the user creation interface and input the required baseline credentials.
- Toggle the access status. Setting a profile to 'Inactive' actively prevents that account from authenticating into the system.
- Assign a numerical value to dictate the operator's PTZ control hierarchy.
  - Users assigned a higher numerical priority can interrupt and override active PTZ commands initiated by lower-tier personnel.
  - While actively operating a live PTZ feed, a user can lock the camera. This action blocks any PTZ input from other operators who have an equal or lower priority rating.
- Bind the appropriate predefined permission groups to the new profile. To verify the exact system of rights tied to a specific role before assigning it, hover your cursor over the role name in the list and click to view its detailed permissions.

## 9.1.2 Managing and Maintaining the User List

The Account and Security module provides a complete overview of all registered profiles. From this primary view, administrators can efficiently locate specific personnel and execute standard lifecycle management tasks against the user list, such as modifying credentials or adjusting access rights.

Only user(s) assigned with the Administrator role can inactivate or activate a user. If a user is inactivated, login with the user account is not allowed.

The screenshot shows the 'Account and Security' module in the Viasecurity Control Center. The interface includes a top navigation bar with tabs for System, Device Management, Person, Face Picture Library, Vehicle, Access Level, Video Intercom, Event and Alarm, and Account and Security. Below the navigation bar, there are tabs for User, Role, and Security Settings. The main area displays a table of users with columns for User Name, Type, Role, Connection Number, Login Status, User Status, and Expiry Time. Annotations with red lines point to various features: 'Force log out an online user.' points to the 'Force Logout' button; 'Click user name to view and edit user settings.' points to the 'User Name' column; 'Get the latest status of all users.' points to the 'Refresh All' button; 'Enter a keyword of the user name to search for users.' points to the search bar; and 'For users whose account is locked due to too many failed login attempts, user(s) assigned with the Administrator role can unlock their accounts for login.' points to the 'Unlock for Login' button.

Force log out an online user.

Click user name to view and edit user settings.

Get the latest status of all users.

Enter a keyword of the user name to search for users.

For users whose account is locked due to too many failed login attempts, user(s) assigned with the Administrator role can unlock their accounts for login.

| User Name | Type        | Role           | Connection Number | Login Status | User Status | Expiry Time      |
|-----------|-------------|----------------|-------------------|--------------|-------------|------------------|
| admin     | Super User  | Administrat... | 2 >               | Online       | Active      | 2023-10-27 15:59 |
| User 1    | Normal User | Operator       | 0 >               | Offline      | Active      | 2023-10-27 15:59 |

Add User

Figure 9.1 User List

## 9.1.3 Configuring System Roles

In the Viasecurity Control Center, roles act as permission templates that dictate what actions a user is authorized to perform. By grouping specific platform privileges into custom roles, you can efficiently distribute and manage user access levels across the system.

### Built-In System Profiles

The platform includes two mandatory default roles. For security and stability, these built-in profiles cannot be edited or deleted:

- **Administrator:** This profile is granted absolute control, possessing every available permission and configuration right within the entire platform.

- **Operator:** This profile is designed for daily monitoring and operation, providing full authorization to interact with operational resources and applications without altering core system settings.

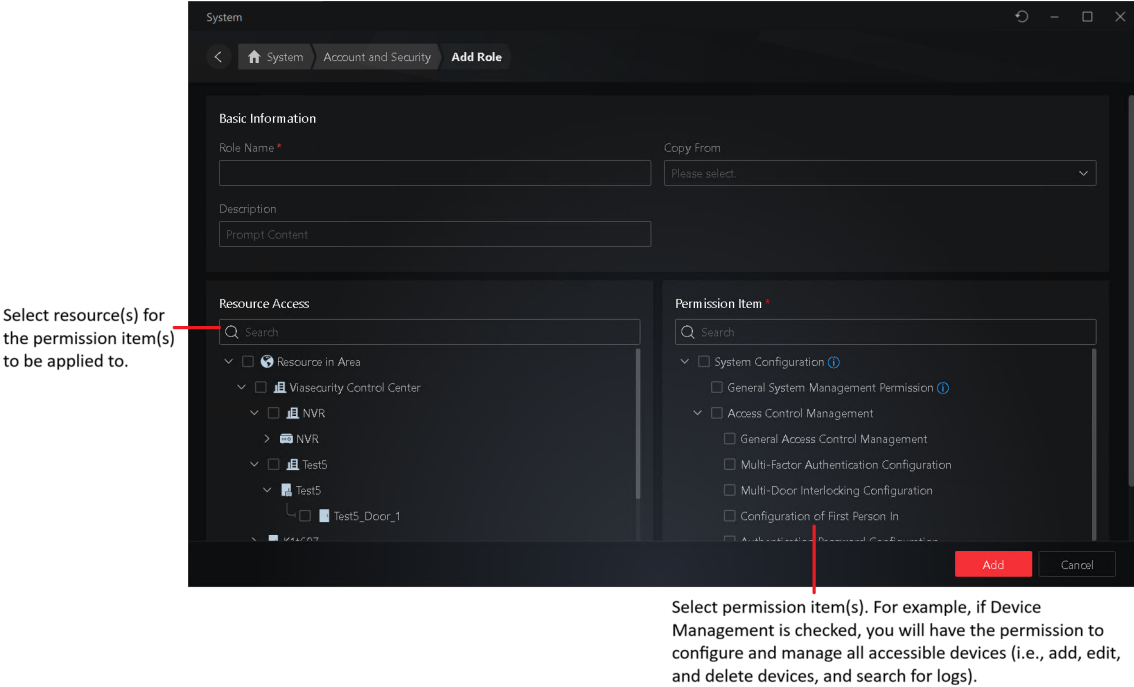


Figure 9.2 Add a Role

Table 9.1 Permission Items

| Category          | Sub-Category                         | Specific Permission                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System Management | General System Management Permission | Permission for system configuration, management of face pictures and human bodies, ANPR, persons, managing events and alarms, managing users and roles, viewing permissions, configuring security settings, and adding/deleting/editing permission for maps.                                                                                                                                                                                                                                                                                                                     |
|                   | Access Control Management            | <p><b>General Access Control Management:</b><br/>Entry to the Access Level module in <b>System:</b> applying access levels by department/person; entry to access schedule management and configuring schedules; entry to access level management and configuring access levels; re-applying access level when applying failed; statistics and details by access level status.</p> <p>For this permission, the resource permission for department(s) and persons within the department is required, and the specific permission items are assigned according to the resource.</p> |
|                   |                                      | <p><b>Multi-Factor Authentication Configuration:</b><br/>Entry the multi-factor authentication configuration and configure multi-factor authentication.</p> <p>For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.</p>                                                                                                                                                                                                                                                               |
|                   |                                      | <p><b>Multi-Door Interlocking Configuration:</b><br/>Entry the multi-door interlocking configuration and configure multi-door interlocking.</p> <p>For this permission, the resource</p>                                                                                                                                                                                                                                                                                                                                                                                         |

|  |  |                                                                                                               |
|--|--|---------------------------------------------------------------------------------------------------------------|
|  |  | permission for door(s) is required, and the specific permission items are assigned according to the resource. |
|--|--|---------------------------------------------------------------------------------------------------------------|

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p><b>Configuration of First Person In:</b></p> <p>Entry to the first person in configuration and configure first person in.</p> <p>For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.</p>                                        |
|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p><b>Authentication Code Configuration:</b></p> <p>Entry the <b>Authentication Password</b> configuration and configure the authentication password on the device.</p> <p>For this permission, the resource permission for door(s) is required, and the specific permission items are assigned according to the resource.</p> |
|                   | View Sharing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Permission for sharing views with other persons and viewing the list of shares.                                                                                                                                                                                                                                                |
| Device Management | <p>Permission for adding/deleting/editing all accessible access control and video intercom devices, monitoring the resources' status in real time, checking the maximum capacity and current number of persons, cards, fingerprints, face pictures, and events under the device, editing the device configuration, importing alarm output/input resources, managing areas and resources under areas, adjusting the hierarchy of areas and belonged resources, and searching for device logs.</p> |                                                                                                                                                                                                                                                                                                                                |



|                         |                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation<br>Permission | <b>General Surveillance<br/>Permission</b> | <ul style="list-style-type: none"> <li>● Permission for controlling alarm outputs: The resource permission for relevant devices is required, and the specific permission items are assigned according to the resource.</li> <li>● Permission for accessing and controlling all maps.</li> <li>● Permission for creating/viewing/exporting statistics and reports of access control and video intercom service: The resource permission for relevant reports is required, and the specific permission items are assigned according to the resource.</li> <li>● Permission for receiving and handling events and alarms: The permission for relevant resources and alarms is required, and the specific permission items are assigned according to the resource.</li> </ul> |
|                         | Search Permission                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | Video Operation                            | Playback                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                         |                                            | Export Video                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                         |                                            | Tag Management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                         | Access Control Operation                   | Remote: Unlock Door                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                         |                                            | Remote: Lock Door                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                         |                                            | Remote: Remain Unlocked                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                         |                                            | Remote: Remain Locked                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                         |                                            | <b>Quick Control All Doors:</b> This permission item only exists in the Administrator role, therefore only available to users assigned                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|  |  |                              |
|--|--|------------------------------|
|  |  | with the Administrator role. |
|--|--|------------------------------|

## 9.2 Account Security and Credential Recovery

This section outlines the protocols for maintaining account integrity and managing access credentials within the Viasecurity Control Center. It provides detailed instructions on configuring defensive security rules.

### 9.2.1 Account Security Configurations

To safeguard the system against unauthorized access, you can establish strict login parameters and recovery options. To apply these parameters, navigate to the **Account and Security** module and select **Security Settings**.

#### Login Protection Parameters

##### Max. Failed Attempts Before Lockout

Define the maximum number of consecutive incorrect password entries allowed. (*Note that this threshold only counts password failures and ignores failed verification code inputs.*) Once this limit is exceeded, the system will instantly lock the targeted account for the current IP address.

##### Lock Duration

Specify the exact duration the account will remain restricted after reaching the failed attempt limit.

##### Security Question Settings

Configure security questions specifically dedicated to the super user (admin) account. These questions provide a fallback method for the admin to verify their identity and recover a forgotten password. All provided answers are case-insensitive during both the setup and recovery process.

### 9.2.2 Reset Login Password

Users have the ability to either update their current password while logged in or reset it if it is forgotten.

#### Updating an Active Session Password

1. Locate and click your logged-in account name in the top right corner of the interface.
2. Select **Change Password** from the menu to establish a new credential.

## **Recovering a Forgotten Password**

To initiate the recovery process, click the **Forget Password** button directly on the main login screen. The available retrieval methods depend strictly on the user's privilege level:

- **Super User (Admin) Recovery Methods:**
  - Security Questions: Successfully answer the pre-configured security questions to regain access.
  - License Code Verification: If the system license is active, input the activation code found in your license file to retrieve the password.
  - Email Verification: If the license has not been activated, the system will send a recovery verification code to the configured admin email address.
- **Standard User Recovery Methods:**
  - Email Verification: Retrieve access using a verification code sent to the user's configured email address.
  - Administrator Assistance: Request a password reset from a user with a higher privilege role. Users without administrator rights can ask an Administrator, while Administrators can request assistance directly from the main admin user.

# Chapter 10 System Configuration

You can manage the core operational parameters of the Viasecurity Control Center through the **System Configuration** module. To access these options, navigate to the top-right corner of the desktop interface and select **System → System Configuration**.

This management section allows administrators to:

- Link mail servers for notifications.
- Establish storage quotas and data retention rules.
- Define holiday schedules.
- Adjust network properties, including NTP synchronization, WAN mapping, and device access protocols.
- Manage account security and SSL/TLS certificates.
- Modify core system capabilities.

## 10.1 Configure Email Parameters

Linking an email account allows the system to dispatch automated event notifications and deliver verification codes for account password recovery.

### Configuration Steps:

1. Navigate to **System → System Configuration → Email** via the top-right corner of the desktop.
2. Define the necessary connection parameters based on your mail provider's requirements:
  - a. **SMTP Server Address:** Input the host name or IP address of your mail provider (for example, smtp.gmail.com).
  - b. **Cryptographic Protocol:** Select the required encryption method to secure outgoing mail, as mandated by your SMTP server.
  - c. **Server Authentication:** Enable this checkbox if your mail server requires login credentials to send messages.
3. Click **Test** to verify that the software can successfully communicate with the mail server.

4. Click **Save** to apply and finalize the configuration.

*(Note: If you are using a Google Workspace or Gmail account, you must first enable 2-Step Verification in your Google security settings, generate a dedicated App Password, and input it here for authentication.)*

## 10.2 Managing Holiday Schedules

Holiday templates allow you to define specific dates that override standard schedules for access control, alarm triggers, and event-based services.

### Creating a Holiday Entry

1. In the **System Configuration** menu, select the **Holiday** tab.
2. Click **Add**, assign a unique name, and specify the **Holiday Type**:
  - a. **Fixed-Date (Regular Holiday)**: Use this for holidays that occur on the same calendar date every year, such as Christmas (December 25th).
  - b. **Movable (Irregular Holiday)**: Use this for holidays based on specific weekdays where the date changes annually, such as Mother's Day (the second Sunday of May).

### Editing Existing Holidays

To update an existing entry, locate it in the list and click directly on the parameter you wish to edit.

No more than 32 holidays can be added and the dates of each holiday cannot overlap.

| Holiday Name ▾ | Holiday Type    | Date ▾                    | Repeat Annually or Not | Operation |
|----------------|-----------------|---------------------------|------------------------|-----------|
| Holiday2       | Regular Holiday | 2024/08/10-<br>2024/08/10 | No                     | 🗑️        |
| + Add          |                 |                           |                        |           |

Figure 10.1 Edit Holiday Parameters

## 10.3 Managing Network and Communication Interfaces

All network-related adjustments can be performed by navigating to **System → System Configuration → Network** from the Home page.

### 10.3.1 Configure Internet Time Sync

You can set NTP parameters for synchronizing the time between resources managed on the platform and the NTP server. Three system time sync modes are supported. See the table below for more details.

#### Time Synchronization Configuration

To guarantee accurate timekeeping across all connected hardware, the system offers three synchronization methods:

- The **Operating System Time Sync** mode relies on your host machine's clock settings and synchronizes devices every 60 minutes by default.
- If you are exclusively utilizing Viasecurity devices, you can select the **Local Server Time Sync** option, which also defaults to a 60-minute interval.
- For broader compatibility, the **NTP Time Sync** mode allows you to specify a custom NTP Server Address, NTP Port, and synchronization interval. If your deployment requires external time servers, this mode supports enabling **Configure WAN Mapping**. You can always verify connectivity with the selected time server by clicking the Test button.

### 10.3.2 Configure Device Access Protocol

Before integrating video surveillance equipment, you must enable the appropriate communication protocol. In the device access protocol settings, you can activate access via the ONVIF protocol.

### 10.3.3 Configure WAN Access

For complex topologies requiring external connectivity, you must activate the WAN Access feature to establish a static IP address, domain name, and specific ports for Wide Area Network communication. Depending on your hardware infrastructure, you will need to assign the appropriate network addresses. In a single NIC environment, define a unified SYS / System Storage Network Address to handle both system network access and storage services.

For high-performance deployments utilizing a dual NIC environment, you can separate the traffic by defining a SYS Network Address for system services and a distinct System Storage Network Address for storage operations. When operating with dual NICs, ensure that both the SYS network address and the Recording Server network address, as well as their respective interface cards, reside on the identical network domain to prevent communication failures.

You can then select your required Application Scenarios and use the Configure Mapping Port function to assign the port number for data transmission. You have the option to save the configuration or export the complete WAN port mapping details, including LAN, WAN, and protocol information, directly into an Excel file. Please be aware that any subsequent changes to the LAN port will require corresponding adjustments to your router's port mapping configuration.

### **10.3.4 Configure NIC Settings**

This section allows you to dedicate specific network interface cards of the current Server to manage distinct types of data traffic. You can explicitly assign the SYS NIC to receive alarm information from hardware connected via the ONVIF protocol. Additionally, you can designate a separate system storage NIC exclusively to handle the heavy data transmission required when archiving video footage, pictures, and operational files.

### **10.3.5 Network Reset Information**

If your system undergoes a network domain change, such as a server migration, previous device configurations will become invalid and disrupt media playback. To adapt your connected devices to the new environment, navigate **Reset Network Information** and apply the **Reset** command.

## **10.4 Securing HTTPS Connections with SSL/TLS Certificates**

To guarantee that the client interacts exclusively with verified and secure servers, the Viasecurity Control Center enforces server certificate validation, which safeguards the communication channel by blocking connections to unverified addresses.



### 10.4.1 Certificate Management

The software provides three distinct certificate validation levels to accommodate various security policies:

- Under the **High** level, the system strictly accepts public certificates issued by a recognized Certificate Authority (CA) or user-generated PKI certificates, actively rejecting any self-signed variants to ensure peak authentication. In this strict mode, users will receive a warning message if they attempt to connect to a system utilizing an invalid certificate or a mismatched hostname.
- The **Medium (Recommended)** level permits the Server to operate using self-signed certificates, provided that any domain name connections are explicitly registered as custom servers.
- The **Basic** level completely bypasses all certificate validation, allowing direct connections without any warning prompts. This disabled validation state is strongly discouraged, as active certificate verification is a fundamental component of system security hardening.

### 10.4.2. Get Your SSL/TLS Certificate

Acquiring a robust SSL/TLS certificate involves purchasing a digital certificate from a trusted Certificate Authority (CA) to secure data transfers and prove server identity. This purchased certificate provides a significantly higher security tier compared to the default platform certificate.

You must first select a trusted CA and generate a certificate signing request (CSR) along with a private key, utilizing standard methods such as Microsoft IIS, OpenSSL, or trusted websites. Submit this generated CSR to your chosen CA to obtain the authorized SSL/TLS certificate and then download it to your local PC. It is critical to verify that the downloaded certificate file is strictly in the PEM format, utilizing conversion tools or extension editing if necessary.

### Certificate Details

|                                     |                                                |
|-------------------------------------|------------------------------------------------|
| Type                                | Standard SSL Certificate                       |
| Status                              | Certificate issued<br><a href="#">(Revoke)</a> |
| Domain name                         | ██████.org.uk                                  |
| Certificate Issuer                  | Starfield SHA-2                                |
| Request Date                        | 7/10/2021 14:55                                |
| Request Submission Type             | Rekey                                          |
| Current Certificate Validity Period | 7/10/2021 - 28/8/2022                          |

### Download Certificate

To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or servers.

First time installing a certificate?  
[View Installation Instructions for the selected server.](#)

Server type

Other ▾

Download Zip File

Figure 10.2 SSL/TLS Certificate Example

### 10.4.3 Upload Your SSL/TLS Certificate to the System

To integrate the issued certificate into the system, you must consolidate its components—typically the PEM certificate file, the private key generated with the CSR, and the PEM certificate chain. Concatenate these exact elements into a single UTF-8 encoded PEM file in a strict sequence: the certificate file first, followed by the private key, and concluding with the certificate chain.

Next, navigate to **System → System Configuration → Security → Certificate Management** on the top of the Desktop interface. Assign Maximum as the Security Requirements for Certificate and utilize the Upload Certificate area to submit your newly concatenated file. Be aware that the Desktop application will automatically restart upon successful upload. Furthermore, if an invalid or incomplete operating system certificate chain causes verification failures, you may utilize the Upper-Level Certificate section to Add the chain directly to the server. In such cases, users also have the option to download the certificate chain, convert it into a CRT format, and install it locally on their PCs.

```

-----BEGIN·CERTIFICATE-----
MIIGbzCCBVegAwIBAgIMUIt4TG0LEB4xyfNBMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
tAqm/TgWlV8dwimlwc6t525+Hr13lOnHA3FF78cwWM15x5dNKhwf632dxMQz4IpB
8XMkRHge9AIdnlVMp2HUB7iOZW3K4Cv9O/YCwuHsnnFCibwWpXZUY2KSi52lRxBJ
0/gC3Cr/WyI5fRzHqnrnxnHmEqQ==
-----END·CERTIFICATE-----

-----BEGIN·RSA·PRIVATE·KEY-----
MIIEowIBAACAQEApeg3HSjP4zoyFCii+Ct2f7501VmzdnYdxEVqBdQtMie27pJk6
G4e5YQKBgCE/n8nqGm9spvRz6GW59tboV8eByZePkyn+8ydv4VeSgL9q5uTbHKtQ
N9VTTuYxmAyUQ46EDWKHAU5445uEUFsBy6X+77zPEvuNpqUSdsEsOjm9s4XmpibK
ptsahzxpzPKCKalnN2nnGpvJ60ailfEMYzP5zMNIeQPbteZ734yR
-----END·RSA·PRIVATE·KEY-----

-----BEGIN·CERTIFICATE-----
MIIHajCCBOqgAwIBAgIQBeEL6xHDBPMqVc/6KaEeljANBgkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzErMCKGA1UEChMiVml0YWx3ZXJrcyBJbnRlcm5ldCBTb2x1
0y3ryvnrPxtYleAljYaH0a08klpIbWlOUZHL5T4DTFj6ko0J15MjGSTOanrvme52
oVOgwRlGPAUBRQyqbNA/N5PgYvnbYnP+3zLjV2fcsTQd9Ryk7ulSbK5ZTjds3PCC
Z/aCk1NiNiyigUKZmFSniwaFMpojLdiBmKZjgepFJxMTiITr8ZqBG+lkJSZB88POf
AAyK5ka+CpCndiSV/gQnsMagCmeyhw==
-----END·CERTIFICATE-----

-----BEGIN·CERTIFICATE-----
MIIF4DCCBMigAwIBAgIQAtzIUa9xYrr53z9VlROxXjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQLEExB3
FrgGtfx1rKPst8yZpX6jBLHy5eUUGJmG3VCGWRDrri1lWSajBC6RffzR7vzb0/wB
QOXi74AB8YHtYlzmjGGA7IY5Mjdur4CgcUWPlopqn4lgPvzRdRDvD0lg3rvpF/ma
ySyHlhO/+GHWldxQRb0QdhxyF4g=
-----END·CERTIFICATE-----

-----BEGIN·CERTIFICATE-----
MIIDjjCCANagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQLEExB3
d3cuZGlnaWNlcnQuYy29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwWUm9vdCBH
Fdtom/DzMNU+MeKNhJ7jitrAlj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTfy8bJZ91
8rGQmaFvE7FBcf6IKshPECBV1/MURexGrPTqh5Uykw7+U0b6LJ3/iYK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZ2m6zNTfl
MrY=
-----END·CERTIFICATE-----

```

Figure 10.3 Example of Concatenated Certificate

## 10.5 Configure Service Component Certificate

To ensure an adequate level of data security, you must synchronize certificates between the main server and the new component before integrating the Streaming Server. This process involves using the **Certificate between Services in System** function, which can be found on the home page by navigating to: **System → System Configuration → Security → Service Component Certificate**.

In this menu, you can view the existing certificate, copy it for configuration, or generate a new one by following the system prompts; please note that you must enter the administrator password for any actions involving the certificate. Only once the certificate details are identical on both servers will you be able to proceed with adding the hardware. Furthermore, if your configuration involves using an additional server for cross-machine backup and recovery, you will need to create a **System Storage AK/SK Authentication Signature**. Updating or creating this signature also requires confirmation with the administrator password.

## 10.6 Privacy and Security

You can manage your privacy settings yourself by navigating to **System → System Configuration → Security → Privacy and Security**.

In this window, you can configure the **User Experience Improvement Program**, which allows the system to send reports on operational logs and software usage metrics to help improve the product. If your security policy does not allow the sharing of such information, you can disable this feature at any time in the relevant settings menu.

# Chapter 11 Maintenance

This section covers the real-time tracking of server and device statuses to ensure optimal security operations. You will find instructions for generating status reports, retrieving notifications, and searching through system logs.

## 11.1 Generate and Display Maintenance Report

The Viasecurity Control Center continuously tracks the system and connected resources for any operational exceptions. You can configure and view these health summaries for servers, access control hardware, and video devices.

### Generate Maintenance Report

To create a new report, navigate to the Home page, right-click on **Statistics** within the Resource Panel, and select **Add Statistics Report**. Choose Maintenance as the statistics type, assign a custom Statistics Name, and specify the desired Device Type.

**Create Your Statistics Report**

**1. Select Statistics Type**

- Maintenance**  
The maintenance report automatically monitors the system and its resources in real time for any exceptions.
- People Counting**  
Select one or multiple people counting cameras of interest and form real-time or historical reports. One could easily re-organize the data for more insights and export on spot.
- Person & Credential**  
Count the total number of persons and credentials in the platform.
- Access Level**  
Count the access level allocation and effective status of all persons in the platform.
- Access Control Events Today**  
List the top 5 normal or abnormal events that occurred today (00:00 to current time) in all access points.
- Top 5 Abnormal Access Control Events Today**  
List the top 5 abnormal events that occurred today (00:00 to current time) in all access points.

**2. Enter Statistics Information**

Statistics Name \*

Device Type \*

Fig

Figure 11.1 Generate Maintenance Report

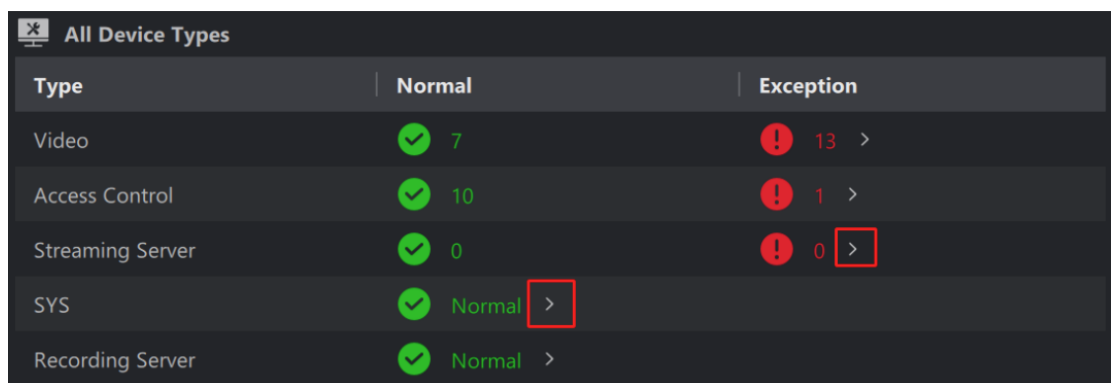
## Display Maintenance Report

Once created, click the icon  to access your compiled statistics and double-click a specific report to review its detailed data. Please be aware that the visual layout of these statistics depends on the hardware category you select.

For accurate metrics regarding video storage, storage location, disk, and NIC, a restart of the SYS is required beforehand. Additionally, data for drive C cannot be displayed when operating within a virtual machine environment. If your statistics fail to appear, first review the system logs to identify any potential disk-related error messages.

### All Device Types

The page provides counts for both  **Normal** and  **Exception** statuses, encompassing all device types, including video devices, access control devices, and servers.



| Type             | Normal                                                                                       | Exception                                                                                 |
|------------------|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Video            |  7        |  13 > |
| Access Control   |  10       |  1 >  |
| Streaming Server |  0        |  0 >  |
| SYS              |  Normal > |                                                                                           |
| Recording Server |  Normal > |                                                                                           |

Figure 11.2 All Device Types

You can click the icon  to view server and device details in a normal or exceptional status.

- For SYS, you can check CPU usage, RAM usage, NIC traffic, and streaming gateway data transfer.

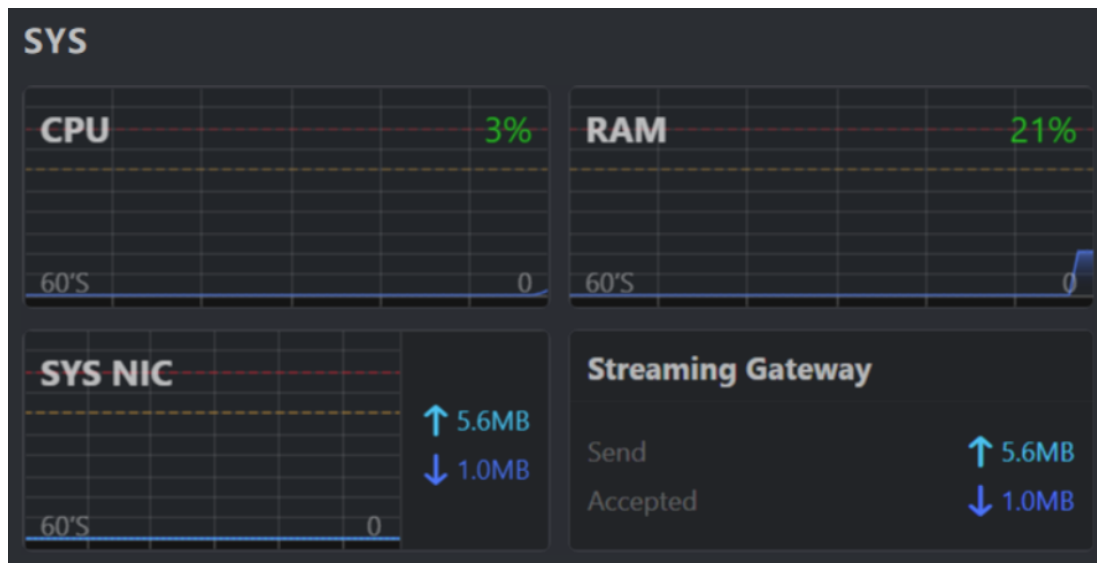


Figure 11.3 SYS

- For Recording Server, you can check NIC traffic, disk I/O, storage location, and video storage.

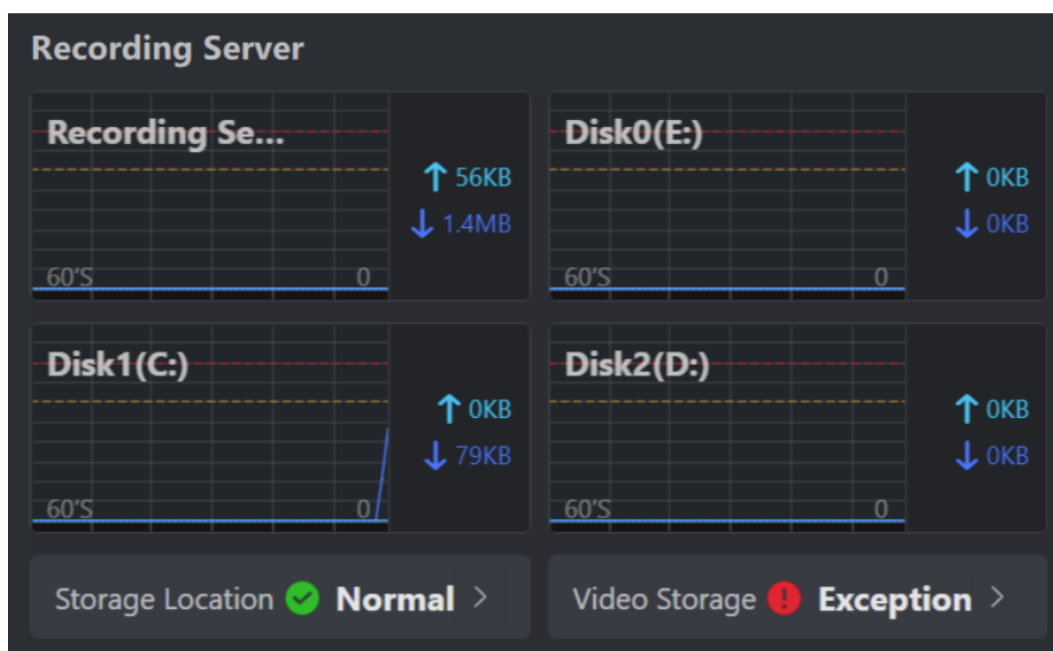
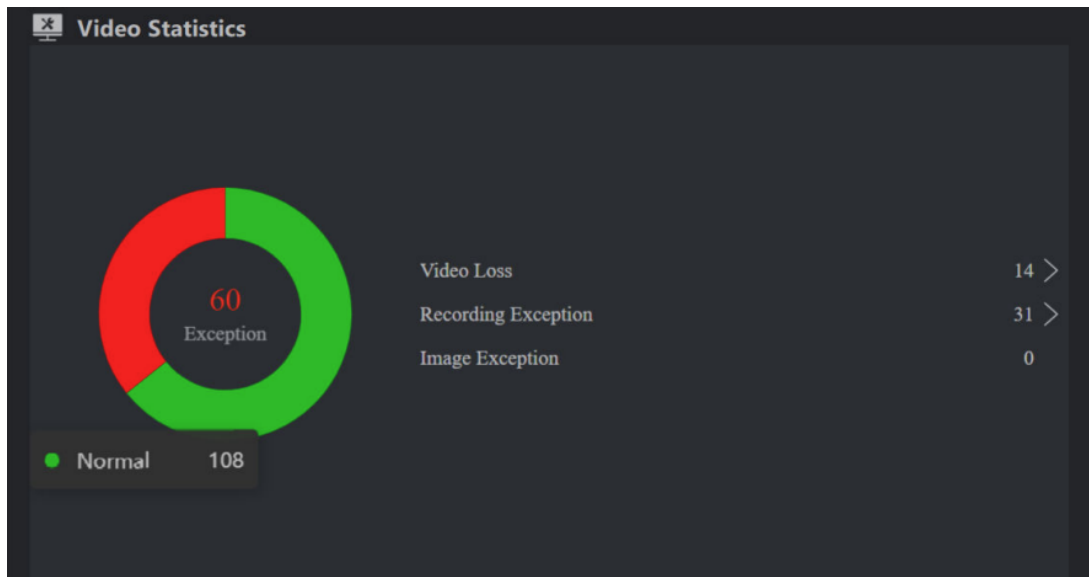


Figure 11.4 Recording Server

- For devices, you will be navigated to the **Device management** page to view exception details.

## Video

- Click the icon beside the number to navigate to the device management page. Here, you can inspect detailed information about video devices that are in video loss/recording exception/image exception state.
- Hover on the pie chart to view the number of normal or exception devices.



**Figure 11.5 Video Statistics**

## Access Control

- Click the icon beside the number to navigate to the device management page. Here, you can inspect detailed information about access control devices that are in device security exception/device network exception/device record reporting exception/device power battery exception state.
- Hover on the pie chart to view the number of normal or exception devices.



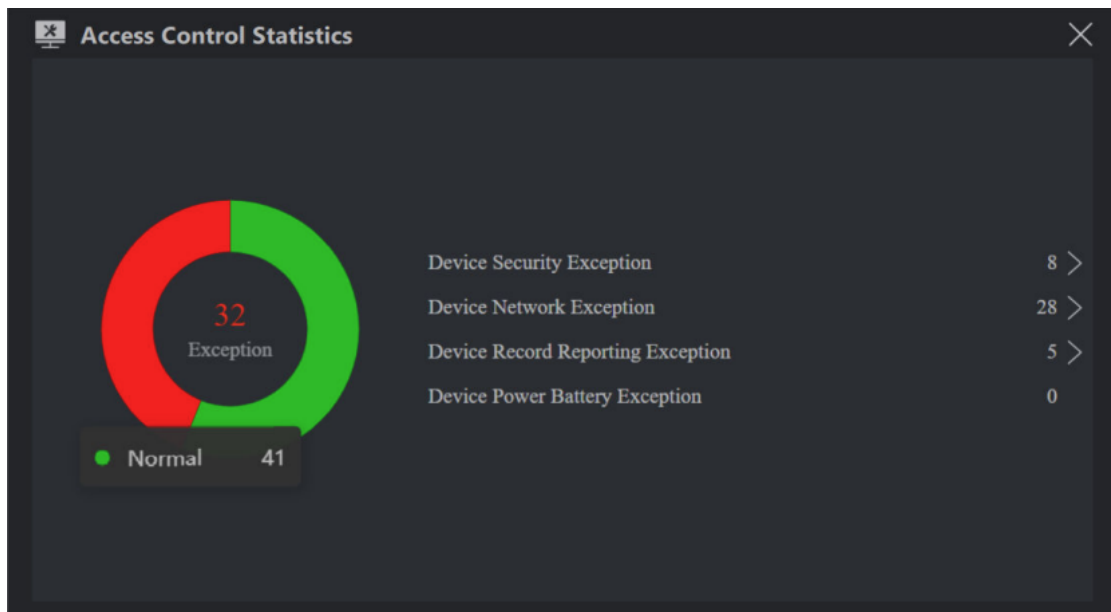


Figure 11.6 Access Control Statistics

## Server

Provides an overview of SYS and Recording Server, including CPU usage, NIC traffic, disk I/O, etc.

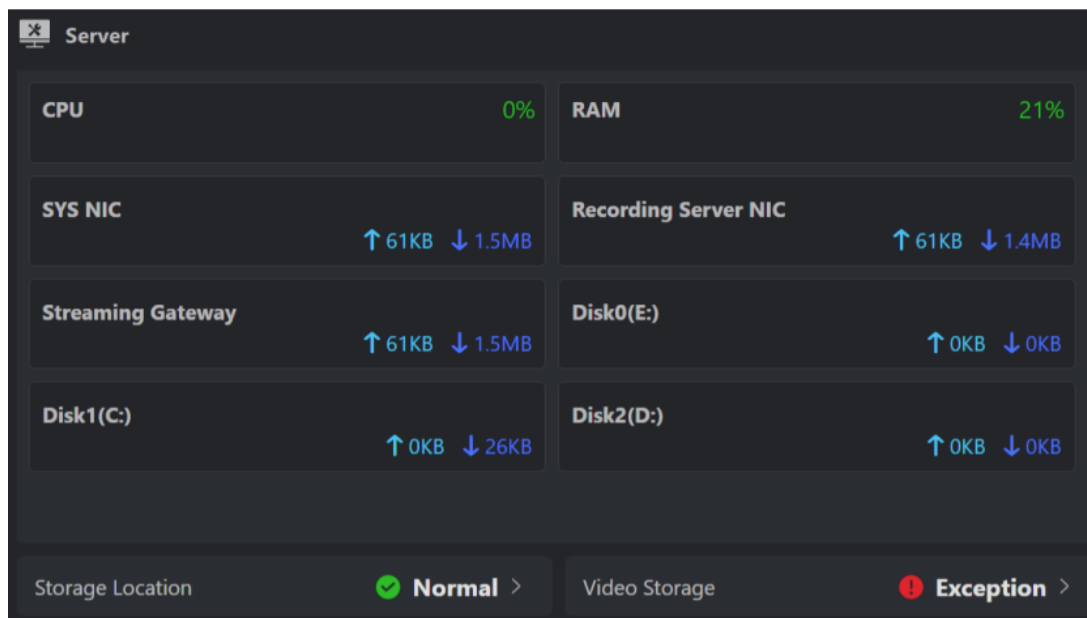


Figure 11.7 Server Statistics

## 11.2 Search for Notifications

Users can review historical notifications to identify and react to system updates or security events.

To search for notifications:

- 1. Navigate to **Home** → **Investigation** → **Notifications**.
- 2. Use the filters to select a specific **Date** and **Notification Type**.
- 3. Recorded notifications include:
  - a. **System Alerts**: Critical issues like "device type not supported".
  - b. **User Operations**: Functional feedback such as "calling video intercom not answered".
- 4. To extract data, click **Export** (upper-left corner) to save the current view as an **Excel**, **PDF**, or **CSV** file.

| Notification Retrieval    |      |        |                                         |
|---------------------------|------|--------|-----------------------------------------|
| SYS:                      |      |        |                                         |
| Export Time:              |      |        |                                         |
| Total Number: 159         |      |        |                                         |
| Title                     | Time | Type   | Description                             |
| Upgrading                 |      | System | Upgrading                               |
| Cardreader                |      | System | Cardreader                              |
| Upgrading Cardreader      |      | System | Upgrading Cardreader                    |
| Upgrading Cardreader      |      | System | Upgrading Cardreader                    |
| Upgrading Cardreader      |      | System | Upgrading Cardreader                    |
| Device Type Not Supported |      | System | Adding device failed. The device type i |
| Device Type Not Supported |      | System | Adding device failed. The device type i |
| Upgrading                 |      | System | Upgrading                               |
| Upgrading cameraguanlian  |      | System | Upgrading cameraguanlian                |
| Upgrading Failed          |      | System | Upgrading fail                          |
| Upgrading Failed          |      | System | Upgrading fail                          |

Fig

re 11.8 Notification Retrieval Excel Template

### 11.3 Search for System Logs

To maintain system integrity and expedite issue resolution, the Viasecurity Control Center allows you to retrieve and analyze both server-side and hardware-level logs.

#### Accessing System Logs

Logs are categorized into **Server Logs**, which are maintained on the central server, and **Device Logs**, which are stored directly on the hardware.

#### Centralized Search

To query both log types from a single interface, navigate to **Home** → **Investigation** → **System Log**.

### Direct Device Retrieval

Provided the hardware supports this functionality, you can access local records through the following methods:

- **Device Management:** Go to **Home** → **System** → **Device Management**, right-click the specific unit, and select **View Log**.
- **Detailed View:** Within the **Device Details** page, right-click the device, choose **View Details**, and click **View Log** in the upper-right corner.

## Log Analysis and Data Export

### Server Log Filtering

Narrow down events by selecting severity levels: **Information**, **Warning**, or **Error**. You can also use the **Resource Name** field to quickly isolate specific entries.

### Data Extraction

To save records for external review, click **Export** in the top-left corner to download the logs in **Excel** or **CSV** format.

| Server Log                |               |        |                              |                 |         |
|---------------------------|---------------|--------|------------------------------|-----------------|---------|
| Basic Information         |               |        |                              |                 |         |
| Export Time: [Time Range] |               |        |                              |                 |         |
| Operator: admin           |               |        |                              |                 |         |
| Export Content: Data      |               |        |                              |                 |         |
| Report Time: [Time Range] |               |        |                              |                 |         |
| Total Number: 5671        |               |        |                              |                 |         |
| Level                     | Time (Client) | Source | Event                        | Resource Name   | Area    |
| Information               | [Time]        | admin  | Add View                     | New View 1      |         |
| Information               | [Time]        | admin  | Start Live View              | [Resource] 8000 | HikCer  |
| Information               | [Time]        | admin  | Start Live View              | [Resource] 8000 | HikCer  |
| Information               | [Time]        | admin  | Start Downloading Video File | 3686 [Resource] | keliu N |
| Information               | [Time]        | admin  | Start Downloading Video File | IPCamera 01     | keliu N |
| Information               | [Time]        | admin  | Search Notification Record   |                 |         |
| Information               | [Time]        | admin  | Start Downloading Video File | 6825 [Resource] | keliu N |
| Information               | [Time]        | admin  | User Login                   |                 |         |
| Information               | [Time]        | admin  | User Logout                  |                 |         |
| Information               | [Time]        | admin  | Delete Encoding Device       | [Resource]      |         |
| Information               | [Time]        | chenqi | Search Alarm Log             |                 |         |

Figure 11.9 Server Log Excel Template

| Encoding Device Operation Log |                               |       |                    |             |
|-------------------------------|-------------------------------|-------|--------------------|-------------|
| <b>Basic Information</b>      |                               |       |                    |             |
| Type:                         | Encoding Device Operation Log |       |                    |             |
| Exporting Time:               |                               |       |                    |             |
| Searched by:                  | admin                         |       |                    |             |
| Report Time:                  |                               |       |                    |             |
| Total Number:                 | 9607                          |       |                    |             |
| Level                         | Device Time                   | User  | Event              | Channel No. |
| Information                   |                               |       | Online             |             |
| Exception                     |                               |       | Offline            |             |
| Operation                     |                               | admin | Remote: Get Status | 0           |
| Operation                     |                               | admin | Remote: Get Status | 0           |
| Operation                     |                               | admin | Remote: Get Status | 0           |
| Operation                     |                               | admin | Remote: Get Status | 0           |
| Operation                     |                               | admin | Remote: Get Status | 0           |

Figure 11.10 Device Log Excel Template

# **A. Product Usage Restrictions: Scenarios & Guidelines**

This topic provides restricted scenarios for the system to help users avoid unintended misuse. It serves as a quick reference for verifying permitted activities across specific use cases.

## **System**

- When you run the client as Administrator, importing data into the system may fail.
- Microsoft Office shall be installed in order to view exported excel files.
- Do not drag the client across screens with varying DPI settings, as this may result in unintended UI scaling issues.
- Make sure the available disk space is no less than 10 GB to avoid the installation failure of the Server.

## **Device Management**

- Cameras containing special characters including \ / : \* ? " < > | in their names cannot be imported.
- When editing the device password on the Web page, stop live view and playback on all clients, and change the password on the device list as quickly as possible. Try to change device password via the system instead of the Web page.

## **Video Monitoring**

- When using TargetTrace / object search, if an incorrect prompt pops up, you can check whether this function is enabled on the device configuration page.
- Do not arbitrarily modify whether the device stream is encrypted or the specific encryption keys.
- Do not use smooth stream and stream encryption simultaneously.
- For devices configured with a dual-stream recording schedule, main stream will be used when playing videos.
- Started recording manually is not supported during live view via smooth stream.

- If connected devices do not support UTC time, when using search functionalities (Video retrieval / Smart Search / all searches via NVR) during Daylight Saving Time (DST) transitions, the system cannot distinguish duplicate time periods (e.g., 01:30 appearing twice when DST ends). All search results will display local device time without UTC offset adjustments. For real-time events & alarms (Alarm Log Retrieval) based on devices without UTC support, duplicate timestamps may appear during DST exit periods (e.g., two entries showing "01:30").
- For live view and playback via Axis and Hanwha devices, make sure you have selected H.264 as the encoding format.
- Reverse playback of videos stored in Axis, Dahua, or Hanwha devices is not supported.
- No more than 12 views support synchronized playback simultaneously.
- To enlarge a fisheye-expanded image, double-click the image before enabling Fisheye Expansion.
- Two-way audio via channels of DVR is not supported.
- When drawing people counting detection areas, only rectangular areas are supported.
- For cameras managed via an NVR/DVR, the system cannot get their presets.
- Videos in AVI format may fail to be played by Windows-provided players, so free-charged players that support all video formats are recommended.

## **Access Control and Video Intercom**

- When importing the zip file of profile pictures, make sure the system language of the PC compressing profile pictures is the same as the system language of the Server.

## **System Storage**

- Up to 128 cameras are supported for video storage.
- Only pictures and files can be stored in the system if the video storage license is not activated.
- For Viasecurity Control Center installation with system storage, ensure the drive meets the following minimum capacity requirement; otherwise, it will not be usable for system storage.
  - 34 GB (if disk  $\leq$  2 TB)
  - 74 GB (if disk  $>$  2 TB)
- Initialization of the disk uses 90% of the remaining disk space.
- Since videos, pictures, and files are stored on the system's disk, system hibernation or sleep can result in the disk losing power, potentially causing storage exceptions. It is recommended to turn off hibernation or sleep mode.

- The minimum space required for each file type is 4 GB (for example, 4 GB for videos, 4 GB for pictures, and 4 GB for files), which includes necessary files for storage management.
- Rebuilding the index may temporarily affect search and playback functionality, but it will not cause data loss.
- Supports 6 data overwritten options.
- In the virtual machine environment, the performance of drive C will not be displayed in the maintenance report. See *11.1 Generate and Display Maintenance Report* for more details.

# Legal Information

## About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Viasecurity website (<https://viasecurity.ua>). Unless otherwise agreed, Viasecurity LLC or its affiliates (hereinafter referred to as "Viasecurity") make no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

## About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

## Acknowledgment of Intellectual Property Rights

- Viasecurity owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Viasecurity. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- Viasecurity and other Viasecurity's trademarks and logos are the properties of Viasecurity in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

## LEGAL DISCLAIMER



- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". VIASECURITY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL VIASECURITY BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF VIASECURITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND VIASECURITY SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, VIASECURITY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.