

Smart Intrusion Prevention Site Survey and Commissioning Guide



Zhejiang Uniview Technologies Co., Ltd.

All Rights Reserved

Document Classification: Public

Document Version: 2.2

Revision Date: 2026-8-10

Revision History

Revision Date	Revision Version	Revised Sections	Author	Description
2026.8.10	V2.2	All Sections	W11893	1) Updated relevant configuration descriptions 2) Updated example images

Contents

1 Overview	4
2 Site Survey Guide	6
2.1 Installation Requirements	6
2.2 Pixel Requirements	10
2.3 Target Speed Requirements	10
2.4 Brightness Requirements	10
2.5 Impact of Occlusion on Pedestrian Detection Rate	11
2.6 Impact of Nighttime Illumination on Target Detection	12
3 Configuration Description	13
3.1 Smart Intrusion Prevention Configuration	13
3.2 Local Configuration	21
3.3 Server Configuration	21
3.4 Using Perimeter Protection on NVR	24
4 Appendix	27
4.1 Calculation Principle	27

1 Overview

This guide provides site survey, position selection, and commissioning guidance for Uniview Smart Intrusion Prevention IPCs (network cameras). The algorithm-based perimeter protection includes four smart functions: Cross Line Detection, Enter Area, Intrusion Detection, and Leave Area.

1.1. Cross Line Detection

Cross Line Detection involves drawing one or more lines in the image and specifying trigger directions to help the algorithm determine whether an object meets the alarm conditions. If a target crosses these lines, the algorithm immediately detects it and triggers an alarm.

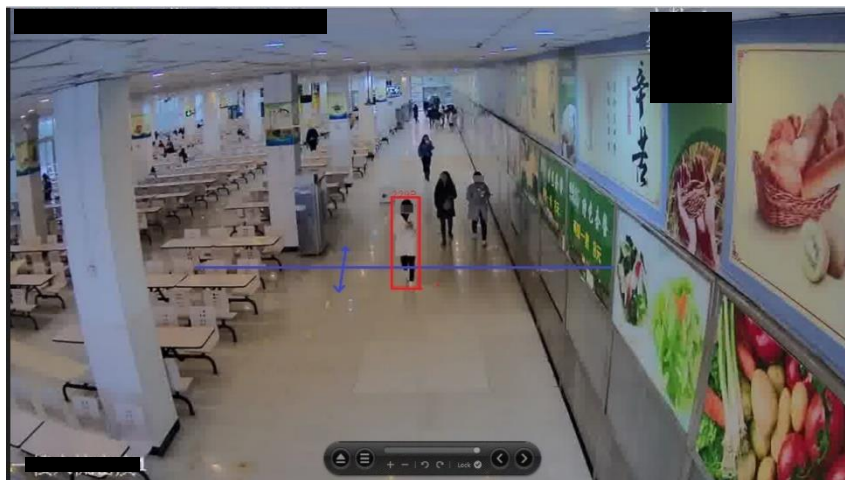


Figure 1. Cross Line Detection Example

1.2. Enter Area

Enter Area involves defining one or more monitored areas in the image. If a target enters these detection areas, the algorithm immediately detects it and triggers an alarm.



Figure 2. Enter Area Example

1.3. Intrusion Detection

Intrusion Detection involves defining one or more monitored areas in the image. If a target enters these detection areas and stays for a period of time, the algorithm detects it and triggers an alarm.

The difference between Intrusion Detection and Enter Area is that Intrusion Detection requires the object to stay in the detection area for a set time threshold before triggering an alarm, whereas Enter Area triggers an alarm immediately when the object enters the detection area.

1.4. Leave Area

Leave Area involves defining one or more monitored areas in the image. If a target leaves these detection areas, the algorithm immediately detects it and triggers an alarm.

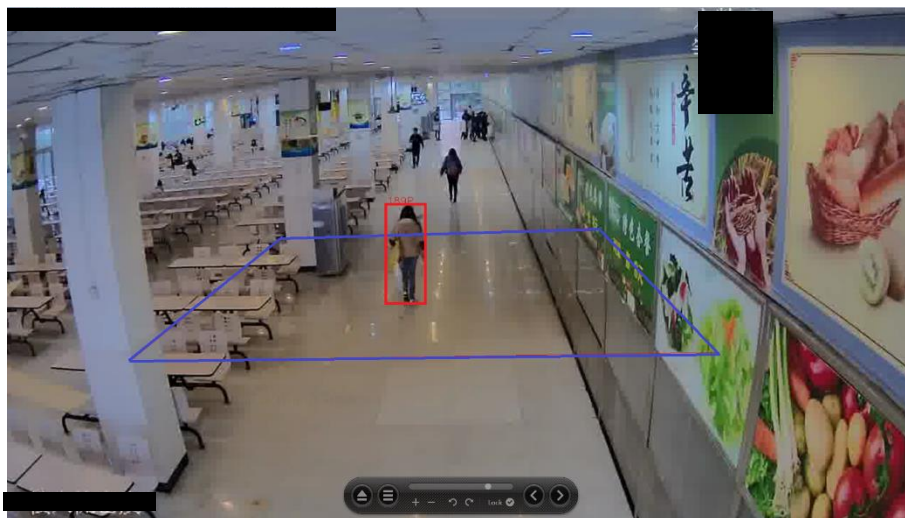


Figure 3. Leave Area Example

2 Site Survey Guide

2.1 Installation Requirements

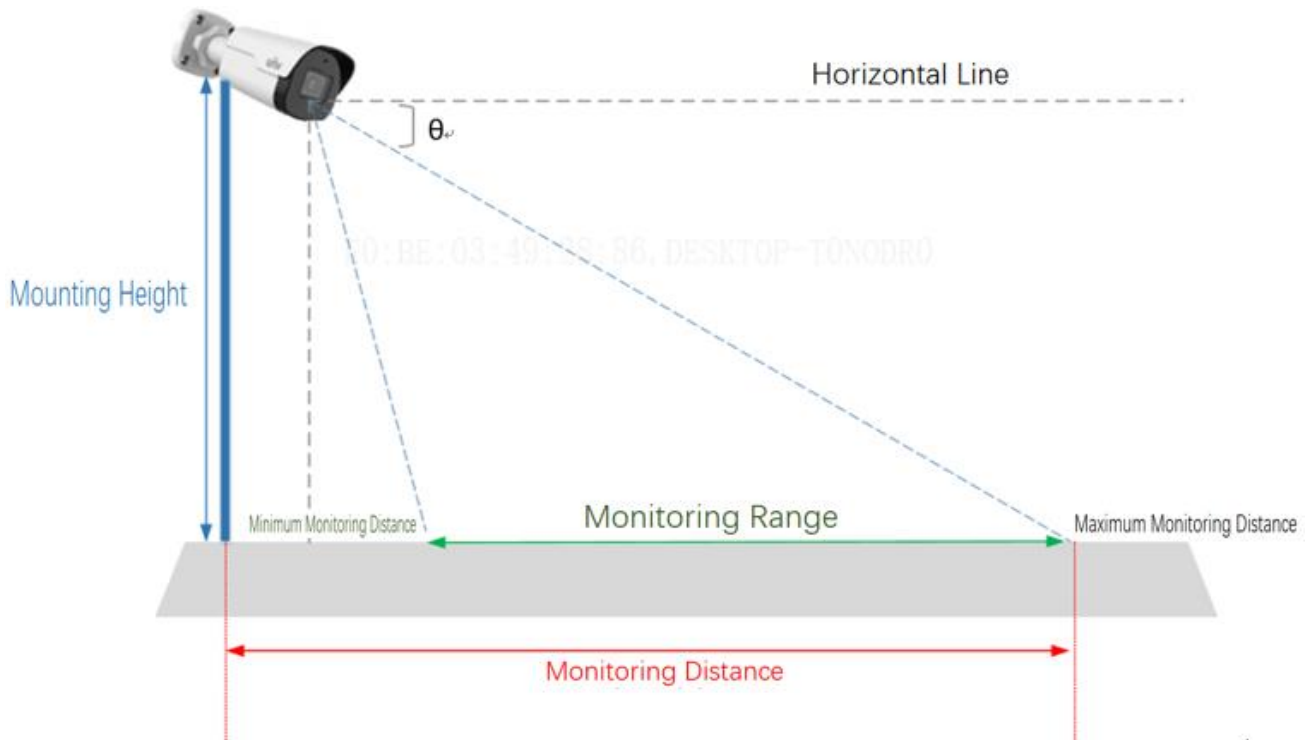


Figure 4. Installation Illustration

➤ Camera Mounting Height:

Indoor: 2.5 m to 5 m, 3 m recommended.

Outdoor: 3 m to 8 m, 4 m recommended.

➤ Camera Installation Angle:

The recommended top-down view angle θ is between 10° and 30° .

➤ Monitoring Distance:

The monitoring distance refers to the maximum monitoring distance of the camera. Factors such as focal length, image resolution, mounting height, installation angle, and lighting conditions all affect the monitoring distance of the camera.

➤ Scenario Examples:

1. In this indoor example, the camera is mounted at a height of 3 m with an installation angle of 15° , providing optimal imaging performance.



Figure 5. Optimal Indoor Monitoring Example

2. In the backyard monitoring example, the camera is mounted at a height of 5 m with an installation angle of 10° .

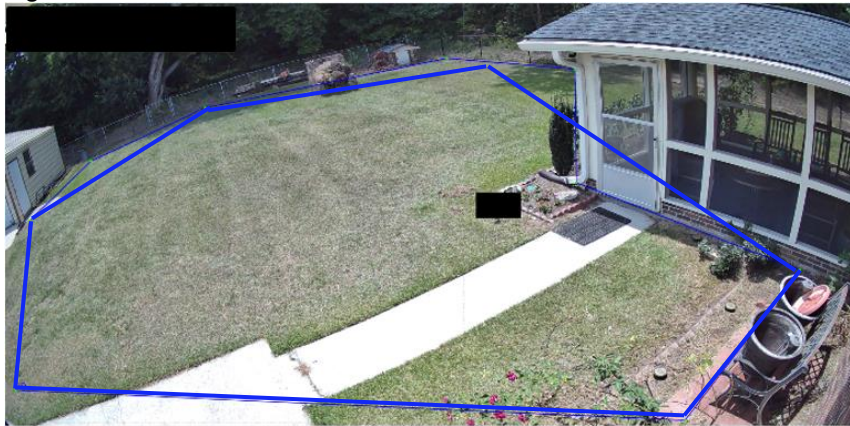


Figure 6. Optimal Outdoor Backyard Monitoring Example

3. In the road monitoring example, the camera is mounted at a height of 8 m with an installation angle of 15° , providing a wider monitoring range.



Figure 7. Optimal Road Monitoring Example

4. Special Monitoring Example.

If the camera needs to be mounted at a very high position, for example, 8 m, and the monitoring range is small, the installation angle should be larger, even exceeding 30° . In this case,

the detection rate for pedestrian targets will be reduced.



Figure 8. Special Monitoring Example

This example shows a field perimeter monitoring scenario where the camera mounting height does not exceed 10 m. The camera lens should be adjusted to face toward the wall. As a result, the detection rate for pedestrian targets will be reduced, especially under low-light conditions.



Figure 9. Special Field Perimeter Monitoring Example.

5. Poor Examples

In this parking lot monitoring example, the camera is mounted too low at approximately 2.5 m, resulting in a very small monitoring range. The correct mounting height should be 5 to 8 m.



Figure 10. Poor Parking Lot Monitoring Example

In this office building monitoring example, the camera is mounted too high at over 10 m, and the installation angle exceeds the specified range. This causes pedestrian targets to appear too small with indistinct features, affecting the detection rate.



Figure 11. Poor Office Building Monitoring Example

2.2 Pixel Requirements

1. Target pixel requirements are as follows:

Maximum Resolution	Pedestrian	Non-Motor Vehicle	Motor Vehicle
	Min. Pixels (W*H)	Min. Pixels (W*H)	Min. Pixels (W*H)
2MP	>32*64	>64*64	>64*64
4MP	>40*80	>80*80	>80*80
8MP	>64*128	>128*128	>128*128

2.3 Target Speed Requirements

Pedestrian lateral speed requirement: normal walking speed.

Non-motor vehicle lateral speed requirement: speed not exceeding 25 km/h.

Motor vehicle lateral speed requirement: speed not exceeding 40 km/h.

2.4 Brightness Requirements

The ambient brightness should be higher than 50 lux and stable. Avoid the following conditions:

- Avoid harsh backlight.



Figure 12. Harsh Backlight Scenario Example

- Avoid strong overexposure.



Figure 13. Strong Overexposure Scenario Example

- Avoid low-light conditions where the target color is almost identical to the background

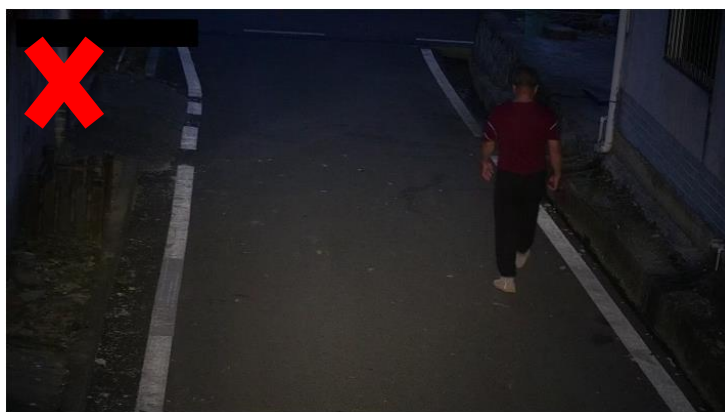


Figure 14. Low-Light Scenario Example

2.5 Impact of Occlusion on Pedestrian Detection Rate

- When a pedestrian is not occluded and there is significant contrast between the pedestrian and the background, as shown in Figure 15 (1), the detection rate is 95%.
- If the occluded area of a pedestrian is greater than 30% and less than 50%, and facial information can be recognized, as shown in Figure 15 (2), the detection rate is 80%.
- If the occluded area of a pedestrian is greater than 50%, and facial information can be recognized, as shown in Figure 15 (3), the detection rate is 60%.
- If the occluded area of a pedestrian is less than 30%, and facial information cannot be recognized, as shown in Figure 15 (4), the detection rate is 60%.

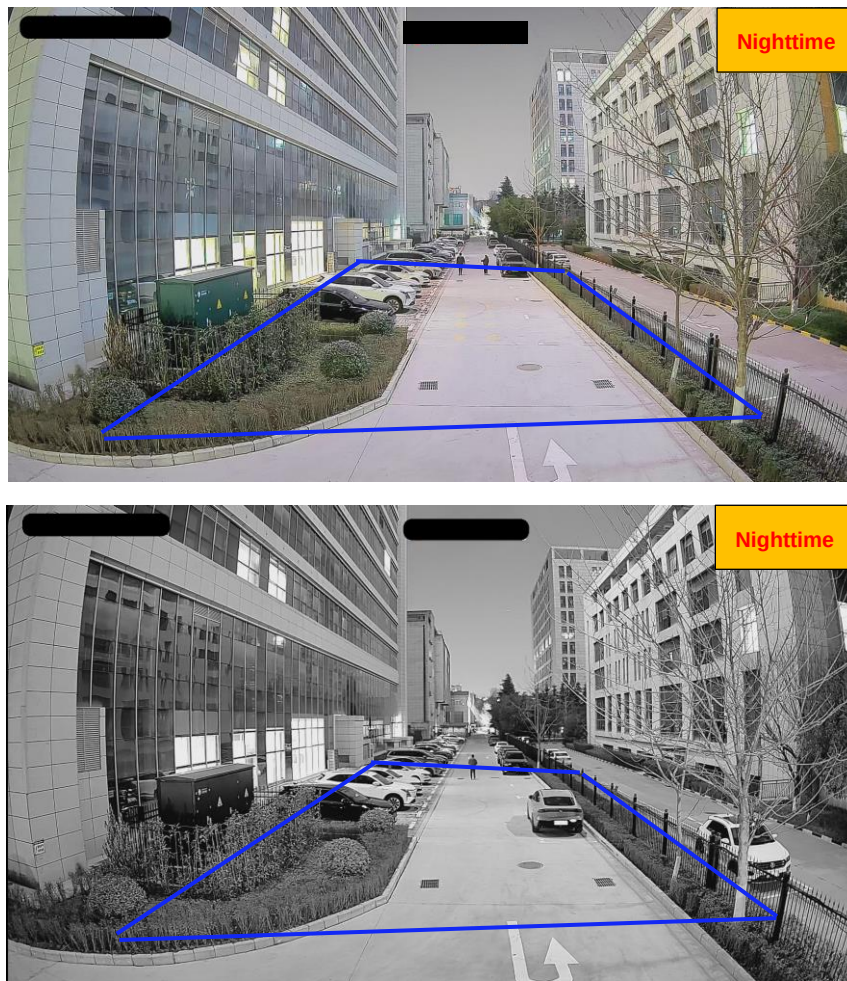


Figure 15. Pedestrian Occlusion Examples

2.6 Impact of Nighttime Illumination on Target Detection

In nighttime white light and nighttime infrared scenarios, the detection rate and detection distance for pedestrians, motor vehicles, and non-motor vehicles are 60% to 80% of those in daytime scenarios.





3 Configuration Description

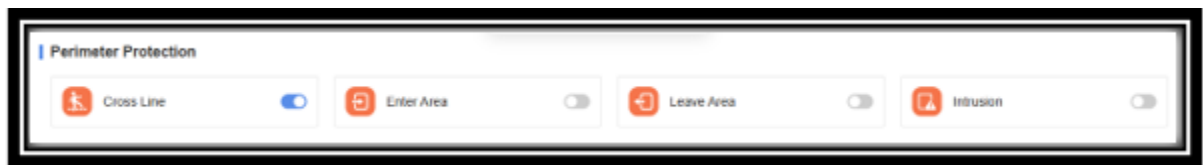
3.1 Smart Intrusion Prevention Configuration

Taking Cross Line Detection and Intrusion Detection as examples, the rule for Cross Line Detection is defined as a line, while the rule for Intrusion Detection is defined as an area. The configuration for Enter Area and Leave Area is similar to that of Intrusion Detection.

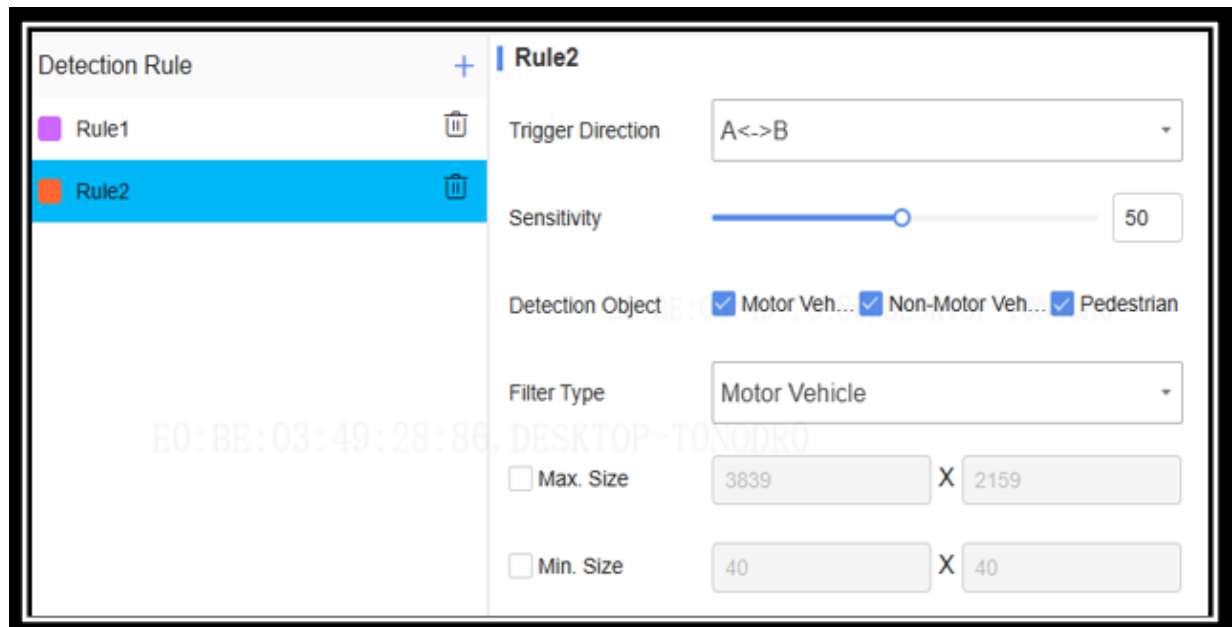
3.1.1 Cross Line Detection

1. Enable Cross Line Detection

Enable Cross Line Detection in Setup > Smart > Cross Line Detection.

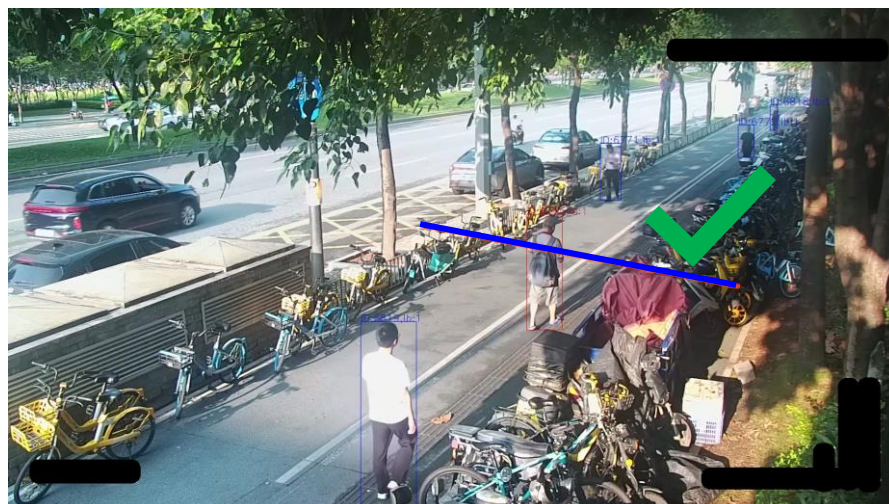


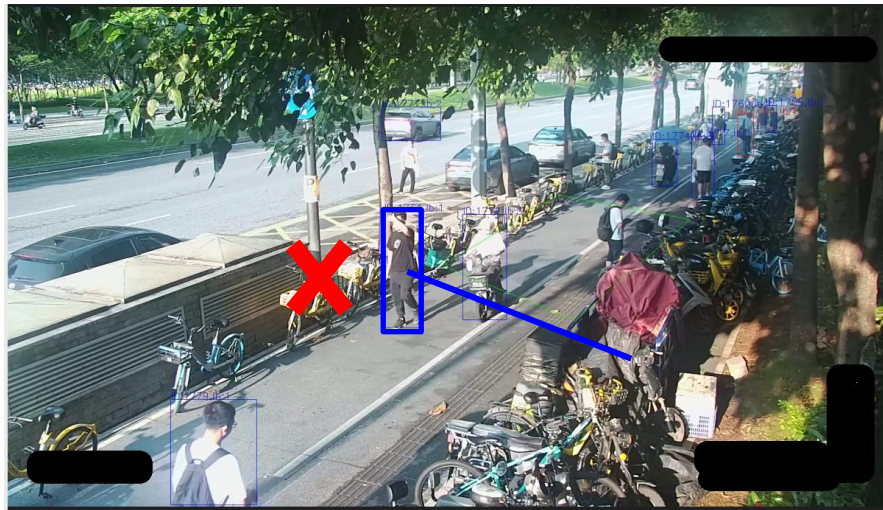
2. Configure Rule Parameters



Draw one or more rule lines in the image. Both ends of the rule lines should cover the areas to be monitored as much as possible, ensuring that all targets intersect the rule lines when passing through. Each rule line must have a clearly defined trigger direction.

Drawing example:





➤ **Trigger Direction**



One-way or two-way, used to filter objects in a specific direction. This parameter applies only to Cross Line Detection.

➤ **Sensitivity**



Sensitivity indicates how sensitive the target detection is. It is recommended to set it to 50.

- To increase the algorithm detection rate, the sensitivity can be increased, but this also increases the risk of false alarms caused by animals, trees, and so on.
- To reduce the number of false detections, the sensitivity can be decreased, but this increases the possibility of missed detections of real objects.

➤ **Detection Object**



The camera can detect three types of objects: Pedestrian, Motor Vehicle, and Non-Motor Vehicle (the supported categories may vary by camera model).

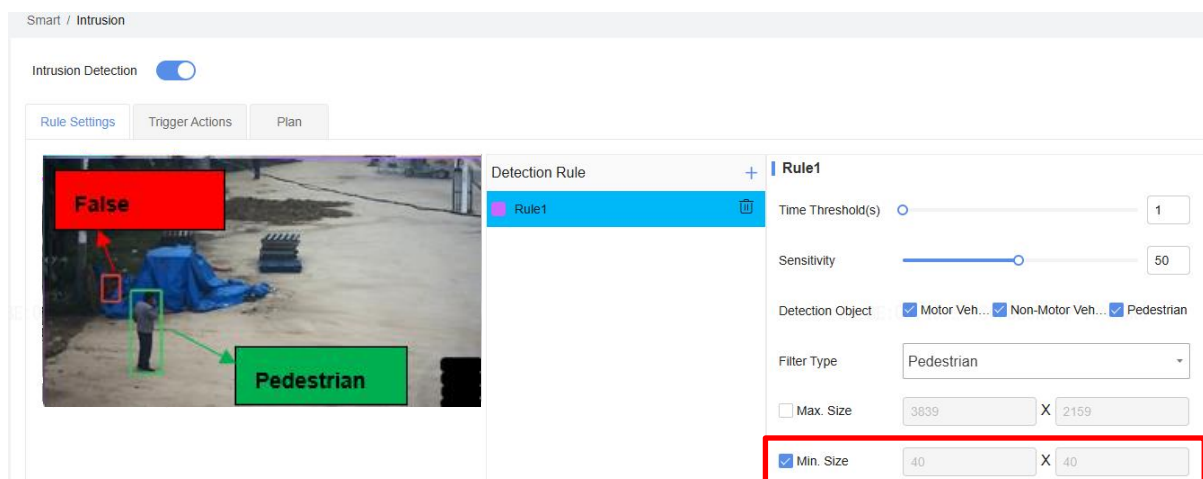
➤ **Filter by Object Size**

The camera supports configuring the Filter by Object Size function as needed. Different size filter thresholds can be configured for different types. If an object's size is larger than the maximum size or smaller than the minimum size, the camera will not capture the object's image. Typical sizes (pixels) for different objects, for example:

	Image	Pedestrian	Motor	Non-Motor
Min. Size	2MP	15*35	20*20	15*35
	4MP	22*52	30*30	22*52
	8MP	30*70	40*40	30*70
Max. Size	2MP	320*640	640*640	320*640
	4MP	480*960	960*960	480*960
	8MP	640*1280	1280*1280	640*1280

When configuring Filter by Object Size, select the filter type and maximum/minimum size below, and use the mouse to select the appropriate size in the image. If debris is falsely detected as a pedestrian, a minimum filter size value can be selected to filter out the false detection while ensuring that normal pedestrians are not filtered out. **NOTE! The recommended sizes here are the minimum/maximum sizes for filtering false detections to ensure performance, which differ from the target pixel requirements in section 2.2.**

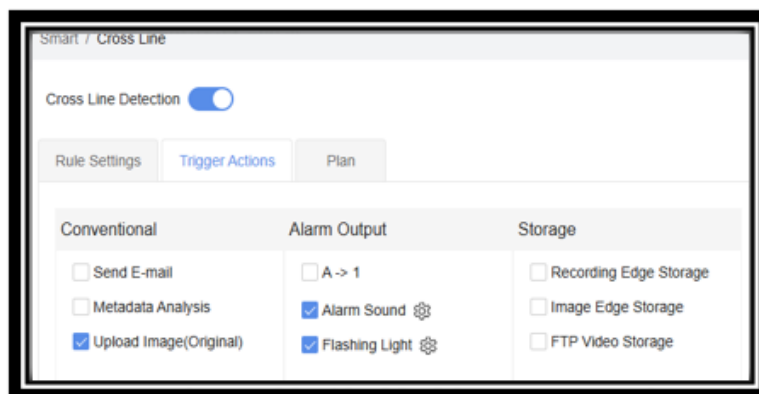
As shown in the example below, the actual pedestrian's pixel size is 380*700, while the debris false detection's pixel size is 240*300. The minimum filter size can be set to a value between them, such as 300*400, which filters out the false detection while ensuring normal pedestrian detection.



Configure Trigger Actions

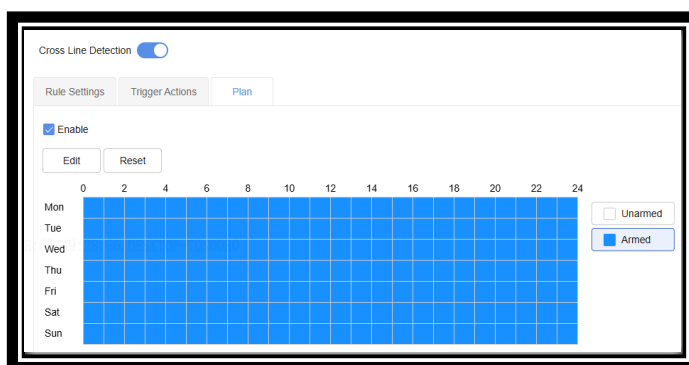
Upload Image(Original): Used to set whether to upload the original captured full image. By default, a small-range cropped image is uploaded.

Trigger Alarm Output: Outputs the triggered alarm to connected alarm devices, such as alarm lights and warning horns.



➤ Configure Arming Schedule

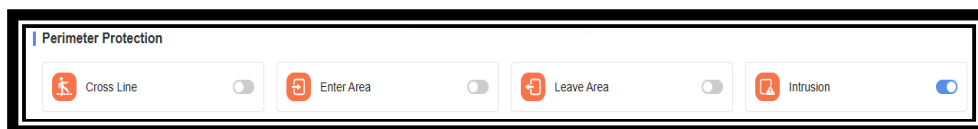
When Enable Schedule is selected, the camera captures and uploads images according to the configured arming schedule.



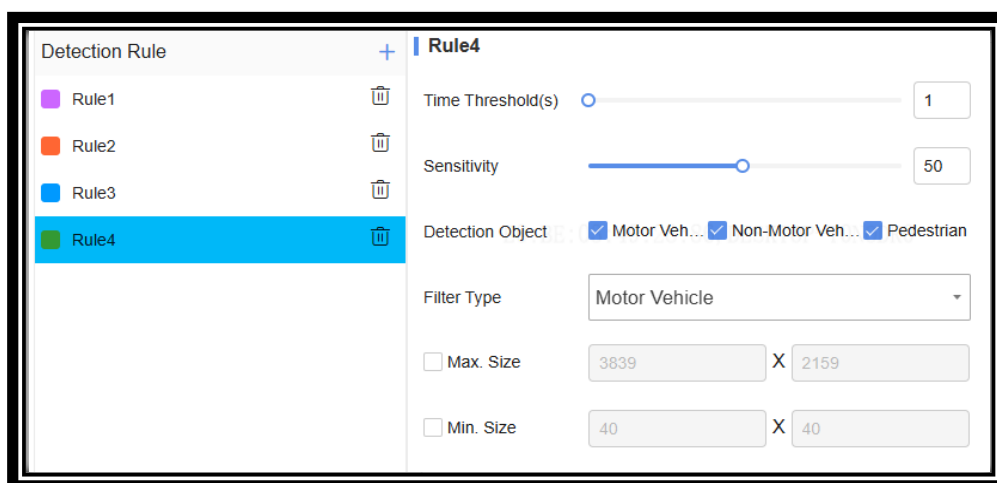
3.1.2 Intrusion Detection

1. Enable Intrusion Detection

Enable Intrusion Detection in Setup > Smart > Intrusion Detection.

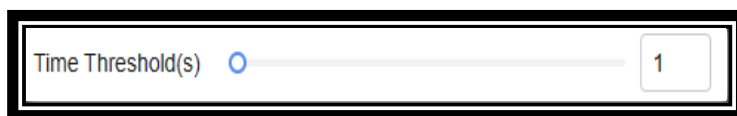


2. Configure Rule Parameters



One or more detection areas can be drawn in the image. The detection area range should not only consider the user's requirements but also match the monitoring distance. These configuration items help set up effective detection areas, ensuring that the monitoring performance meets expectations.

➤ Time Threshold(s)



Indicates the alarm time threshold, that is, an alarm is triggered only when the target stays in the area for longer than this threshold. This parameter applies only to Intrusion Detection.

➤ Other Parameters

Sensitivity, Detection Object, and Filter Type are the same as those in Cross Line Detection, so refer to the parameter configuration in the Cross Line Detection section. These configuration items help more precisely control the alarm conditions and other detection parameters to meet specific monitoring needs.

NOTE! If the application scenario is a parking lot as shown below, the sensitivity can be adjusted to 45 to enter Parking Lot Mode. This mode is applied to parking lot scenarios where multiple vehicles are parked side by side. In such scenarios, mutual occlusion between vehicles causes unstable detection and frequent false alarms for stationary motor vehicles. This mode can significantly improve the accuracy of Intrusion Detection.



Application Scenario Example:



3.1.3 Enter Area

Enter Area is very similar to Intrusion Detection, with the only difference being that Enter Area does not have a Time Threshold(s) parameter.

3.1.4 Leave Area

Leave Area triggers an alarm when a target leaves the detection area, with no time threshold.

NOTE!

When drawing detection areas for perimeter protection, do not fill the entire screen or make the detection area boundaries too close to the image edges.

It is recommended to draw rules according to the area to be monitored, leaving at least 10% of blank space between the detection area boundaries and the image edges to ensure proper algorithm operation and optimal algorithm performance.



Figure 16. Full-Screen Drawing Example.



Figure 17. Detection Area Too Close to the Screen Edge



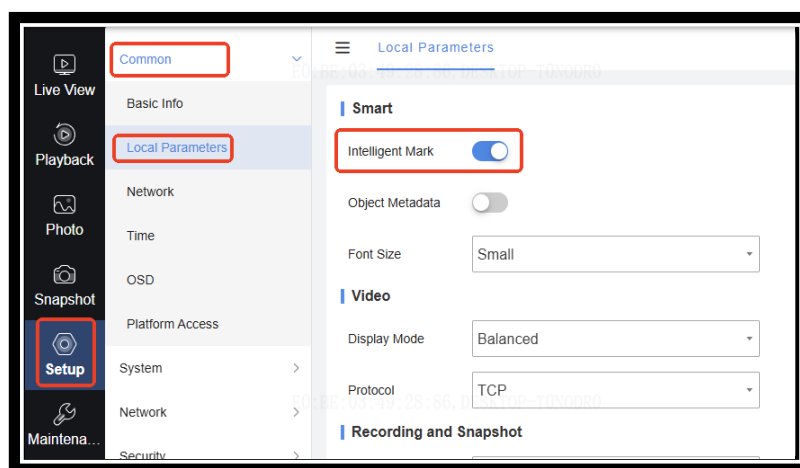
Figure 18. Optimal Example

3.2 Local Configuration

3.2.1 Display Intelligent Mark

Go to Setup > Common > Local Parameters, and enable Intelligent Mark.

When enabled, bounding boxes are displayed for detected objects on the live view page.



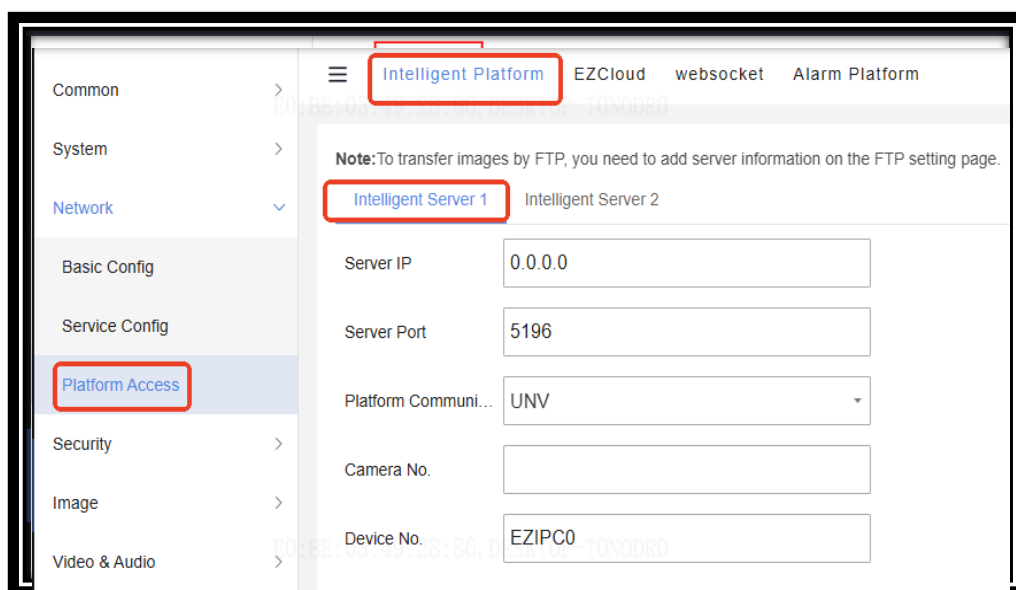
3.3 Server Configuration

The platform communication type dropdown list includes four options: UNV, FTP, and GA/T1400. (All support LAPI, allowing users to enable smart functions on IPCs connected to NVRs)

3.3.1 UNV

UNV is the Uniview proprietary protocol, typically used to connect to Uniview servers for uploading captured images (snapshots). The camera needs to be configured according to actual requirements.

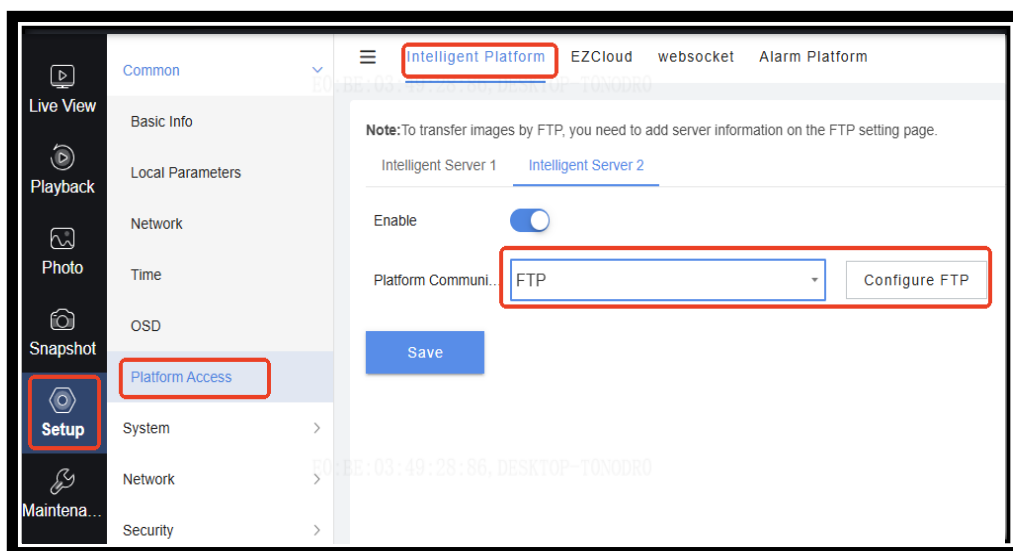
- Server Address: Enter the IP address of the image server.
- Server Port: Enter the port number of the image server.
- Platform Communication Type: Select UNV.
- Camera ID: Fill in as needed.
- Device Code: Fill in as needed.

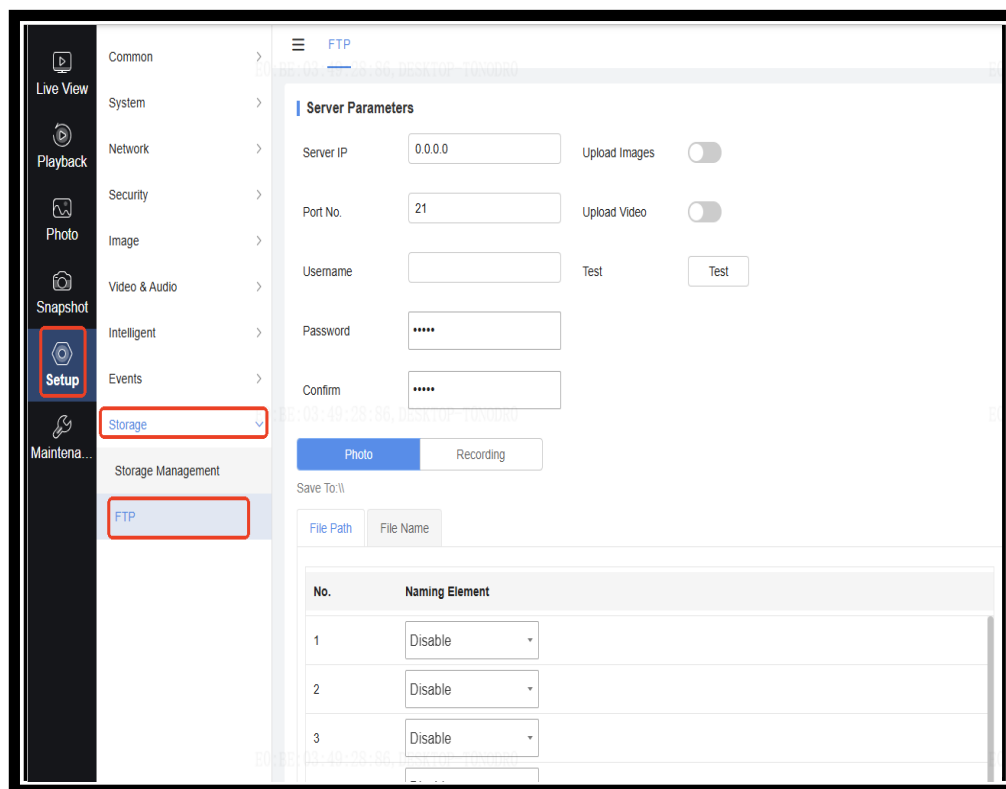


3.3.2 FTP

FTP is the standard FTP protocol, typically used to connect to third-party servers for uploading captured images (snapshots).

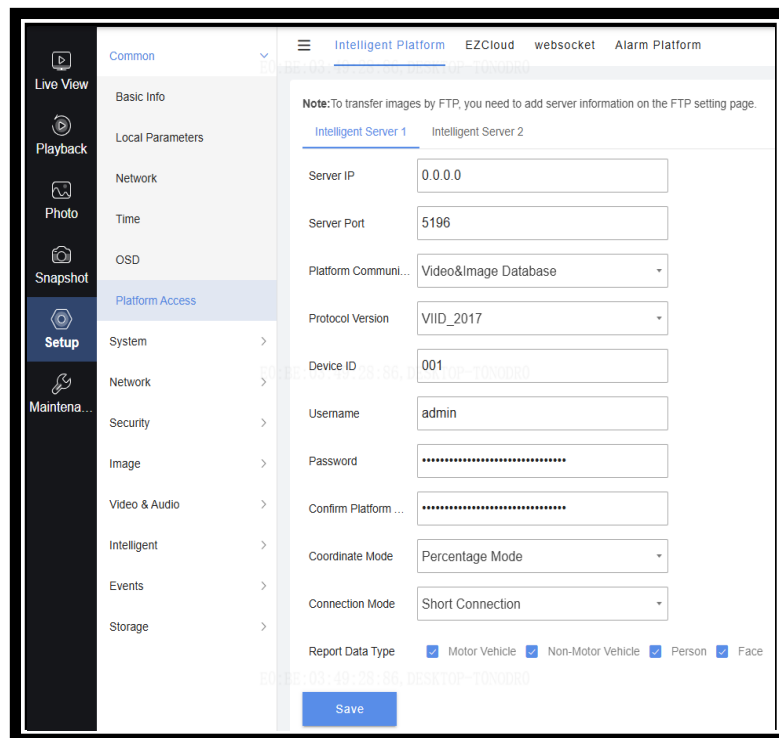
The server parameters and image upload rules must be correctly set on the IPC web page (Setup > Storage > FTP).





3.3.3 GA/T1400

GA/T 1400 is the standard protocol of the national standard, typically used to connect to third-party servers. The camera needs to be configured according to actual requirements.



The screenshot shows the 'Platform Access' configuration page for the 'Intelligent Platform'. The left sidebar contains navigation options: Live View, Playback, Photo, Snapshot, Setup (highlighted), and Maintenance. The 'Setup' menu is expanded, showing sub-options: System, Network, Security, Image, Video & Audio, Intelligent, Events, and Storage. The main content area is titled 'Intelligent Platform' and includes tabs for 'Intelligent Server 1' and 'Intelligent Server 2'. A note at the top states: 'Note: To transfer images by FTP, you need to add server information on the FTP setting page.' The configuration fields for 'Intelligent Server 1' are as follows:

Field	Value
Server IP	0.0.0.0
Server Port	5196
Platform Communi...	Video&Image Database
Protocol Version	VIID_2017
Device ID	001
Username	admin
Password	
Confirm Platform ...	
Coordinate Mode	Percentage Mode
Connection Mode	Short Connection
Report Data Type	☒ Motor Vehicle ☒ Non-Motor Vehicle ☒ Person ☒ Face

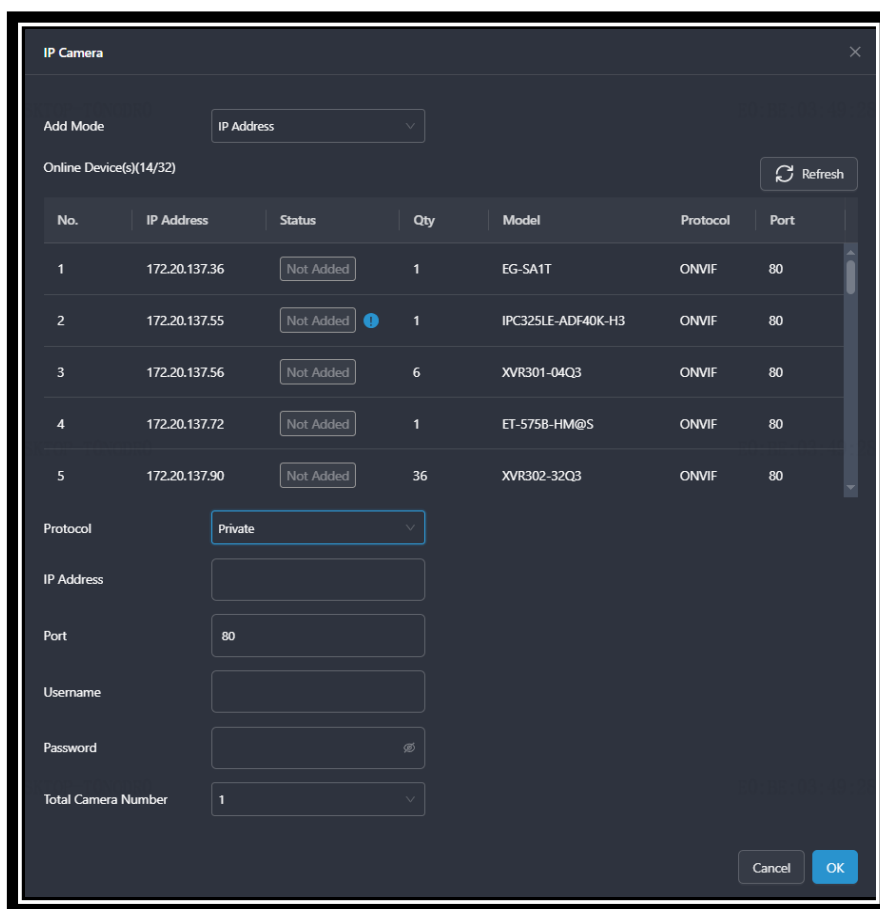
A 'Save' button is located at the bottom of the configuration area.

- Server Address: Enter the IP address of the VIID platform.
- Server Port: Enter the port number of the VIID platform.
- Device ID: A 20-digit code assigned by the VIID platform. Digits 11 through 13 must be 119.
- Platform Access Username: The username for accessing the VIID platform. Assigned by the VIID platform.
- Platform Access Password: Assigned by the VIID platform.

3.4 Using Perimeter Protection on NVR

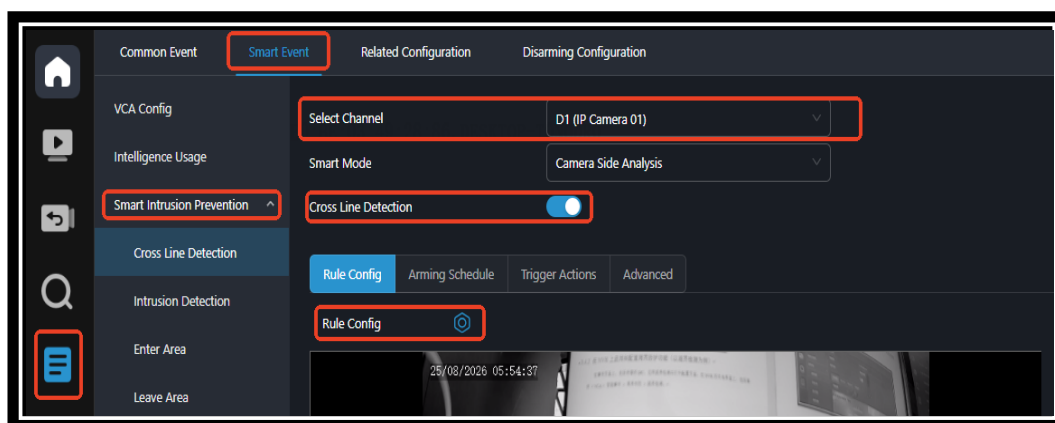
3.4.1 Add Camera to NVR

Add the IPC to the NVR via the Private protocol and check whether the IPC is online.

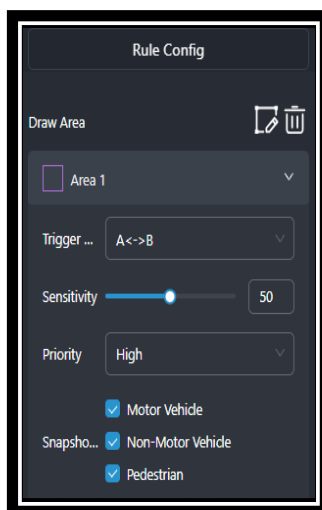


3.4.2 Enable and Configure Perimeter Protection on NVR (Taking Cross Line Detection as an Example)

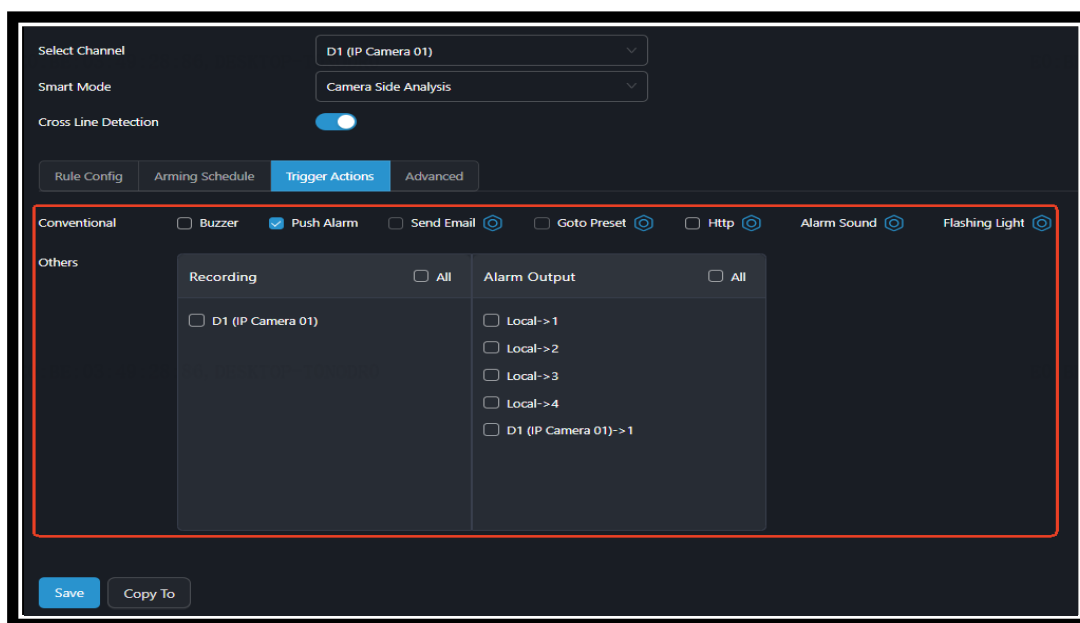
On the Event page, select the desired IPC, enable Cross Line Detection, and open the configuration page. On the NVR local interface, go to Event > VCA > Smart Event > Smart Intrusion Prevention > Cross Line Detection.



Click Rule Configuration to draw rules, set the maximum and minimum sizes, trigger direction, and sensitivity for the target, and save after completing the settings.

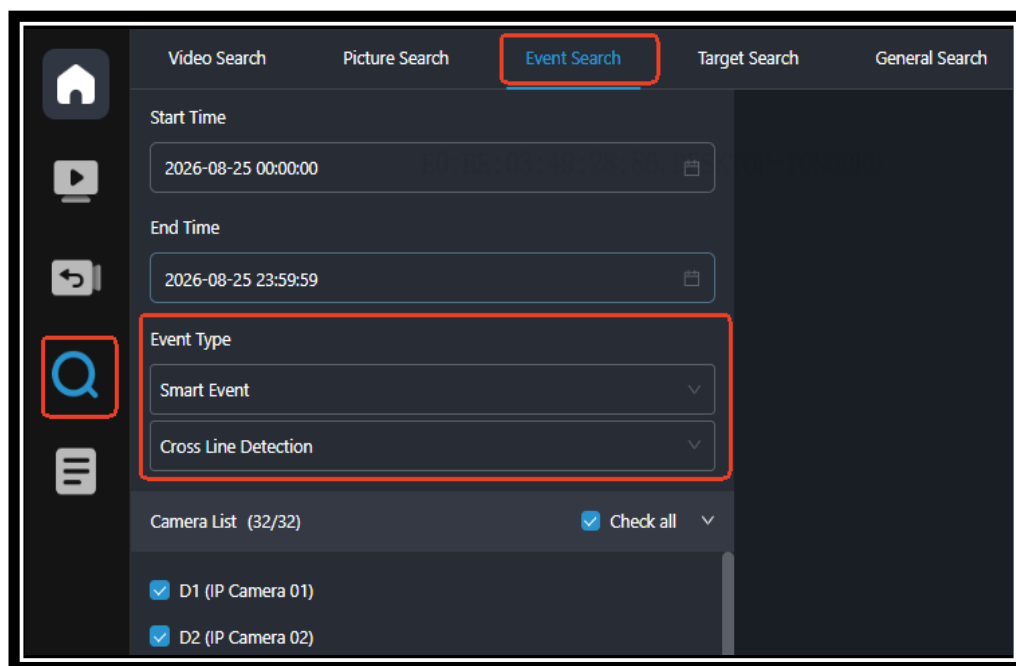


Enable alarm sound and light as needed, and set the actions to trigger on the NVR when a Cross Line Detection event occurs.



3.4.3 Searching Captured Images on the NVR

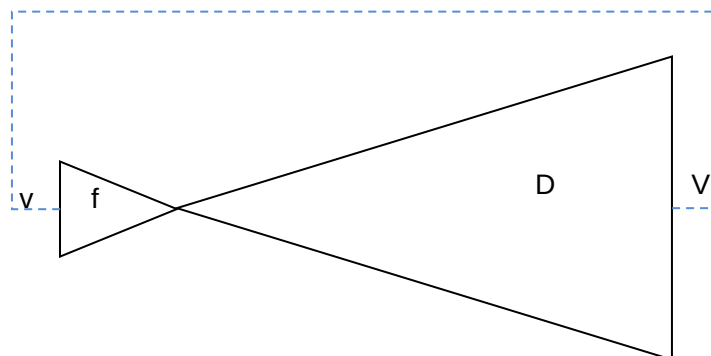
Use the event type condition to search for alarm-triggered snapshots on the NVR local and web interfaces.



4 Appendix

4.1 Calculation Principle

Basically, the imaging of an optical system can be shown as follows:



In the figure, f represents the focal length, D represents the distance, V represents the size of the target object, and v represents the pixel size of the imaged object.

According to the lens imaging principle: $f/v = D/V$, that is, $v = f \cdot V/D$

Since the size of a single pixel p is determined by the device hardware and is known, the number of pixels of the imaged target object can be calculated.