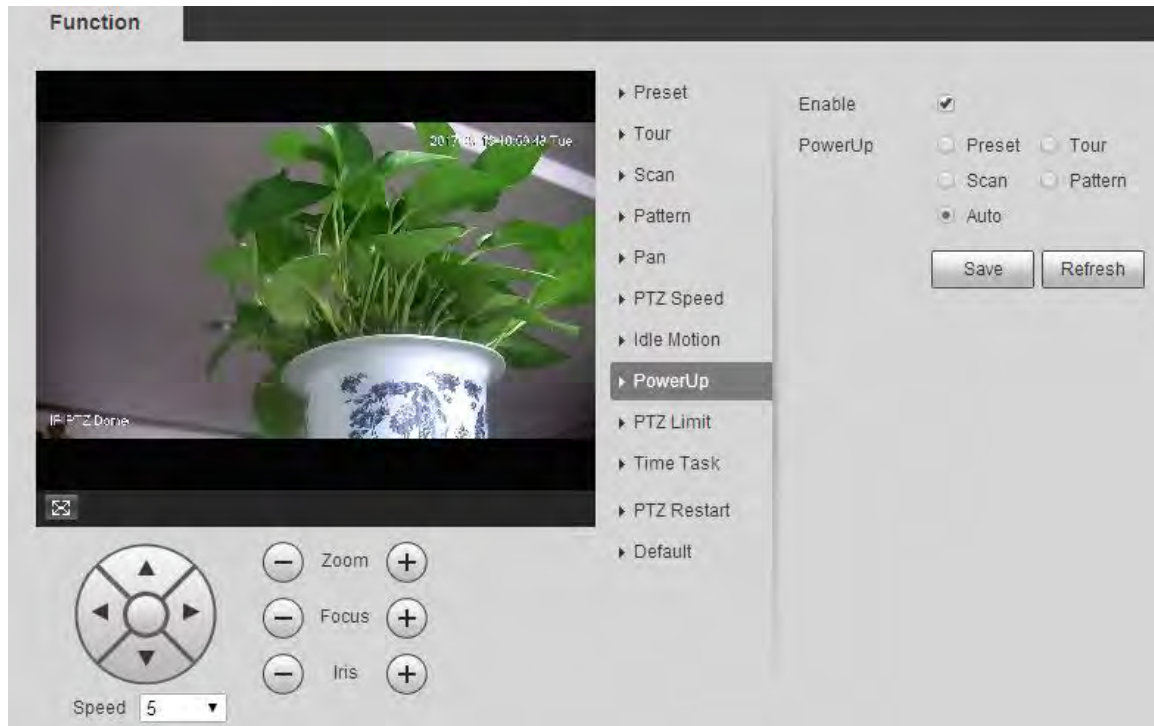


Figure 5-76 PowerUp settings



Step 2 Select the **Enable** checkbox to enable power up motion.

Step 3 Select power up motion from **Preset, Tour, Scan, Pattern** or **Auto**.



Select **Auto** and the last motion before you shut down the Device last time will be performed.

Step 4 Select the action number of the selected motion.

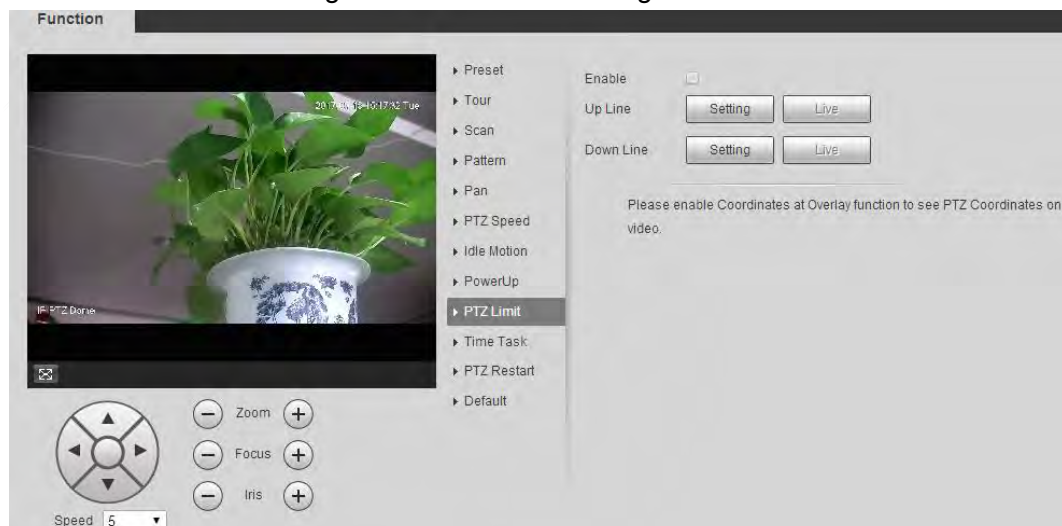
Step 5 Click **Save**.

5.4.2.9 PTZ Limit

After you set the PTZ limit, the Device can only move in the defined area.

Step 1 Select **Setting > PTZ > Function > PTZ Limit**.

Figure 5-77 PTZ limit settings



Step 2 Adjust the PTZ direction, and then click **Setting** to set the **Up Line**.

- Step 3 Adjust the PTZ direction, and then click **Setting** to set the **Down Line**.
- Step 4 Click **Live** to preview the already-set up line and down line.
- Step 5 Select the **Enable** checkbox to enable the PTZ limit function.

5.4.2.10 Time Task

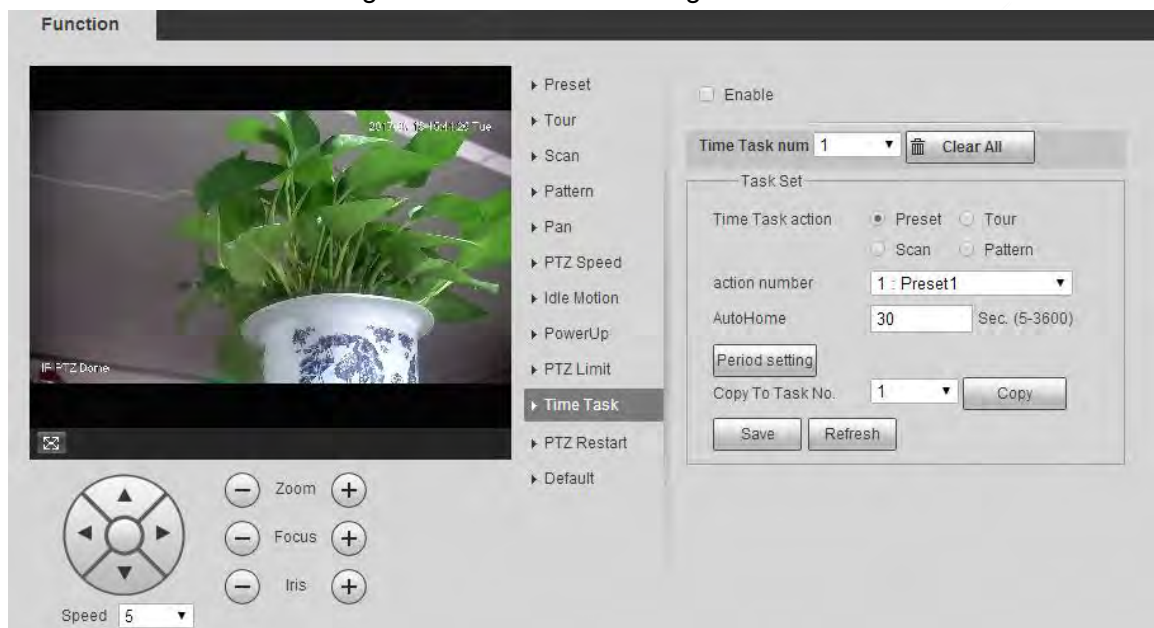
After you set time task, the Device performs the selected motions during the defined period.



Set **Preset, Tour, Scan** or **Pattern** in advance.

- Step 1 Select **Setting > PTZ > Function > Time Task**.

Figure 5-78 Time task settings



- Step 2 Select the **Enable** checkbox to enable time task function.
- Step 3 Set the time task number.



Click **Clear All** to delete all set time tasks.

- Step 4 Select **Time Task** action such as **Preset, Tour, Scan** or **Pattern**.
- Step 5 Select the action number of the selected motion.
- Step 6 Set the time for **AutoHome**.



AutoHome refers to the time needed to automatically recover the time task in case of manually calling the PTZ to stop the time task.

- Step 7 Click **Period setting** to set the period to perform time tasks.
- Step 8 Select the task number to copy settings to the selected task, and then click **Copy**.
- Step 9 Click **Save**.

5.4.2.11 PTZ Restart

- Step 1 Select **Setting > PTZ > Function > PTZ Restart**.

Figure 5-79 PTZ restart



Step 2 Click **PTZ Restart**.
The PTZ is restarted.

5.4.2.12 Default

With the function, you can restore the PTZ to factory defaults.



This function will restore the Device to defaults. Think twice before performing the operation.

Step 1 Select **Setting > PTZ > Function > Default**.

Figure 5-80 Default setting



Step 2 Click **Default**.

The PTZ will be restored to factory defaults.

5.5 Event Management

5.5.1 Video Detection

Video detection includes three event types: **Motion Detection**, **Video Tamper** and **Scene Changing**.

5.5.1.1 Motion Detection

When the moving object appears and moves fast enough to reach the preset sensitivity value, alarms will be triggered.

Step 1 Select **Setting > Event > Video Detection > Motion Detection**.

Figure 5-81 Motion detection settings

Step 2 Select the **Enable** check box, and then configure motion detection parameters.

- Set arming and disarming period.
 1. Click **Setting**, and then set the arming period on the page.

Figure 5-82 Arming period settings

2. Set the alarm period to enable alarm events in the period you set.
 - ◇ There are 6 time periods for each day. Select the check box for the time

- ◇ Select the day of week (**Sunday** is selected by default; If **All** is selected, the setting is applied to the whole week. You can also select the check box next to the day to set it separately).
- 3. After completing the settings, click **Save**.
You will return to the **Motion Detection** page.
- Set the area.
Click **Setting**, and the **Area** page is displayed. Refer to Table 5-25 and Table 5-26 for parameters description. Each color represents a certain region, and you can set different motion detection regions for each area. The detection region can be irregular and discontinuous.

Figure 5-83 Area setting

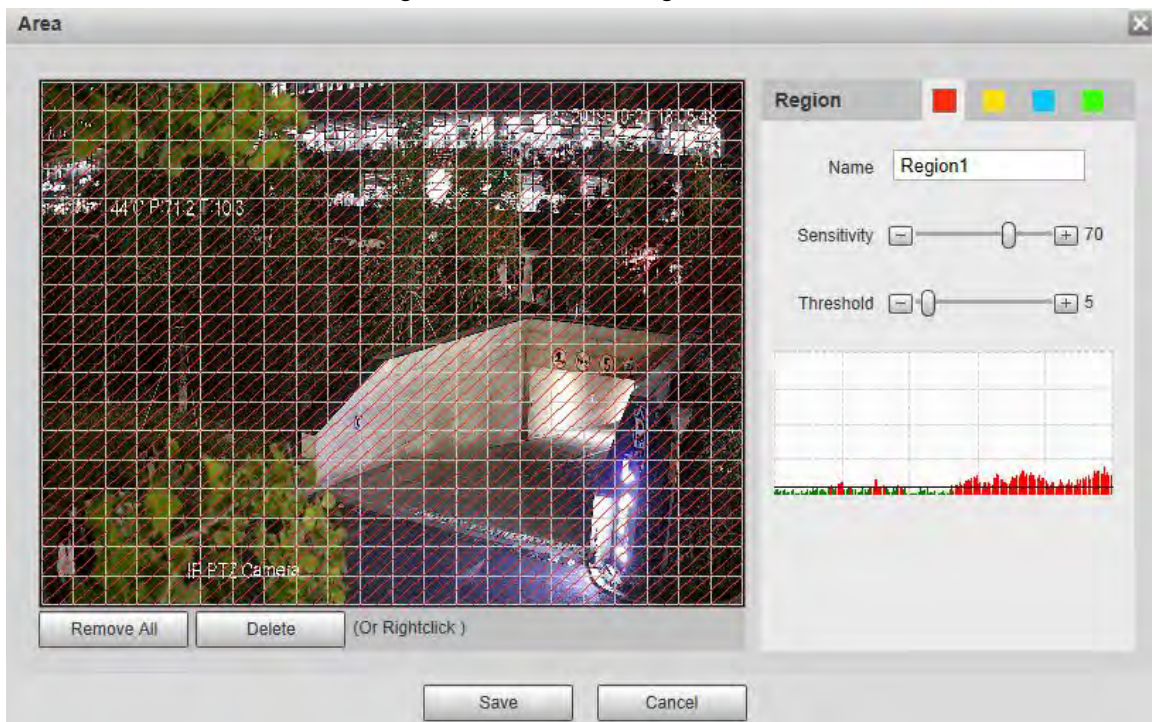


Table 5-25 Description of area setting parameter

Parameter	Description
Name	The default names are Region1, Region2, Region3 and Region4, and the names can be customized.
Sensitivity	Sensitivity to brightness change. The higher the sensitivity is, the easier the motion detection event will occur. You can set different sensitivities for each region, with values ranging from 0 to 100, and 30 to 70 is recommended.
Threshold	Detect the relation between the object and the region. The smaller the threshold is, the easier the motion detection will occur. Set different thresholds for each region, with values ranging from 0 to 100, and 1 to 10 is recommended.
Waveform graph	The red line indicates that motion detection is triggered, and the green line indicates that it is not triggered.
Remove All	Remove all detection regions.
Delete	Delete the detection region of the selected color block.

- Other parameters

Table 5-26 Description of video detection parameter

Parameter	Description
Anti-Dither	The system records only one motion detection event within the defined period. The value range is 0–100 s.
Enable Manual Control Trigger	After you enable the function, the motion detection events that occur when you control the PTZ manually will be excluded. In this way, you can reduce the false alarm rate of such events.
Record	After you enable the function, when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control page.
Record Delay	When the alarm is over, the alarm recording will continue for an extended period of time. The time unit is second, and the value range is 10–300.
Relay-out	Select the check box, and you can enable the alarm linkage output port, and link corresponding relay-out devices after an alarm is triggered.
Alarm Delay	When the alarm is over, the alarm will continue for an extended period of time. The time unit is second, and the value range is 10–300.
Send Email	After you select the check box, when an alarm is triggered, the system sends email to the specified email address. You can configure the email address in "5.2.5 SMTP (Email)."
PTZ	Select PTZ , and then configure the linkage action. When an alarm is triggered, the system links PTZ to rotate to the preset. The Activation options include None , Preset , Tour and Pattern .
Snapshot	Select the Snapshot check box, and then the system takes snapshot automatically when an alarm is triggered. You need to set the alarm snapshot period as described in "5.5.1.2 Snapshot."

Step 3 Click **Save**.

5.5.1.2 Video Tamper

Alarms will be triggered if there is video tampering.

Step 1 Select **Setting > Event > Video Detection > Video Tamper**.

Figure 5-84 Video tamper settings

Step 2 Select the **Enable** check box, and then configure video tamper parameters.



For parameters configuration, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.1.3 Scene Changing

Alarms will be triggered if there is scene changing.

Step 1 Select **Setting > Event > Video Detection > Scene Changing**.

Figure 5-85 Scene changing settings

Step 2 Select the **Enable** check box, and then configure scene changing parameters.



For parameters configuration, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.2 Smart Motion Detection

After you set smart motion detection, when the human, non-motor vehicles and motor vehicles appear and move fast enough to reach the preset sensitivity value, the alarm linkage actions will be performed. The function can help you to avoid the alarms triggered by natural environment change.



- The function depends on the result of motion detection, and all other parameters (except sensitivity) of motion detection function are used, including arming period, area settings, and linkage configurations. If no motion detection is triggered, smart motion detection will not be triggered.
- If motion detection is not enabled, when smart motion detection is enabled, motion detection will also be enabled. If both functions are enabled, when motion detection is disabled, smart motion detection will also be disabled.
- When smart motion detection is triggered and recording is linked, back-end devices can filter recording with human or vehicles through smart search function. For details, see the corresponding user's manual.

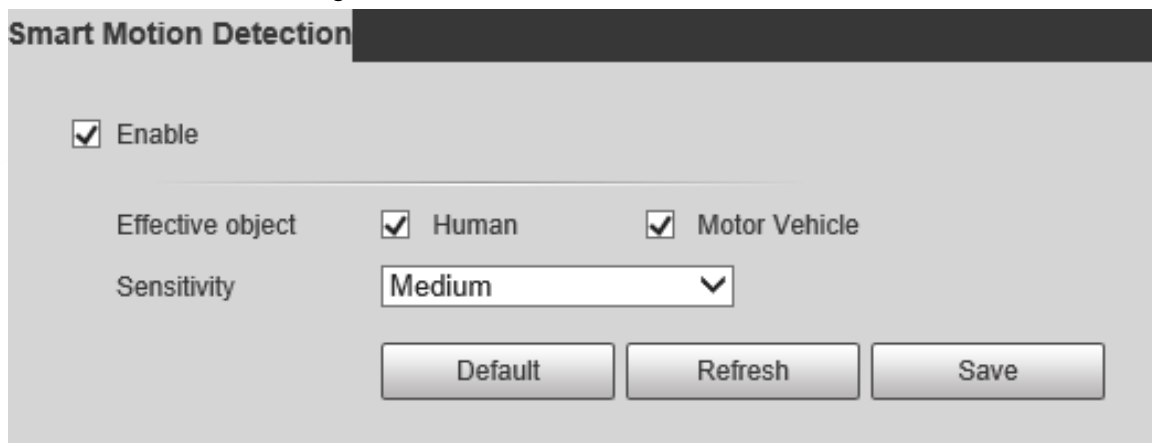
Prerequisites

- Select **Setting > Event > Video Detection > Motion Detection**, and then enable the motion detection function.
- Set the arming period and detection area. The sensitivity of each region is larger than 0, and the threshold is not equal to 100.

Procedure

1. Select **Setting > Event > Smart Motion Detection**.

Figure 5-86 Smart motion detection



2. Select the **Enable** check box to enable **Smart Motion Detection**.

3. Select the effective object and sensitivity.
 - **Effective object:** Select **Human** or **Motor Vehicle**. When **Human** is selected, both people and non-motor vehicles will be detected.
 - **Sensitivity:** Select **High**, **Medium**, or **Low**. The higher the sensitivity, the easier the alarm is triggered.
4. Click **Save**.

5.5.3 Audio Detection

Step 1 Select **Setting > Event > Audio Detection > Audio Detection**.

Figure 5-87 Audio detection settings

Audio Detection

Input Abnormal

Intensity Change

Sensitivity 50

Threshold 50

Period

Anti-Dither s (0~100)

Record

Record Delay s (10~300)

Relay-out

Alarm Delay s (10~300)

Send Email

PTZ

Snapshot

Step 2 Configure audio detection parameter.

Table 5-27 Description of audio detection parameter

Parameter	Description
Input Abnormal	Select Input Abnormal , and then an alarm is triggered when there is abnormal audio input.
Intensity Change	Select Intensity Change , and then an alarm is triggered when the change in sound intensity exceeds the defined threshold.
Sensitivity	The value ranges from 1 to 100. The smaller this value is, the larger the input sound volume changes are needed for it to be judged as an audio anomaly. You need to adjust it according to the actual condition.
Threshold	The value ranges from 1 to 100. Configure the ambient sound intensity you need to filter. The louder the ambient noise is, the larger this value shall be. You need to adjust it according to the actual condition.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.4 Smart Plan

Smart plans include IVS, face recognition, heat map, people counting, video metadata, construction monitoring and so on. Only after smart plans have been enabled, can the corresponding smart function come into effect.



Before configuring the smart plan, you need to set presets in advance. For setting methods, see "5.4.2.1 Preset".

Step 1 Select **Setting > Event > Smart Plan**.

Figure 5-88 Smart plan (1)

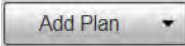


Step 2 (Optional) Click  to enable **Auto Tracking**.

When enabling auto tracking, you do not need to configure smart plans, and the Device performs auto tracking based on internal mechanism. If auto tracking and alarm track of the smart plan (such as IVS) are both enabled, the Device perform tracking in the order of triggering time.



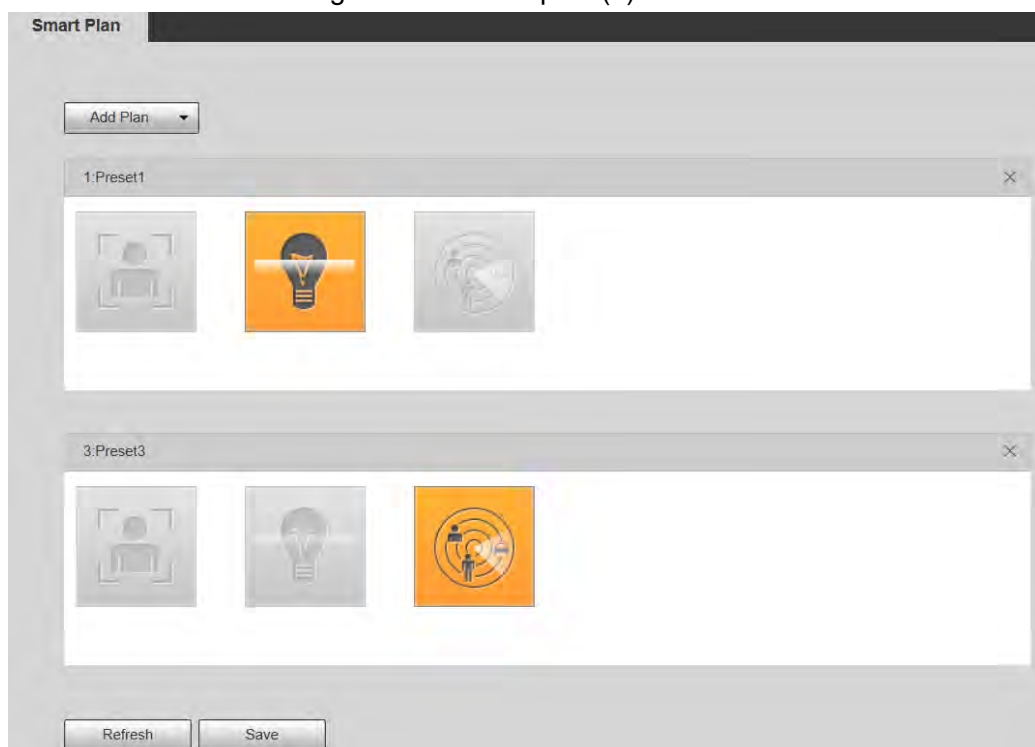
It is recommended to disable auto tracking when alarm track is enabled to avoid disordered tracking.

Step 3 Click  to select the presets to be configured.

Step 4 Select smart plans.

The selected function will be highlighted. Click it again to cancel the selection.

Figure 5-89 Smart plan (2)



Step 5 Click **Save**.

5.5.5 IVS

Basic Requirements for the Scene

- The target size shall not exceed 10% of the image.
- The pixel of the target shall be no less than 10×10; the pixel of abandoned object shall be no less than 15×15 (CIF image); the width and height of the target shall be no more than 1/3 of the image. It is recommended that the height of the target is 10% of the image.
- The brightness difference between the target and the background is no less than 10 gray values.
- The target shall be present in the image for no less than 2 consecutive seconds, and the moving distance shall be larger than its width and no less than 15 pixels (CIF image).

- Try to reduce the complexity of monitoring scenes. It is not recommended to enable IVS in scenes with dense targets and frequent light changes.
- Try to avoid the following scenes: scenes with reflective surfaces such as glass, bright ground or water; scenes that disturbed by tree branches, shadows or winged insects; scenes that against light or under direct light exposure.

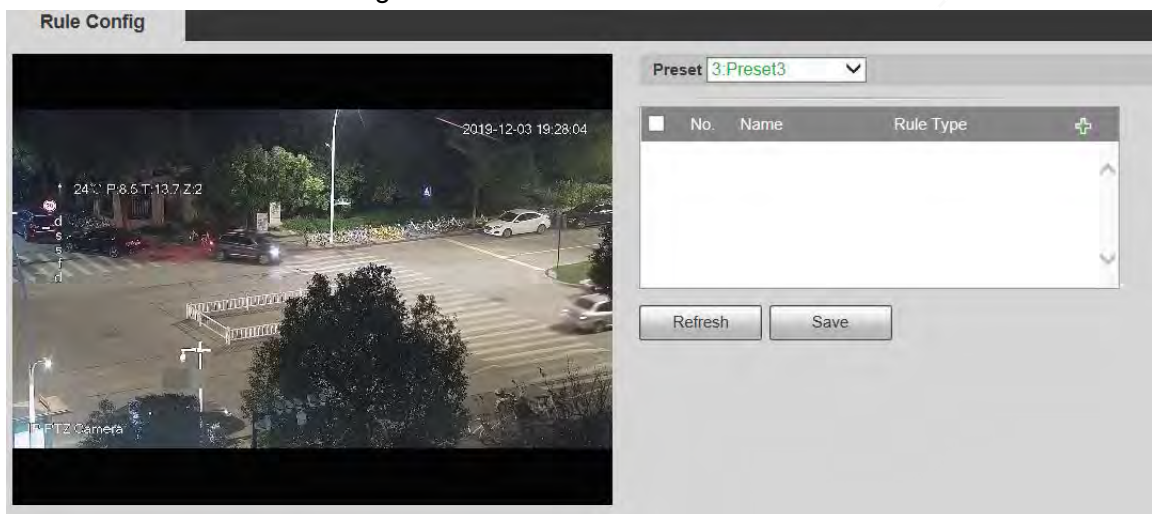



Before using the function, you need to set presets in advance. For setting methods, see "5.3.2.1 Preset."

Rule Config

1. Select **Setting > Event > IVS > Rule Config**.

Figure 5-90 Add smart rules



2. Select the presets to be configured with smart rules.
3. Click  to add smart rules.



Double-click rule type to modify the type of rules.

4. Click **Save**.

5.5.5.1 Tripwire

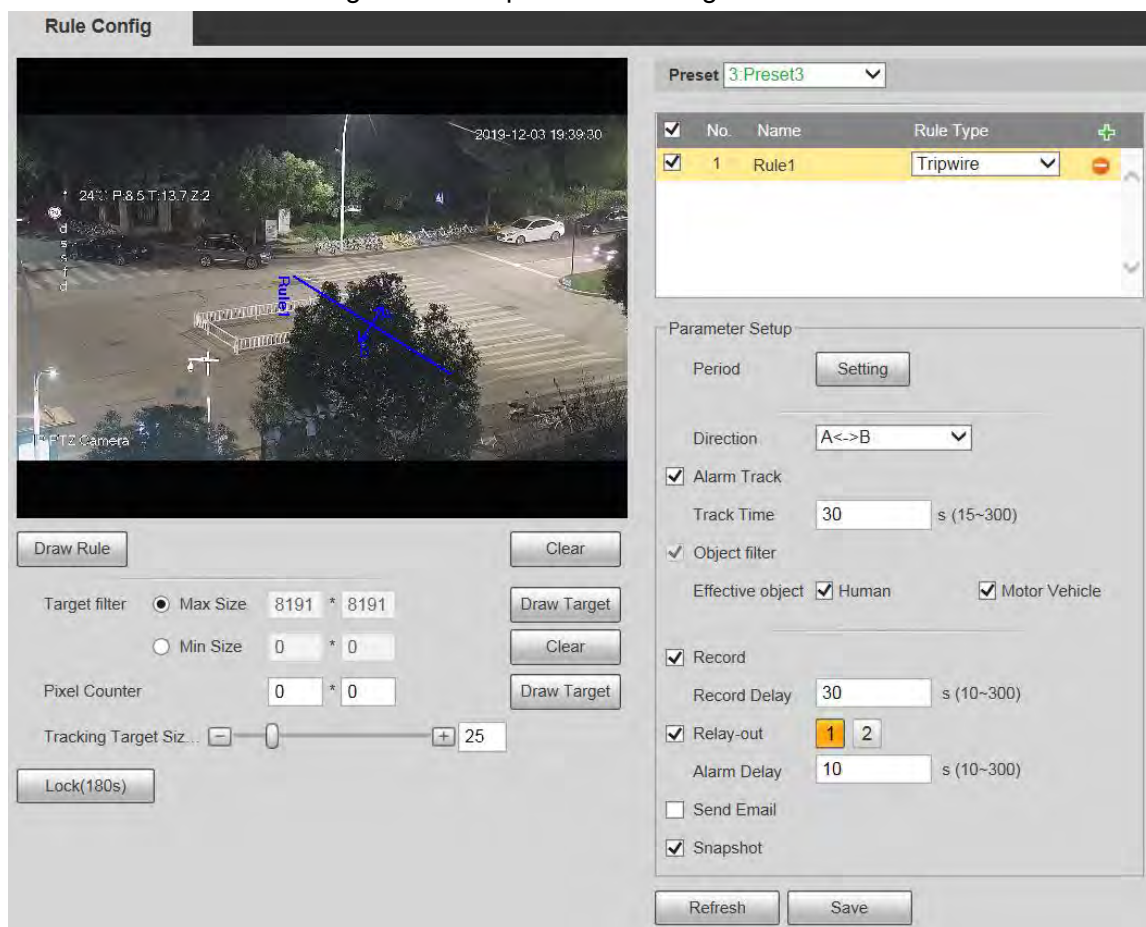
Alarms are triggered when the target crosses the warning line in the defined direction. It requires certain stay time and moving space for the target to be confirmed, so you need to leave some space at both sides of the warning line during configuration and do not draw it near obstacles.

Applicable scenes: Scenes with sparse targets and no occlusion between targets, such as perimeter protection of unattended areas.

Procedure

- Step 1 Select **Tripwire** from the **Rule Type** list.

Figure 5-91 Tripwire rule settings




Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.



Click **Clear** to the right of **Draw Rule** to clear all drawn rules.

Table 5-28 Description of rule drawing parameter

Parameter	Description
Max Size	Set the size range of detection targets to be filtered, and select the maximum or minimum size. <ul style="list-style-type: none"> Max Size: Set the maximum size of targets to be filtered. When the target is larger than this size, the system will ignore it. The unit is pixel. Min Size: Set the minimum size of targets to be filtered. When the target is smaller than this size, the system will ignore it. The unit is pixel.
Min Size	
Pixel Counter	Help to accurately draw the target area. Enter the length and width of the target area in Pixel Counter , and click Draw Target to generate the target area in the monitoring screen. The unit is pixel.

Parameter	Description
Lock/Unlock	<p>Enter the rule configuration page, and the locking function will be automatically enabled, and the locking time is 180 s. During this period, the device cannot track the target. Click Unlock to release the control.</p>  <p>The locking function only takes effect in the rule configuration page. After switching to the Live page, the Device can track the target normally.</p>

Step 3 Configure tripwire parameter.

Table 5-29 Description of tripwire parameter

Parameter	Description
Period	<p>Set the alarming period to enable alarm events in the defined period.</p> <ol style="list-style-type: none"> 1. Click Setting, and then the Period interface is displayed. 2. Enter the time value or press and hold the left mouse button, and drag directly on the setting interface. There are six periods for each day. Select the check box next to the period for it to take effect. 3. Select the day of week (Sunday is selected by default; If All is selected, the setting is applied to the whole week. You can also select the check box next to the day to set it separately). 4. After completing the setting, click Save to go back to the rule configuration interface.
Direction	Configure the tripwire direction. You can select A->B , B->A or A<->B .
Alarm Track	Select the check box, and there will be alarm tracking when a smart rule is triggered.
Track Time	Set the alarm tracking time.
Record	Select the check box, and when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control interface.
Record Delay	When the alarm is over, the recording will continue for an extended period of time. The value range is 10–300 s.
Relay-out	Select the check box, and you can enable the alarm linkage output port, and link corresponding relay-out devices when an alarm is triggered.
Alarm Delay	When the alarm is over, the alarm will continue for an extended period of time. The value range is 10–300 s.
Send Email	Select the Send Email check box, and when an alarm is triggered, the system sends an email to the specified mailbox. You can configure the mailbox in Setting > Network > SMTP (Email) .
Snapshot	Select the check box, and the system will automatically take snapshots in case of alarms. You need to set snapshot period in Storage > Schedule .

Step 4 Click **Save**.

5.5.5.2 Intrusion

Intrusion includes crossing areas and in-area functions.

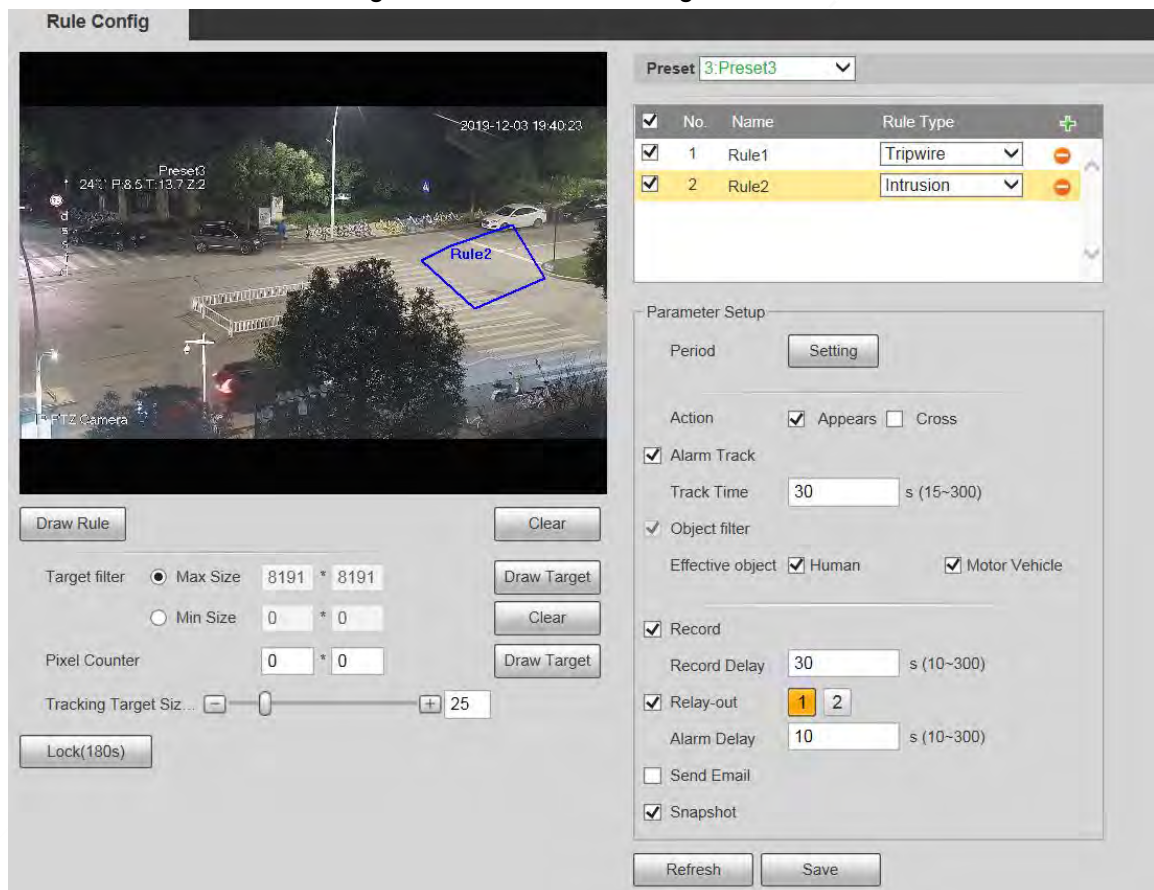
- Crossing area means an alarm will be triggered when a target enters or leaves the area.
- In-area function means an alarm will be triggered when a specified number of targets appear in a set alarming area at a given time. In-area function only counts the number of targets in the detection area, regardless of whether they are the same targets.
- For the reporting time interval of the in-area functions, the system will trigger the first alarm and then detect whether the same event occurs in the interval period. If no same event occurs in this period, the alarm counter will be cleared.

Similar to the warning line, to detect an entry/exit event, a certain movement space should be reserved at the periphery of the area line.

Applicable scenes: Scenes with sparse targets and no occlusion between targets, such as perimeter protection of unattended areas.

Step 1 Select **Intrusion** from the **Rule Type** list.

Figure 5-92 Intrusion settings



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-28.



Click **Clear** to the right of **Draw Rule** to clear all drawn rules.

Step 3 Configure intrusion parameter.

Table 5-30 Description of intrusion parameter

Parameter	Description
Action	Configure intrusion action, and you can select Appear or Cross .
Direction	Select the crossing direction from Enters , Exits , and Enter & Exit .



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.5.3 Abandoned Object

An alarm will be triggered when the selected target in the monitoring scene stays in the screen for more than the defined time.

Pedestrians or vehicles that stay for too long would be regarded as abandoned objects. To filter out such alarms, you can use **Target filter**. In addition, the duration can be properly extended to avoid false alarm due to a short stay of people.

Applicable scenes: Scenes with sparse targets, no obvious and frequent light changes. For scenes with intensive targets or too many obstacles, missed alarms would increase; for scenes in which too many people stay, false alarms would increase. Select detection areas with simple texture, because this function is not applicable to scenes with complex texture.

Step 1 Select **Abandoned Object** from the **Rule Type** list.

Figure 5-93 Abandoned object settings

The screenshot shows the 'Rule Config' interface. On the left, a video feed displays a street scene with a blue rectangular rule area labeled 'Rule3'. Below the video are controls for 'Draw Rule', 'Clear', 'Target filter' (Max Size: 8191 * 8191), 'Pixel Counter' (0 * 0), 'Tracking Target Siz...' (25), and 'Lock(180s)'. On the right, the 'Parameter Setup' section includes a 'Preset' dropdown (3.Preset3), a table of rules, and various time-based settings.

No.	Name	Rule Type
1	Rule1	Tripwire
2	Rule2	Intrusion
3	Rule3	Abandoned Ot

Parameter Setup:

- Period: Setting
- Duration: 10 s (6~3600)
- Alarm Track: Track Time 30 s (15~300)
- Record: Record Delay 30 s (10~300)
- Relay-out: 1 2
- Alarm Delay: 10 s (10~300)
- Send Email
- Snapshot

Buttons: Refresh, Save

Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.

For parameter description, see Table 5-28.



Click **Clear** to the right of **Draw Rule**, and you can clear all drawn rules.

Step 3 Configure abandoned object parameter.

Table 5-31 Description of abandoned object parameter

Parameter	Description
Duration	For abandoned object, the duration is the shortest time to trigger an alarm after an object is abandoned.



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.5.4 Missing Object

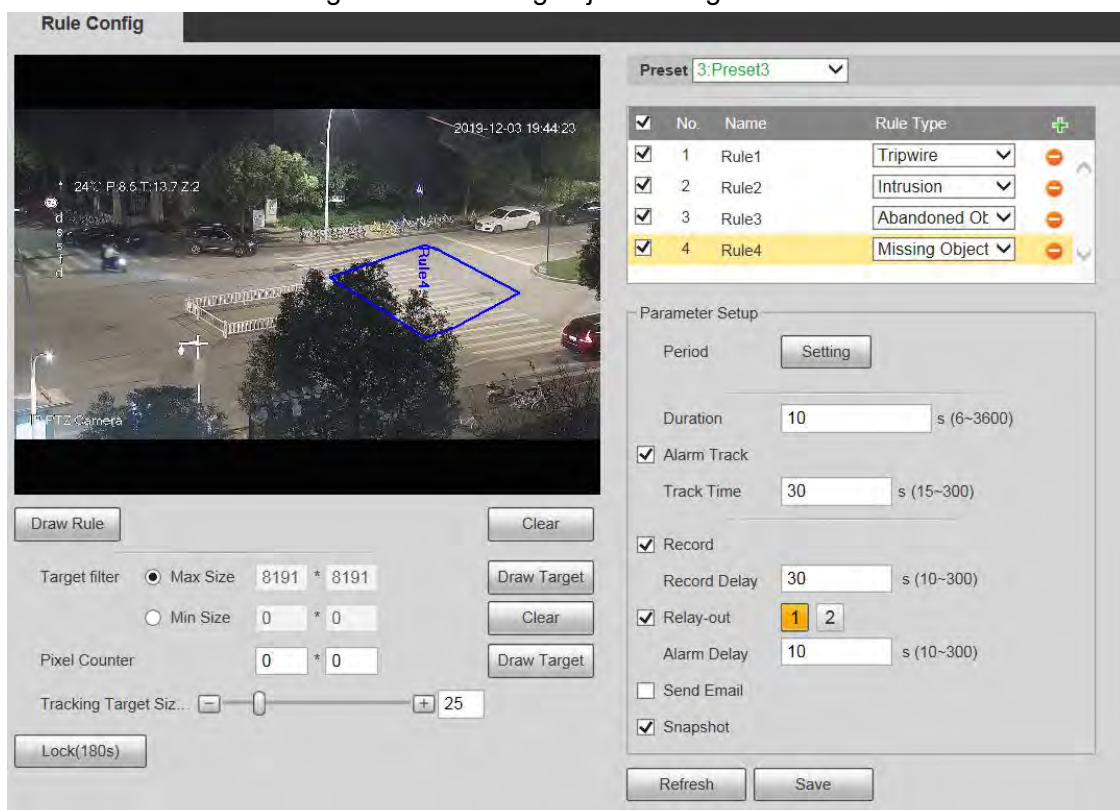
An alarm will be triggered when the selected target in the scene is taken away for the time longer than the set duration.

The system analyzes static areas from the foreground, and determines whether it is missing object or abandoned object from the similarity of its foreground and background. When the time exceeds the set period, an alarm is triggered.

Applicable scenes: Scenes with sparse targets, no obvious and frequent light changes. For scenes with intensive targets or too many obstacles, the missed alarm would increase; for scenes in which too many people stay, the false alarm would increase. Keep the detection area texture as possible simple as possible, because this function is not applicable to scenes with complex texture.

Step 1 Select **Missing Object** from the **Rule Type** list.

Figure 5-94 Missing object setting



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen.
For parameter description, see Table 5-28.



Click **Clear** to the right of **Draw Rule** to clear all drawn rules.

Step 3 Configure missing object parameter.

Table 5-32 Description of missing object parameter

Parameter	Description
Duration	Configure the shortest time from the object disappearing to the alarm being triggered.



For other parameters, see "5.5.5.1 Tripwire".

Step 4 Click **Save**.

5.5.6 Construction Monitoring

The Device can be used for construction monitoring which include helmet detection, workwear detection, lone working detection and absence detection.

Prerequisites

Select **Setting > Event > Smart Plan** to enable **Construction Monitoring**.

Procedure

Step 1 Select **Setting > Event > Construction Monitoring**.

Step 2 Select **Global** or a preset from the **Preset** list.

- If global plan is selected, detection area and rule are set by default, and the detection area cannot be changed.
- If a preset is selected, you need to set detection area and rule manually. The following section uses selecting Preset 1 as an example.

Figure 5-95 Global plan

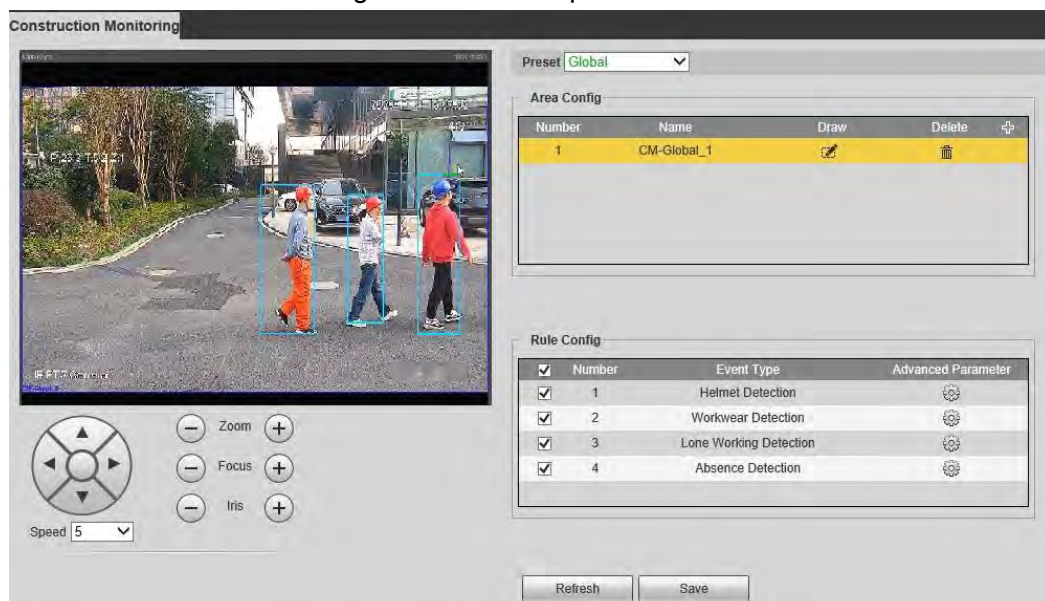
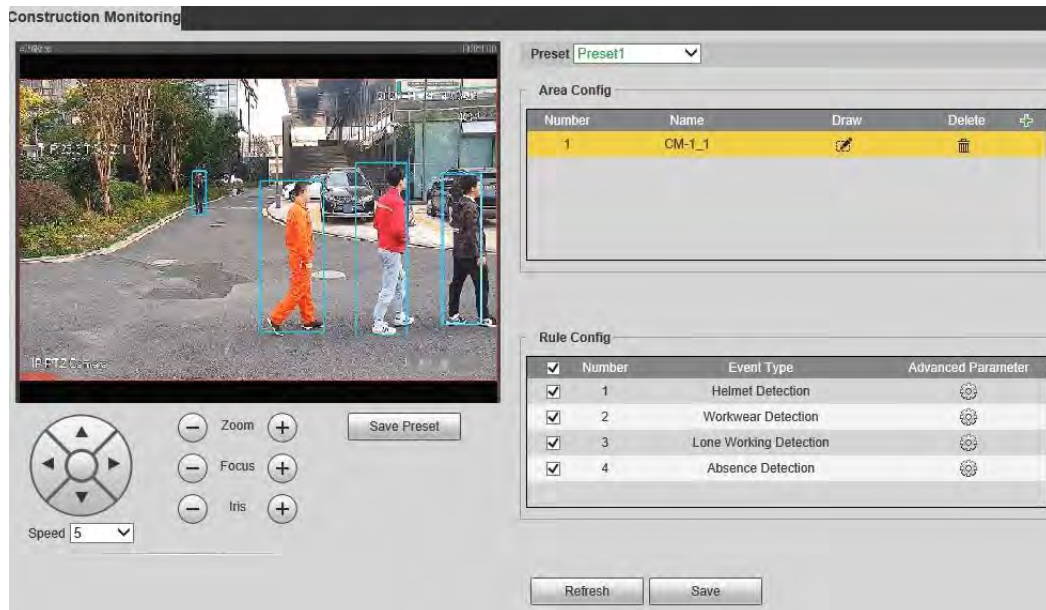


Figure 5-96 Plan by preset



Step 3 Click at the upper-right corner of the **Area Config** section.



Double click the rule name to modify it.

Step 4 Click to draw rule box on the video image, and then right-click to complete drawing.



- After drawing is complete, drag the corners of the drawn area to adjust the detection area.
- If you select preset plan, 8 detection areas can be drawn at most.

Step 5 Select the check box before the event type to enable the corresponding detection rule.

Table 5-33 Rule description

Rule	Description
Helmet Detection	When the Device detects person not wearing helmet or not wearing helmet in the specified color, alarm linkage actions will be performed.
Workwear Detection	When the Device detects person not wearing workwear in accordance with the rule, alarm linkage actions will be performed. The rule for workwear is long-sleeved tops and trousers in the same color. If short-sleeved shirts, shorts or different colors are detected, it means the rule is not followed.
Lone Working Detection	When the Device detects a single person working in the detection area, alarm linkage actions will be performed.
Absence Detection	When the Device detects nobody working in the detection area, alarm linkage actions will be performed.

Step 6 Click next to the detection rule, configure parameters on the **Advanced Parameter** interface, and then click **Save**.

Figure 5-97 Helmet detection

Advanced Parameter

Rule Parameter

Allowed Color

White Yellow Red Blue

Duration s (1~3600)

Repeat Alarm Time s (10~3600)

Record

Record Delay s (10~300)

Relay-out

Alarm Delay s (10~300)

Send Email

Audio Linkage

Play Count (1~3)

File

Message Link

Snapshot

Period

Figure 5-98 Workwear detection

Advanced Parameter

Rule Parameter

Duration s (1~3600)

Repeat Alarm Time s (10~3600)

Record

Record Delay s (10~300)

Relay-out

Alarm Delay s (10~300)

Send Email

Audio Linkage

Play Count (1~3)

File

Message Link

Snapshot

Period

Figure 5-99 Lone working detection

Figure 5-100 Absence detection

Table 5-34 Parameter description

Parameter	Description
Allowed Color	When configuring helmet detection, you can set allowed colors. When the helmet detected is not in the selected colors, alarms will be triggered.

Parameter	Description
Duration	When events not following the rule are detected and the duration exceeds the defined value, alarms will be triggered. For example, when the duration of helmet detection is 5 seconds, if the Device detects a person not wearing helmet or the helmet color is not allowed for more than 5 seconds, an alarm will be triggered.
Repeat Alarm Time	After an alarm is triggered, when the event lasts for the time reaching repeated alarm time, an alarm will be triggered again.
Record	After you enable the function, when an alarm is triggered, the system will start recording automatically. Before using the function, you need to set the recording period of the alarm in Storage > Schedule , and select Auto for Record Mode on the Record Control interface.
Record Delay	When an alarm is over, the alarm recording will continue for an extended period of time.
Relay-out	Select the check box, and you can enable the alarm linkage output port, and link corresponding relay-out devices after an alarm is triggered.
Alarm Delay	When an alarm is over, the alarm will continue for an extended period of time.
Send Email	After you select the check box, when an alarm is triggered, the system sends email to the specified email address. You can configure the email address in "5.2.8 SNMP".
Audio Linkage	Select the check box to play alarm audio when alarms are triggered. You can set the play count and select the audio file. For how to set the audio file, see "5.1.3.2 Configuring Alarm Audio".
Message Link	Select the check box to receive message when alarms are triggered.
Snapshot	Select the check box, and the system will automatically take snapshots in case of alarms. You need to set snapshot period in Storage > Schedule .
Period	Set the alarm period to enable alarm events in the defined period. <ol style="list-style-type: none"> 1. Click Setup, and the Period interface is displayed. 2. Enter the time value or press and hold the left mouse button, and drag directly on the setting interface. There are six periods for each day. Select the check box next to the period for it to take effect. 3. Select the day of week (Sunday is selected by default; If All is selected, the setting is applied to the whole week. You can also select the check box next to the day to set it separately). 4. After completing the setting, click Save to go back to the rule configuration interface.

Step 7 Click **Save** on the **Construction Monitoring** interface.



If you want to see the alarm information on the **Alarm** tab, you need to subscribe the corresponding alarm type. For details, see "6 Alarm".

Result

Click the **AI Live** tab to view construction monitoring results. For details, see "3.2 AI Live Settings".

5.5.7 Face Recognition

The function can detect faces and compare them with those in the configured face database.



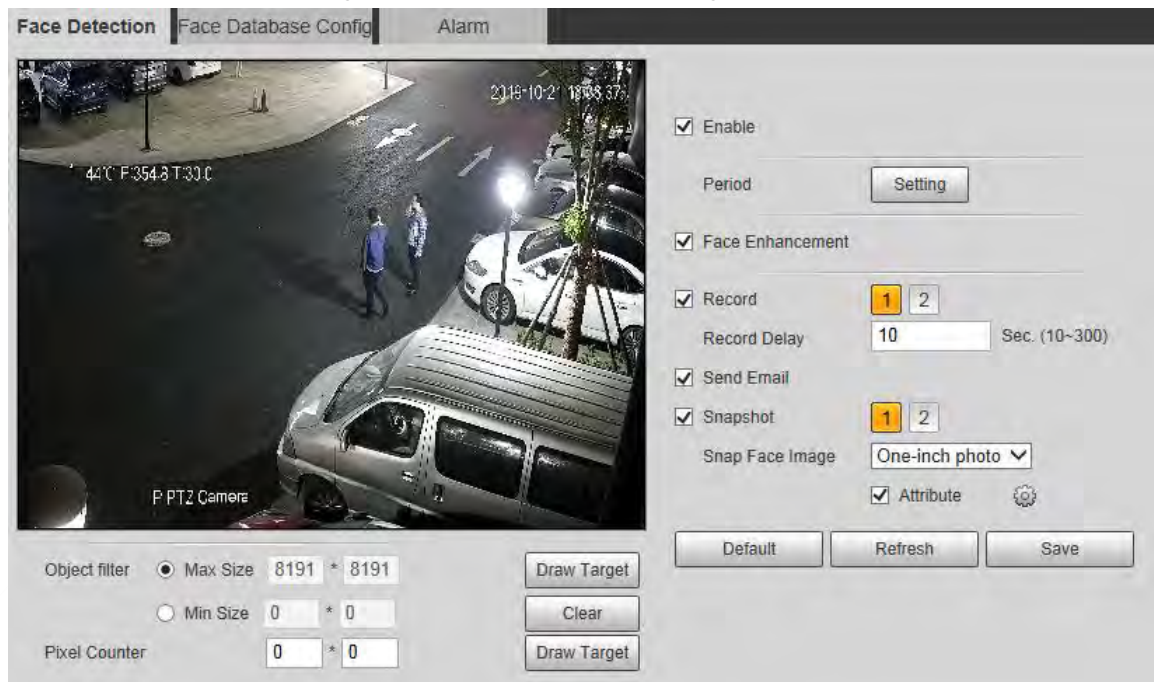
- Select **Setting > Event > Smart Plan** to enable face recognition.
- This function is available on select models.

5.5.7.1 Face Detection

When human face is detected in the monitoring screen, an alarm is triggered and the linked action is performed.

Step 1 Select **Setting > Event > Face Recognition > Face Detection**.

Figure 5-101 Face detection page






Step 2 Select **Enable** to enable the face detection function.

Step 3 Configure face detection parameters.

Table 5-35 Description of face detection parameter

Parameter	Description
Period	Alarm event will be triggered only within the defined period. For details, see "5.5.1.1 Motion Detection".

Parameter	Description
Face Enhancement	Select Face Enhancement to preferably guarantee clear faces with low stream.
Record	<p>Select Record, and the system records video when alarms are triggered.</p>  <p>To enable video recording, you need to make sure that:</p> <ul style="list-style-type: none"> • The motion detection recording is enabled. For details, see "5.6.1.1 Record". • The auto recording is enabled. For details, see "5.6.4 Record Control".
Record Delay	The video recording will not stop until the record delay time you set has passed.
Send Email	Select Send Email , and when alarms are triggered, the system sends email to the specified mailbox. For the email settings, see "5.2.5 SMTP (Email)".
Snapshot	<p>Select Snapshot, and the system takes snapshot when alarms are triggered.</p>  <ul style="list-style-type: none"> • Enable the motion detection snapshot first. For details, see "5.6.1.1 Record". • For searching and setting snapshot storage path, see "5.1.2.5 Path".
Snap Face Image	Set the snapshot scope, including Face and One-inch photo .
Attribute	Select the Attribute check box, click  , and then you can set the human attributes during face detection.

Step 4 Click **Save**.

5.5.7.2 Face Database Config

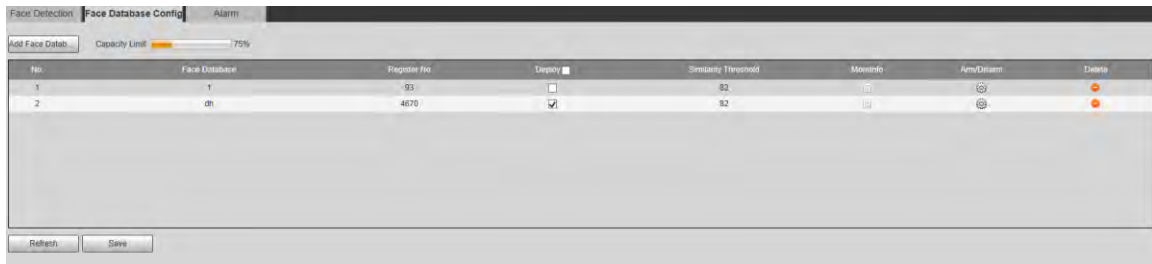
After you successfully configure the face database, the detected faces can be compared with the information in the face database. Configuring a face database includes creating a face database, adding face images, and face modeling.

5.5.7.2.1 Adding Face Database

Create a face database, and then register face images to add face images to the newly created face database.

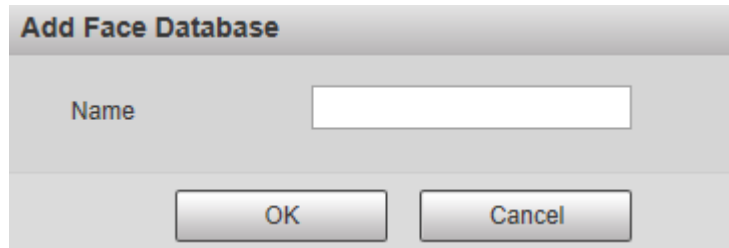
Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

Figure 5-102 Face database config



Step 2 Click **Add Face Database**.

Figure 5-103 Add face database



Step 3 Set face database name.

Step 4 Click **OK** to complete the addition.

Figure 5-104 Add face database completed



Step 5 Configure face database configuration parameters.

Table 5-36 Description of face database config parameter

Parameter	Description
Deploy	Select Deploy and the face database takes effect.
Similarity Threshold	The comparison is successful only when the similarity between the detected face and the face feature in face database reaches the set similarity threshold. After this, the comparison result is displayed on the Live page.
More Info	Click More Info to manage face database. You can set search conditions, register people, and modify people information.
Arm/Disarm	Alarm event will be triggered only within the defined time period. For details, see "5.5.1.1 Motion Detection".
Delete	Delete the selected face database.

5.5.7.2.2 Adding Face Images

You can add face images to the created face database. Manual addition and batch import are supported.

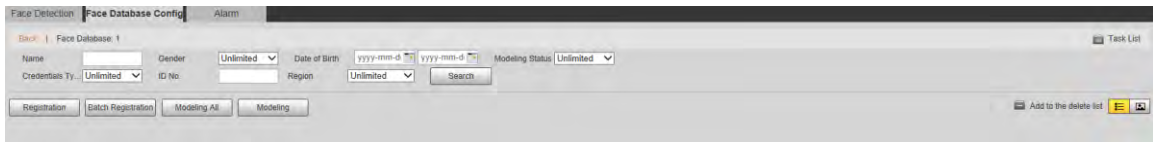
Manual Addition

Add a single face image. Use this method when registering a small number of face images.

Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

Step 2 Click **More Info** for the face database to be configured.

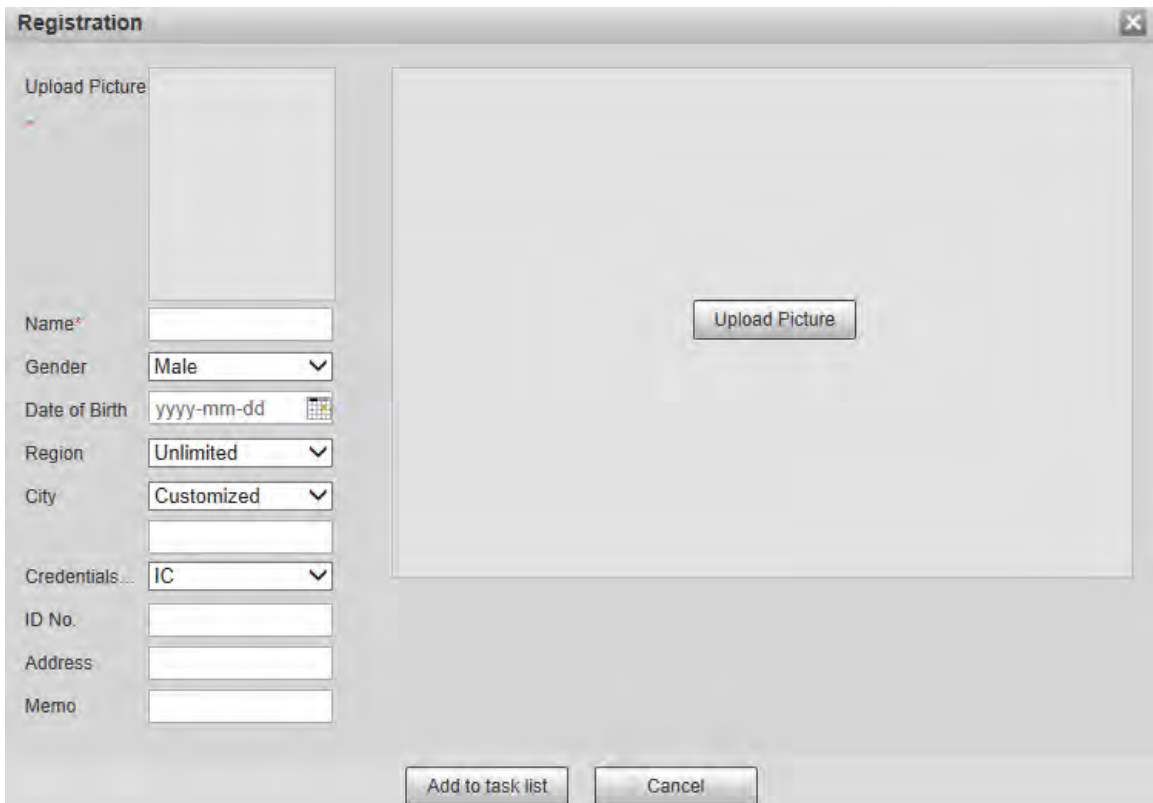
Figure 5-105 More info



Set filtering conditions, and then click **Search**. The search result is displayed.

Step 3 Click **Registration**.

Figure 5-106 Registration interface



Step 4 Click **Upload Picture**, and then import the face pictures to be uploaded.



You can manually select a face area. After uploading the picture, select a face area and click **OK**. If there are multiple faces in a image, select the target face and click **OK** to save the face image.

Figure 5-107 Addition completed

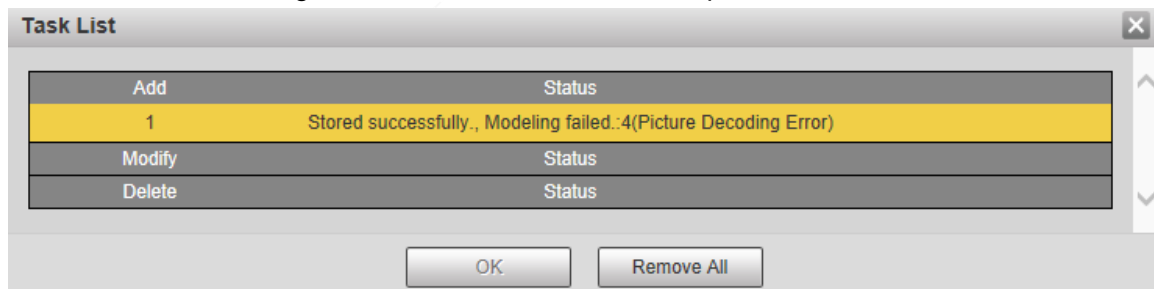


Step 5 Fill in face image information.

Step 6 Click **Add to task list**.

Step 7 Click  **Task List 1**.

Figure 5-108 Task list addition completed



Click **Remove All** to remove all the tasks.

Batch Registration

You can import multiple face images in batches. Use this method when registering a large number of face images.

Before importing images in batches, name the face images in the format of "Name#SGender#BDate of Birth#NRegion#TCredentials Type#MID No. jpg" (for example, "John#S1#B1990-01-01#NCN#T1#M330501199001016222").



Name is required and the rest are optional.

Table 5-37 Naming rules for batch import

Naming Rules	Description
Name	Enter the corresponding name.
Gender	Enter a number. 1: Male; 2: Female.
Date of Birth	Enter numbers in the format of yyyy-mm-dd. For example, 2017-11-23.
Region	Enter the region name.
Credentials Type	Enter a number. 1: ID card; 2: passport.
ID No.	Enter ID No.

Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

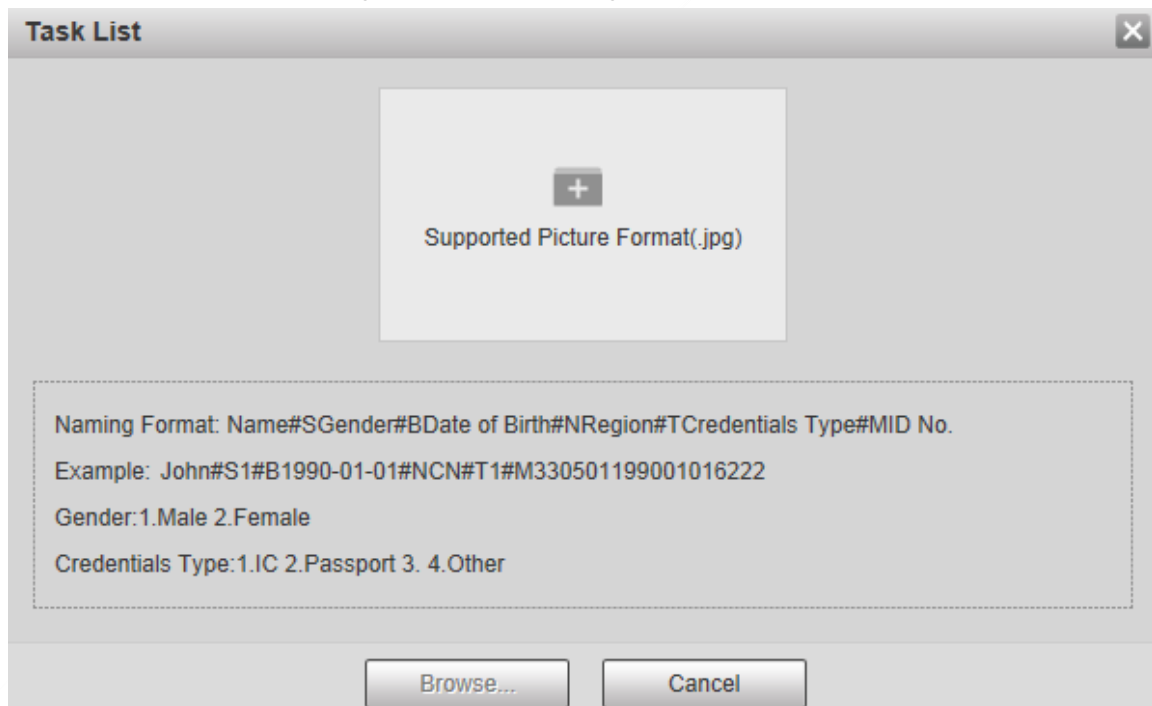
The **Face Database Config** interface is displayed.

Step 2 Click **More Info** for the face database to be configured.

The **Face Database** interface is displayed.

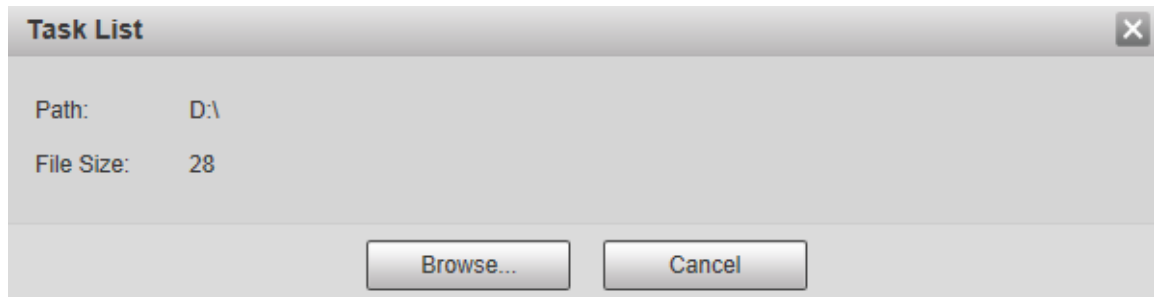
Step 3 Click **Batch Registration**.

Figure 5-109 Batch registration



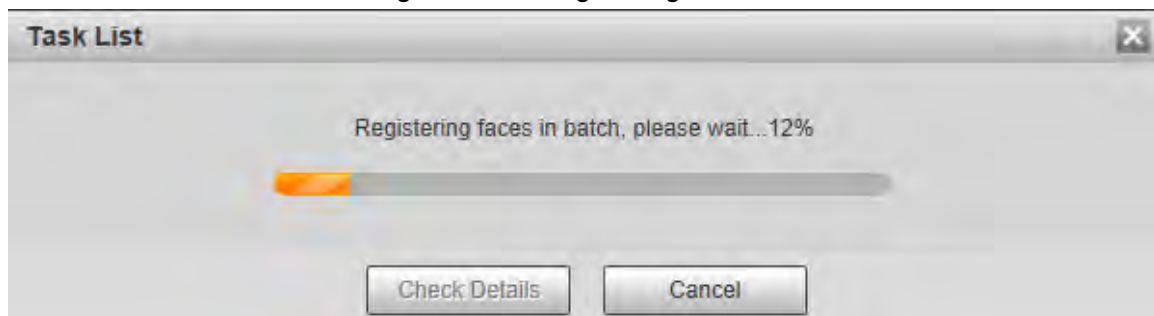
Step 4 Click to select the file path.

Figure 5-110 Batch registration



Step 5 Click **Browse**.

Figure 5-111 Registering



Step 6 After the registration is completed, click **Next** to view the registration result.

5.5.7.2.3 Managing Face Images

You can add face images to face database; manage and maintain face images to ensure correct information.

Modifying Face Information



On the **Face Database Config** page, move the mouse pointer to the face image or person information line, and then click  or . After modifying the face image information, click **Add to task list**.

Figure 5-112 Registration page

Deleting Face Images

Enter face database, and then delete the created face image.

- Single deletion: Move the mouse pointer to the face image or people information line, and then click or to delete the face image.
- Batch deletion: Move the mouse pointer to the face image or people information line, and then click at the upper right corner of the face images, or click on person information line. After selecting multiple items, click **Add to the delete list**, click Task List 1, and then click **OK** to delete the selected face images.
- Delete all: When viewing face images in a list, click on people information line (or select **All** when viewing face images in images), click **Add to the delete list**, click Task List 1, and then click **OK** to delete all face images.

5.5.7.2.4 Face Modeling

You can extract and import the relevant information of face images into the database through face modeling, and create a face feature mode for smart detection such as face comparison.

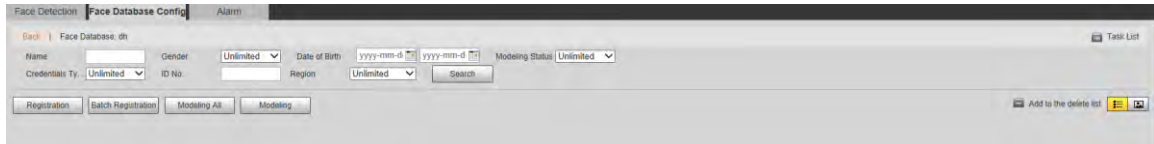


- The more face images you choose, the longer the modeling time is.
- During the modeling process, some smart detection functions (such as face comparison) are temporarily unavailable and can be resumed after the modeling is complete.

Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

Step 2 Click **More Info** for the face database to be configured.

Figure 5-113 Face database page



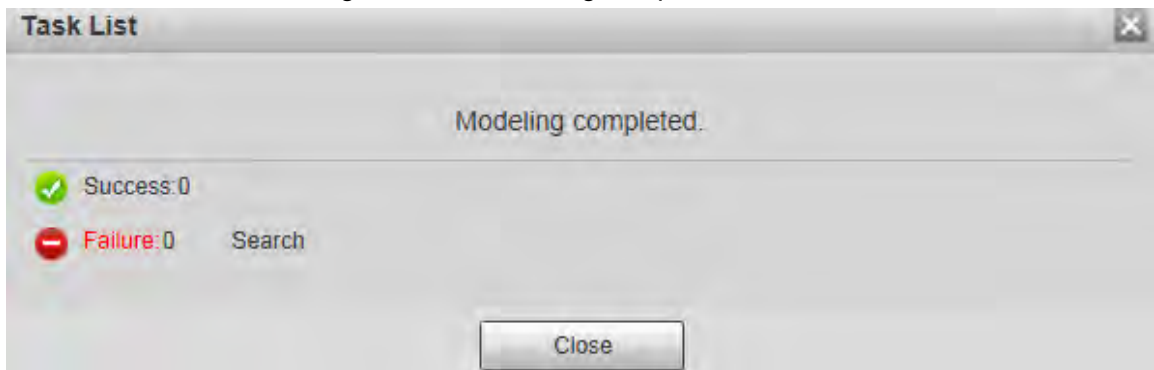
Step 3 Select the face images for modeling



Click to view the face image in a list. Click to view the face image as a thumbnail.

- **Modeling All**
Click **Modeling All**, and all face images in the face database will be modeled.
- **Selective Modeling**
If there are many face images in the face database, set filtering conditions and then click **Search** to select face images for modeling.

Figure 5-114 Modeling completed

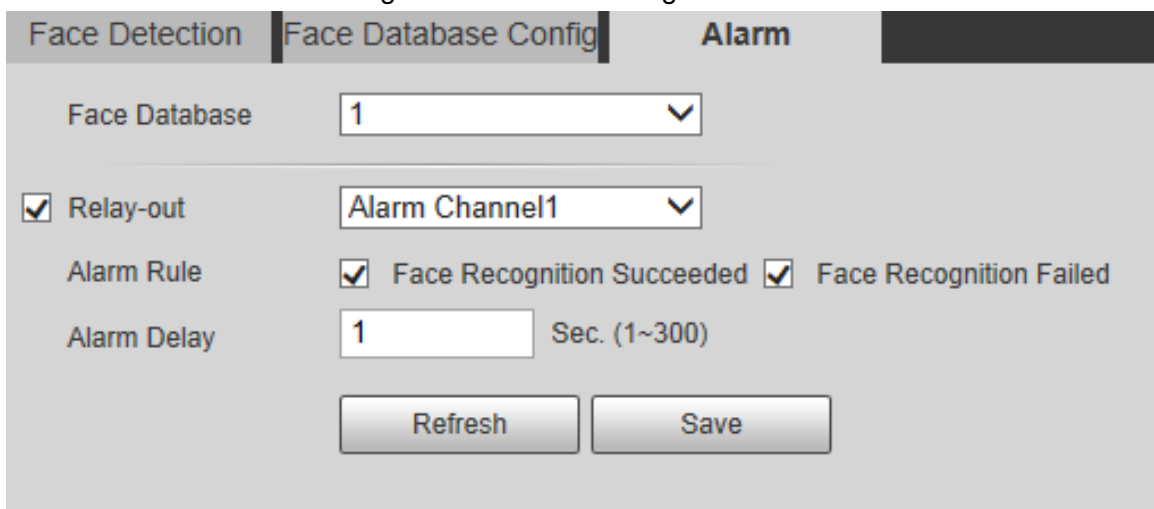


5.5.7.3 Alarm Linkage

Set the alarm linkage mode for face comparison.

Step 1 Select **Setting > Event > Face Recognition > Alarm**.

Figure 5-115 Alarm linkage



Step 2 Configure alarm linkage parameter.

Table 5-38 Description of alarm linkage parameter

Parameter	Description
Face Database	Select the face database to be configured with alarm linkage.
Alarm Rule	Select the alarm rule as needed.
Relay-out	Select the Relay-out check box, and when an alarm is triggered, the system interacts with the linked alarm devices.
Alarm Delay	The alarm will continue for an extended period of time. The value range is 1–300 s.

Step 3 Click **Save**.

5.5.8 People Counting

You can use this function to count the number of people in the area and generate reports.



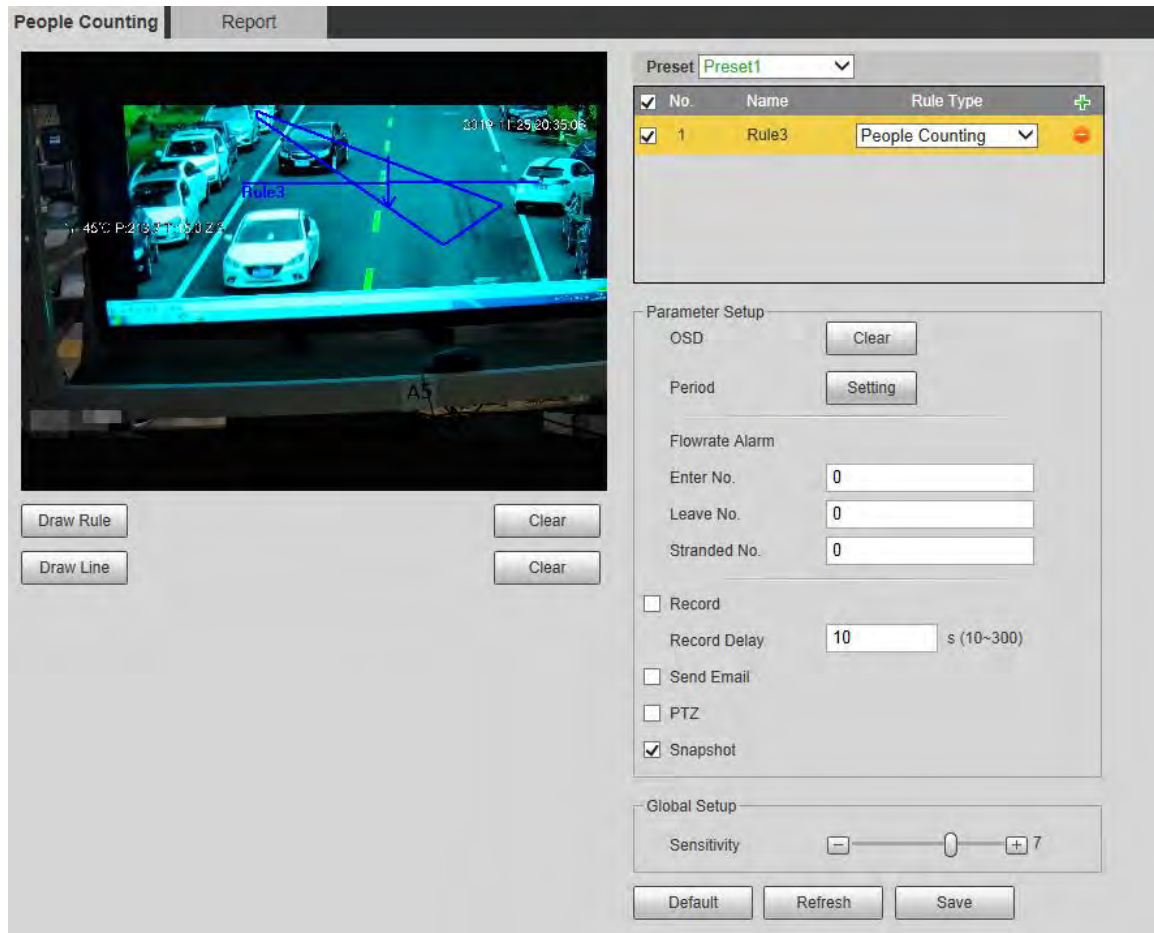
- Before using this function, you need to enable **People Counting in Smart Plan**.
- The people counting data will be overwritten if the disk is full. Back up the data in time as needed.
- This function is available on select models.

5.5.8.1 People Counting Settings

With the function, the system can count the number of people appearing in the monitoring screen within a certain period.

Step 1 Select **Setting > Event > People Counting > People Counting**.

Figure 5-116 People counting settings



Step 2 Select the presets to be configured.

Step 3 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-28.



Click **Clear** to the right of **Draw Rule**, and you can clear all drawn rules.

Step 4 Configure people counting parameter.

Table 5-39 Description of people counting parameter

Parameter	Description
OSD	Display the number of people displayed in the area in real time. Click Clear , and the current number will be zero.
Enter No.	Set the Enter No. , and when the number of people entering reaches the set value, an alarm will be triggered.
Leave No.	Set the Leave No. , and when the number of people leaving reaches the set value, an alarm will be triggered.
Stranded No.	Set the Stranded No. , and when the number of people staying reaches the set value, an alarm will be triggered.



For other parameters, see "5.5.5.1 Tripwire".

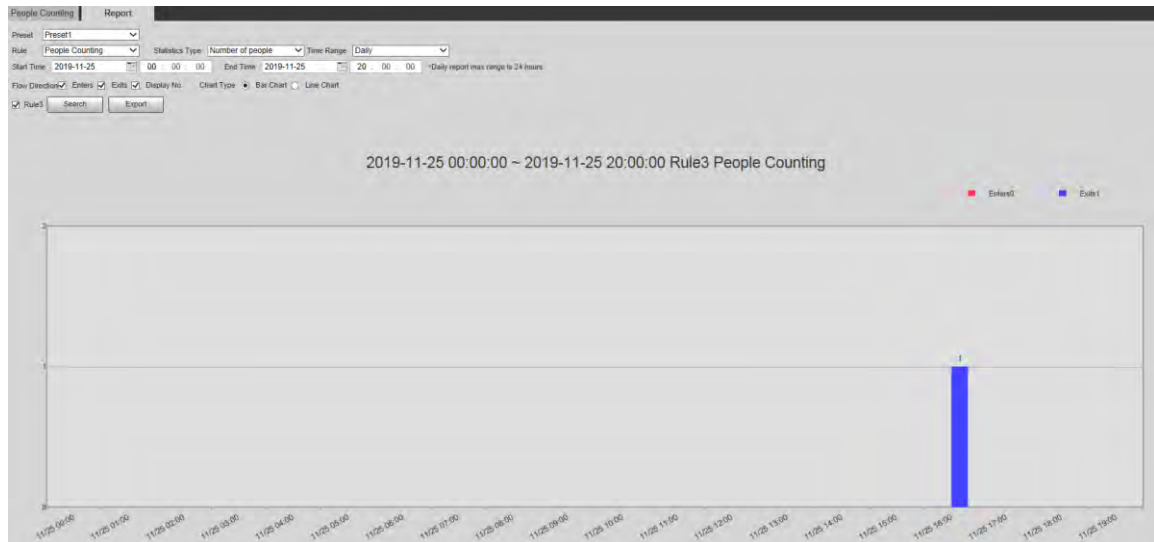
Step 5 Click **Save**.

5.5.8.2 Report

You can view the statistics results of people in the scene during the selected period.

Step 1 Select **Setting > Event > People Counting > Report**.

Figure 5-117 People counting report



Step 2 Select a preset.

Step 3 Select the **Rule, Statistics Type, and Time Range**.

Step 4 Select the start time and end time for searching reports.

Step 5 Select **Flow Direction** and **Chart Type**.

Step 6 Click **Search** to generate reports, and then click **Export** to export the report to local storage.

5.5.9 Heat Map



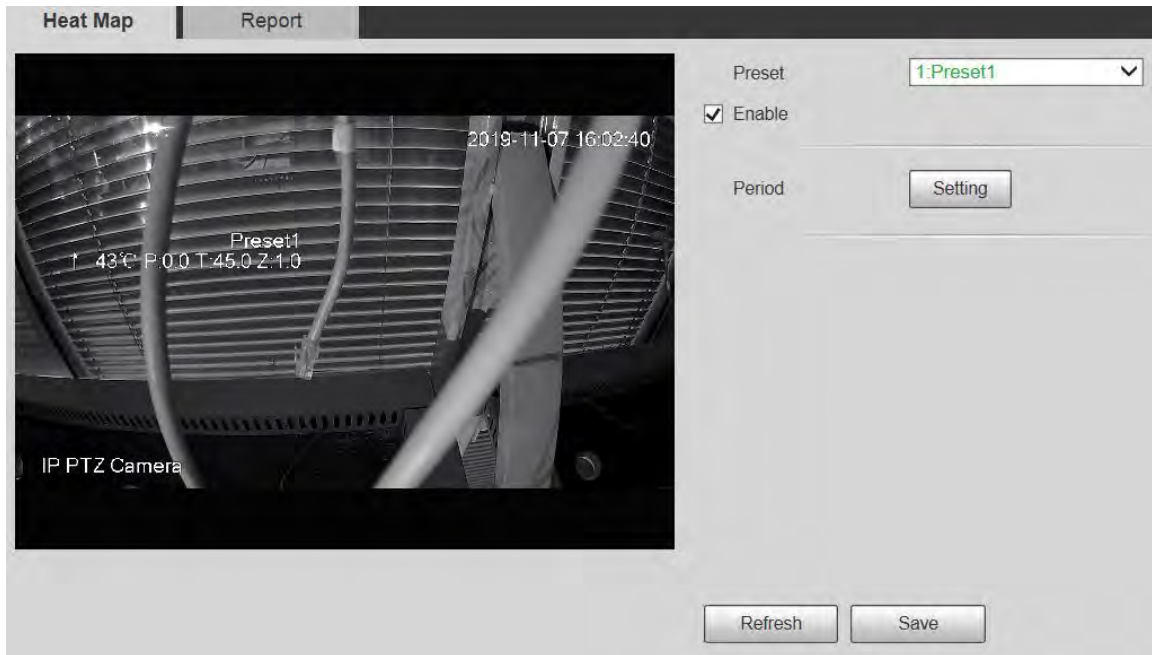
- Before enabling **Heat Map**, you need to set presets in **PTZ** section, and select the function in the **Smart Plan**.
- The data will be overwritten if the disk is full. Back up the data in time.
- This function is available on select models.

5.5.9.1 Heat Map Settings

The function can be used to detect the activity level of moving objects in the scene during a certain period.

Step 1 Select **Setting > Event > Heat Map > Heat Map**.

Figure 5-118 Heat map



- Step 2 Select the presets to be configured.
- Step 3 Select the **Enable** check box to enable heat map function.
- Step 4 Click **Setting** to set the arming period. For details, see "5.5.1.1 Motion Detection".
- Step 5 Click **Save**.

5.5.9.2 Report

You can view the heat map report for the scene in the selected period.

- Step 1 Select **Setting > Event > Heat Map > Report**.
- Step 2 Set the start time and end time to search for the heat map report.
- Step 3 Select a preset.
- Step 4 Click **Search**, and the search results will be displayed on the page.

Figure 5-119 Report



5.5.10 Video Metadata

With the function, the system can count the number of motor vehicles, non-motor vehicles and people in the monitoring screen, identify the features of the vehicles and people in the scene, and take snapshots.



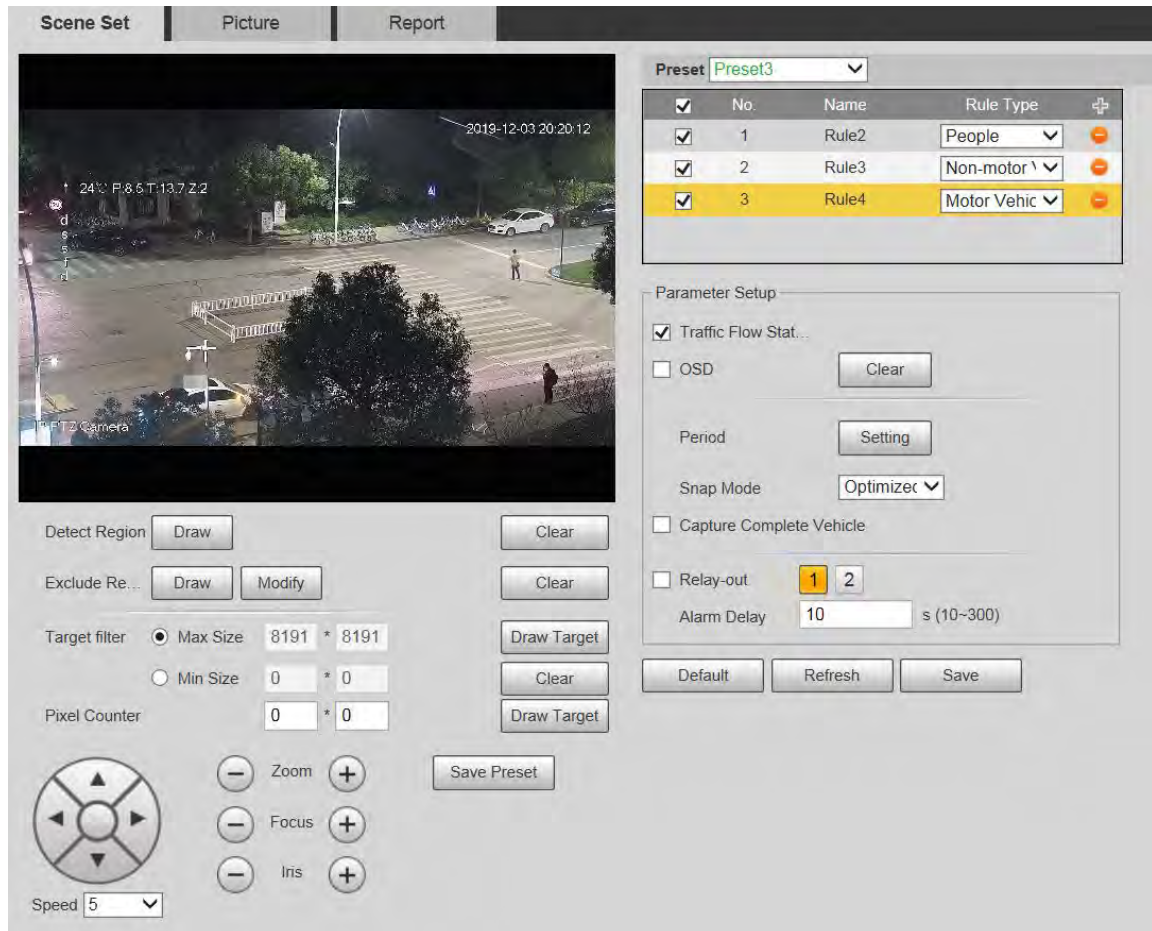
- Before using video metadata, you need to enable the function in the **Smart Plan**.
- This function is available on select models.

5.5.10.1 Scene Setting

Set the parameters of snapshot, analysis and alarm in the scene.

Step 1 Select **Setting > Event > Video Metadata**.

Figure 5-120 Scene setting



Step 2 Click the **Preset** list to select the preset to configure video metadata.

Step 3 Click to add a rule type.

Step 4 Modify the parameters.

- Double-click the name to modify the rule name.
- Select the rule type from **People**, **Non-motor Vehicle** and **Motor Vehicle**.
- Click the corresponding to delete detection items.

Step 5 Configure scene setting parameters.

Table 5-40 Description of scene setting parameter

Parameter	Description
People Flow Statistics	After selection, traffic flow statistics will be displayed on the screen.
Non-motor Vehicle Flow Statistics	
Traffic Flow Statistics	
OSD	Select the check box to enable the OSD overlay. The statistics will be displayed on the Live page in the form of OSD information.
Clear	Click it to clear the statistics of motor vehicles, non-motor vehicles and people.



For other parameters, see "5.5.5.1 Tripwire".

Step 6 Click **Save**.

5.5.10.2 Picture Overlay

Set the overlay information on the snapshot.

Step 1 Select **Setting > Event > Video Metadata > Overlay**.

Step 2 Select **Picture Overlay Type** from **People, Non-motor Vehicle** and **Motor Vehicle**.

Figure 5-121 Picture overlay–motor vehicle

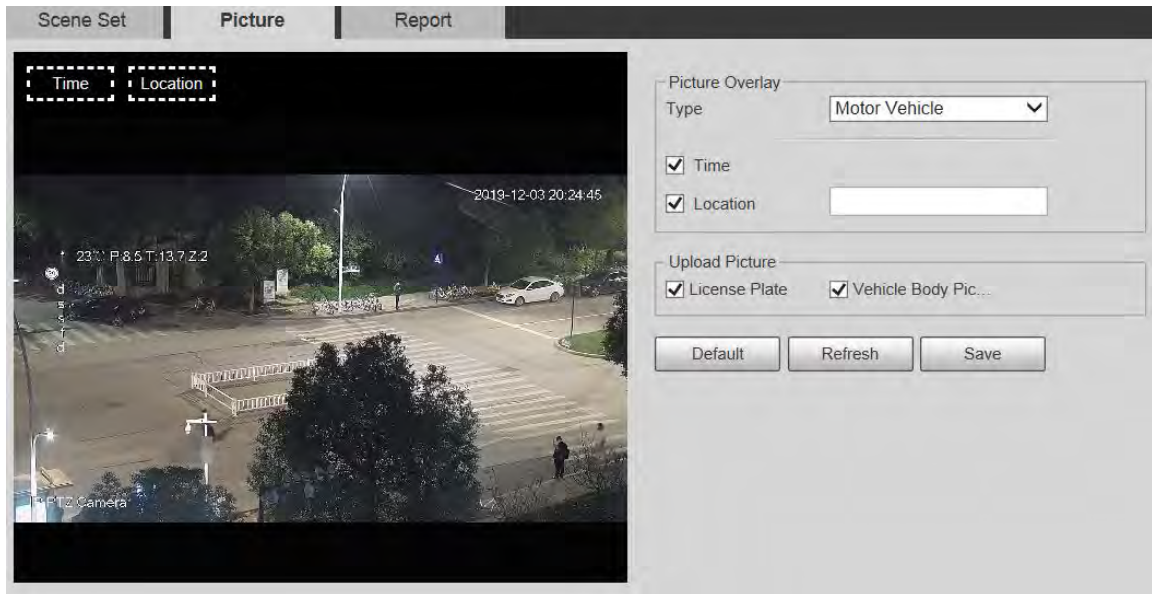


Figure 5-122 Picture overlay–non-motor vehicle

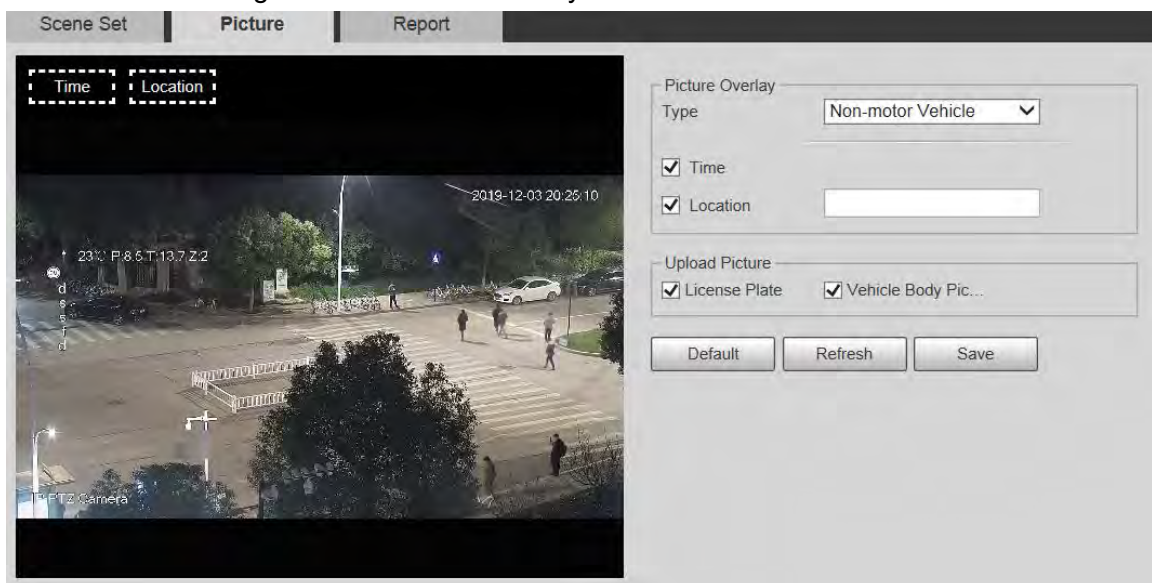
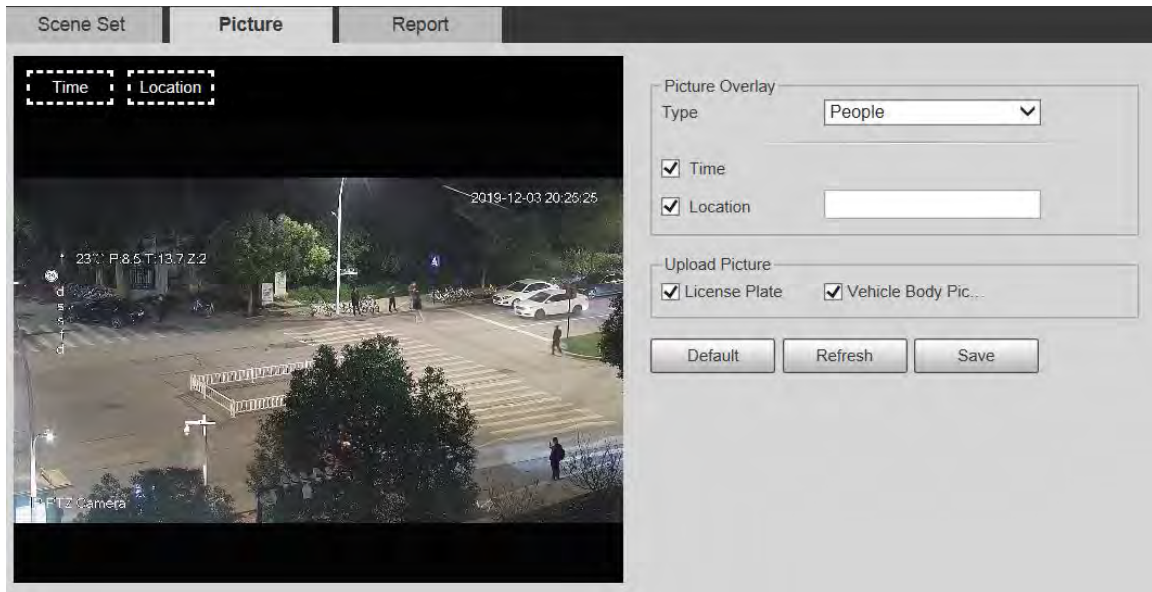


Figure 5-123 Picture overlay–people



Step 3 Select overlay information.



If you select **Location**, you need to manually enter the location of the Device.

Step 4 Click **Save**.

5.5.10.3 Report

You can view the number of vehicles, non-vehicles and people in the scene during the selected period.

Step 1 Select **Setting > Event > Video Metadata > Report**.

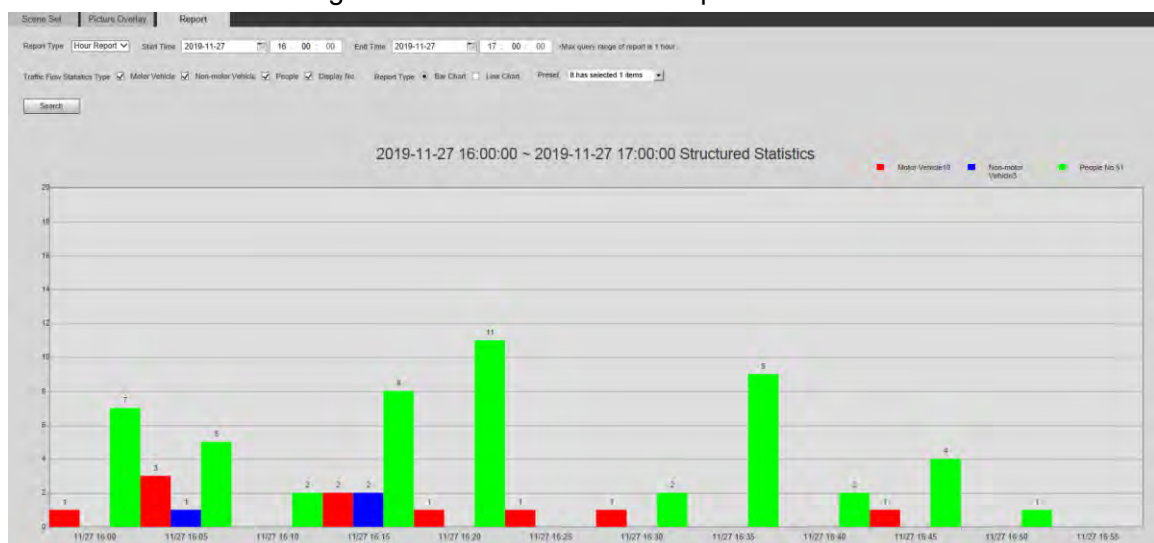
Step 2 Select the **Report Type**.

Step 3 Select the start time and end time for searching reports.

Step 4 Select **Traffic Flow Statistics Type**.

Step 5 Click **Search** to generate reports.

Figure 5-124 Video metadata report



5.5.11 Alarm

Step 1 Select **Setting > Event > Alarm**.

Figure 5-125 Alarm

Step 2 Configure alarm setting parameters.

Table 5-41 Description of alarm setting parameter

Parameter	Description
Enable	Select the Enable check box, and then the alarm linkage is enabled.
Relay-in	Select alarm input, and 7 alarm inputs are available.
Sensor Type	There are two types: NO (normally open) and NC (normally closed). Switch from NO to NC , and alarm event will be enabled. Switch from NC to NO , and alarm event will be disabled.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12 Abnormality

Abnormality includes 7 alarm events: **No SD Card**, **Capacity Warning**, **SD Card Error**, **Disconnection**, **IP Conflict**, **Illegal Access**, and **Security Exception**.

5.5.12.1 SD Card

In case of an SD card exception, an alarm will be triggered.

Step 1 Select **Setting > Event > Abnormality > SD Card**.

Figure 5-126 No SD card

The screenshot shows the 'SD Card' configuration page with the 'No SD Card' event type selected. The 'Event Type' dropdown is set to 'No SD Card'. The 'Enable' checkbox is unchecked, 'Relay-out' is checked, and 'Alarm Delay' is set to 10 seconds. The 'Send Email' checkbox is unchecked. At the bottom, there are 'Default', 'Refresh', and 'Save' buttons.

Figure 5-127 SD card error

The screenshot shows the 'SD Card' configuration page with the 'SD Card Error' event type selected. The 'Event Type' dropdown is set to 'SD Card Error'. The 'Enable' checkbox is unchecked, 'Relay-out' is checked, and 'Alarm Delay' is set to 10 seconds. The 'Send Email' checkbox is unchecked. At the bottom, there are 'Default', 'Refresh', and 'Save' buttons.

Figure 5-128 Capacity warning

The screenshot shows the 'SD Card' configuration page with the 'Capacity Warning' event type selected. The 'Event Type' dropdown is set to 'Capacity Warning'. The 'Enable' checkbox is unchecked, 'Capacity Limit' is set to 10%, 'Relay-out' is checked, and 'Alarm Delay' is set to 10 seconds. The 'Send Email' checkbox is unchecked. At the bottom, there are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Configure SD card exception parameters.

Table 5-42 Description of SD card exception parameter

Parameter	Description
Enable	Select the check box to enable this function.
Capacity Limit	Configure the free space percentage, and if the free space in the SD card is less than the defined percentage, an alarm is triggered.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.2 Network Exception

In case of a network exception, an alarm will be triggered.

Step 1 Select **Setting > Event > Abnormality > Network**.

Figure 5-129 Disconnection

SD Card | **Network** | Illegal Access | Security Exception

Event Type: Disconnection

Enable

Record

Record Delay: 10 s (10~300)

Relay-out: 1

Alarm Delay: 10 s (10~300)

Default Refresh Save

Figure 5-130 IP conflict

SD Card | **Network** | Illegal Access | Security Exception

Event Type: IP Conflict

Enable

Record

Record Delay: 10 s (10~300)

Relay-out: 1

Alarm Delay: 10 s (10~300)

Default Refresh Save

Step 2 Configure network exception parameters.

Table 5-43 Description of network exception parameter

Parameter	Description
Enable	Select the check box to enable this function.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.3 Illegal Access

Illegal access alarm is triggered when the login password has been wrongly entered for more than the times you set.

Step 1 Select **Setting > Event > Abnormality > Illegal Access**.

Figure 5-131 Illegal access

Step 2 Configure illegal access parameters.

Table 5-44 Description of illegal access parameter

Parameter	Description
Enable	Select the check box to set the illegal access alarm.
Login Error	After entering a wrong password for the set times, the alarm for illegal access will be triggered, and the account will be locked.



For other parameters, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.4 Security Exception

When an event affecting the Device safety occurs, an alarm for safety exception will be triggered.

Step 1 Select **Setting > Event > Abnormality > Security Exception**.

Figure 5-132 Security exception

Step 2 Configure security exception parameter.
For details, see "5.5.1.1 Motion Detection".

Step 3 Click **Save**.

5.5.12.5 Battery Exception

When overtemperature of the battery is detected, alarm linkage actions are performed.

Step 1 Select **Setting > Event > Abnormality > Battery Exception**.

Figure 5-133 Battery exception

Step 2 Select the **Enable** check box to enable battery exception detection.

Step 3 Set alarm linkage actions.

Step 4 Click **Save**.

5.6 Storage

5.6.1 Schedule

Before setting the schedule, make sure that the **Record Mode** is **Auto** in **Record Control**.

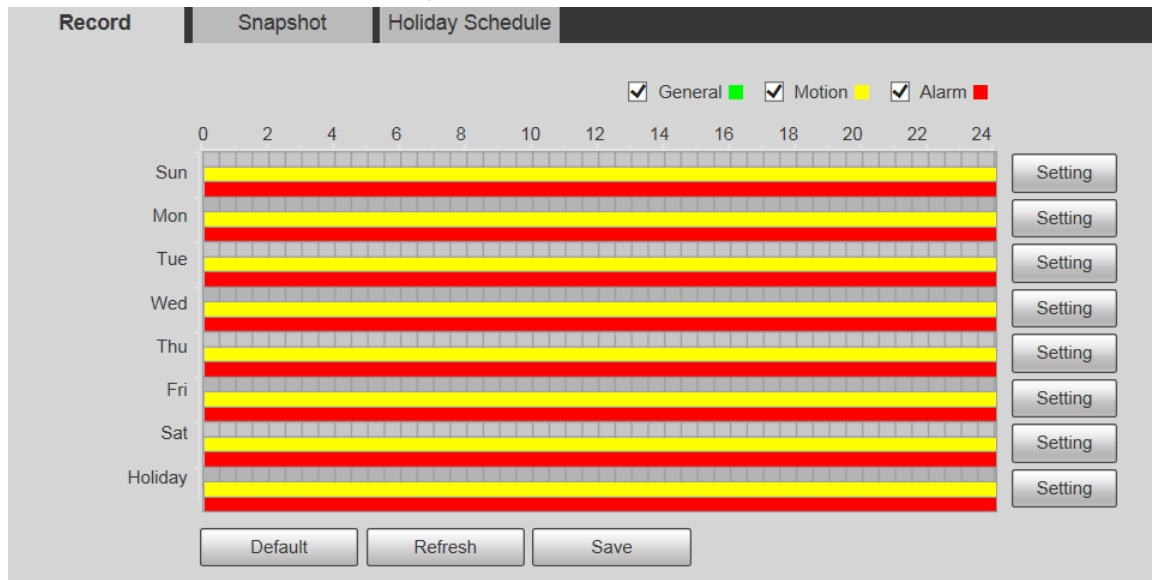


If the **Record Mode** is **Off**, the Device will not record or take snapshots according to the schedule.

5.6.1.1 Record

Step 1 Select **Setting > Storage > Schedule > Record**.

Figure 5-134 Record



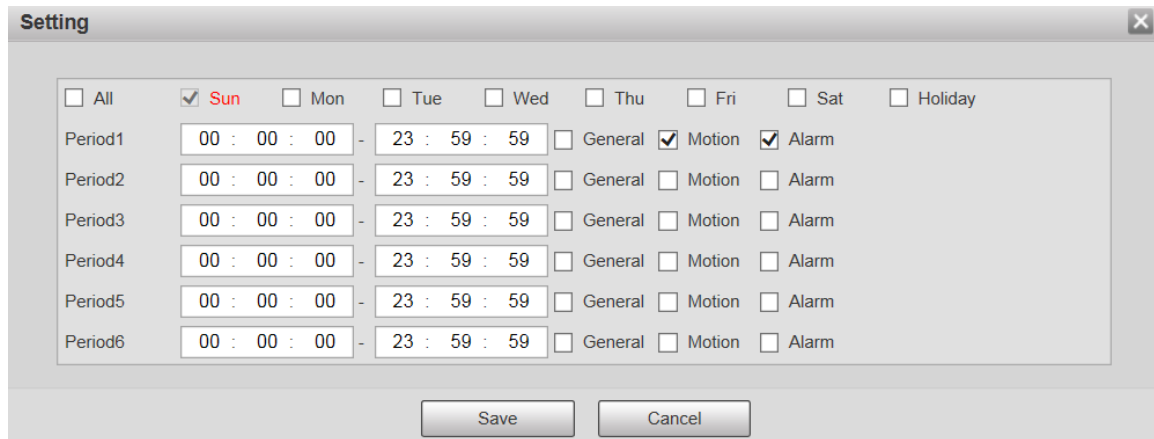
Step 2 Select the day for recording from Monday to Sunday, and then click **Setting** on the right.

- Set the recording period. You can set up to six periods for one day.
- You can select 3 types of recording: **General**, **Motion** and **Alarm**.



To set the time period, you can also press and hold the left mouse button and drag directly on the **Record** page.

Figure 5-135 Record schedule setting

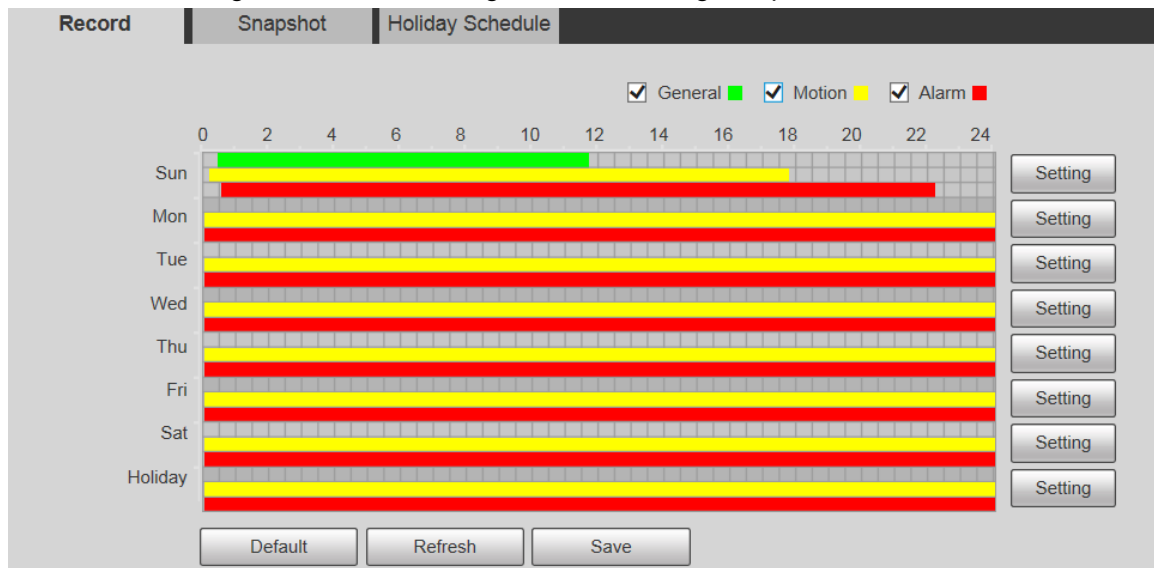


Step 3 Click **Save** to return to the **Record** page.

At this time, the colored chart visually displays the defined period.

- : Represents general recording.
- : Represents motion detection recording.
- : Represents alarm recording.

Figure 5-136 Recording schedule setting completed

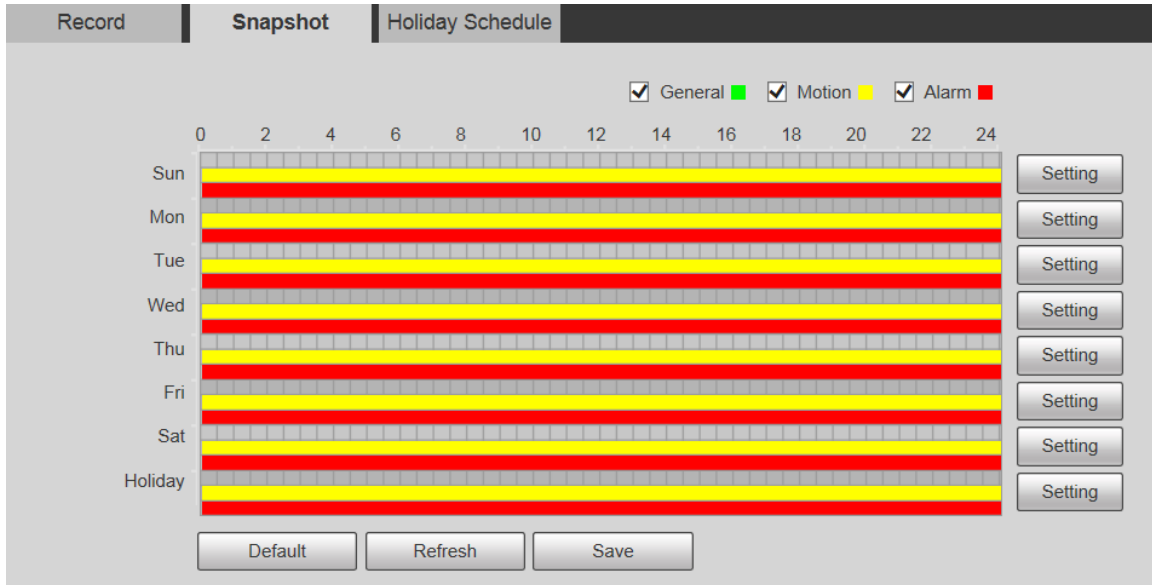


Step 4 On the **Record** page, click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the recording schedule has been set.

5.6.1.2 Snapshot

Step 1 Select **Setting > Storage > Schedule > Snapshot**.

Figure 5-137 Snapshot



Step 2 Set snapshot schedule.

For details, refer to **Step 2** and **Step 3** in "5.6.1.1 Record".

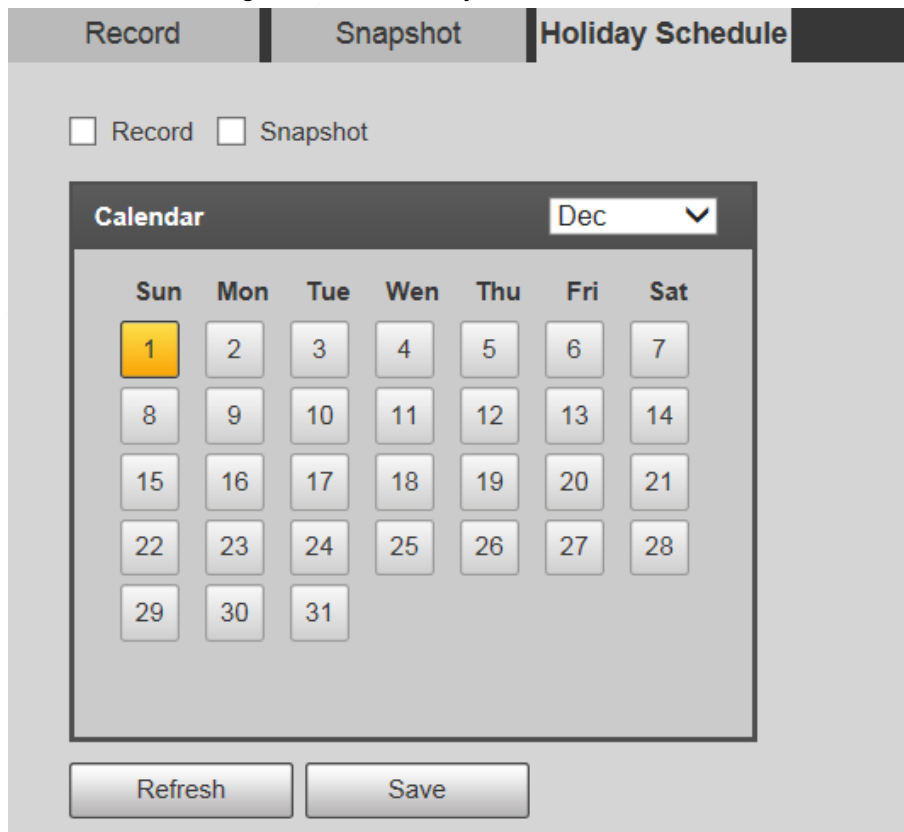
Step 3 Click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the snapshot schedule has been set.

5.6.1.3 Holiday Schedule

You can set specific dates as holidays.

Step 1 Select **Setting > Storage > Schedule > Holiday Schedule**.

Figure 5-138 Holiday schedule



Step 2 Select a date.

The selected date will be a holiday and displayed in yellow.

Step 3 Select **Record** or **Snapshot**, and then click **Save**.

The **Save Succeeded!** prompt will be displayed.

Step 4 On the **Record** or **Snapshot** page, click **Setting** to the right of **Holiday**.



The setting method is the same as that of Monday to Sunday.

Step 5 Set the period of one day for the **Holiday**, and the recording or snapshot will be taken according to the holiday time period.

5.6.2 Snapshot by Location

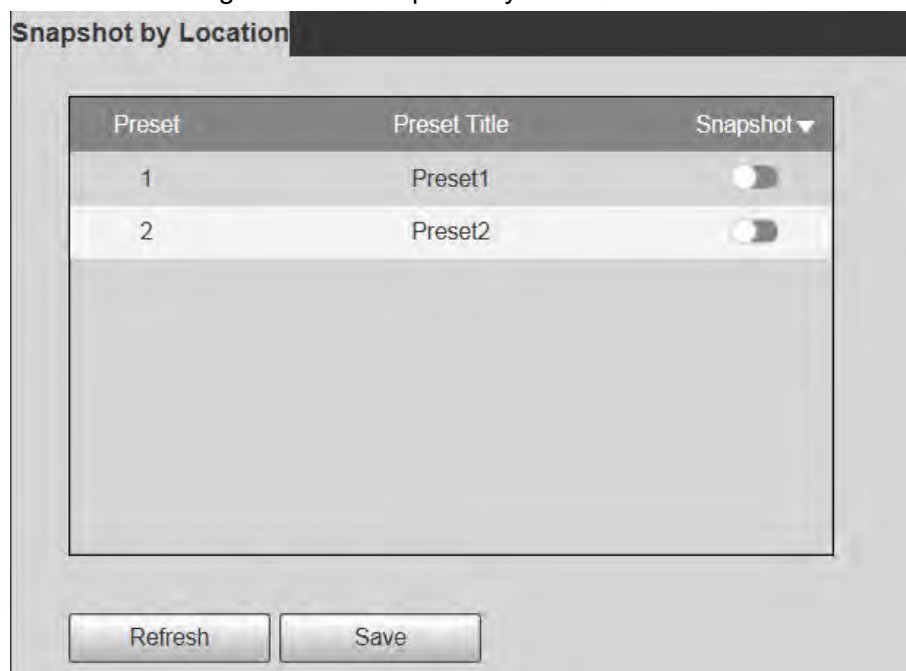
The system can take snapshots when the Device rotates to certain presets.



You need to set presets in advance.

Step 1 Select **Setting** > **Storage** > **Snapshot by Location**.

Figure 5-139 Snapshot by location



Step 2 Select presets.

- Enable snapshot by location.
 - ◇ Click to enable the function for the corresponding preset.
 - ◇ Click **Snapshot** ▾, and then select **All Enabled** to enable the function for all presets.
- Disable snapshot by location.
 - ◇ Click to disable the function for the corresponding preset.
 - ◇ Click **Snapshot** ▾, and then select **All Disabled** to disable the function for all presets.

Step 3 Click **Save**.

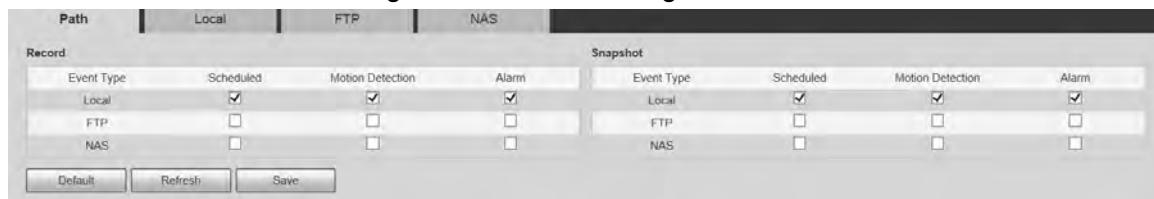
5.6.3 Destination

5.6.3.1 Path

Configure the storage path of recordings and snapshots of the Device, and select local SD card, FTP and NAS for storage. Store recordings and snapshots according to the event type, respectively corresponding to **General**, **Motion** and **Alarm** in the schedule, and then select the corresponding type of recordings or snapshots for storage.

Step 1 Select **Setting > Storage > Destination > Path**.

Figure 5-140 Path settings



Record				Snapshot			
Event Type	Scheduled	Motion Detection	Alarm	Event Type	Scheduled	Motion Detection	Alarm
Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Local	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	FTP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NAS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Step 2 Select the corresponding event type and storage method.

Table 5-45 Description of path parameter

Parameter	Description
Event Type	Select Scheduled , Motion Detection or Alarm .
Local	Save recordings or snapshots to the SD card.
FTP	Save recordings or snapshots to the FTP server.
NAS	Save recordings or snapshots to the NAS server.

Step 3 Click **Save**.

5.6.3.2 FTP

FTP function can be enabled only when it is selected as a destination path. When the network is disconnected or does not work, you can save recordings and snapshots to the SD card by using **Emergency (Local)** function.

Step 1 Select **Setting > Storage > Destination > FTP**.

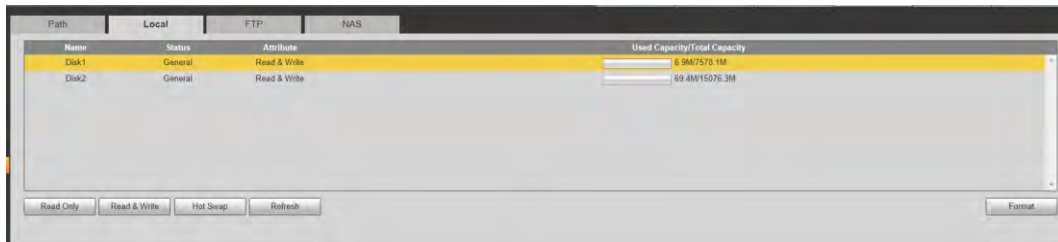


Dual SD cards are supported by some devices. For such devices, the SD card first inserted is called Local Disk 1, and the SD card inserted later is called Local Disk 2.

- If no recordings in both cards, the recording will be saved to Local Disk 1, and then saved to Local Disk 2 when Disk 1 is full.
- If there are recordings in both cards, the recording will be saved to the card with the latest recordings, and then saved to the other card when this card is full.

Step 1 Select **Setting > Storage > Destination > Local**.

Figure 5-142 Local storage



Step 2 Select the SD card to be set, and then perform the following operations as needed.

- Click **Read Only** to set the SD card to be read only.
- Click **Read & Write** to set the SD card to be read and write.
- Click **Hot Swap** to remove or insert the SD card when the Camera is running.
- Click **Format** to format the SD card.



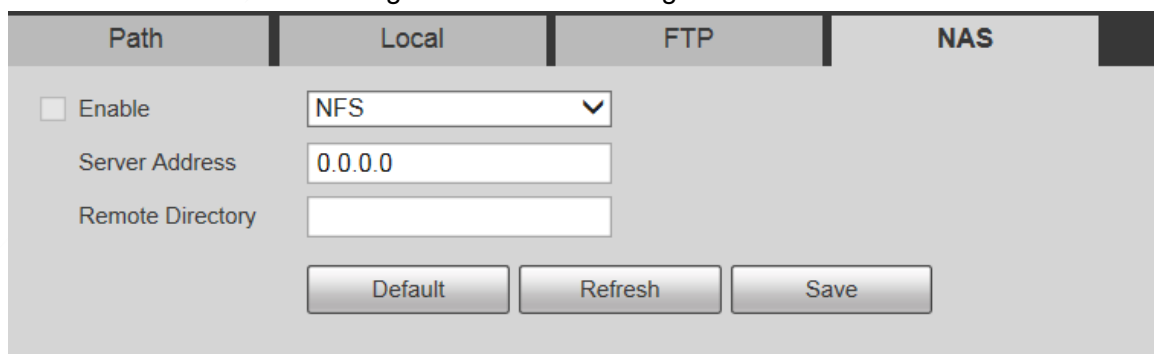
After formatting the SD card, all data on it will be cleared. Be cautious.

5.6.3.4 NAS

This function can be enabled only when NAS is selected as a destination path. Select NAS to store files on the NAS server.


Step 1 Select **Setting > Storage > Destination > NAS**.

Figure 5-143 NAS settings



Step 2 Configure NAS setting parameters.

Table 5-47 NAS parameter description

Parameter	Description
Enable	Select the check box to enable NAS function. Select NFS or SMB function.  There might be risks if NFS or SMB is enabled. Think twice before enabling the function.
Server Address	The IP address of the NAS server.
Remote Directory	The destination path on the NAS server.

Step 3 Click **Save**.


5.6.4 Record Control


Step 1 Select **Setting > Storage > Record Control**.

Figure 5-144 Record control

Step 2 Configure record control parameters.

Table 5-48 Record control parameter description

Parameter	Description
Pack Duration	Set the pack duration of each recording file. It is 30 minutes by default.
Pre-event Record	Set the pre-recording time. For example, if you enter 5, when an alarm is triggered, the system reads the recording of the first 5 seconds in memory, and then records it into a file.  If alarm recording or motion detection recording occurs, if there is no recording before, the video data within N seconds before the recording is started will also be recorded into the video file.

Parameter	Description
Disk Full	You can select Stop or Overwrite . <ul style="list-style-type: none"> • Stop: The system stops recording when the disk is full. • Overwrite: The system overwrites the oldest files and keeps recording when the disk is full.  The data will be overwritten if the disk is full. Back up the file in time as needed.
Record Mode	You can select Auto , Manual or Off . Select Manual mode to start recording immediately, and select Auto mode to record within the schedule.
Record Stream	Select Main Stream or Sub Stream .

Step 3 Click **Save**.

5.7 System Management

5.7.1 Device Settings


5.7.1.1 General

Step 1 Select **Setting > System > General > General**.

Figure 5-145 General settings

Step 2 Configure general setting parameters.

Table 5-49 Description of general setting parameter

Parameter	Description
Name	Set the device name.  Different devices have different names.
Language	Select the language to be displayed.
Video Standard	Select video standard from PAL and NTSC .

Step 3 Click **Save**.


5.7.1.2 Date & Time

Step 1 Select **Setting** > **System** > **General** > **Date&Time**.

Figure 5-146 Date & time

Step 2 Configure date &time parameters.

Table 5-50 Description of date & time parameter

Parameter	Description
Date Format	Select the date format. Three formats are available: YYYY-MM-DD , MM-DD-YYYY and DD-MM-YYYY .
Time Format	Select the time format. Two formats are available: 24-Hour and 12-Hour .
Time Zone	Set the local time zone.
Current Time	The current time of the Device.
DST	Set the Start Time and End Time of DST in the Date format or Week format.
NTP	Select the NTP check box to enable the network time sync function.
Server	Set the address of the time server.  Set the network timing function of NTP server, and the Device time will be synchronized with the server time.
Port	Set the port number of the time server.
Interval	Set the synchronization interval of the Device and the time server.

Step 3 Click **Save**.

5.7.1.3 Screen Off Settings

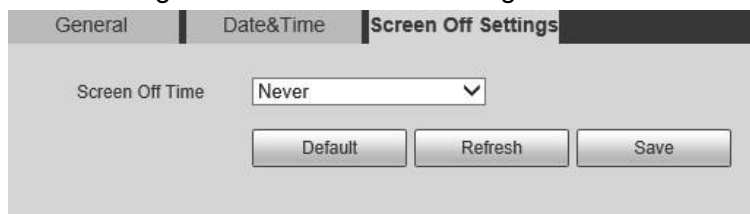


The function is available on select models.

You can set the screen-off time of the device display.

Step 1 Select **Setting > System > General > Screen Off Settings**.

Figure 5-147 Screen off settings



Step 2 Set screen-off time.

- **Never:** The screen is never turned off.
- **Custom:** Customize the screen-off time.

Step 3 Click **Save**.

5.7.2 Account Settings

5.7.2.1 Account

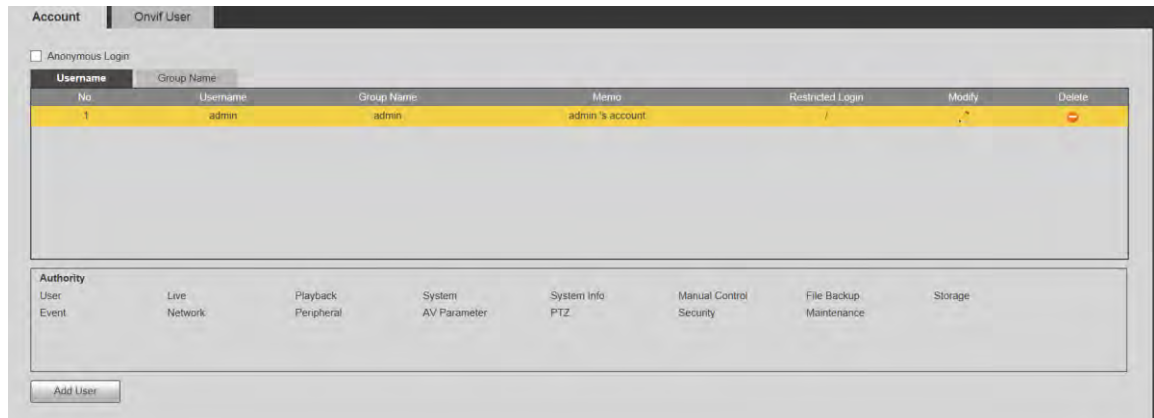
User management is only available for admin users.

- For **Username** and **Group Name**, the maximum length is 15 characters. Username can only consist of numbers, letters, underlines, dots and @; group name can only consist of numbers, letters and underlines.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : &). The confirming password shall be the same as the new password. Set a high security password according to the prompt of password strength.
- The number of users and groups is 19 and 8 respectively by default.
- User management adopts a two-level method of group and user. Neither group names nor user names can be duplicated, and a user can only belong to one group.
- Users currently logged in cannot modify their own permissions.
- The user is admin by default. The **admin** account is defined as high privileged user.

5.7.2.1.1 Username

Select **Setting > System > Account > Account > Username** to enable anonymous login, add users, delete users, modify user passwords or perform other operations.

Figure 5-148 Account interface



No permission is available for version information and other buttons except **Relay-out, Mark,** and **Wiper Control** on the **Live** interface for the time being.

Anonymous Login

Select the **Anonymous Login** check box, and you can log in to the Device anonymously without username and password after entering IP. Anonymous users only have preview permission in the permission list. In the anonymous login, click **Logout** to log in to the Device by using other usernames.



After **Anonymous Login** is enabled, the user can view audio and video data without authentication. Think twice before enabling the function.

Adding Users

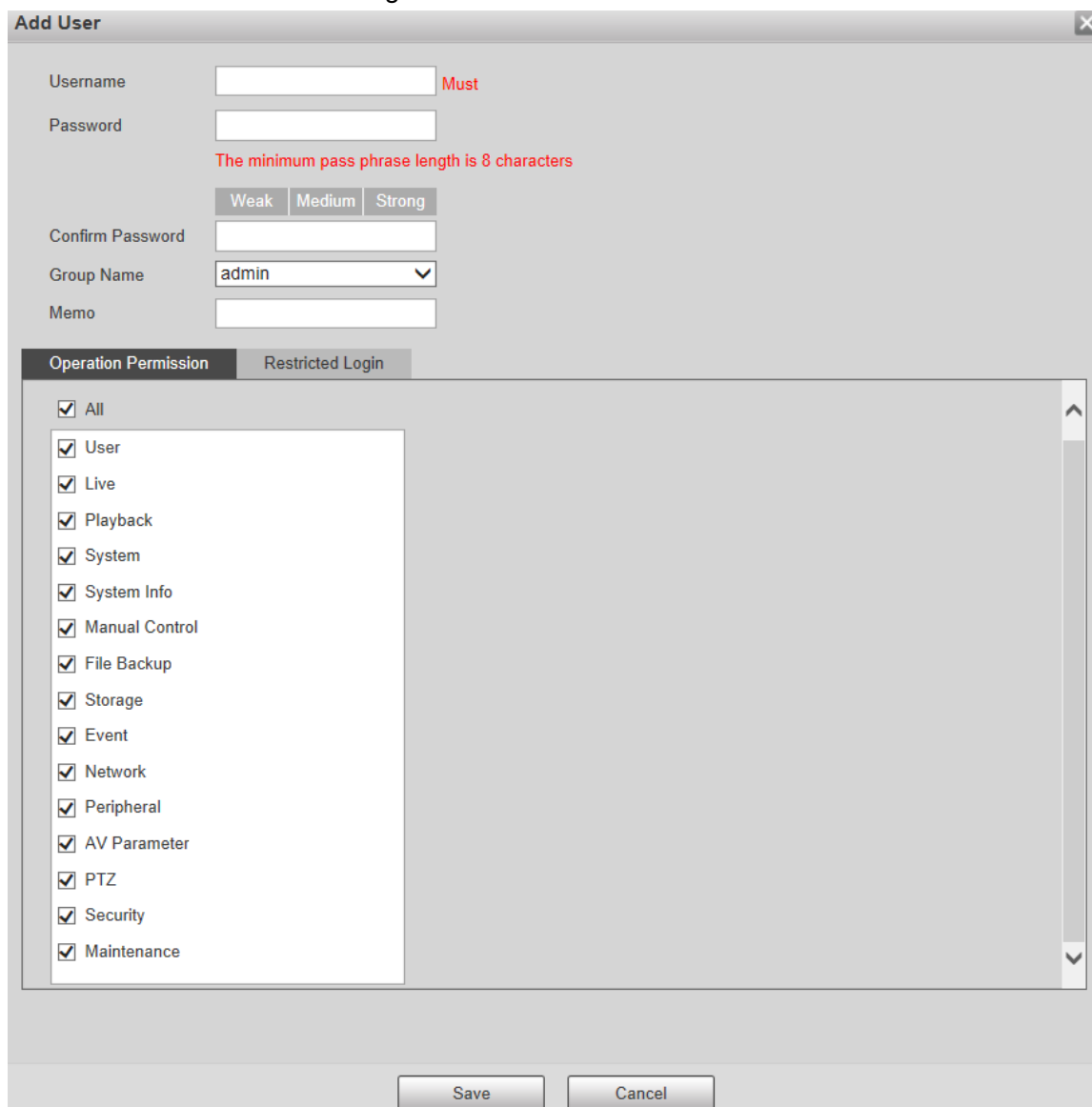
Add users in the group and set permissions.



As the default user with the highest authority, admin cannot be deleted.

Step 1 Click **Add User**.

Figure 5-149 Add users



Step 2 Enter **Username** and **Password**, confirm password, select **Group Name**, and then add **Memo**.

Step 3 Set **Operation Permission** and **Restricted Login**.

- Operation Permission: Click **Operation Permission**, and then select the operation permission of the user as needed.
- Restricted Login: **Click Restricted Login**, and the interface shown in Figure 5-150 is displayed. You can control login to the Device by setting the **IP Address**, **Validity Period** and **Time Range**.



- Once the group is selected as needed, the user permission can only be a subset of the group, and cannot exceed its permission attributes.
- It is recommended to give less permissions to general users than advanced users.

Figure 5-150 Restricted login

Add User

Username **Must**

Password

The minimum pass phrase length is 8 characters

Confirm Password

Group Name

Memo

Operation Permission **Restricted Login**

IP Address

Validity Period

Begin Time

End Time

Time Range

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Sun														<input type="button" value="Setting"/>
Mon														<input type="button" value="Setting"/>
Tue														<input type="button" value="Setting"/>
Wed														<input type="button" value="Setting"/>
Thu														<input type="button" value="Setting"/>
Fri														<input type="button" value="Setting"/>
Sat														<input type="button" value="Setting"/>

Step 4 Click **Save**.

Modifying Users


Step 1 Click  corresponding to the user you want to modify.

Figure 5-151 Modify users

Step 2 Modify user information.

Step 3 Click **Save**.


Modifying Password

Step 1 Select the **Modify Password** check box.

Step 2 Enter old password and new password, and then confirm password.

Step 3 Click **Save**.

Deleting Users

Click  corresponding to the user to be deleted, and the user can be deleted.



Users/user groups cannot be recovered after deletion. Think twice before performing the operation.

5.7.2.1.2 Group Name

Select **Setting > System > Account > Account > Group Name** to add groups, delete groups, modify group passwords or perform other operations.

Figure 5-152 User group settings

No.	Group Name	Memo	Modify	Delete
1	admin	administrator group		
2	user	user group		

Configuring User Group

The default authorities of Admin group includes live, playback, storage, file backup, user, system, system info, manual control, maintenance, peripheral, PTZ, security, network, event and AV parameters; the default authorities of User group include live and playback.

Table 5-51 Description of user group parameters

Group Authority	Admin	User	Functions
User	YES	NA	Add, delete and check user/user group.
Live	YES	YES	Real-time stream view.
Playback	YES	YES	Playback view.
System	YES	NA	System time setting and more.
System Info	YES	NA	Version information, system logs and more.
Manual Control	YES	NA	PTZ settings.
File Backup	YES	NA	File backup.
Storage	YES	NA	Storage point configuration, snapshot recording time configuration, SFTP configuration and more.
Event	YES	NA	Video detection settings, audio detection settings, alarm settings and more.
Network	YES	NA	IP settings, SMTP settings, SNMP settings, AP Hotspot settings and more.
Peripheral	YES	NA	External light, wiper and serial port settings.
AV Parameter	YES	NA	Camera property settings, audio and video settings and more.
PTZ	YES	NA	Preset settings, tour settings and more.
Security	YES	NA	HTTPS settings, RTSP over TLS settings and more.
Maintenance	YES	NA	Automatic maintenance settings and more.



- Any user in the **Admin** group has **User** authority to modify group authority. The **User** group does not have this authority.
- The functions of the device correspond to the authority control respectively. Only user with specified authority can use corresponding function; the **Admin** group has all the authorities.

Adding Groups

For specific operations, refer to "5.7.2.1.1 Username".

Modifying Groups

For specific operations, refer to "5.7.2.1.1 Username".

Deleting Groups

For specific operations, refer to "5.7.2.1.1 Username".

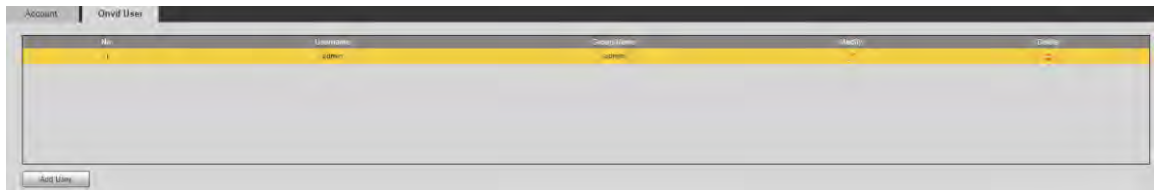
5.7.2.2 ONVIF User

On the web page, you can add ONVIF users, or modify existing users.

Procedure

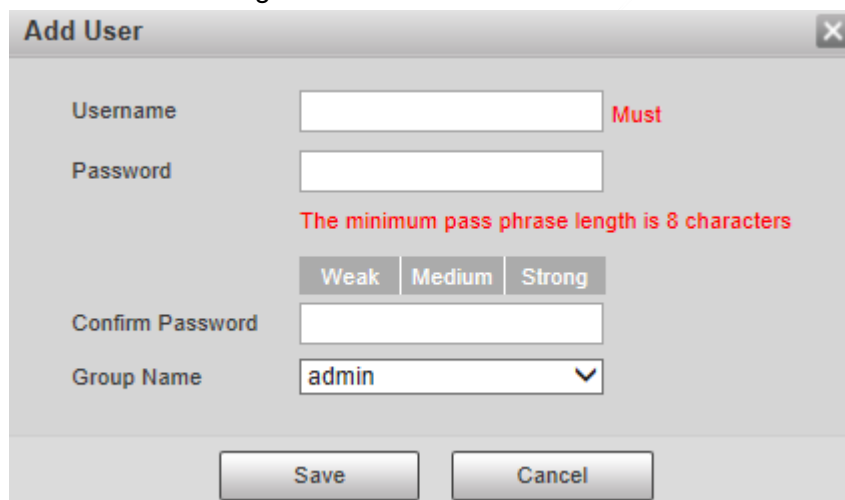
Step 1 Select **Setting > System > Account > Onvif User**.

Figure 5-153 Onvif user



Step 2 Click **Add User**.



Figure 5-154 Add users



Step 3 Set the username and password, confirm password, and then select the group name.

Step 4 Click **Save**.

Related Operations

- Click  to modify user information.
- Click  to delete users.

5.7.3 Safety

5.7.3.1 RTSP Authentication

Set the authentication method for media stream.

Step 1 Select **Setting > System > Safety > RTSP Authentication**.

Figure 5-155 RTSP authentication

Step 2 Select the **Authorize Mode**.

You can select from **Digest**, **Basic** and **None**. It is **Digest** by default.



- Click **Default**, and **Digest** is selected automatically.
- Select **None**, and "Non-authentication mode may have risk. Are you sure to enable it" prompt will be displayed. Think twice before selecting the mode.
- Select **Basic** mode, and "Basic authentication mode may have risk. Are you sure to enable it?" prompt will be displayed. Think twice before selecting the mode.

5.7.3.2 System Service








You can configure system service to ensure system security.

Step 1 Select **Setting > System > Safety > System Service**.

Figure 5-156 System service

Step 2 Configure system service parameters.

Table 5-52 Description of system service parameter

Function	Description
SSH	<p>You can enable SSH authentication to perform safety management. The function is disabled by default.</p>  <p>It is recommended to disable SSH. If this function is enabled, there might be security risks.</p>
Multicast/Broadcast Search	<p>Enable this function, and when multiple users are viewing the monitoring screen simultaneously through network, they can find the Device through multicast/broadcast protocol.</p>  <p>It is recommended to disable the multicast/broadcast search function. If this function is enabled, there might be security risks.</p>
Password Reset	<p>You can enable Password Reset to perform security management. The function is enabled by default.</p>  <p>If the function is disabled, you can only reset the password after restoring the Device to factory defaults through pressing the Reset button on the device.</p>
CGI Service	<p>You can access the Device through this protocol. The function is enabled by default.</p>  <p>It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Onvif Service	<p>You can access the Device through this protocol. The function is enabled by default.</p>  <p>It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Audio and Video Transmission Encryption	<p>Enable this function to encrypt the stream transmitted through the private protocol.</p>  <ul style="list-style-type: none"> • Make sure that the matched devices or software support video decryption function. • It is recommended to enable the function. If the function is disabled, there might be risk of data leakage.
Mobile Push	<p>Push the alarm snapshot triggered by the Device to the mobile phone. The function is enabled by default.</p>  <p>It is recommended to disable the function. If this function is enabled, there might be security risks.</p>
Private Protocol Authentication Mode	<p>You can select Security Mode and Compatible Mode. Security mode is recommended. If you select compatibility mode, there might be security risks.</p>

Step 3 Click **Save**.

5.7.3.3 HTTPS



It is recommended to enable HTTPS service. If the service is disabled, there might be risk of data leakage.

Create certificate or upload signed certificate, and then you can log in through HTTPS with your PC. HTTPS can ensure data security, and protect user information and device security with reliable and stable technology.

Step 1 Create certificate or upload the signed certificate.

- If you select **Create Certificate**, refer to the following steps.
- 1) Select **Setting > System > Safety > HTTPS**.

Figure 5-157 HTTPS (1)

The screenshot shows the 'HTTPS' configuration page. At the top, there are tabs for 'RTSP Authentication', 'System Service', 'HTTPS', and 'Firewall'. The 'HTTPS' tab is selected. Below the tabs, there are several sections:

- Enable HTTPS:** A checkbox that is currently unchecked.
- Protocol Version:** A section containing a checked checkbox for 'Enable TLSv1.0'.
- Create Certificate:** A section with a 'Create' button.
- Request Created:** A table with one row containing a text input field for 'Request Created', and three buttons: 'Delete', 'Install', and 'Download'.
- Install Signed Certificate:** A section with two rows. The first row has a 'Certificate Path' input field and a 'Browse...' button. The second row has a 'Certificate Key Path' input field, a 'Browse...' button, and an 'Upload' button.
- Certificate Installed:** A section with one row containing a 'Certificate Installed' input field and a 'Delete' button. Below this is an 'Attribute' input field.

At the bottom of the form, there are 'Refresh' and 'Save' buttons.

- 2) Click **Create**.

Figure 5-158 HTTPS (2)

3) Enter the required information, and then click **Create**.



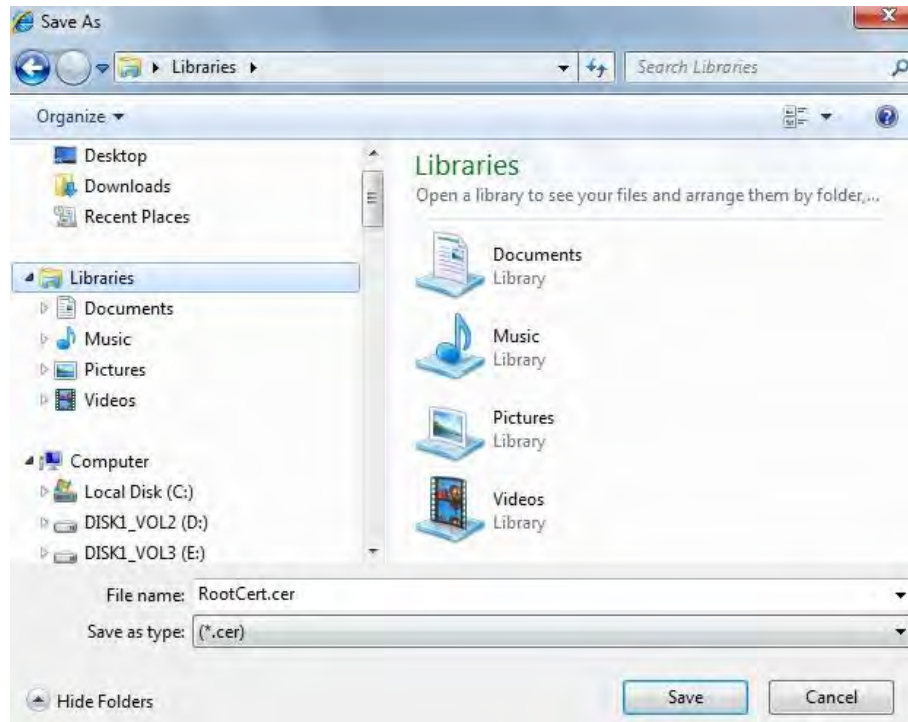
The entered IP or domain name must be the same as the IP or domain name of the Device.

4) Click **Install** to install the certificate on the Device.

Figure 5-159 Certificate installation

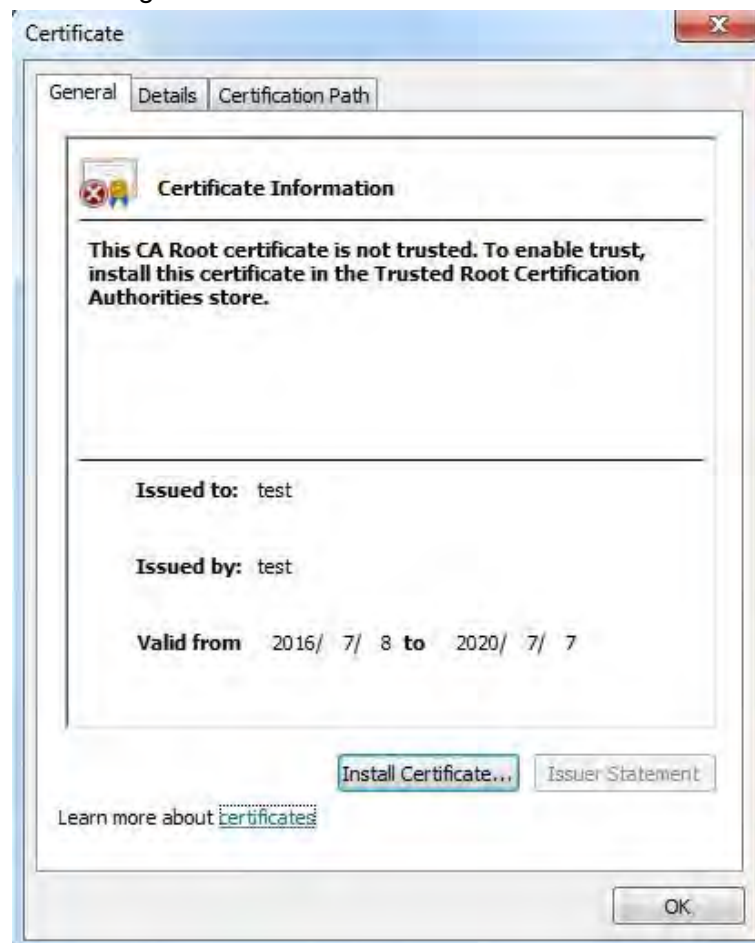
5) Click **Download** to download root certificate.

Figure 5-160 Download root certificate



- 6) Select storage path, and then click **Save**.
- 7) Double-click the **RootCert.cer** icon.

Figure 5-161 Certificate information



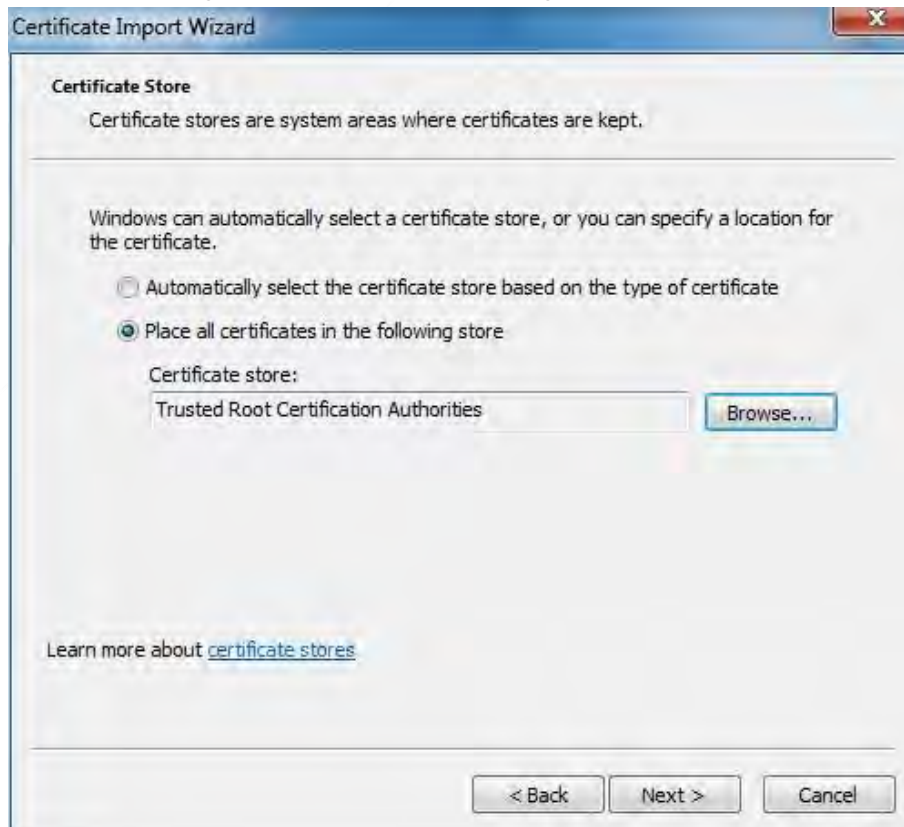
- 8) Click **Install Certificate**.

Figure 5-162 Certificate import wizard



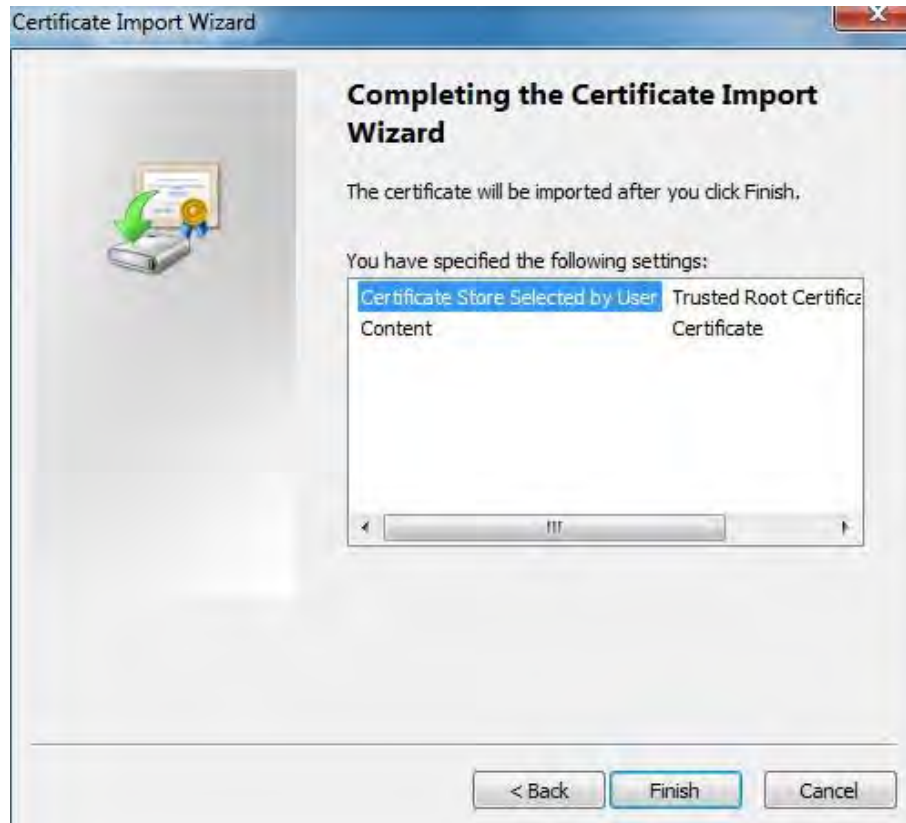
- 9) Click **Next**, and then select **Trusted Root Certification Authorities**.

Figure 5-163 Certificate storage area



- 10) Click **Next**.

Figure 5-164 Completing the certificate import wizard



11) Click **Finish**.

Figure 5-165 Security warning



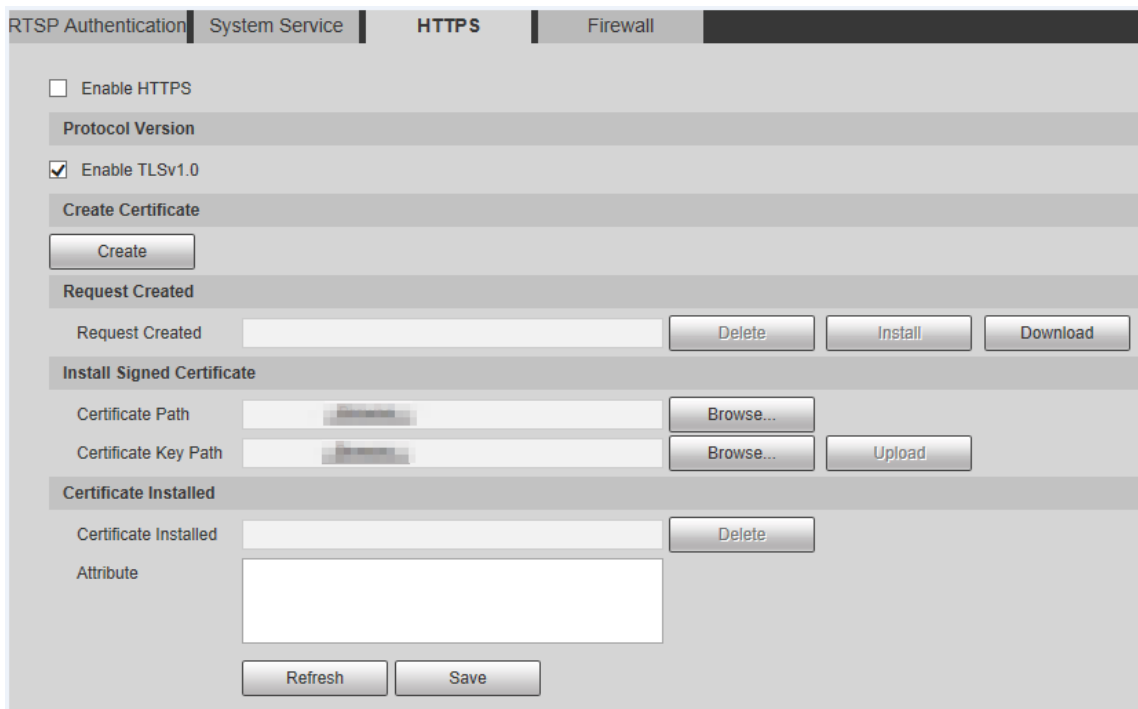
12) Click **Yes**, and then click **OK** to complete the certificate installation.

Figure 5-166 Import success



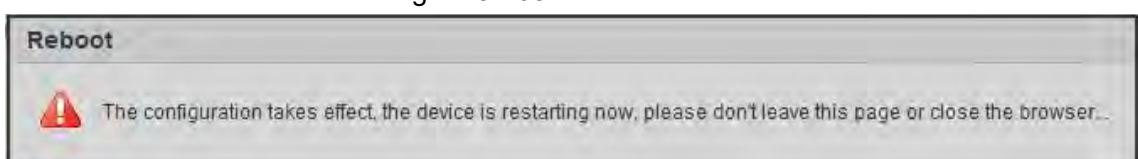
- If you select **Install Signed Certificate**, refer to the following steps.
 - 1) Select **Setting > System > Safety > HTTPS**.

Figure 5-167 Install signed certificate



- 2) Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.
 - 3) Install the root certificate. For details, see [5](#)) to [12](#)) in [Step1](#).
- Step 2** Select **Enable HTTPS**, and then click **Save**.
The configuration takes effect after reboot.

Figure 5-168 Reboot



Enter `https://xx.xx.xx.xx` in the browser to open the login interface. If no certificate is installed, a certificate error prompt will be displayed.



- If HTTPS is enabled, you cannot access the Device through HTTP. The system will switch to HTTPS if you access the Device through HTTP.
- The deletion of created and installed certificates cannot be restored. Think twice before deleting them.

5.7.3.4 Firewall

Set a firewall for the Device to prevent network attacks after the Device is connected to the network.

Step 1 Select **Setting > System > Safety > Firewall**.

Figure 5-169 Firewall

Step 2 Select the type of network attack that the firewall resists. You can select **Network Access**, **PING Prohibited**, or **Prevent Semijoin**.

Step 3 Select **Enable** to enable **Firewall** ifunction.

Step 4 Click **Save**.

5.7.4 Peripheral



The peripheral functions might vary with different models.

Step 1 Select **Setting > System > Peripheral > Wiper**.

Figure 5-170 Wiper settings

Step 2 Configure wiper parameters.

Table 5-53 Description of wiper setting parameter

Parameter	Description
Mode	Set the wiper mode. It is Manual by default. In Manual mode, you need to manually start the wiper.
Interval Time	The time between wiper starting to wiper ending.
Working Duration	Set the maximum duration of the wiper operating once in Manual mode. The value ranges from 10 minutes to 1440 minutes.

Step 3 Click **Save**.

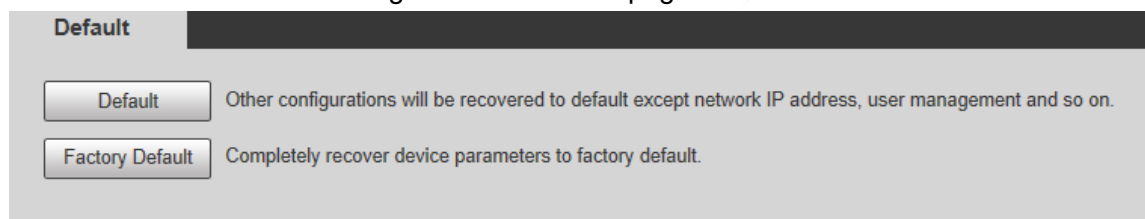
5.7.5 Default



All information except IP address and user management will be restored to defaults. Think twice before performing the operation.

Select **Setting > System > Default**, and click **Default** to restore the Device.

Figure 5-171 Default page



Select the recovery mode.

- **Default**: All information except IP address and user management will be restored to defaults.
- **Factory Default**: The function is equivalent to the Reset button of the Device. All configuration information of the Device can be restored to the factory defaults, and the IP address can also be restored to the original IP address. After clicking **Factory Default**, you need to enter the password of admin user on the page displayed. The Device can be restored to factory defaults only after the system confirms that the password is correct.



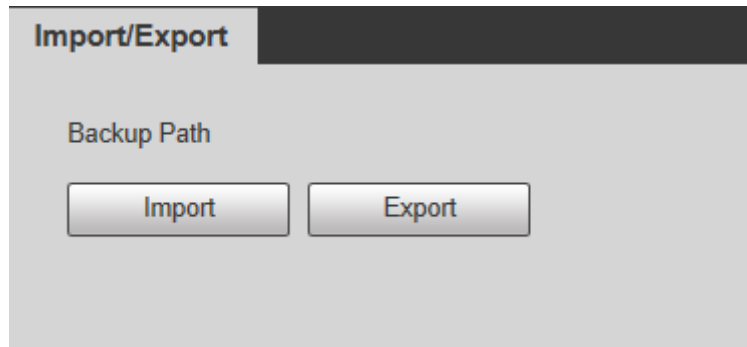
- Only admin user can use this function.
- When the Device is restored to factory defaults, all information except the data in the external storage media will be erased. Delete data in external storage media by formatting and other methods.

5.7.6 Import/Export

When multiple devices share the same configuration methods, they can be quickly configured by importing and exporting configuration files.

Step 1 On the web page of one device, select **Setting > System > Import/Export**.

Figure 5-172 Import/Export



Step 2 Click **Export** to export the configuration file (.backup file) to the local storage path.

Step 3 Click **Import** on the **Import/Export** page of the Device to be configured to import the configuration file, and the Device will complete the configurations.

5.7.7 System Maintenance

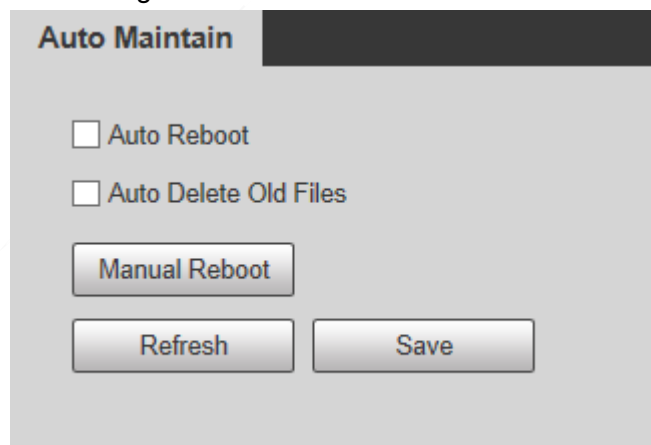
5.7.7.1 Auto Maintain

You can select **Auto Reboot** or **Auto Delete Old Files**.

- If you select **Auto Reboot**, the frequency and time need to be set.
- If you select **Auto Delete Old Files**, you need to set the time period for the files to be deleted.


Step 1 Select **Setting > System > Auto Maintain**.

Figure 5-173 Auto maintain



Step 2 Configure parameters of auto maintain.

Table 5-54 Description of auto maintain parameter

Parameter	Description
Auto Reboot	Select the check box to set the Device reboot time.
Auto Delete Old Files	Select the check box to customize the time period for the files to be deleted. The value ranges from 1 day to 31 days.  When you enable the function, The deleted files cannot be recovered. Are you sure to enable this function now? prompt will be displayed. Think twice before enabling the function.

Step 3 Click **Save**.

5.7.7.2 Emergency Maintenance

By enabling emergency maintenance, you can fix most issues caused by upgrade and configuration.

Step 1 Select **Setting > System > Auto Maintain > Emergency Maintenance**.

Figure 5-174 Auto maintain



Step 2 Click **Save**.

5.7.8 Upgrade

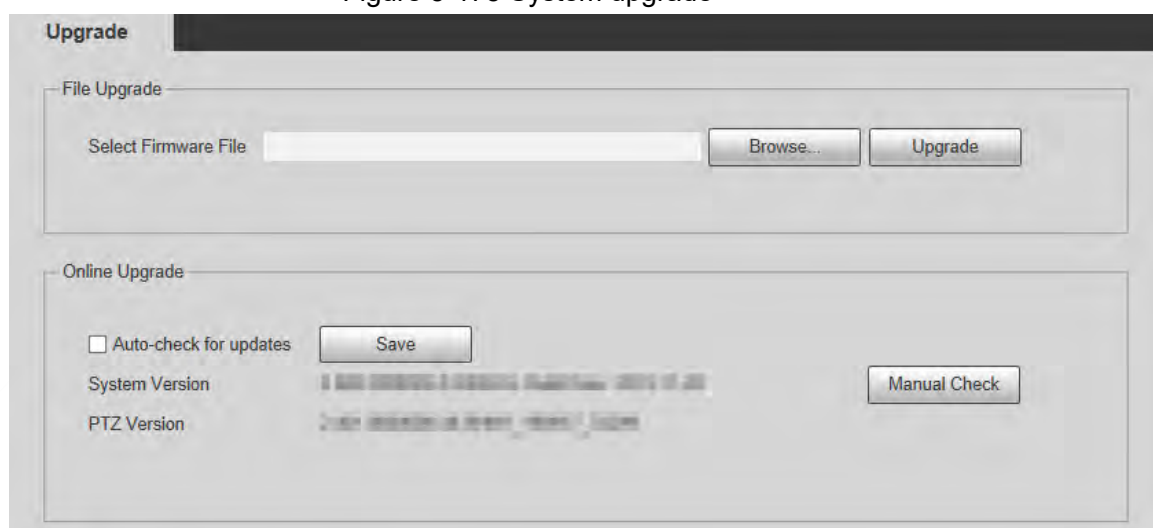
Upgrade the system to improve device function and stability.



If wrong upgrade file has been used, restart the Device; otherwise some functions might not work properly.

Select **Setting > System > Upgrade**.

Figure 5-175 System upgrade



- File Upgrade: Click **Browse**, select the upgrade file, and then click **Upgrade** to upgrade the firmware. The upgrade file is in the format of *.bin.
- Online Upgrade
 1. Select the **Auto-check for updates** check box.
This will enable the system to check for upgrade once a day automatically, and there

will be system notice if any upgrade is available.



We need to collect the data such as IP address, device name, firmware version, and device serial number to perform auto-check. The collected information is only used to verify the legitimacy of the Device, and push the upgrade notification.

2. Click **Save**.



Click **Manual Check**, and you can check for upgrade manually.

5.8 Information

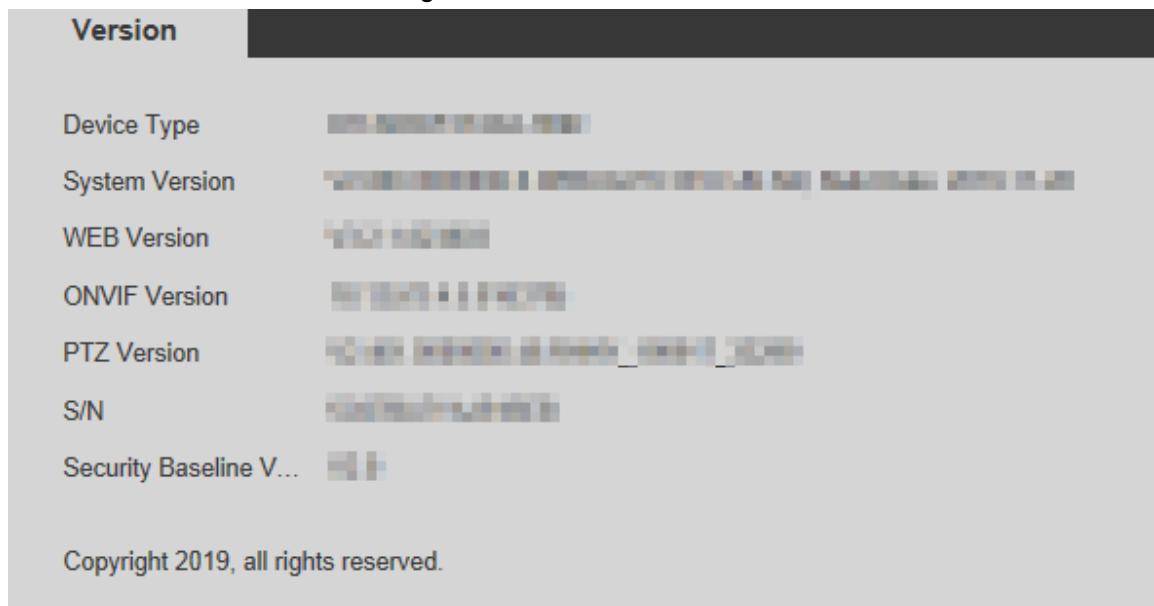
You can view information such as version, online users, log, and life statistics.

5.8.1 Version

You can view information such as system hardware features, software version and release date.

Select **Setting** > **Information** > **Version** > **Version** to view the version information of current web interface.

Figure 5-176 Version



5.8.2 Log Information

5.8.2.1 Log

Select **Setting** > **Information** > **Log** > **Log** to view the operation information of the Device and system information.

Figure 5-177 Log

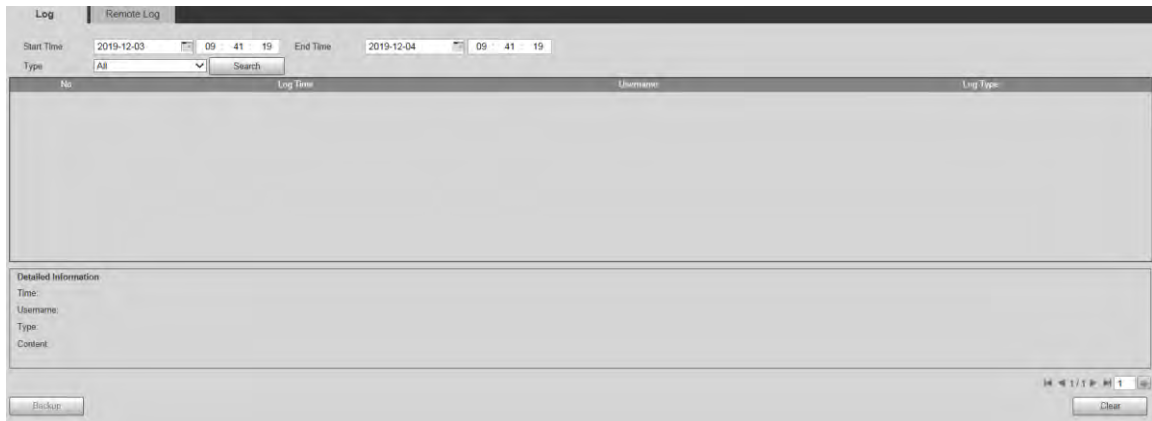



Table 5-55 Log parameter description

Parameter	Description
Start Time	The start time of the log to be searched (January 1, 2000 is the earliest time).
End Time	The end time of the log to be searched (December 31, 2037 is the latest time).
Type	The log type includes All, System, Setting, Data, Event, Record, Account, Clear Log, and Safety.
Search	Set the start time and end time of the log to be searched, select the log type, and then click Search . The searched log number and time period will be displayed.
Detailed Information	Click a log to display the details.
Clear	Clear all logs of the Device, and classified clearing is not supported.
Backup	Back up the searched system logs to the PC currently used by the user.  The data will be overwritten if the disk is full. Back up the data in time as needed.

Here are the meanings of different log types.

- **System**: Includes program launch, force exit, exit, program reboot, device shutdown/restart, system reboot, and system upgrade.
- **Setting**: Includes saving configurations, and deleting configuration files.
- **Data**: Includes disk type configurations, data erasing, hot swap, FTP state, and recording mode.
- **Event** (records events such as video detection, smart plan, alarm, and abnormality): Includes starting events, and ending events.
- **Record**: Includes file access, file access error, and file search.
- **Account** (records modification of user management, login, and logout): Includes login, logout, adding user, deleting user, modifying user, adding group, deleting group, and

modifying group.

- **Safety**: Includes security-related information.
- **Clear Log**: Clearing logs.

5.8.2.2 Remote Log

Upload the Device operations to the log server.

Step 1 Select **Setting > Information > Log > Remote Log**.

Figure 5-178 Remote log

Step 2 Select **Enable** to enable remote log function.

Step 3 Set the **IP Address**, **Port** and **Device Number** of the log server.



Click **Default** to restore the Device to the default settings.

5.8.3 Online User

Select **Setting > Information > Online User** to view online users.

Figure 5-179 Online users

No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	192.168.0.102	2010-10-26 10:10:10

5.8.4 Life Statistics

Select **Setting > Information > Life Statistics** to view the life statistics of the Device.



The function is available on select models.

Figure 5-180 Online users

Life Statistics	
Total Working Time	62 day(s) 1 hour(s) 0 minute(s)
Upgrade Times	20 time
Last Upgrade Date	2021-02-23 11:53:22

5.8.5 Battery Status

Select **Setting > Information > Battery Status** to view battery usage of the Device.



The function is available on select models.

Figure 5-181 Battery status

Battery Status	
Capacity Limit	100 %
Voltage	8.303 V
Charging or Not	No
<input type="button" value="Refresh"/>	

5.8.6 Legal Information

Select **Setting > Information > Legal Info** to view legal information of the Device. Click **Software License Agreement**, **Privacy Policy** and **Open Source Software Notice** to respectively view the corresponding content.



The function is available on select models.

Figure 5-182 Legal information



6 Alarm



You can select alarm types on the page. When the selected alarms are triggered, detailed alarm information will be displayed on the right side of the page. You can also select **Prompt** or **Play Alarm Tone**. When an alarm occurs, the alarm prompt or tone will be triggered.

Figure 6-1 Alarm setting page



Table 6-1 Description of alarm setting parameter

Category	Parameter	Description
Alarm Type	Motion Detection	Record alarm information in case of motion detection.
	Disk Full	Record alarm information in case of full disk.
	Disk Error	Record alarm information in case of disk error.
	Video Tamper	Record alarm information in case of video tampering.
	External Alarm	Record alarm information in case of an external alarm.
	Illegal Access	Record alarm information in case of illegal access.
	Audio Detection	Record alarm information in case of audio detection.
	IVS	Record alarm information in case of smart events.
	Scene Changing	Record alarm information in case of scene changing.
	Security Exception	Record alarm information in case of security exception.

Category	Parameter	Description
Operation	Prompt	<p>Select the Prompt check box. When you are not on the Alarm page, and the selected alarm event is triggered, the Relay-out button on the main menu will change to , and the alarm information will be automatically recorded. After you click the Alarm menu bar, the button disappears.</p> <p></p> <p>If you are on the Alarm page, there will be no image prompt when the selected alarm event is triggered, but the corresponding alarm information will be recorded in the alarm list on the right.</p>
Alarm Tone	Play Alarm Tone	Select the check box, and then select the tone file path. When the selected alarm event is triggered, the selected tone file will be played to prompt you that an alarm event is triggered.
	Tone Path	Customize the storage path for alarm tones.

7 Logout

Click **Logout** to log out, and the login page is displayed. Enter the username and password to log in again.

Figure 7-1 Login page



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883