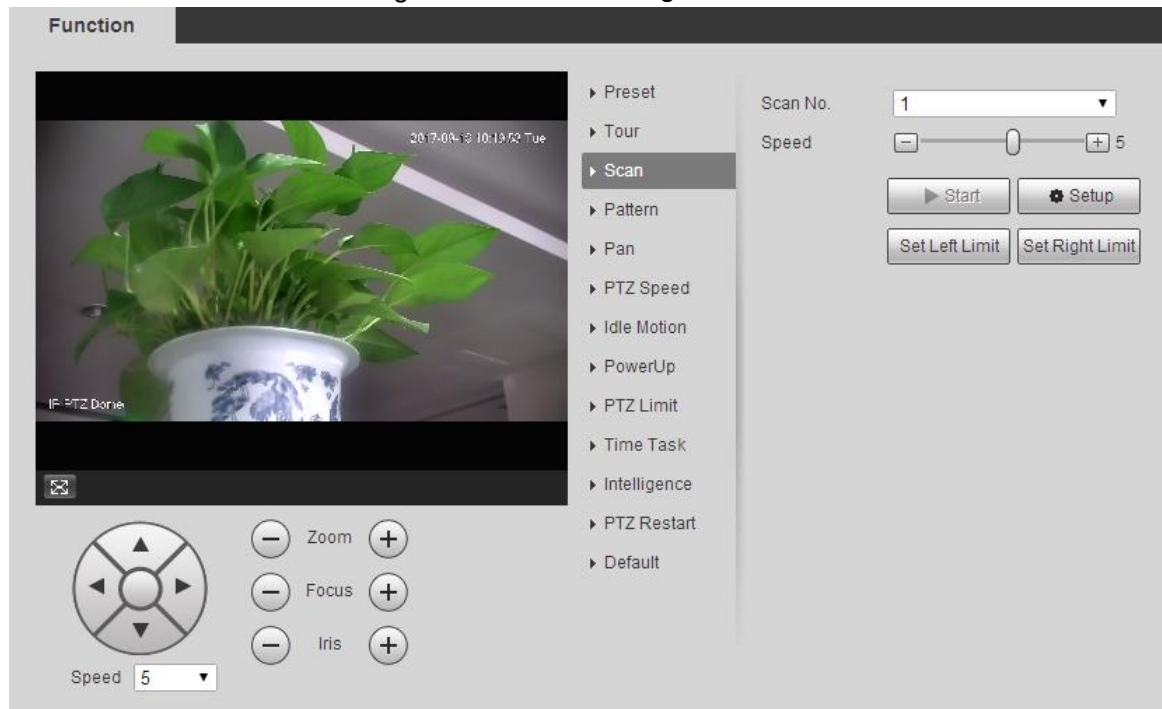


The **Scan** interface is displayed. See Figure 5-68.

Figure 5-68 Scan settings



Step 2 Select the **Scan No.**

Step 3 Drag the slider to adjust the scan speed.

Step 4 Click **Setup** to adjust the Device to an ideal position.

Step 5 Click **Set Left Limit** and **Set Right Limit** to set the left and right boundaries of the Device.

Step 6 Click **Start**, and the Device starts scanning.

Step 7 Click **Stop**, and the scanning stops.

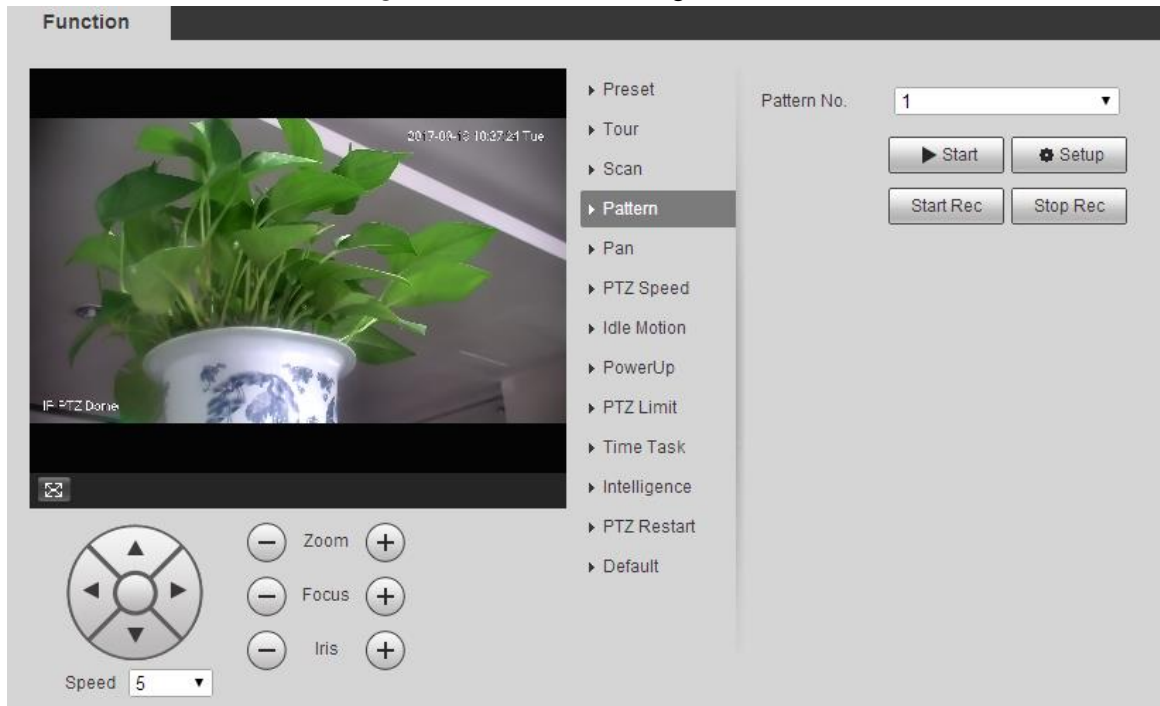
5.3.2.4 Pattern

Pattern means a record of a series of operations that users make to the Device. The operations include horizontal and vertical movements, zoom and preset calling. Record and save the operations, and then you can call the pattern path directly.

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

The **Pattern** interface is displayed. See Figure 5-69.

Figure 5-69 Pattern settings



Step 2 Select the **Pattern No.**

Step 3 Click **Setup** and **Start Rec**, and then operate the PTZ as needed.

Step 4 Click **Stop Rec** to stop recording.

Step 5 Click **Start**, and the Device starts patterning.

Step 6 Click **Stop**, and the patterning stops.

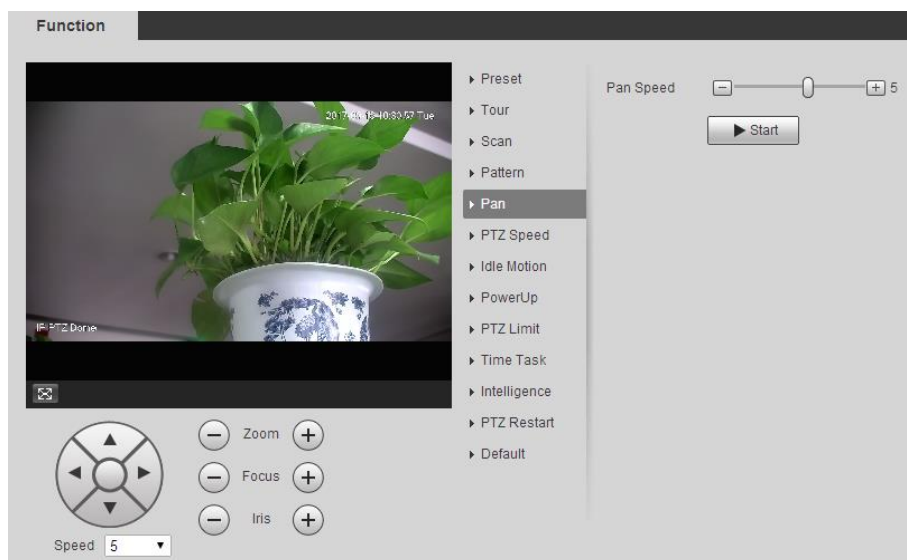
5.3.2.5 Pan

Pan refers to the continuous 360° rotation of the Device at a certain speed.

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

The **Pan** interface is displayed. See Figure 5-70.

Figure 5-70 Pan settings



Step 2 Drag the slider to set the **Pan Speed**.

Step 3 Click **Start**, and the Device starts to rotate horizontally at this speed.

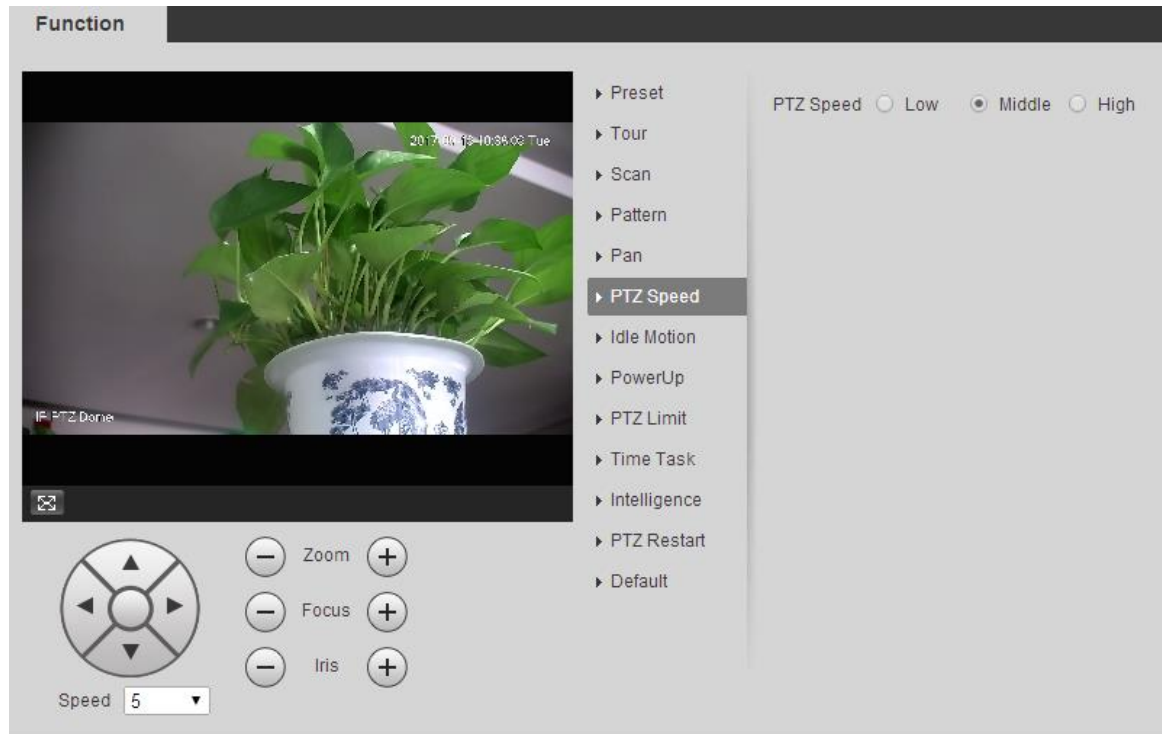
5.3.2.6 PTZ Speed

PTZ speed is the automatical running speed of the Device when touring, patterning, or auto tracking.

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

The **PTZ Speed** interface is displayed. See Figure 5-71.

Figure 5-71 PTZ speed settings



Step 2 Select **Low**, **Middle** or **High**.

The PTZ will operate at this speed.

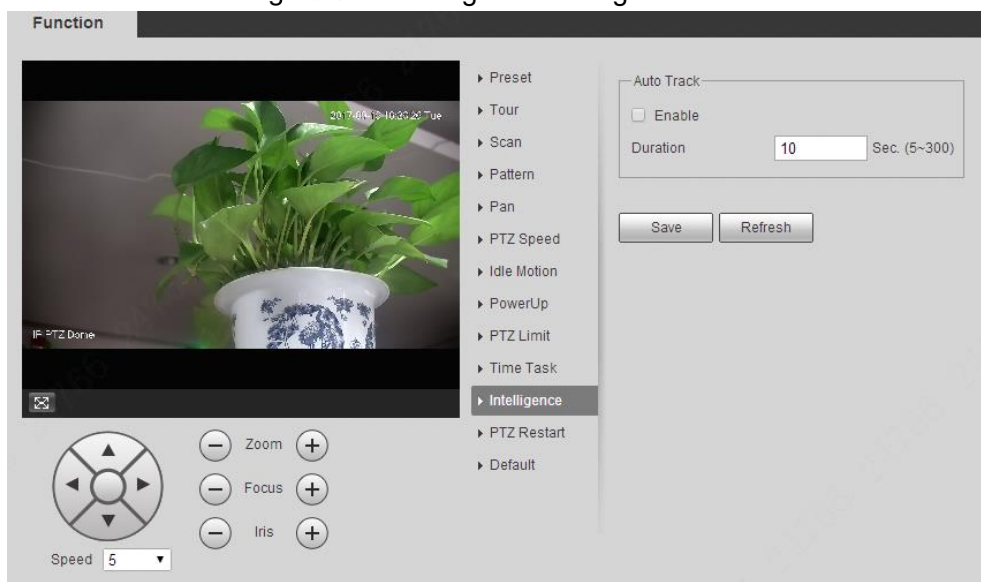
5.3.2.7 Intelligence

Set the duration of intelligent tracking.

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

The **Intelligence** interface is displayed. See Figure 5-72.

Figure 5-72 Intelligence settings



Step 2 Select the **Enable** check box, and intelligent tracking is enabled.

Step 3 Enter the duration of intelligent tracking.

Step 4 Click **Save**.



The function is available on select models.

5.3.2.8 Idle Motion

Idle motion refers to a set motion when the Device does not receive any valid command within a certain period.

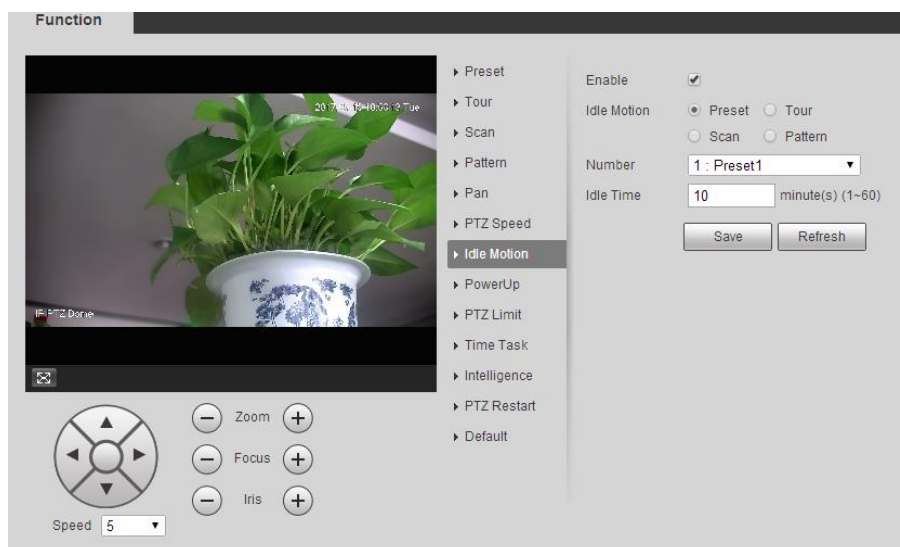


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

Step 1 Select **Setting > PTZ > Function > Idle Motion**.

The **Idle Motion** interface is displayed. See Figure 5-73.

Figure 5-73 Idle motion settings



Step 2 Select the **Enable** check box to enable the idle motion.

Step 3 Select idle motion from **Preset**, **Tour**, **Scan** and **Pattern**.

Step 4 Select the action number of the selected motion.

Step 5 Set **Idle Time** for the selected motion.

Step 6 Click **Save**.

5.3.2.9 PowerUp

PowerUp means the automatic operation of the Device after it is powered on.

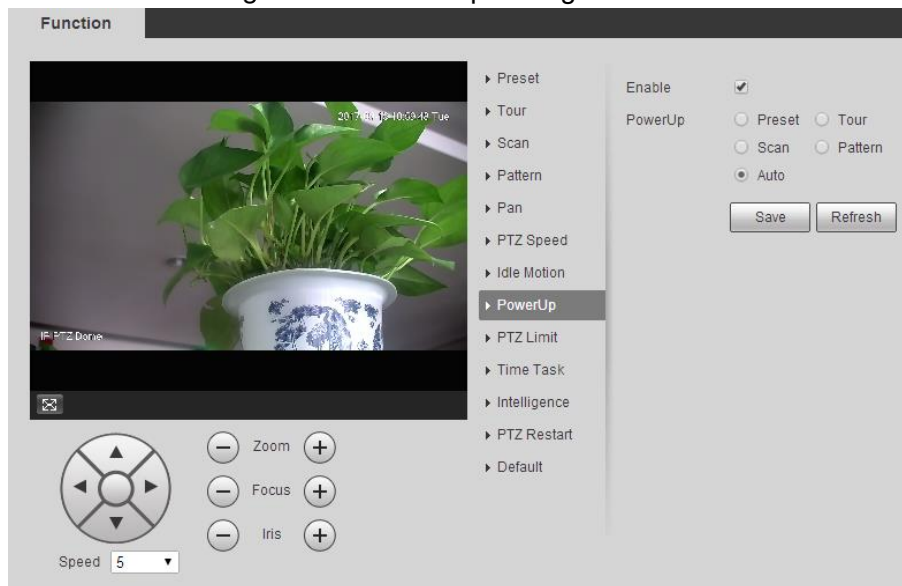


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

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

The **PowerUp** interface is displayed. See Figure 5-74.

Figure 5-74 PowerUp settings



Step 2 Select the **Enable** check box 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**.

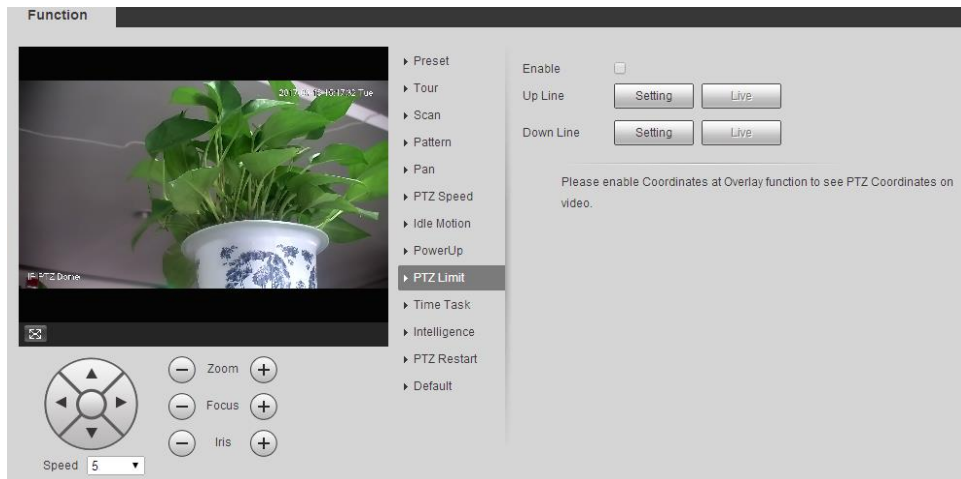
5.3.2.10 PTZ Limit

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

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

The **PTZ Limit** interface is displayed. See Figure 5-75.

Figure 5-75 PTZ limit settings



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

Step 3 Adjust the PTZ direction and 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** check box to enable the PTZ limit function.

5.3.2.11 Time Task

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

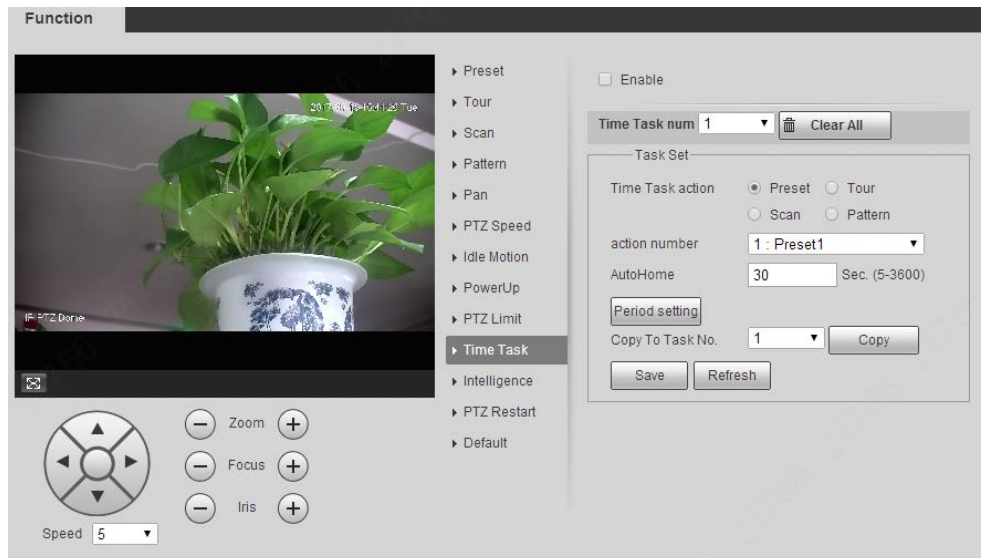


Set **Preset**, **Tour**, **Scan** or **Pattern** in advance.

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

The **Time Task** interface is displayed. See Figure 5-76.

Figure 5-76 Time task settings



Step 2 Select the **Enable** check box 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**.

5.3.2.12 PTZ Restart

Restart the PTZ. Follow these steps to complete the configuration.

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

The **PTZ Restart** interface is displayed. See Figure 5-77.

Figure 5-77 PTZ restart



Step 2 Click **PTZ Restart**.

The PTZ is restarted.

5.3.2.13 Default

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**.

The **Default** interface is displayed. See Figure 5-78.

Figure 5-78 Default setting



Step 2 Click **Default**.

The PTZ will be restored to factory defaults.

5.4 Event Management

5.4.1 Video Detection

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

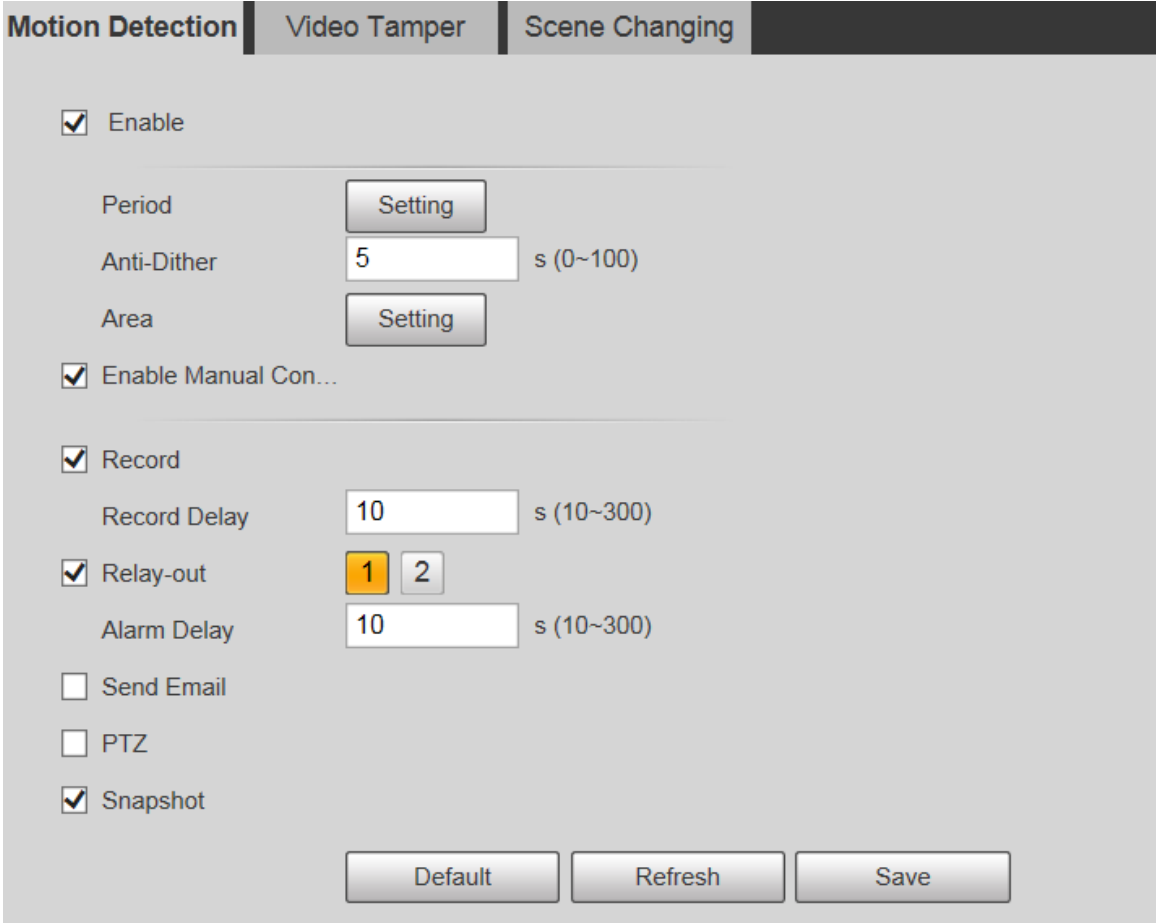
5.4.1.1 Motion Detection

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**.

The **Motion Detection** interface is displayed. See Figure 5-79.

Figure 5-79 Motion detection settings



The image shows a web-based configuration interface for motion detection. At the top, there are three tabs: 'Motion Detection' (selected), 'Video Tamper', and 'Scene Changing'. The 'Motion Detection' tab contains several settings:

- ☒ **Enable**
- Period**: A button labeled 'Setting'.
- Anti-Dither**: A text input field with the value '5' and a unit 's (0~100)'.
- Area**: A button labeled 'Setting'.
- ☒ **Enable Manual Con...**
- ☒ **Record**
- Record Delay**: A text input field with the value '10' and a unit 's (10~300)'.
- ☒ **Relay-out**: Two buttons labeled '1' and '2', with '1' highlighted in orange.
- Alarm Delay**: A text input field with the value '10' and a unit 's (10~300)'.
- ☐ **Send Email**
- ☐ **PTZ**
- ☒ **Snapshot**

At the bottom of the interface, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Select the **Enable** check box, and then configure parameters as needed.

- Set arming and disarming period.

1) Click **Setting**, and then set the arming and disarming period on the interface. See Figure 5-80.

Figure 5-80 Arming and disarming period settings

The 'Period' settings window displays a 24-hour timeline at the top. Below the timeline, seven rows represent the days of the week (Sun to Sat). Each row has a green bar indicating the active period. To the right of each row is a 'Setting' button. Below the days, there are checkboxes for 'All', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. The 'Sun' checkbox is checked. Below these are six 'Period' settings (Period1 to Period6). Each period has a checkbox and a time range selector (HH : MM : SS - HH : MM : SS). Period1 is checked and shows a time range of 00 : 00 : 00 - 23 : 59 : 59. At the bottom are 'Save' and 'Cancel' buttons.

- 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 period to enable it.
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** interface.
- Set the area.
Click **Setting**, and the **Area** interface is displayed. See Figure 5-81. Refer to Table 5-24 and Table 5-25 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 5-81 Area setting

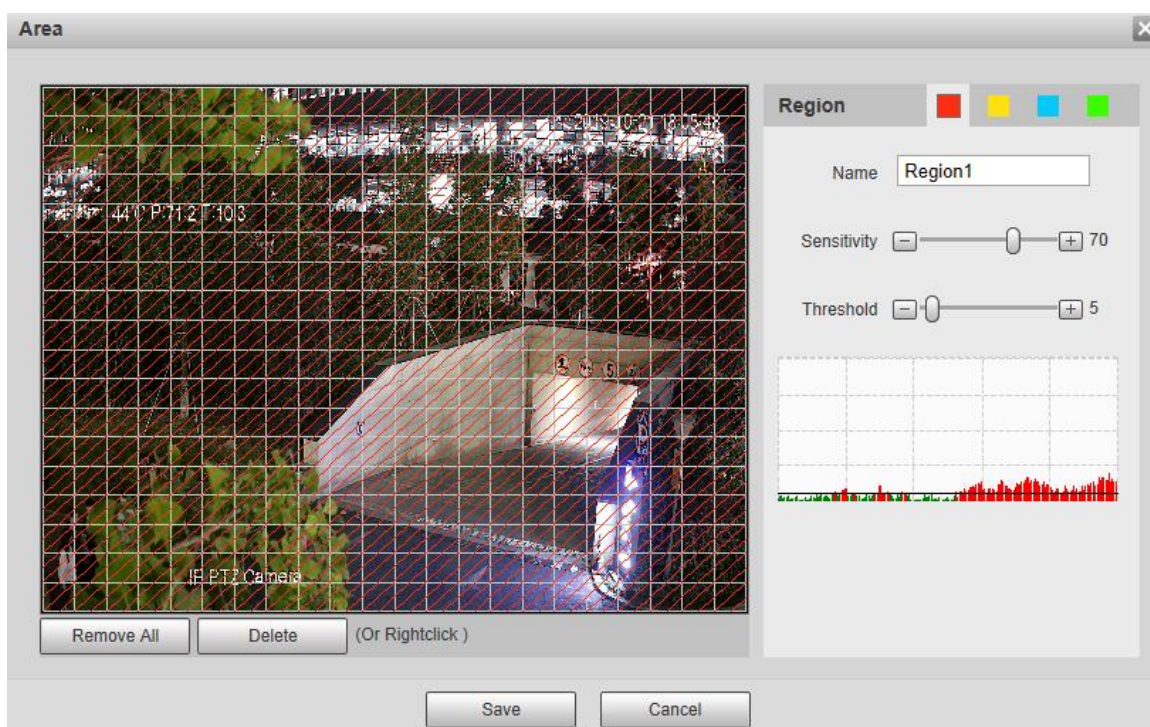


Table 5-24 Area setting parameter description

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 5-25 Video detection parameter description

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.

Parameter	Description
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 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**.

5.4.1.2 Video Tamper

Alarms will be triggered if there is video tampering.

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

The **Video Tamper** interface is displayed. See Figure 5-82.

Figure 5-82 Video tamper settings

Motion Detection | **Video Tamper** | Scene Changing

☐ Enable

Period Setting

☒ Record

Record Delay s (10~300)

☒ Relay-out 1 2

Alarm Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default Refresh Save

Step 2 Select the **Enable** check box, and then configure parameters as needed.



For parameters configuration, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.1.3 Scene Changing

Alarms will be triggered if there is scene changing.

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

The **Scene Changing** interface is displayed. See Figure 5-83.

Figure 5-83 Scene changing settings

Motion Detection | Video Tamper | **Scene Changing**

☐ Enable

Period Setting

☒ Record

Record Delay s (10~300)

☒ Relay-out 1 2

Alarm Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default Refresh Save

Step 2 Select the **Enable** check box, and then configure parameters as needed.



For parameters configuration, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.2 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.

Preparation

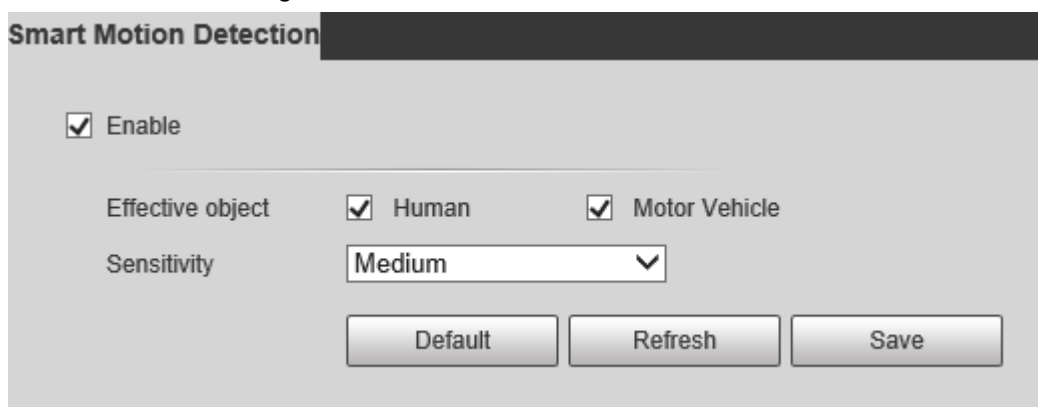
- Select **Setting > Event > Video Detection > Motion Detection**, and then enable the motion detection function.
- Set the arming period and detection area. The sensitivity of each region is larger than 0, and the threshold is not equal to 100.

Procedure

Step 4 Select **Setting > Event > Smart Motion Detection**.

The **Smart Motion Detection** interface is displayed. See Figure 5-84.

Figure 5-84 Smart motion detection



The screenshot shows the 'Smart Motion Detection' configuration window. At the top, the title 'Smart Motion Detection' is visible. Below the title, there is a section with a checked checkbox labeled 'Enable'. Underneath, there are two options for 'Effective object': 'Human' and 'Motor Vehicle', both of which are checked. Below these, there is a 'Sensitivity' dropdown menu currently set to 'Medium'. At the bottom of the window, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 5 Select the **Enable** check box, and then the **Smart Motion Detection** is enabled.

Step 6 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.

Step 7 Click **Save**.

5.4.3 Audio Detection

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

The **Audio Detection** interface is displayed. See Figure 5-85.

Figure 5-85 Audio detection settings

Step 2 Configure parameters as needed. For the parameter description, see Table 5-26.

Table 5-26 Audio detection parameter description

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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.4 Smart Plan

Each preset can be configured with different smart functions. You need to select a certain function for it to come into effect.

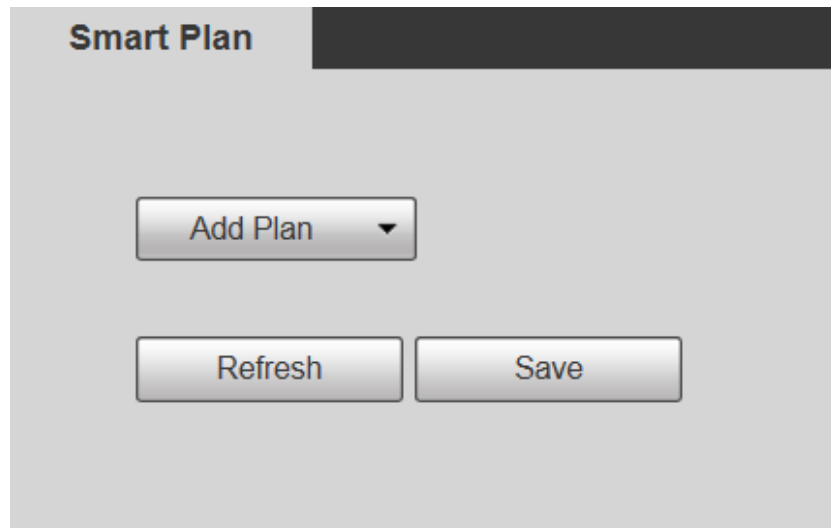


Before configuring the smart plan, you need to set presets in advance. For setting methods, see "5.3.2.1 Preset."

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

The **Smart Plan** interface is displayed, see Figure 5-86.

Figure 5-86 Smart plan (1)



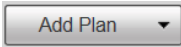
Step 2 Click  to select the presets to be configured. See Figure 5-87.

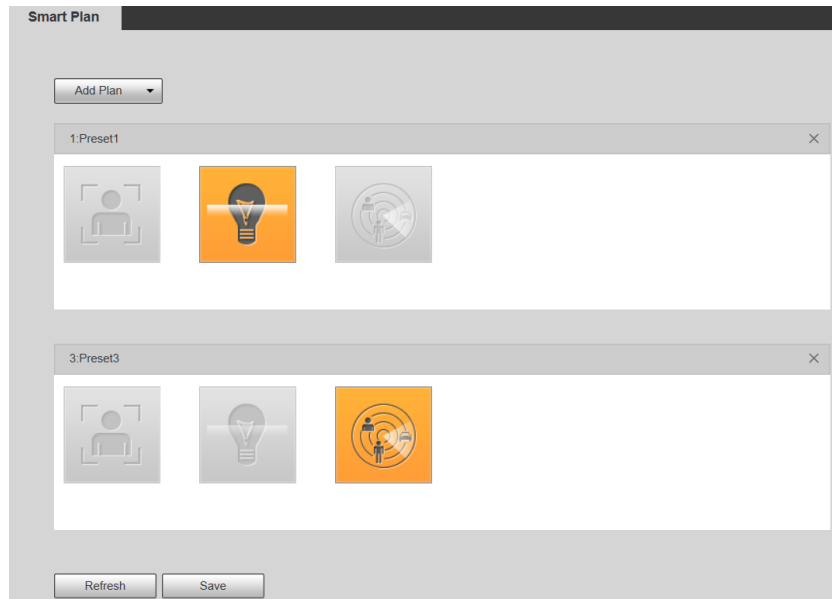
Figure 5-87 Smart plan (2)



Step 3 Select smart function as needed.

The selected function will be highlighted. See Figure 5-88. Click it again to cancel the selection.

Figure 5-88 Smart plan (3)



Step 4 Click **Save**.

5.4.5 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."

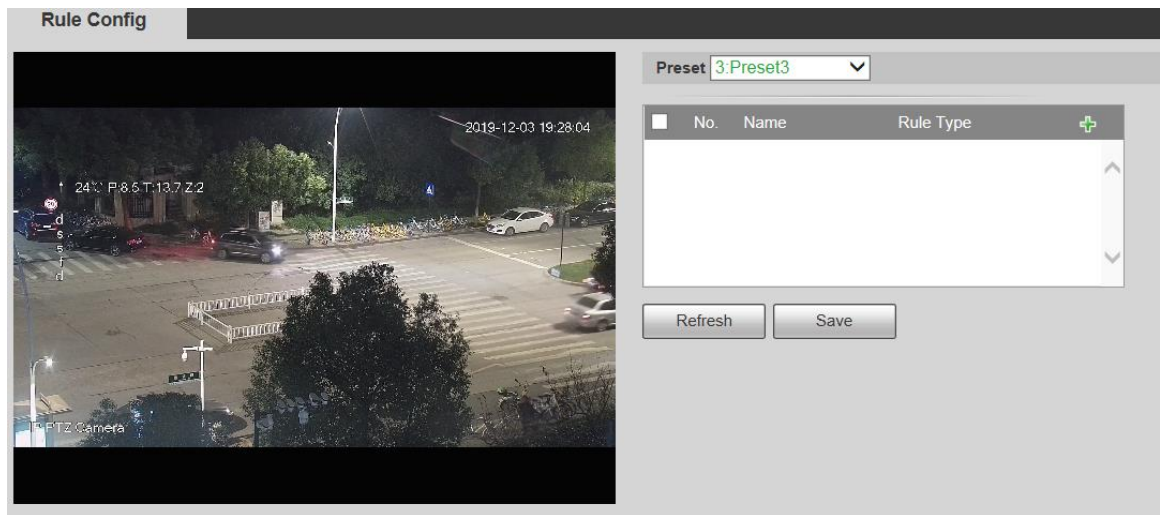
5.4.5.1 Rule Config

Set smart rules. Follow these steps to complete the configuration.

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

The **Rule Config** interface is displayed. See Figure 5-89.

Figure 5-89 Adding smart rules



Step 2 Select the presets to be configured with smart rules.

Step 3 Click  to add smart rules.



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

Step 4 Click **Save**.

5.4.5.1.1 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.

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

The configuration interface is displayed. See Figure 5-90.

Figure 5-90 Tripwire rule settings

Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Table 5-27 Rule drawing parameter description

Parameter	Description
Max Size	Set the size range of detection targets to be filtered, and select the maximum or minimum size.
Min Size	- 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.
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.
Lock/Unlock	Enter the rule configuration interface, 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.  The locking function only takes effect in the rule configuration interface. After switching to the Live interface, the Device can track the target normally.

Step 3 Configure parameters as needed. For the parameter description, see Table 5-28.

Table 5-28 Tripwire parameter description

Parameter	Description
Period	 Set the alarming period to enable alarm events in the period you set. 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 setting each day. Select the check box next to the period, and the set period will be effective. 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 return 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 an 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 in 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**.

5.4.5.1.2 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.

The configuration interface is displayed. See Figure 5-91.

Figure 5-91 Intrusion settings

Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-29.

Table 5-29 Intrusion parameter description

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 "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.5.1.3 Abandoned Object

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

The configuration interface is displayed. See Figure 5-92.

Figure 5-92 Abandoned object settings

Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-30.

Table 5-30 Abandoned object parameter description

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 "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.5.1.4 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.

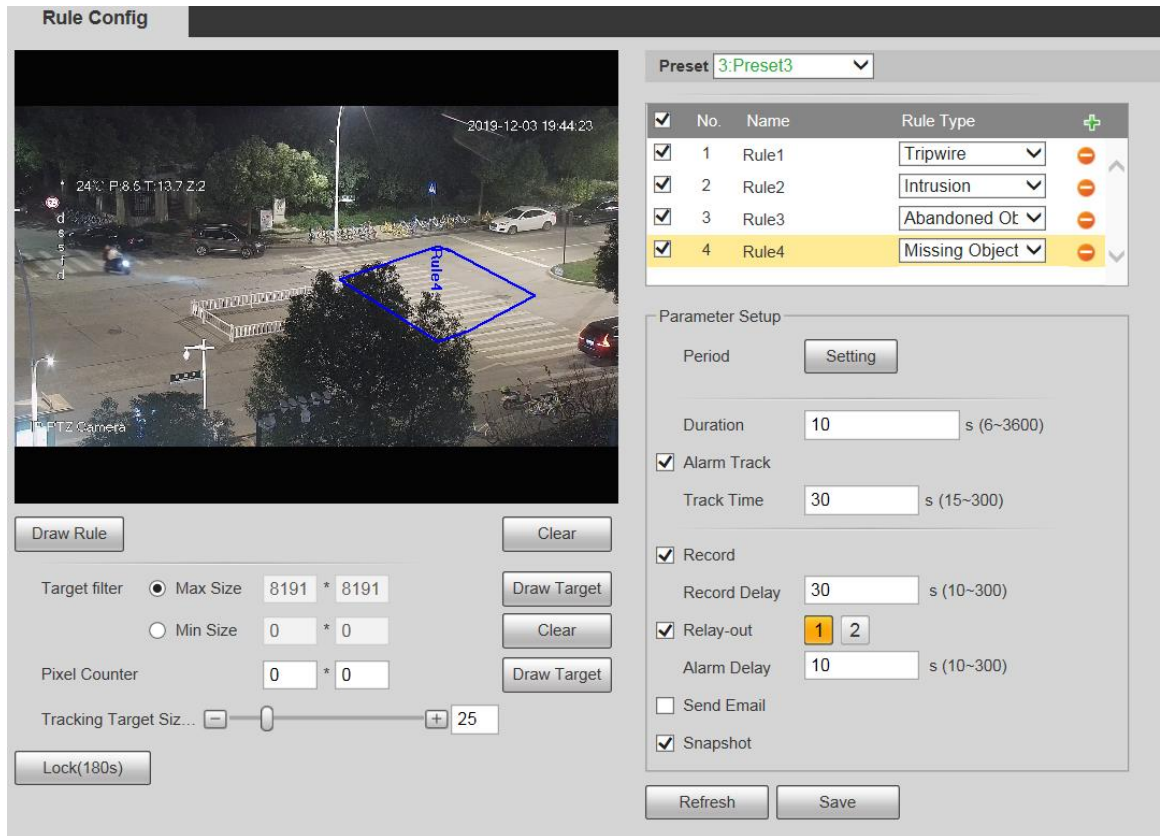
The system analyzes static areas from the foreground, and determines whether it is missing object or abandoned object from the similarity of its foreground and background. When the time exceeds the set period, an alarm is triggered.

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 **Moving Object** from the **Rule Type** list.

The configuration interface is displayed. See Figure 5-93.

Figure 5-93 Missing object setting



Step 2 Click **Draw Rule**, and you can draw rules on the monitoring screen. For parameter description, see Table 5-27.



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

Step 3 Configure parameters as needed. For the parameter description, see Table 5-31.

Table 5-31 Missing object parameter description

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

For other parameters, see "5.4.5.1.1 Tripwire."

Step 4 Click **Save**.

5.4.6 Face Recognition



- Select **Setting > Event > Smart Plan**, and then enable face recognition.

- This function is available on select models.

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

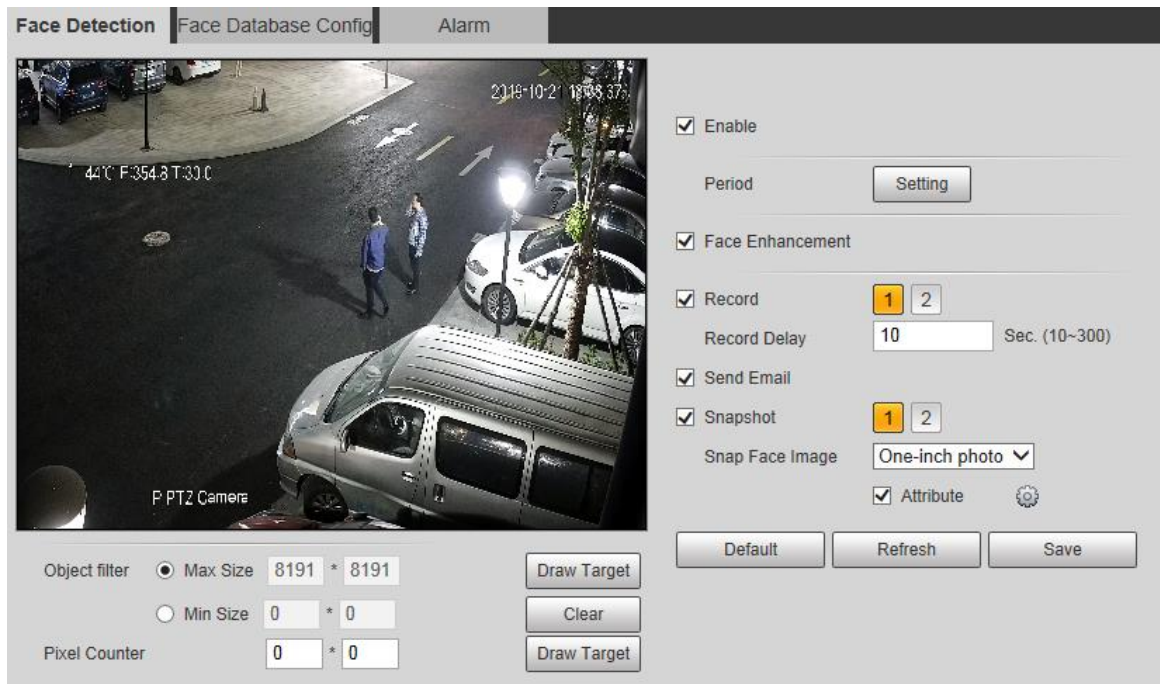
5.4.6.1 Face Detection

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

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

The **Face Detection** interface is displayed. See Figure 5-94.

Figure 5-94 Face detection interface



Step 2 Select **Enable**, and you can enable the face detection function.

Step 3 Configure parameters as needed. For the parameter description, see Table 5-32.

Table 5-32 Face detection parameter description

Parameter	Description
Period	Alarm event will be triggered only within the defined time period. See "5.4.1.1 Motion Detection."
Face Enhancement	Select Face Enhancement to preferably guarantee clear faces with low stream.
Record	Select Record, and the system records video when alarms are triggered.  To enable video recording, you need to make sure that: • The motion detection recording is enabled. For details, see "5.5.1.1 Record." • The auto recording is enabled. For details, see "5.5.4 Record Control."
Record Delay	The video recording will not stop until the record delay time you set has passed.

Parameter	Description
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	Select Snapshot , and the system takes snapshot when alarms are triggered.  - Enable the motion detection snapshot first. For details, see "5.5.1.1 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**.

5.4.6.2 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 pictures, and face modeling.

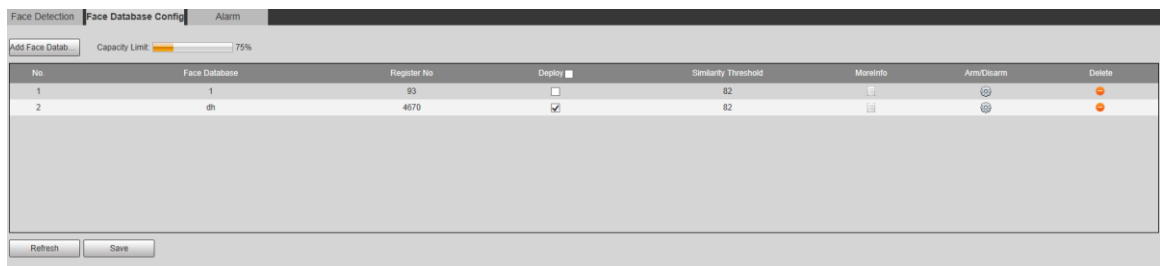
5.4.6.2.1 Adding Face Database

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

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

The **Face Database Config** interface is displayed. See Figure 5-95.

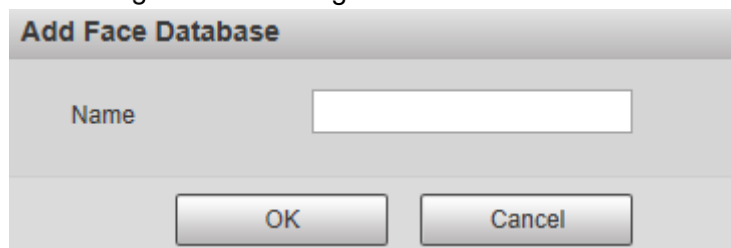
Figure 5-95 Face database config



Step 2 Click **Add Face Database**.

The **Add Face Database** interface is displayed. See Figure 5-96.

Figure 5-96 Adding face database

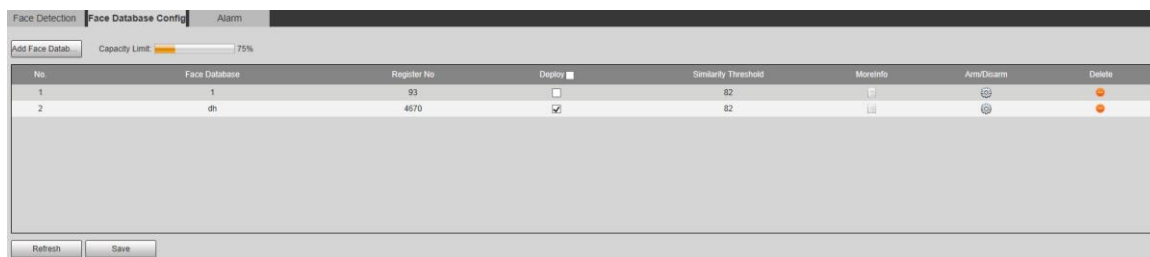


Step 3 Set face database name.

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

The added face database is displayed. See Figure 5-97.

Figure 5-97 Adding face database completed



Step 5 Configure parameters as needed. For the parameter description, see Table 5-33.

Table 5-33 Face database config parameter description

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 interface.
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. See "5.4.1.1 Motion Detection."
Delete	Delete the selected face database.

5.4.6.2.2 Adding Face Pictures

Add face pictures to the created face database. Manual addition and batch import are supported.

Manual Addition

Add a single face picture. Use this method when registering a small number of face pictures.

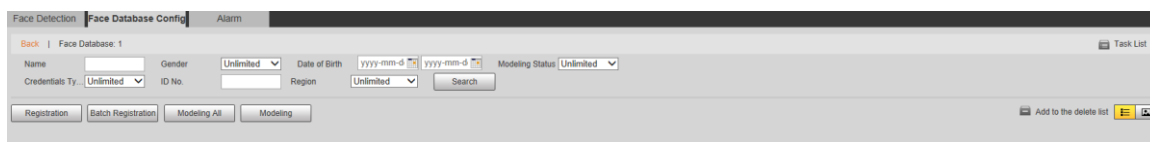
Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

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

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

The interface is displayed. See Figure 5-98.

Figure 5-98 More info

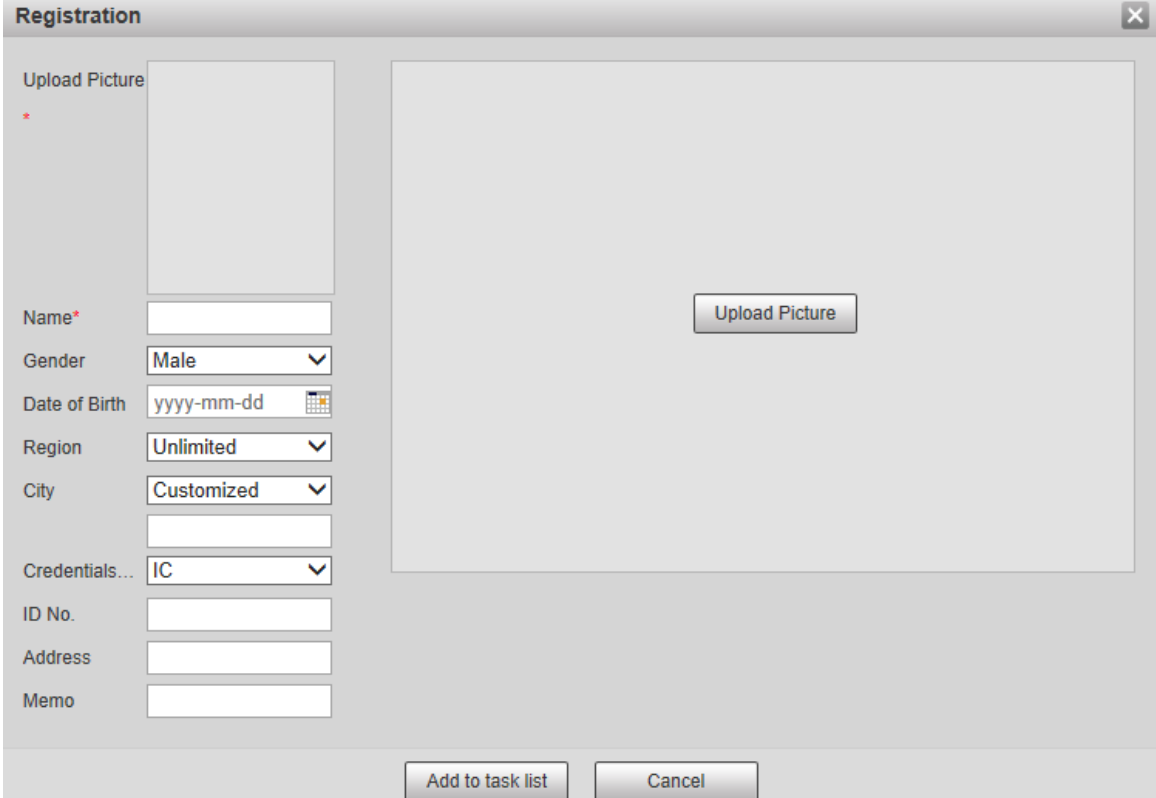


Set filtering conditions as needed, and then click **Search**. The search result is displayed.

Step 3 Click **Registration**.

The **Registration** interface is displayed. See Figure 5-99.

Figure 5-99 Registration interface



The image shows a software window titled "Registration" with a close button in the top right corner. The window is divided into two main sections. On the left is a form with several fields: "Upload Picture" with a red asterisk and a large empty box; "Name*" with a text input; "Gender" with a dropdown menu showing "Male"; "Date of Birth" with a text input showing "yyyy-mm-dd" and a calendar icon; "Region" with a dropdown menu showing "Unlimited"; "City" with a dropdown menu showing "Customized" and a text input; "Credentials..." with a dropdown menu showing "IC"; "ID No." with a text input; "Address" with a text input; and "Memo" with a text input. On the right is a large empty rectangular area. In the center of this area is a button labeled "Upload Picture". At the bottom of the window are two buttons: "Add to task list" and "Cancel".

Step 4 Click **Upload Picture**.

Import the face pictures to be uploaded. The interface is displayed. See Figure 5-100.



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 picture, select the target face and click **OK** to save the face picture.

Figure 5-100 Addition completed

The Registration window contains the following elements:

- Upload Picture:** A small thumbnail of the man's face and a large preview window showing the full face. The preview window has "OK" and "Cancel" buttons at the top.
- Form Fields:**
 - Name* (text input)
 - Gender (dropdown menu, currently "Male")
 - Date of Birth (calendar icon and "yyyy-mm-dd" text)
 - Region (dropdown menu, currently "Unlimited")
 - City (dropdown menu, currently "Customized")
 - Credentials... (dropdown menu, currently "IC")
 - ID No. (text input)
 - Address (text input)
 - Memo (text input)
- Buttons:** "Add to task list" and "Cancel" at the bottom right.

Step 5 Fill in face picture information as needed.

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

Step 7 Click  **Task List 1**.

The **Task List** interface is displayed. See Figure 5-101.

Figure 5-101 Task list addition completed

The Task List window displays a table with the following data:

Add	Status
1	Stored successfully., Modeling failed.:4(Picture Decoding Error)
Modify	Status
Delete	Status

Buttons at the bottom: "OK" and "Remove All".



Click **Remove All**, and you can remove all the tasks.

Batch Registration

Import multiple face pictures in batch. Use this method when registering a large number of face pictures.

Before importing pictures in batches, name the face pictures 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"). For naming rules, see Table 5-34.



Name is required and the rest are optional.

Table 5-34 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.

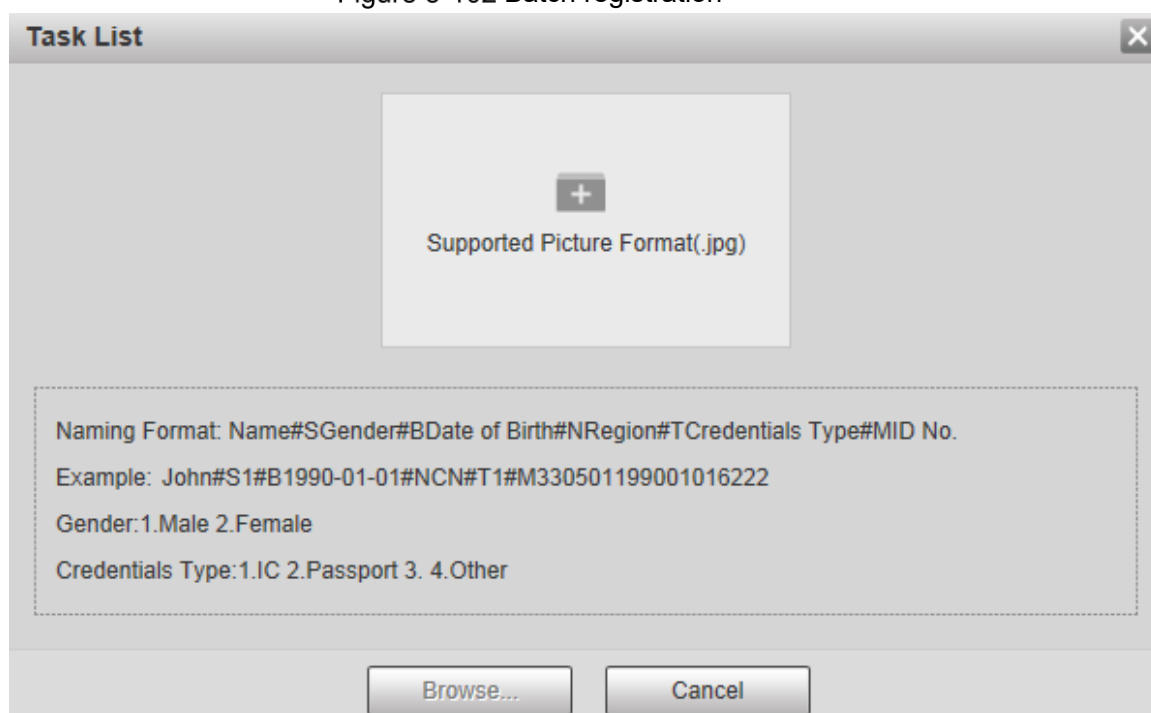
Step 2 Click  **More Info** for the face database to be configured.

The **Face Database** interface is displayed.

Step 3 Click **Batch Registration.**

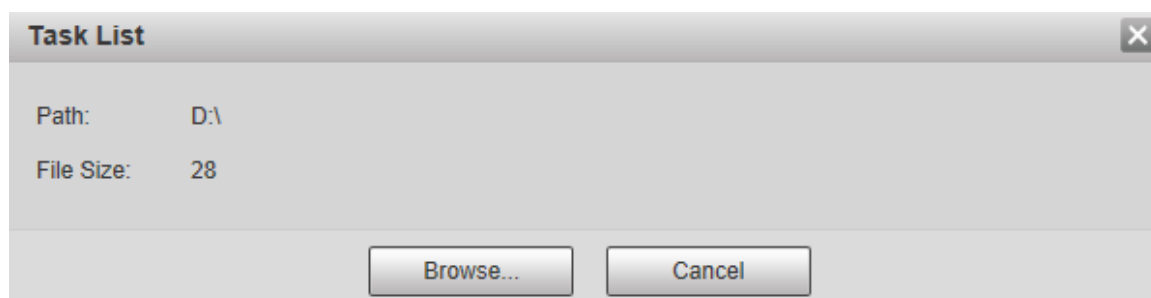
The **Task List** interface is displayed. See Figure 5-102.

Figure 5-102 Batch registration



Step 4 Click  to select the file path.

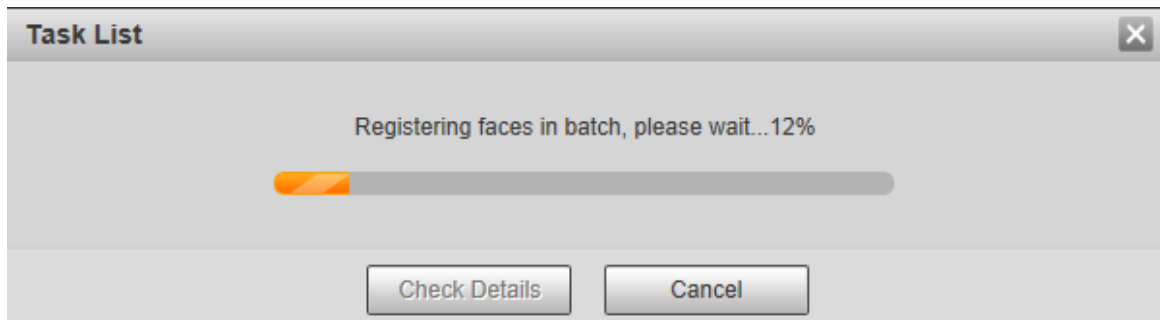
Figure 5-103 Batch registration



Step 5 Click **Browse.**

The registering interface is displayed. See Figure 5-103.

Figure 5-104 Registering



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

5.4.6.2.3 Managing Face Pictures

Add face pictures to face database; manage and maintain face pictures to ensure correct information.

Modifying Face Information

On the **Face Database Config** interface, move the mouse pointer to the face picture or person information line. Click  or , and the **Registration** interface is displayed. See Figure 5-105. After modifying the face picture information as needed, click **Add to task list**.

Figure 5-105 Registration interface

A "Registration" dialog box with a close button (X) in the top right corner. On the left, there is a form with the following fields: "Upload Picture" (with a red asterisk and a placeholder image of a man's face), "Name*" (text input), "Gender" (dropdown), "Date of Birth" (text input with "yyyy-mm-dd" and a calendar icon), "Region" (dropdown with "Unlimited"), "City" (dropdown with "Customized"), "Credentials..." (dropdown with "Other"), "ID No." (text input), "Address" (text input), and "Memo" (text input). On the right, there is a large empty rectangular area with an "Upload Picture" button in the center. At the bottom, there are two buttons: "Add to task list" and "Cancel".

Deleting Face Pictures

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

- Single deletion: Move the mouse pointer to the face picture or people information line, and then click  or  to delete the face picture.

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

5.4.6.2.4 Face Modeling

Extract and import the relevant information of face pictures into the database through face modeling, and create a face feature mode for smart detection such as face comparison.



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

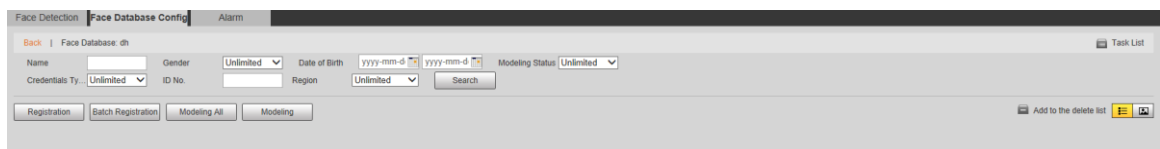
Step 1 Select **Setting > Event > Face Recognition > Face Database Config**.

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. See Figure 5-106.

Figure 5-106 Face database interface



Step 3 Choose the face pictures for modeling as needed.



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

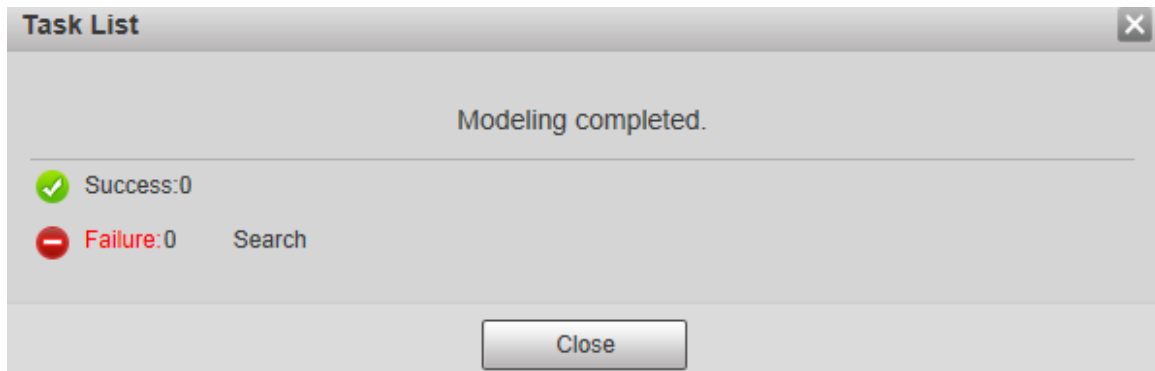
- Modeling All

Click **Modeling All**, and all face pictures in the face database will be modeled.

- Selective Modeling

If there are many face pictures in the face database, set filtering conditions and click **Search** to select face pictures for modeling.

Figure 5-107 Modeling completed



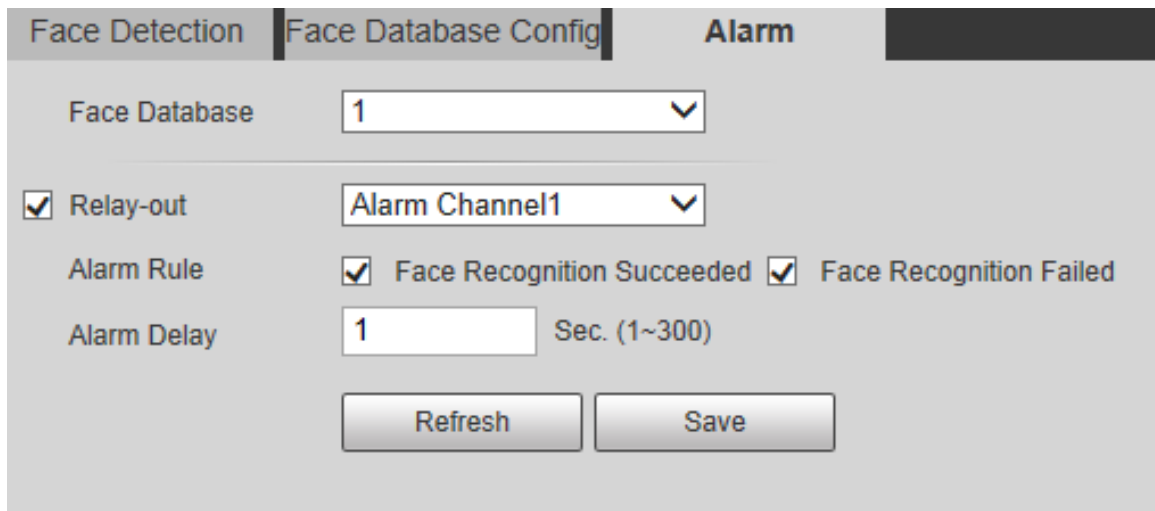
5.4.6.3 Alarm Linkage

Set the alarm linkage mode for face comparison.

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

The **Alarm** interface is displayed. See Figure 5-108.

Figure 5-108 Alarm linkage



Step 2 Configure parameters as needed. For the parameter description, see Table 5-35.

Table 5-35 Alarm linkage parameter description

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**.

5.4.7 People Counting



- 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.

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

5.4.7.1 People Counting

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

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

The **People Counting** interface is displayed. See Figure 5-109.

Figure 5-109 People counting settings

No.	Name	Rule Type
1	Rule3	People Counting

Parameter Setup

OSD

Period

Flowrate Alarm

Enter No.

Leave No.

Stranded No.

☐ Record

Record Delay s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Global Setup

Sensitivity

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 5-27.



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

Step 4 Configure parameters as needed. For the parameter description, see Table 5-36.

Table 5-36 People counting parameter description

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, refer to "5.4.5.1.1 Tripwire."

Step 5 Click **Save**.

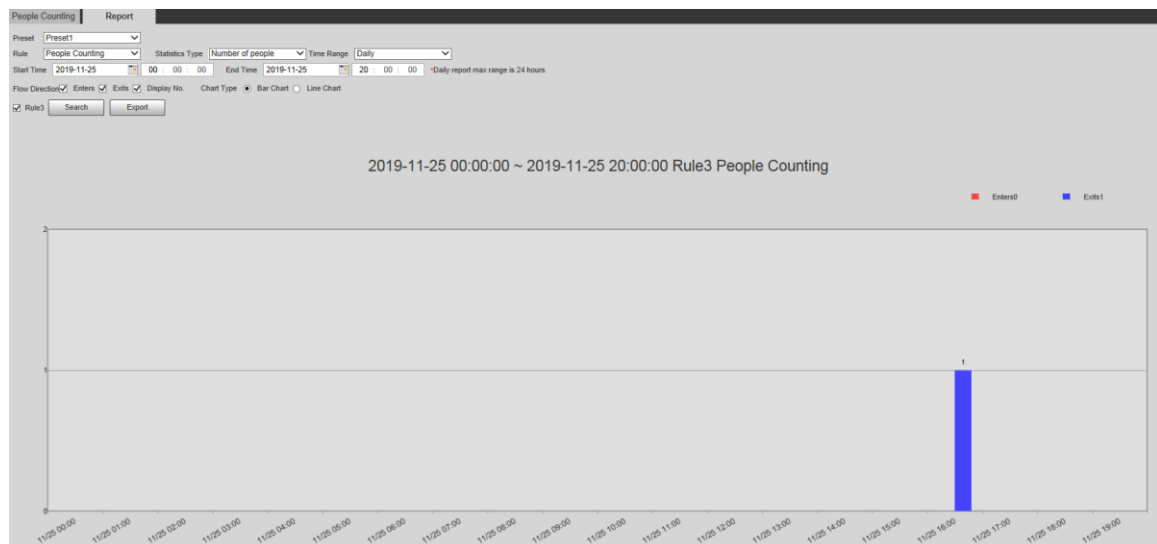
5.4.7.2 Report

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

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

The **Report** interface is displayed. See Figure 5-110.

Figure 5-110 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 click **Export** to export the report to local storage.

5.4.8 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 as needed.

- This function is available on select models.

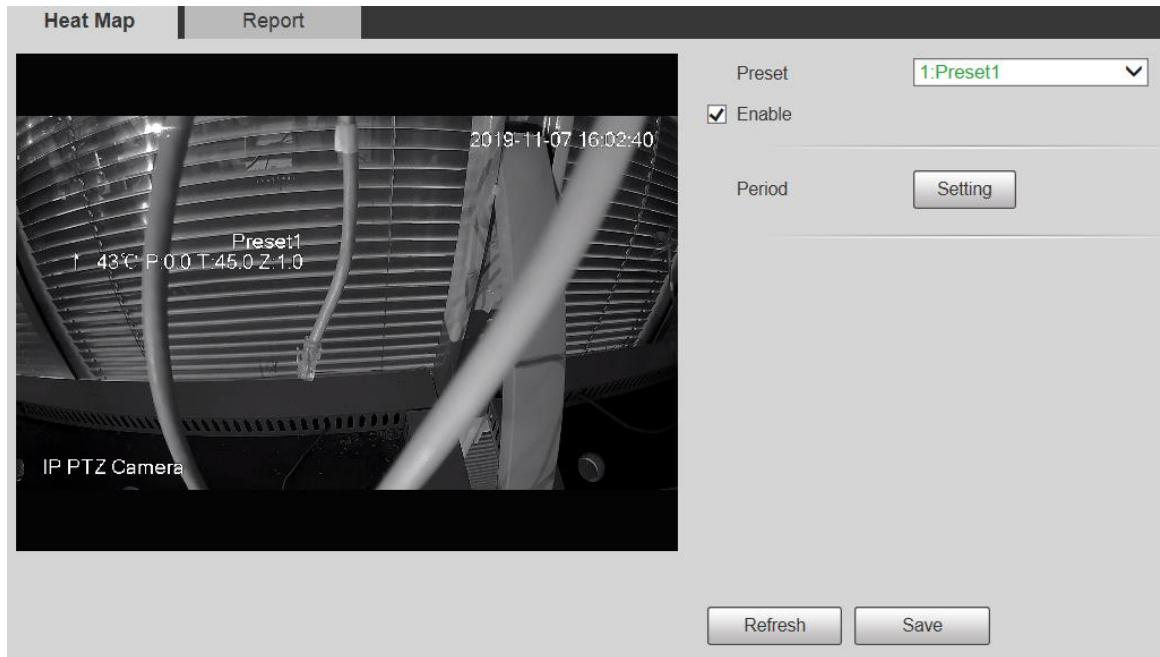
5.4.8.1 Heat Map

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

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

The **Heat Map** interface is displayed. See Figure 5-111.

Figure 5-111 Heat map interface



Step 2 Select the presets to be configured.

Step 3 Select the **Enable** check box, and then the heat map function is enabled.

Step 4 Click **Setting** to set the arming period. For details, see "5.4.1.1 Motion Detection."

Step 5 Click **Save**.

5.4.8.2 Report

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

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

The **Report** interface is displayed.

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 interface. See Figure 5-112.

Figure 5-112 Report



5.4.9 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.

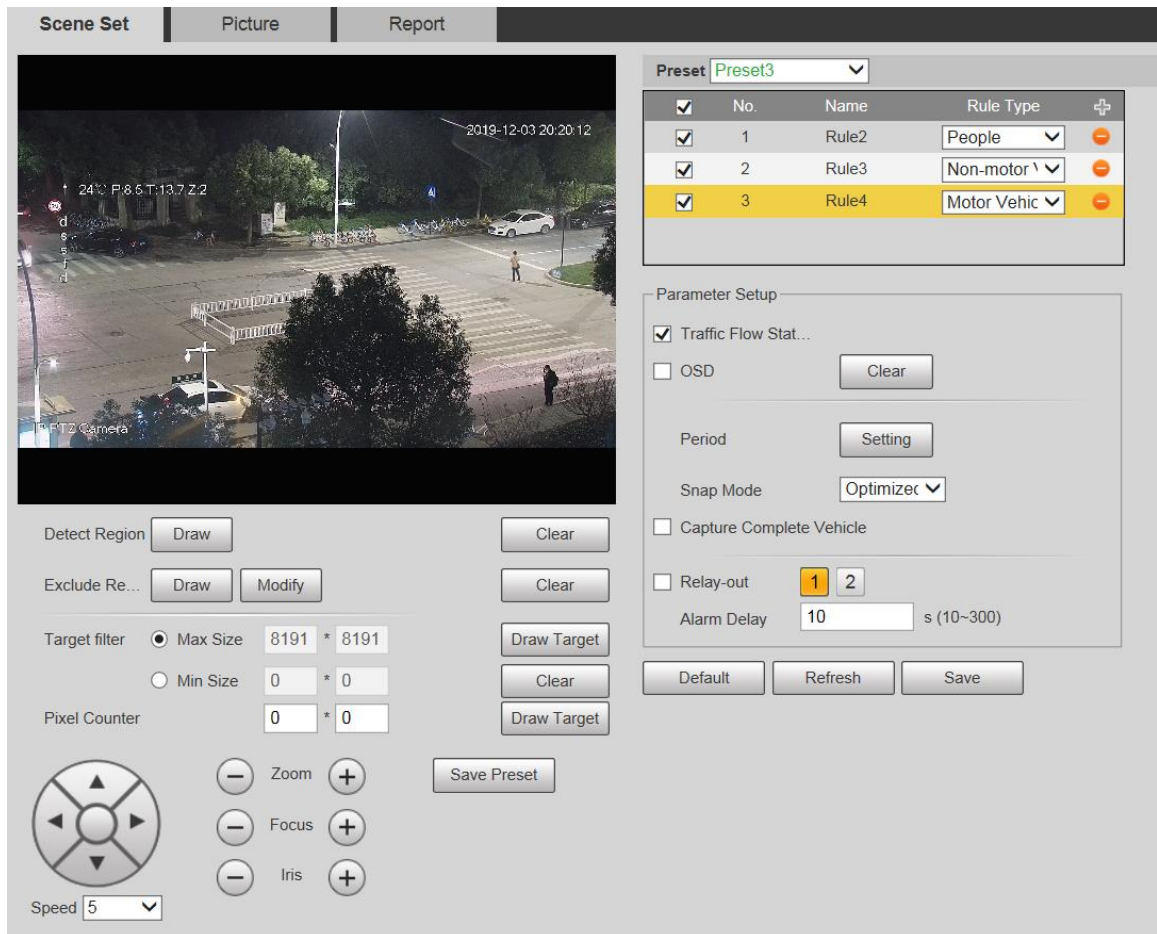
5.4.9.1 Scene Setting

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

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

The **Scene Set** interface is displayed. See Figure 5-113.

Figure 5-113 Video metadata–scene set



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 as needed.

- 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 parameters as needed. For parameter description, see Table 5-37.

Table 5-37 Scene set parameter description

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 interface 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 "5.4.5.1.1 Tripwire."

Step 6 Click **Save**.

5.4.9.2 Picture Overlay

Set the overlay information on the snapshot.

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

The **Picture** interface is displayed.

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

See Figure 5-114, Figure 5-115 and Figure 5-116.

Figure 5-114 Picture overlay–motor vehicle

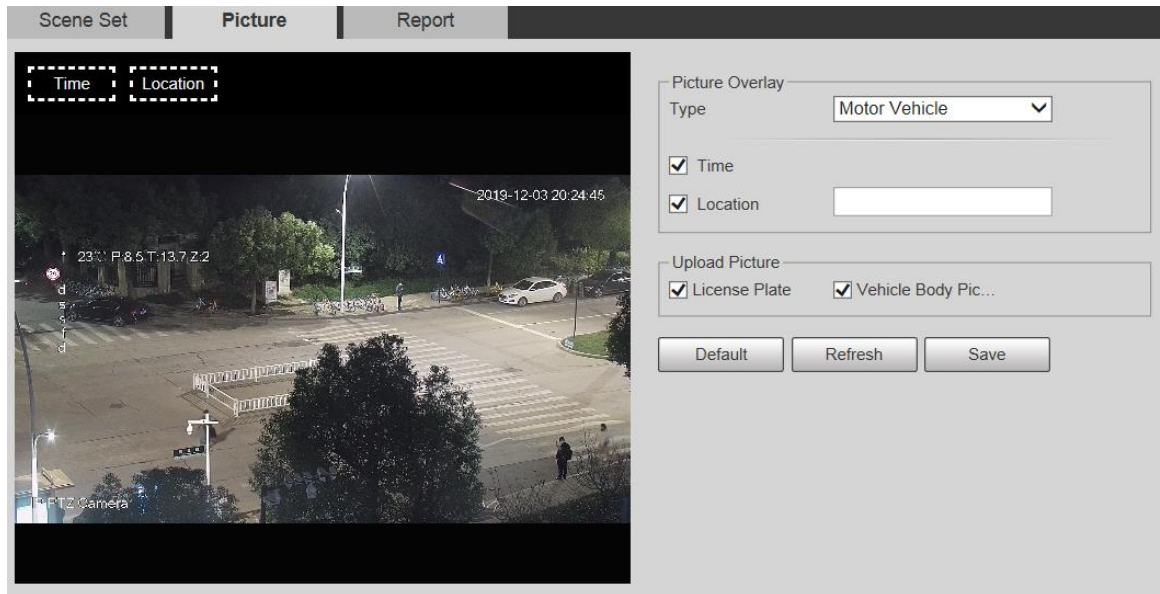


Figure 5-115 Picture overlay–non-motor vehicle

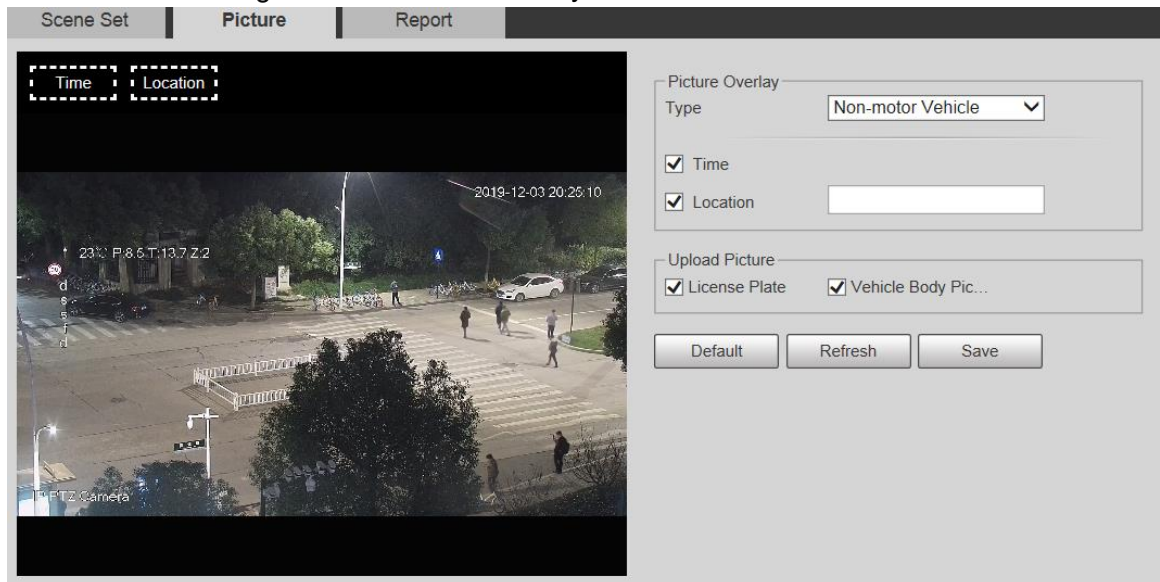


Figure 5-116 Picture overlay–people

Step 3 Select overlay information as needed.



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

Step 4 Click **Save**.

5.4.9.3 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**.

The **Report** interface is displayed.

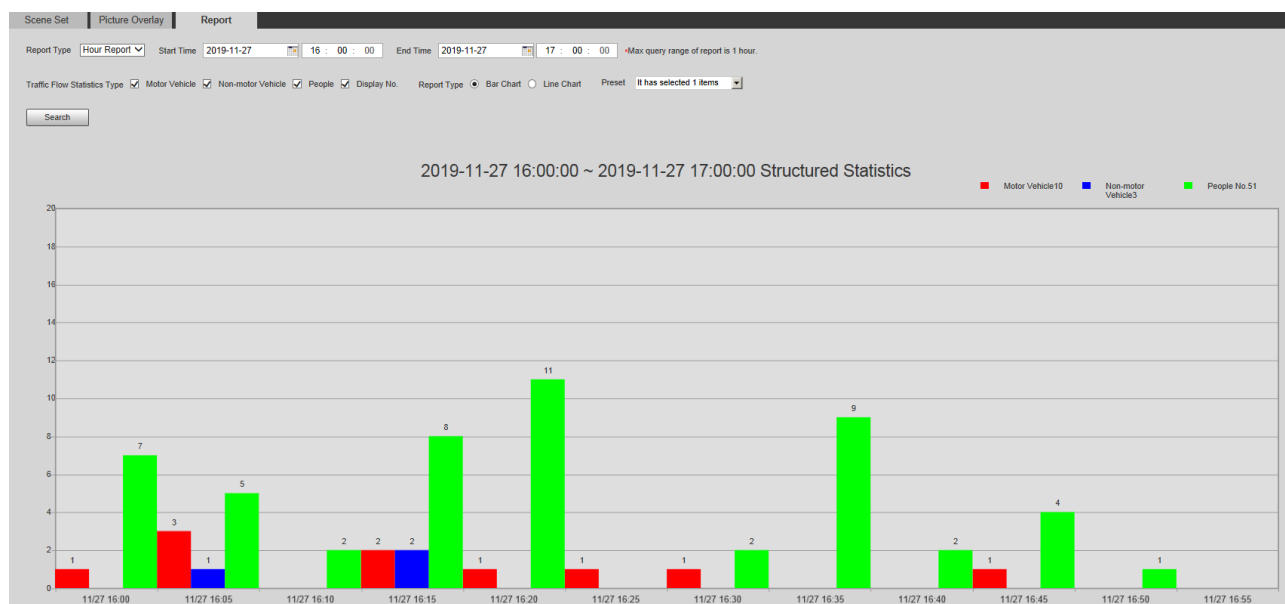
Step 2 Select the **Report Type**.

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

Step 4 Select the Traffic Flow Statistics Type.

Step 5 Click **Search** to generate reports. See Figure 5-117.

Figure 5-117 Video metadata report



5.4.10 Alarm

- Step 1** Select **Setting > Event > Alarm**.
The **Alarm** interface is displayed. See Figure 5-118.
Figure 5-118 Alarm

Alarm

☐ Enable

Relay-in

Alarm1

Period

Setting

Anti-Dither

0

s (0~100)Sensor Type

NO

☒ Record

Record Delay

10

s (10~300)

☒ Relay-out

12

Alarm Delay

10

s (10~300)

☐ Send Email

☐ PTZ

☒ Snapshot

Default

Refresh

Save

- Step 2** Configure parameters as needed. For parameter description, see Table 5-38.

Table 5-38 Alarm setting parameter description

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 "5.4.1.1 Motion Detection."

- Step 3** Click **Save**.

5.4.11 Abnormality

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

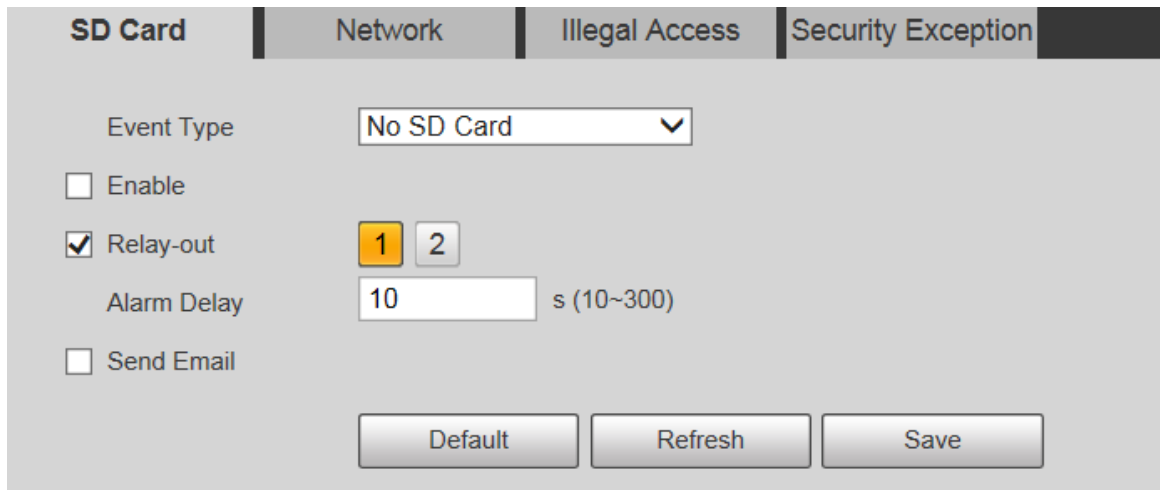
5.4.11.1 SD Card

In case of an SD card exception, an alarm will be triggered. Follow these steps to complete the configuration.

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

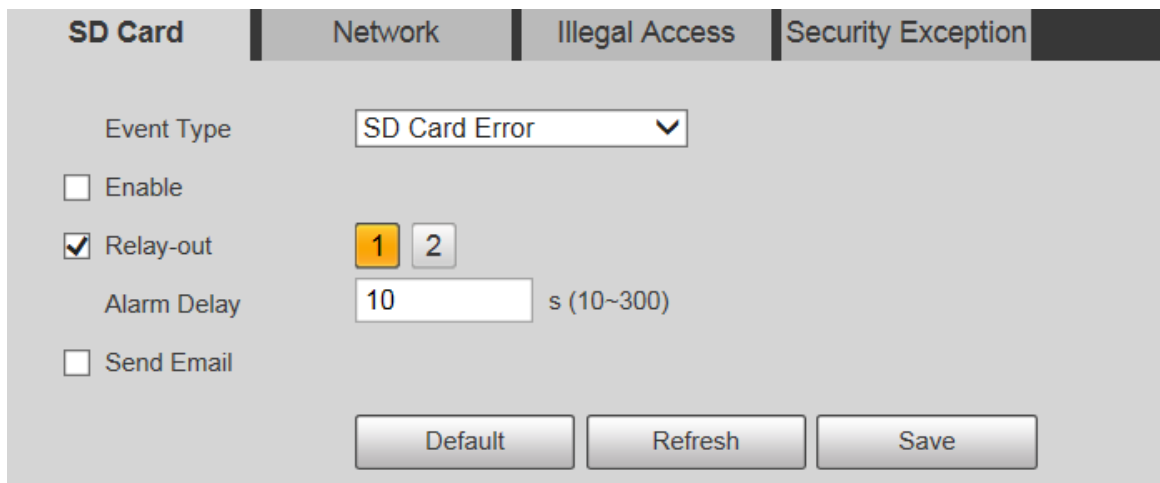
The **SD Card** interface is displayed. See Figure 5-119, Figure 5-120, and Figure 5-121.

Figure 5-119 No SD card



The screenshot shows the 'SD Card' configuration page. At the top, there are four tabs: 'SD Card', 'Network', 'Illegal Access', and 'Security Exception'. The 'SD Card' tab is selected. Below the tabs, the 'Event Type' dropdown menu is set to 'No SD Card'. There are three checkboxes: 'Enable' (unchecked), 'Relay-out' (checked), and 'Send Email' (unchecked). The 'Relay-out' checkbox is accompanied by two small buttons labeled '1' and '2'. Below these, the 'Alarm Delay' is set to '10' seconds, with a range of '(10~300)' indicated. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Figure 5-120 SD card error



The screenshot shows the 'SD Card' configuration page. At the top, there are four tabs: 'SD Card', 'Network', 'Illegal Access', and 'Security Exception'. The 'SD Card' tab is selected. Below the tabs, the 'Event Type' dropdown menu is set to 'SD Card Error'. There are three checkboxes: 'Enable' (unchecked), 'Relay-out' (checked), and 'Send Email' (unchecked). The 'Relay-out' checkbox is accompanied by two small buttons labeled '1' and '2'. Below these, the 'Alarm Delay' is set to '10' seconds, with a range of '(10~300)' indicated. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Figure 5-121 Capacity warning

The screenshot shows the 'SD Card' configuration tab. The 'Event Type' is set to 'Capacity Warning'. The 'Enable' checkbox is unchecked. The 'Capacity Limit' is set to '10' with a unit of '%(0~99)'. The 'Relay-out' checkbox is checked, and it has two sub-indicators, '1' and '2', where '1' is highlighted in orange. The 'Alarm Delay' is set to '10' with a unit of 's (10~300)'. The 'Send Email' checkbox is unchecked. At the bottom, there are three buttons: 'Default', 'Refresh', and 'Save'.

Step 2 Configure parameters as needed. For parameter description, see Table 5-39.

Table 5-39 SD card exception parameter description

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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.2 Network Exception

In case of a network exception, an alarm will be triggered. Follow these steps to complete the configuration.

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

The **Network** interface is displayed. See Figure 5-122 and Figure 5-123.

Figure 5-122 Disconnection

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

Event Type: Disconnection

☒ Enable

☐ Record

Record Delay: 10 s (10~300)

☐ Relay-out: 1 2

Alarm Delay: 10 s (10~300)

Default Refresh Save

Figure 5-123 IP conflict

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

Event Type: IP Conflict

☒ Enable

☐ Record

Record Delay: 10 s (10~300)

☐ Relay-out: 1 2

Alarm Delay: 10 s (10~300)

Default Refresh Save

Step 2 Configure parameters as needed. See Table 5-40.

Table 5-40 Network exception parameter description

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



For other parameters, see "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.3 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**.

The **Illegal Access** interface is displayed. See Figure 5-124.

Figure 5-124 Illegal access

Step 2 Configure parameters as needed. For parameter description, see Table 5-41.

Table 5-41 Illegal access parameter description

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 "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.4.11.4 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**.

The **Security Exception** interface is displayed. See Figure 5-125.

Figure 5-125 Security exception

Step 2 Configure each parameter as needed. For details, refer to "5.4.1.1 Motion Detection."

Step 3 Click **Save**.

5.5 Storage

5.5.1 Schedule

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



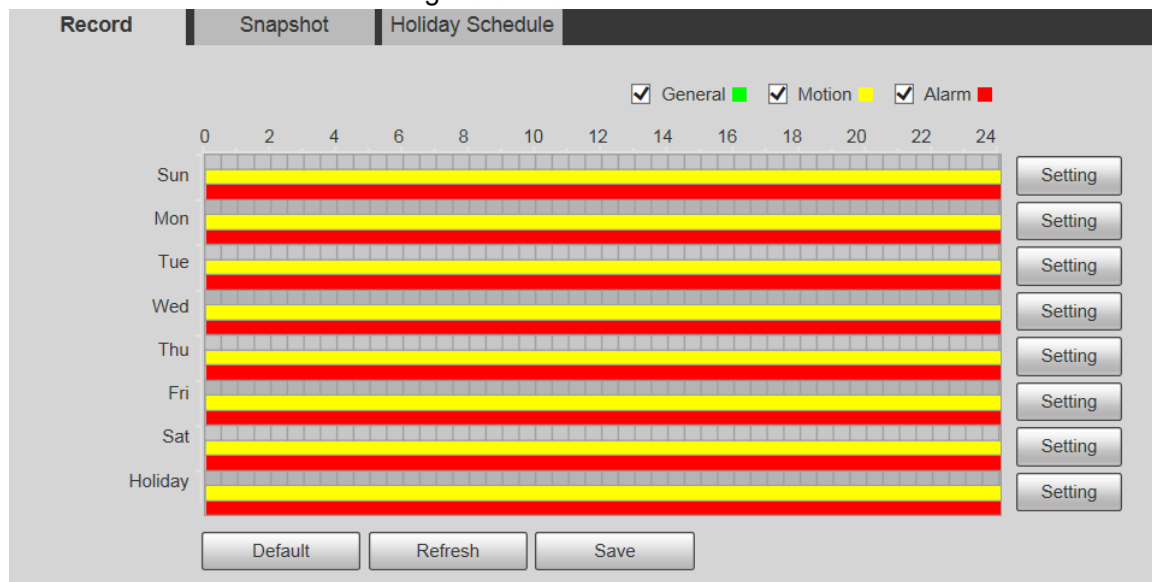
If the **Record Mode** is **Off**, the Device will not record or take snapshots according to the schedule.

5.5.1.1 Record

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

The **Record** interface is displayed. See Figure 5-126.

Figure 5-126 Record



Step 2 Select the day for recording from Monday to Sunday. Click **Setting** on the right, and the **Setting** interface is displayed. See Figure 5-127.

- Set the recording period as needed. 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** interface.

Figure 5-127 Record schedule setting

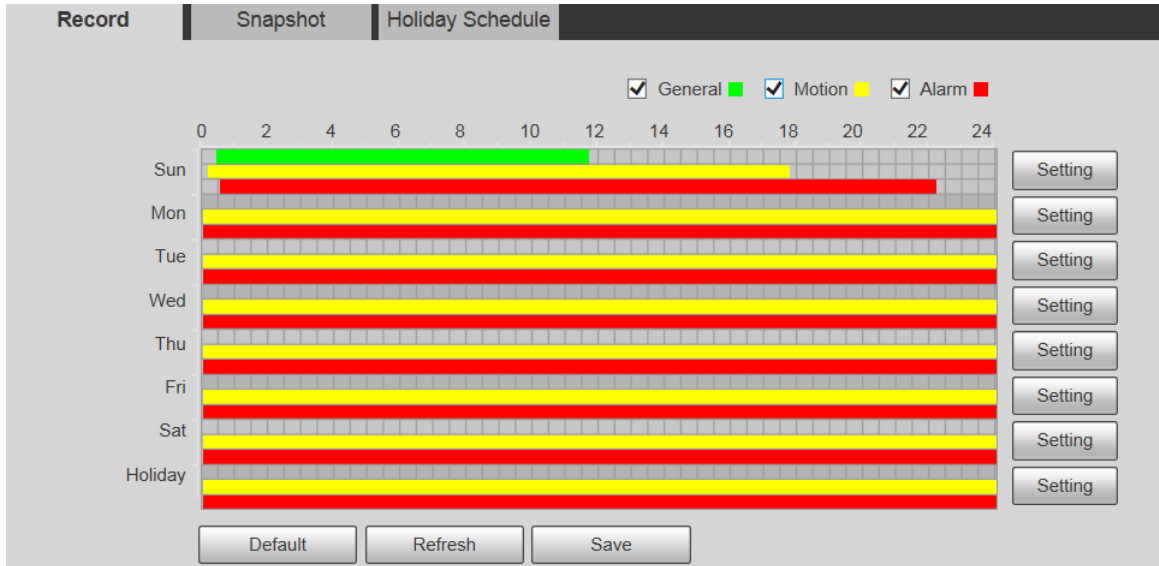
The 'Setting' window displays a configuration interface for recording schedules. At the top, there are checkboxes for days of the week: All, Sun (checked), Mon, Tue, Wed, Thu, Fri, Sat, and Holiday. Below this, there are six rows labeled Period1 through Period6. Each row contains two time selection fields (HH : MM : SS) separated by a hyphen, and three checkboxes: General, Motion, and Alarm. For Period1, the time range is 00 : 00 : 00 - 23 : 59 : 59, and the Motion and Alarm checkboxes are checked. The other periods have the same time range but with all checkboxes unchecked. At the bottom of the window are 'Save' and 'Cancel' buttons.

Step 3 Click **Save** to return to the **Record** interface. See Figure 5-128.

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

- ☒ Green: Represents general recording.
- ☒ Yellow: Represents motion detection recording.
- ☒ Red: Represents the alarm recording.

Figure 5-128 Recording schedule setting completed



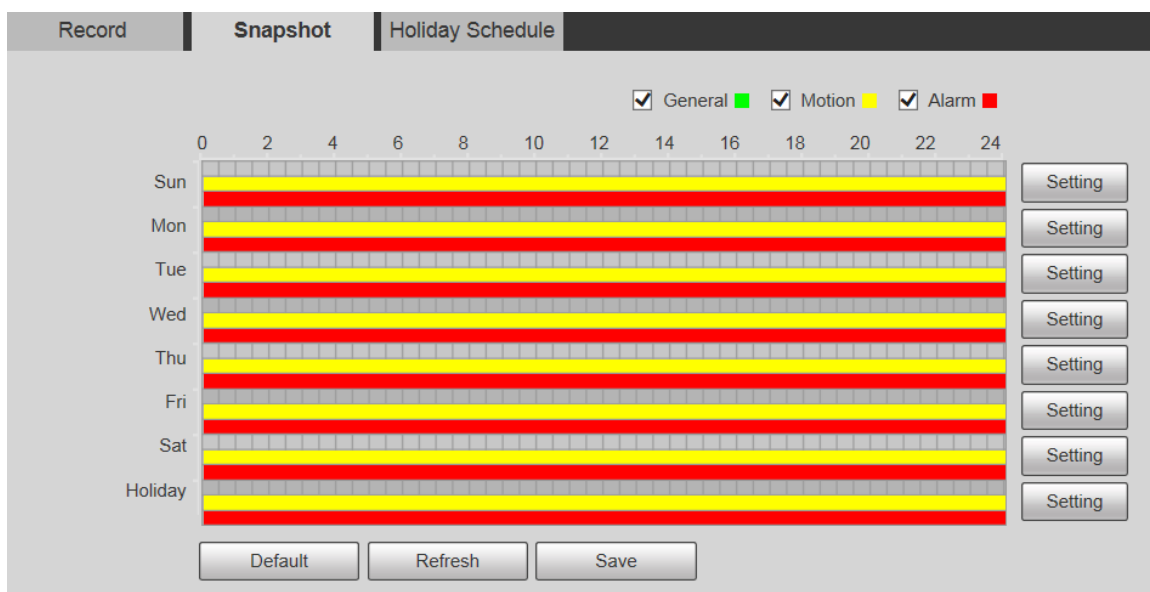
Step 4 On the **Record** interface, click **Save**, and the **Save Succeeded!** prompt will be displayed, which means the recording schedule has been set.

5.5.1.2 Snapshot

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

The **Snapshot** interface is displayed. See Figure 5-129.

Figure 5-129 Snapshot



Step 2 For the snapshot schedule settings, refer to Step 2 and Step 3 in "5.5.1.1 Record."

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

5.5.1.3 Holiday Schedule

You can set specific dates as holidays.

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

The **Holiday Schedule** interface is displayed. See Figure 5-130.

Figure 5-130 Holiday schedule

The interface shows the 'Holiday Schedule' tab selected. Below the tabs, there are checkboxes for 'Record' and 'Snapshot'. The calendar widget displays the month of December. The date '1' is selected and highlighted in yellow. The calendar grid is as follows:

Sun	Mon	Tue	Wen	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

At the bottom of the calendar widget are two buttons: 'Refresh' and 'Save'.

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** interface, click **Setting** to the right of **Holiday**. The setting method is the same as that of Monday to Sunday.

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

5.5.2 Snapshot by Location

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

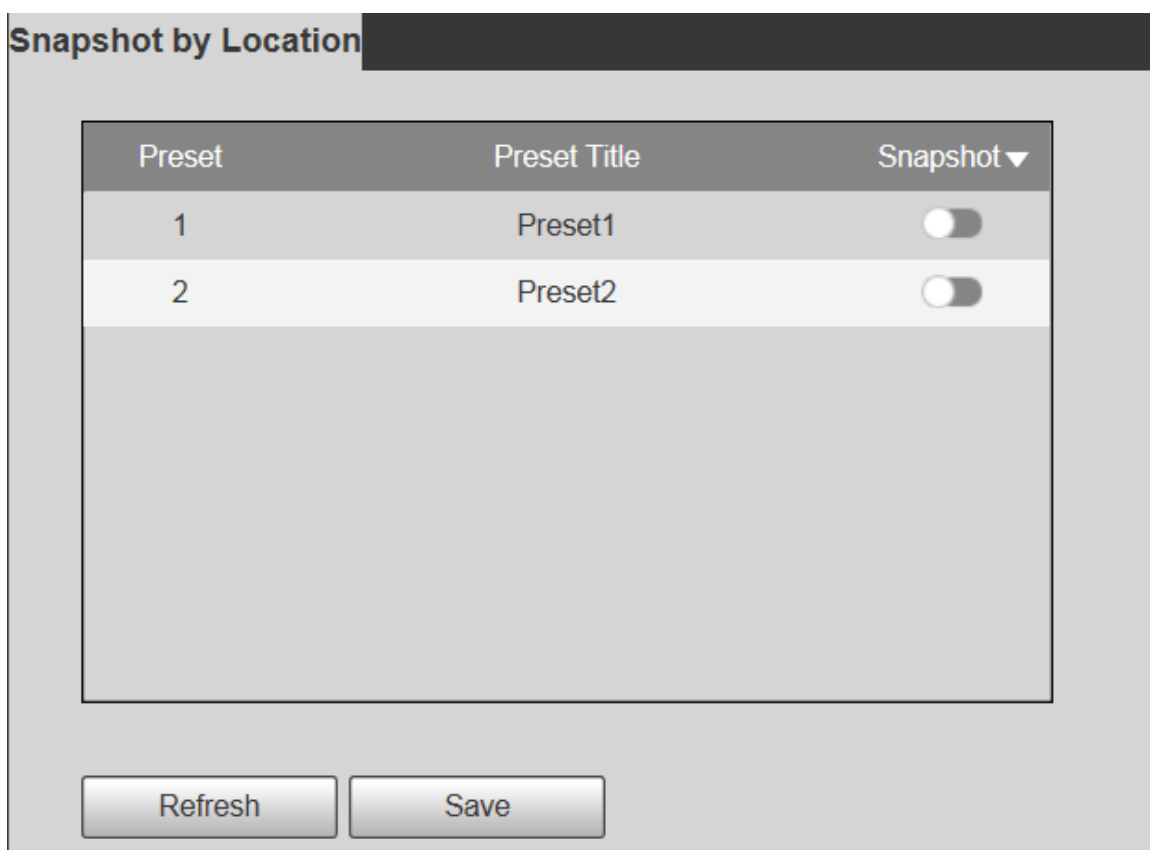


You need to set presets in advance.

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

The **Snapshot by Location** interface is displayed. See Figure 5-131.

Figure 5-131 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**.

5.5.3 Destination

5.5.3.1 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**.

The **Path** interface is displayed, see Figure 5-132.

Figure 5-132 Path settings

Step 2 Select the corresponding event type and storage method as needed. For details, refer to Table 5-42.

Table 5-42 Path parameter description

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**.

5.5.3.2 Local

Display the SD card information. You can set it as read only or read & write; you can also hot swap or refresh it.

Select **Setting > Storage > Destination > Local**, and the **Local** interface is displayed. See Figure 5-133.

Figure 5-133 Local storage

- Click **Read Only**, and the SD card is set to read only.
- Click **Read & Write**, and the SD card is set to read & write.
- Click **Hot Swap** to remove the SD card.
- Click **Refresh** to start formatting the SD card.



After the SD card is formatted, the data will be cleared. Think twice before performing the operation.

5.5.3.3 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**.

The **FTP** interface is displayed. See Figure 5-134.

Figure 5-134 FTP settings

The screenshot shows the FTP settings interface. At the top, there are four tabs: 'Path', 'Local', 'FTP' (which is selected), and 'NAS'. Below the tabs, the following settings are visible: an 'Enable' checkbox which is currently unchecked; a 'Server Address' text field containing '0.0.0.0'; a 'Port' text field containing '22' with a range '(0~65535)' to its right; a 'Username' text field containing 'anonymity'; a 'Password' text field filled with dots; a 'Remote Directory' text field containing 'share'; and an 'Emergency (Local)' checkbox which is also unchecked. At the bottom of the form, there are three buttons: 'test', 'Default', and 'Save'.

Step 2 Select the **Enable** check box, and the FTP function is enabled.



- There might be risks if the FTP function is enabled. Think twice before enabling the function.
- **SFTP** is recommended to ensure network security.

Step 3 Configure parameters as needed. For parameter description, see Table 5-43.

Table 5-43 FTP parameter description

Parameter	Description
Server Address	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Remote Directory	The destination path on the FTP server.
Emergency (Local)	If you enable the function, in case of FTP storage exception, the recordings and snapshots will be stored on the local SD card.

Step 4 Click **test** to verify the username and password, and test whether FTP is connected to the Device.

Step 5 Click **Save**.

5.5.3.4 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**.

The **NAS** interface is displayed. See Figure 5-135.

Figure 5-135 NAS settings

Step 2 Configure parameters as needed. For parameter description, see Table 5-44.

Table 5-44 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**.

5.5.4 Record Control

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

The **Record Control** interface is displayed. See Figure 5-136.

Figure 5-136 Record control

Step 2 Configure parameters as needed. For parameter description, see Table 5-45.

Table 5-45 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.
Disk Full	You can select Stop or Overwrite. • 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**.

5.6 System Management

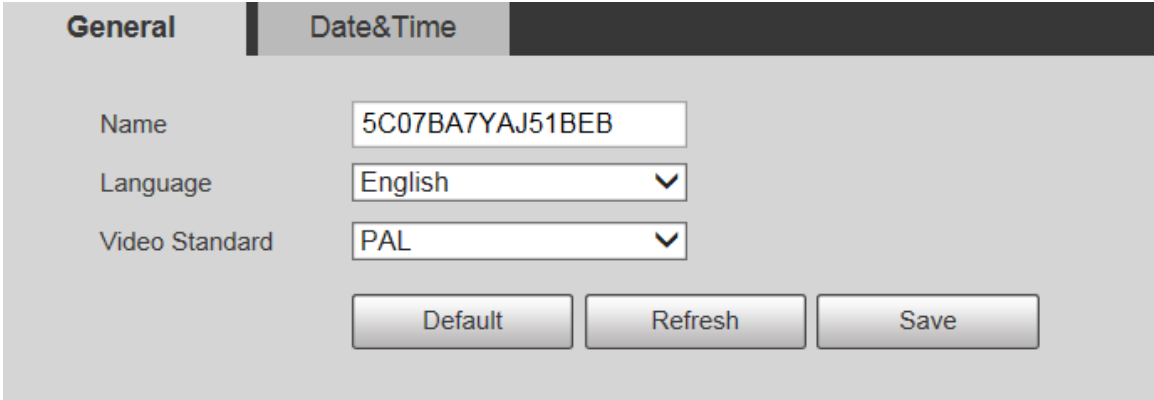
5.6.1 Device Settings

5.6.1.1 General

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

The **General** interface is displayed. See Figure 5-137.

Figure 5-137 General settings



Step 2 Configure parameters as needed. For parameter description, see Table 5-46.

Table 5-46 General setting parameter description

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 .

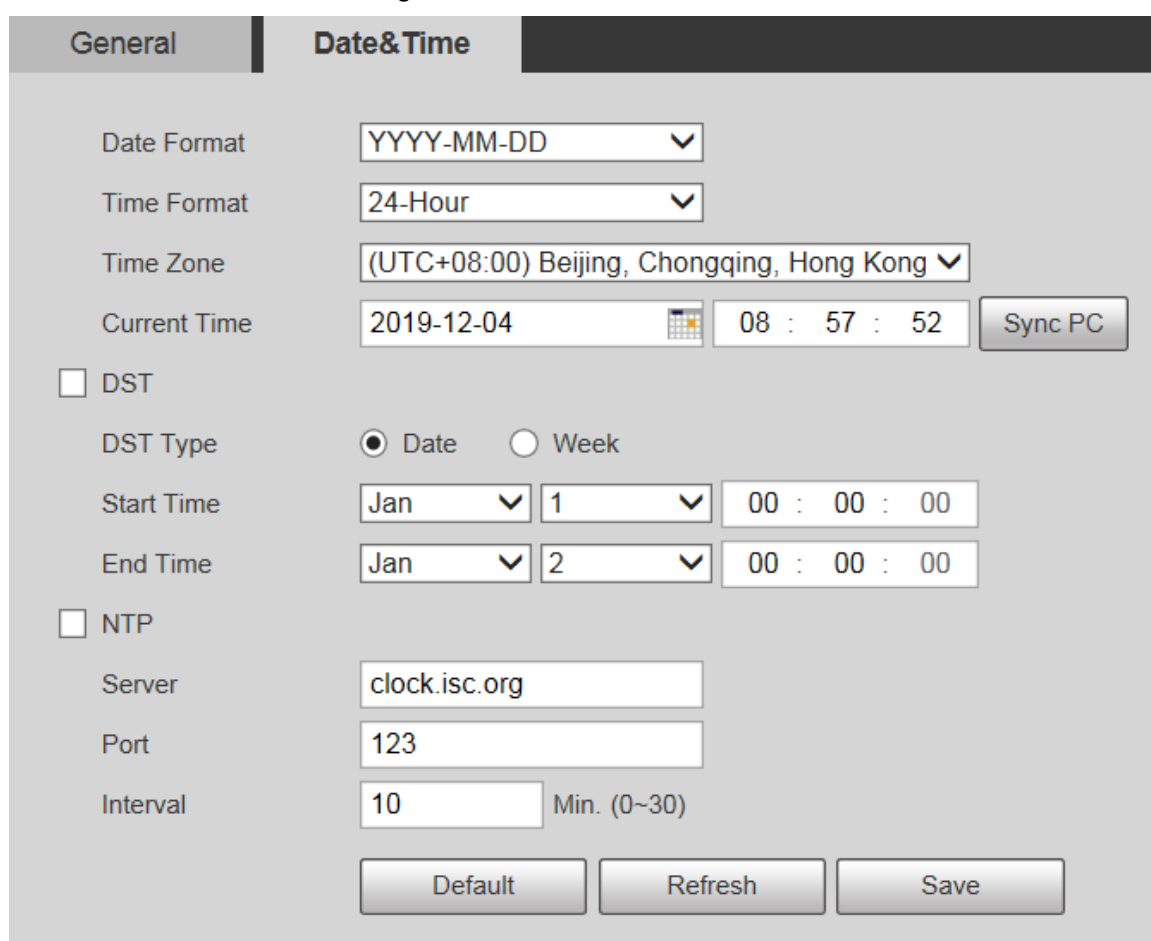
Step 3 Click **Save**.

5.6.1.2 Date & Time

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

The **Date&Time** interface is displayed. See Figure 5-138.

Figure 5-138 Date & time



The screenshot shows the 'Date&Time' configuration page. It includes dropdown menus for date and time formats, a time zone selector, a current time display with a calendar icon, and checkboxes for DST and NTP. For DST, there are radio buttons for 'Date' and 'Week', and fields for start and end times. For NTP, there are fields for server, port, and interval. At the bottom, there are 'Default', 'Refresh', and 'Save' buttons.

Step 2 Configure parameters as needed. See Table 5-47.

Table 5-47 Date & time parameter description

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

Parameter	Description
	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**.

5.6.2 Account Settings

5.6.2.1 Account

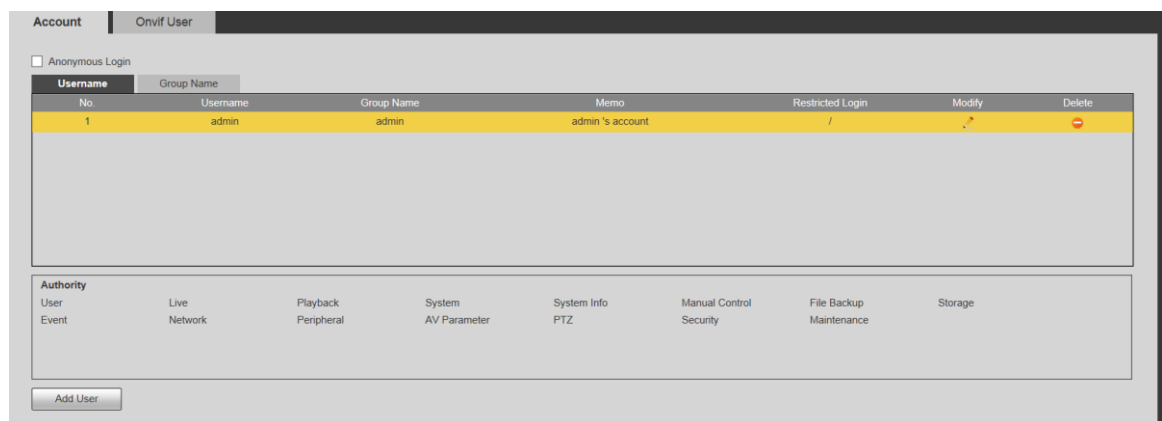
User management is only available for admin users.

- 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.

5.6.2.1.1 Username

Select **Setting > System > Account > Account > Username**, and you can enable anonymous login, add users, delete users, modify user passwords, and perform other operations. For the configuration interface, see Figure 5-139.

Figure 5-139 Account interface





No permission is available for version information and other buttons except **Relay-out**, **Mark**, and **Wiper Control** in **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**.

The **Add User** interface is displayed. See Figure 5-140.

Figure 5-140 Adding users

Add User

Username **Must**

Password

The minimum pass phrase length is 8 characters

Confirm Password

Group Name

Memo

Operation Permission **Restricted Login**

☒ All

☒ User

☒ Live

☒ Playback

☒ System

☒ System Info

☒ Manual Control

☒ File Backup

☒ Storage

☒ Event

☒ Network

☒ Peripheral

☒ AV Parameter

☒ PTZ

☒ Security

☒ Maintenance

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 5-141 is displayed. You can control login to the Device by setting the **IP Address**, **Validity Period** and **Time Range**.

Figure 5-141 Restricted login



- 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.

Step 4 Click **Save**.

Modifying Users

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

The **Modify User** interface is displayed. See Figure 5-142.

Figure 5-142 Modifying users

Modify User

Username: admin

☐ Modify Password

Group Name: admin

Memo: admin's account

Authority: ☒ All

- ☒ User
- ☒ Live
- ☒ Playback
- ☒ System

Save Cancel

Step 2 Modify user information as needed.

Step 3 Click **Save**.

Modifying Password

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

Step 2 Enter old password and new password, and 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.

5.6.2.1.2 Group Name

Select **Setting > System > Account > Account > Group Name**, and you can add groups, delete groups, modify group passwords, and perform other operations. For the interface, see Figure 5-143.

Figure 5-143 User group settings

Account Onvif User

☐ Anonymous Login

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

Authority: User, AV Parameter, Live: PTZ, Playback: Security, System: Maintenance, System Info, Manual Control, File Backup, Storage, Event, Network, Peripheral

Add Group

Adding Groups

For specific operations, refer to "5.6.2.1.1 Username."

Modifying Groups

For specific operations, refer to "5.6.2.1.1 Username."

Deleting Groups

For specific operations, refer to "5.6.2.1.1 Username."

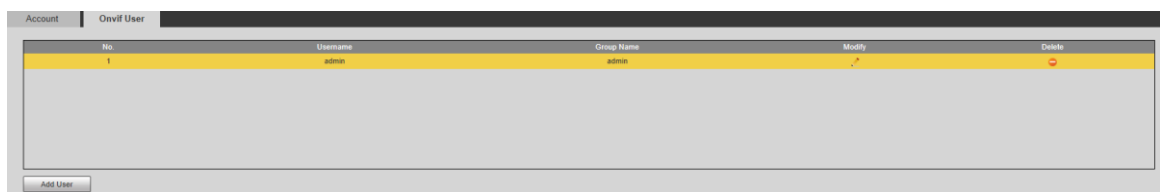
5.6.2.2 Onvif User

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

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

The **Onvif User** interface is displayed. See Figure 5-144.

Figure 5-144 Onvif user



Step 2 Click **Add User**.

The **Add User** interface is displayed. See Figure 5-145.

Figure 5-145 Adding users

The screenshot shows a 'Add User' dialog box. It has the following fields and controls: 'Username' with a text input field and a red 'Must' label; 'Password' with a text input field and a red label 'The minimum pass phrase length is 8 characters'; three radio buttons labeled 'Weak', 'Medium', and 'Strong'; 'Confirm Password' with a text input field; 'Group Name' with a dropdown menu showing 'admin'; and 'Save' and 'Cancel' buttons at the bottom.

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

Step 4 Click **Save**.



- Click  to modify user information.

- Click  to delete users.

5.6.3 Safety

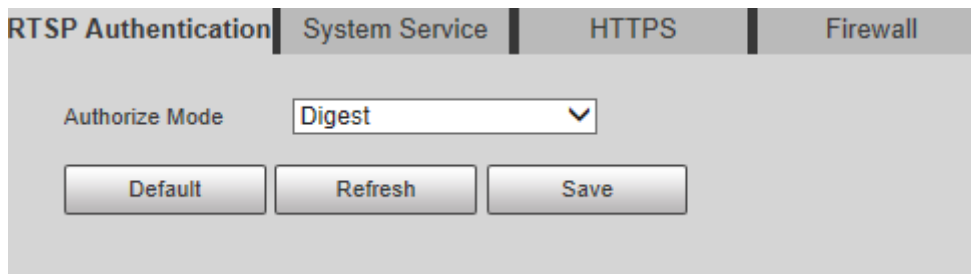
5.6.3.1 RTSP Authentication

Set the authentication method for media stream.

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

The **RTSP Authentication** interface is displayed. See Figure 5-146.

Figure 5-146 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.

5.6.3.2 System Service

You can configure system service to ensure system security.

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

The **System Service** interface is displayed. See Figure 5-147.

Figure 5-147 System service

RTSP Authentication | **System Service** | HTTPS | Firewall

SSH ☐ Enable

Multicast/Broadcast Search ☒ Enable

Password Reset ☒ Enable Email Address

CGI Service ☒ Enable

Onvif Service ☒ Enable

Genetec Service ☒ Enable

Audio and Video Transcoding ☐ Enable *Please make sure matched device or software supports video decryption function.

Mobile Push ☒ Enable

Private Protocol Authentication: Security Mode (Recommended) ▼

Default Refresh Save

Step 2 Configure system service parameters. For the detailed description, see Table 5-48.

Table 5-48 System service parameter description

Function	Description
SSH	You can enable SSH authentication to perform safety management. The function is disabled by default. It is recommended to disable SSH. If this function is enabled, there might be security risks.
Multicast/Broadcast Search	Enable this function, and when multiple users are viewing the monitoring screen simultaneously through network, they can find the Device through multicast/broadcast protocol. It is recommended to disable the multicast/broadcast search function. If this function is enabled, there might be security risks.
Password Reset	You can enable Password Reset to perform security management. The function is enabled by default. 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.
CGI Service	You can access the Device through this protocol. The function is enabled by default. It is recommended to disable the function. If this function is enabled, there might be security risks.
Onvif Service	You can access the Device through this protocol. The function is enabled by default.

Function	Description
	It is recommended to disable the function. If this function is enabled, there might be security risks.
Audio and Video Transmission Encryption	Enable this function to encrypt the stream transmitted through the private protocol.  - 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	Push the alarm snapshot triggered by the Device to the mobile phone. The function is enabled by default.  It is recommended to disable the function. If this function is enabled, there might be security risks.
Private Protocol Authentication Mode	You can select Security Mode and Compatible Mode . Security mode is recommended. If you select compatibility mode, there might be security risks.

Step 3 Click **Save**.

5.6.3.3 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.
 - Select **Setting > System > Safety > HTTPS**.
The **HTTPS** interface is displayed. See Figure 5-148.

Figure 5-148 HTTPS (1)

RTSP Authentication | System Service | **HTTPS** | Firewall

☐ Enable HTTPS

Protocol Version

☒ Enable TLSv1.0

Create Certificate

Create

Request Created

Request Created	Delete	Install	Download

Install Signed Certificate

Certificate Path Browse...

Certificate Key Path Browse... Upload

Certificate Installed

Certificate Installed Delete

Attribute

Refresh Save

- 2) Click **Create**.

The **HTTPS** dialog box is displayed. See Figure 5-149.

Figure 5-149 HTTPS (2)

HTTPS [X]

Country *e.g. CN

IP or Domain name *

Validity Period Day*Range :1-5000

Province

Location

Organization

Organization Unit

Email

Create Cancel

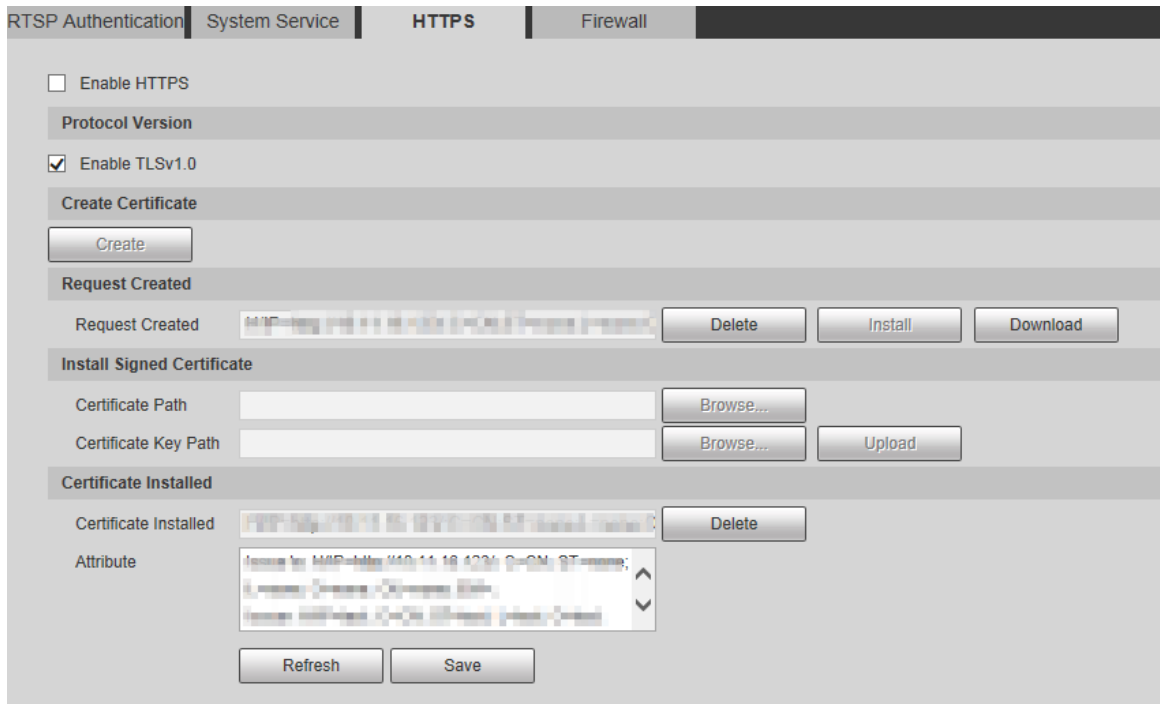
- 3) Enter the required information, and then click **Create**.



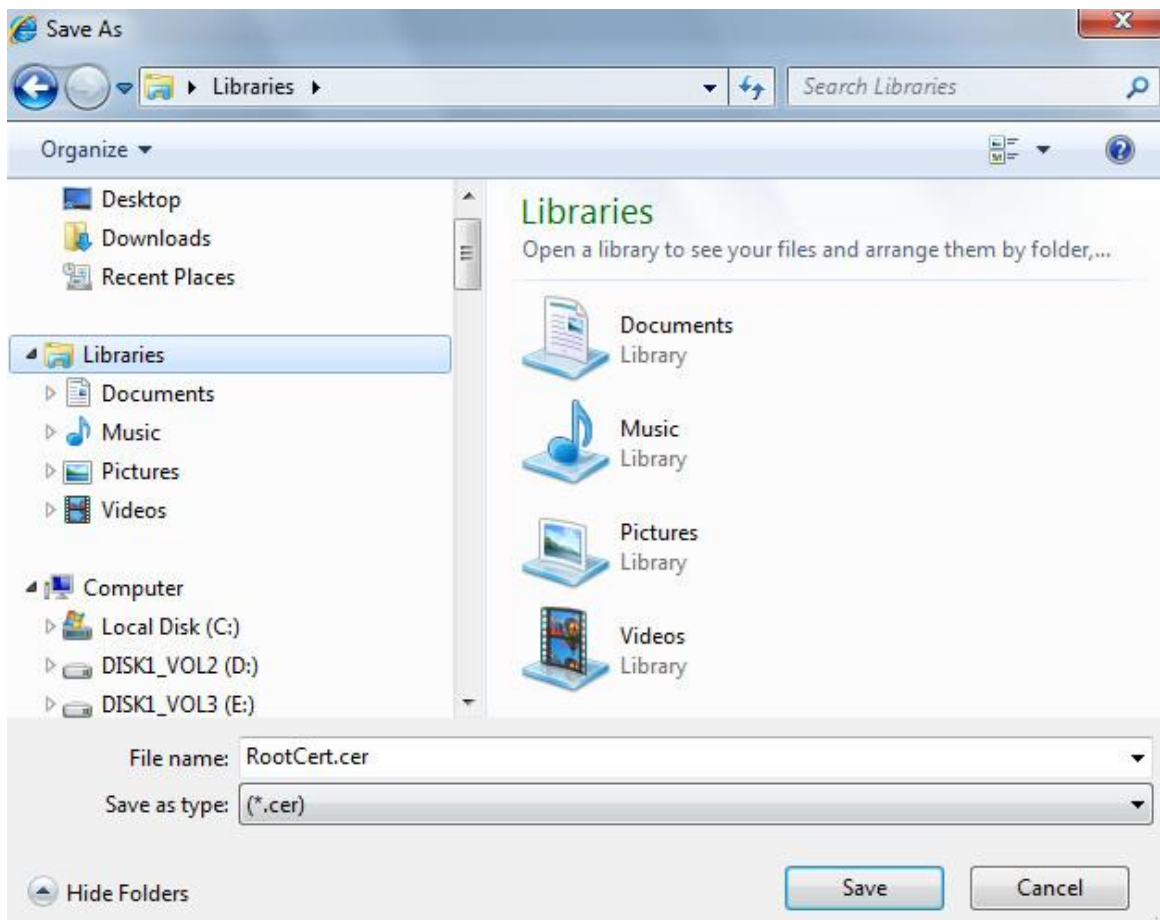
The entered IP or domain name must be the same as the IP or domain name of the Device.

- 4) Click **Install** to install the certificate on the Device. See Figure 5-150.

Figure 5-150 Certificate installation

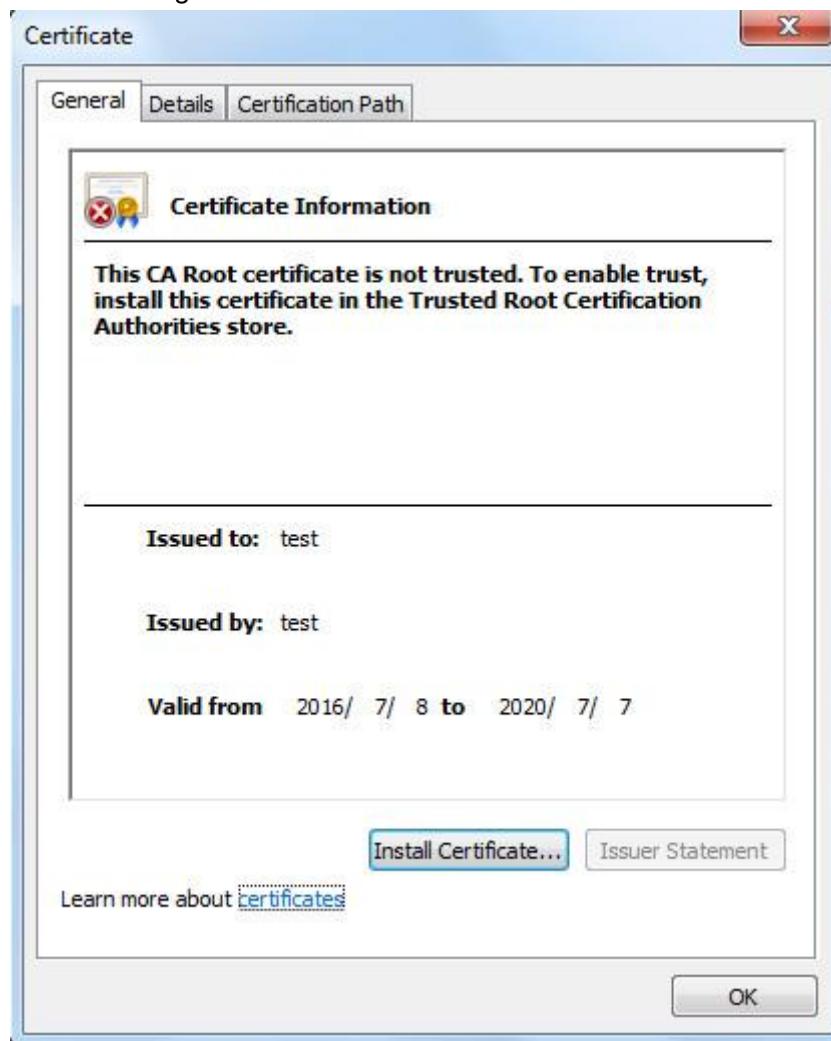


- 5) Click **Download** to download root certificate.
The **Save As** dialog box is displayed. See Figure 5-151.
- Figure 5-151 Downloading root certificate



- 6) Select storage path, and then click **Save**.
- 7) Double-click the **RootCert.cer** icon.
The **Certificate** interface is displayed. See Figure 5-152.

Figure 5-152 Certificate information



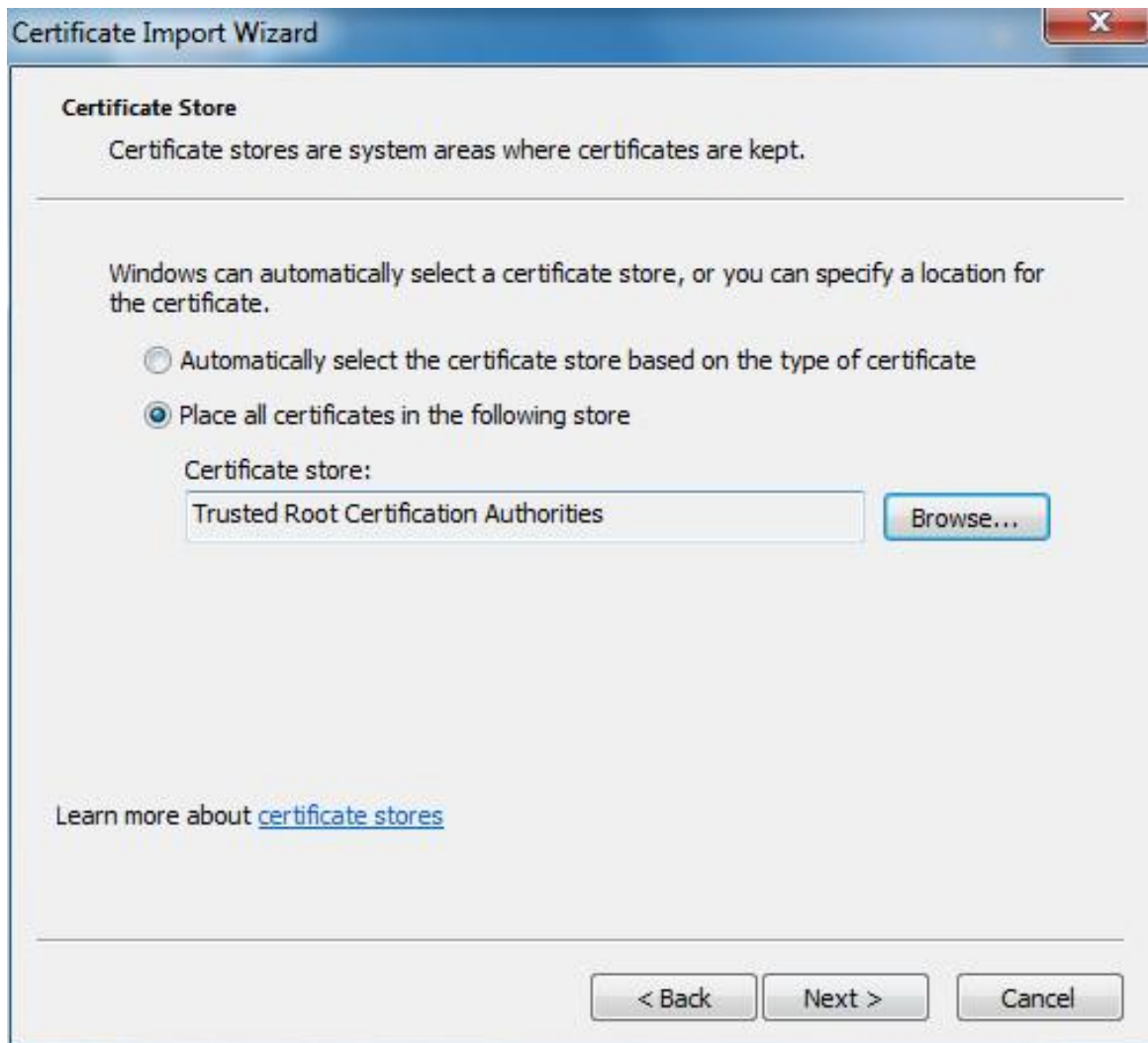
- 8) Click **Install Certificate**.
The **Certificate Import Wizard** interface is displayed. See Figure 5-153.

Figure 5-153 Certificate import wizard



- 9) Click **Next**.
Select **Trusted Root Certification Authorities**. See Figure 5-154.

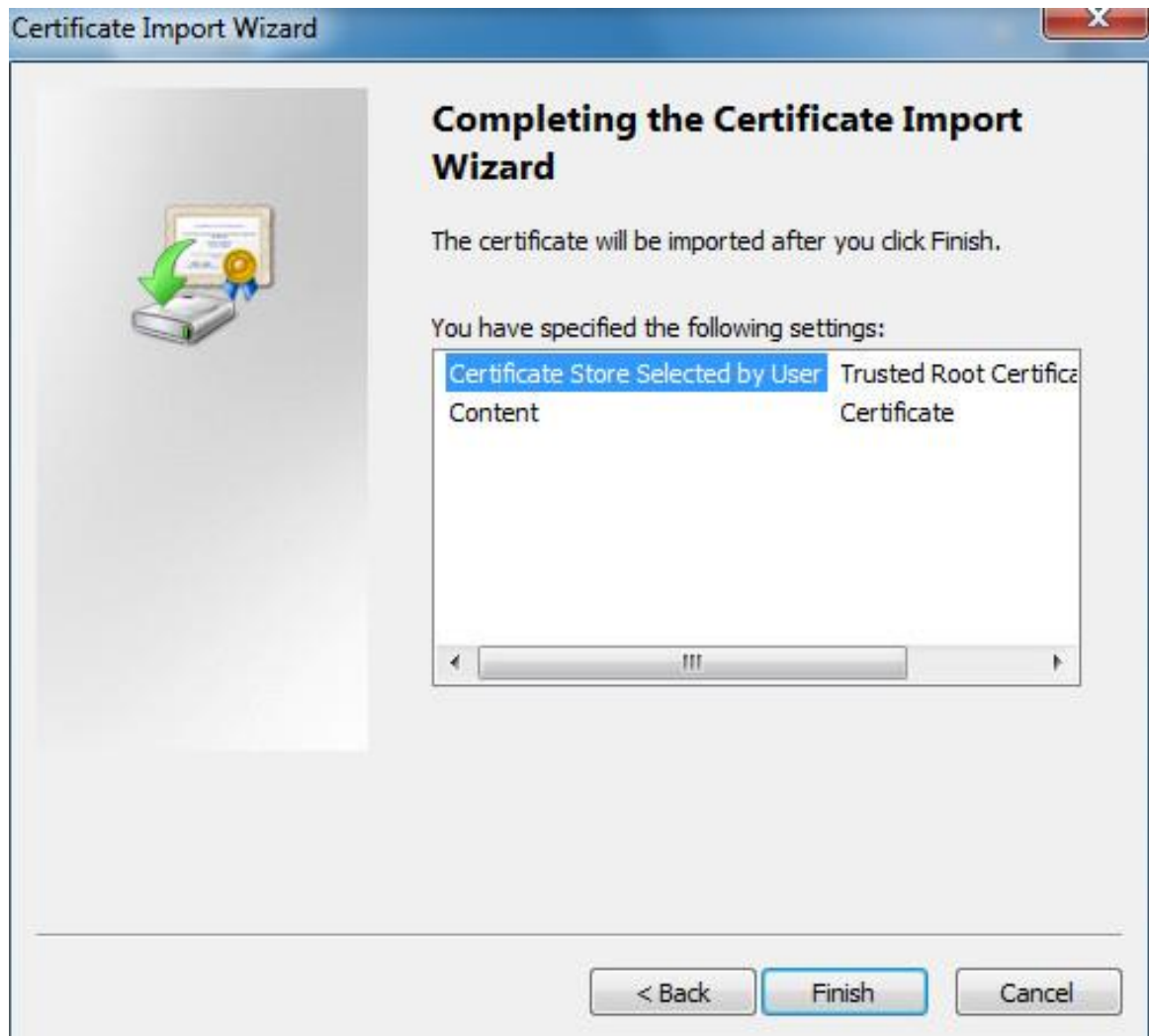
Figure 5-154 Certificate storage area



10) Click **Next**.

The **Completing the Certificate Import Wizard** interface is displayed, see Figure 5-155.

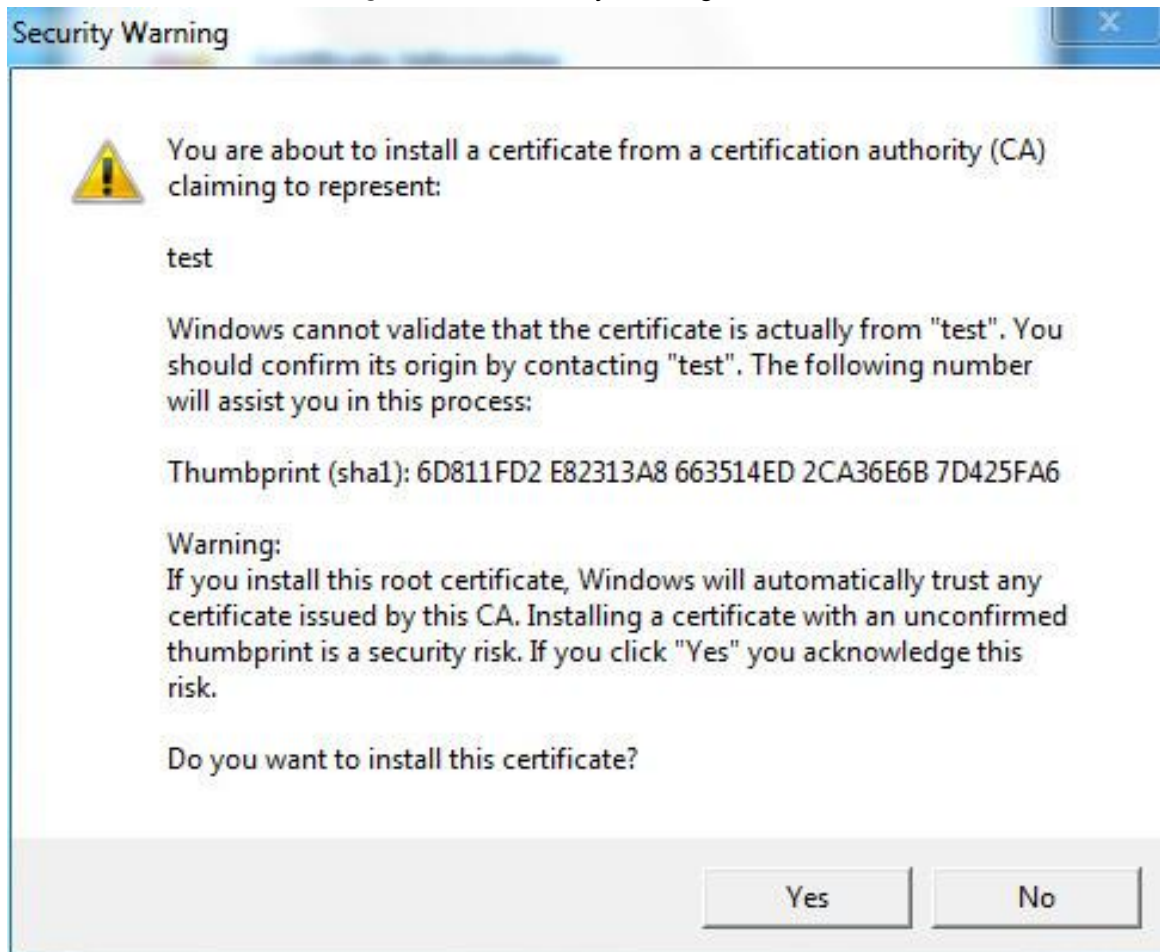
Figure 5-155 Completing the certificate import wizard



11) Click **Finish**.

The **Security Warning** dialog box is displayed. See Figure 5-156.

Figure 5-156 Security warning



12) Click **Yes**.

The **import was successful** dialog box is displayed. Click **OK** to complete the certificate installation. See Figure 5-157.

Figure 5-157 Import success



- If you select **Install Signed Certificate**, refer to the following steps.

1) Select **Setting > System > Safety > HTTPS**.

The **HTTPS** interface is displayed. See Figure 5-158.

Figure 5-158 Install signed certificate

The screenshot shows the 'HTTPS' tab in a configuration menu. It includes sections for 'Enable HTTPS', 'Protocol Version', 'Create Certificate', 'Request Created', 'Install Signed Certificate', and 'Certificate Installed'. The 'Install Signed Certificate' section has fields for 'Certificate Path' and 'Certificate Key Path', each with a 'Browse...' button, and an 'Upload' button. At the bottom are 'Refresh' and 'Save' buttons.

2) Click **Browse** to upload the signed certificate and certificate key, and then click **Upload**.

3) To install the root certificate, refer to Step 5) to 12) in **Create Certificate**.

Step 2 Select **Enable HTTPS** and click **Save**.

The **Reboot** interface is displayed, and the configuration takes effect after reboot. See Figure 5-159.

Figure 5-159 Reboot

The screenshot shows a 'Reboot' dialog box with a red warning icon. The text inside says: 'The configuration takes effect, the device is restarting now, please don't leave this page or close the browser...'.

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.

5.6.3.4 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**.

The **Firewall** interface is displayed. See Figure 5-160.

Figure 5-160 Firewall

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

Step 3 Select **Enable**, and then the **Firewall** is enabled.

Step 4 Click **Save**.

5.6.4 Peripheral



The peripheral functions might vary with different models, and the actual interface shall prevail.

5.6.4.1 Wiper

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

The **Wiper** interface is displayed. See Figure 5-161.

Figure 5-161 Wiper settings

Step 2 Configure parameters as needed. For parameter description, see Table 5-49.

Table 5-49 Wiper setting parameter description

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**.

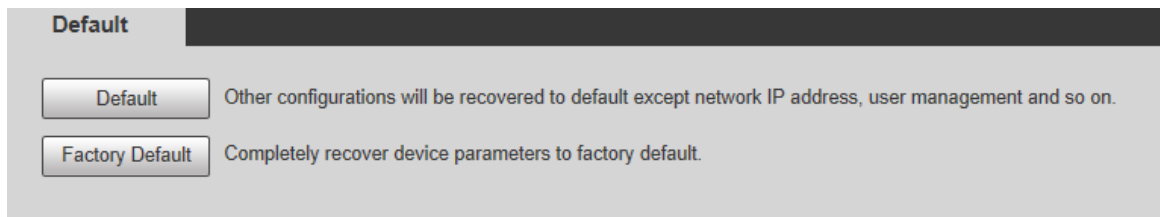
5.6.5 Default



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. The configuration interface is displayed. See Figure 5-162.

Figure 5-162 Default interface



Select the recovery mode as needed.

- **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 interface 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.

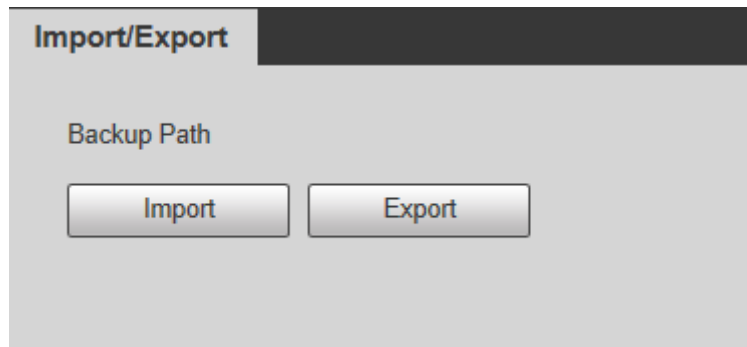
5.6.6 Import/Export

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

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

The **Import/Export** interface is displayed. See Figure 5-163.

Figure 5-163 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** interface of the Device to be configured to import the configuration file, and the Device will complete the configurations.

5.6.7 Auto Maintain

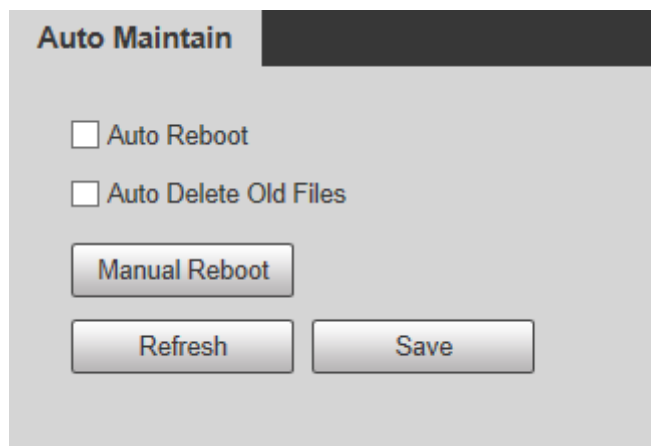
You can select **Auto Reboot** or **Auto Delete Old Files**.

- 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**.

The **Auto Maintain** interface is displayed. See Figure 5-164.

Figure 5-164 Auto maintain



Step 2 Configure parameters as needed. For parameter description, see Table 5-50.

Table 5-50 Auto maintain parameter description

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** and the configuration will take effect.

5.6.8 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**. The configuration interface is displayed. See Figure 5-165.

Figure 5-165 System upgrade

The screenshot shows the 'Upgrade' configuration window. The 'File Upgrade' section has a text input for 'Select Firmware File' with 'Browse...' and 'Upgrade' buttons. The 'Online Upgrade' section has an 'Auto-check for updates' checkbox, a 'Save' button, and a 'Manual Check' button. Below these are labels for 'System Version' and 'PTZ Version' with their respective values.

- 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.

5.7 Information

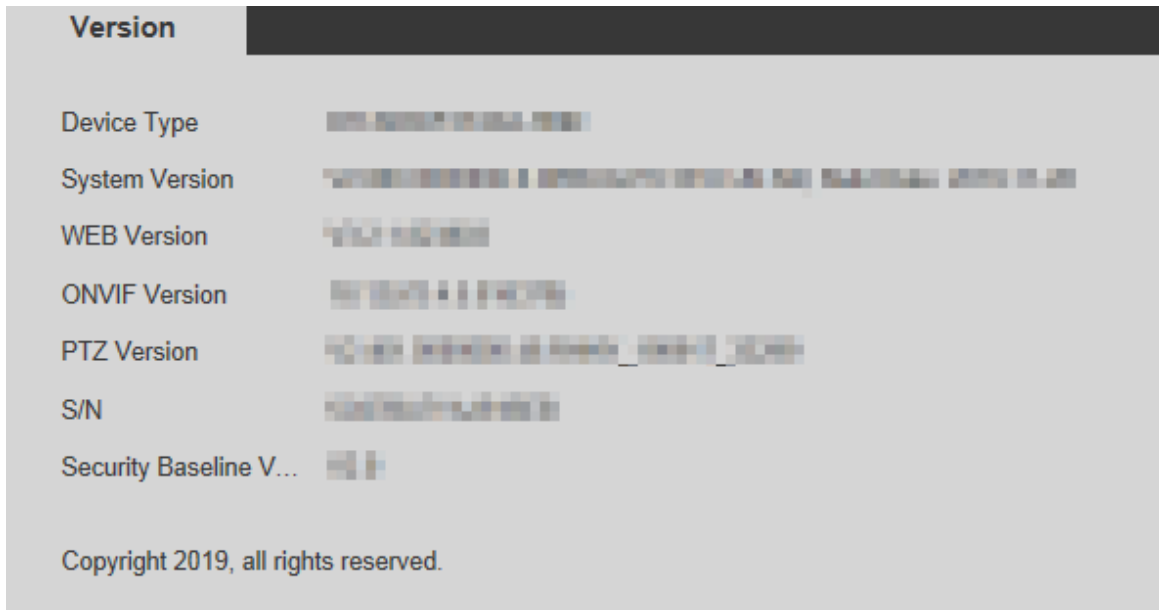
You can view information such as version, online users, log, and life statistics.

5.7.1 Version

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

Select **Setting > Information > Version > Version**, and then you can see the version information of current web interface. See Figure 5-166.

Figure 5-166 Version



5.7.2 Log Information

5.7.2.1 Log

Select **Setting > Information > Log > Log**, and then you can see the operation information of the Device, and some system information. See Figure 5-167. For parameter description, see Table 5-51.

Figure 5-167 Log

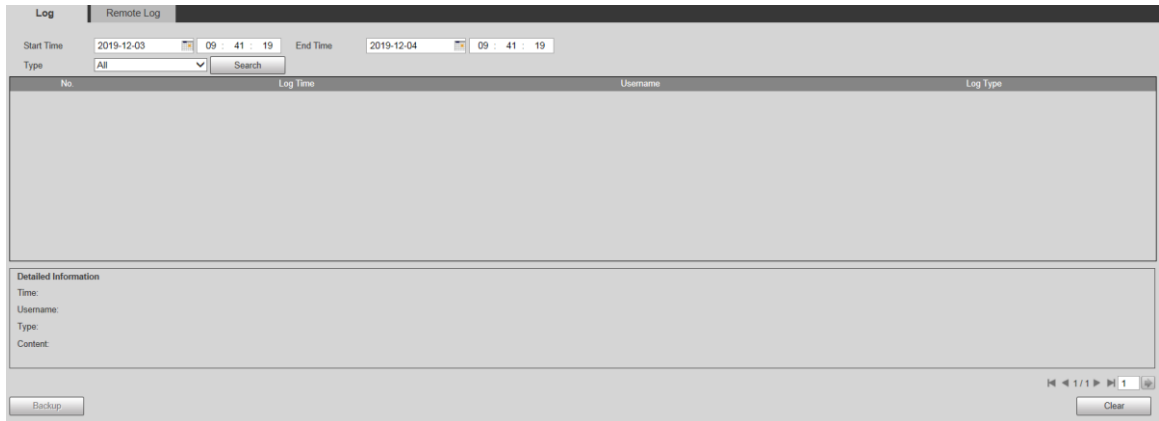


Table 5-51 Log parameter description

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.

5.7.2.2 Remote Log

Upload the Device operations to the log server.

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

The **Remote Log** interface is displayed. See Figure 5-168.

Figure 5-168 Remote log

Log | **Remote Log**

☐ Enable

IP Address: 192 . 168 . 0 . 108

Port: 514 (1~65534)

Device Number: 22 (0~23)

Default Refresh Save

Step 2 Select **Enable**, and then remote log function is enabled.

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



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

5.7.3 Online User

Select **Setting > Information > Online User**, and the **Online User** interface is displayed. See Figure 5-169.

Figure 5-169 Online users

No.	Username	User Local Group	IP Address	User Login Time
1	admin	admin	192.168.1.108	2019-10-14 10:51:56

Refresh

5.7.4 Life Statistics

Select **Setting > Information > Life Statistics > Life Statistics**, and then you can view the **Total Working Time**, **Upgrade Times**, and **Last Upgrade Date** of the Device. See Figure 5-170.

Figure 5-170 Life statistics

Life Statistics	
Total Working Time	70 day(s) 14 hour(s) 30 minute(s)
Upgrade Times	21 time(s)
Last Upgrade Date	2019-10-14 10:51:56

6 Alarm

You can select alarm types on the interface. When the selected alarms are triggered, detailed alarm information will be displayed on the right side of the interface. You can also select **Prompt** or **Play Alarm Tone**. When an alarm occurs, the alarm prompt or tone will be triggered. For the **Alarm** setting interface, see Figure 6-1. For parameter description, see Table 6-1.

Figure 6-1 Alarm setting interface

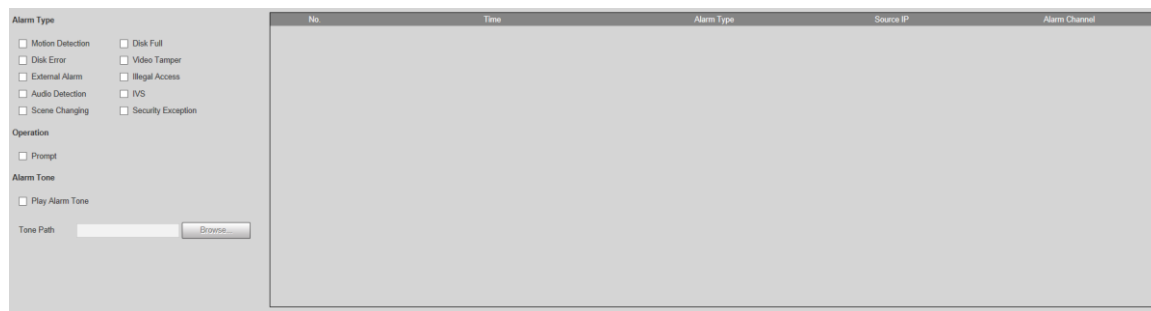


Table 6-1 Alarm setting parameter description

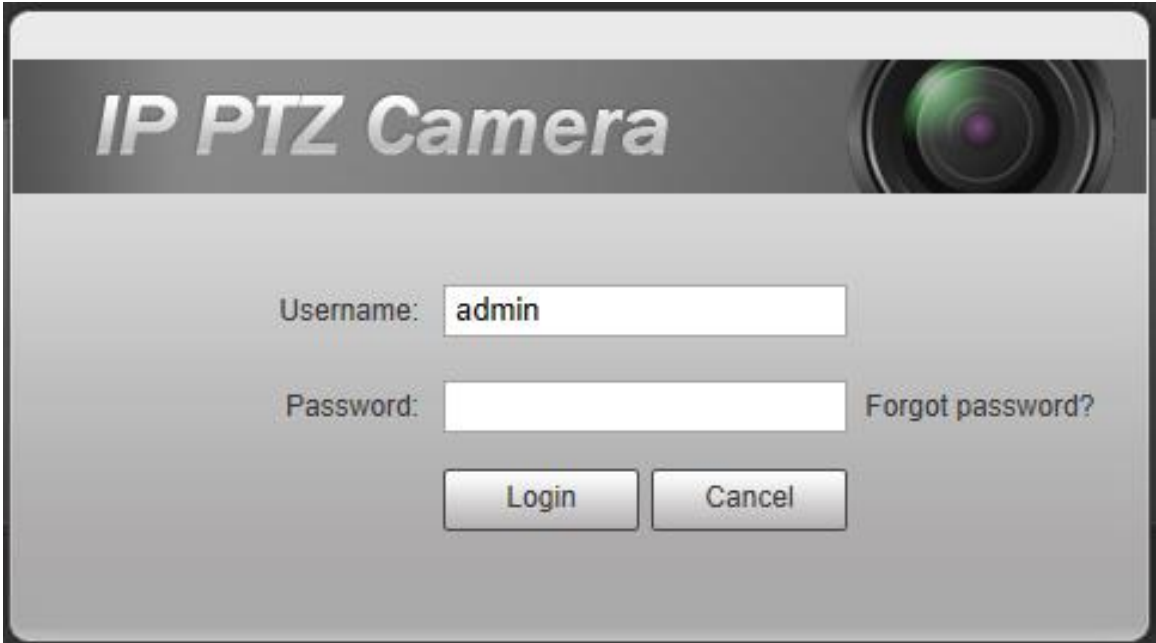
Category	Parameter	Description
Alarm Type	Motion Detection	Record alarm information in case of motion detection.
	Disk Full	Record alarm information in case of full disk.
	Disk Error	Record alarm information in case of disk error.
	Video Tamper	Record alarm information in case of video tampering.
	External 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.
Operation	Prompt	Select the Prompt check box. When you are not on the Alarm interface, 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.  If you are on the Alarm interface, 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.
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

Category	Parameter	Description
		triggered.
	Tone Path	Customize the storage path for alarm tones.

7 Logout

Click **Logout** to log out, and the login interface is displayed. See Figure 7-1. Enter the username and password to log in again.

Figure 7-1 Login interface

The image shows a web-based login interface for an IP PTZ camera. At the top, there is a dark grey header bar with the text "IP PTZ Camera" in a light grey, italicized font on the left, and a realistic camera lens graphic on the right. Below the header, the main area has a light grey gradient background. It contains two input fields: "Username:" with the text "admin" entered, and "Password:" which is currently empty. To the right of the password field is a link that says "Forgot password?". At the bottom of the form are two buttons: "Login" and "Cancel".

IP PTZ Camera

Username:

Password: [Forgot password?](#)

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 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. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. 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.

9. Assign Accounts and Privileges Reasonably

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

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.