Related Operations

- Switch chart type.
  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.
  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.6 IVS

The IVS function processes and analyzes the images to extract the key information to match the specified rules. When the detected behaviors match the rules, the system activates alarms.

- This function is available on select models.
- IVS and face detection cannot be enabled at the same time.

5.9.6.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

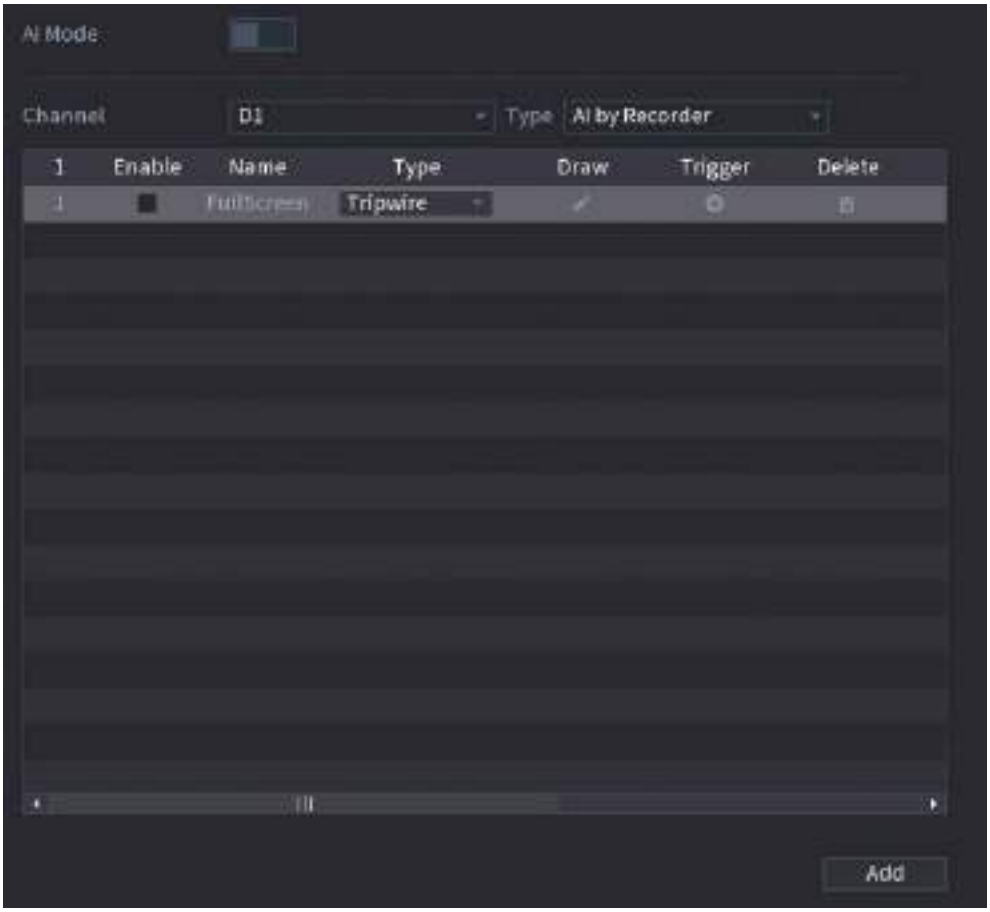
5.9.6.2 Configuring IVS

5.9.6.2.1 Tripwire

When the detection target crosses the warning line along the set direction, the system performs an alarm linkage action.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-103 IVS



Step 2 Select channel and AI type.

Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Tripwire**.

Step 5 Draw the detection rule.

1) Click to draw a straight line or a curve on the surveillance video image. Right-click the image to stop drawing.

Figure 5-104 Tripwire (AI by camera)

Figure 5-105 Tripwire (AI by recorder)

2) Click to draw the minimum size or maximum size to filter the target.
   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3) Configure the parameters.

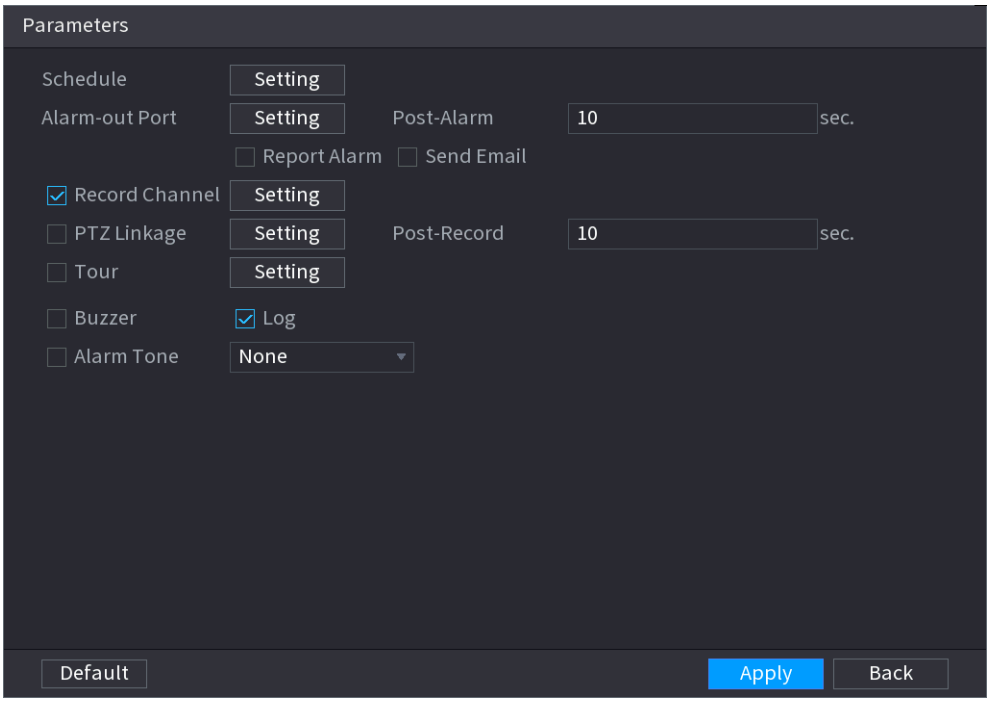
Table 5-27 Tripwire parameters

Parameter	Description
Name	Customize the rule name.
Direction	Set the tripwire direction, including A→B, B→A and A↔B.
Target Filter	Click and then select effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-106 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

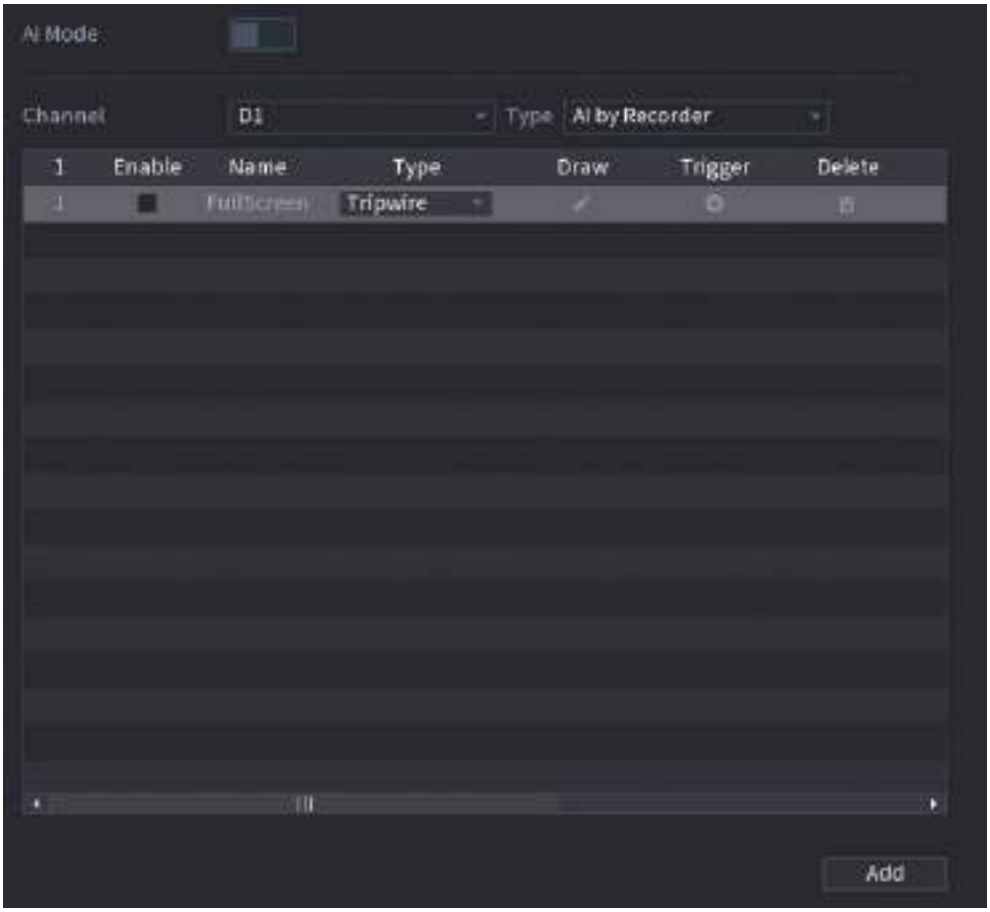
Step 7 Select the **Enable** checkbox and then click **Apply**.

5.9.6.2.2 Intrusion

When the detection target passes the edge of the monitoring area, and enters, leaves or traverses the monitoring area, the system performs an alarm linkage action.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-107 IVS



Step 2 Select channel and AI type.

Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Intrusion**.

Step 5 Draw the detection rule.

1) Click to draw the rule on the surveillance video image. Right-click the image to stop drawing.

Figure 5-108 Intrusion (AI by camera)

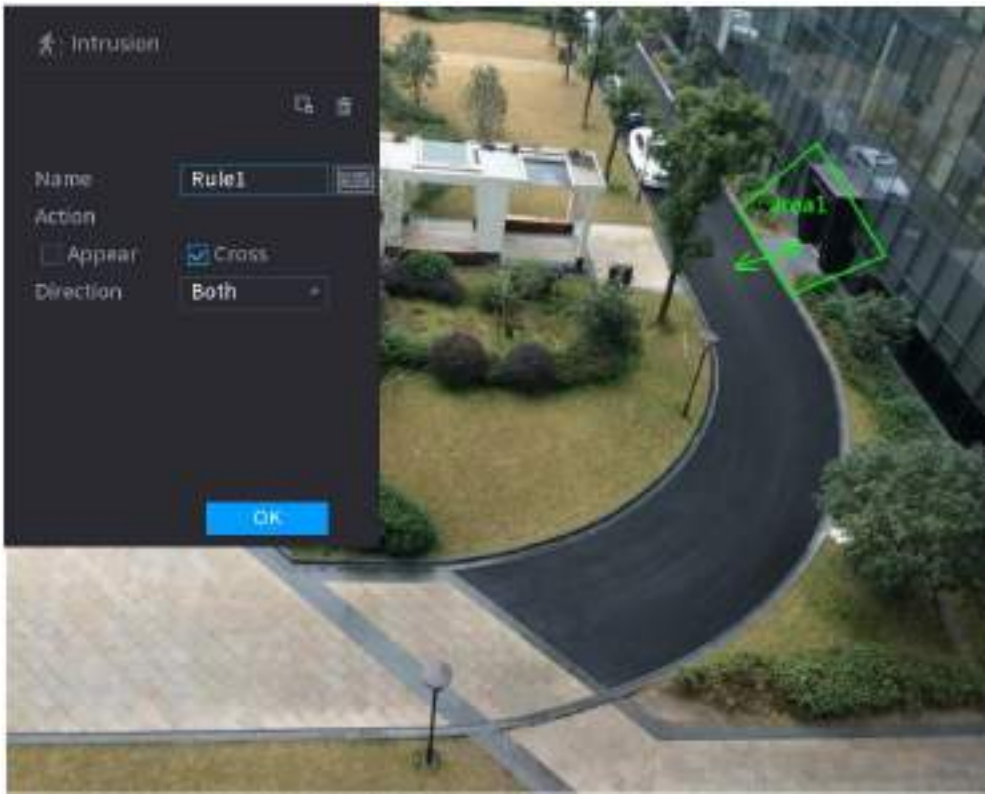
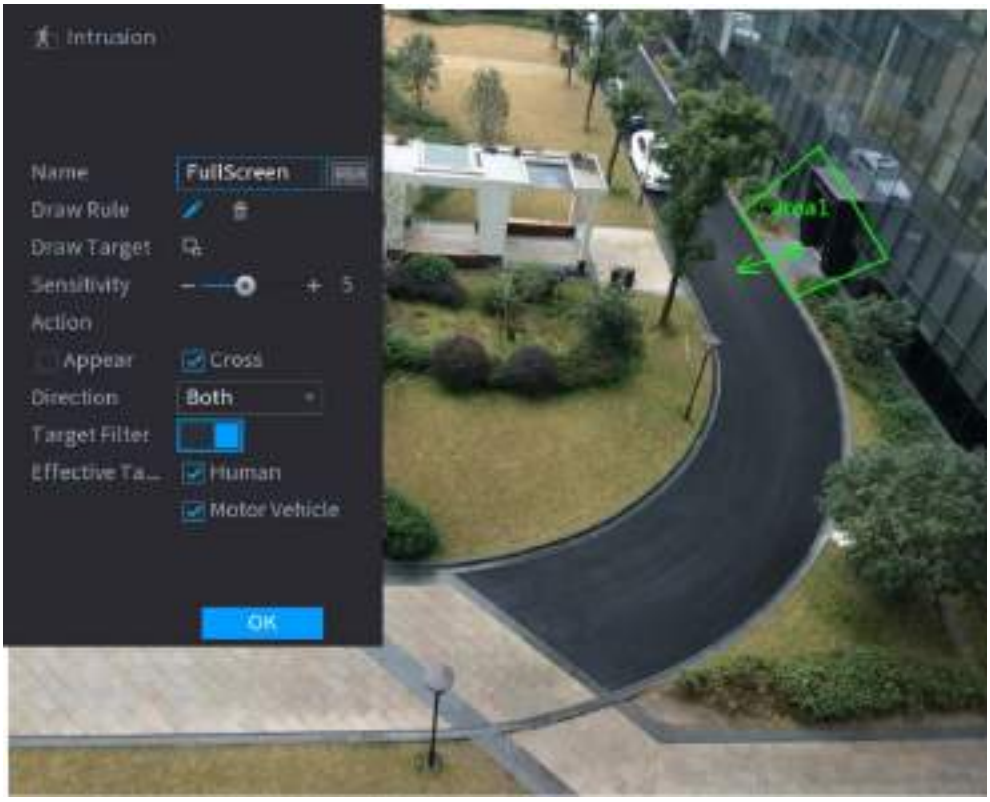


Figure 5-109 Intrusion (AI by recorder)



2) Click to draw the minimum size or maximum size to filter the target.
   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3) Configure the parameters.

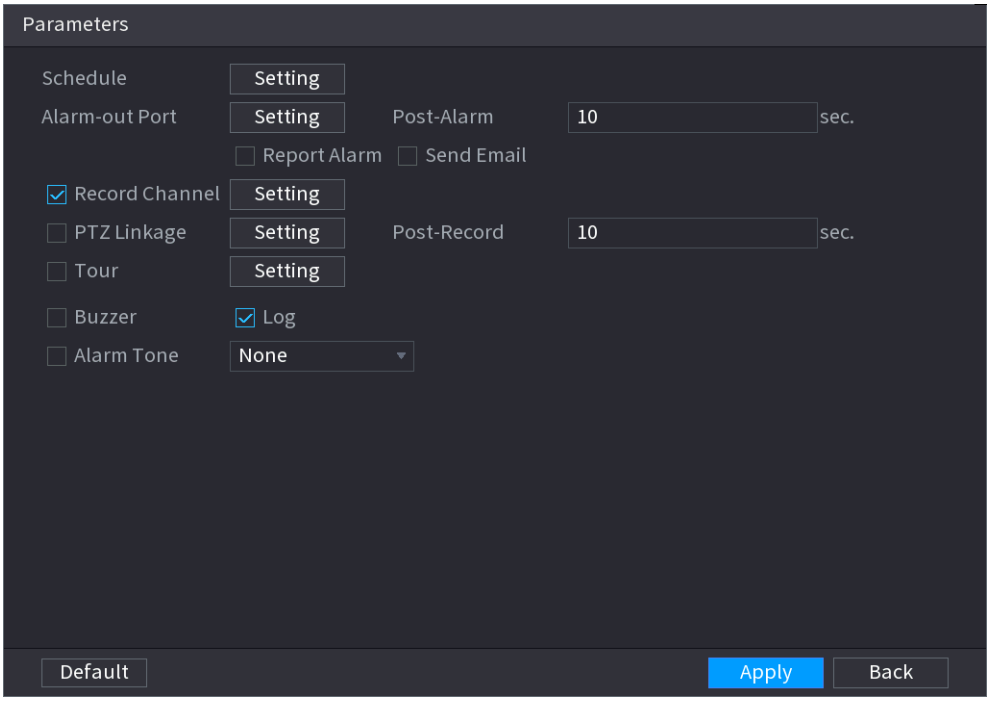
Table 5-28 Intrusion parameters

Parameter	Description
Name	Customize the rule name.
Action	Set the intrusion action, including appear and crossing area.
Direction	Set the direction to cross the area, including enter, exit and both.
Target Filter	Click and then select effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-110 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

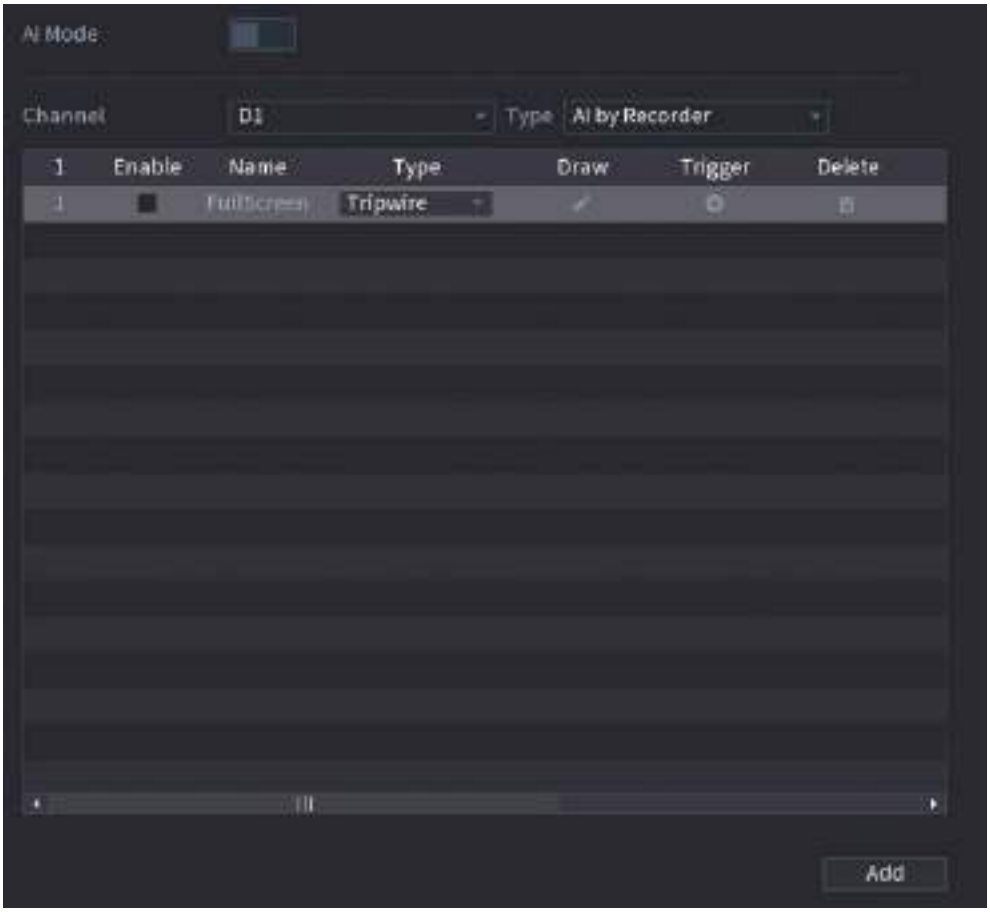
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.3 Abandoned Object Detection

The system generates an alarm when there is an abandoned object in the specified zone.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-111 IVS



Step 2 Select channel and AI type.

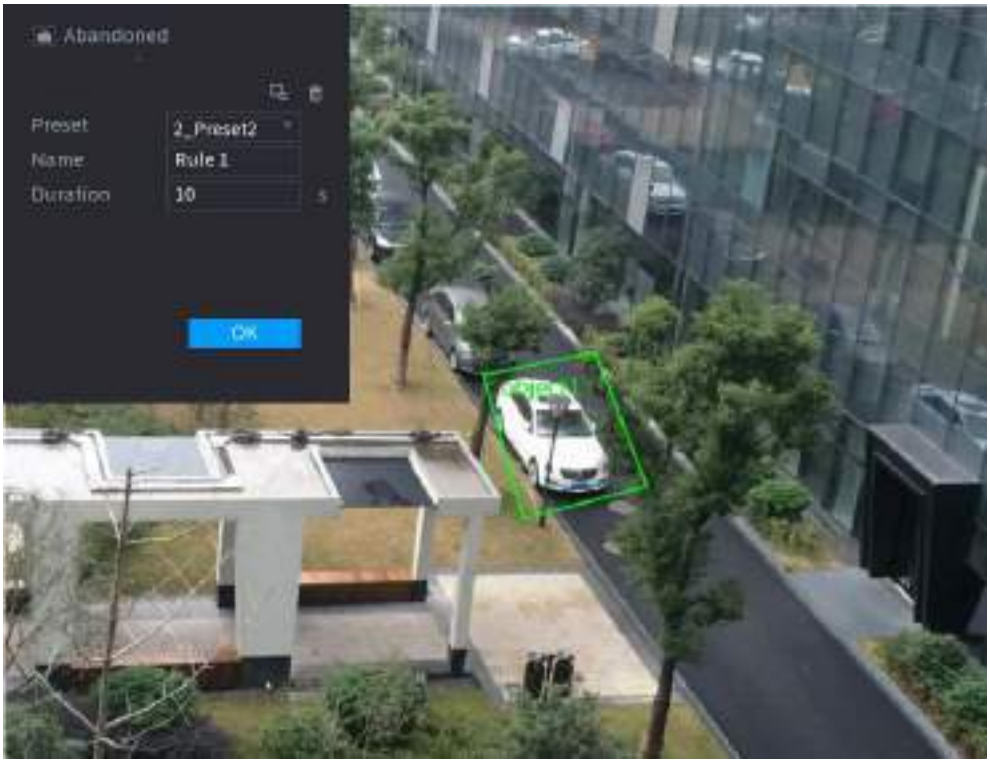
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Abandoned Object**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-112 Abandoned object rule



2) Click to draw the minimum size or maximum size to filter the target.

The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

3) Configure parameters.

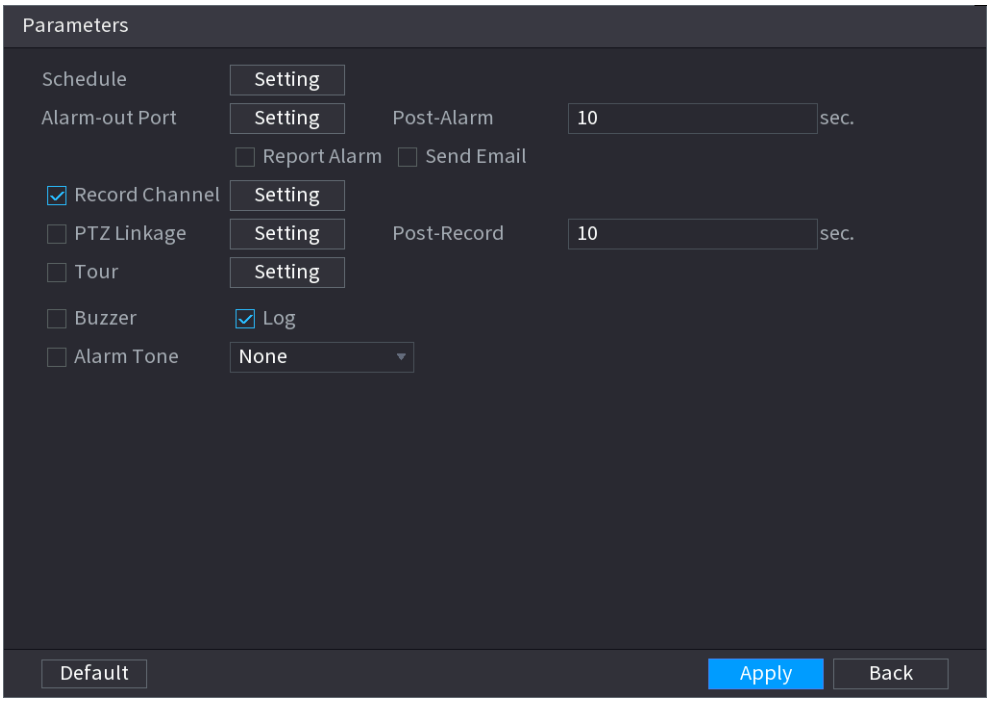
Table 5-29 Parameters of abandoned object detection

Parameter	Description
Preset	Select a preset you want to use IVS.
Name	Customize the rule name.
Duration	The system generates an alarm once the object is in the zone for the defined period.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-113 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

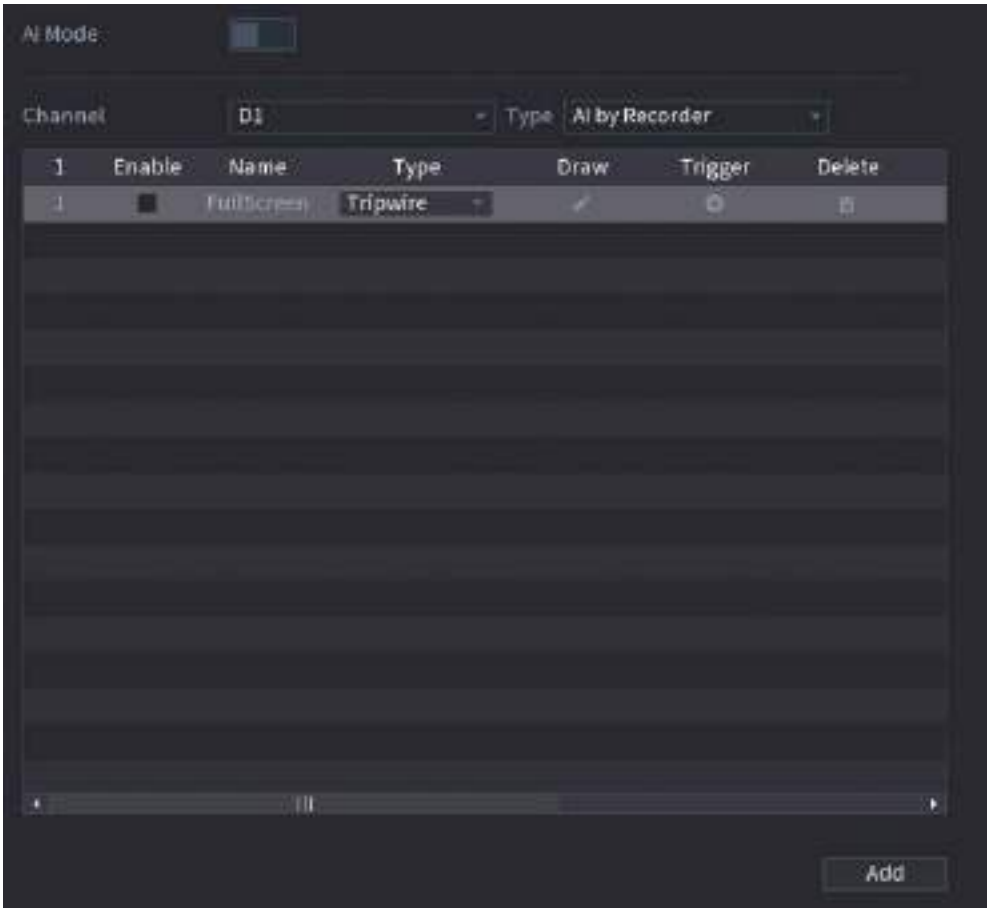
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.4 Fast Moving

You can detect the fast moving object in the specified zone.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-114 IVS



Step 2 Select channel and AI type.

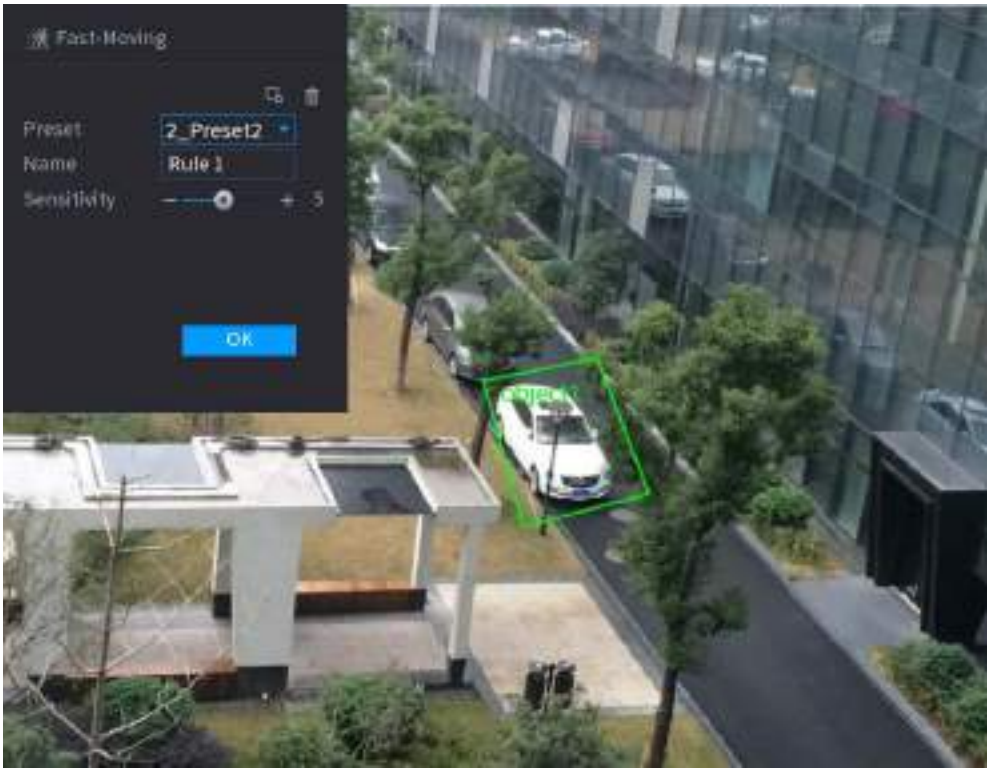
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Fast Moving**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-115 Fast moving



2) Click  to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

3) Configure parameters.

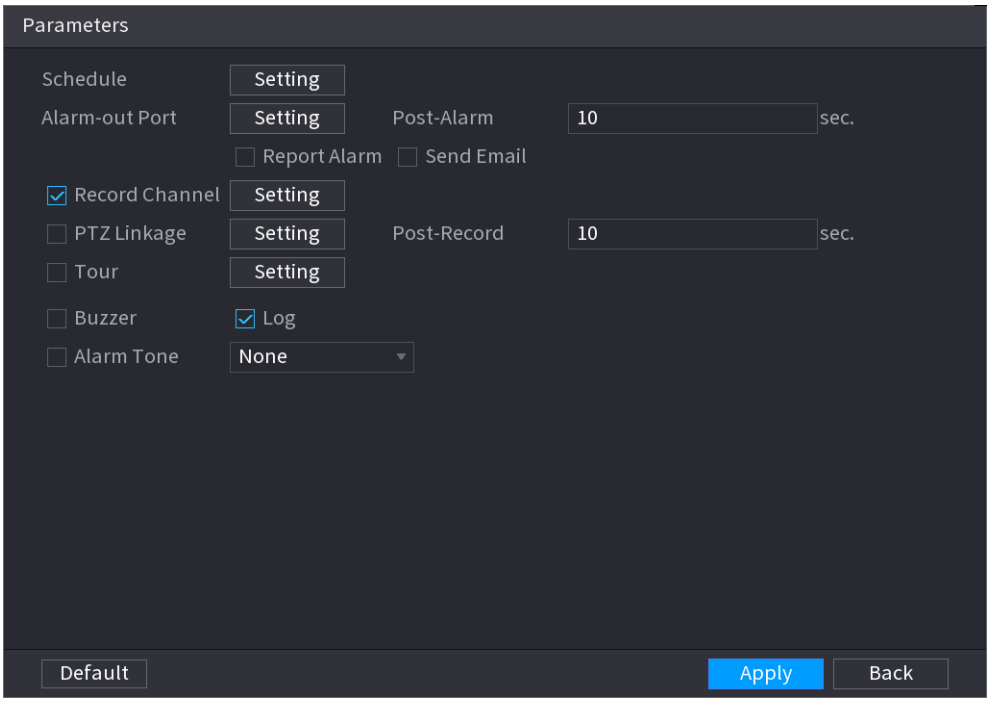
Table 5-30

Parameter	Description
Preset	Select a preset you want to use IVS
Name	Customize the rule name.
Sensitivity	You can set alarm sensitivity. The higher the value, the easier to detect a fast moving object but meanwhile the higher false alarm rate.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-116 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

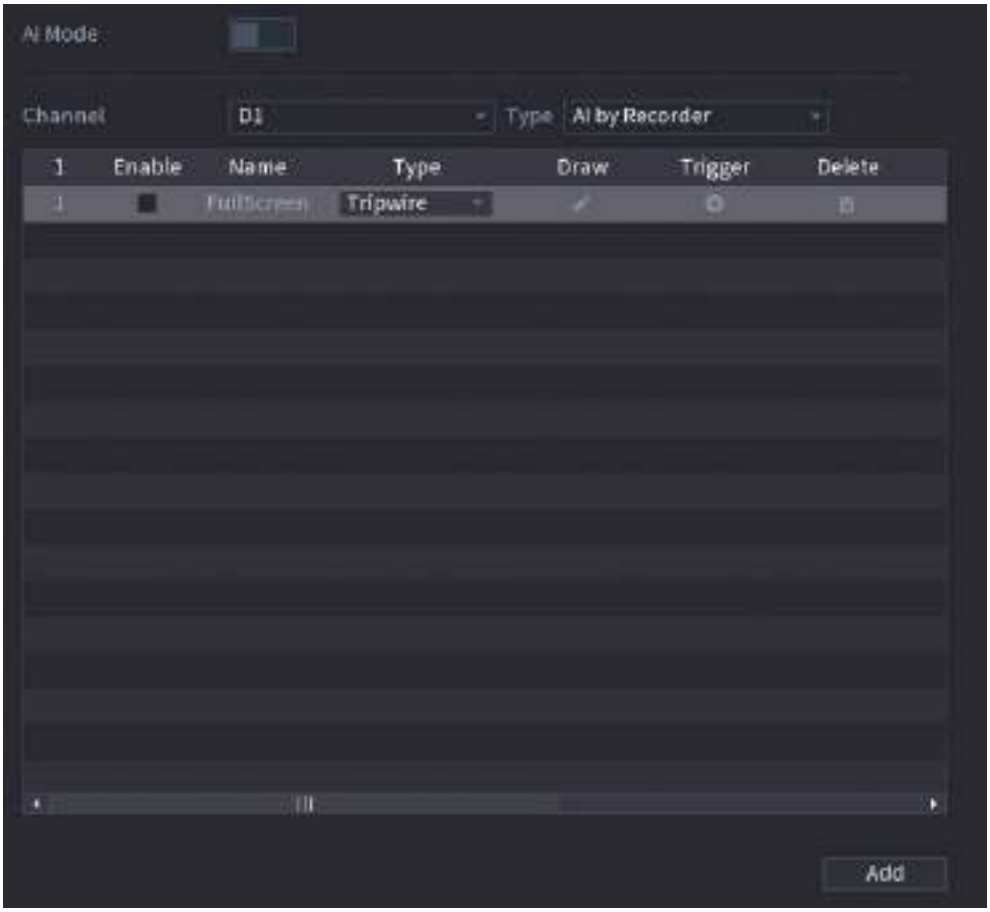
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.5 Parking

When the detection target stays in the monitoring area longer than the set duration, the system performs alarm linkage action.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-117 IVS



Step 2 Select channel and AI type.

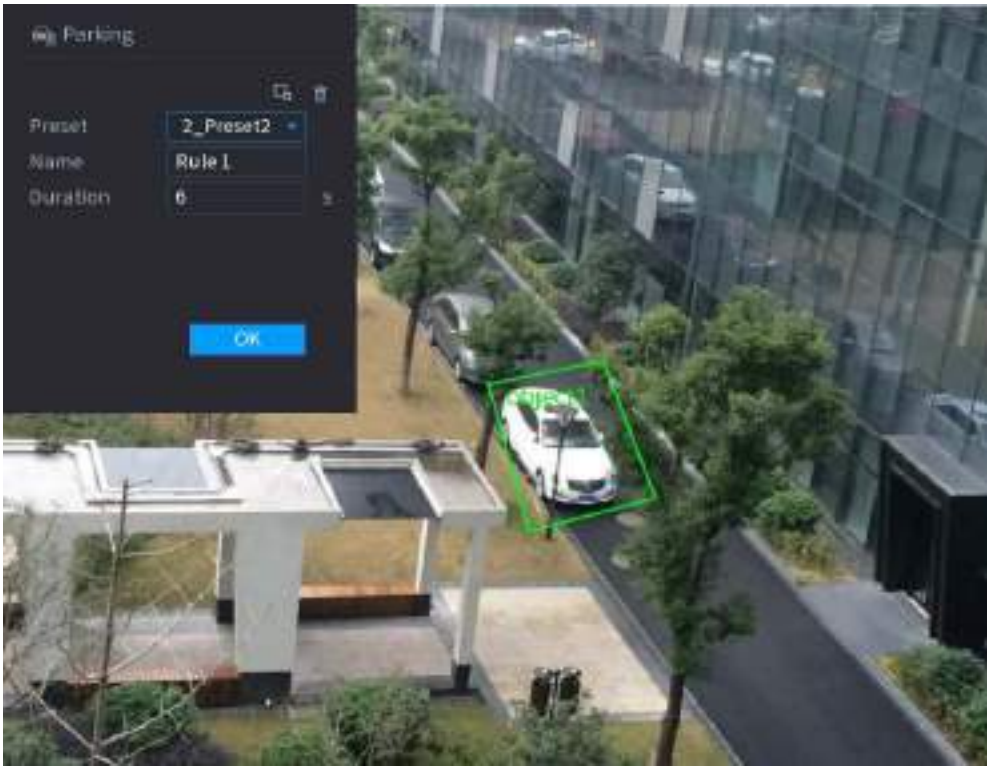
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Parking**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-118 Parking



2) Click to draw the minimum size or maximum size to filter the target.
   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3) Configure parameters.

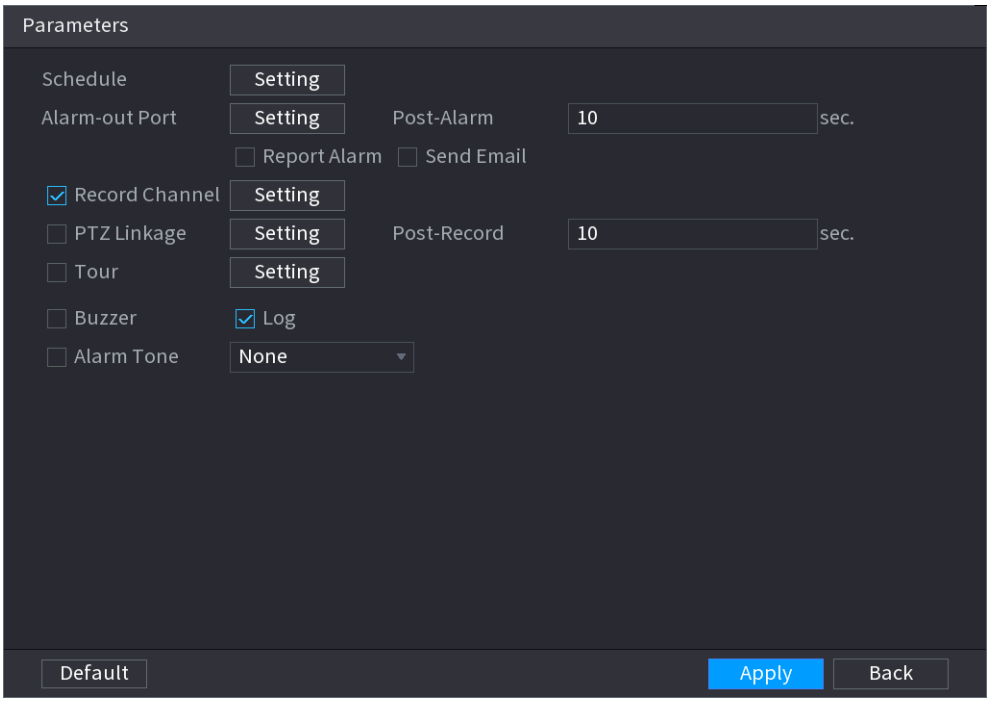
Table 5-31

Parameter	Description
Preset	Set the preset point for IVS detection.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-119 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

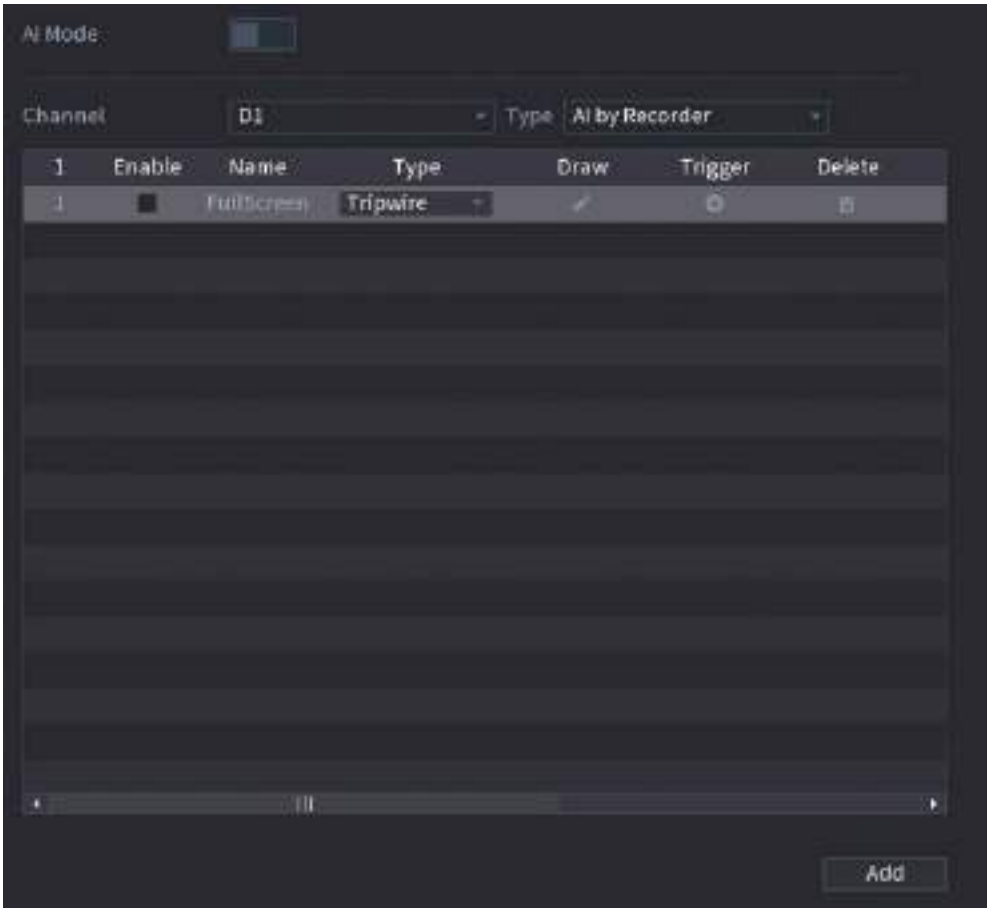
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.6 Crowd Gathering

The system generates an alarm once people are gathering in the specified zone longer than the defined duration.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-120 IVS



Step 2 Select channel and AI type.

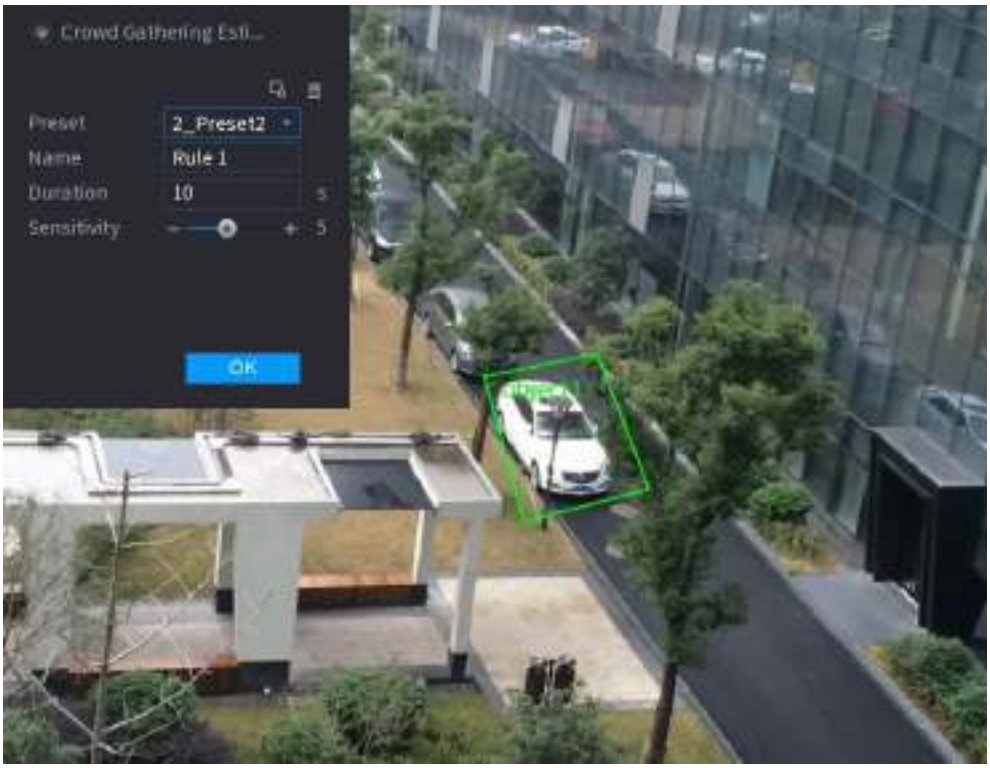
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Crowd Gathering Estimation**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-121 Crowd gathering



2) Click  to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

3) Set parameters.

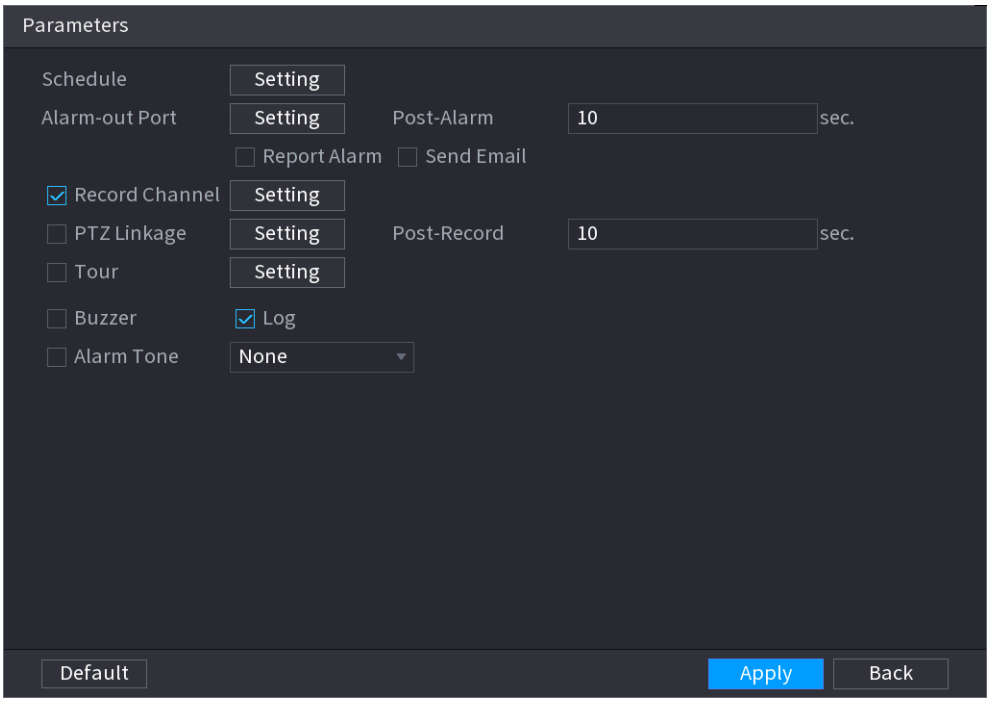
Table 5-32 Crowd gathering parameters

Parameter	Description
Preset	Select a preset you want to use IVS.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.
Sensitivity	You can set alarm sensitivity. The higher the value, the easier to detect crowd gathering but meanwhile the higher false alarm rate.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-122 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

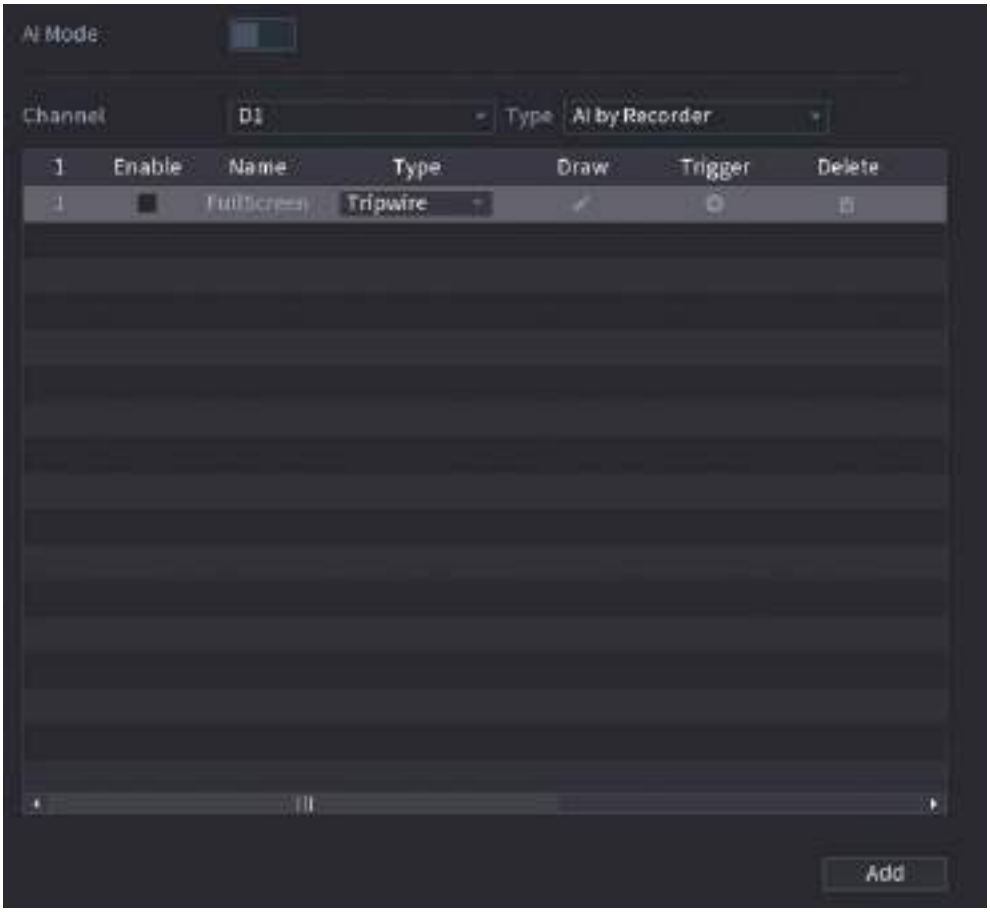
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.7 Missing Object Detection

The system generates an alarm when there is missing object in the specified zone.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-123 IVS



Step 2 Select channel and AI type.

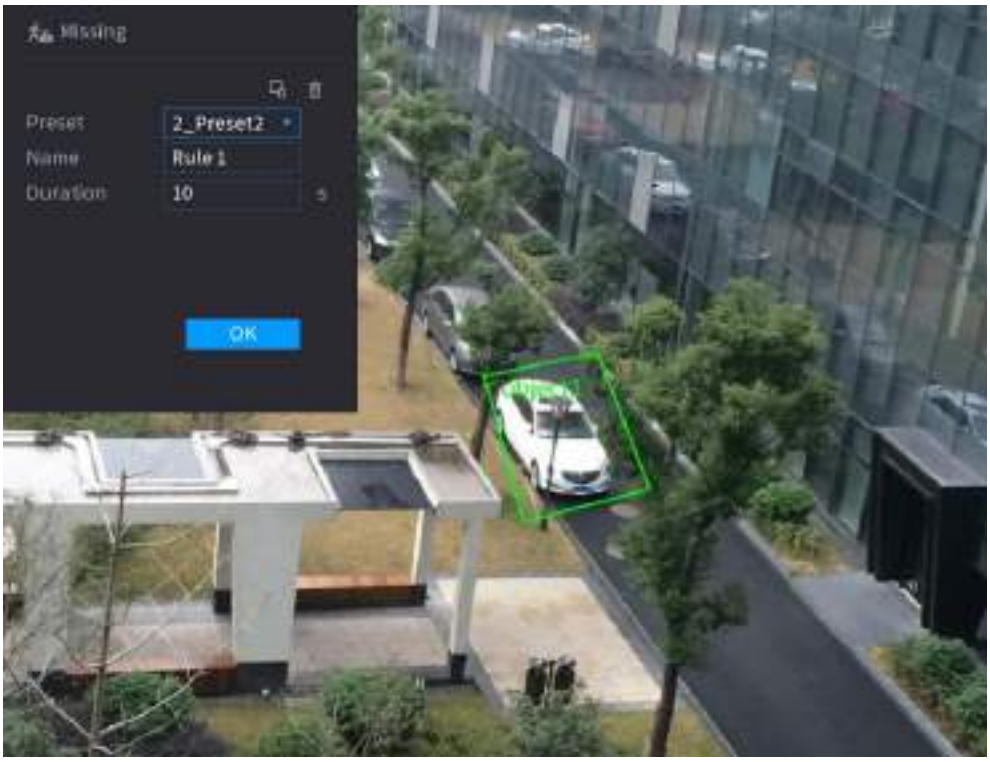
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Missing**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-124 Missing object



2) Click  to draw the minimum size or maximum size to filter the target.

The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

3) Configure parameters.

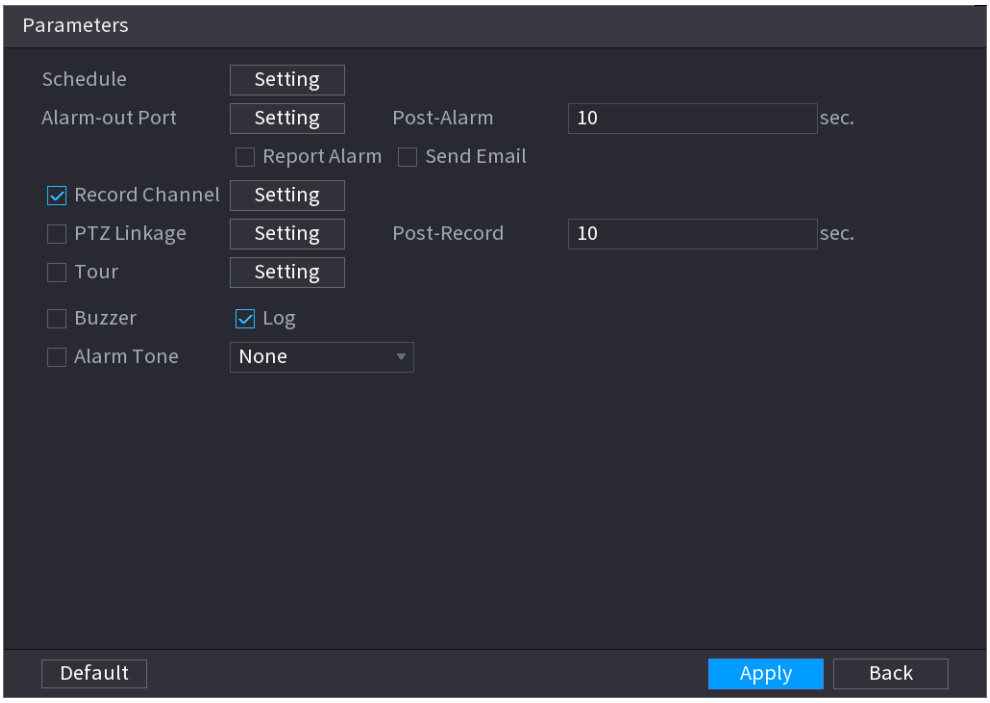
Table 5-33 Parameters of missing object detection

Parameter	Description
Preset	Set the preset point for IVS detection according to the actual needs.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-125 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

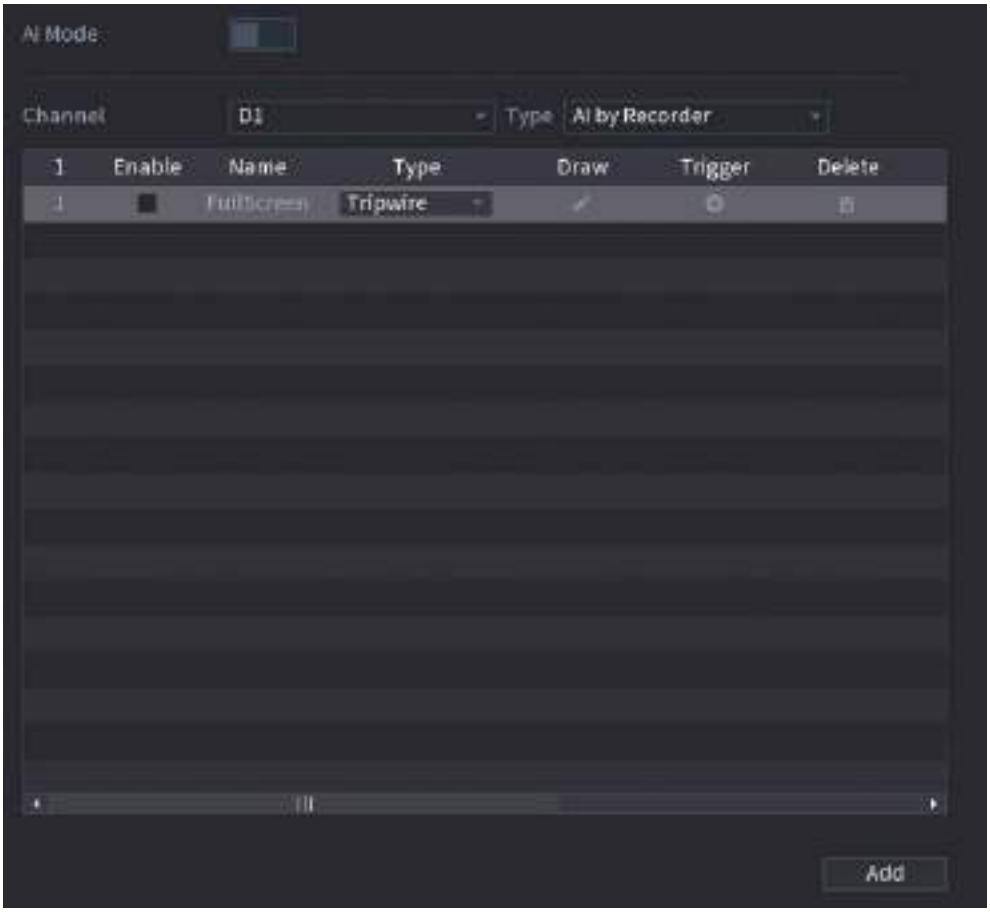
Step 7 Select **Enable** checkbox and then click **Apply**.

5.9.6.2.8 Loitering Detection

The system generates an alarm once the object is staying in the specified zone longer than the defined duration.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-126 IVS



Step 2 Select channel and AI type.

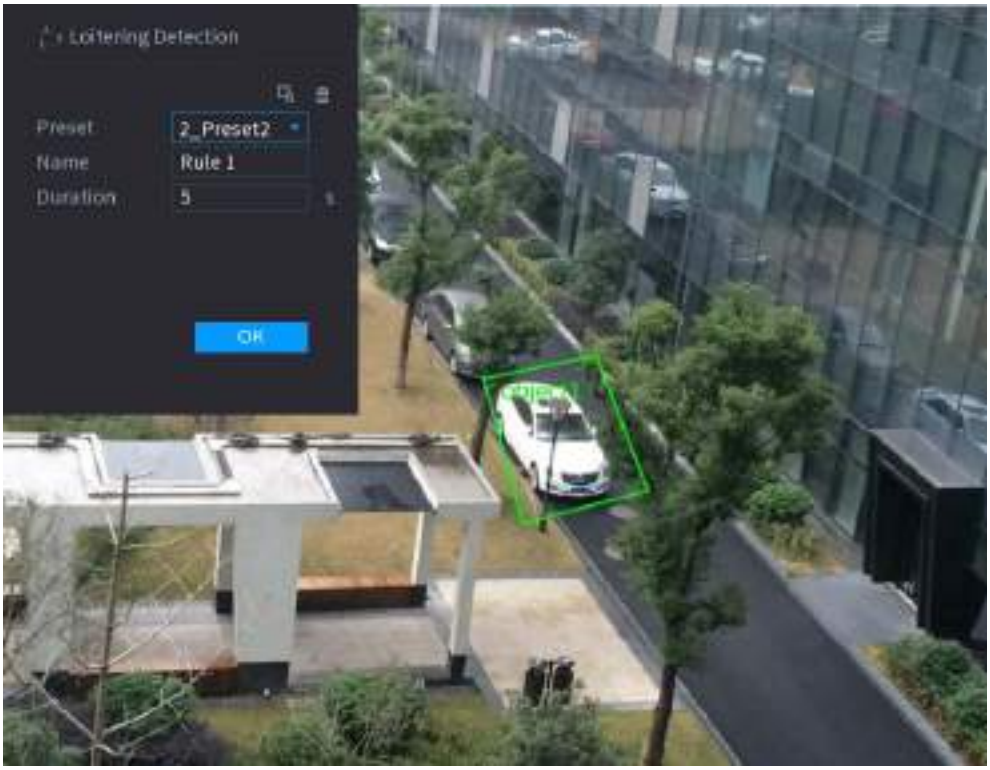
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Loitering Detection**.

Step 5 Draw the detection rule.

1) Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-127 Loitering detection



2) Click to draw the minimum size or maximum size to filter the target.
   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3) Configure parameters.

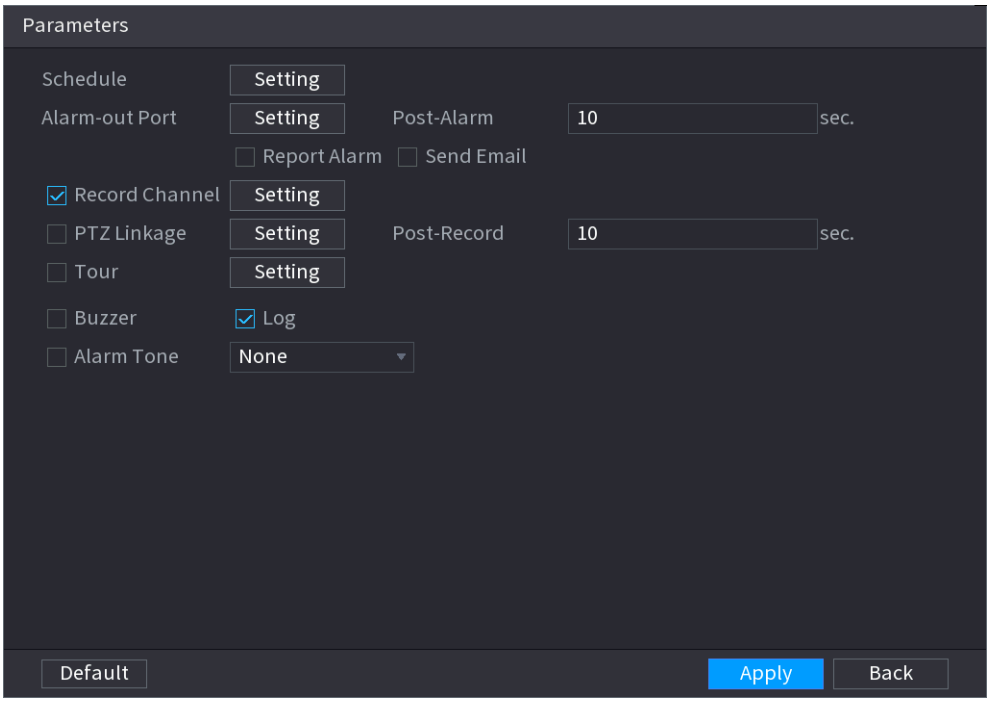
Table 5-34 Loitering detection parameters

Parameter	Description
Preset	Set the preset point for IVS detection.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.

4) Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-128 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

Step 7 Select **Enable** checkbox and then click **Apply**.

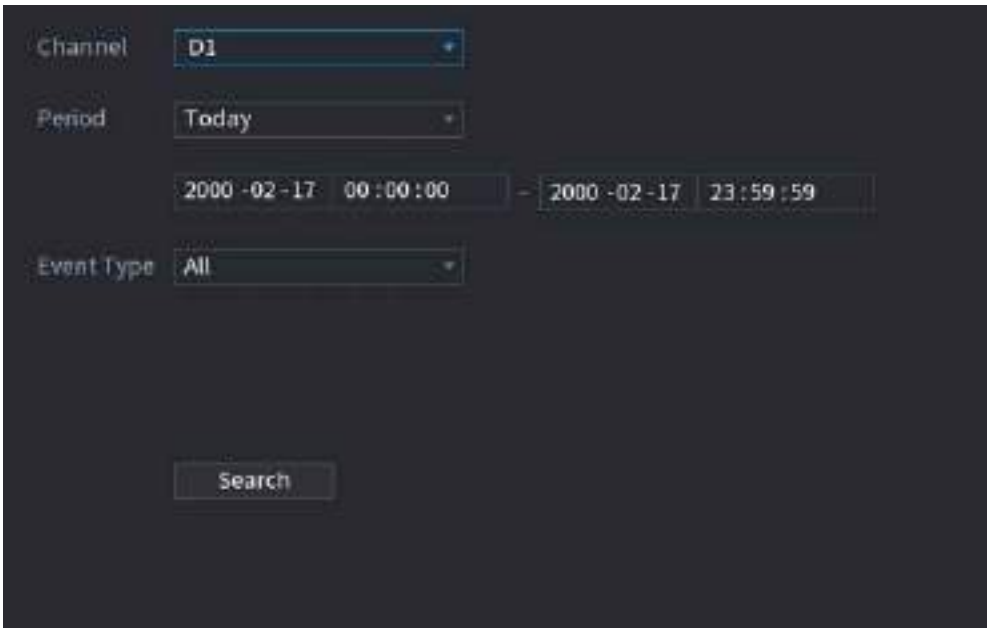
5.9.6.3 AI Search (IVS)

You can search for IVS detection results.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **IVS**.

Figure 5-129 IVS search



Step 2 Select a channel, start time, end time, event type, and then click **Search**.
The search results are displayed.

Related Operations

- Play back video.
  Click an image, and then click  to play back the related video.
  During playback, you can:
  - Click  to pause.
  - Click to stop.
  - Click  to display AI rule. The icon changes to  .
- Add tags.
  Select one or more images, and then click **Add Tag**.
- Lock.
  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.
  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.
  Select one or more images, click **Backup**, select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.7 Stereo Analysis

By drawing and setting the rules of stereo behavior analysis, the system will perform alarm linkage actions when the video matches the detection rule. Types of events include: people approach detection, fall detection, violence detection, people No. exception detection and people stay

detection.

- This function requires access to a camera that supports stereo behavior analysis.
- Stereo analysis and IVS are mutually exclusive and cannot be enabled at the same time.

5.9.7.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.7.2 Configuring Stereo Analysis

5.9.7.2.1 People Approach Detection

When two people stay in the same detection area longer than the defined duration or when the distance between two people is larger or smaller than the defined threshold, an alarm will be triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People Approach Detection**.

Step 4 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2) Configure parameters.

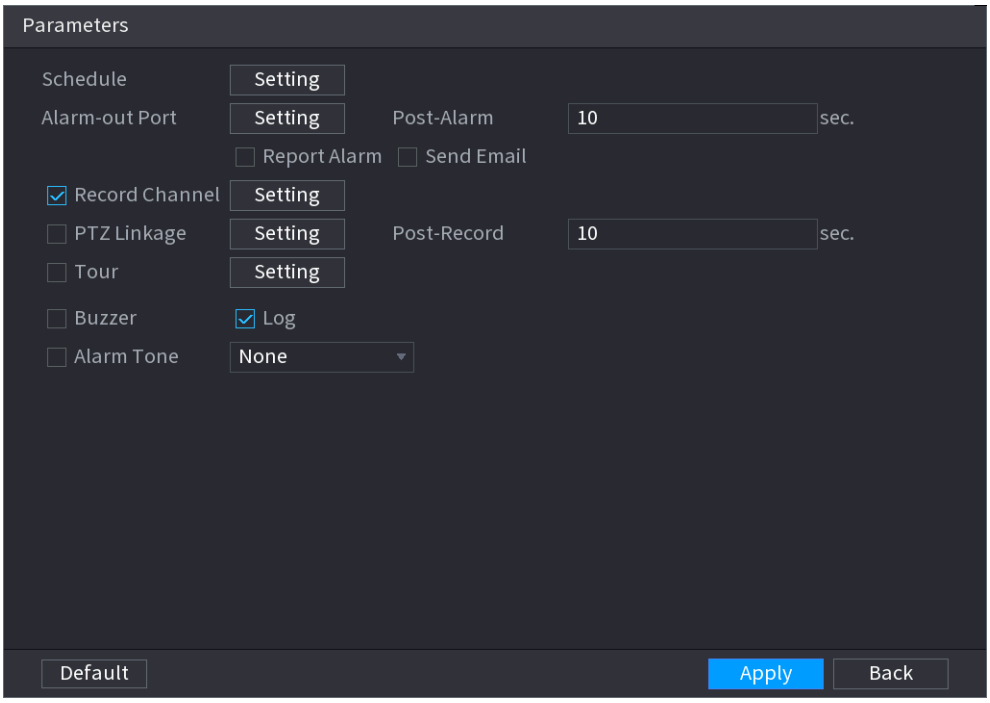
Table 5-35 Parameters of people approach detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set how long two people stay in the same detection area until an alarm is triggered.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.
Interval Threshold	When the distance between people in the area is greater than or less than the defined threshold, an alarm will be triggered.

3) Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-130 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

Step 6 Click **Apply**.

5.9.7.2.2 Fall Detection

When someone falls from a height in the detection area and the duration of the action is greater than the defined threshold, an alarm will be triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **Fall Detection**.

Step 4 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2) Configure parameters.

Table 5-36 Parameters of fall detection

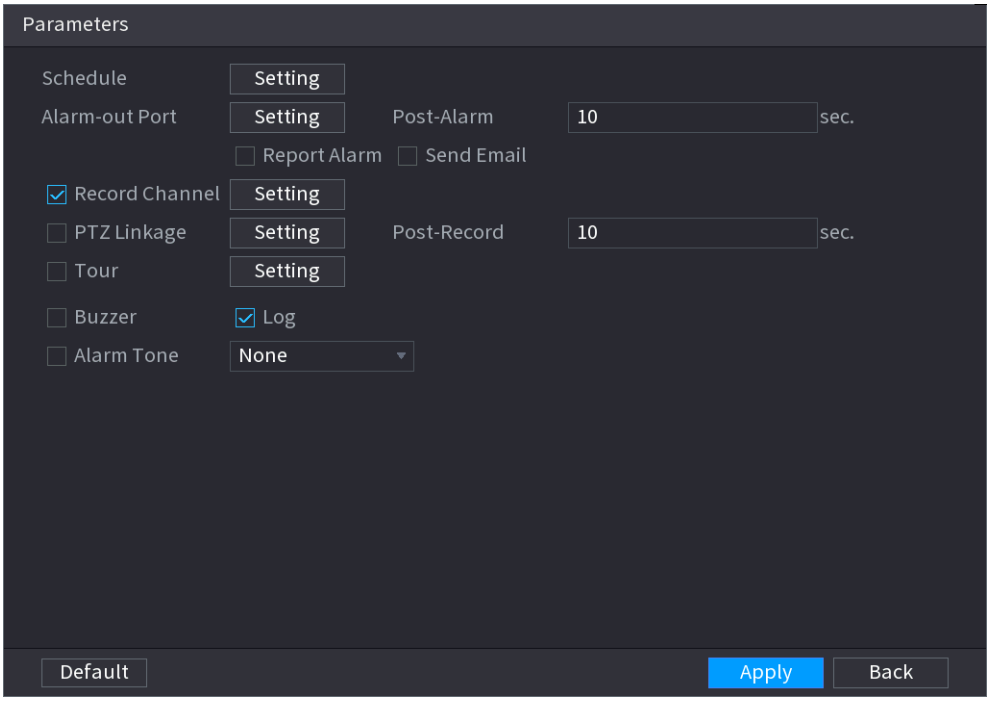
Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set the minimum time of triggering an alarm when people fall.

Parameter	Description
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3) Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-131 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

Step 6 Click **Apply**.

5.9.7.2.3 Violence Detection

When the target in the detection region has large body movements such as smashing and fighting, an alarm will be triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **Violence Detection**.

Step 4 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2) Configure parameters.

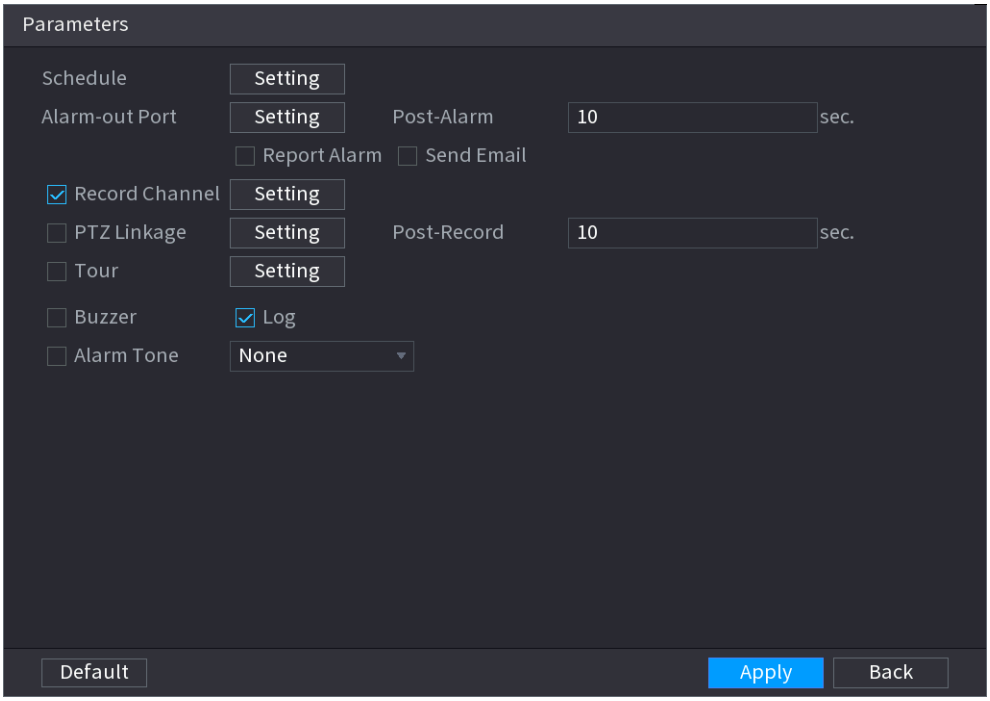
Table 5-37 Parameters of violence detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.

3) Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-132 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

Step 6 Click **Apply**.

5.9.7.2.4 People No. Exception Detection

When the system detects an abnormal number of people in the same detection area, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People No. Exception Detection**.

Step 4 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.

2) Configure parameters.

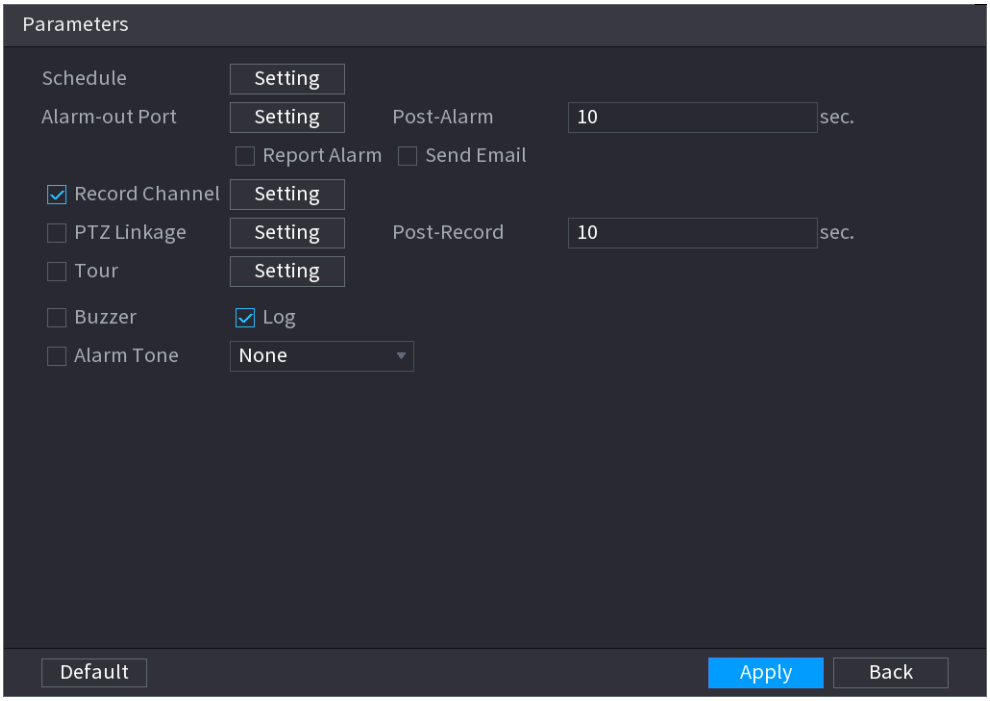
Table 5-38 Parameters of people No. exception detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set the minimum time to trigger an alarm after the system detects an abnormal number of people.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.
Alarm People No.	When the number of people in the area is greater than, equal to, or less than the defined threshold, an alarm will be triggered.

3) Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-133 Schedule and alarm linkage



1) Click .

2) Click **Setting** next to **Schedule** to configure the alarm period.

The system performs linkage actions only for alarms during the arming period.

- On the time line, drag to set the period.
- You can also click to set the period.

3) Configure alarm linkage. For details, see Table 5-42.

4) Click **Apply**.

Step 6 Click **Apply**.

5.9.7.2.5 People Stay Detection

When the target stays in the detection area longer than the defined duration, an alarm will be

triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People Stay Detection**.

Step 4 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2) Configure parameters.

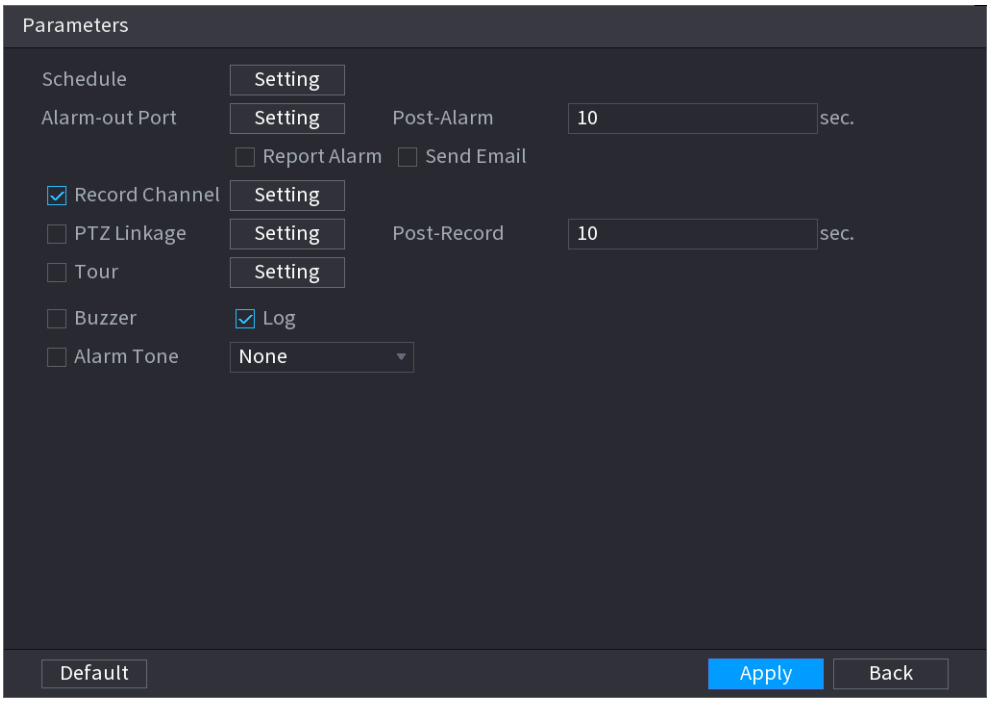
Table 5-39 Parameters of people stay detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set low long people stay in the detection area until an alarm is triggered.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3) Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-134 Schedule and alarm linkage



1) Click .
2) Click **Setting** next to **Schedule** to configure the alarm period.
   The system performs linkage actions only for alarms during the arming period.
   - On the time line, drag to set the period.
   - You can also click to set the period.
3) Configure alarm linkage. For details, see Table 5-42.
4) Click **Apply**.

Step 6 Click **Apply**.

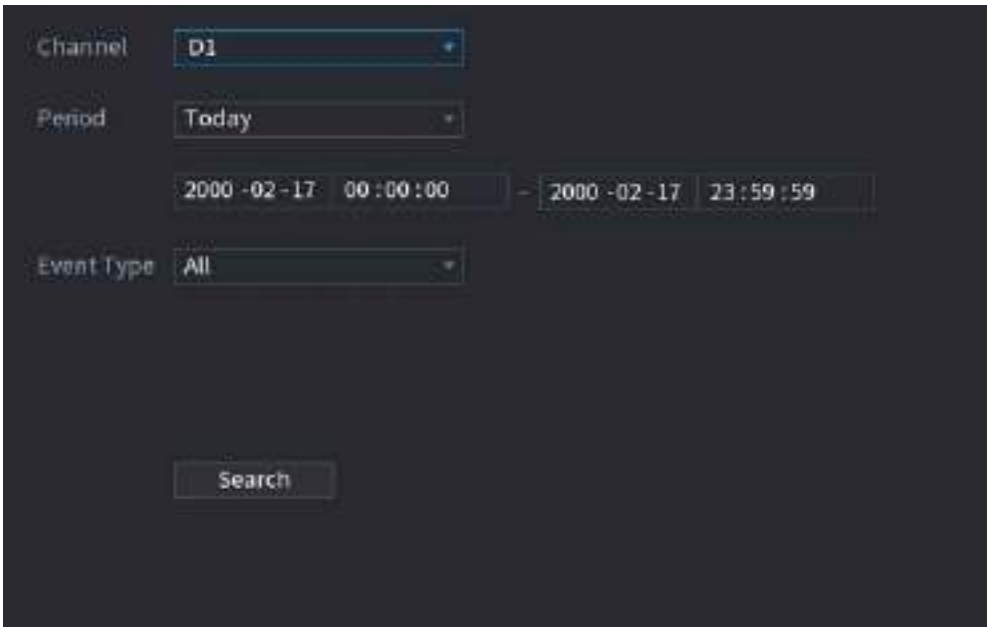
5.9.7.3 AI Search (Stereo Analysis)

You can search for detection results of stereo analysis.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Stereo Analysis**.

Figure 5-135 Stereo analysis search



Step 2 Select a channel, start time, end time, event type, and then click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click  to play back the related video.

  During playback, you can:

  - Click  to pause.
  - Click  to stop.
  - Click  to display AI rule. The icon changes to  .

- Add tags.

  Select one or more images, and then click **Add Tag**.

- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.

- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.

- Back up.

  Select one or more images, click **Backup**, select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.8 Video Metadata

The system analyzes real-time video stream to detect the existence of human, motor vehicle, and non-motor vehicle. Once a target is detected, an alarm is triggered.

5.9.8.1 Enabling Smart Plan

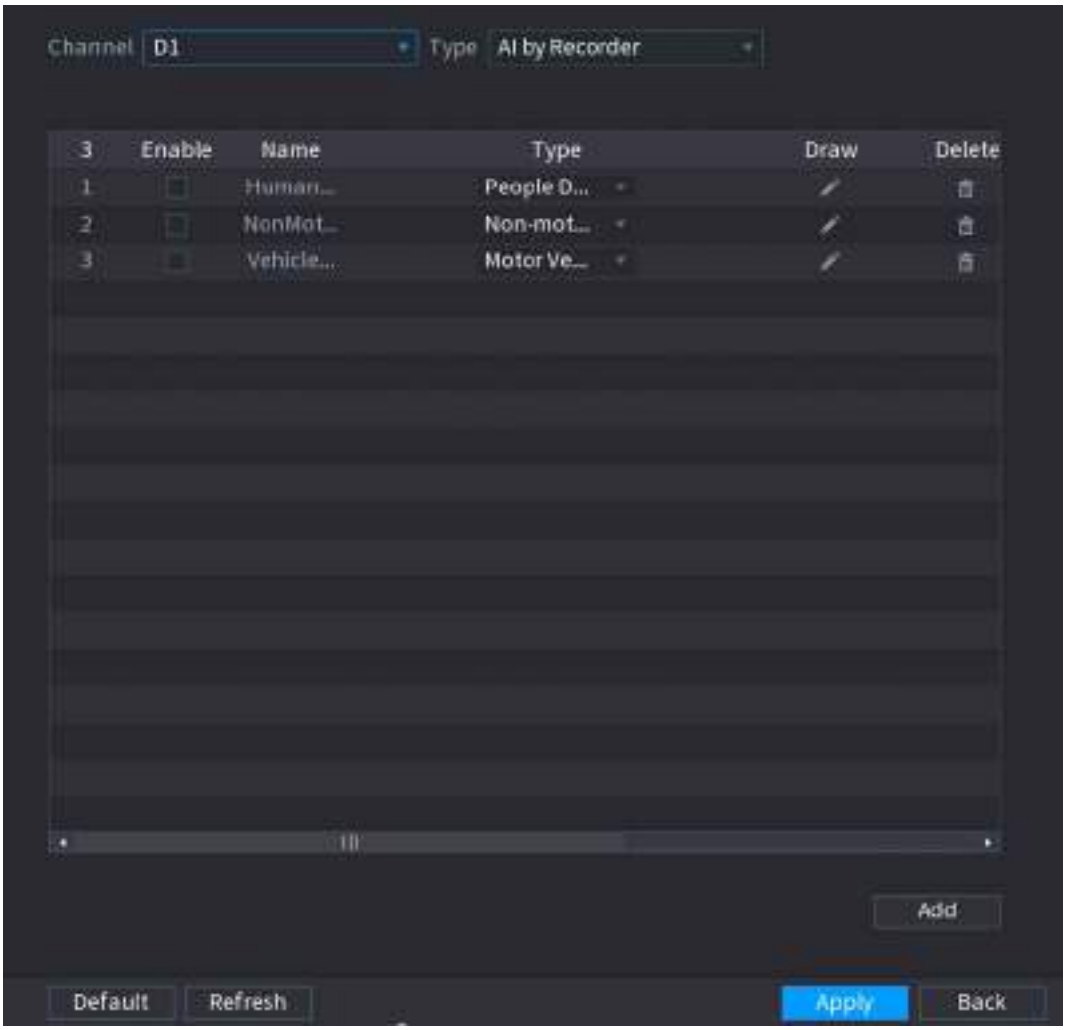
To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.8.2 Configuring Video Metadata

When a metadata alarm is triggered, the system links the corresponding camera to record videos and logs and take snapshots. Other alarm linkage actions are not supported for video metadata.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Video Metadata**.

Figure 5-136 Video metadata



Step 2 Select a channel and AI type.

AI by Recorder is available on select models.

Step 3 Click **Add** to add a rule.

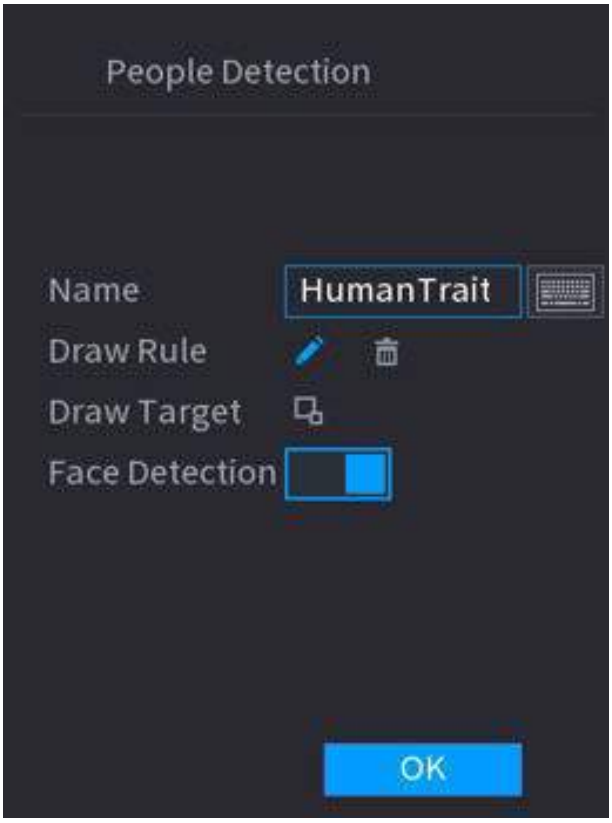
Step 4 Select **Enable** and then set **Type** to **People Detection**, **Non-motor Vehicle Detection** or

Motor Vehicle Detection.

Step 5 Draw detection rule.

1) Click , and then draw a detection area on the video image. Right-click the image to stop drawing.

Figure 5-137 People detection



2) Enter the rule name.
3) Click to draw the minimum size or maximum size to filter the target.
   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
4) Click to enable face detection.
5) Select **A to B**, **B to A**, or **Both** as direction for tripwire counting.

   Tripwire counting is available when AI by Camera is used and the camera supports this function.
6) Click **OK**.

Step 6 Click **Apply**.

5.9.8.3 AI Search (Video Metadata)

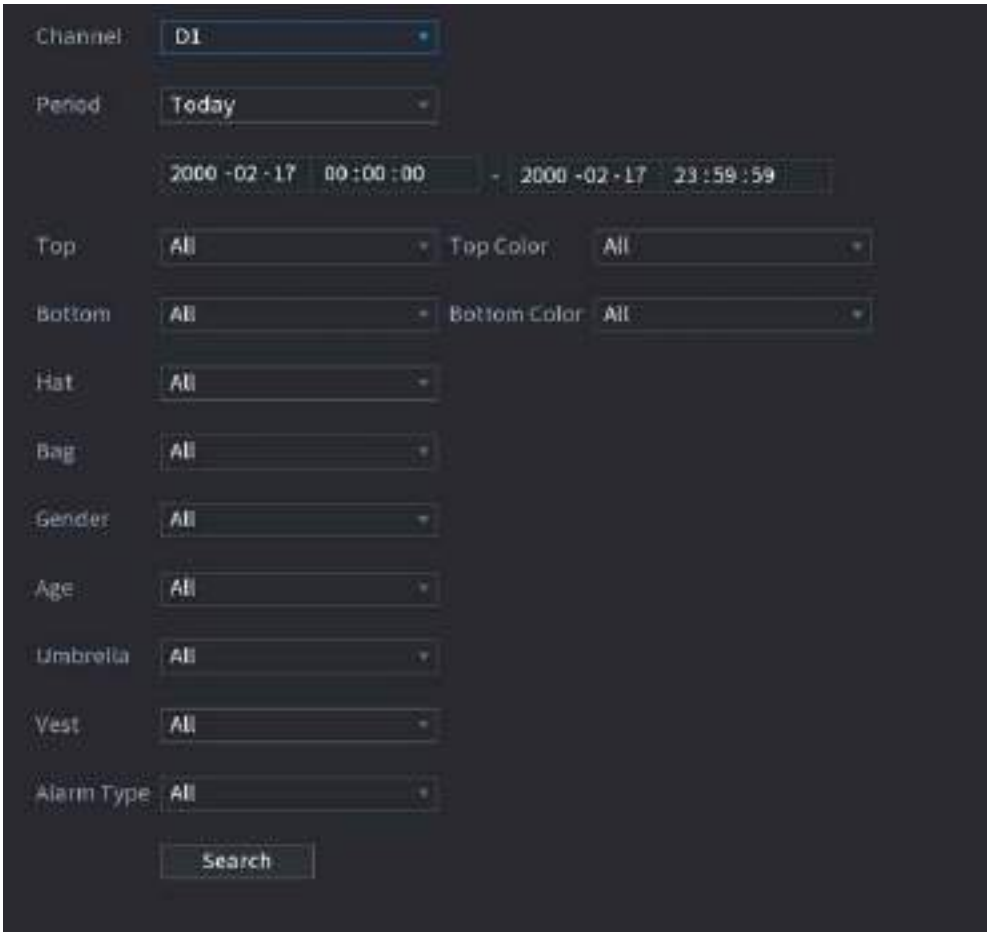
You can search for the video metadata detection results and play back related videos.

5.9.8.3.1 Human Detection

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Human Detection**.

Figure 5-138 Human detection

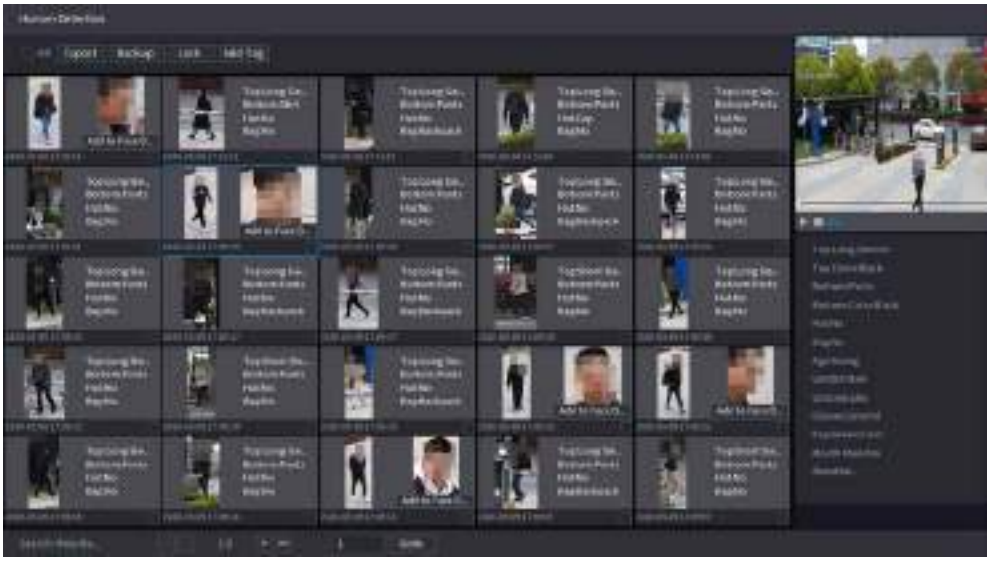


Step 2 Select a channel, start time, end time, and set corresponding parameters.

Step 3 Click **Search**.

For privacy protection, the faces are intentionally blurred.

Figure 5-139 Search results



Related Operations

- Play back video.

  Click an image, and then click  to play back the related video.

  During playback, you can:

  - Click  to pause.
  - Click  to stop.
  - Click  to display AI rule. The icon changes to  .

- Add tags.

  Select one or more images, and then click **Add Tag**.

- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.

- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.

- Back up.

  Select one or more images, click **Backup**, select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.8.3.2 Motor Vehicle Detection

Background Information

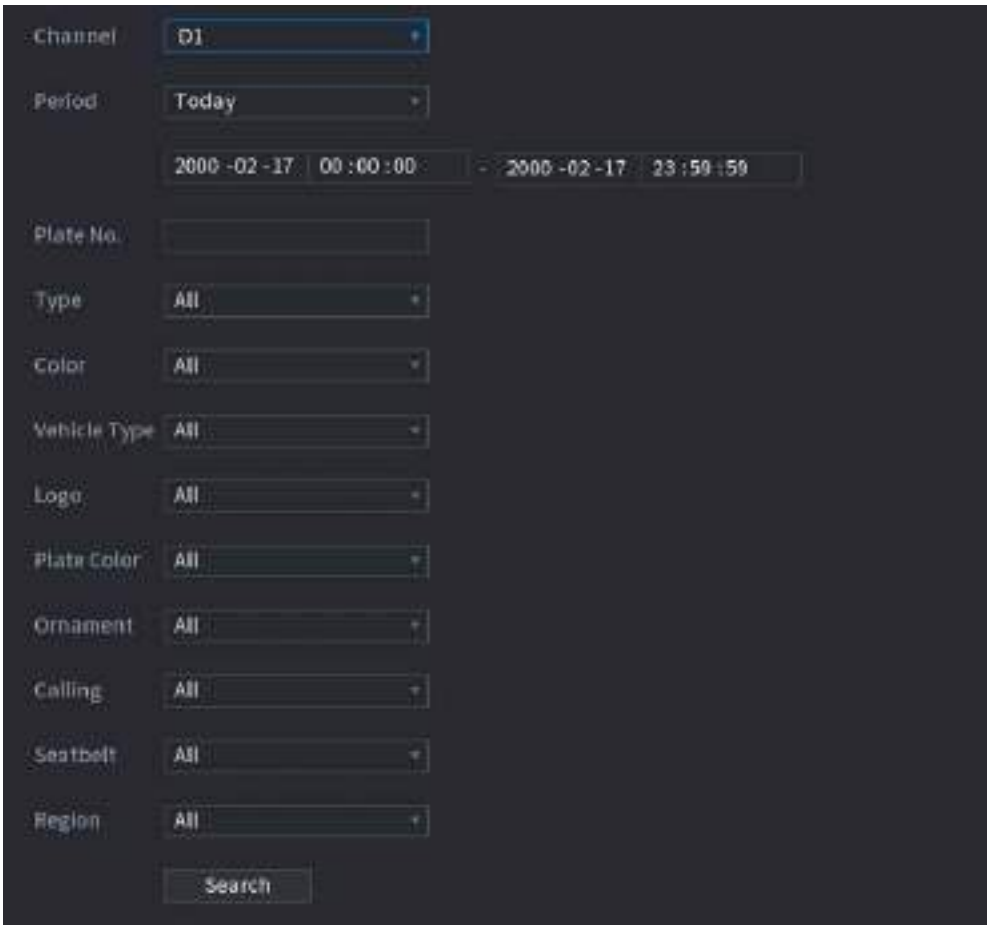
You can search for motor vehicle detection results according to the vehicle parameters.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Motor Vehicle Detection**.

Figure 5-140 Motor vehicle detection



Step 2 Select a channel and then set parameters.

- The system supports fuzzy search of plate numbers.
- The system searches all plate numbers by default if you have not set a plate number.

Step 3 Click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.

- Back up.
  Select one or more images, click **Backup**, select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.8.3.3 Non-motor Vehicle Detection

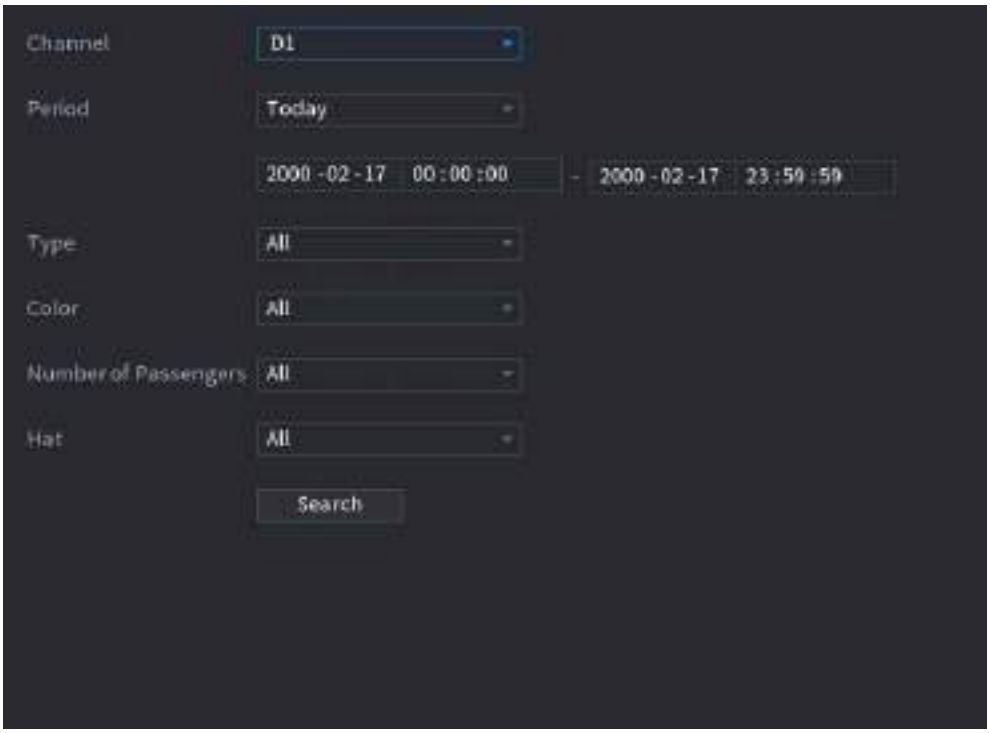
You can search for non-motor vehicle detection results according to the non-motor vehicle parameters.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Non-Motor Vehicle Detection** .

Figure 5-141 Non-motor vehicle detection



Step 2 Select a channel and then set parameters.

Step 3 Click **Search**.

Figure 5-142 Search results

Related Operations

- Play back video.

  Click an image, and then click  to play back the related video.

  During playback, you can:

  - Click  to pause.
  - Click  to stop.
  - Click  to display AI rule. The icon changes to  .

- Add tags.

  Select one or more images, and then click **Add Tag**.

- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.

- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.

- Back up.

  Select one or more images, click **Backup**, select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.8.3.4 Report Query

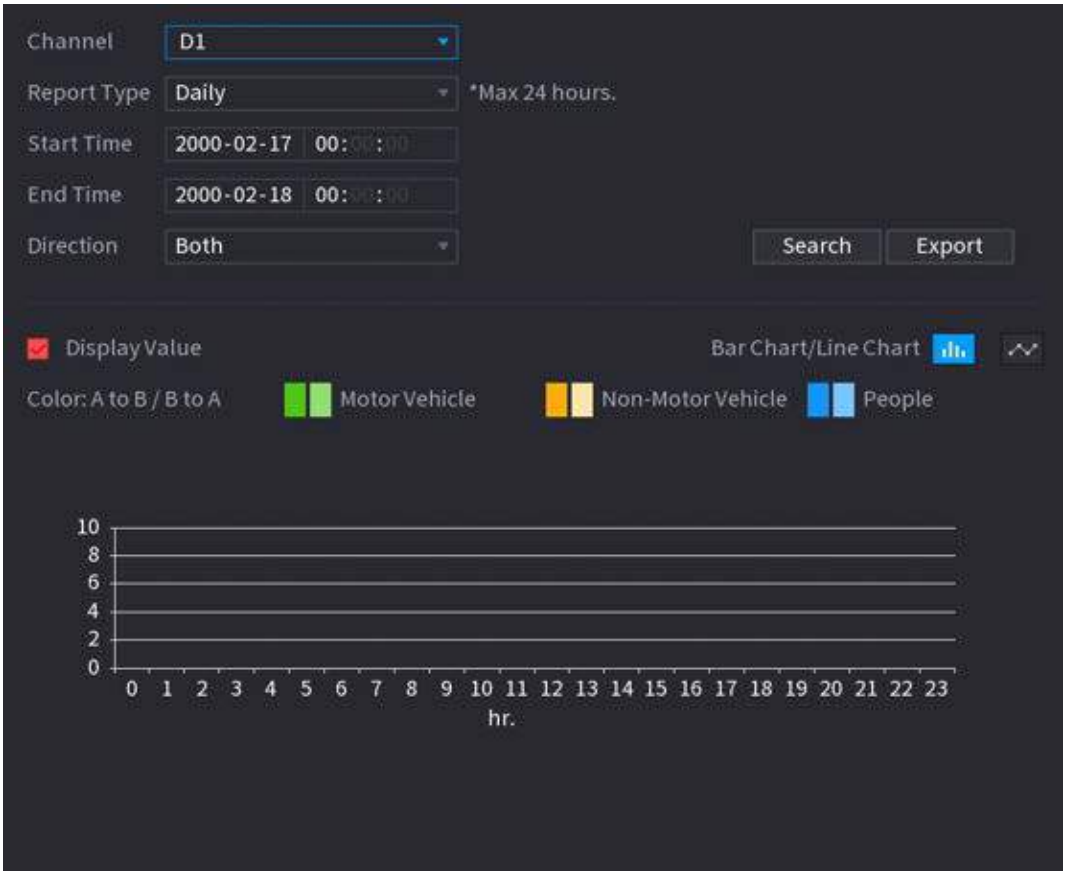
You can search for and export video metadata statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Video Metadata**.

Figure 5-143 Metadata statistics



Step 2 Select channel, report type, start time and end time, direction and then click **Search**.

Related Operations

- Switch chart type.
  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.
  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.9 ANPR

The system extracts the plate number on the surveillance video and then compare it with the specified plate information. When a match is detected, the system triggers an alarm.

5.9.9.1 Adding Vehicle Blocklist and Allowlist

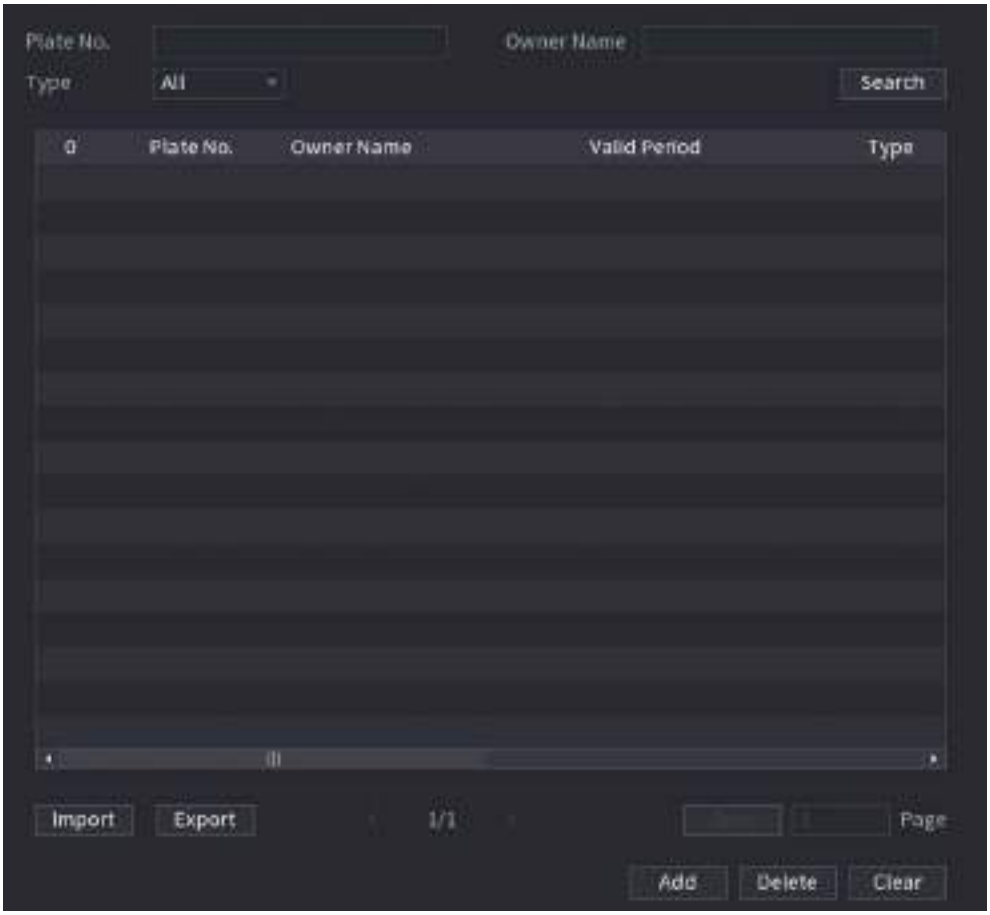
To facilitate vehicle management, you can add the plate numbers to the blocklist or allowlist. The system can compare the detected plate information with the plate on the blocklist and allowlist and then trigger the corresponding alarm linkage.

- With the blocklist and allowlist enabled, on the live page, the plate on the blocklist is displayed as red on the plate list and the plate on the allowlist is displayed as green. For the plate not on the blocklist or allowlist, the color is white.
- The added blocklist and allowlist will be synchronized to the connected ITC camera.

Procedure

Step 1 Select **Main Menu** > **AI** > **Database** > **Vehicle Blocklist/Allowlist**.

Figure 5-144 Vehicle blocklist/allowlist



Step 2 Click **Add**.

Step 3 Set plate information such as plate number, car owner name, select **Block List** or **Allow List**, and then set validity period.

Step 4 Click **OK**.

Related Operations

- Search.
  Enter keywords for **Plate No.** and **Owner Name**, select type and then click **Search**.
- Import and export plate information.
  - Import: Click **Import**, select the corresponding file, and then click **Browse** to import the file.
  - Export: Click **Export**, select the file storage path and then click **Save**.
- Delete plate information.
  - Delete one by one: Click the of the corresponding plate number.
  - Delete in batches: Select the plate numbers and then click **Delete**.

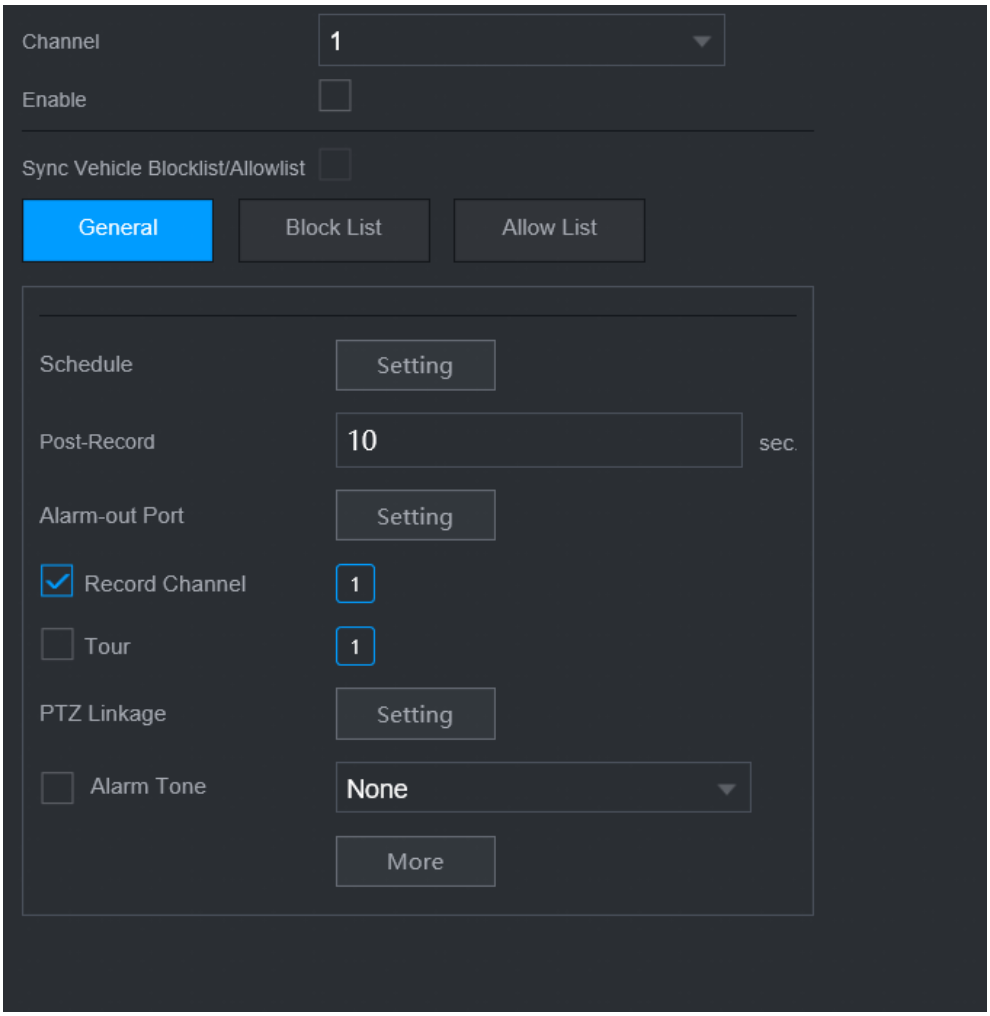
5.9.9.2 Configuring ANPR

Configure the ANPR alarm rules.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **ANPR**.

Figure 5-145 ANPR



Step 2 Select a channel and then select the **Enable** checkbox to enable ANPR.

Step 3 (Optional) Enable **Sync Vehicle Blocklist/Allowlist** to synchronize the blocklist and allowlist on the NVR to the connected camera.

Step 4 Click **General** (default), **Blocklist** or **Allowlist** tab.

Before enabling the blocklist alarm or allowlist alarm, you need to add the corresponding plate information.

- **General**: The system triggers an alarm when it detects any plate number.
- **Block List**: The system triggers an alarm when it detects plate number on the blocklist.
- **Allow List**: The system triggers an alarm when it detects plate number on the allowlist.

Step 5 Click **Setting** next to **Schedule** to configure the arming period.

The system triggers corresponding alarm actions only during the arming period.

- On the time line, drag to set the period.
- You can also click to set the period.

Step 6 Configure alarm linkage actions. For details, see Table 5-42.

Step 7 Click **Apply**.

5.9.9.3 AI Search (ANPR)

You can search for the ANPR detection results. For details, see "5.9.8.3.2 Motor Vehicle Detection".

5.9.10 Crowd Distribution

The system detects the crowd distribution. When the crowd density exceeds the defined threshold, an alarm is triggered.

5.9.10.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.10.2 Configuring Crowd Distribution

Configure the alarm rules of crowd distribution detection.

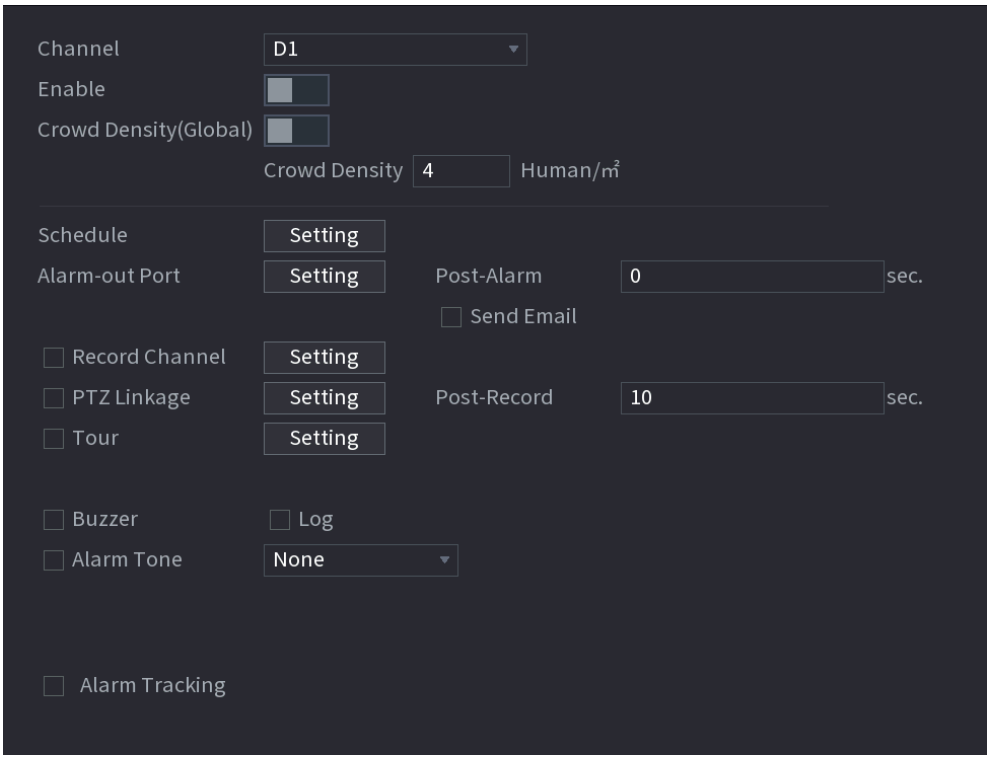
Prerequisites

Make sure that the connected camera supports the crowd distribution function.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Crowd Distribution**.

Figure 5-146 Crowd distribution



Step 2 Select a channel and then click  next to **Enable**.

Step 3 Configure parameters.

Table 5-40 Crowd distribution parameters

Parameter	Description
Crowd Density (Global)	Click and then configure the density threshold.
Crowd Density	
Alarm Tracking	After an alarm occurs, the system tracks the target automatically.

Step 4 Click **Setting** next to **Schedule** to configure the arming period.

The system triggers corresponding alarm actions only during the arming period.

- On the time line, drag to set the period.
- You can also click to set the period.

Step 5 Configure alarm linkage actions. For details, see Table 5-42.

Step 6 Click **Apply**.

5.9.10.3 Report Query

You can search for and export video metadata statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Crowd Density**.

Step 2 Select the channel, report type, start time and end time, and then click **Search**.

Related Operations

- Switch chart type.
  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.
  Select the file type, and then click **Export** to export the report in picture or csv format.

5.9.11 People Counting

The system can calculate the number of entry or exit people in the detection zone. An alarm is triggered when the number has exceeded the threshold.

Make sure that the connected camera supports people counting.

5.9.11.1 Enabling Smart Plan

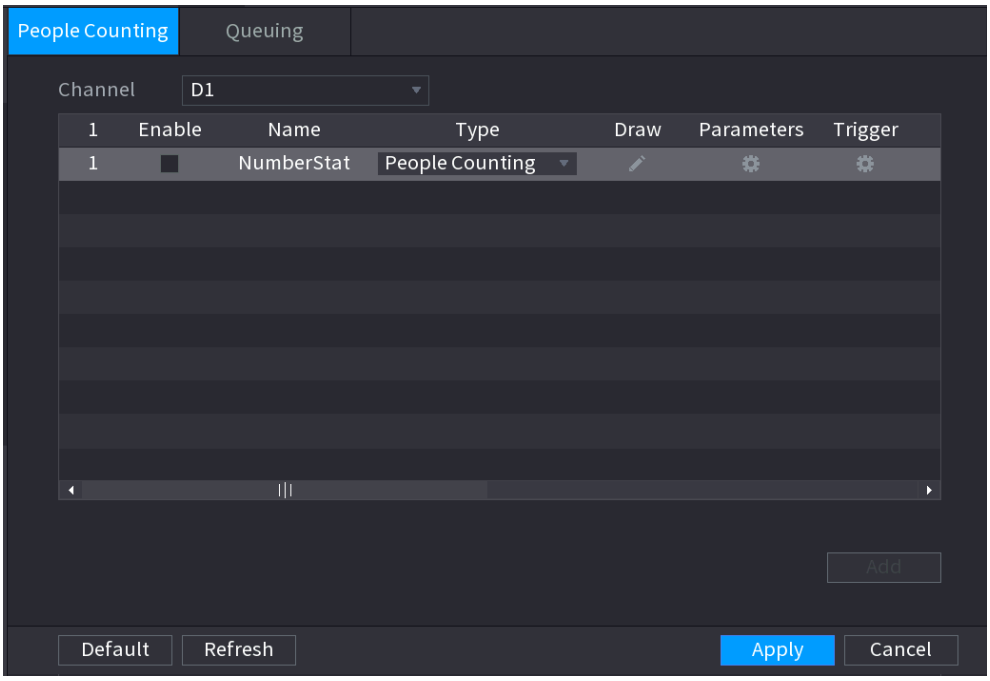
To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.11.2 Configuring People Counting

The system counts the number of people in and out of the detection area. When the number of entry, exit or staying people exceeds the threshold, an alarm is triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **People Counting** > **People Counting**.

Figure 5-147 People counting



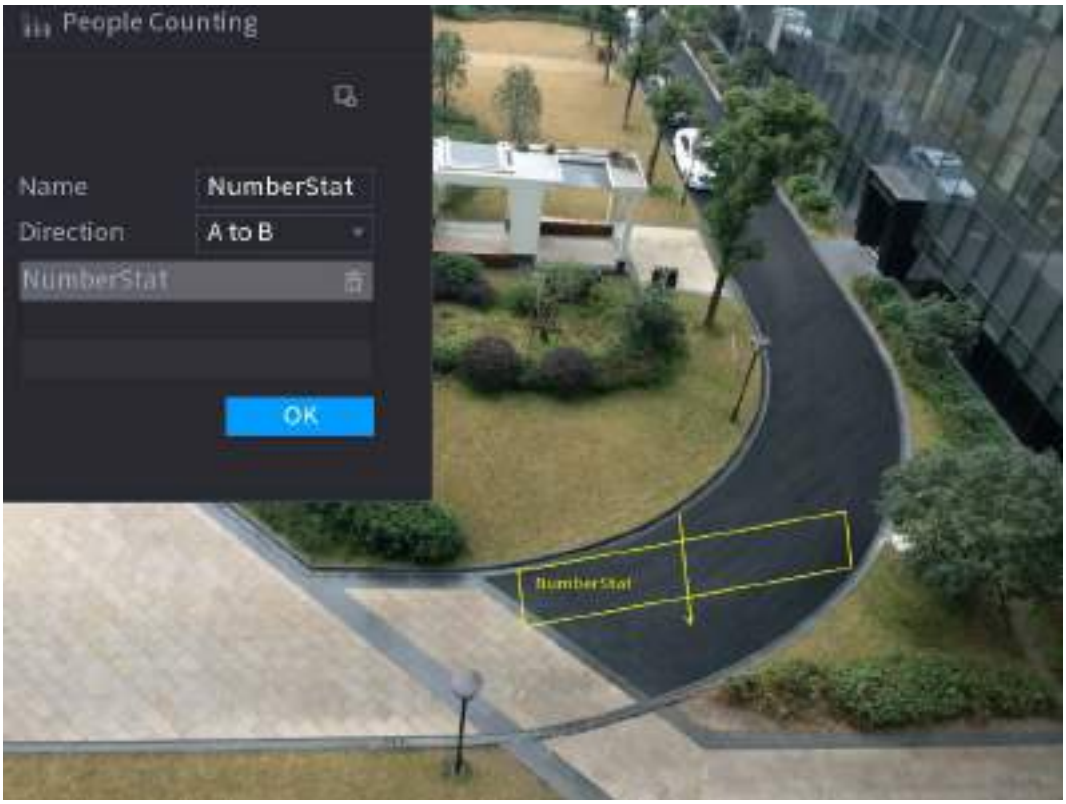
Step 2 Select a channel and then click **Add**.

Step 3 Select the **Enable** checkbox and then set **Type** to **People Counting**.

Step 4 Draw people counting rule.

1) Click to draw people counting rule. Right-click the image to stop drawing.

Figure 5-148 People counting rule



2) Customize the rule name and then select direction.
3) Click **OK**.

Step 5 Click under **Parameters** and then configure the parameters.

Table 5-41 People counting parameters

Parameter	Description
OSD	• Select **Enter No.**, and then the number of people entering the detection zone will be displayed on the live page. • Select **Exit No.**, and then the number of people leaving the detection zone will be displayed on the live page.
Setting	• **Enter No.**: An alarm is triggered when the number of people entering the detection zone exceeds the defined threshold. • **Exit No.**: An alarm is triggered when the number of people leaving the detection zone exceeds the defined threshold. • **Stay No.**: An alarm is triggered when the number of people staying the detection zone exceeds the defined threshold.

Step 6 Click under **Trigger** to configure alarm schedule and linkage. For details on alarm linkage, see Table 5-42.

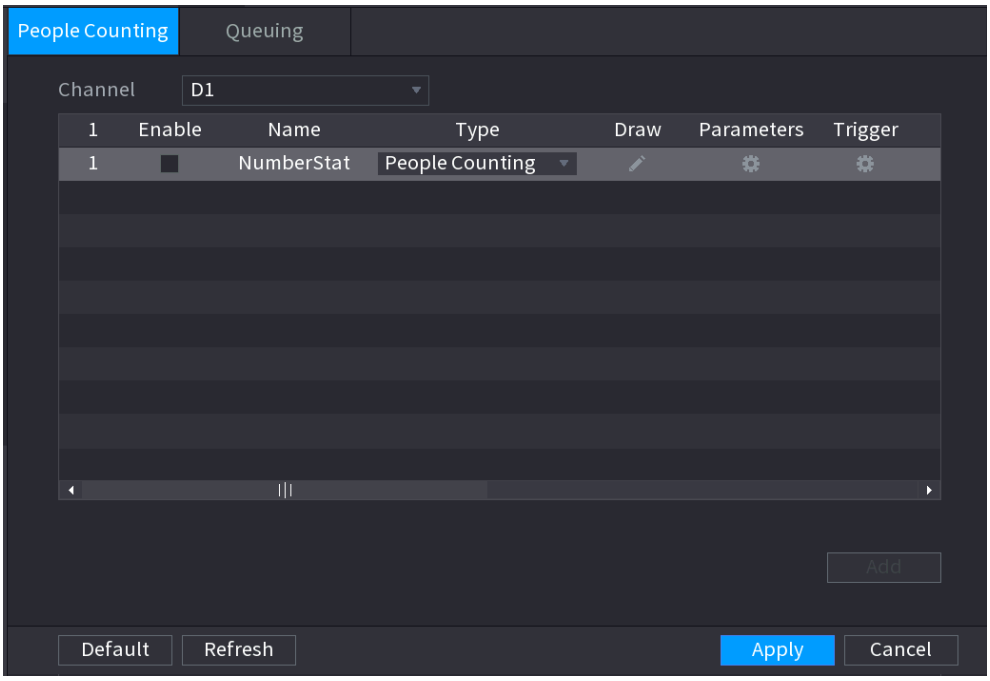
Step 7 Click **Apply**.

5.9.11.3 Configuring In Area No.

When the number of people in the detection area is larger or lower than the defined threshold, or when the staying period exceeds the defined duration, an alarm is triggered.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **People Counting** > **People Counting**.

Figure 5-149 People counting



Step 2 Select a channel and then click **Add**.

Step 3 Select the **Enable** checkbox and then set **Type** to **In Area No.**

Step 4 Draw people counting rule.

1) Click to draw a rule. Right-click the image to stop drawing.
2) Configure the parameters.
3) Click **OK**.

Step 5 Click and then enable in-area people number alarm and stay alarm.

Step 6 Click under **Trigger** to configure the alarm schedule and linkage

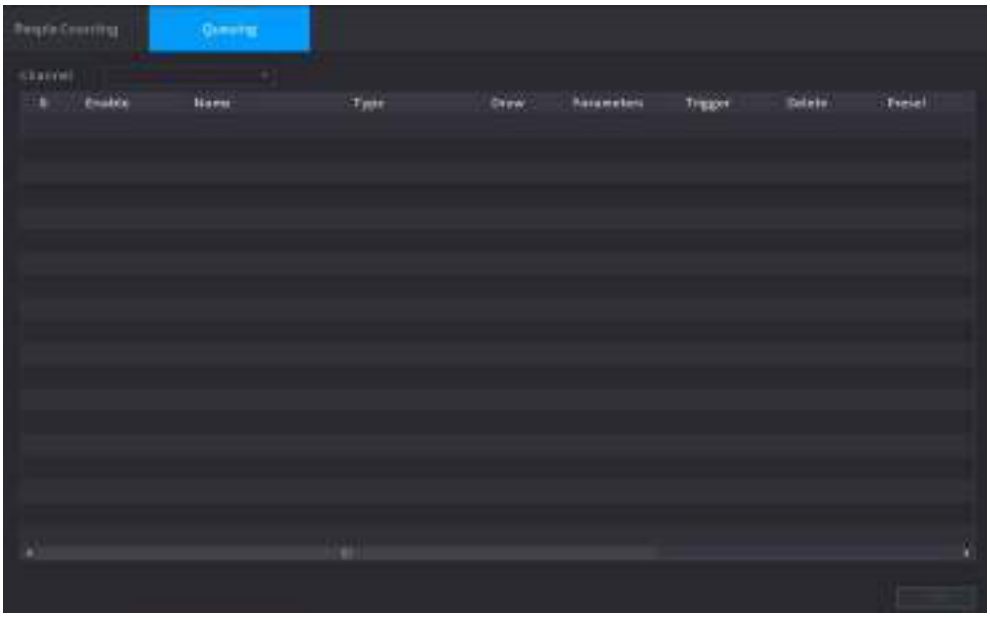
Step 7 Click **Apply**.

5.9.11.4 Queuing

After configuring queuing alarm, the system can realize the corresponding linkage actions once the number of people in the queue or the waiting time has triggered an alarm.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **People Counting** > **Queuing**.

Figure 5-150 Queuing



Step 2 Select a channel, and then click **Add**.

Step 3 Select the **Enable** checkbox.

Step 4 Click to draw queuing rule and area.

Step 5 Click under **Parameters**, and then enable **Queue People No. Alarm** or **Queue Time Alarm**.

Step 6 Click under **Trigger** to configure alarm schedule and linkage.

Step 7 Click **Apply**.

5.9.11.5 Report Query

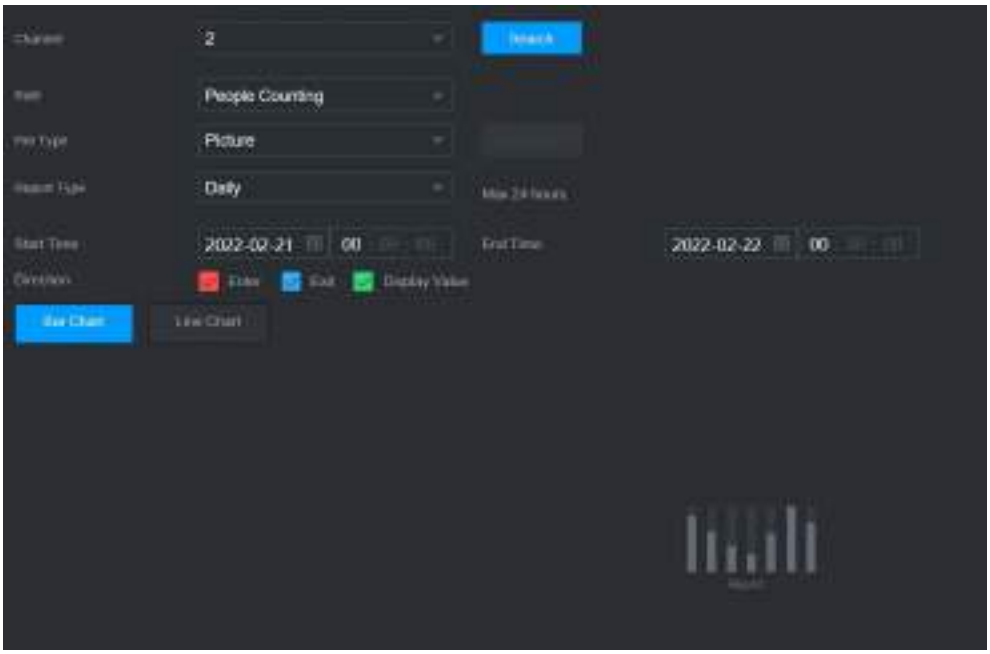
You can search for and export the people counting statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **People Counting**.

Figure 5-151 People counting



Step 2 Select channel, rule, report type, start and end time, and direction, and then click **Search**.

Related Operations

- Switch chart type.
  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.
  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.12 Heat Map

The Device can monitor the distribution of active objects in the detection zone during a period of time, and use different colors to display the objects on the heat map.

5.9.12.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.12.2 Configuring Heat map

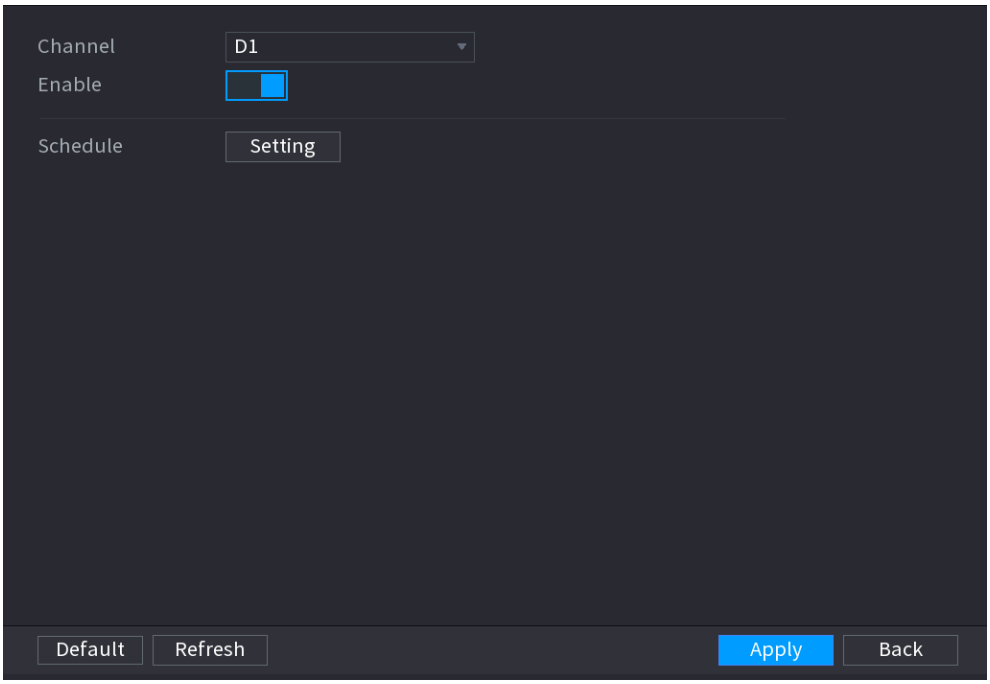
Background Information

Heat map technology can monitor the active objects distribution status on the specified zone during a period of time, and use the different colors to display on the heat map.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Heat Map**.

Figure 5-152 Heat map



Step 2 Select a channel and then click  to enable the function.

Step 3 Click **Setting** to configure the alarm schedule.

Figure 5-153 Schedule

Step 4 Click **Apply**.

5.9.12.3 Report Query

You can search for and export the heat map report of general and fisheye cameras.

5.9.12.3.1 General

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Heat Map** > **General**.

Figure 5-154 General

Step 2 Select the channel, start time, and end time.

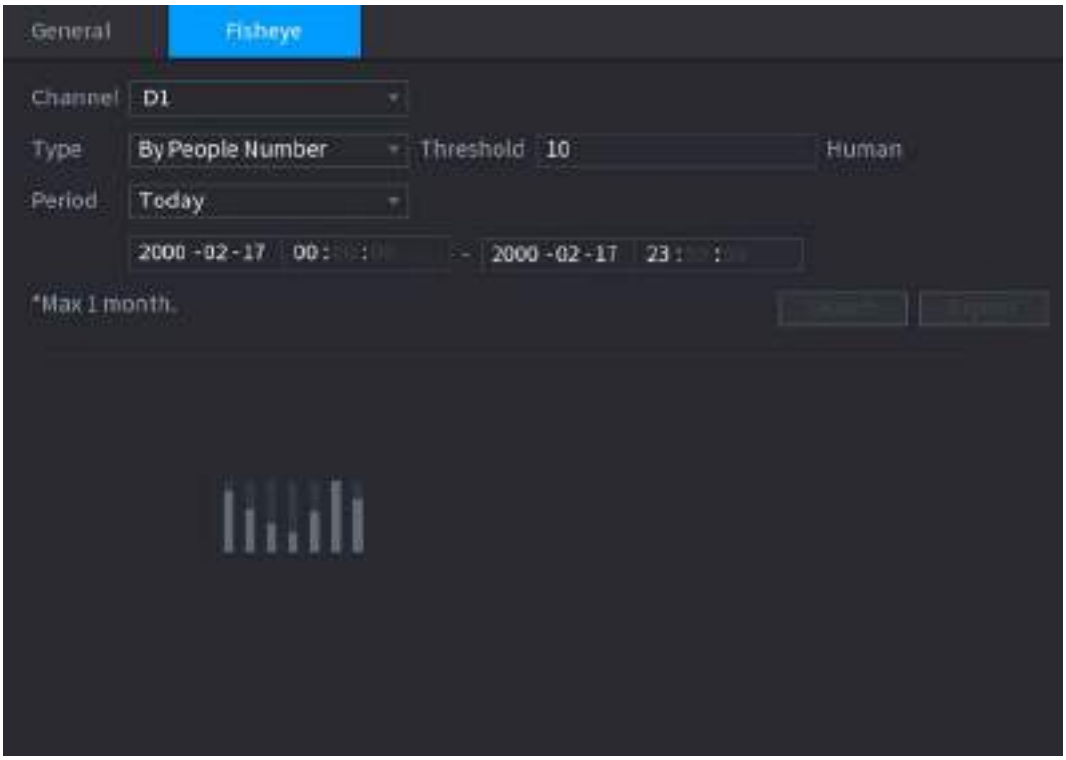
Step 3 Click **Search**.

Step 4 Click **Export** to export the heat map.

5.9.12.3.2 Fisheye

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Heat Map** > **Fisheye**.

Figure 5-155 Fisheye



Step 2 Set channel, type and period, and then click **Search**.

Step 3 Click **Export** to export the heat map.

5.9.13 SMD

You can use SMD (Smart Motion Detection) to detect humans and vehicles in the video, and store the detection results in structured storage for fast retrieval.

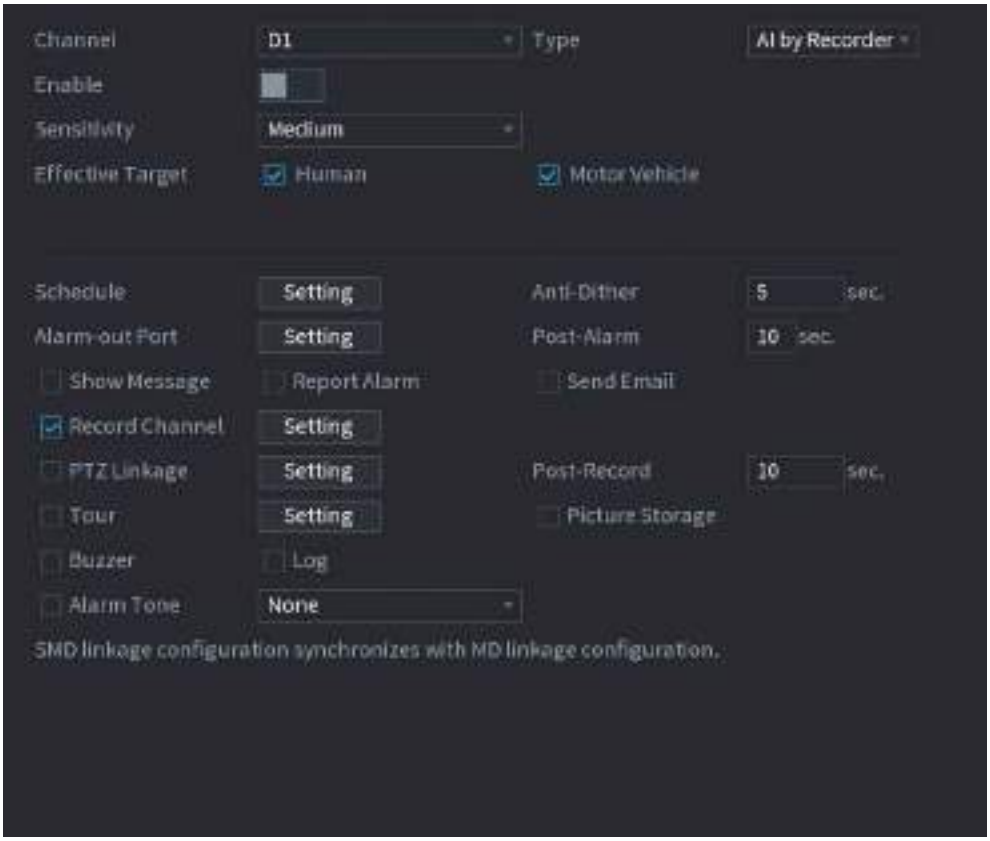
5.9.13.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.13.2 Configuring SMD

Step 1 Select **Main Menu** > **AI** > **Parameters** > **SMD**.

Figure 5-156 SMD



Step 2 Select a channel and AI type.

Step 3 Click  to enable the function.

Step 4 Configure the sensitivity.

The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur. The default value is recommended.

Step 5 Select effective target from **Human** and **Motor Vehicle**.

Step 6 Click **Setting** next to schedule to configure the alarm period.

Step 7 Configure alarm linkage.

Table 5-42 Alarm linkage parameters

Parameter	Description
Anti-Dither	The system records only one motion detection event within the defined period.
Alarm-out Port	When an alarm occurs, the NVR links the alarm output device to generate an alarm. The alarm lasts a period of time depending on the defined value for **Post-Alarm**. - Make sure that the alarm devices are connected to the alarm output port of NVR. - In **Main Menu** > **ALARM** > **Alarm-out Port**, set the mode to **Auto** so that the system can link the alarm output device to generate an alarm.
Post-Alarm	
Show Message	Enable on-screen prompt when an alarm occurs.
Report Alarm	Enable the system to report the alarm to the alarm center. Make sure that alarm center has been configured in **Main Menu** > **NETWORK** > **Alarm Center**.
Send Email	Enable the system to send an email to notify you when an alarm occurs. Make sure that the email settings have been configured in **Main Menu** > **NETWORK** > **Email**.
Record Channel	When an alarm occurs, the system activates recording of the selected channel. After the alarm ends, the recording continues for a period of time depending on the defined value for **Post-Record**. Make sure that intelligent recording schedule and auto recording have been configured. For details, see "5.8.1 Recording Schedule".
Post-Record	
PTZ Linkage	When an alarm occurs, the NVR associates the channel to perform the corresponding PTZ action. For example, rotate the PTZ to the preset point. Make sure that PTZ actions have been configured. For details, see "5.6.7 PTZ".
Tour	When an alarm occurs, the local interface of the NVR displays the image of the selected channels in turn. Make sure that the time interval and mode for tour have been configured in **Main Menu** > **DISPLAY** > **Tour Setting**.

Parameter	Description
Picture Storage	When an alarm occurs, the system takes a snapshot of the channel and stores the snapshot on the Device. Make sure that snapshot schedule and snapshot mode have been configured. For details, see "5.8.1 Recording Schedule".
Buzzer	The system activates the buzzer when an alarm occurs.
Log	When an alarm occurs, the system records the event in the logs.
Alarm Tone	When an alarm occurs, the system plays the selected audio file. Make sure that the audio files have been uploaded to the system. For details, see "5.18.1 File Management".

Step 8 Click **Apply**.

5.9.13.3 AI Search (SMD)

You can search for and play back videos that triggered SMD alarms.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **SMD**.

Step 2 Select channel, type, start time and end time, and then click **Search**.

- Click to play back the video.
- Select a video and click **Export** to export video file to a USB flash drive.

5.9.14 Vehicle Density

You can configure the rules for traffic congestion and parking upper limit, , and view the counting data on the live page.

- Traffic congestion: The system counts the vehicles in the detection area. When the counted vehicle number and the continuous congestion time exceed the configured values, an alarm is triggered and the system performs an alarm linkage.
- Parking upper limit: The system counts the vehicles in the detection area. When the counted vehicle number exceeds the configured value, an alarm triggered and the system performs an alarm linkage.

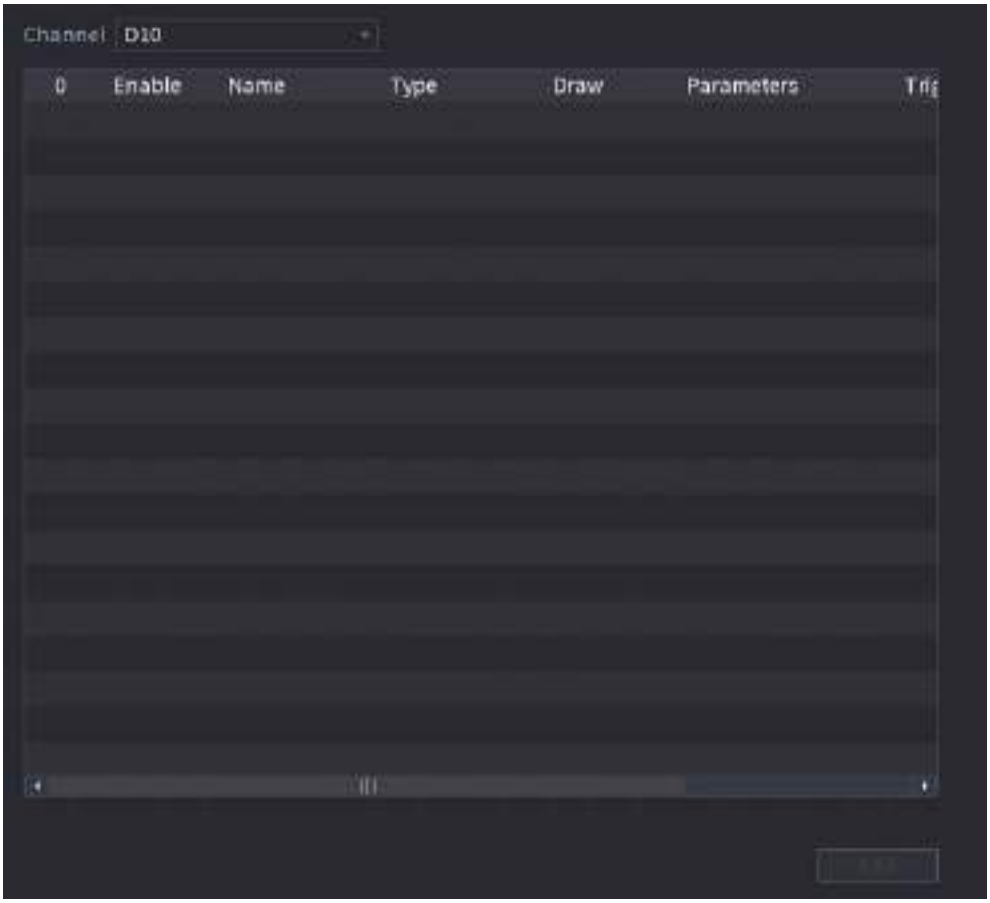
5.9.14.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

5.9.14.2 Configuring Vehicle Density

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Vehicle Density**.

Figure 5-157 Vehicle density



Step 2 Select a channel and then click **Add**.

Step 3 Select the **Enable** checkbox and then select a detection type.

Step 4 Click to draw the detection rule.

Step 5 Click under **Parameters** and then configure the parameters.

Step 6 Click under **Trigger** to configure alarm schedule and linkage.

Step 7 Click **Apply**.

5.9.14.3 Report Query

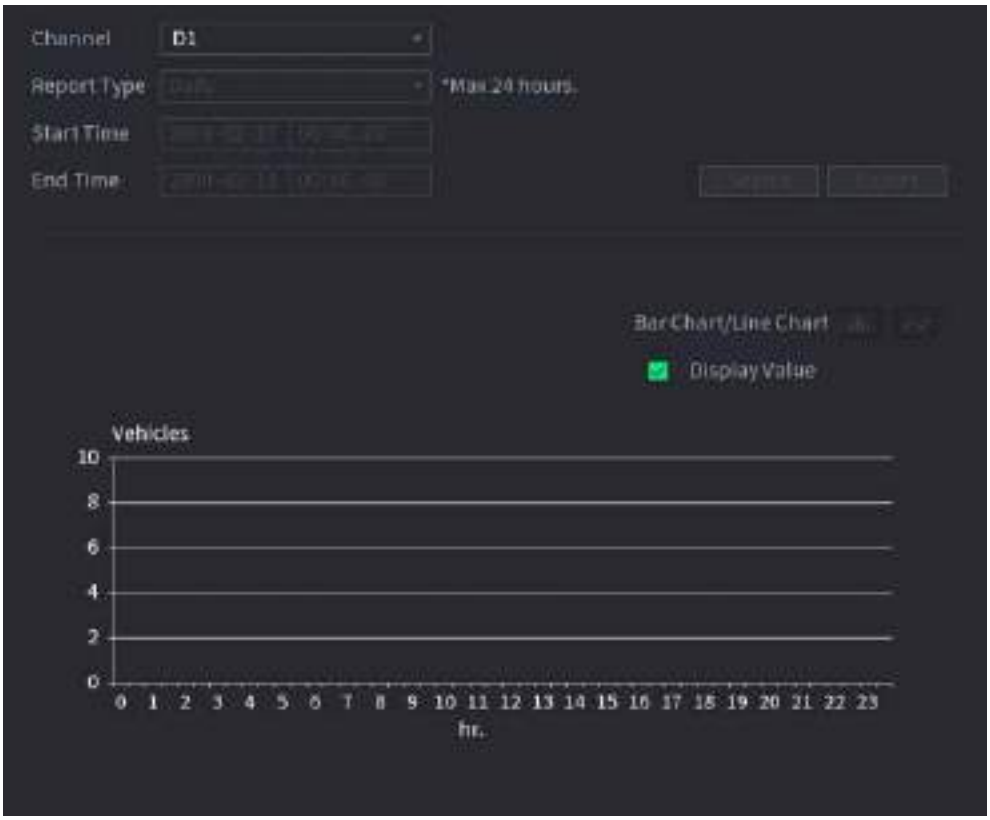
You can search for and export statistics on vehicle density.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Vehicle Density**.

Figure 5-158 Vehicle density



Step 2 Select channel, report type, start and end time, and then click **Search**.

Related Operations

- Switch chart type.
  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.
  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.15 Main-sub Tracking

Main-sub tracking refers to fisheye camera and speed dome linkage system. The fisheye camera serves as the main camera and captures panoramic videos. The speed dome serves as the sub camera and captures details of the video.

Prerequisites

- The monitoring areas of fisheye camera and speed dome are the same area.
- Fisheye camera and speed dome are added through private protocol.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Main-Sub Tracking**.

Step 2 Add monitoring area.

1) Click **Add**.
2) Configure parameters.

Table 5-43 Main-sub tracking parameters

Parameter	Description
Type	Select a type according to the number of fisheye and PTZ cameras: ● 1 Fisheye + 1 PTZ. ● 1 Fisheye + 2 PTZ. ● 1 Fisheye + 3 PTZ.
Scene Name	Customize the scene name.
Main Camera	Select a fisheye camera. 1. Click **Select** in **Main Camera** line. 2. Select a fisheye camera. 3. Click **Apply**.
Sub Camera	Select speed domes as needed. 1. Click **Select** in **Sub Camera** line. 2. Select speed domes. 3. Click **Apply**.

Step 3 Click **Apply**.

The monitoring area is successfully added.

Step 4 Configure calibration points to set the binding relationship of fisheye camera and speed dome.

Set a distant place as the first calibration point to improve accuracy.

1) Click  or double-click the target scene.
2) Click the target place on the video of fisheye camera, or move  to the target place.

   The video at upper-left corner is the fisheye camera screen, and the video at upper-right corner is the speed dome screen.
3) Adjust position through the icons below the speed dome screen to make the center of speed dome identical to the  of fisheye camera.

   The  on the speed dome screen is the center of speed dome.

Table 5-44 Icon description

Icon	Description
	Zoom in and zoom out.
	Adjust resolution.
	Adjust height.
	Electronic mouse. You can use this icon to move the mouse to control PTZ direction.
	Quick positioning key. Click this icon to select a place, and the screen will be focused and centered on the selected place.

4) Click **Add**.

   The calibration point will be displayed on the list at lower-right corner.

Step 5 Click to save the newly added calibration point.

Step 6 Repeat Step 2 to Step 5 to add more calibration points.

Set 3–8 calibration points for a speed dome.

Step 7 Click **Apply**.

5.9.16 Video Quality Analytics

When conditions such as blurry, overexposure, or the color changes appear on the screen, the system triggers the alarm.

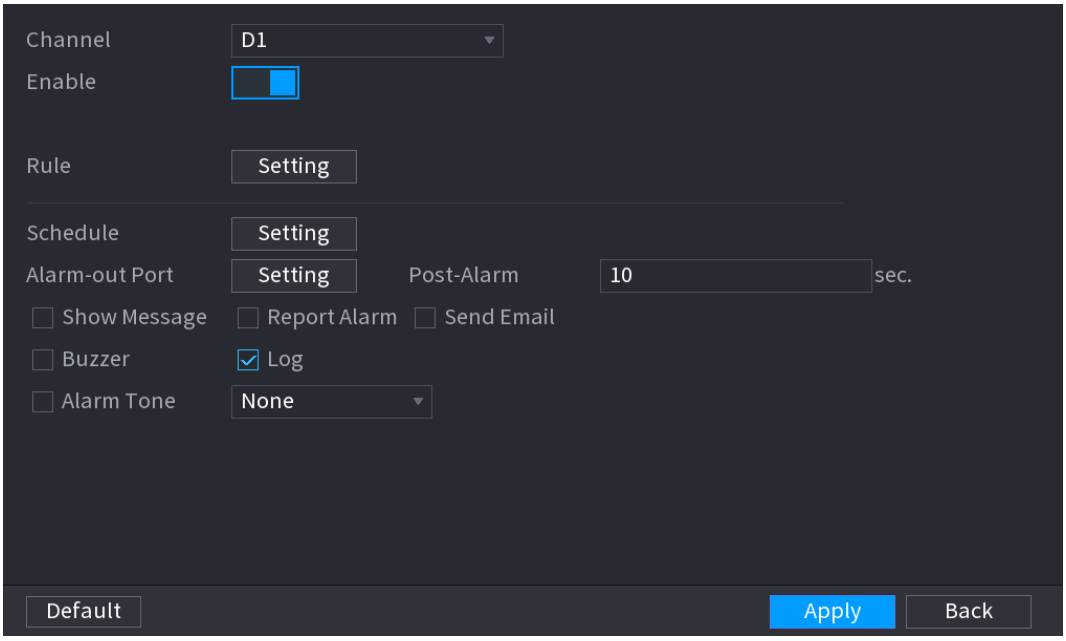
- This function takes effect only when the remote IPC supports video quality analytics.
- This function is available on select models.

5.9.16.1 Configuring Video Quality Analytics

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Video Quality Analytics**.

Step 2 Select a channel and click **Enable**.

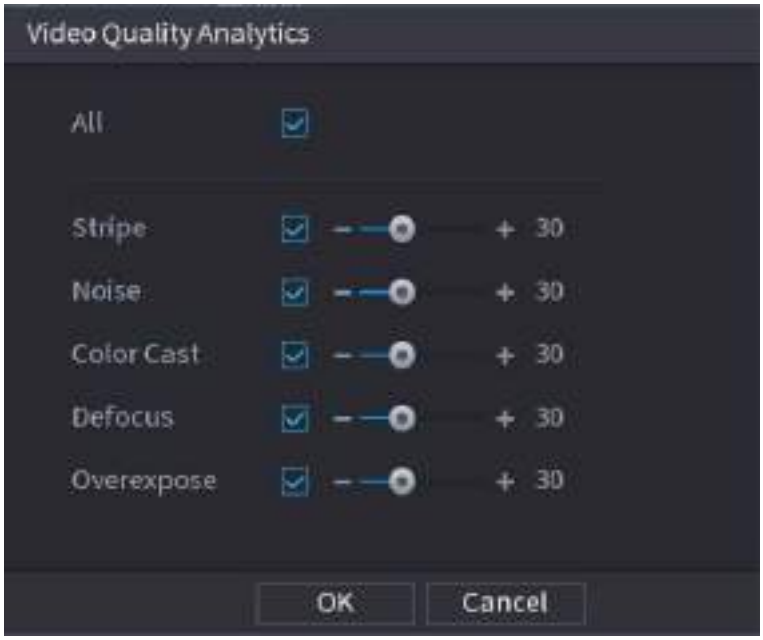
Figure 5-159 Video quality analytics



Step 3 Click **Setting** next to **Rule**.

Step 4 Select items and set thresholds as needed.

Figure 5-160 Video quality analytics settings



The value range of threshold is 0–100, and the default value is 30. When the value exceeds the set threshold, an alarm will be triggered.

Table 5-45 Video quality analytics parameters

Parameter	Description
Stripe	Stripes refer to the striped interferences in the video which might be due to device aging or signal interference. The stripe might be horizontal, vertical, or oblique.
Noise	Video noise refers to the distortion of optical system or the degradation of image quality caused by hardware equipment during transmission.
Color Cast	An image in the video is generally a colorful image that contains color information, such as RGB. When these three components appear at some unusual scale in an image, the image is biased.
Defocus	An image with high resolution contains more details, but image blur is a common problem of image quality decrease which is caused by many factors in the process of image acquisition, transmission and processing, and is defined as virtual focus in video diagnosis.
Overexpose	The brightness of the image refers to the intensity of the image pixels. Black is the darkest and white is the brightest. Black is represented by 0 and white is represented by 255. When the brightness value exceeds the threshold, the image is over exposed.

Step 5 Click **OK**.

Step 6 Click **Setting** next to **Schedule** to configure the arming period.

The system triggers corresponding alarm actions only during the arming period.

- On the time line, drag to set the period.
- You can also click  to set the period.

Step 7 Configure alarm linkage actions. For details, see Table 5-42.

Step 8 Click **Apply**.

5.9.16.2 Analytics List

Search for the results of video quality analytics.

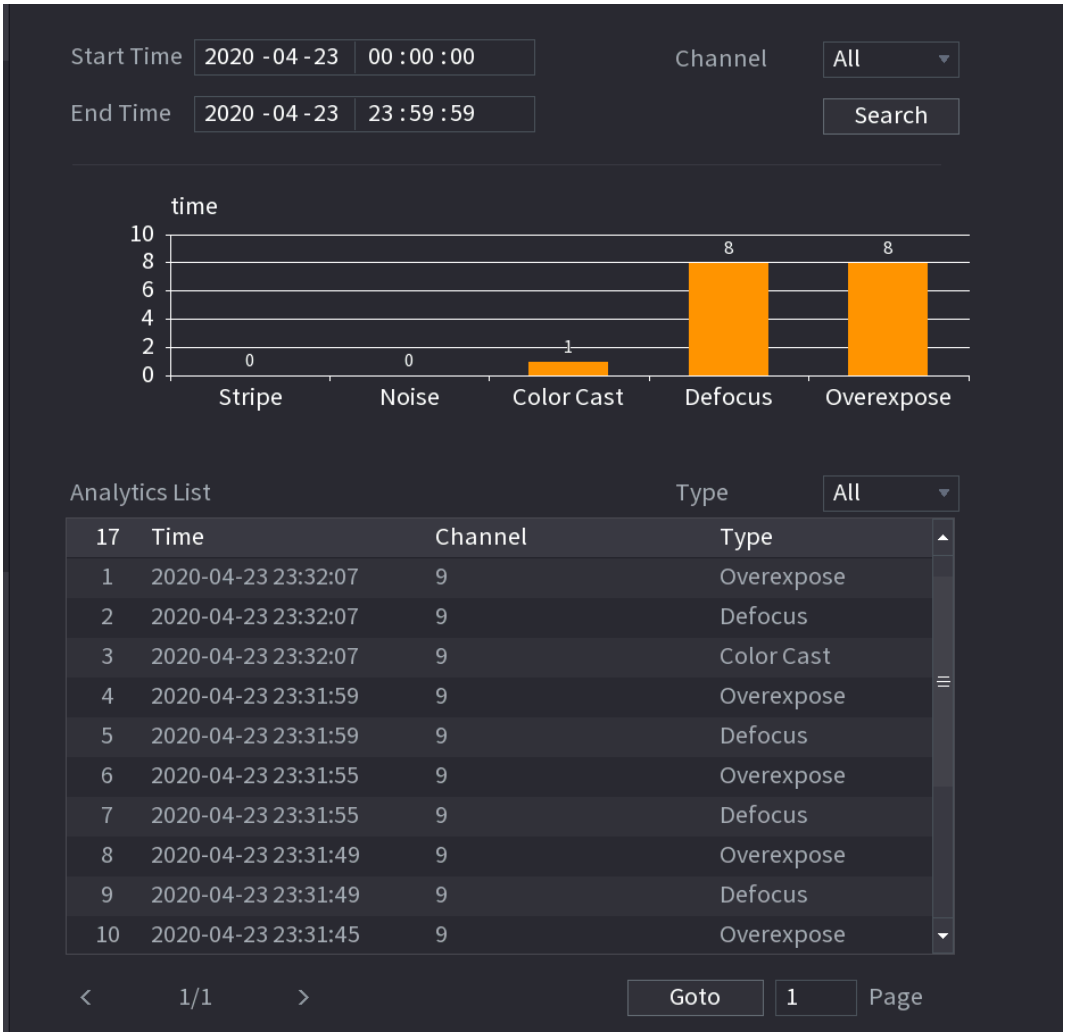
Step 1 Select **Main Menu** > **AI** > **AI Search** > **Analytics List**.

Step 2 Select the start time and end time.

Step 3 Select one or more channels.

Step 4 Click **Search**.

Figure 5-161 Analytics list



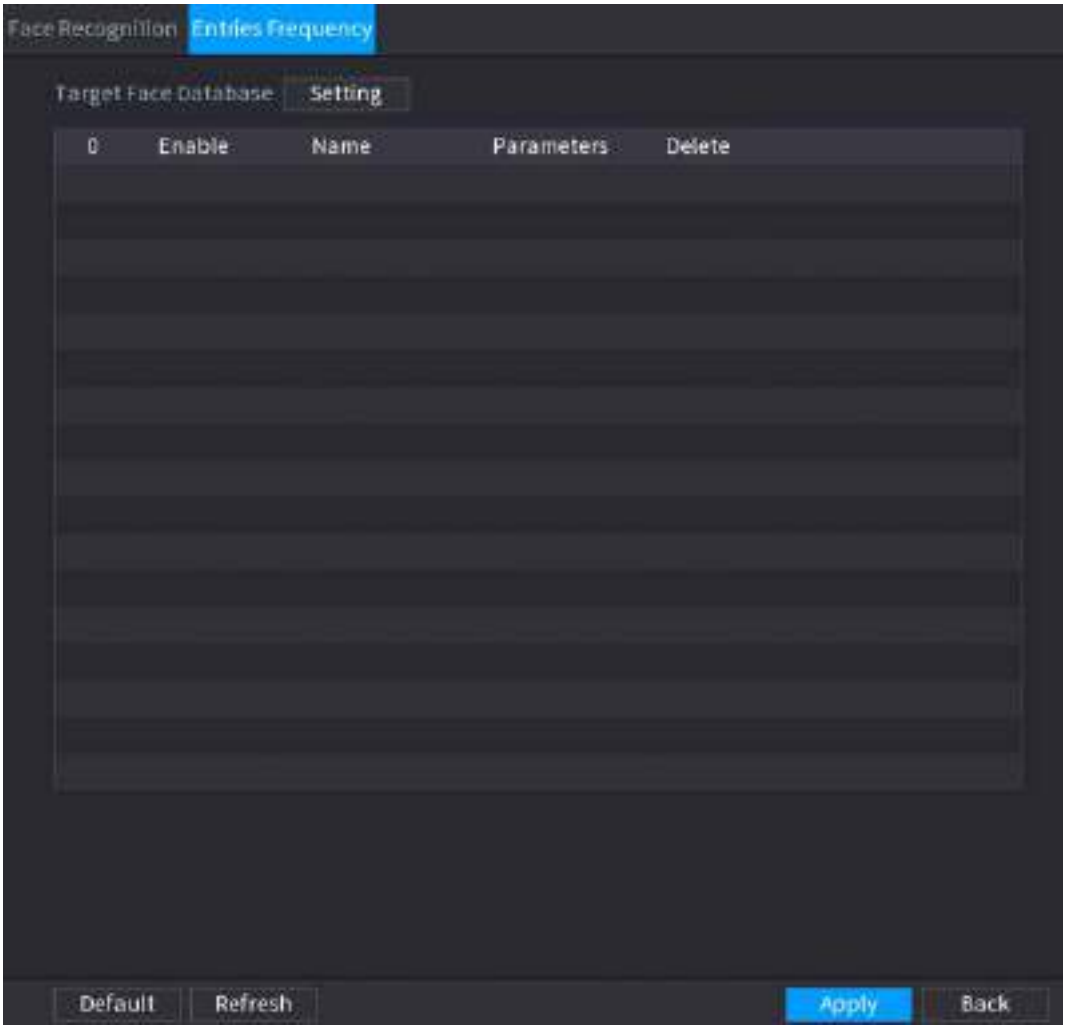
5.9.17 Entries Frequency

After setting entries frequency, when the entries detected of a person reach or exceed the threshold, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Face Recognition** > > **Entries Frequency**.

Figure 5-162 Entries frequency



Step 2 Click **Setting** to select a database and then click **OK**.

Step 3 Click  and then configure the parameters.

Figure 5-163 Configure entries frequency

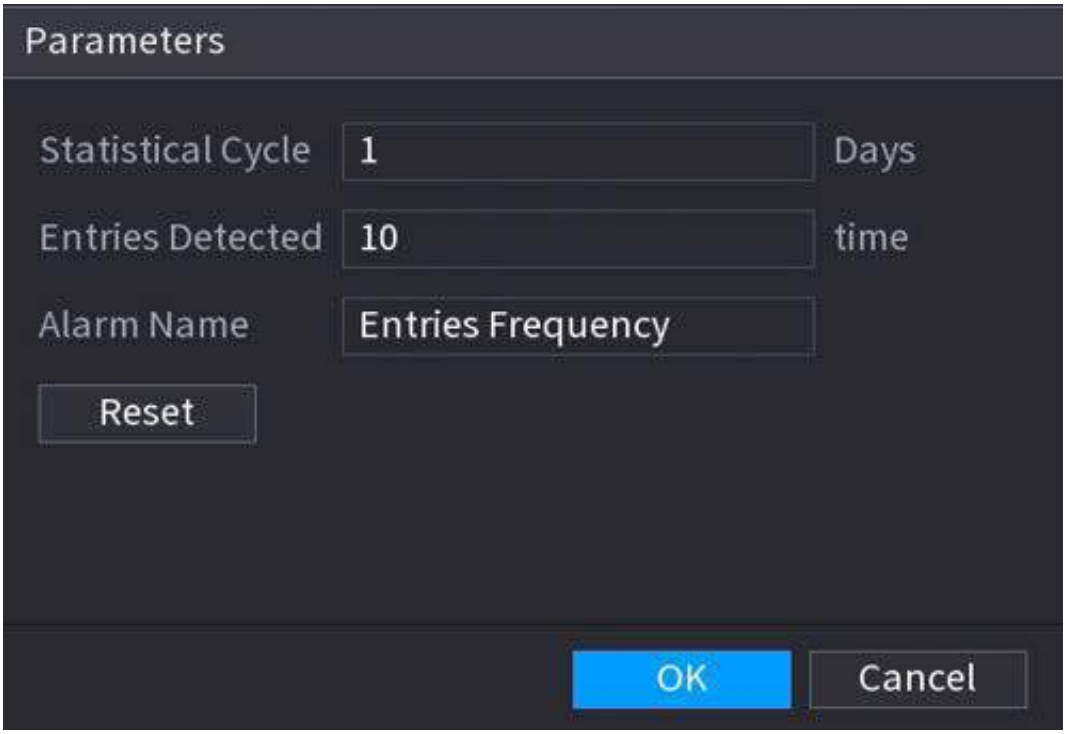


Table 5-46 Entries frequency parameters

Parameter	Description
Statistical Cycle	Set the cycle for counting the entries frequency.
Entries Detected	Set the threshold of entries frequency. When the entries detected reaches or exceeds the threshold, an alarm is triggered.
Alarm Name	The name is **Entries Frequency** by default. You can change the name.

Step 4 Click **Apply**.

5.10 Alarm Settings

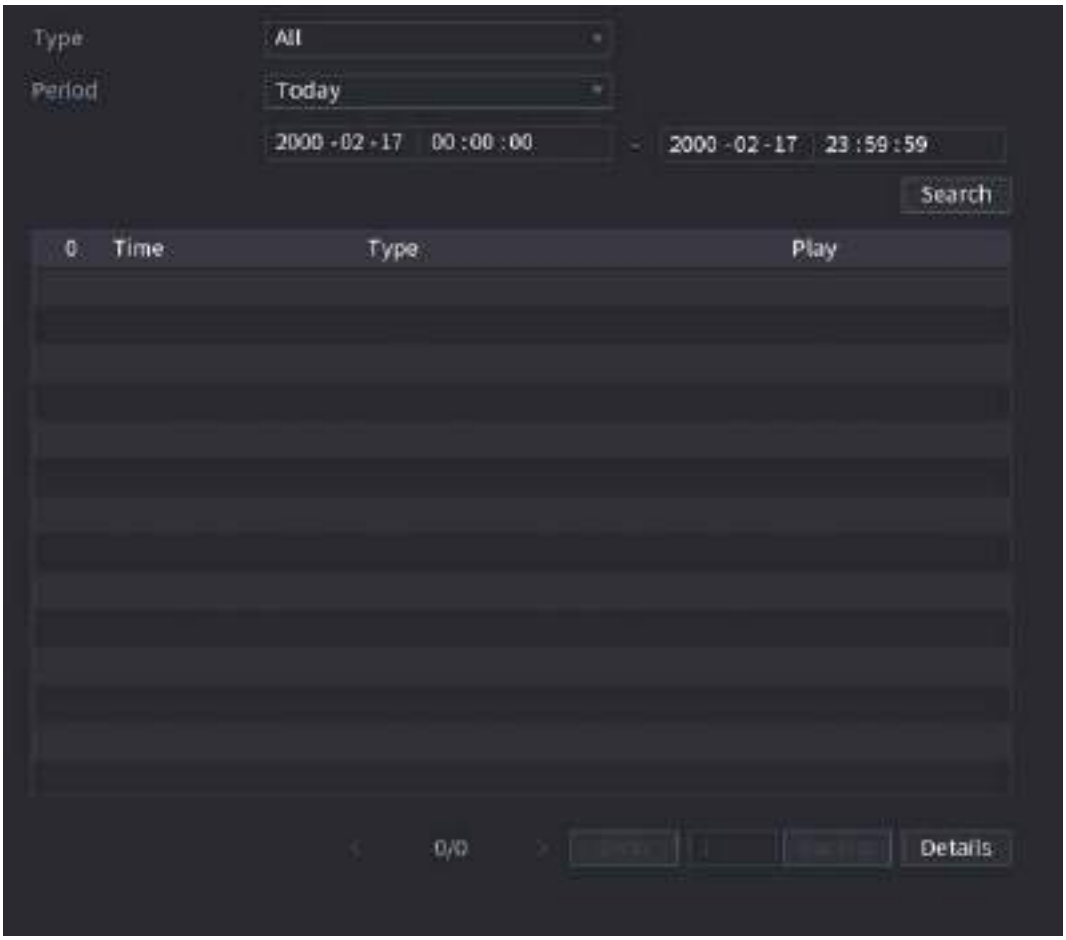
5.10.1 Alarm Information

You can search for, view and back up the alarm information.

Procedure

Step 1 Select **Main Menu** > **ALARM** > **Alarm Info**.

Figure 5-164 Alarm information



Step 2 Select the event type, and then set the search period.

Step 3 Click **Search**.

The search results are displayed.

Related Operations

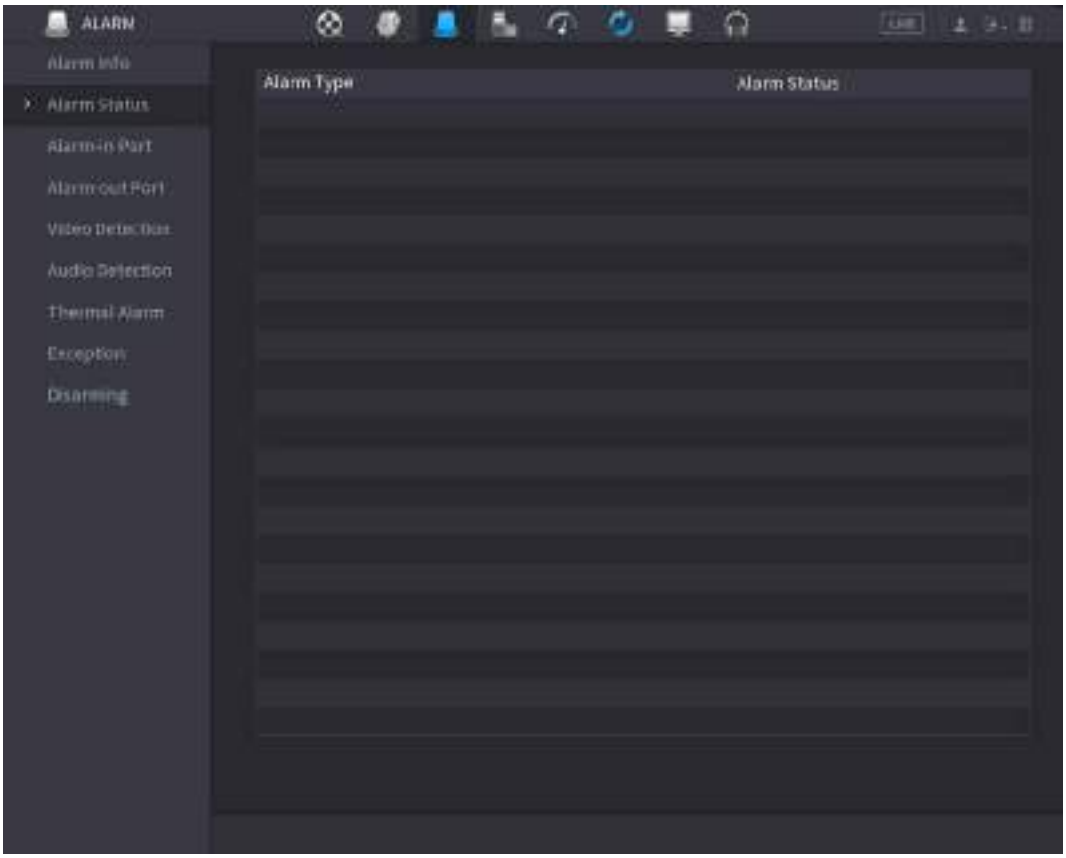
- Play back alarm videos.
  Select an alarm event log, click to play the recorded video of alarm event.
- Back up.
  Select an alarm event log and then click **Backup** to back up it to peripheral USB device.
- View alarm details.
  Double-click a log or click **Details** to view the detailed information of the event.

5.10.2 Alarm Status

You can view NVR alarm event, and remote channel alarm event.

Select **Main Menu** > **ALARM** > **Alarm Status**.

Figure 5-165 Alarm status



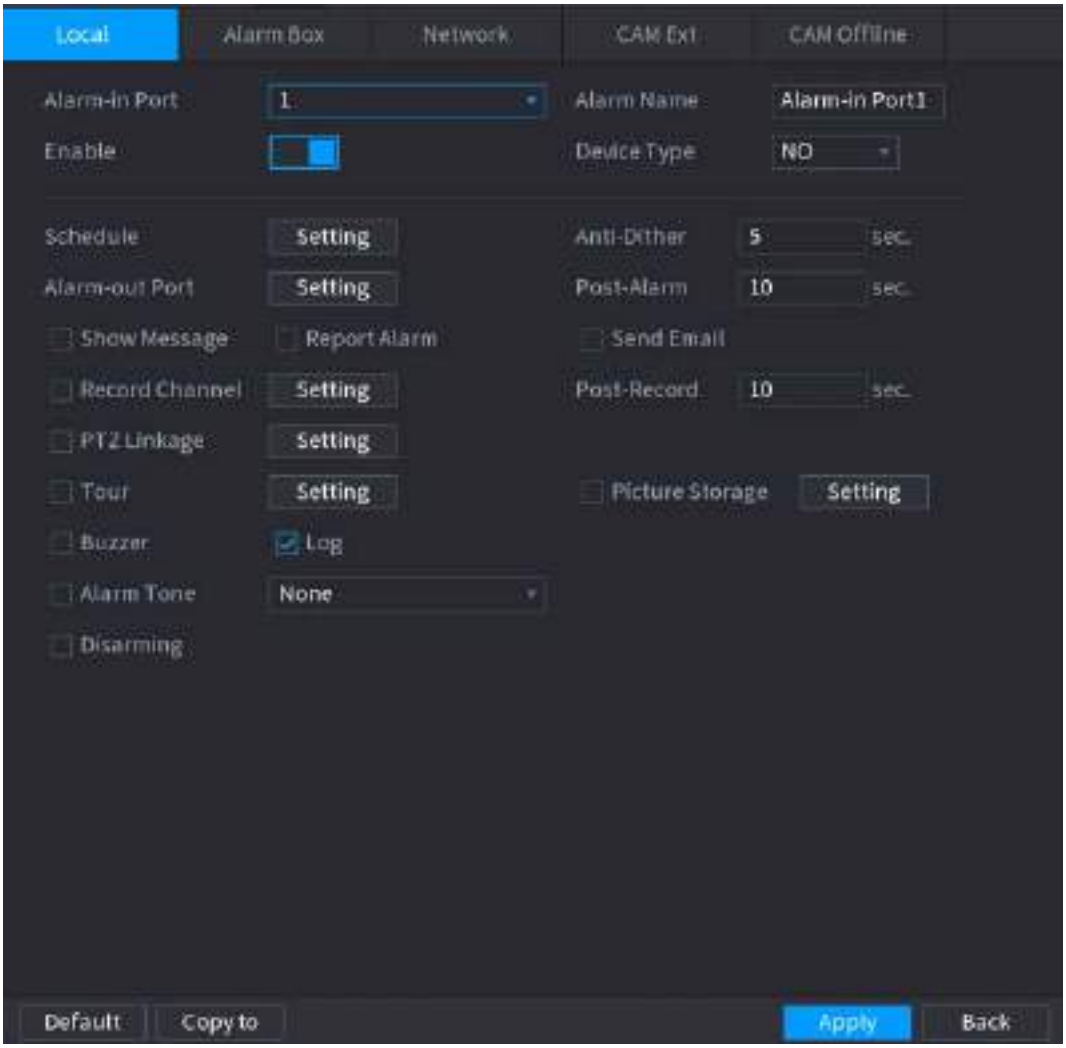
5.10.3 Alarm Input

Step 1 Select **Main menu** > **ALARM** > **Alarm-in Port**.

Step 2 Click each tab to configure alarm input settings.

- Local alarm: After connect the alarm device to the NVR alarm input port, the system performs alarm linkage actions when there is an alarm signal from the alarm input port to the NVR.
- Alarm box: You can connect the alarm box to the RS-485 port of the Device. When the alarm is detected by the alarm box, the alarm information will be uploaded to the Device, and then the Device performs alarm linkage actions.
- Network alarm: NVR performs alarm linkage actions when it receives the alarm signal via the network transmission.
- IPC external alarm: When the peripheral device connected to the camera has triggered an alarm, the camera uploads the alarm signal to the NVR via the network transmission. The system performs the corresponding alarm linkage actions.
- IPC offline alarm: When the network connection between the NVR and the network camera is off, the system performs alarm linkage actions.

Figure 5-166 Local alarm



Step 3 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 4 Configure the anti-dither period.

If multiple alarms occur during the anti-dither period, the system only record the event once.

Step 5 Configure alarm linkage. For details, see Table 5-42.

Step 6 Enable **Disarming** so that you can connect a switch to the alarm input port for disarming control.

Step 7 Click **Apply**.

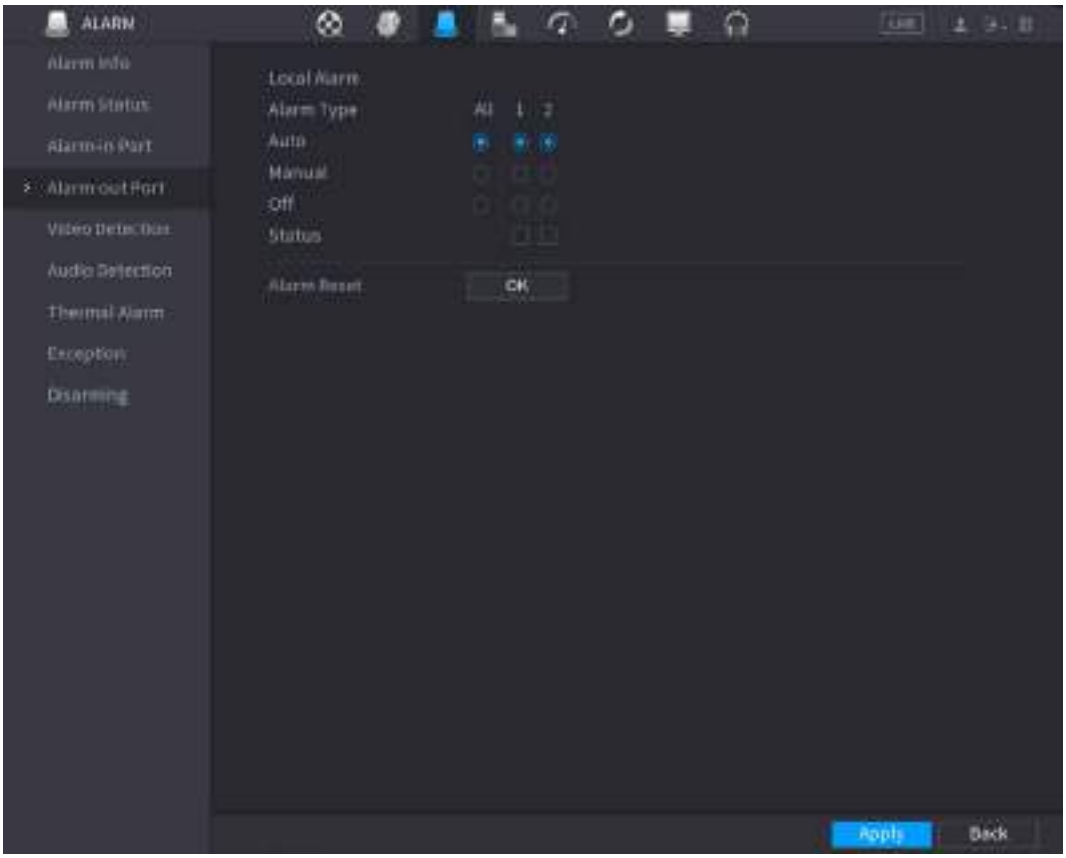
5.10.4 Alarm Output

You can set proper alarm output mode to auto, manual or off. After you connect the alarm device to the alarm output port of NVR, and set the mode to auto, the system performs alarm linkage actions when an alarm occurs.

- Auto: Once an alarm event occurs, the system generates an alarm.
- Manual: Alarm device is always on the alarming mode.
- Off: Disable alarm output function.

Step 1 Select **Main Menu** > **ALARM** > **Alarm-out Port**.

Figure 5-167 Alarm-out port



Step 2 Select the alarm mode of the alarm output channel.

Step 3 Click **Apply**.

- Click **OK** next to **Alarm Reset** to clear all alarm output statuses.
- View the alarm output status on the **Status** column.

5.10.5 Video Detection

The system can analyze the video and check whether there is considerable change or not. Once video has changed considerably (for example, there is any moving object, video is distorted), the system performs alarm linkage actions.

5.10.5.1 Motion Detection

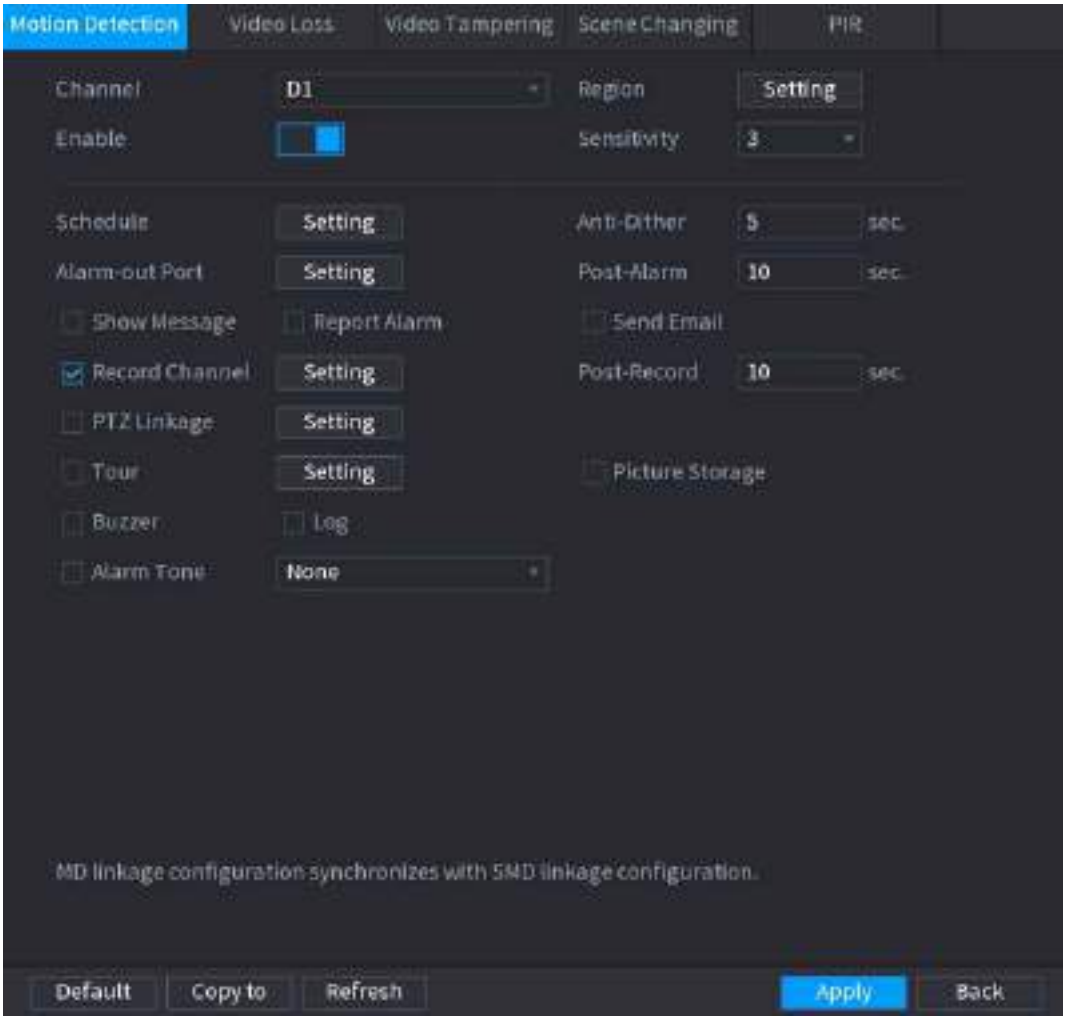
Background Information

When the moving object appears and moves fast enough to reach the preset sensitivity value, the system performs alarm linkage actions.

Procedure

Step 1 Select **Main Menu** > **ALARM** > **Video Detection** > **Motion Detection**.

Figure 5-168 Motion detection



Step 2 Select a channel and then click  to enable the function.

Step 3 Configure the detection region.

1) Click **Setting** next to **Region**.
2) Point to the middle top of the page.
3) Select one region, for example, click  .
4) Drag on the screen to select the region that you want to detect.
5) Configure the parameters.

Table 5-47 Detection region parameters

Parameter	Description
Name	Enter a name for the region.
Sensitivity	Every region has an individual sensitivity value. The bigger the value is, the easier to trigger an alarm.
Threshold	Adjust the threshold for motion detection. Every region of every channel has an individual threshold.

You can configurer up to four detection regions. When any one of the four regions activates motion detection alarm, the channel where this region belongs to will activate motion detection alarm.

6) Right-click the page to exit.

Step 4 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 5 Configure the anti-dither period.

If multiple alarms occur during the anti-dither period, the system only record the event once.

Step 6 Configure alarm linkage. For details, see Table 5-42.

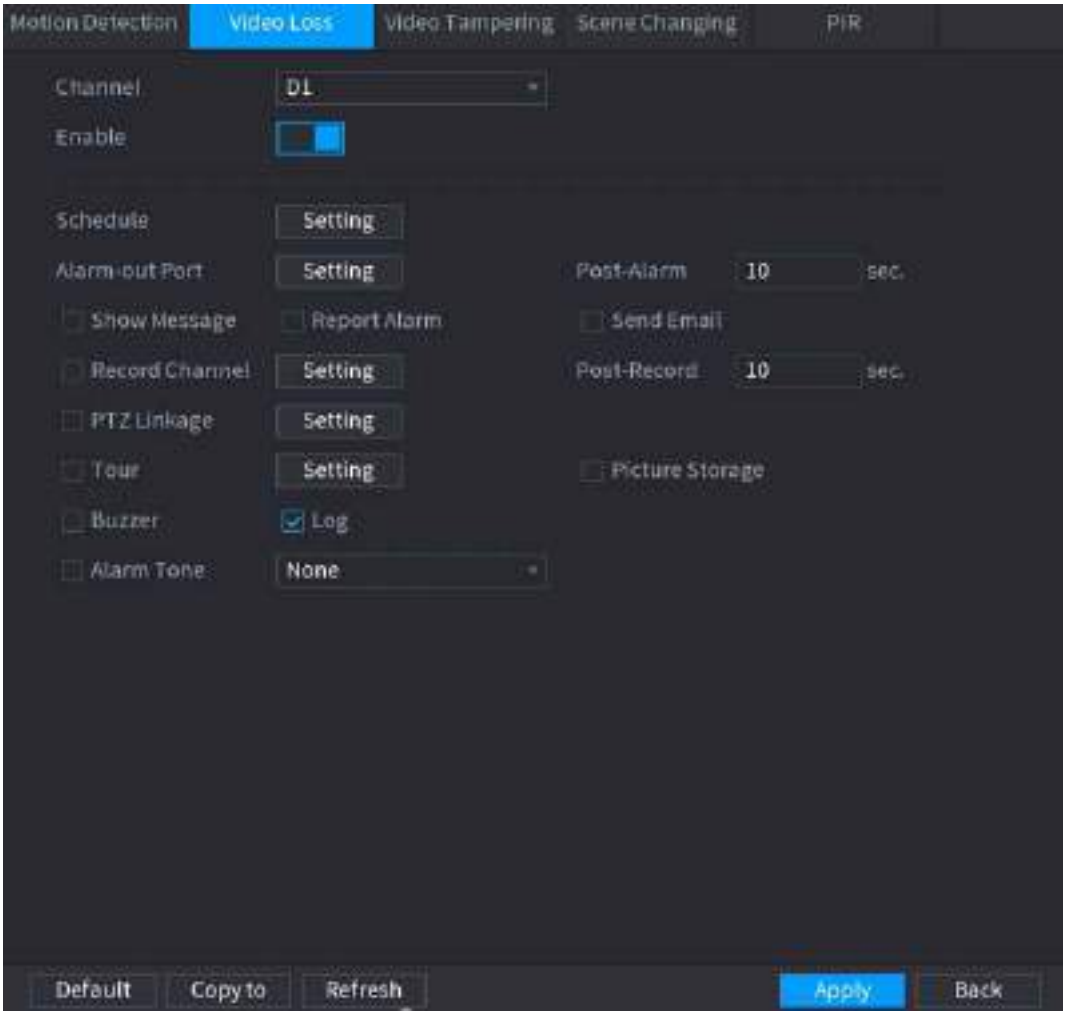
Step 7 Click **Apply**.

5.10.5.2 Video Loss

When the video loss occurs, the system performs alarm linkage actions.

Step 1 Select **Main Menu** > **ALARM** > **Video Detection** > **Video Loss**.

Figure 5-169 Video Loss



Step 2 Select a channel and then click  to enable the function.

Step 3 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 4 Configure alarm linkage. For details, see Table 5-42.

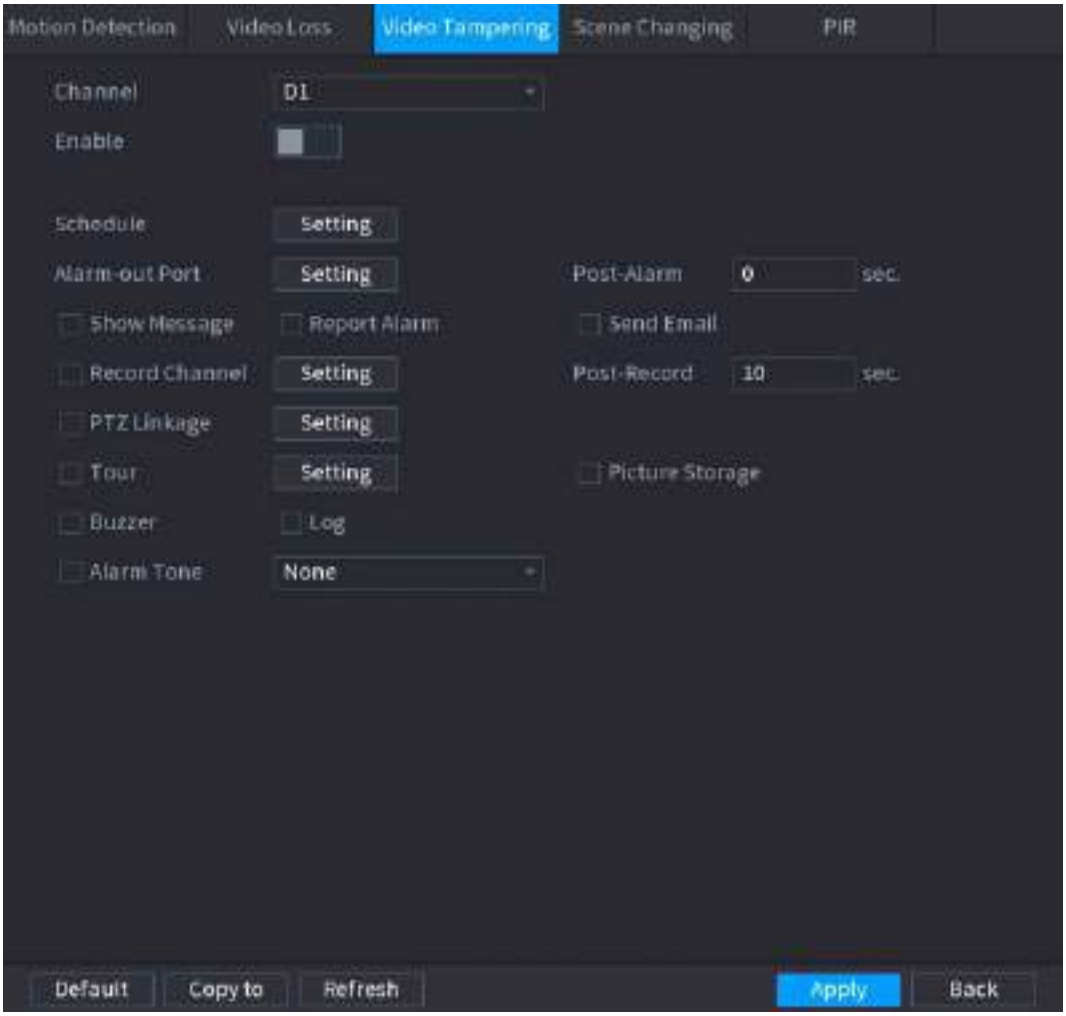
Step 5 Click **Apply**.

5.10.5.3 Video Tampering

When the camera lens is covered, or the video is displayed in a single color because of sunlight status, the monitoring cannot be continued normally. To avoid such situations, you can configure the tampering alarm settings.

Step 1 Select **Main Menu** > **ALARM** > **Video Detection** > **Video Tampering**.

Figure 5-170 Video tampering



Step 2 Select a channel and then click  to enable the function.

Step 3 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 4 Configure alarm linkage. For details, see Table 5-42.

Step 5 Click **Apply**.

5.10.5.4 Scene Change

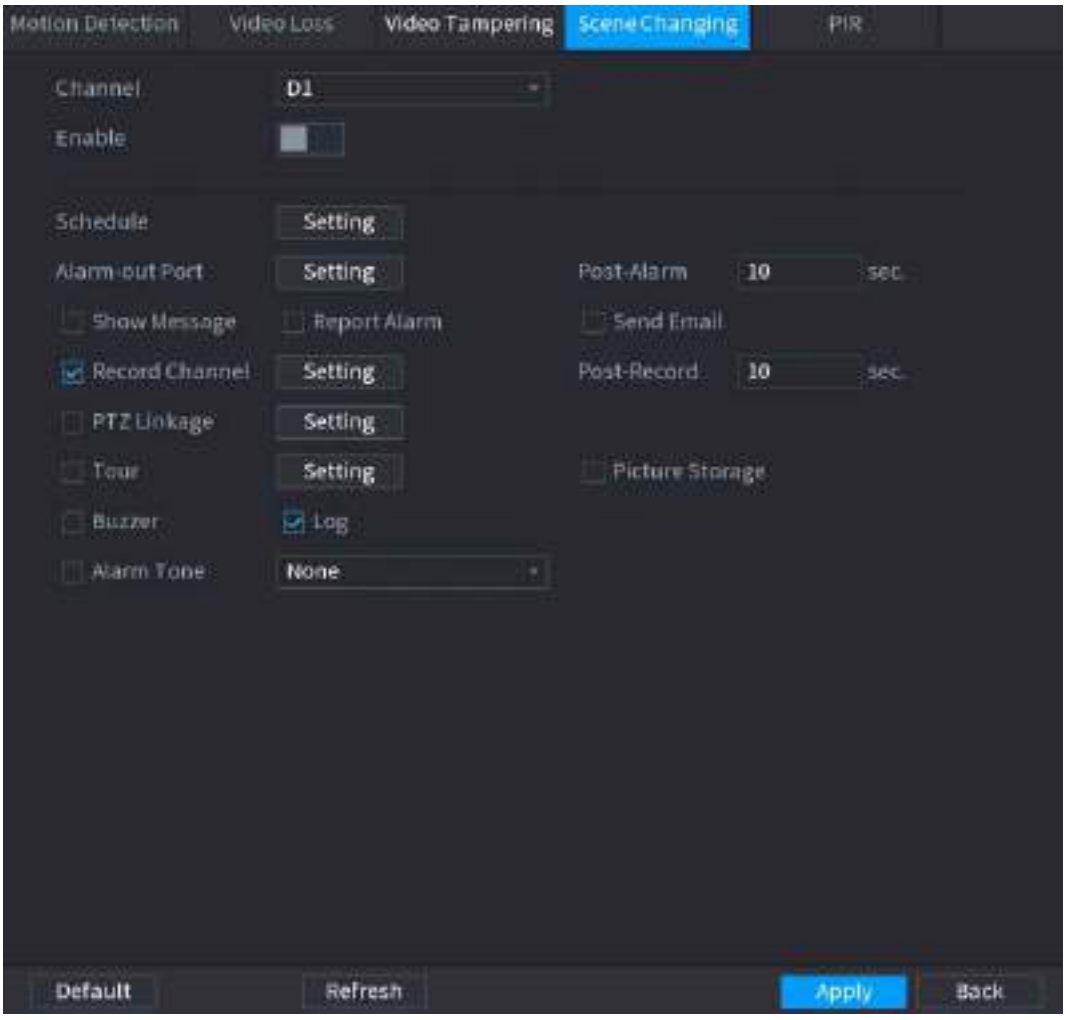
Background Information

When the detected scene has changed, system performs alarm linkage actions.

Procedure

Step 1 Select **Main Menu** > **ALARM** > **Video Detection** > **Scene Changing**.

Figure 5-171 Scene changing



Step 2 Select a channel and then click  to enable the function.

Step 3 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 4 Configure alarm linkage. For details, see Table 5-42.

Step 5 Click **Apply**.

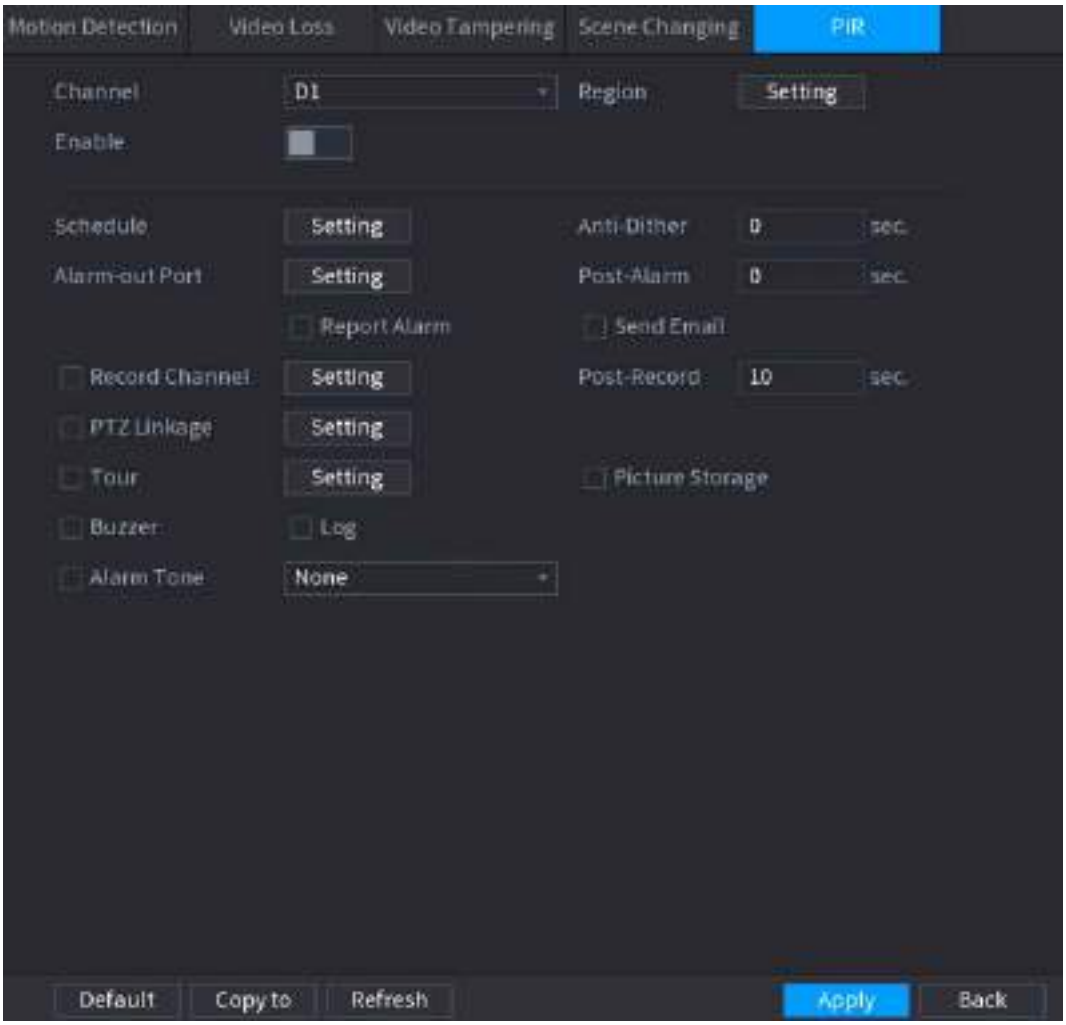
5.10.5.5 PIR Alarm

PIR function helps enhancing the accuracy and validity of motion detect. It can filter the meaningless alarms that are activated by the objects such as falling leaves and flies. The detection range by PIR is smaller than the field angle.

PIR function is enabled by default if it is supported by the cameras. Enabling PIR function will get the motion detection to be enabled automatically to generate motion detection alarms.

Step 1 Select **Main Menu** > **ALARM** > **Video Detection** > **PIR**.

Figure 5-172 PIR



Step 2 Select a channel and then click  to enable the function.

Step 3 Configure the detection region.

1) Click **Setting** next to **Region**.
2) Point to the middle top of the page.
3) Select one region, for example, click  .
4) Drag on the screen to select the region that you want to detect.
5) Configure the parameters.

Table 5-48 Detection region parameters

Parameter	Description
Name	Enter a name for the region.
Sensitivity	Every region of every channel has an individual sensitivity value. The bigger the value is, the easier to trigger an alarm.
Threshold	Adjust the threshold for motion detection. Every region of every channel has an individual threshold.

You can configure up to four detection regions. When any one of the four regions activates an alarm, the channel where this region belongs to will activate an alarm.

6) Right-click to exit the page.

Step 4 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 5 Configure the anti-dither period.

If multiple alarms occur during the anti-dither period, the system only record the event once.

Step 6 Configure alarm linkage. For details, see Table 5-42.

Step 7 Click **Apply**.

5.10.6 Audio Detection

Background Information

The system can generate an alarm once it detects the audio is not clear, the tone color has changed or there is abnormal or audio volume change.

Procedure

Step 1 Select **Main Menu** > **ALARM** > **Audio Detection**.

Step 2 Select a channel and then click  to enable detection of audio exception and intensity change.

- **Audio Exception**: The system generates an alarm when the audio input is abnormal.
- **Intensity Change**: Set the sensitivity and threshold. An alarm is triggered when the change in sound intensity exceeds the defined threshold.

Step 3 Click **Setting** next to **Schedule** to configure the alarm schedule.

Step 4 Configure alarm linkage. For details, see Table 5-42.

Step 5 Click **Apply**.

5.10.7 Thermal Alarm

After receiving the alarm signal from the connected thermal devices, the system can recognize the alarm type, and then trigger the corresponding alarm actions.

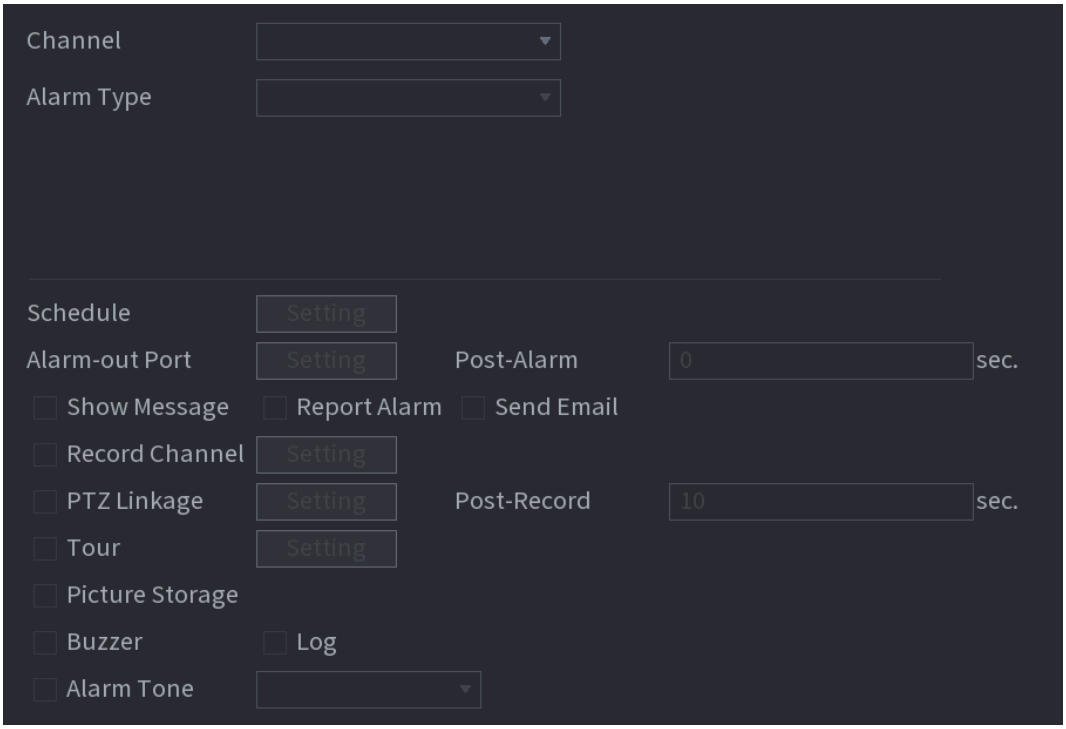
The system supports heat alarm, temperature (temperature difference) and cold/hot alarm.

- Heat alarm: The system generates an alarm once it detects there is a fire.
- Temperature (temperature difference): The system triggers an alarm once the temperature difference between two positions is higher or below the specified threshold.
- Cold/hot alarm: The system triggers an alarm once the detected position temperature is higher or below the specified threshold.

- Make sure that the connected camera supports temperature monitoring function.
- This function is available on select models.
- The thermal detection functions might vary depending on the connected camera. This section uses heat alarm as an example.

Step 1 Select **Main Menu** > **ALARM** > **Thermal Alarm**.

Figure 5-173 Thermal alarm



Step 2 Select a channel and set alarm type to heat alarm, and then enable the function.

Step 3 Select fire mode. The system supports preset mode and zone excluded mode.

- Preset mode: Select a preset and then enable the function. The system generates an alarm once it detects there is a fire.
- Zone excluded mode: The system filters the specified high temperature zone. The system generates an alarm once the rest zone has fire.

Step 4 Configure alarm linkage. For details, see Table 5-42.

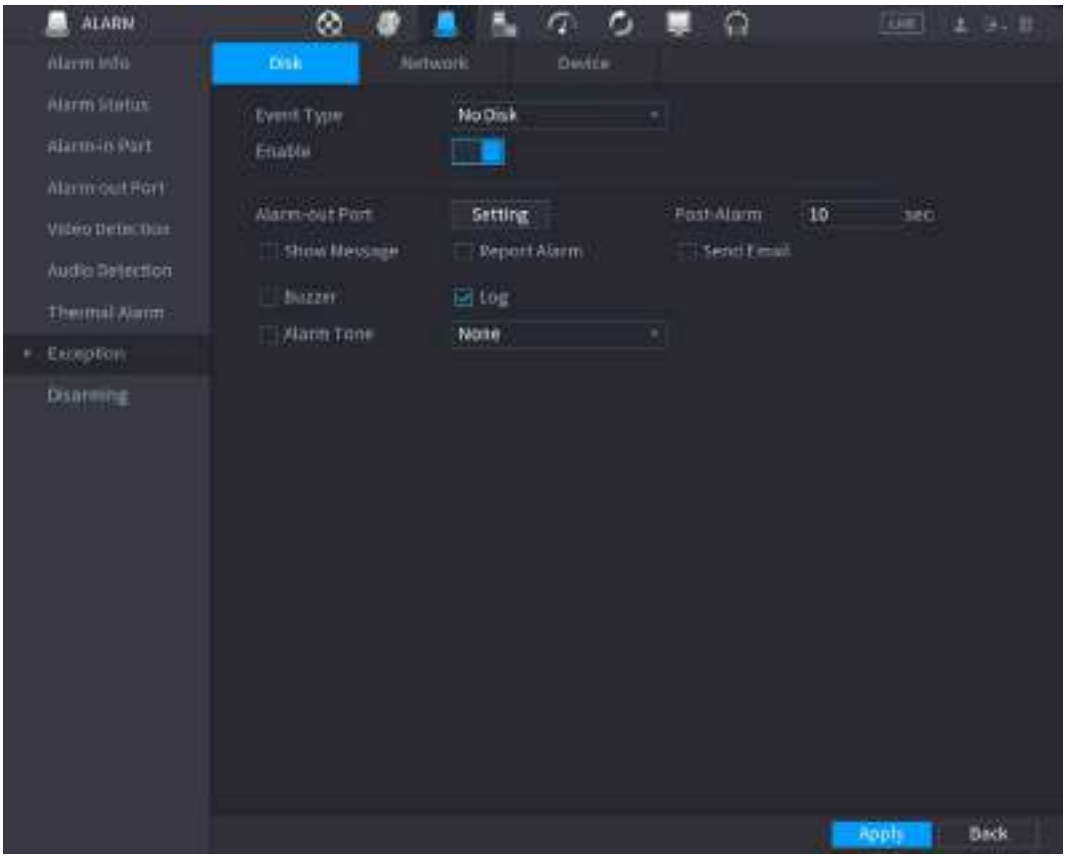
Step 5 Click **Apply**.

5.10.8 Exception

When an error in HDD, network, and device occurs, the system performs alarm linkage actions.

Step 1 Select **Main Menu** > **ALARM** > **Exception**.

Figure 5-174 Disk exception



Step 2 Click each tab and then select an event type.

- **Disk**: The system detects HDD error, no HDD, no space, and other HDD events.
- **Network**: The system detects network errors such as disconnection, IP conflict, and MAC conflict.
- **Device**: The system detects device errors such as abnormal fan speed and network security error.

Step 3 Click  to enable the function.

Step 4 (Optional) If the event type is **Low Space**, you need to configure the threshold of storage space.

When the storage space is lower than the threshold, an alarm is triggered.

Step 5 Configure alarm linkage. For details, see Table 5-42.

Step 6 Click **Apply**.

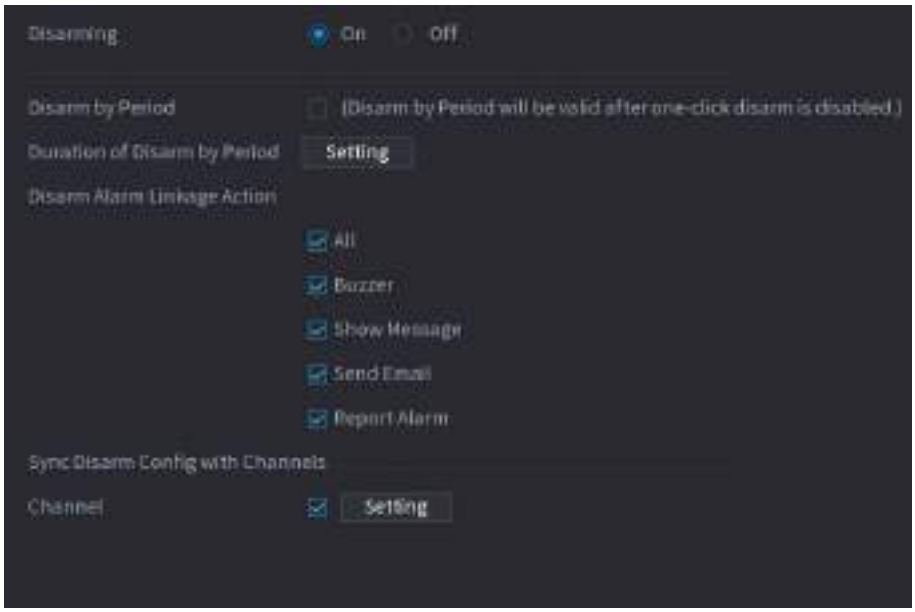
5.10.9 Disarming

You can disarm all alarm linkage actions as needed through one click.

Step 1 Select **Main Menu** > **ALARM** > **Disarming**.

Step 2 Select **On** for **Disarming** to enable disarming.

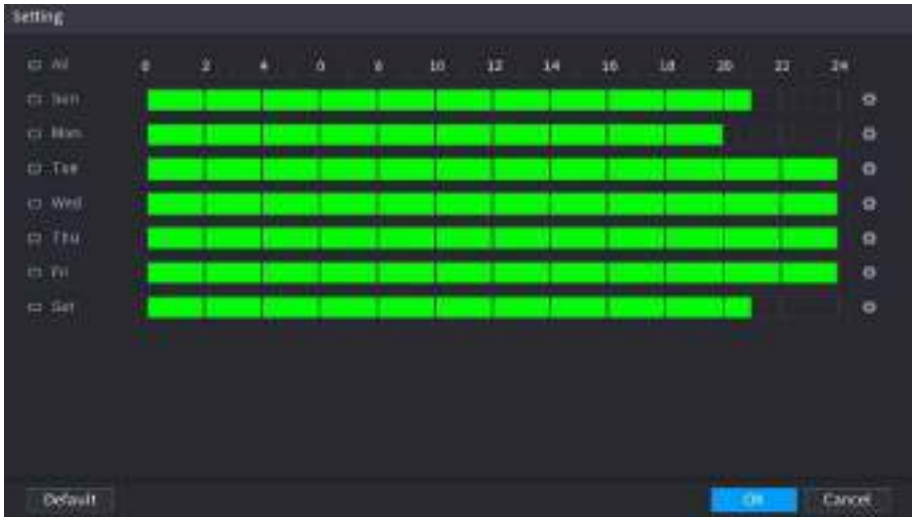
Figure 5-175 Disarming



Step 3 (Optional) To enable scheduled disarming, click **Setting** next to **Duration of Disarm by Period**, and then set periods.

Scheduled disarming is only effective when **Disarming** is **Off**.

Figure 5-176 Scheduled disarming



- Drag your mouse to select time blocks.
- Green blocks indicates that disarming is enabled.
- You can also click to set time periods. One day can have 6 periods at most.

Step 4 Select the alarm linkage actions to disarm.

All alarm linkage actions will be disarmed if you select **All**.

Step 5 To disarm remote channels, select the checkbox at **Channel**, and then click **Setting** to select channels.

This function is only effective when the connected camera supports one-click disarming.

Step 6 Click **Apply**.

5.11 Network

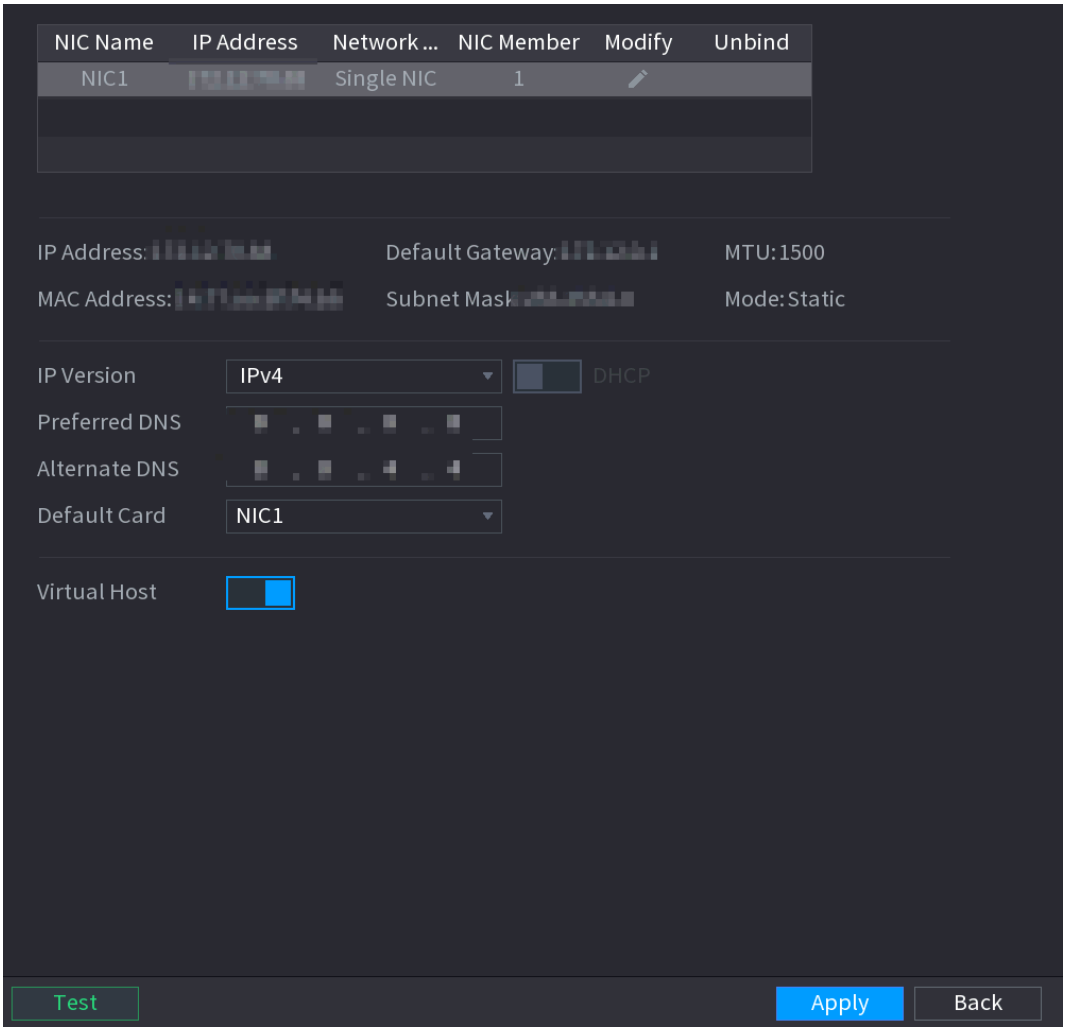
Configure the network settings to ensure the Device can communicate with other devices on the same LAN.

5.11.1 TCP/IP

You can configure the settings for the Device such as IP address, DNS according to the networking plan.

Step 1 Select **Main Menu** > **NETWORK** > **TCP/IP**.

Figure 5-177 TCP/IP



Step 2 Click to configure the NIC card, and then click **OK**.

Figure 5-178 TCP/IP

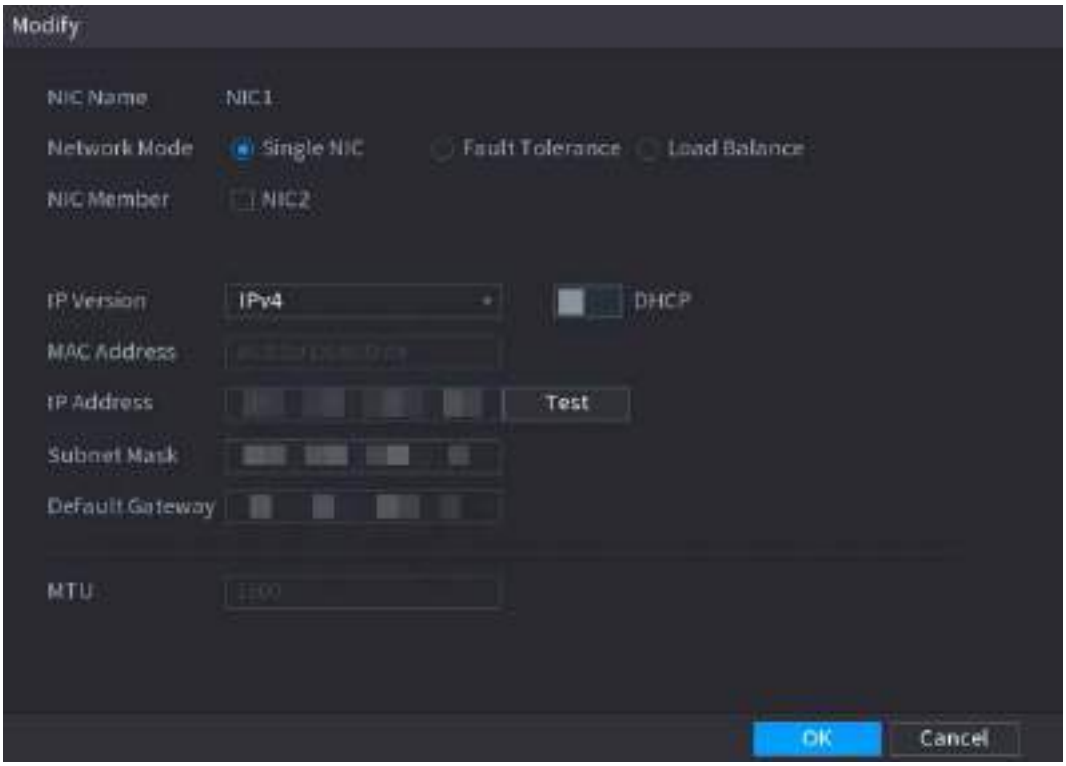


Table 5-49 TCP/IP parameters

Parameter	Description
Network Mode	• **Single NIC**: The current NIC card works independently. If the current NIC card is disconnected, the Device becomes offline. • **Fault Tolerance**: Two NIC cards share one IP address. Normally only one NIC card is working. When this card fails, the other NIC card will start working automatically to ensure the network connection. The Device is regarded as offline only when both NIC cards are disconnected. • **Load Balance**: Two NIC cards share one IP address and work at the same time to share the network load averagely. When one NIC card fails, the other card continues to work normally. The Device is regarded as offline only when both NIC cards are disconnected. The Device with single Ethernet port does not support this function.
NIC Member	When the network mode is **Fault Tolerance** or **Load Balance**, you need to select the checkbox to bind NIC cards. • Make sure that at least two NIC cards are installed. • NIC cards using different ports such as optical port and electrical port cannot be bound together. • After binding NIC cards, you need to restart the Device to make the change effective.
IP Version	Select IPv4 or IPv6. Both versions are supported for access.

Parameter	Description
MAC Address	Displays the MAC address of the Device.
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to set IP address manually. ● If you want to manually configure the IP information, disable the DHCP function first. ● If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. ● The IP address and default gateway must be on the same network segment. ● Click **Test** to check whether the IP address is available.
Subnet Mask	
Default Gateway	
MTU	Displays the MTU value of the NIC card.

Step 3 On the **TCP/IP** page, configure the DNS server.

This step is compulsive if you want to use the domain service.

- Obtain DNS server automatically.
  When there is DHCP server on the network, you can enable **DHCP** so that the Device can automatically obtain a dynamic IP address.
- Configure DNS server manually.
  Select the IP version, and then enter the IP addresses of preferred and alternate DNS server.

Step 4 Select a NIC card as the default card.

Step 5 Click **Apply**.

5.11.2 Routing Table

You can configure the routing table so that the system can automatically calculate the best path for data transmission.

Step 1 Select **Main Menu** > **NETWORK** > **TCP/IP** > **Routing Table**.

Figure 5-179 Routing table

Step 2 Add the routing table.

- Auto add.
  When you add a camera to the NVR and the IP address of the camera is not on the existing routing table, the system will add the routing information.
- Manual add.
  Configure the parameters such as destination address, netmask, and gateway, and then click **Add**.

  - The destination address and netmask must not be on the same LAN.
  - The netmask must be valid and on the same LAN with the NIC card.
  - You can configure up to eight pieces of routing information.

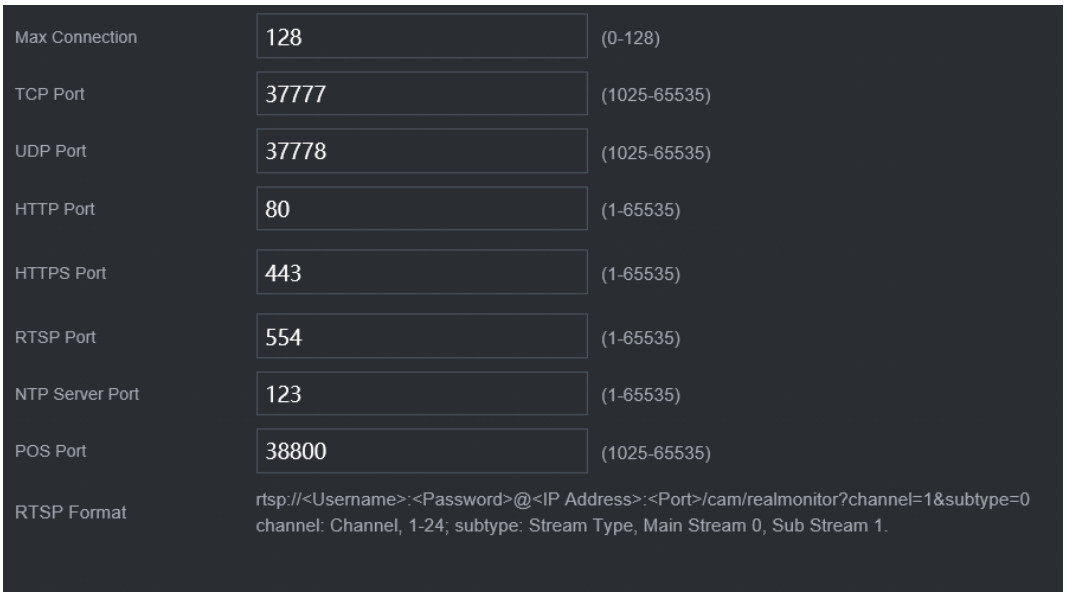
Step 3 Click **Apply**.

5.11.3 Port

You can configure the maximum connection for accessing the Device from web, platform, mobile phone or other clients at the same time, and configure each port number.

Step 1 Select **Main Menu** > **NETWORK** > **Port**.

Figure 5-180 Port



Step 2 Configure the parameters.

The parameters except **Max Connection** take effect after the Device restarts.

Table 5-50 Port parameters

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as web client, platform, and mobile client.
TCP Port	Transmission control protocol port. Enter the value according to your actual situation.
UDP Port	User datagram protocol port. Enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you change the HTTP port number to, for example, 70, then you need to enter 70 after the IP address when logging in to the Device through the browser.
HTTPS Port	HTTPS communication port. The default value is 443. You can enter the value according to your actual situation.
RTSP Port	The default value is 554. You can enter the value according to your actual situation.
POS Port	POS data transmission port. The value range from 1 through 65535. The default value is 38800.

Step 3 Click **Apply**.

5.11.4 External Wi-Fi

The Device can be connected to wireless network with an external Wi-Fi module.

Prerequisites

Make sure that external Wi-Fi module is installed on the Device.

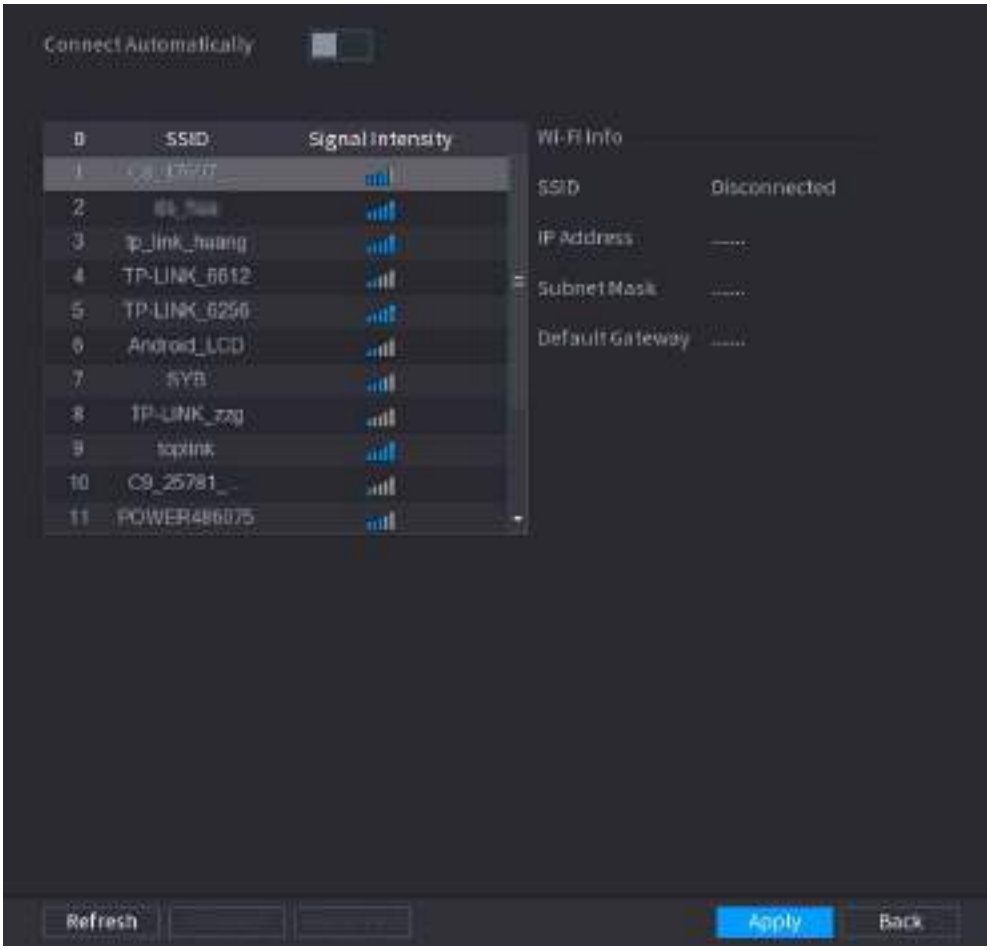
Background Information

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Wi-Fi**.

Figure 5-181 Wi-Fi



Step 2 Configure the parameters.

Table 5-51 Wi-Fi parameters

Parameter	Description
Connect Automatically	After the function is enabled, the NVR will connect to the nearest site that was previously successfully connected after the Device starts.
Refresh	Search for the sites again.
Disconnect	Disconnect the current connection.

Parameter	Description
Connect	Select an available site and then click **Connect**.

Step 3 Click **Apply.**

- After the connection is successful, a Wi-Fi connection signal flag appears in the upper-right corner of the live view page.
- The Wi-Fi module models currently supported are D-LINK, dongle and EW-7811UTC wireless cards.

5.11.5 Wi-Fi AP

You can configure Wi-Fi parameters for the NVR to ensure that a wireless IPC can connect to the NVR through Wi-Fi AP.

This function requires the built-in Wi-Fi module in the Device.

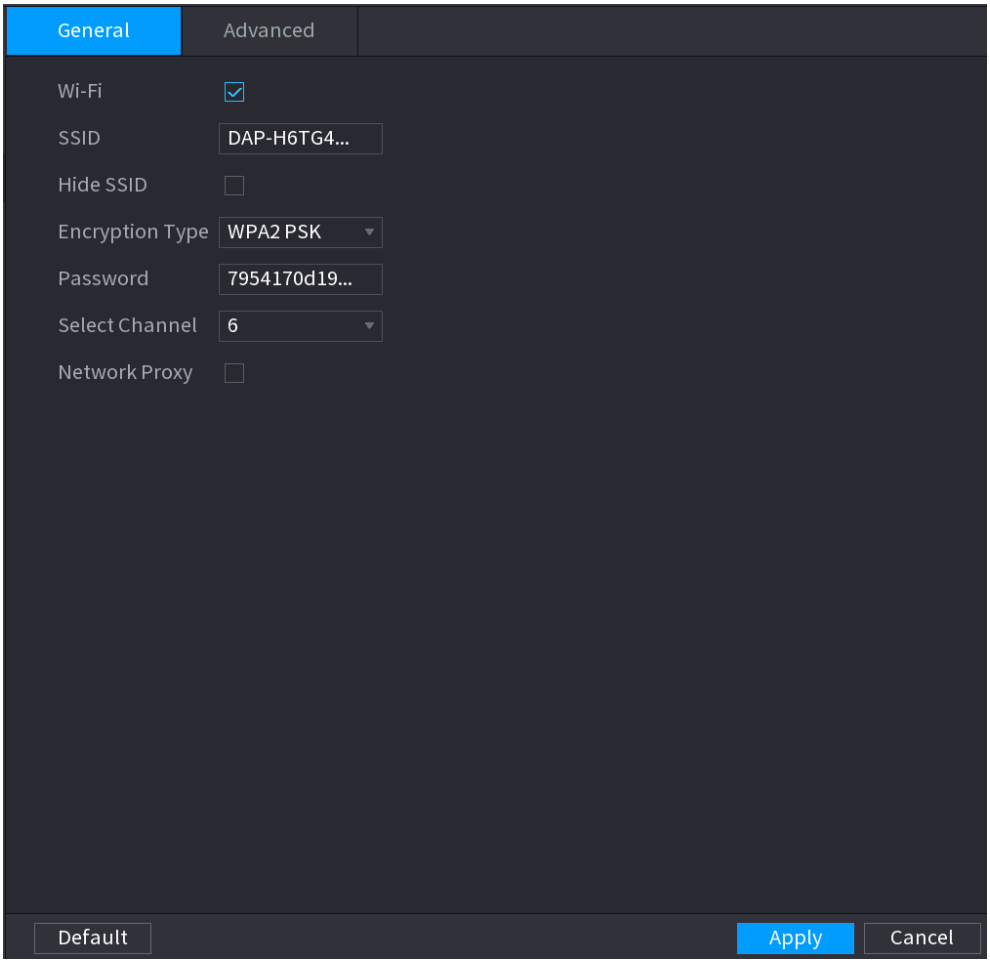
5.11.5.1 General Settings

You can configure SSID, encryption type, password and channel of the device.

- This function is supported on select wireless models.
- When the wireless IPC and NVR are matched, the pairing will be completed in 120 seconds after they are powered on.

Step 1 Select **Main Menu** > **NETWORK** > **Wi-Fi AP** > **General**.

Figure 5-182 General settings



Step 2 Select **Wi-Fi** to enable Wi-Fi.

Step 3 Configure parameters.

Table 5-52 Parameters of general settings

Parameter	Description
SSID	Wi-Fi name for the device.
Hide SSID	Hide the Wi-Fi name.
Encryption Type	Select an encryption mode from WPA2 PSK and WPA PSK.
Password	Set the Wi-Fi password for the Device.
Select Channel	Select the channel for device communication.
Network Proxy	Enable the external network access through the Device for a wireless IPC.

Step 4 Click **Apply**.

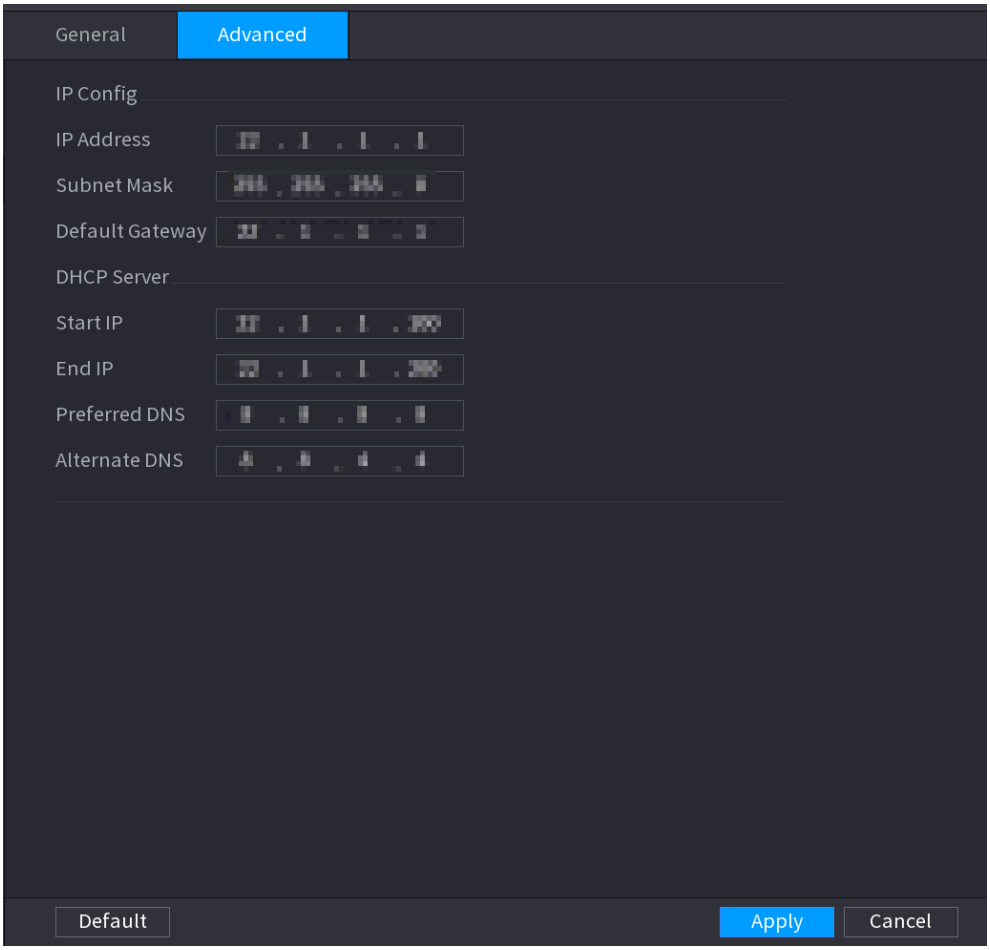
5.11.5.2 Advanced Settings

This function is supported on select wireless models.

You can configure IP address, subnet mask, default gateway, DHCP server of the Device.

Step 1 Select **Main Menu** > **NETWORK** > **Wi-Fi AP** > **Advanced**.

Figure 5-183 Advanced settings



Step 2 Configure parameters.

Table 5-53 Parameters of advanced settings

Parameter	Description
IP Address	Set IP address, subnet mask and default gateway for the Wi-Fi of NVR. IP address and default gateway must be on the same network segment.
Subnet Mask	
Default Gateway	
Start IP	Set the start IP address and end IP address of the DHCP server.
End IP	
Preferred DNS	Set preferred and alternate DNS server address.
Alternate DNS	

Step 3 Click **Apply**.

5.11.6 3G/4G

Prerequisites

Make sure that 3G/4G module is installed on the device.

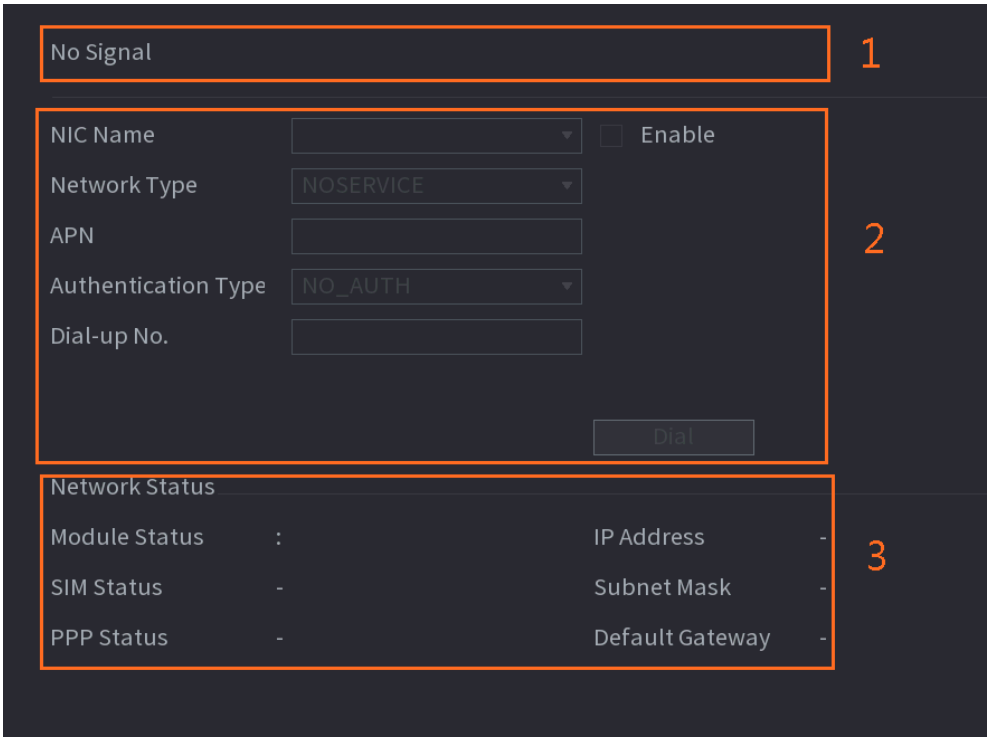
Background Information

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **3G/4G**.

Figure 5-184 3G/4G



The page is divided into three main areas:

- Zone 1 displays a 3G/4G signal indication.
- Zone 2 displays 3G/4G module configuration information.
- Zone 3 displays the status information of the 3G/4G module.

Zone 2 displays the corresponding information when the 3G/4G module is connected, while Zone 1 and Zone 3 will only display the corresponding content when the 3G/4G is enabled.

Step 2 Configure parameters.

Table 5-54 3G/4G parameters

Parameter	Description
NIC Name	Select a NIC name.
Network Type.	Select a 3G/4G network type to distinguish between 3G/4G modules from different vendors.
APN, Dial-up No.	Main parameters of PPP dial.
Authentication Type	Select PAP, CHAP or NO_AUTH. NO_AUTH represents no authentication for 3G/4G.

Step 3 Click **Apply**.

5.11.7 Cellular Network

Connect the Device to mobile network and view network status and traffic of the cellular network.

Prerequisites

A SIM card is inserted in the recorder.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Cellular Network** > **Cellular Network**.

Step 2 Enable cellular network and configure parameters.

Figure 5-185 Configuring cellular network

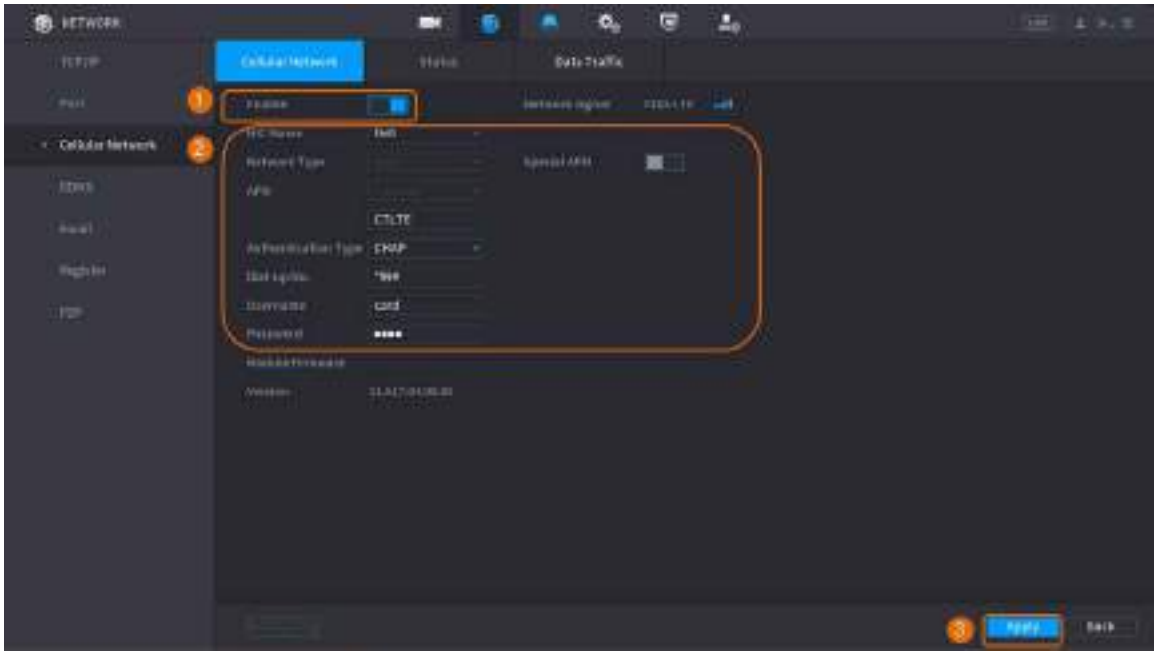


Table 5-55 4G cellular network parameters

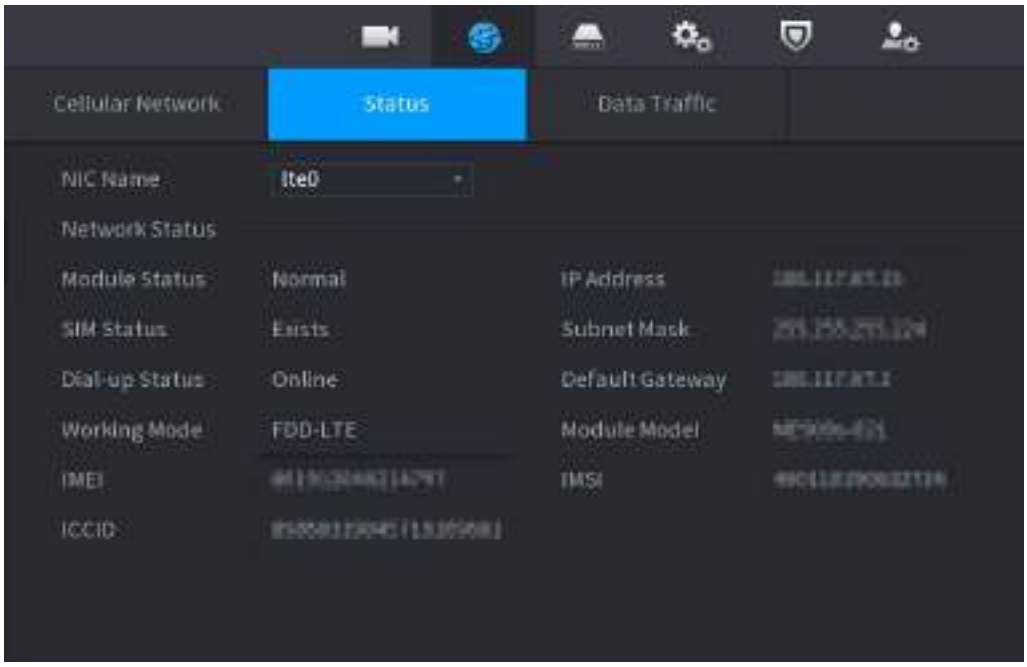
Parameter	Description
NIC Name	Select a NIC.
Network Type	Select a network from the SIM card provider.
APN, Dial-up No.	The two main parameters of PPP dial-up connection.
Authentication Type	Select **PAP**, **CHAP** or **NO-AUTH**.
Username	The username for dial-up connection.
Password	The password for dial-up connection.

Step 3 Click **Apply**.

Related Operations

- View network status.
  Click the **Status** tab to check cellular network status such as IP address, SIM card status and dial-up status.

Figure 5-186 Network status



- View data traffic.
  Click the **Data Traffic** tab to view the daily and monthly data usage.

Figure 5-187 Cellular data usage

5.11.8 Repeater

The Device supports relay settings for the wireless relay IPC to extend video transmission distance and range.

Prerequisites

- The Device has the built-in Wi-Fi module.

- The IPC has wireless relay module.

This function is available on select models.

Procedure

Step 1 Power on the NVR and wireless relay IPC, and connect all IPCs to the NVR through Wi-Fi.

Step 2 Select **Main Menu** > **NETWORK** > **REPEATER**.

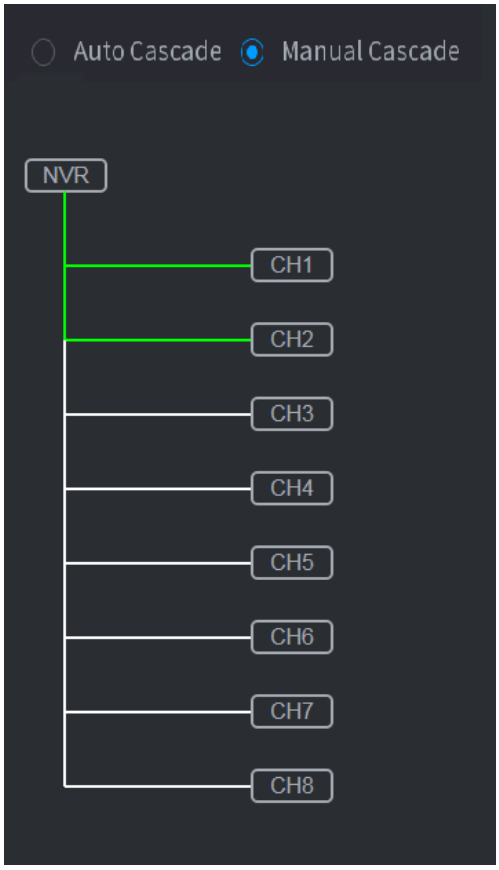
- Green connection line represents the successful connection between channel and wireless IPC.
- Auto cascade: After selecting auto cascade, the IPC can cascade to NVR automatically.

Figure 5-188

Step 3 Select **Manual Cascade**.

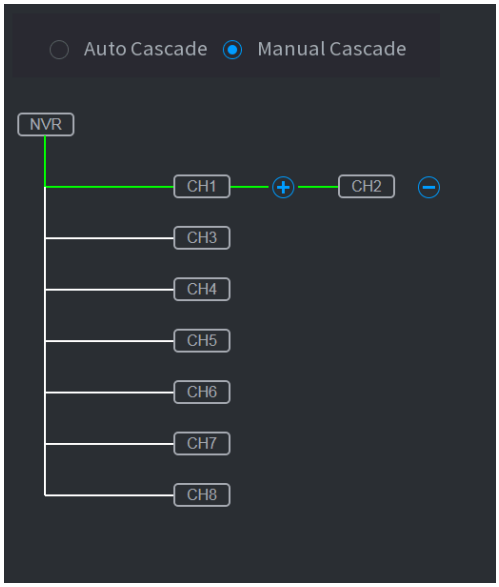
You can use manual cascade when there are at least two IPCs on the network.

Figure 5-189 Manual cascade



Step 4 Click ⊕ and select the channel to be added.

Figure 5-190 Added channel



Step 5 Click **Apply**.

5.11.9 PPPoE

PPPoE is another way for the Device to access the network. You can establish network connection by configuring PPPoE settings to give the Device a dynamic IP address on the WAN.
To use this function, firstly you need to obtain the username and password from the Internet Service Provider.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **PPPoE**.

Figure 5-191 PPPoE

Step 2 Enable the PPPoE function.

Step 3 Enter the username and password provided by the Internet Service Provider.

Step 4 Click **Apply**.

The IP address appears on the PPPoE page. You can use this IP address to access the Device.

When the PPPoE function is enabled, the IP address on the **TCP/IP** page cannot be modified.

5.11.10 DDNS

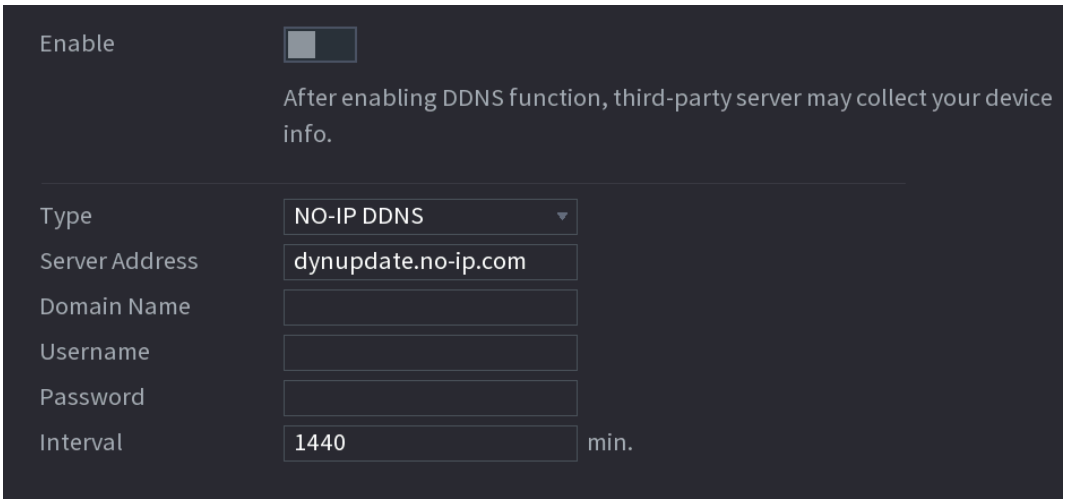
When the IP address of the Device changes frequently, the DDNS function can dynamically refresh the correspondence between the domain on DNS and the IP address. You can access the Device by using the domain.
Check the type of DDNS that the Device supports and then log in to the website provided by the DDNS service provider to register domain and other information.

After registration, you can log in to the DDNS website to view the information of all the connected devices under the registered account.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **DDNS**.

Figure 5-192 DDNS



Step 2 Enable DDNS and then configure the parameters.

After you enable DDNS function, the third-party server might collect your device information.

Table 5-56 DDNS parameters

Parameter	Description
Type	Displays the type and address of DDNS service provider. • For **Dyndns DDNS**, the default address is members.dyndns.org. • For **NO-IP DDNS**, the default address is dynupdate.no-ip.com. • For **CN99 DDNS**, the default address is members.3322.org.
Server Address	
Domain Name	Enter the domain name that you have registered on the website of DDNS service provider.
Username	Enter the username and password obtained from DDNS service provider. You need to register the username, password and other information on the website of DDNS service provider.
Password	
Interval	Enter the interval at which you want to update the DDNS.

Step 3 Click **Apply**.

Enter the domain name in the browser on your PC, and then press the Enter key. If the web interface of the Device is displayed, the configuration is successful. If not, the configuration failed.

5.11.11 UPnP

You can map the relationship between the LAN and the WAN to access the Device on the LAN through the IP address on the WAN.

5.11.11.1 Configuring Router

Procedure

Step 1 Log in to the router to set the WAN port to enable the IP address to connect into the WAN.

Step 2 Enable the UPnP function on the router.

Step 3 Connect the Device with the LAN port on the router to connect into the LAN.

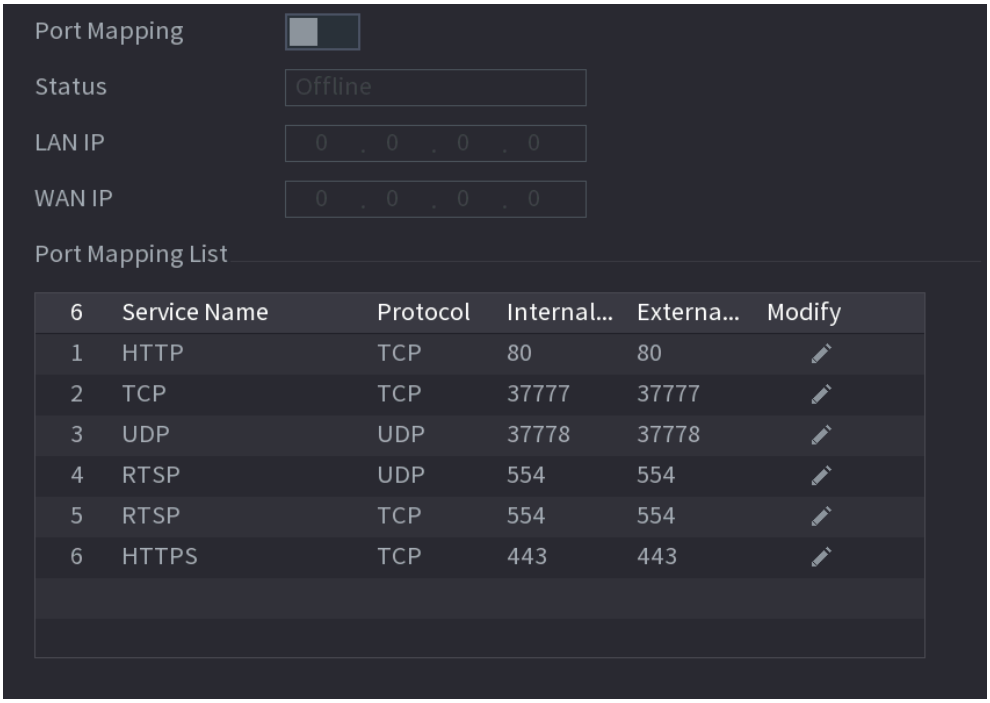
Step 4 Select **Main Menu** > **NETWORK** > **TCP/IP**, configure the IP address into the router IP address range, or enable the DHCP function to obtain an IP address automatically.

5.11.11.2 Configuring UPnP

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **UPnP**.

Figure 5-193 UPnP



Step 2 Configure the settings for the UPnP parameters.

Table 5-57 UPnP parameters

Parameter	Description
Port Mapping	Enable the UPnP function.
Status	Indicates the status of UPnP function. ● Offline: Failed. ● Online: Succeeded.
LAN IP	Enter IP address of router on the LAN. After mapping succeeded, the system obtains IP address automatically.
WAN IP	Enter IP address of router on the WAN. After mapping succeeded, the system obtains IP address automatically.

Parameter	Description
Port Mapping List	The settings on port mapping list correspond to the UPnP port mapping list on the router. ● Service Name: Name of network server. ● Protocol: Type of protocol. ● Internal Port: Internal port that is mapped on the Device. ● External Port: External port that is mapped on the router. ● To avoid the conflict, when setting the external port, try to use the ports from 1024 through 5000 and avoid popular ports from 1 through 255 and system ports from 256 through 1023. ● When there are several devices on the LAN, properly arrange the ports mapping relations to avoid mapping to the same external port. ● When establishing a mapping relationship, ensure the mapping ports are not occupied or limited. ● The internal and external ports of TCP and UDP must be the same and cannot be modified. ● Click to modify the external port.

Step 3 Click **Apply** to complete the settings.

In the browser, enter http://WAN IP: External IP port. You can visit the Device on the LAN.

5.11.12 Email

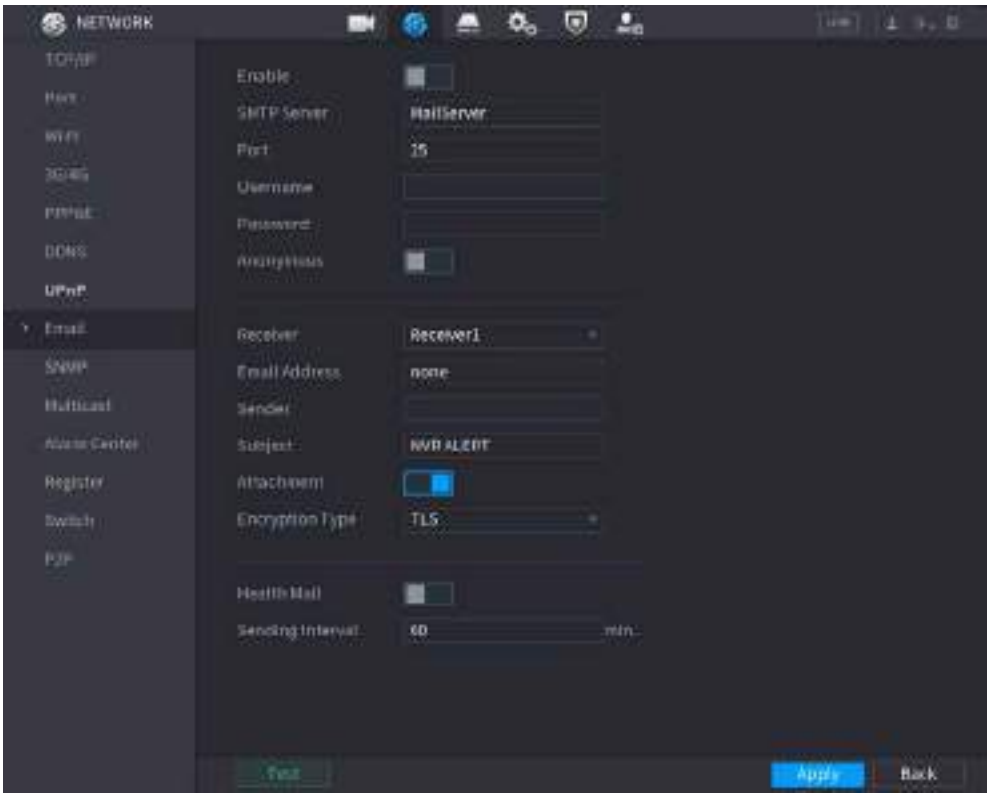
Background Information

You can configure the email settings to enable the system to send the email as a notification when an alarm event occurs.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Email**.

Figure 5-194 Email



Step 2 Click  to enable the function.

Step 3 Configure the email parameters.

Table 5-58 Email parameters

Parameter	Description
SMTP Server	Enter the address of SMTP server of sender's email account.
Port	Enter the port of SMTP server. The default value is 25.
Username	Enter the username and password of sender's email account.
Password	
Anonymous	Enable anonymous login.
Receiver	Select the receiver to receive the notification. You can select up to three receivers.
Email Address	Enter the email address of mail receivers.
Sender	Enter the sender's email address. You can enter up to three senders separated by comma.
Subject	Enter the email subject. You can enter Chinese, English and numerals with the length limited to 64 characters.
Attachment	Enable the attachment function. When there is an alarm event, the system can attach snapshots as an attachment to the email.
Encryption Type	Select the encryption type from **NONE**, **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.

Parameter	Description
Interval (Sec.)	Set the interval at which the system sends an email for the same type of alarm event to avoid excessive pileup of emails caused by frequent alarm events. The value ranges from 0 to 3600. 0 means that there is no interval.
Health Mail	Enable the health test function. The system can send a test email to check the connection.
Sending Interval	Set the interval at which the system sends a health test email. The value ranges from 30 to 1440. 0 means that there is no interval.
Test	Click **Test** to test the email sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click **Apply** to save the settings.

Step 4 Click **Apply**.

5.11.13 SNMP

You can connect the Device with some software such as MIB Builder and MG-SOFT MIB Browser to manage and control the Device from the software.

Prerequisites

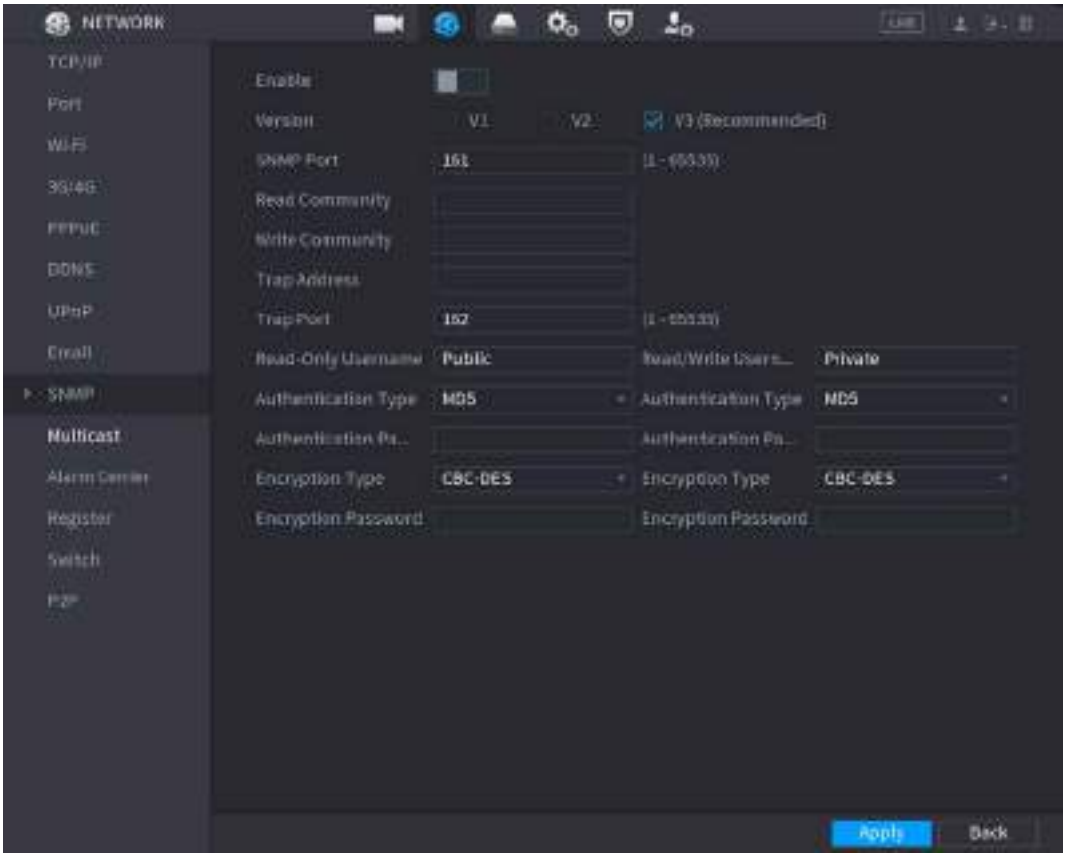
- Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser
- Obtain the MIB files that correspond to the current version from the technical support.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **SNMP**.

Figure 5-195 SNMP



Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Table 5-59 SNMP parameters

Parameter	Description
Version	Select the checkbox of SNMP version that you are using. The default version is **V3**. There is a risk if you use V1 or V2.
SNMP Port	Enter the monitoring port on the agent program.
Read Community	Enter the read and write strings supported by the agent program.
Write Community	
Trap Address	Enter the destination address for the agent program to send the Trap information.
Trap Port	Enter the destination port for the agent program to send the Trap information.
Read-Only Username	Enter the username that is allowed to access the Device and has the read-only permission.
Read/Write Username	Enter the username that is allowed to access the Device and has the read and write permission.
Authentication Type	Select MD5 or SHA. The system recognizes the type automatically.
Authentication Password	Enter the password for authentication. The password should be no less than eight characters.

Parameter	Description
Encryption Type	Select an encryption type. The default setting is CBC-DES.
Encryption Password	Enter the encryption password.

Step 4 Click **Apply**.

Step 5 Compile the two MIB files by MIB Builder.

Step 6 Run MG-SOFT MIB Browser to load in the module from compilation.

Step 7 On the MG-SOFT MIB Browser, enter the device IP that you want to manage, and then select the version number to query.

Step 8 On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

5.11.14 Multicast

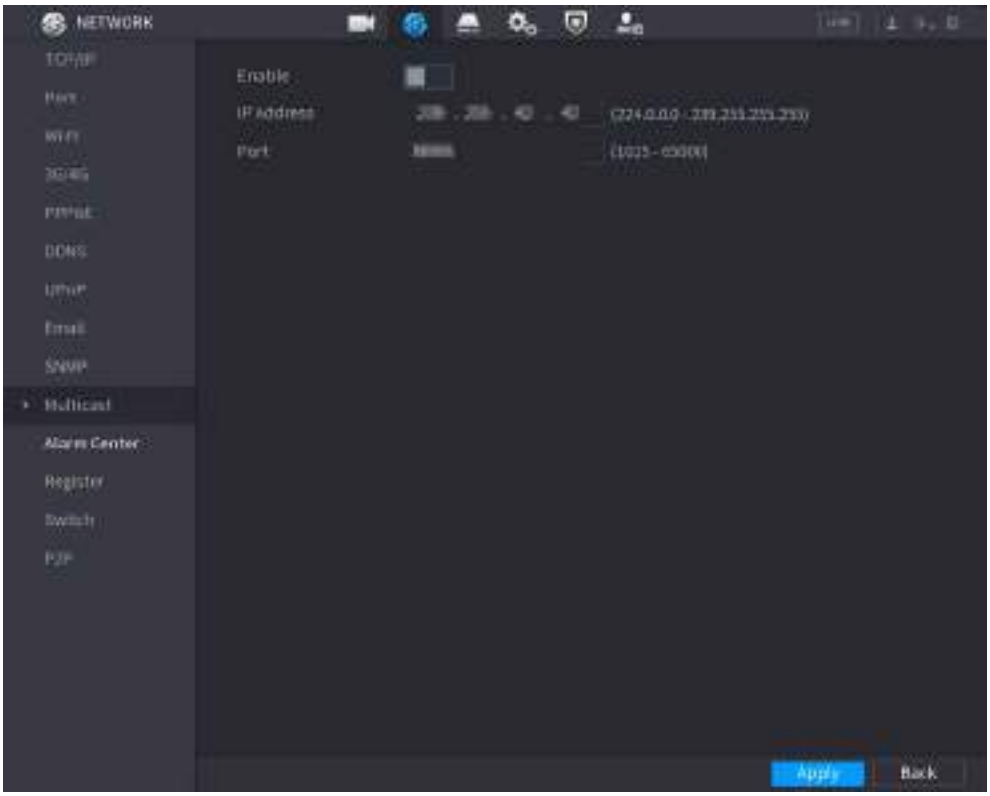
Background Information

When you access the Device from the network to view the video, if the access is exceeded, the video will not display. You can use the multicast function to group the IP to solve the problem.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Multicast**.

Figure 5-196 Multicast



Step 2 Configure the parameters.

Table 5-60

Parameter	Description
Enable	Enable the multicast function.

Parameter	Description
IP Address	Enter the IP address that you want to use as the multicast IP. The IP address ranges from 224.0.0.0 through 239.255.255.255.
Port	Enter the port for the multicast. The port ranges from 1025 through 65000.

Step 3 Click **Apply**.

You can use the multicast IP address to log in to the web.

On the web login page, on the **Type** list, select **Multicast**. The web will automatically obtain the multicast IP address and join the multicast group. Then you can view the video through multicast function.

5.11.15 Alarm Center

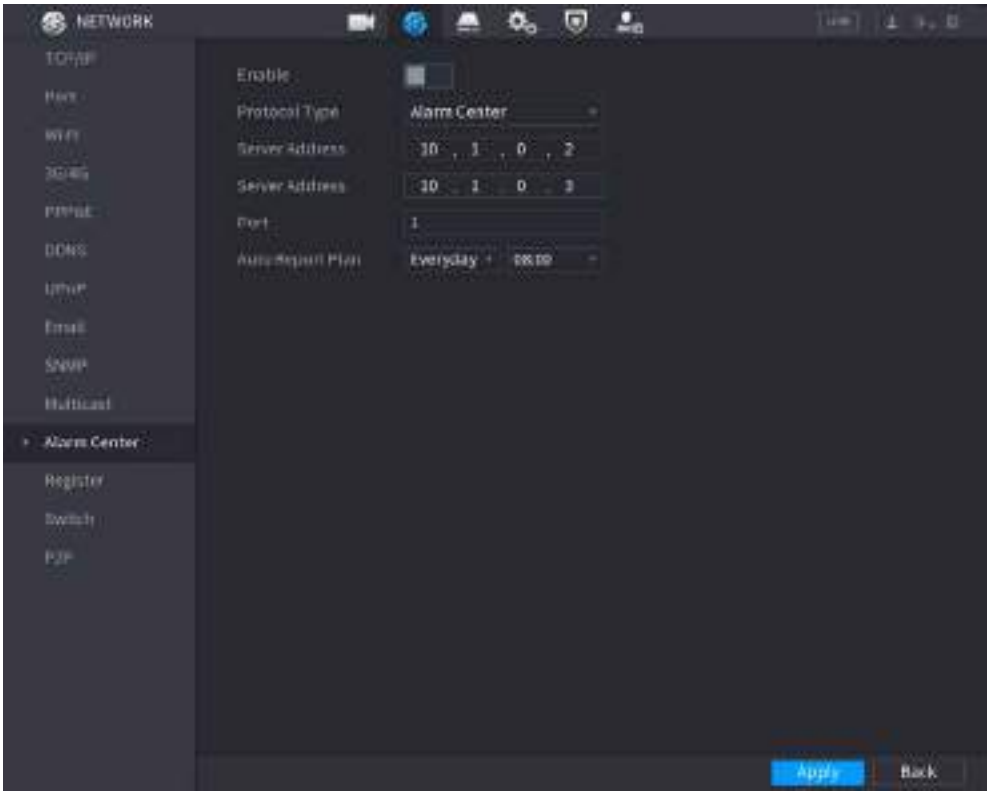
Background Information

You can configure the alarm center server to receive the uploaded alarm information.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Alarm Center**.

Figure 5-197 Alarm center



Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Table 5-61 Alarm center parameters

Parameter	Description
Protocol Type	Select a protocol type.

Parameter	Description
Server Address	The IP address and communication port of the PC installed with alarm client.
Port	
Auto Report Plan	Select time cycle and specific time for uploading alarm.

Step 4 Click **Apply**.

5.11.16 Register

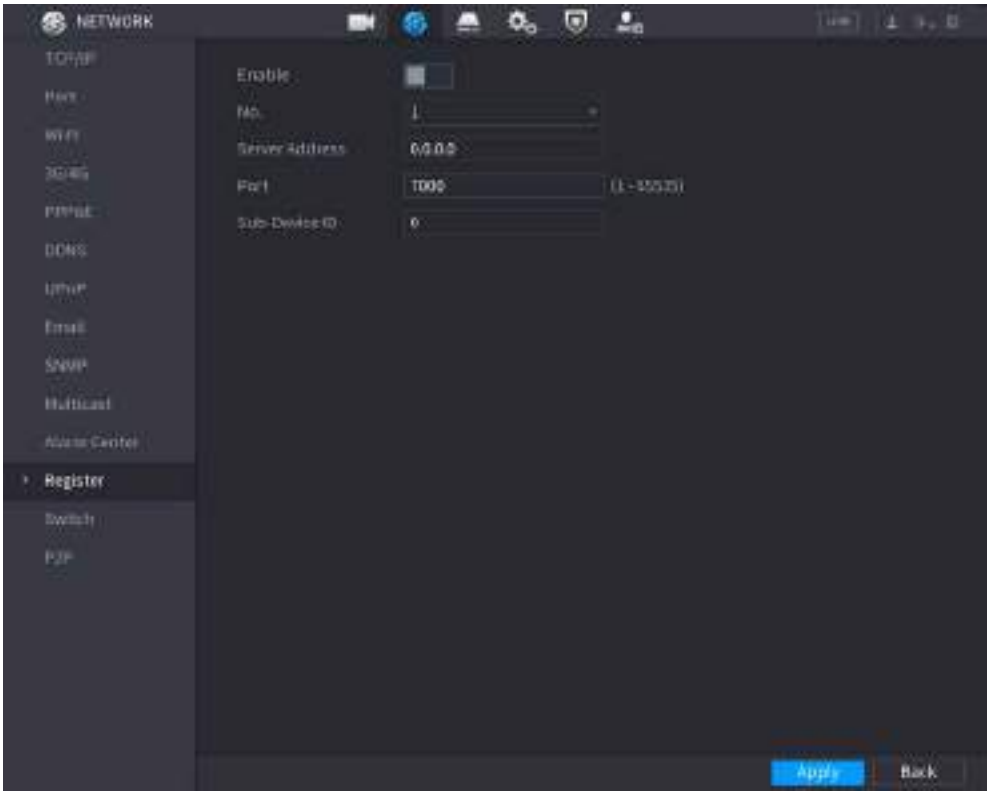
You can register the Device into the specified proxy server which acts as the transit to enable the client software to access the Device

- The proxy server has been deployed.
- The Device, the proxy server and the device running the client software are on the same network.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Register**.

Figure 5-198 Register



Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Table 5-62 Register parameters

Function	Description
Server Address	Enter the IP address or domain name of the server that you want to register to.
Port	Enter the port of the server.

Function	Description
Sub-Device ID	Enter the ID allocated by the server.

Step 4 Click **Apply**.

5.11.17 Switch

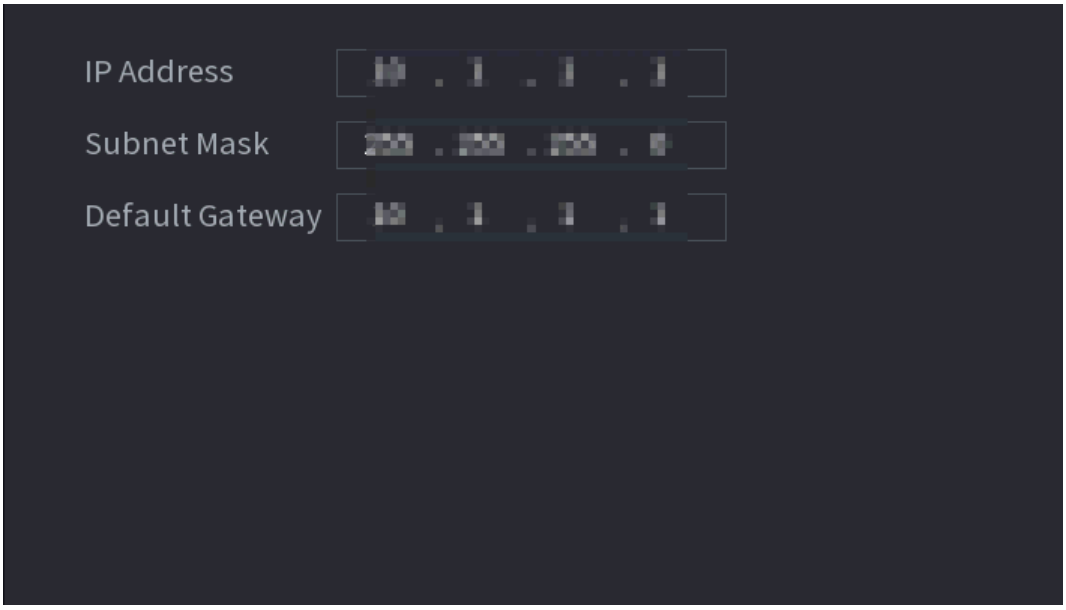
After setting **Switch**, when an IPC is connected to the PoE port, the system automatically assigns the IP address to the IPC according to the defined IP segment, and the NVR will automatically connect to the IPC.

- Only models with PoE ports support this function.
- Do not connect the PoE port with a switch, otherwise it will cause connection failure.
- This function is enabled by default, and the IP segment start from 10.1.1.1. We recommend you use the default setting.
- When connecting to a third-party IPC, make sure that the IPC supports ONVIF protocol and DHCP is enabled.

Procedure

Step 1 Select **Main Menu** > **NETWORK** > **Switch**.

Figure 5-199 Switch



Step 2 Configure IP address, subnet mask, and default gateway..

Do not set the IP address to the same network segment with the NVR. We recommend you use the default setting.

Step 3 Click **Apply**.

When connecting IP camera to PoE port, if all the channels are occupied, the system prompts you whether to take place of one channel.

PoE operation

Table 5-63

PoE operation	Description
Connect to PoE port	When an IPC is connected to the PoE port, the system automatically assigns the IP address to the IPC according to the set IP segment. The NVR will try the method of arp ping to assign the IP address. If DHCP is enabled on the NVR, the NVR will use DHCP to assign the IP address. • When IP address is successfully set, the system will broadcast through the switch function. If there is a response from the IPC, it means the connection is successful, and the NVR will log in to the IPC. You can find the corresponding channel occupied and there is a PoE icon at the upper-left corner. • You can also view PoE status such as channel number and PoE port number on the **Added Device** list in **Main Menu** > **CAMERA** > **Camera List**.
Disconnect PoE port	When an IPC is disconnected form PoE port, you will find the information of **Failed to find network host** on the live channel window.
PoE connection mapping	The PoE ports are bound to corresponding channels. When an IPC is connected to PoE port 1, the corresponding channel is Channel 1.

5.11.18 P2P

P2P is a kind of convenient private network penetration technology. Instead of applying for dynamic domain name, mapping ports or deploying transit server, you can add NVR devices to the app for remote management.

Step 1 Select **Main Menu** > **NETWORK** > **P2P**.

Figure 5-200 P2P

Step 2 Enable the P2P function.

After you enable the P2P function and connect to the Internet, the system will collect the information such as email address and MAC address for remote access.

Step 3 Click **Apply**.

The P2P function is enabled. You can use your phone to scan the QR code under **Mobile Client** to download and install the mobile client. After that, you can use the mobile client to scan the QR code under **Device SN** to add the Device for remote management. For details on the app operation, see the user's manual of the app.

5.12 Storage

You can manage the storage resources (such as record file) and storage space. So that it is easy for you to use and enhance storage space usage.

5.12.1 Basic

Background Information

You can set basic storage parameters.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **Basic**.

Figure 5-201 Basic storage

Step 2 Set parameters.

Table 5-64 Basic storage parameters

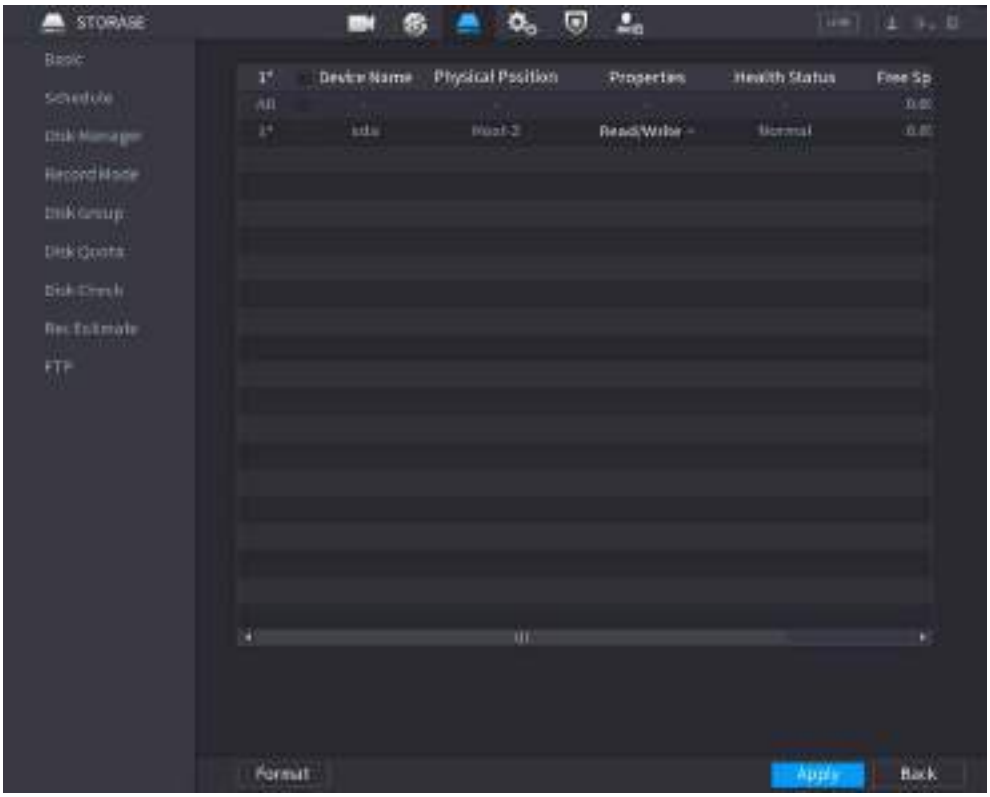
Parameter	Description
Disk Full	Configure the storage strategy to be used when no more storage space is available ● **Stop**: Stop recording ● **Overwrite**: The newest files overwrite the oldest ones.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired Files	Configure whether to delete the old files. ● Select **Auto** and then configure how long you want to keep the old files. ● Select **Never** if you do not want to use this function. Deleted files cannot be recovered.
Sleep Strategy	● **Auto**: The system sleeps automatically after idling for a period of time. ● **Never**: The system keeps running all the time.

Step 3 Click **Apply**.

5.12.2 Disk Manager

Select **Main Menu** > **STORAGE** > **Disk Manager**, and then you can set HDD properties and format HDD.

Figure 5-202 Disk manager



View HDD Information

You can view the physical position, properties, status and storage capacity of each HDD.

Configure HDD Properties

In the **Properties** column, you can set read and wire, read-only and redundant HDD.

When there are two or more HDDs installed on the Device, you can set one HDD as redundant disk to back up recorded files.

Format HDD

Select an HDD, click **Format**, and then follow the on-screen prompts to format the HDD.

- Formatting will erase all data in the HDD, proceed with caution.
- You can select whether to erase the HDD database. If the HDD database is erased, the AI search data and the uploaded audio files will be deleted.

5.12.3 RAID

RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

RAID function is available on select models.

Table 5-65 Disk quantity for different RAID types

RAID type	Required disk quantity
RAID 0	At least 2.
RAID 1	Only 2.
RAID 5	At least 3. We recommend using 4 disks to 6 disks.
RAID 6	At least 4.
RAID 10	

5.12.3.1 Creating RAID

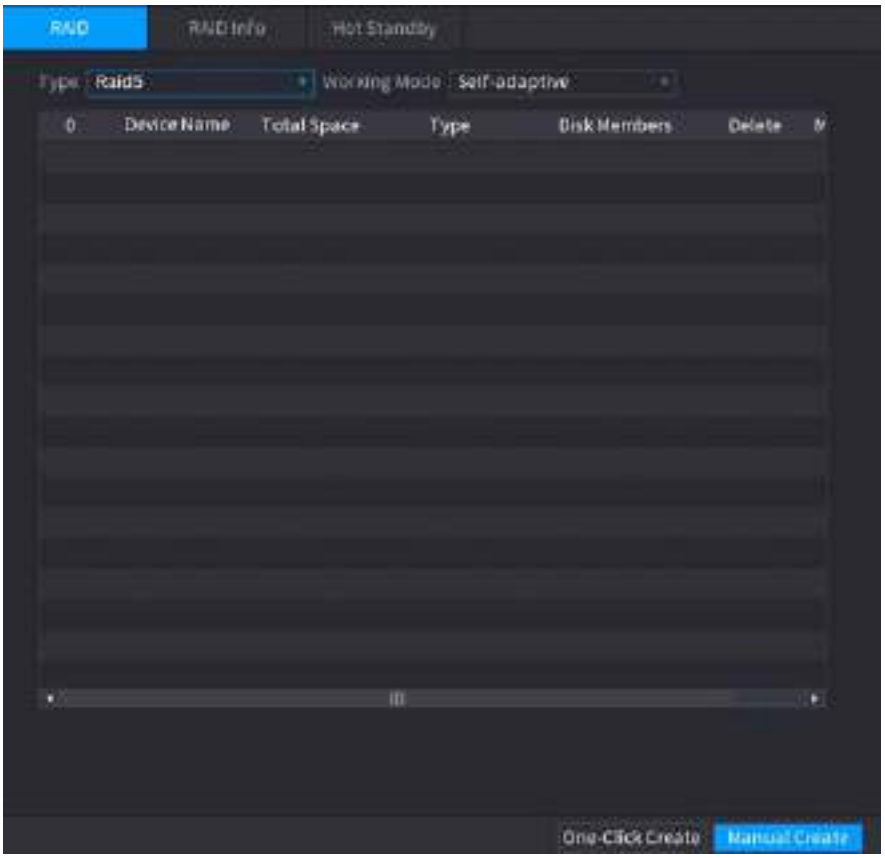
RAID has different levels, such as RAID 5 and RAID 6. Each level has different data protection, data availability, and performance grade. You can create different types of RAID as needed.

When you create RAID, the disks in the RAID group will be formatted. Back up data in time.
You can create different types of RAID as needed.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **RAID** > **RAID**.

Figure 5-203 RAID



Step 2 Select RAID type and working mode.

The working mode determines how the system allocate resources.

- **Self-Adaptive**: Automatically adjust the RAID synchronization speed according to the business status.
  - When there is no business running, synchronization is performed at a high speed.
  - When there is business running, synchronization is performed at a low speed.
- **Sync First**: Resource priority is assigned to RAID synchronization.
- **Business First**: Resource priority is assigned to business operations.
- **Balance**: Resource is evenly distributed to RAID synchronization and business operations.

Step 3 Create RAID.

- Automatic creation.
  Select disks, and then click **Create RAID**. The system will create RAID 5 automatically.

  Automatic creation of RAID is available only when the RAID type is **Raid5**.
- Manual creation.
  Select disks, click **Create Manually** and then follow the on-screen instructions to create RAID.

- Change working mode.
  Click  to change the working mode of the RAID group.
- Delete RAID.
  Click  to delete the RAID group.

  When you delete a RAID group, the disks in the RAID group will be formatted.

5.12.3.2 Viewing RAID Information

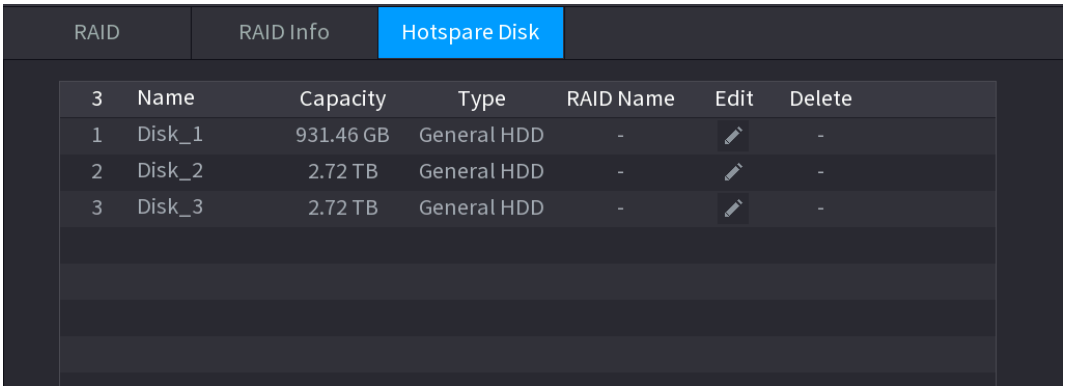
Select **Main Menu** > **STORAGE** > **RAID** > **RAID Info**. You can view the RAID information, including type, disk space, hot spare, and status.

5.12.3.3 Creating Hot Spare Disk

You can create a hot spare disk. When a disk of the RAID group malfunctions, the hot spare disk can replace the malfunctioning disk.

Step 1 Select **Main Menu** > **STORAGE** > **RAID** > **Hotspare Disk**.

Figure 5-204 Hotspare disk



Step 2 Click .

Figure 5-205 Local hotspare

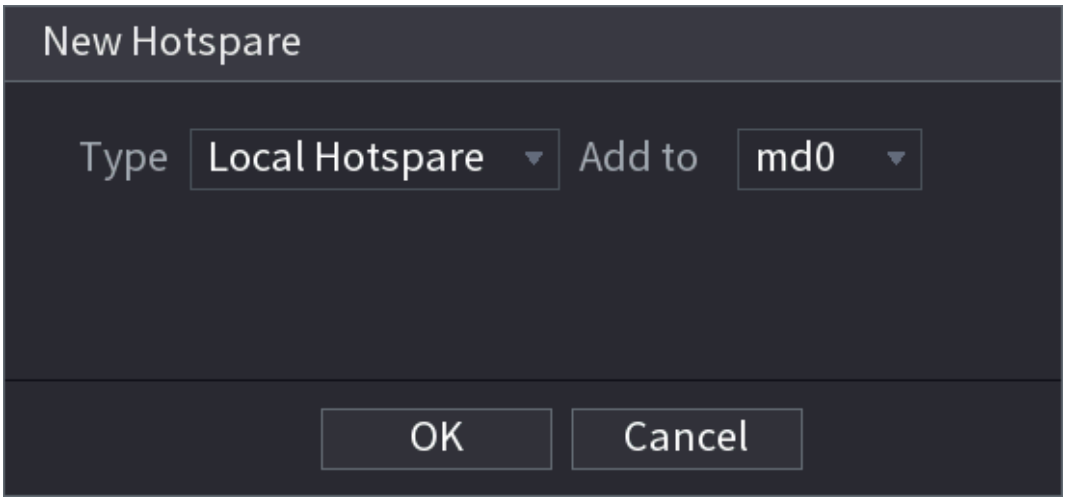
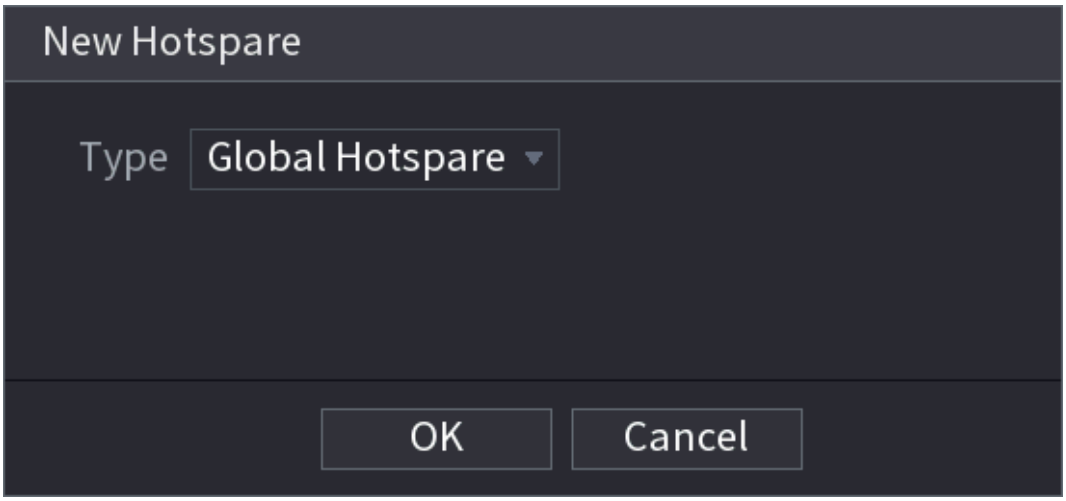


Figure 5-206 Global hotspare



Step 3 You can select **Local Hotspare** or **Global Hotspare**.

- **Local Hotspare**: Select the target disk, and the current disk will serve as the hot spare disk for the selected target disk.
- **Global Hotspare**: The current disk will serve as the hot spare disk of the entire RAID.

Step 4 Click **OK**.

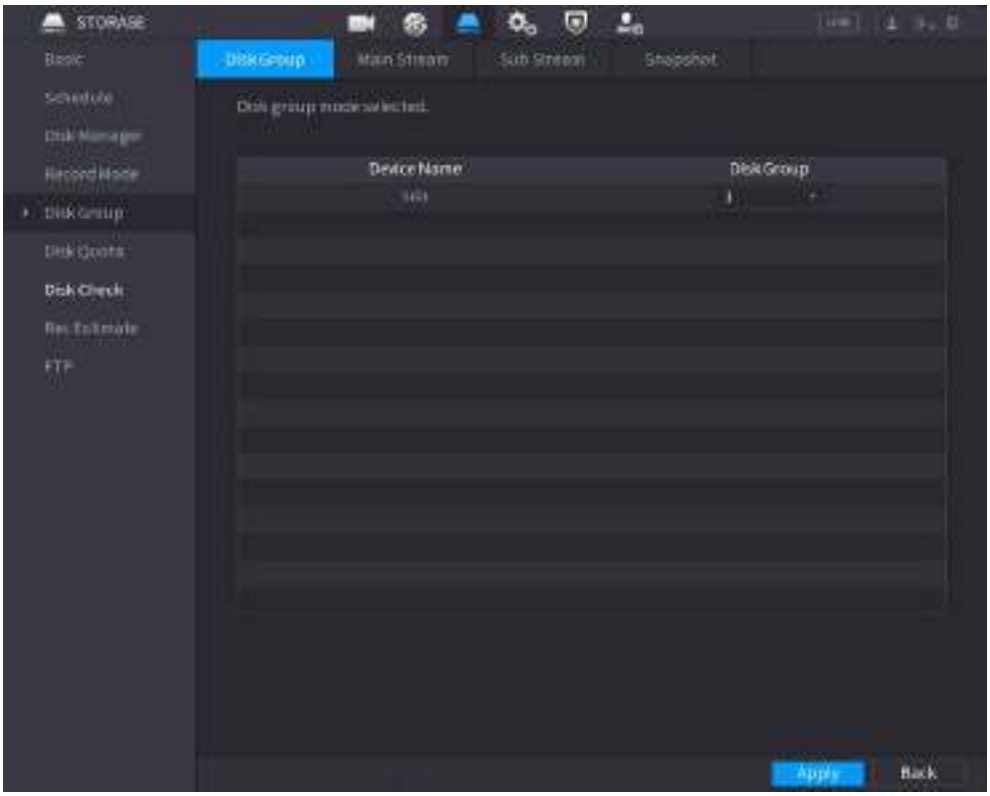
Click to delete a hot spare disk.

5.12.4 Disk Group

By default, the installed HDD and created RAID are in Disk Group 1. You can set HDD group, and HDD group setup for main stream, sub stream and snapshot operation.

Step 1 Select **Main Menu** > **STORAGE** > **Disk Group**.

Figure 5-207 Disk group



Step 2 (Optional) If **Disk Quota is selected** is shown on the page, click **Switch to Disk Group Mode** and then follow the on-screen instructions to format disks.

Step 3 Select the group for each HDD, and then click **Apply**.

After configuring HDD group, under the **Main Stream** tab, **Sub Stream** tab and **Snapshot** tab, configure settings to save the main stream, sub stream and snapshot to different disk groups.

5.12.5 Disk Quota

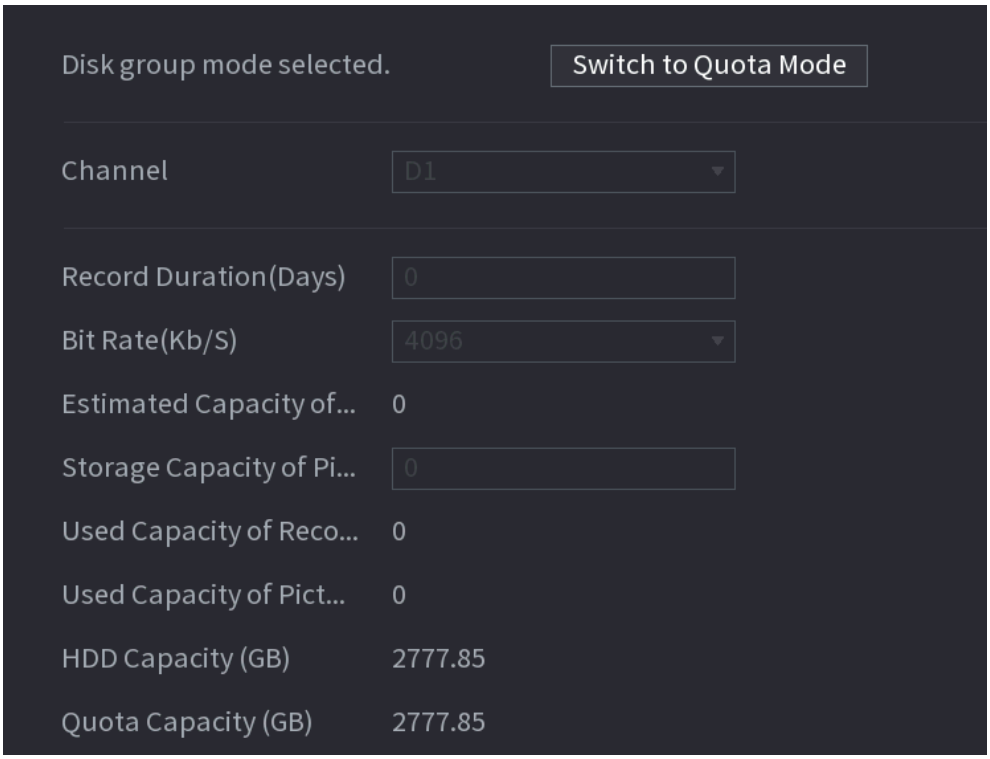
You can allocate a certain storage capacity for each channel to manage the storage space properly.

- If **Disk group mode selected.** is shown in the interface, click **Switch to Quota Mode.**
- Disk quota mode and disk group mode can not be selected at the same time.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **Disk Quota**.

Figure 5-208 Disk Quota



Step 2 (Optional) If **Disk group mode selected** is shown on the page, click **Switch to Quota Mode** and then follow the on-screen instructions to format disks.

Step 3 Select a channel and set the record duration, bit rate and storage capacity of picture.

Step 4 Click **Apply**.

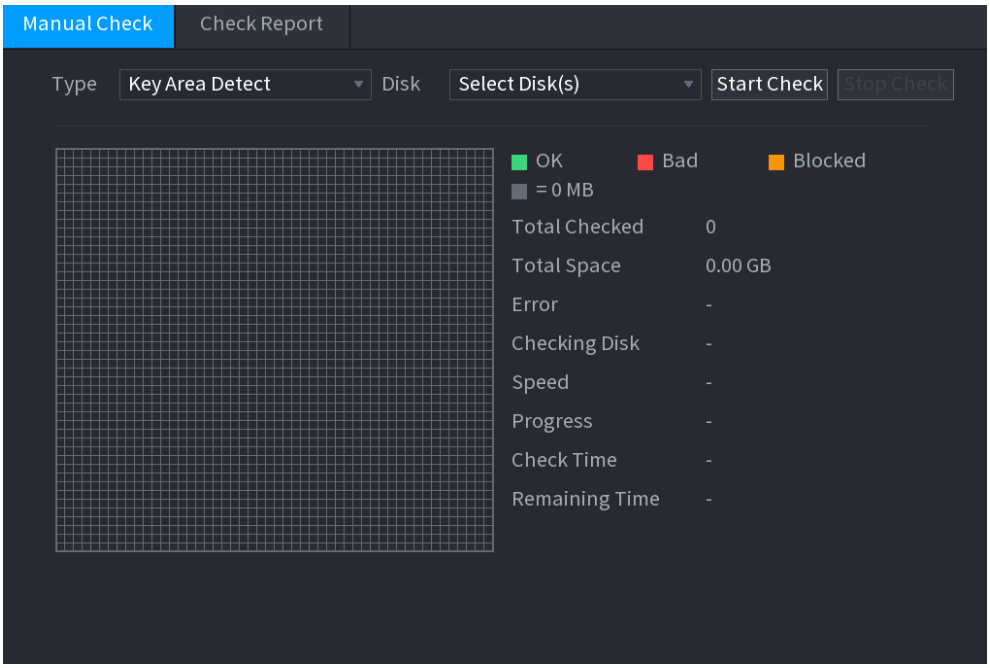
5.12.6 Disk Check

The system can detect HDD status so that you can clearly understand the HDD performance and replace the malfunctioning HDD.

5.12.6.1 Manual Check

Step 1 Select **Main Menu** > **STORAGE** > **Disk Check** > **Manual Check**.

Figure 5-209 Manual check



Step 2 Select the detection type.

- Key area detection: The system detects the used space of the HDD through the built-in file system. This type of detection is efficient.
- Global detection: The system detects the entire HDD through Window. This type of detection takes time and might affect the HDD that is recording.

Step 3 Select the HDD that you want to detect

Step 4 Click **Start Check**.

The system starts detecting the HDD and displays the detection information.

When system is detecting HDD, click **Stop Check** to stop current detection. Click **Start Check** to detect again.

5.12.6.2 Detection Report

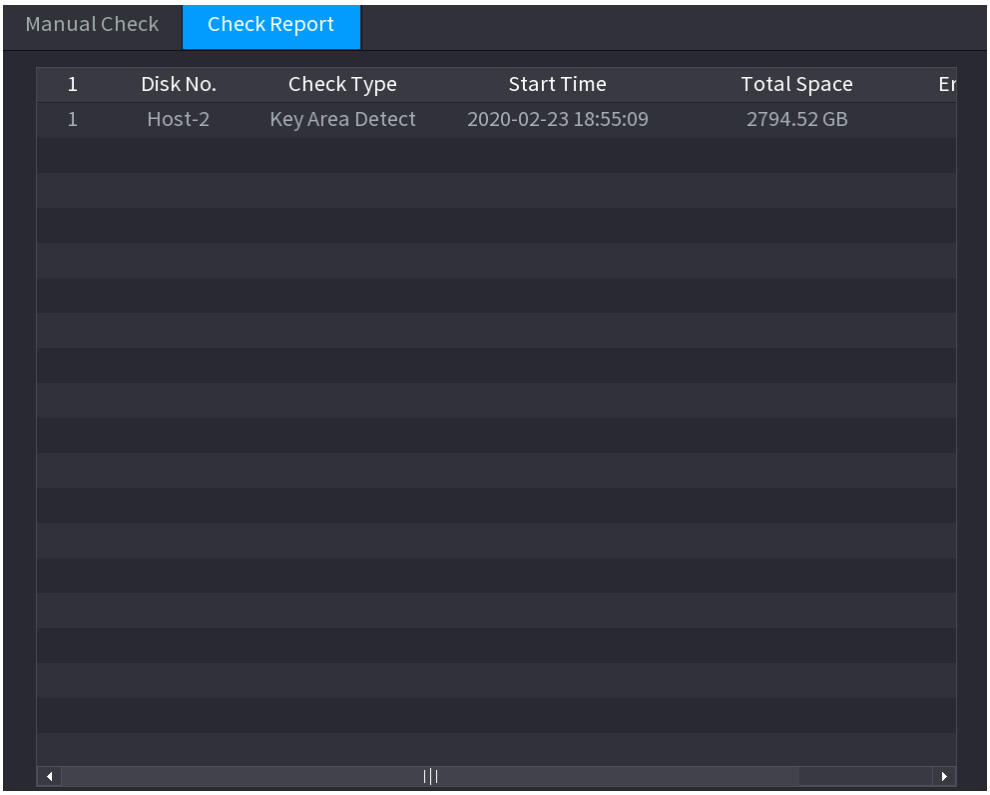
Background Information

After the detection operation, you can view the detection report.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **Disk Check** > **Check Report**.

Figure 5-210 Check report



Step 2 Click to view detection results and S.M.A.R.T report.

Figure 5-211 Results

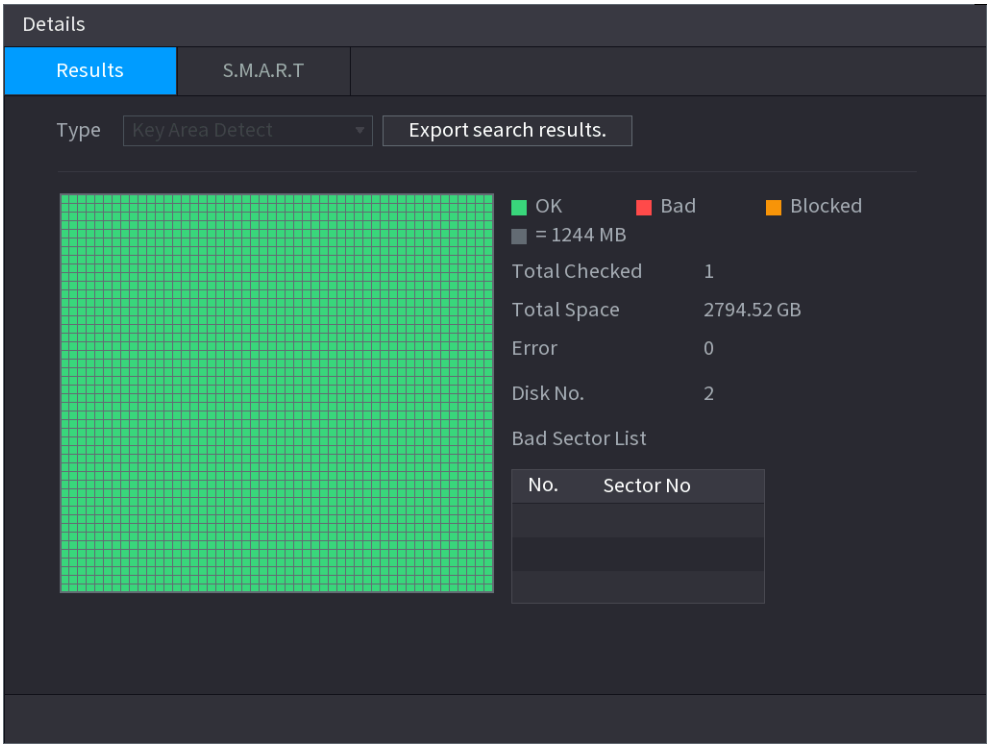
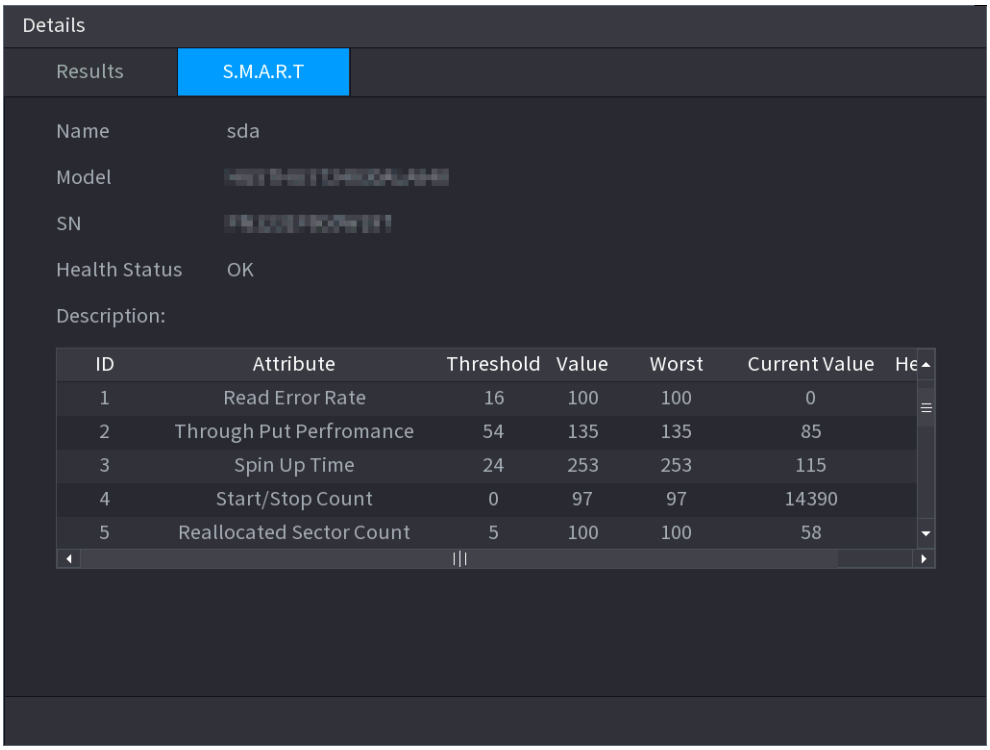


Figure 5-212 S.M.A.R.T



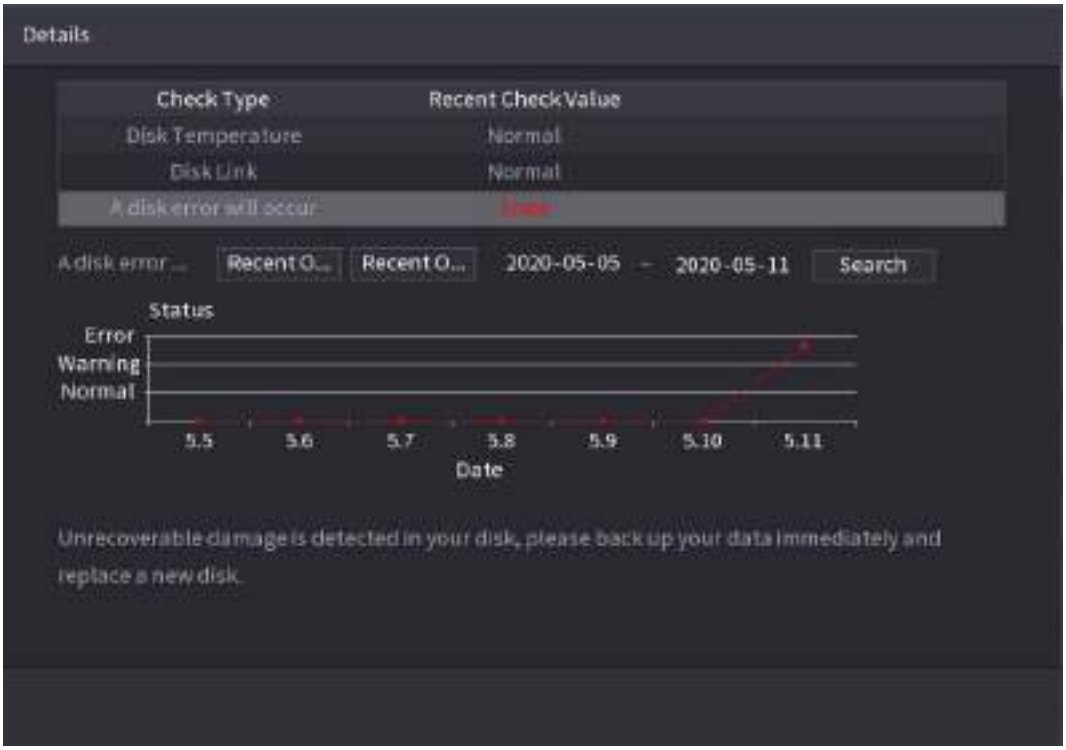
5.12.6.3 Disk Health Monitoring

Monitor health status of disks, and repair if any exceptions are found so as to avoid data loss.

Select **Main Menu** > **STORAGE** > **Disk Check** > **Health Monitoring**.

Click ⓘ to show disk details interface. Then select **Check Type**, set time period, and then click **Search**. The system shows the details of disk monitoring status.

Figure 5-213 Disk details

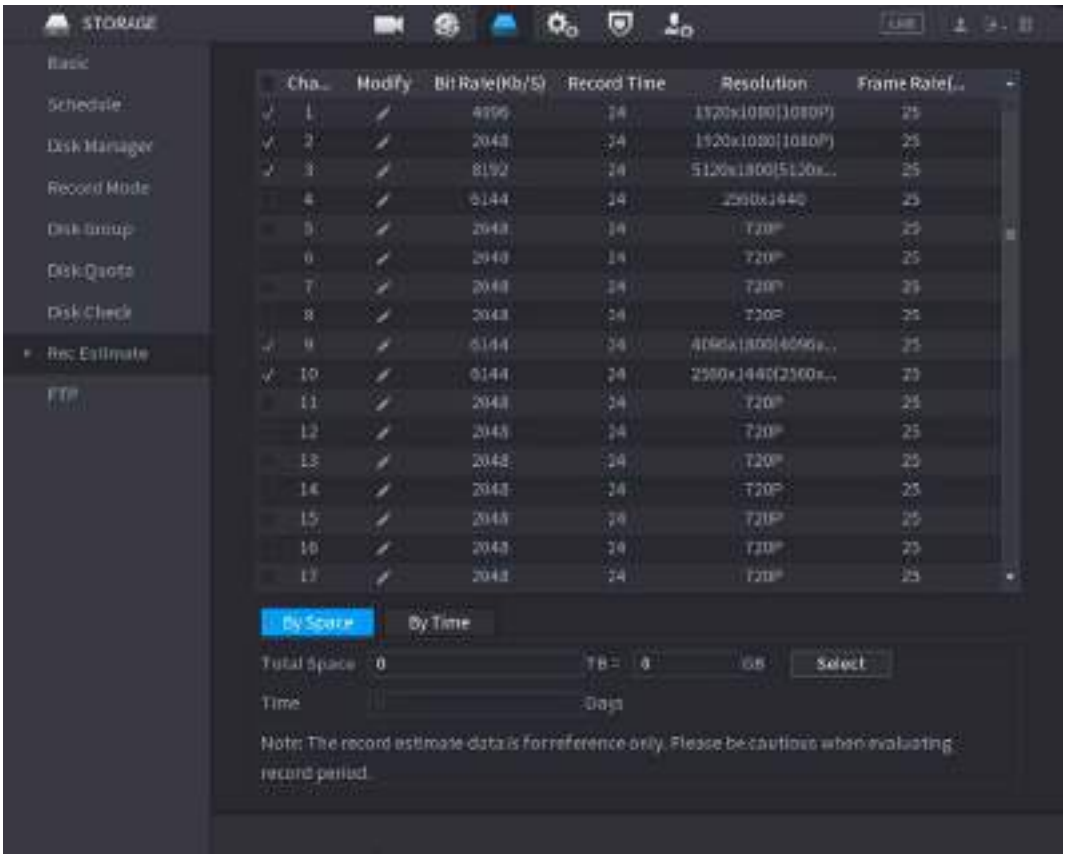


5.12.7 Record Estimate

Record estimate function can calculate how long you can record video according to the HDD capacity, and calculate the required HDD capacity according to the record period.

Step 1 **Select Main Menu** > **STORAGE** > **Rec Estimate**.

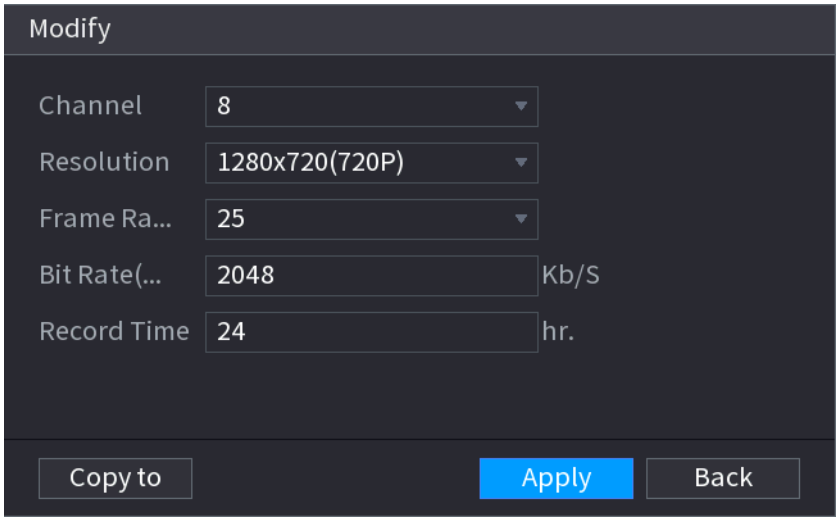
Figure 5-214 Record estimation



Step 2 Click .

You can configure the **Resolution**, **Frame Rate**, **Bit Rate** and **Record Time** for the selected channel.

Figure 5-215 Modify channel settings



Step 3 Click **Apply**.

Then the system will calculate the time period that can be used for storage according to

the channels settings and HDD capacity.

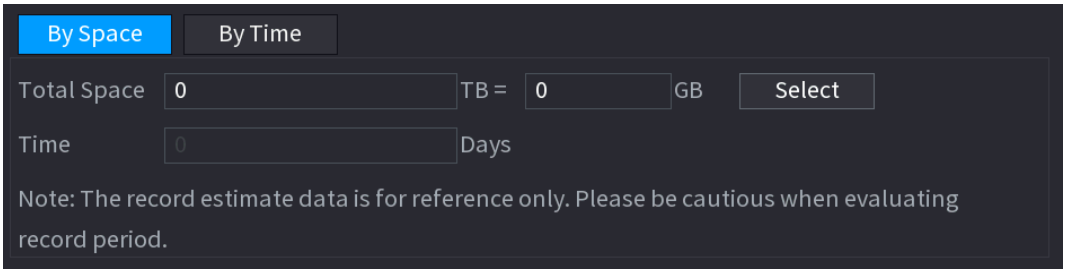
Click **Copy to** to copy the settings to other channels.

5.12.7.1 Calculating Recording Time

Procedure

Step 1 On the **Rec Estimate** interface, click the **By Space** tab.

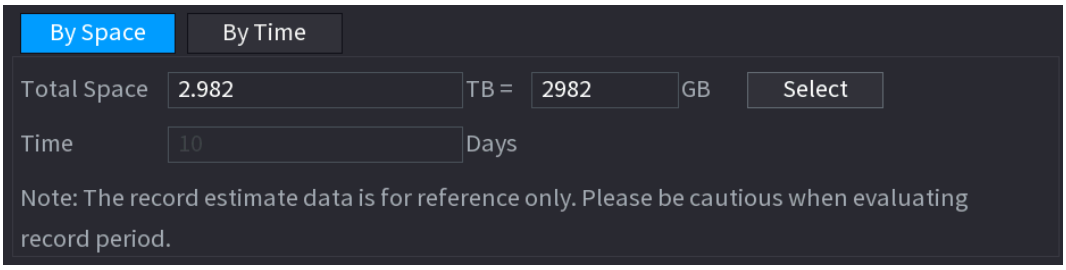
Figure 5-216 By space



Step 2 Click **Select**.

Step 3 Select the checkbox of the HDD that you want to calculate.

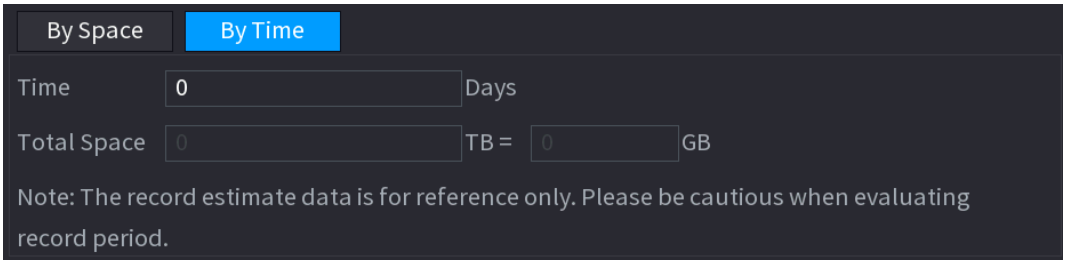
Figure 5-217 Recording time



5.12.7.2 Calculating HDD Capacity for Storage

Step 1 On the **Rec Estimate** interface, click the **By Time** tab.

Figure 5-218 By time



Step 2 In the **Time** box, enter the time period that you want to record.

In the **Total Space** box, the required HDD capacity is displayed.

5.12.8 FTP

You can store and view the recorded videos and snapshots on the FTP server.

Prerequisites

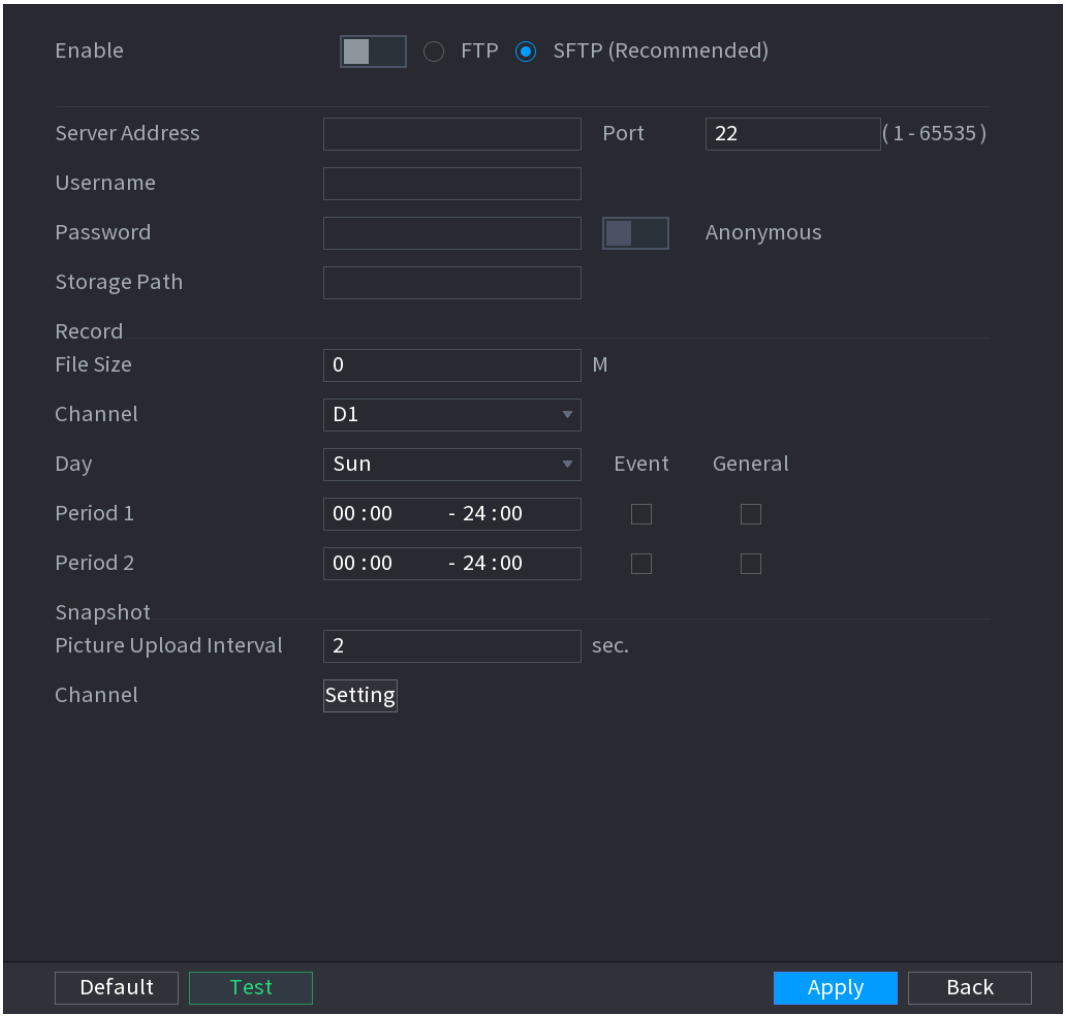
Purchase or download a FTP (File Transfer Protocol) server and install it on your PC.

For the created FTP user, you need to set the write permission; otherwise the upload of recorded videos and snapshots will be failed.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **FTP**.

Figure 5-219 FTP



Step 2 Configure the parameters.

Table 5-66 FTP parameters

Parameter	Description
Enable	Enable the FTP upload function.

Parameter	Description
FTP type	Select FTP type. ● FTP: Plaintext transmission. ● SFTP: Encrypted transmission (recommended).
Server Address	IP address of FTP server.
Port	Enter the port of the FTP server. ● FTP: The default is 21. ● SFTP: The default is 22.
Username	Enter the username and password to log in to the FTP server. If you enable the anonymity function, you can log in anonymously without entering the username and password.
Password	
Anonymous	
Storage Path	Create folder on FTP server. ● If you do not enter the name of remote directory, the system automatically creates the folders according to the IP and time. ● If you enter the name of remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.
File Size	Enter the length of the uploaded recorded video. ● If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. ● If the entered length is more than the recorded video length, the whole recorded video can be uploaded. ● If the entered length is 0, the whole recorded video will be uploaded.
Picture Upload Interval	● If this interval is longer than snapshot interval, the system takes the recent snapshot to upload. For example, the interval is 5 seconds, and snapshot interval is 2 seconds per snapshot, the system uploads the recent snapshot every 5 seconds. ● If this interval is shorter than snapshot interval, the system uploads the snapshot per the snapshot interval. For example, the interval is 5 seconds, and snapshot interval is 10 seconds per snapshot, the system uploads the snapshot every 10 seconds. ● To configure the snapshot interval, go to **Main Menu** > **CAMERA** > **Encode** > **Snapshot**.
Channel	Select the channel that you want to apply the FTP settings.
Day	Select the week day and set the time period that you want to upload the recorded files. You can set two periods for each week day.
Period 1, Period 2	
Record type	Select the record type (Alarm, Intel, MD, and General) that you want to upload. The selected record type will be uploaded during the configured time period.

Step 3 Click **Test** to validate the FTP connection.

If FTP connection failed, check the network and FTP settings.

Step 4 Click **Apply**.

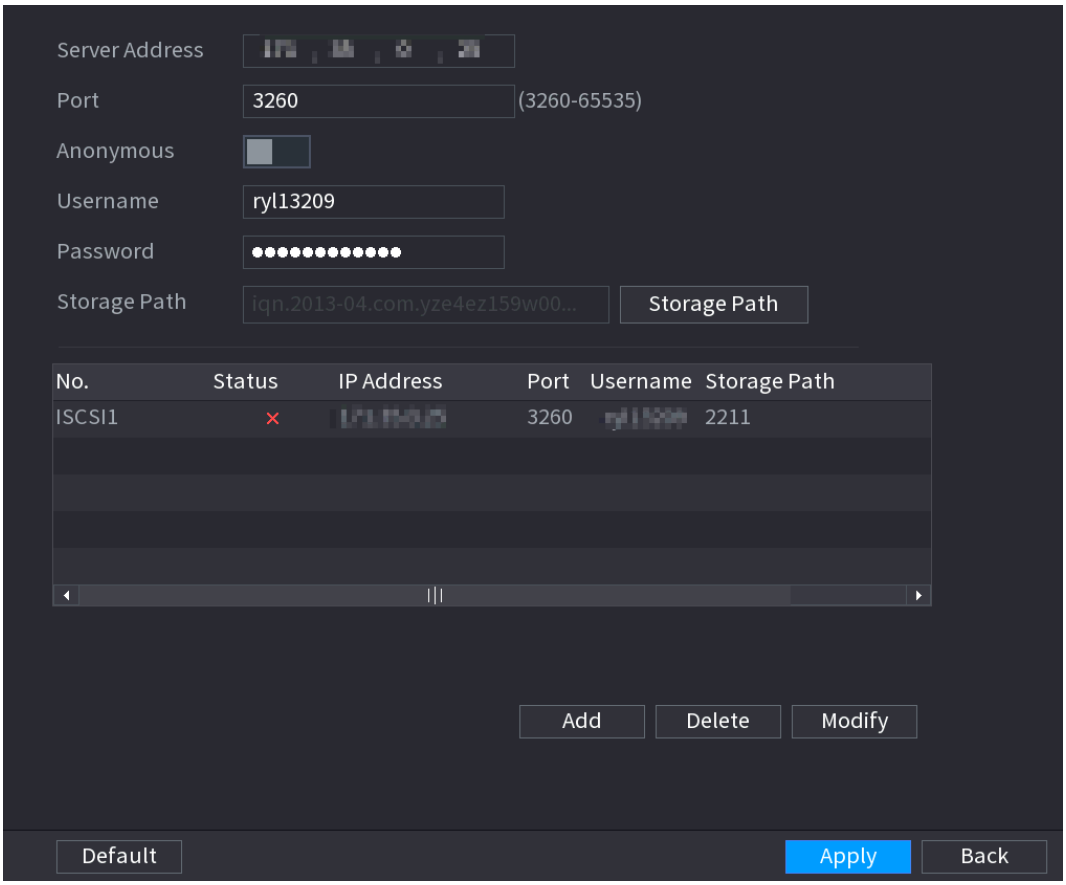
5.12.9 iSCSI

Internet Small Computer Systems Interface (iSCSI) is a transport layer protocol that works on top of the Transport Control Protocol (TCP), and enables block-level SCSI data transport between the iSCSI initiator and the storage target over TCP/IP networks. After the network disk is mapped to the NVR device through iSCSI, the data can be stored on the network disk.

This function is available on select models.

Step 1 Select **Main Menu** > **STORAGE** > **iSCSI**.

Figure 5-220 iSCSI



Step 2 Set parameters.

Table 5-67 iSCSI parameters

Parameter	Description
Server Address	Enter the server address of iSCSI server.
Port	Enter the port of iSCSI server, and the default value is 3260.
Storage Path	Click **Storage Path** to select a remote storage path. Each path represents an iSCSI shared disk and these paths are generated when created on the server
Username, Password	Enter the username and password of iSCSI server. If anonymous login is supported by iSCSI server, you can enable **Anonymous** to log in as an anonymous user.

Step 3 Click **Apply**.

5.13 Account

You can manage users, user group and ONVIF user, and set admin security questions.

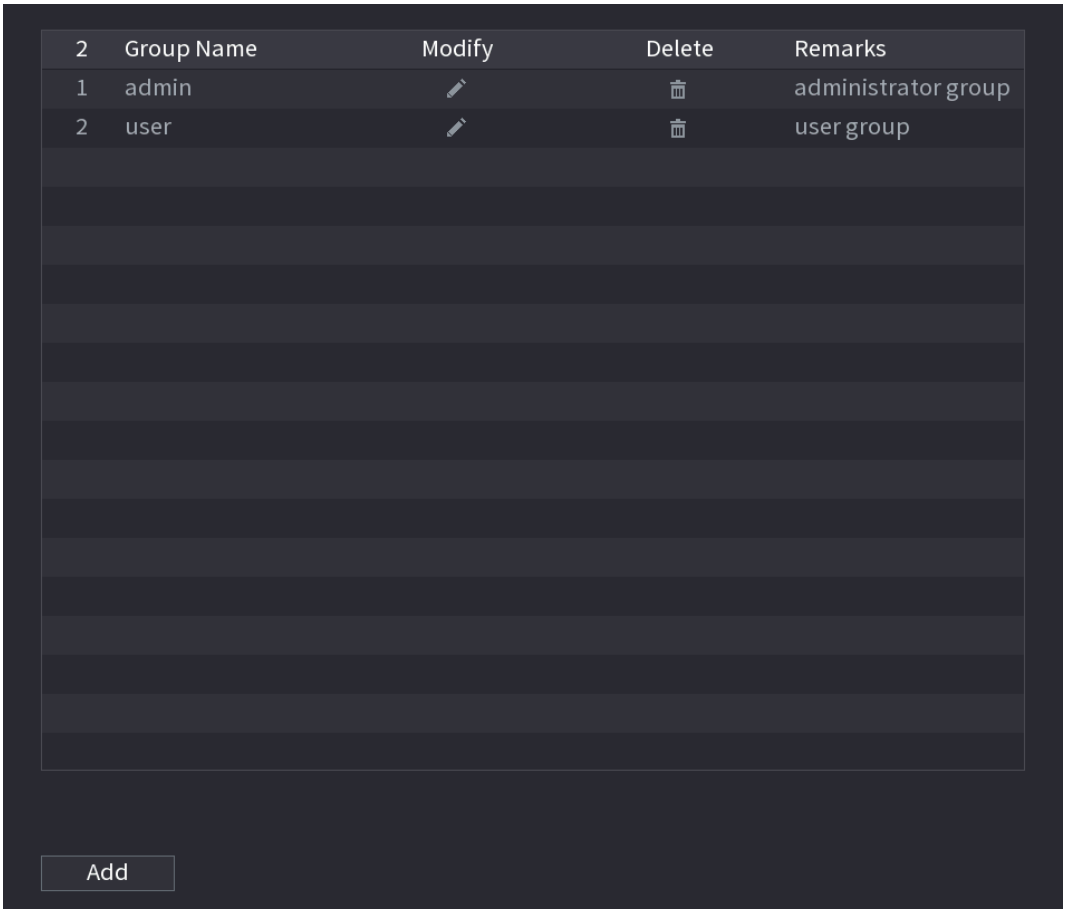
5.13.1 Group

The accounts of the Device adopt two-level management mode: user and user group. Every user must belong to a group, and one user only belongs to one group.

The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

Step 1 Select **Main Menu** > **ACCOUNT** > **Group**.

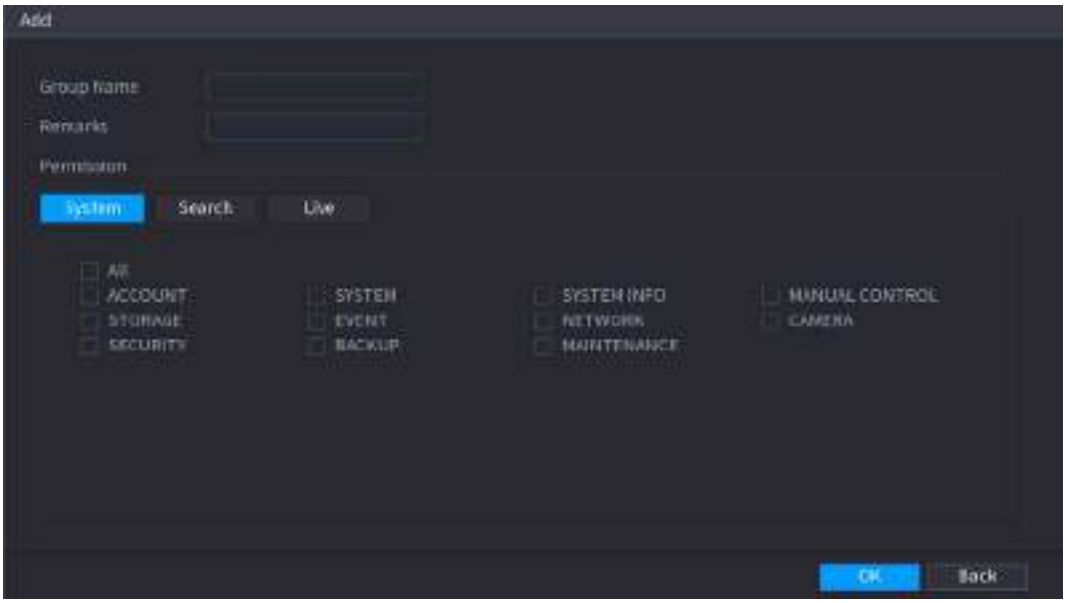
Figure 5-221 Group



Step 2 Click **Add**.

Step 3 Enter group name and then enter some remarks if necessary.

Figure 5-222 Add group



Step 4 Select the checkboxes to select permissions.

Step 5 Click **OK**.

Click to modify the corresponding group information, click to delete the group.

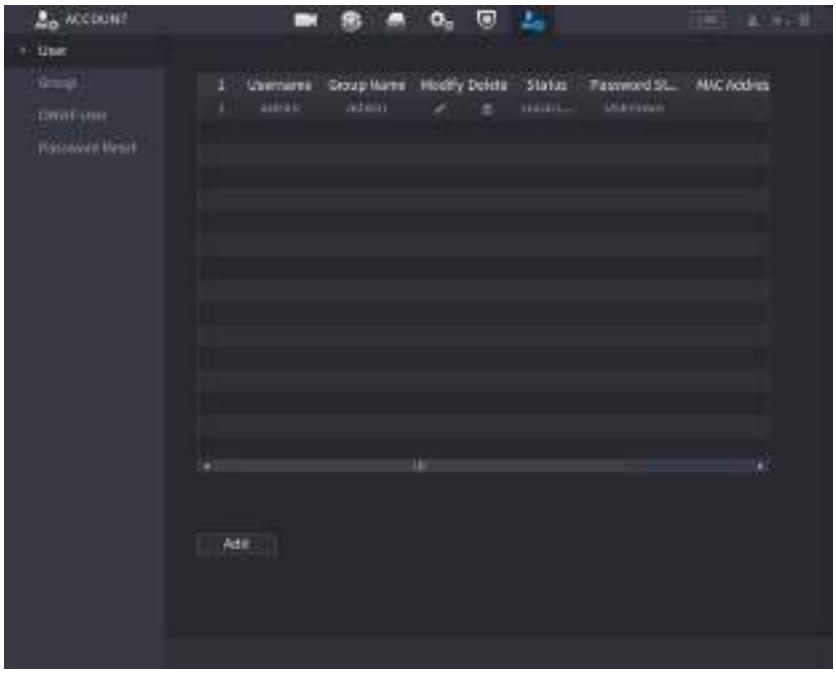
5.13.2 User

5.13.2.1 Adding User

Procedure

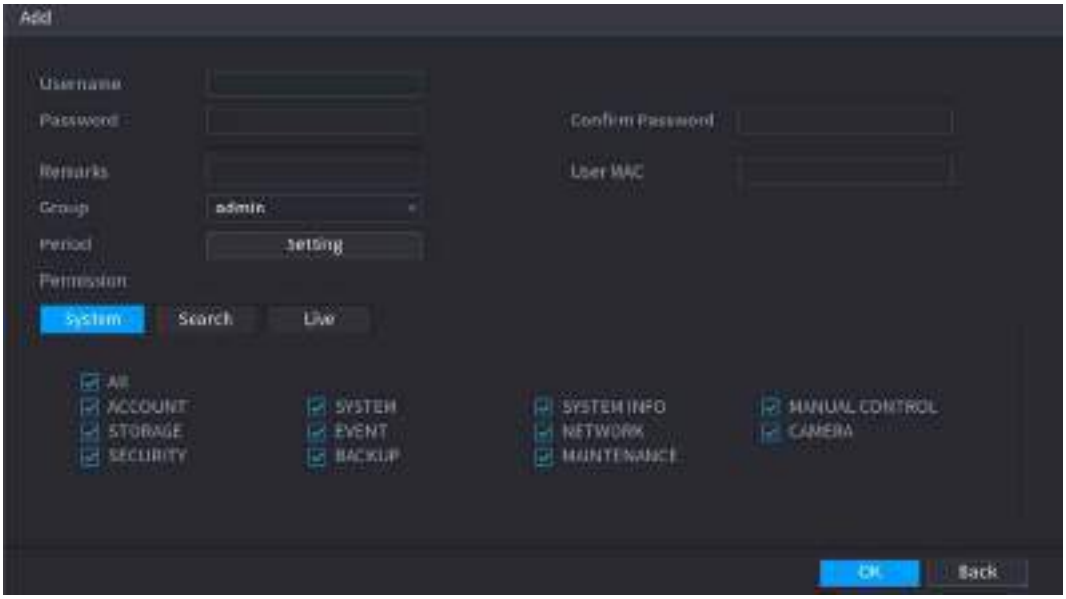
Step 1 Select **Main Menu** > **ACCOUNT** > **User**.

Figure 5-223 User



Step 2 Click **Add**.

Figure 5-224 Add user



Step 3 Configure the parameters.

Table 5-68 Parameters of adding user

Parameter	Description
Username	Enter a username and password for the account.
Password	
Confirm Password	Enter the password again to confirm it.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address
Group	Select a group for the account. The user rights must be within the group permissions.
Period	Click **Setting** to define a period during which the new account can log in to the Device. The new account cannot access the device during other periods.
Permission	Select the checkboxes to grant permissions to the user. To manage the user account easily, when defining the user account permission, do not give the authority to the common user account higher that the advanced user account.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete the user.

5.13.2.2 Changing Password

We recommend you change the password regularly to enhance device security.

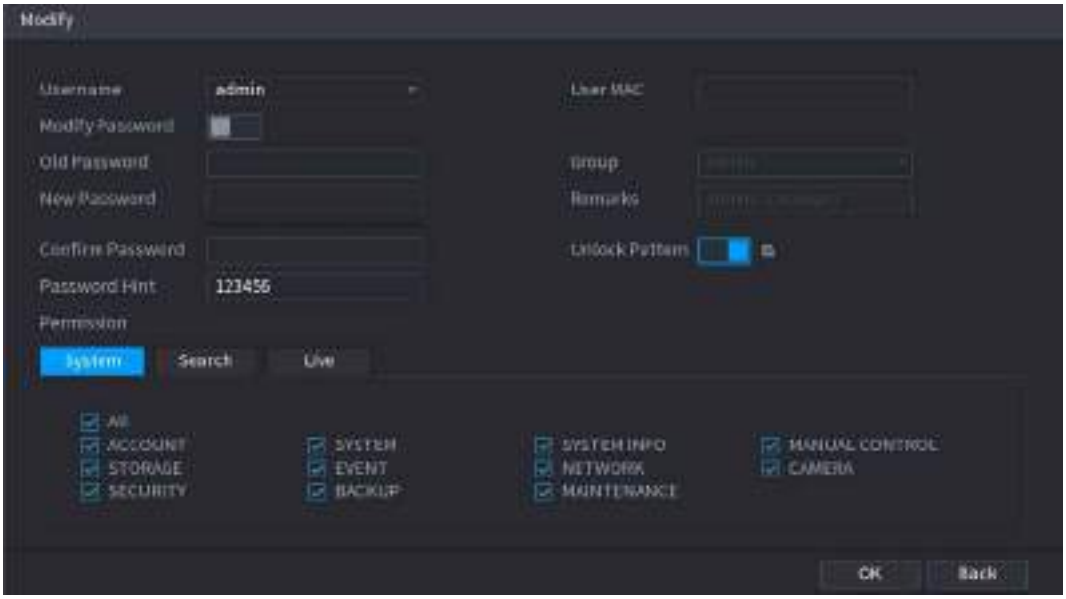
Users with account permissions can change the password of other users.

Procedure

Step 1 Select **Main Menu** > **ACCOUNT** > **User**.

Step 2 Click of the corresponding user.

Figure 5-225 Change password



Step 3 Click to enable the **Modify Password** function.

Step 4 Enter old password and then enter new password twice.

- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- For your device security, create a strong password.
- Check the box to enable Unlock Pattern function, click .

Step 5 Click to enable **Unlock Pattern** and then click to draw the pattern.

Step 6 Click **OK**.

5.13.3 Resetting Password

You can reset the password when you forget the password.

5.13.3.1 Enabling Password Reset

Enable the password reset function and configure the linked email address and security questions that are used to reset the password.

Step 1 Select **Main Menu** > **ACCOUNT** > **Password Reset**.

Step 2 Click to enable the password reset function.

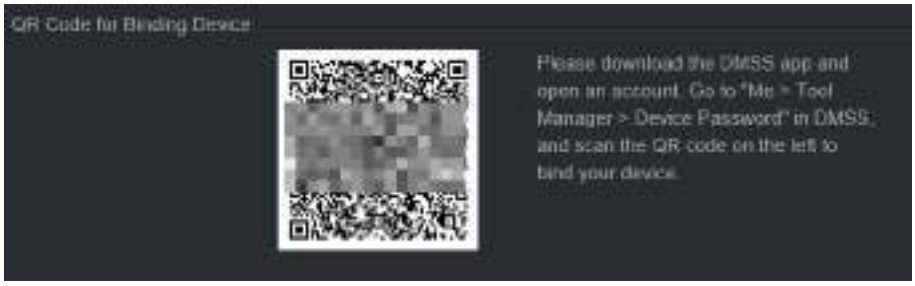
This function is enabled by default.

Step 3 Enter an email address to receive the security code used to reset the password.

Step 4 Configure security questions and answers.

Step 5 (Optional) Follow the on-screen instructions to bind the Device to DMSS app.

Figure 5-226 Bind device



Step 6 Click **OK**.

5.13.3.2 Resetting Password on Local Interface

Procedure

Step 1 Right-click the live page and then select any item on the shortcut menu.

- If you have configured unlock pattern, the unlock pattern login window is displayed. Click **Forgot Pattern** to switch to password login.
- If you did not configure unlock pattern, the password login window is displayed.

Figure 5-227 Pattern login

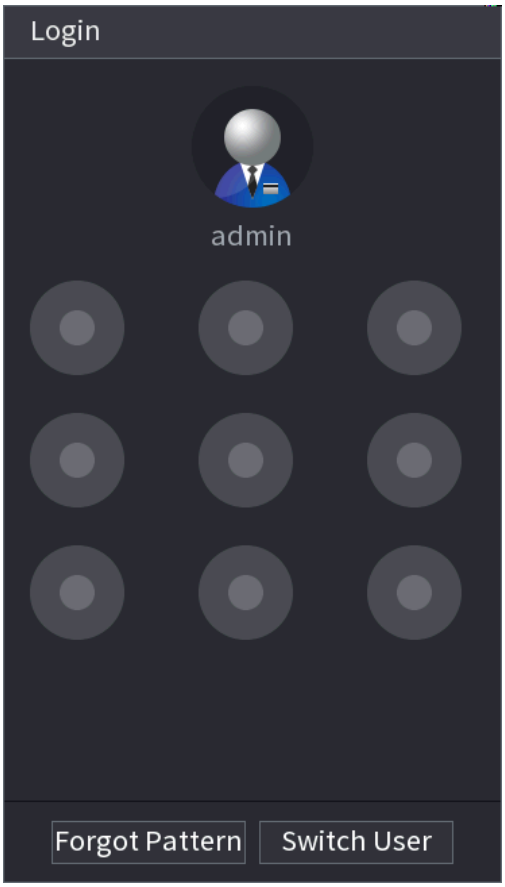
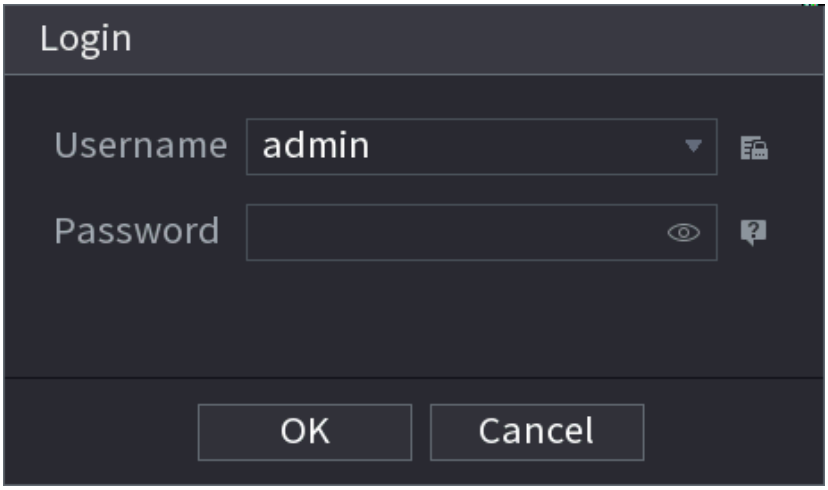


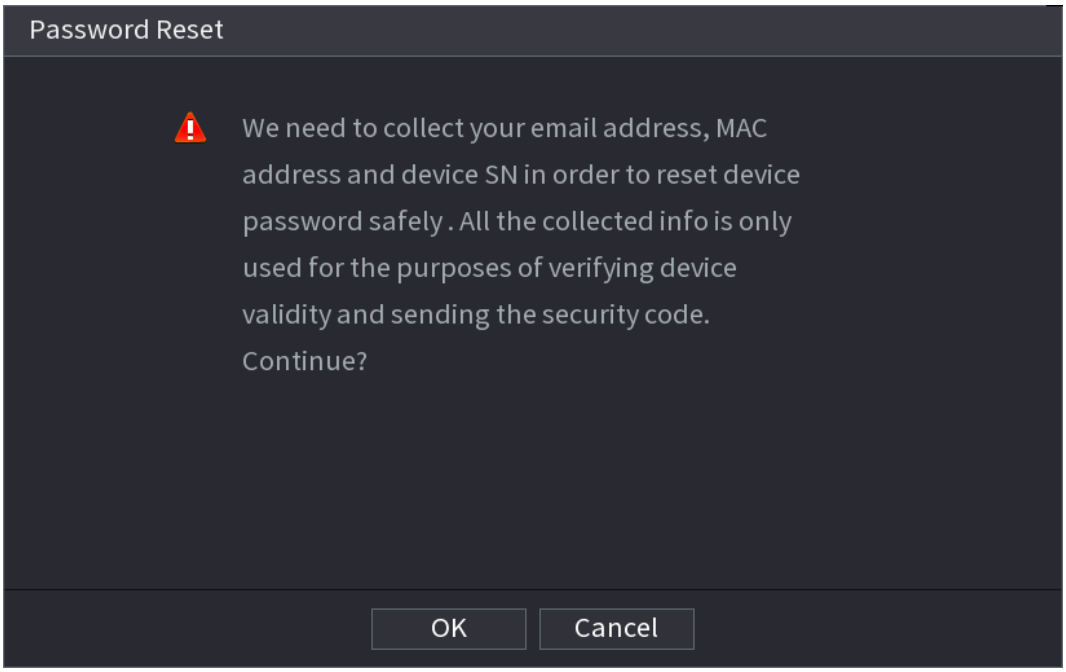
Figure 5-228 Password login



Step 2 Click .

- If you have set the linked email address, the system will notify you of data collection required for resetting password. Click **OK**.
- If you did not set the linked email address, the system prompts you to enter an email address. Enter the email address and then click **Next**. Then the system will notify you of data collection required for resetting password.

Figure 5-229 Notification on data colleciton



Step 3 Read the prompt and then click **OK**.

Step 4 Click **Next**.

After clicking **Next**, the system will collect your information for password reset, purpose and the information includes but not limited to email address, MAC address, and device serial number. Read the prompt carefully before clicking **Next**.

Step 5 Reset the password.

- Email.
  Select **Email** as the reset mode, and then follow the on-screen instructions to get the security code in your linked email address. After that, enter the security code in the **Security Code** box.

Figure 5-230 Reset mode (email)

- App.

Select **QR Code for Binding Device** as the reset mode, and then follow the on-screen instructions to get the security code on the DMSS app. After that, enter the security code in the **Security Code** box.

Figure 5-231 Reset mode (app)

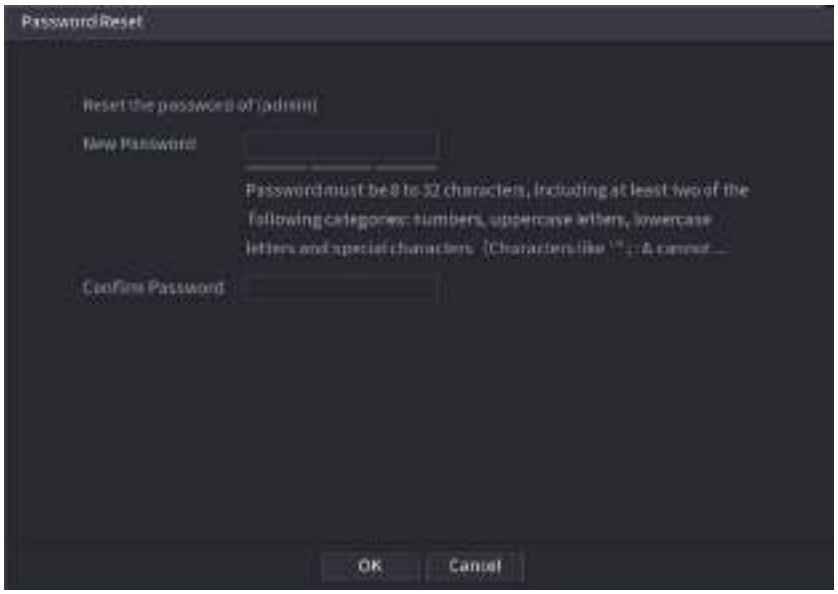
- Security question
  Select **Security Question** as reset mode and then answer the security questions.

  If you did not configure the security questions in advance , **Security Question** is not available on the **Reset Mode** list.

Step 6 Click **Next**.

Step 7 Enter the new password and then enter the password again to confirm it.

Figure 5-232 Enter new password



Step 8 Click **OK**.

The password is reset.

Step 9 (Optional) When the system prompts whether to synchronize the password with the remote devices accessed through the private protocol, click **OK** to synchronize the

password.

5.13.4 ONVIF User

Background Information

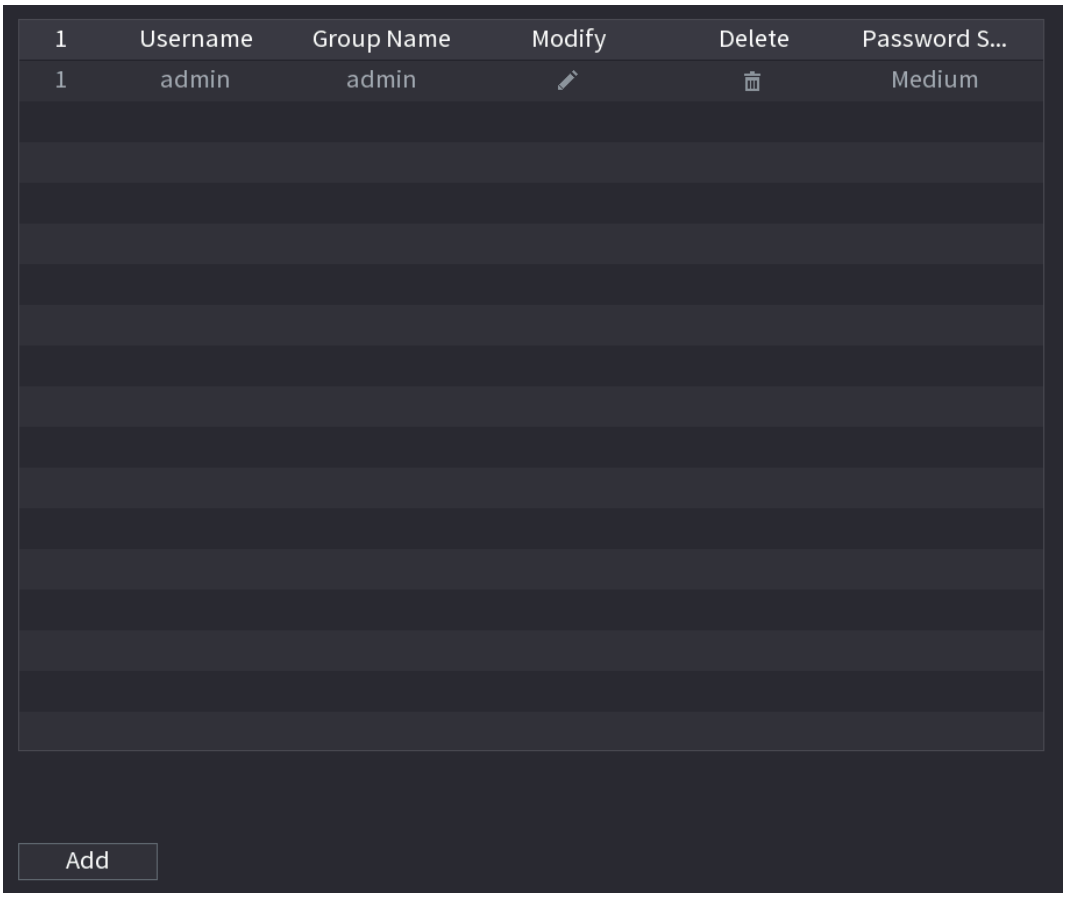
To connect the camera from the third party to the NVR via the ONVIF protocol, you need to use a verified ONVIF account.

The default ONVIF user is **admin**. It is created after you initialize the NVR and cannot be deleted.

Procedure

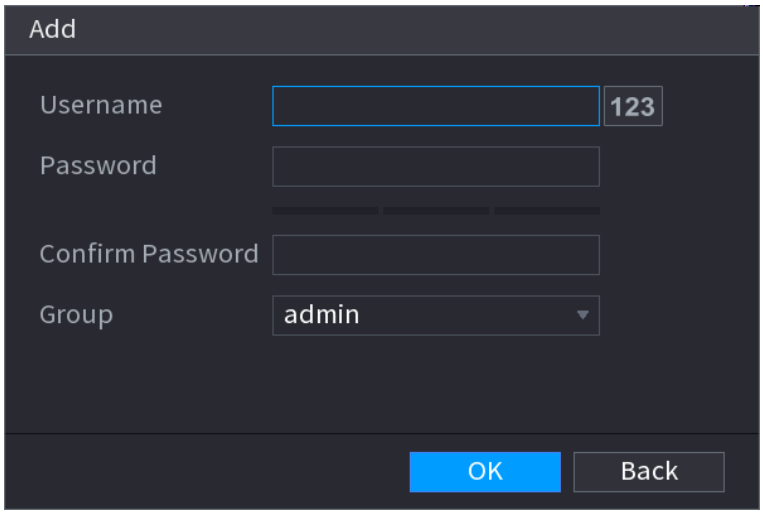
Step 1 Select **Main Menu** > **ACCOUNT** > **ONVIF User**.

Figure 5-233 ONVIF user



Step 2 Click **Add**.

Figure 5-234 Add ONVIF user



Step 3 Configure username, password and user group.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete current user.

5.14 Security

5.14.1 Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information on the security status of the device.

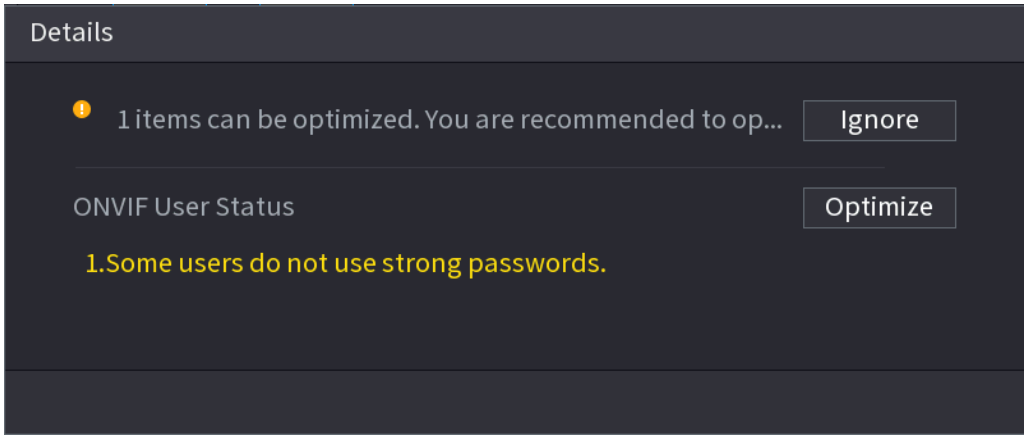
Detecting User and Service

Green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- User Status: When one of device users or ONVIF users uses weak password, the icon will be in orange to warn risk. You can click **Details** to optimize or ignore the risk warning.

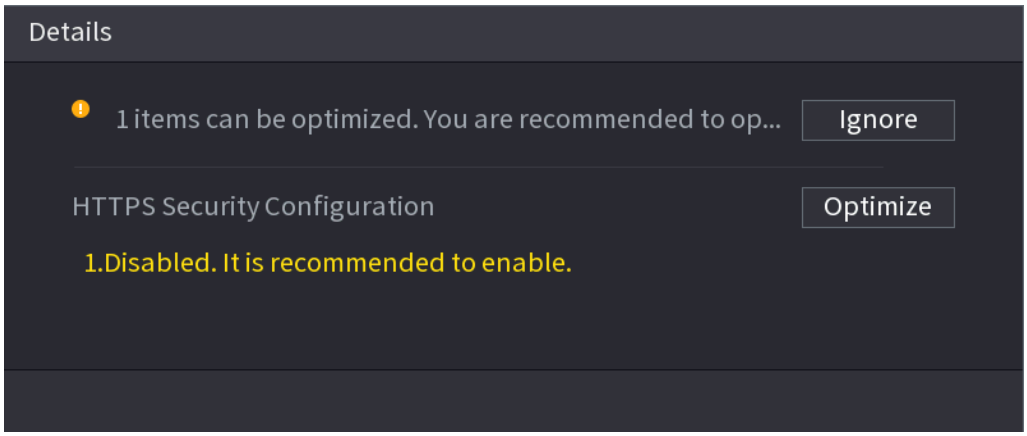
Figure 5-235 Security status

Figure 5-236 Details (1)



- Configuration Security: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

Figure 5-237 Details (2)



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, point to the icon to see the on-screen instructions.

Re-scanning Security Status

You can click **Rescan** to scan security status.

5.14.2 System Service

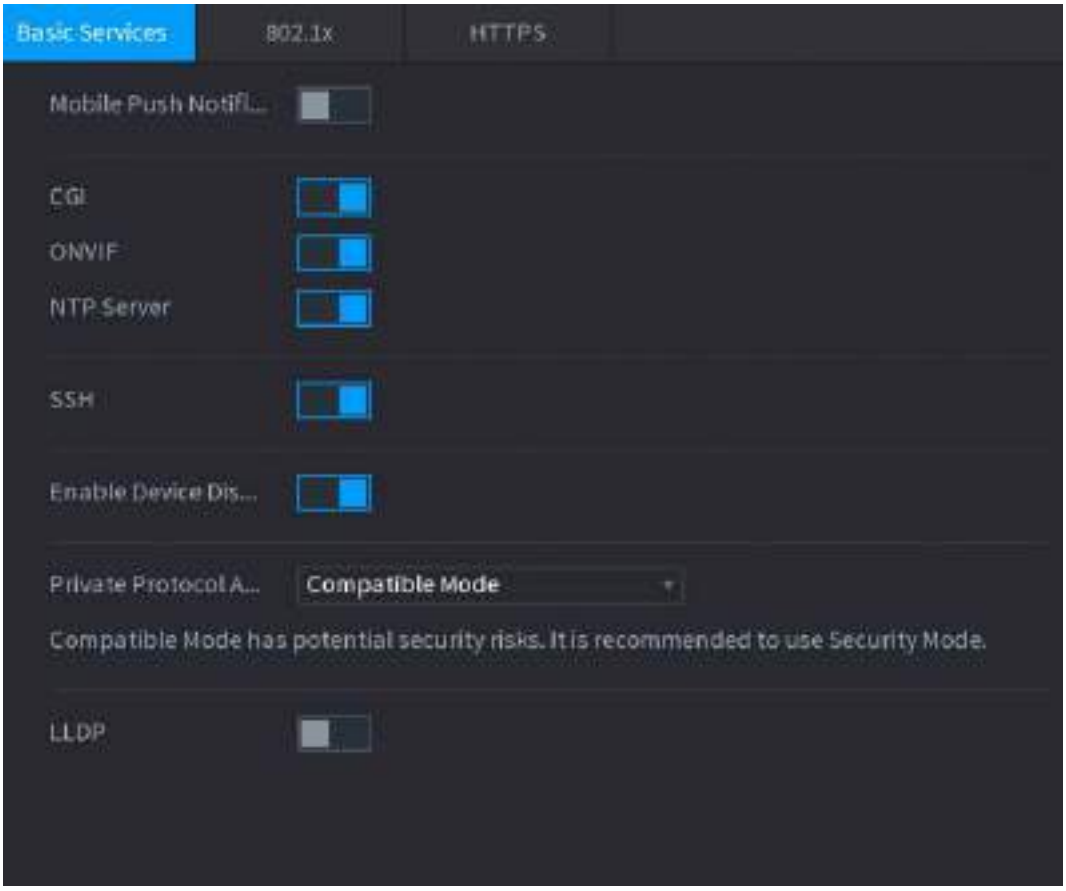
You can set NVR basic information such as basic services, 802.1x and HTTPS.

5.14.2.1 Basic Services

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **Basic Services**.

Figure 5-238 Basic services



Step 2 Enable the system services.

⚠

There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled. Disable these functions when they are not needed.

Table 5-69 Basic service parameters

Parameter	Description
Mobile Push Notifications	After enabling this function, the alarm triggered by the NVR can be pushed to a mobile phone. This function is enabled by default.
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default.
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default.
NTP Server	After enabling this function, a NTP server can be used for time synchronization. This function is enabled by default.
SSH	After enabling this function, you can use SSH service. This function is disabled by default.
Enable Device Discovery	After enabling this function, the NVR can be found by other devices through searching.

Parameter	Description
Private Protocol Authentication Mode	• Security Mode (Recommended): Uses Digest access authentication when connecting to NVR. • Compatible Mode: Select this mode when the client does not support Digest access authentication.
LLDP	Enable the LLDP service. The Link Layer Discovery Protocol (LLDP) allows two different devices to collect hardware and protocol information about neighboring devices, which is useful in troubleshooting the network.

Step 3 Click **Apply**.

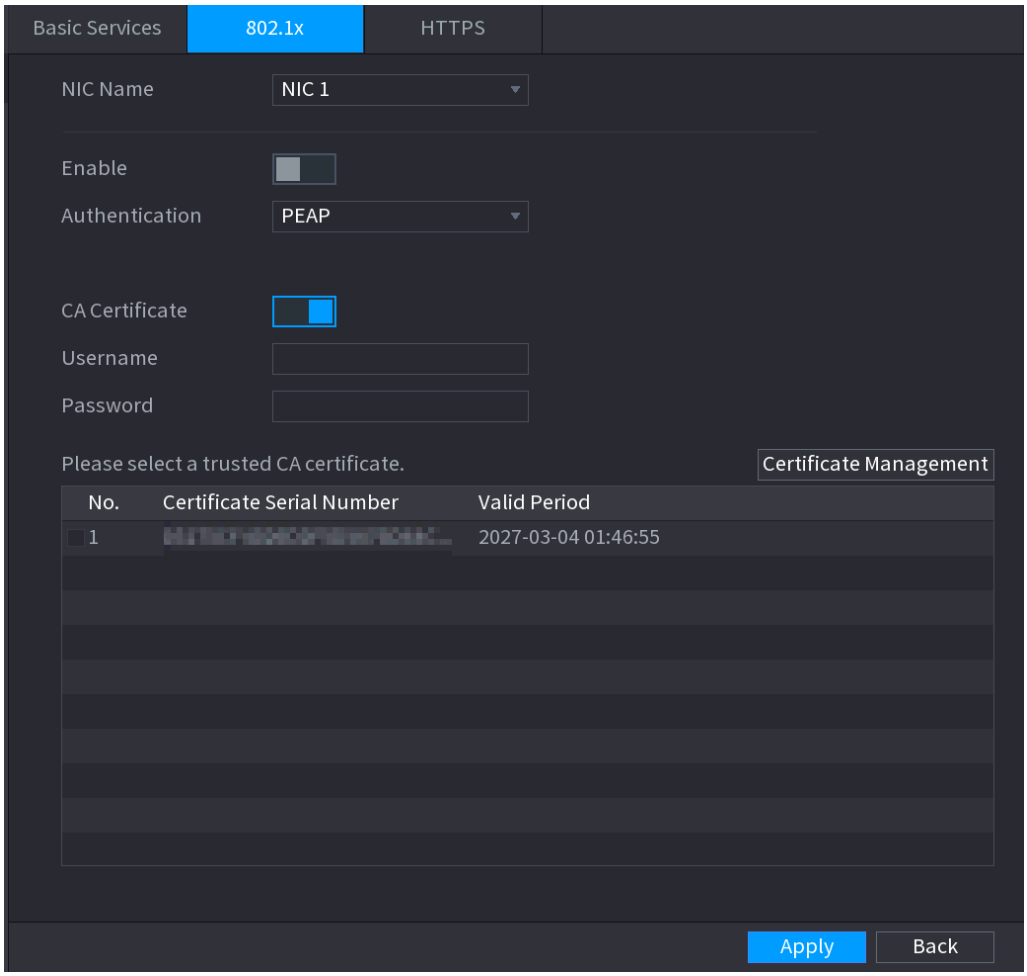
5.14.2.2 802.1x

The Device needs to pass 802.1x certification to enter the LAN.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **802.1x**.

Figure 5-239 802.1x



Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters.

Table 5-70 802.1x parameters

Parameter	Description
Authentication	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details about importing and creating a certificate, see "5.14.4 CA Certificate".
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

Step 4 Click **Apply**.

5.14.2.3 HTTPS

Background Information

We recommend you enable HTTPS function to enhance system security.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **HTTPS**.

Figure 5-240 HTTPS

Step 2 Enable HTTPS function.

Step 3 (Optional) Enable **Compatible with TLSv1.1 and earlier versions** to allow protocol compatibility.

Step 4 Click **Certificate Management** to create or import a HTTPS certificate from USB drive. For details about importing or creating a CA certificate, see "5.14.4 CA Certificate".

Step 5 Select a HTTPS certificate.

Step 6 Click **Apply**.

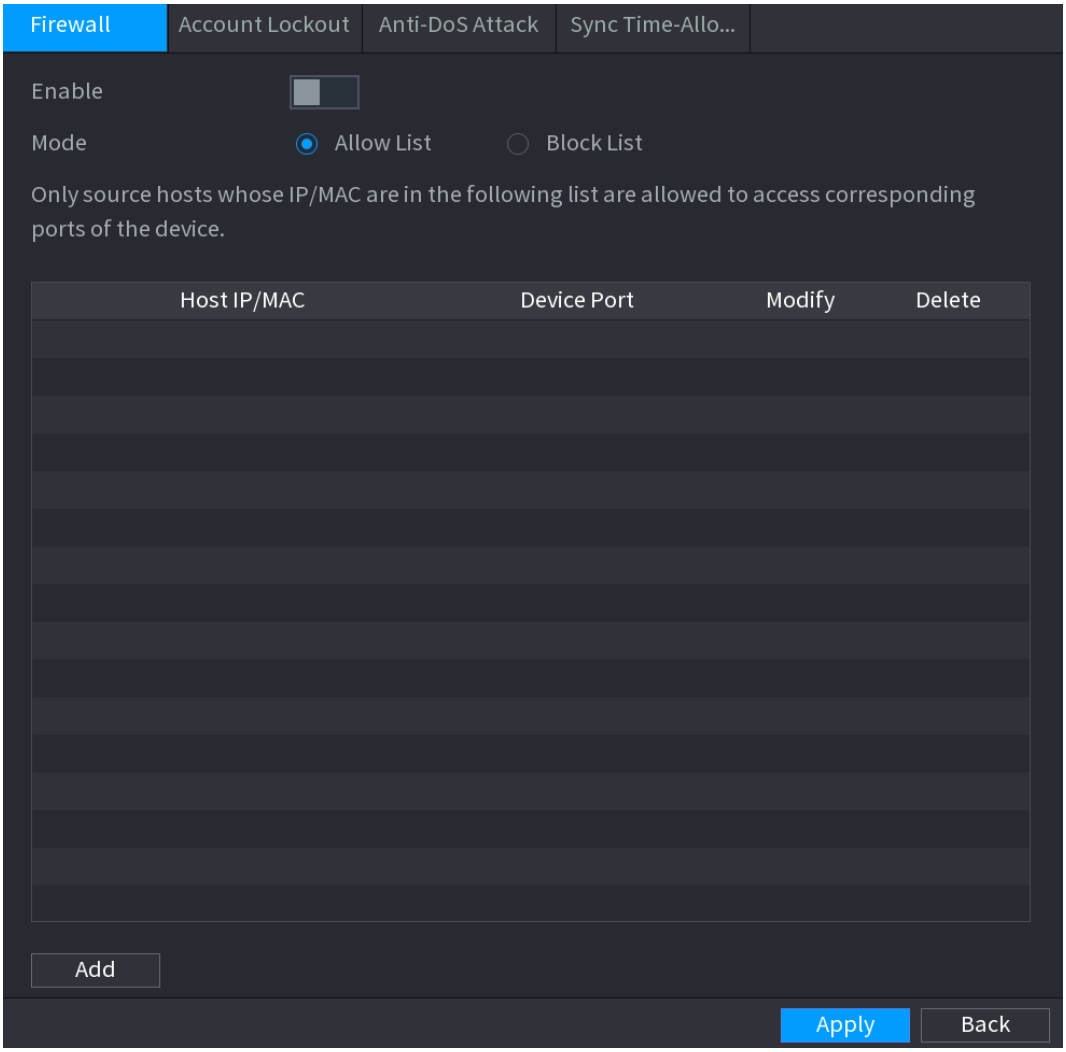
5.14.3 Attack Defense

5.14.3.1 Firewall

You can configure the hosts that are allowed or prohibited to access the Device.

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Firewall** .

Figure 5-241 Firewall



Step 2 Click  to enable the firewall.

Step 3 Select a firewall mode.

- **Allow List**: The hosts on the allowlist can access the Device.
- **Block List**: The hosts on the blocklist are prohibited to access the Device.

Step 4 Click **Add** and then select a type for the allowlist or blocklist.

You can allow or prohibit hosts through a specific IP address, a network segment, or a MAC address.

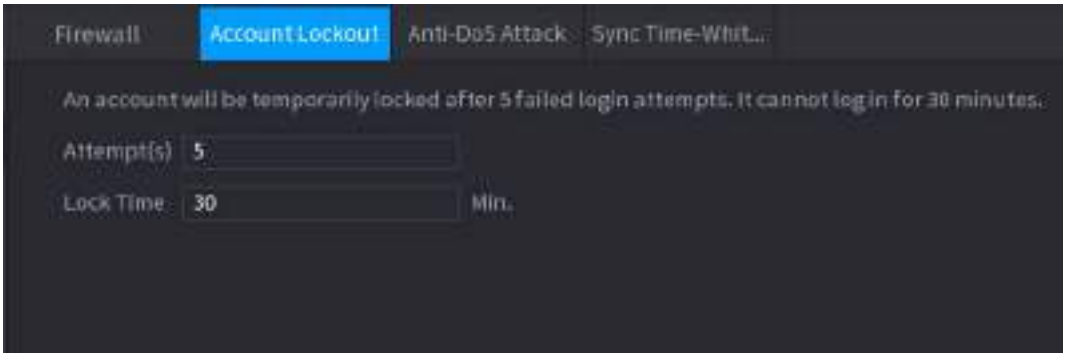
- IP address.
  Enter the IP address, start port and end port, and then click **OK**.
- IP segment.
  Enter the start address and end address, starting port and ending port, and then click **OK**.
- MAC address.
  Enter the MAC address, and then click **OK**.

Step 5 Click **Apply**.

5.14.3.2 Account Lockout

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Account Lockout**.

Figure 5-242 Account lockout



Step 2 Set parameters.

Table 5-71 Account lockout parameters

Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number.
Lock Time	Set how long the account is locked for.

Step 3 Click **Apply**.

5.14.3.3 Anti-Dos Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attack.

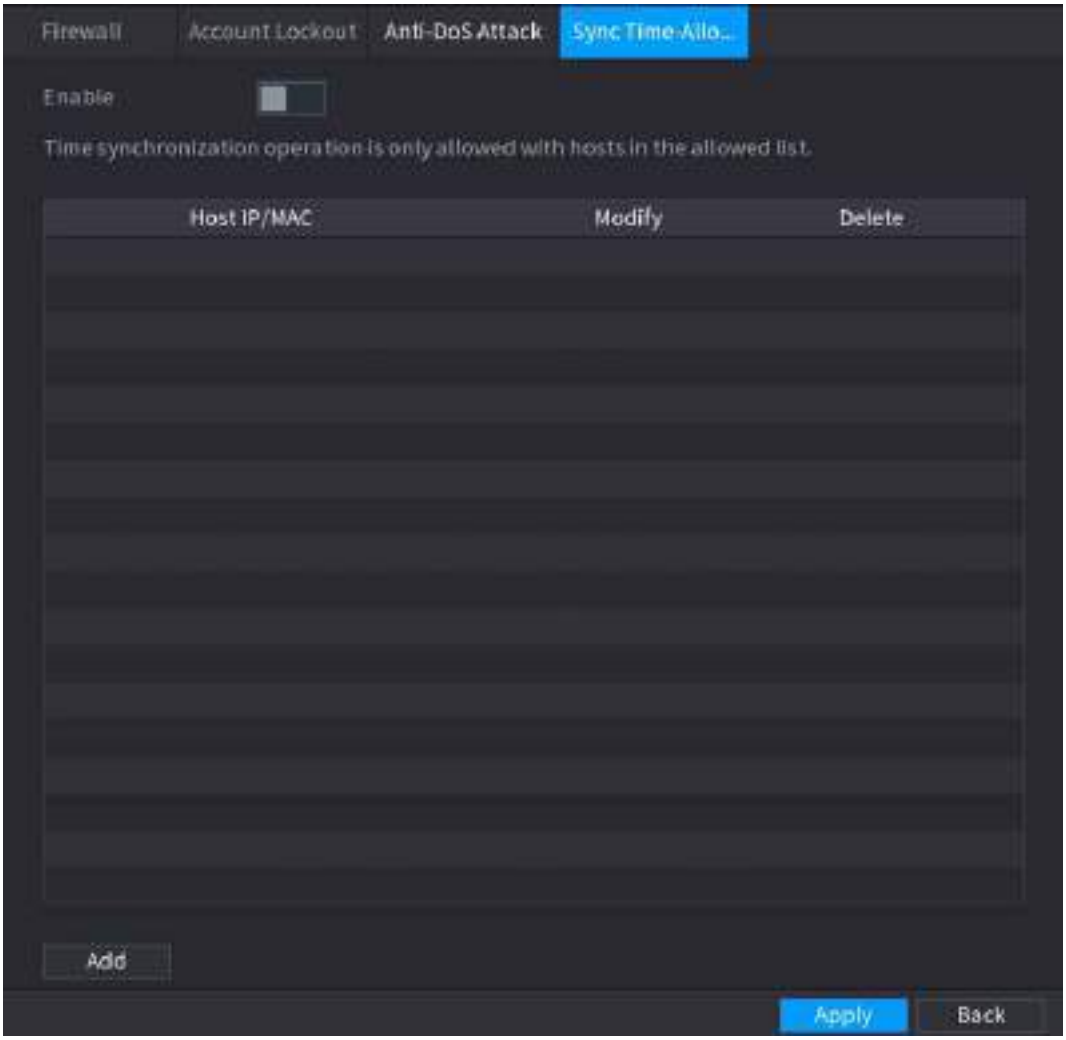
Figure 5-243 Anti-Dos Attack

5.14.3.4 Sync Time-Allowlist

You can configure which hosts are allowed to synchronize time with the Device.

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Sync Time-Allowlist**.

Figure 5-244 Sync Time-Allowlist



Step 2 Click  to enable the function.

Step 3 Click **Add** to add trusted hosts for time synchronization.

- If you set **Type** to **IP Address**, enter the IP address, and then click **OK**.
- If you set **Type** to **IP Segment**, enter the start address and end address, and then click **OK**.

Step 4 Click **Apply**.

5.14.4 CA Certificate

5.14.4.1 Device Certificate

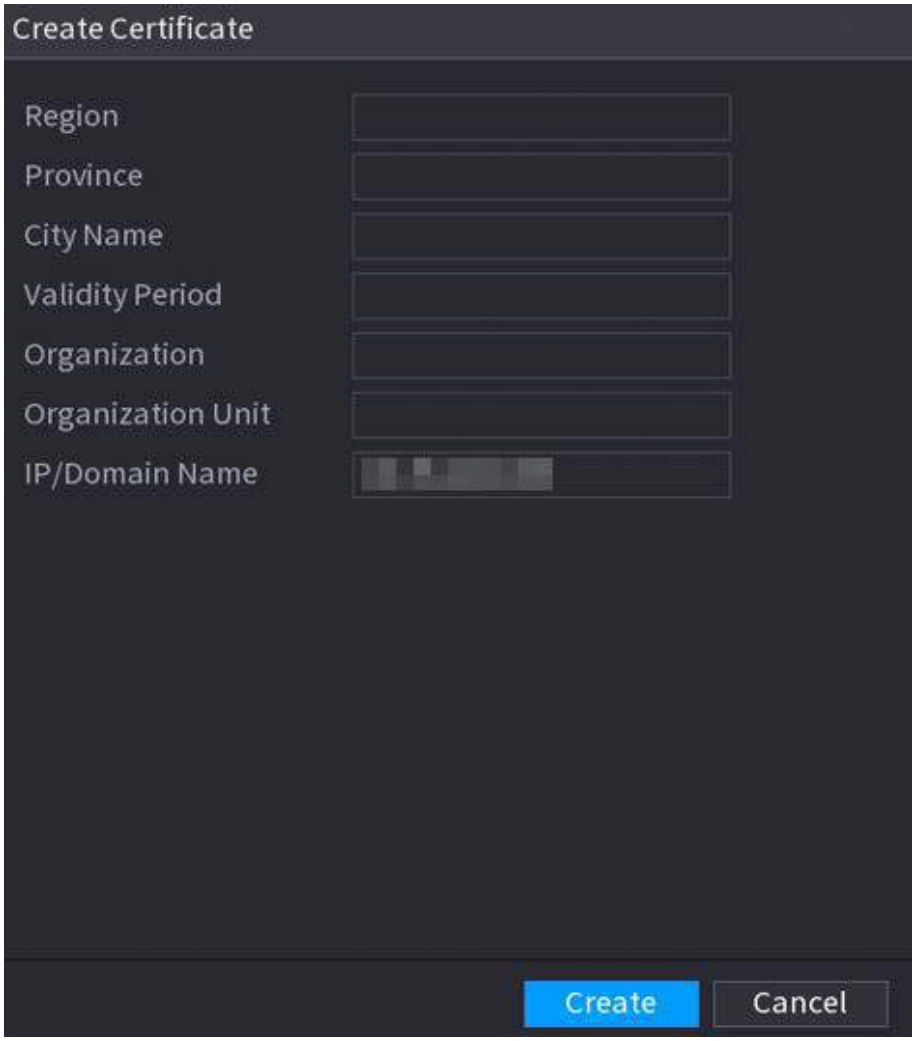
Create Certificate

1. Select **Main Menu** > **SECURITY** > **CA Certificate** > **Device Certificate**.

Figure 5-245 Device certificate

2. Click **Create Certificate**.

Figure 5-246 Create certificate



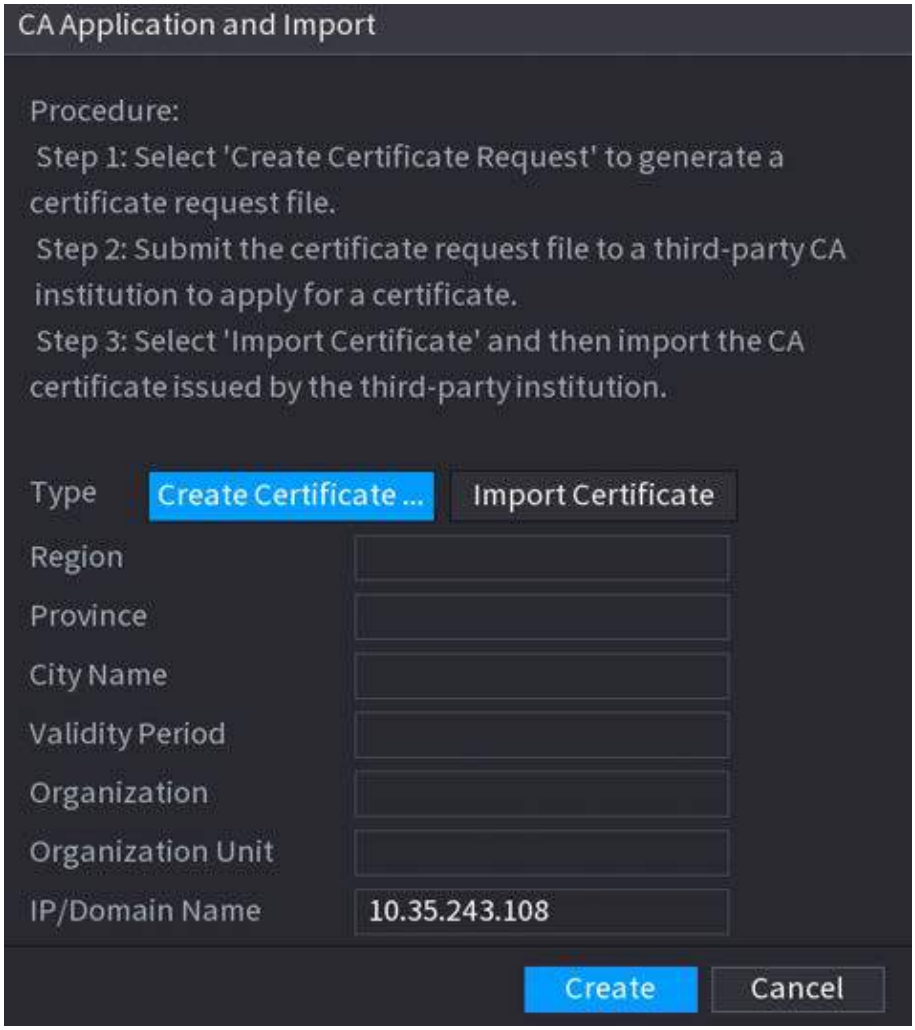
3. Configure the parameters.
4. Click **Create**.

CA Application and Import

Click **CA Application and Import** and then follow the on-screen instructions to finish CA application

and import.

Figure 5-247 CA application and import



Import Third-Party Certificate

1. Click **Import Third-Party Certificate**
2. Configure the parameters.

Table 5-72 Parameters for importing third-party certificate

Parameter	Description
Path	Click **Browse** to find the third-party certificate path on the USB drive.
Private Key	Click **Browse** to find the third-party certificate private key on the USB drive.
Private Key Password	Input the private key password.

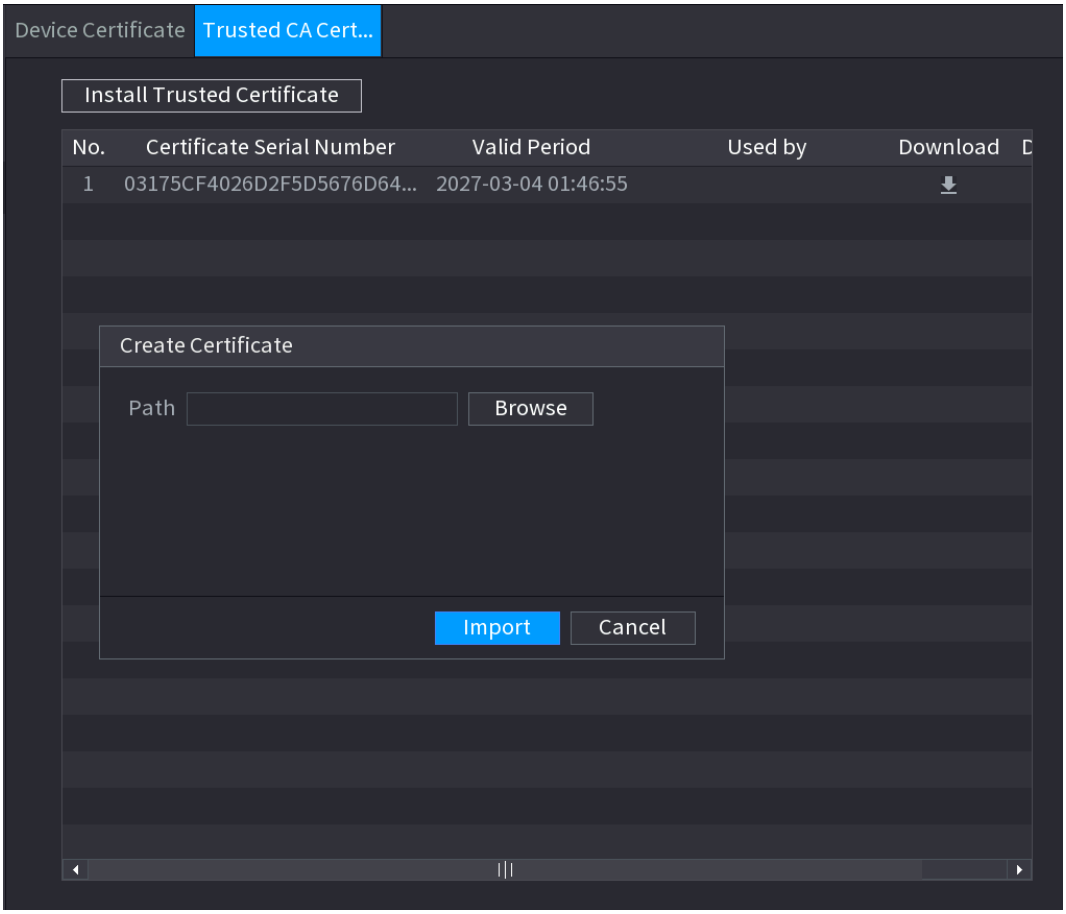
3. Click **Create**.

5.14.4.2 Trusted CA Certificate

Step 1 Select **Main Menu** > **SECURITY** > **CA Certificate** > **Trusted CA Certificate**.

Step 2 Click **Install Trusted Certificate**.

Figure 5-248 Create certificate



Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import**.

5.14.5 Audio/Video Encryption

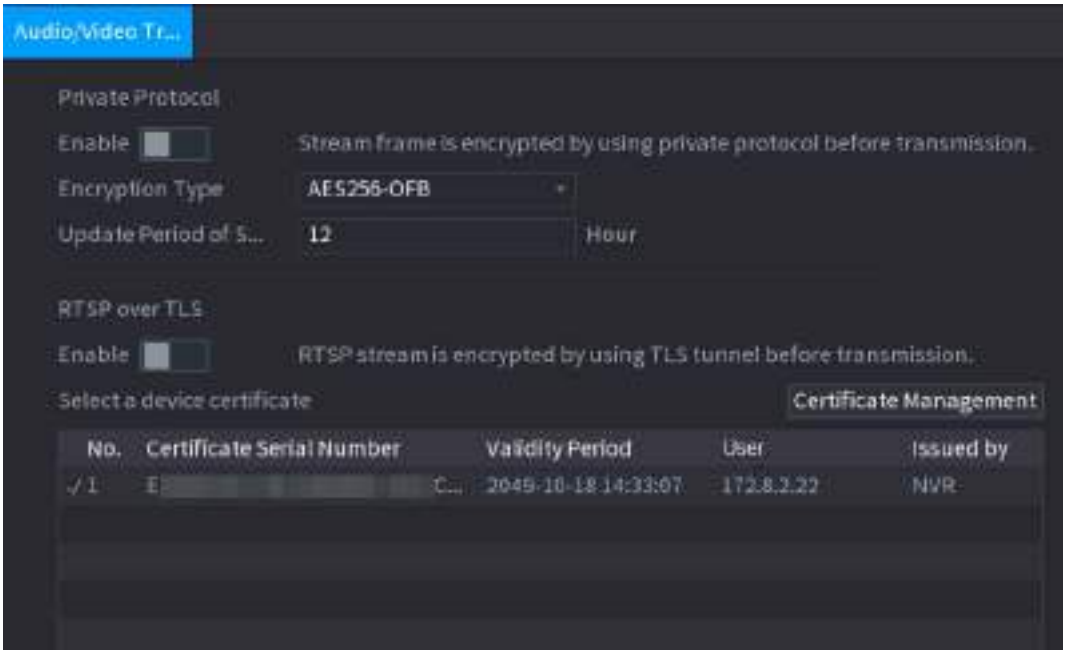
Background Information

The Device supports audio and video encryption during data transmission.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **AUDIO/VIDEO ENCRYPTION** > **Audio/Video Transmission**.

Figure 5-249 Audio and video transmission



Step 2 Configure parameters.

Table 5-73 Audio and video transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "5.14.4.1 Device Certificate".

Step 3 Click **Apply**.

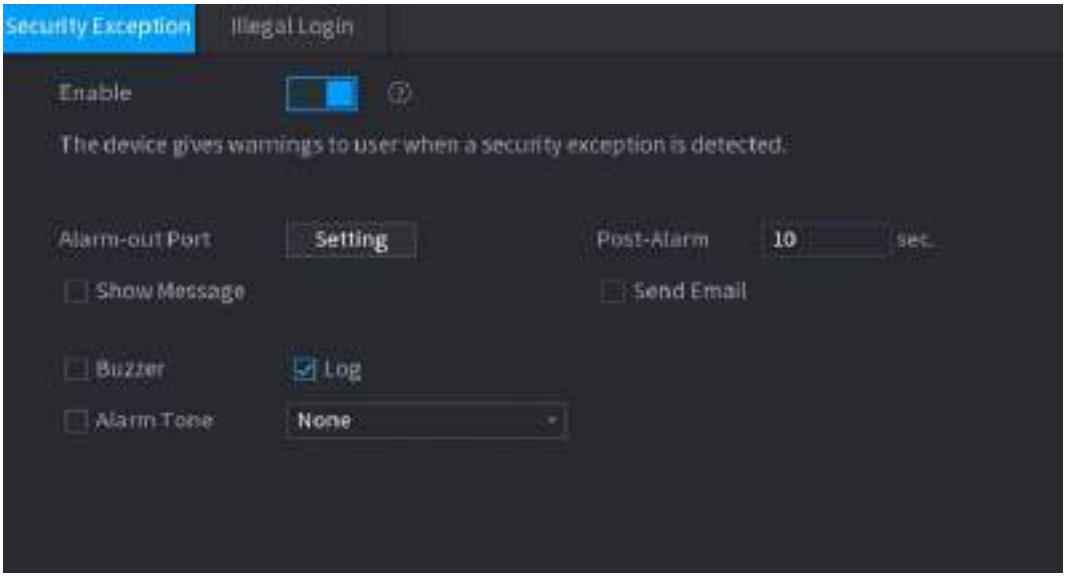
5.14.6 Security Warning

5.14.6.1 Security Exception

The Device gives warnings to the user when a security exception occurs.

Step 1 Select **Main Menu** > **SECURITY** > **Security Warning** > **Security Exception**.

Figure 5-250 Security exception



Step 2 Click to enable the function.

Click to view the list of security exception events.

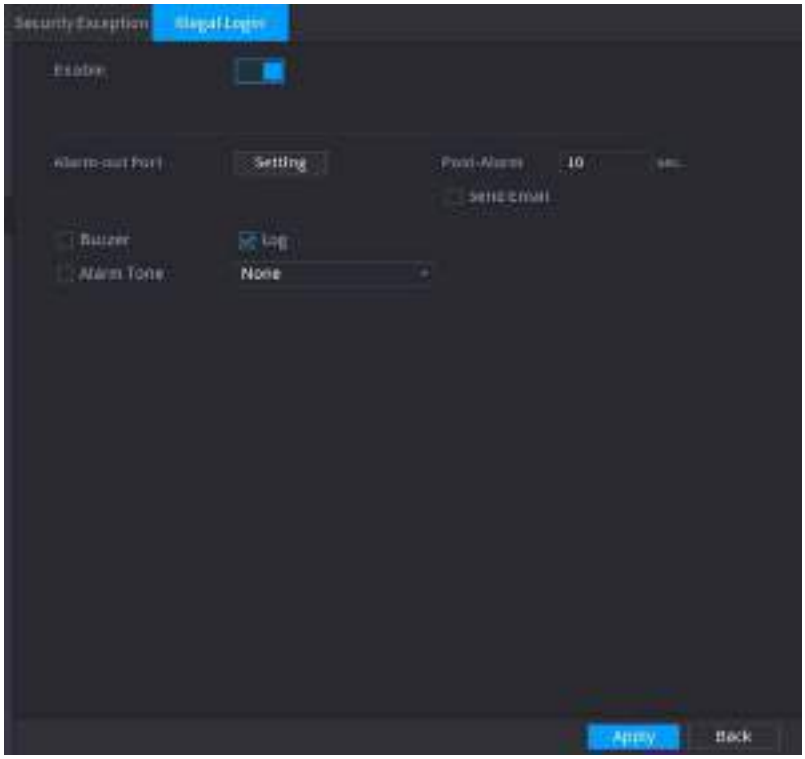
Step 3 Configure alarm linkage actions. For details, see Table 5-42.

Step 4 Click **Apply**.

5.14.6.2 Illegal Login

Step 1 Select **Main Menu** > **SECURITY** > **Security Warning** > **Illegal Login**.

Figure 5-251 Illegal login



Step 2 Click to enable the function.

Step 3 Configure alarm linkage actions. For details, see Table 5-42.

Step 4 Click **Apply**.

5.15 System

5.15.1 General

You can set NVR basic information such as system date and holiday.

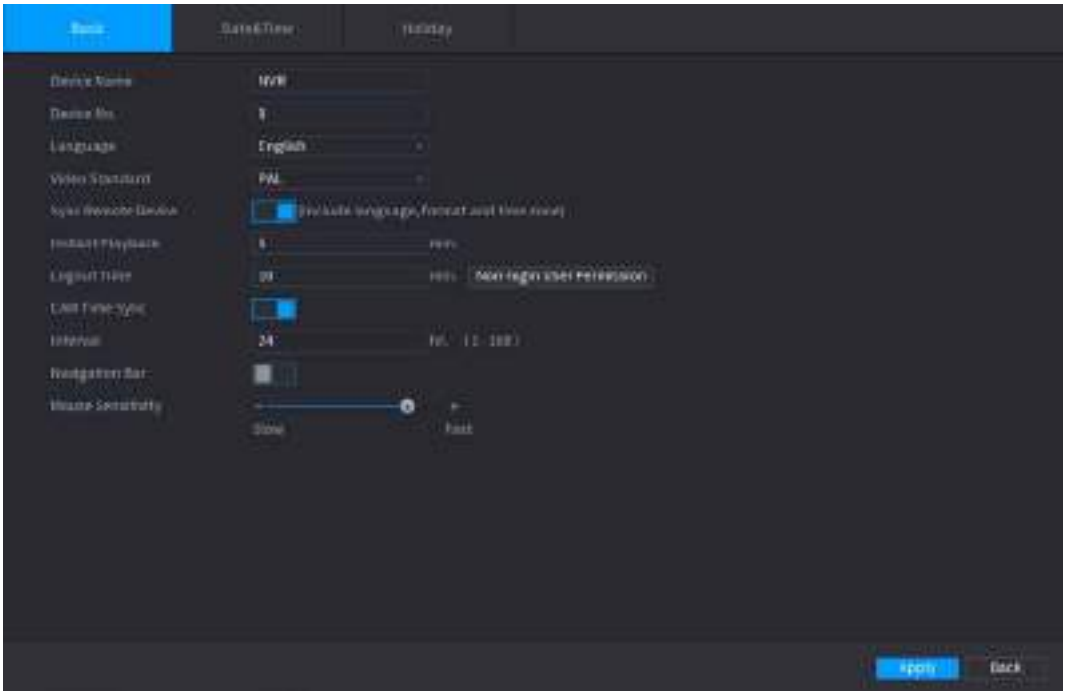
5.15.1.1 General

Background Information

You can set device basic information such as device name, and serial number.

Step 1 Select **Main Menu** > **SYSTEM** > **General** > **Basic**.

Figure 5-252 Basic settings



Step 2 Set parameters.

Table 5-74 Basic parameters

Parameter	Description
Device Name	Enter the Device name.
Device No.	Enter a number for the Device.
Language	Select a language for the Device system.
Video Standard	Select **PAL** or **NTSC** as needed.
Sync Remote Device	Enable this function; the NVR can synchronize information with the remote device such as Language, video standard and time zone.

Parameter	Description
Instant Playback	In the **Instant Play** box, enter the time length for playing back the recorded video. The value ranges from 5 to 60. On the live view control bar, click the instant playback button to play back the recorded video within the configured time.
Logout Time	Enter the standby time for the Device. The Device automatically logs out when it is not working in the configured period. You need to login the Device again. The value ranges from 0 to 60. 0 indicates there is not standby time for the Device. Click **Monitor Channel(s) when logout**. You can select the channels that you want to continue monitoring when you logged out.
CAM Time Sync	Syncs the Device time with IP camera.
Interval	Enter the interval for time sync.
Logout Time	You can set auto logout interval once login user remains inactive for a specified time. Value ranges from 0 to 60 minutes.
Navigation Bar	Enable the navigation bar. When you click on the live view screen, the navigation bar is displayed.
Mouse Sensitivity	Adjust the speed of double-click by moving the slider. The bigger the value is, the faster the speed is.

Step 3 Click **Apply** button to save settings.

5.15.1.2 Date and Time

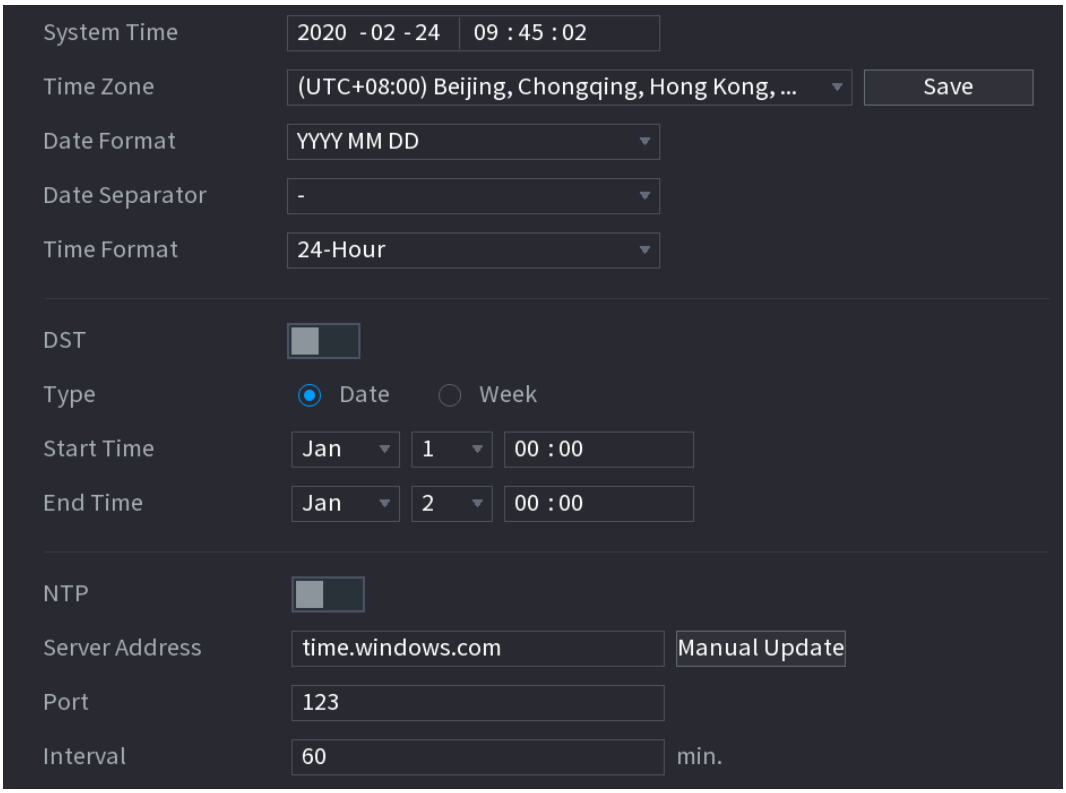
Background Information

You can set device time. You can enable NTP (Network Time Protocol) function so that the device can sync time with the NTP server.

You can also configure date and time settings by selecting **Main Menu** > **SYSTEM** > **General** > **Date&Time**.

Step 1 Click **Date&Time** tab.

Figure 5-253 Date and time



Step 2 Configure the settings for date and time parameters.

Table 5-75 Data and time parameters

Parameter	Description
System Time	In the **System Time** box, enter time for the system. Click the time zone list, you can select a time zone for the system, and the time in adjust automatically. ⚠ Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.
Time Zone	In the **Time Zone** list, select a time zone for the system.
Date Format	In the **Date Format** list, select a date format for the system.
Date Separator	In the **Date Separator** list, select a separator style for the date.
Time Format	In the **Time Format** list, select **12-HOUR** or **24-HOUR** for the time display style.
DST	Enable the Daylight Saving Time function. Click **Week** or **Date**.
Start Time	Configure the start time and end time for the DST.
End Time	

Parameter	Description
NTP	Enable the NTP function to sync the Device time with the NTP server. If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the **Server Address** box, enter the IP address or domain name of the corresponding NTP server. Click **Manual Update**, the Device starts syncing with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the **Interval** box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

Step 3 Click **Next** to save settings.

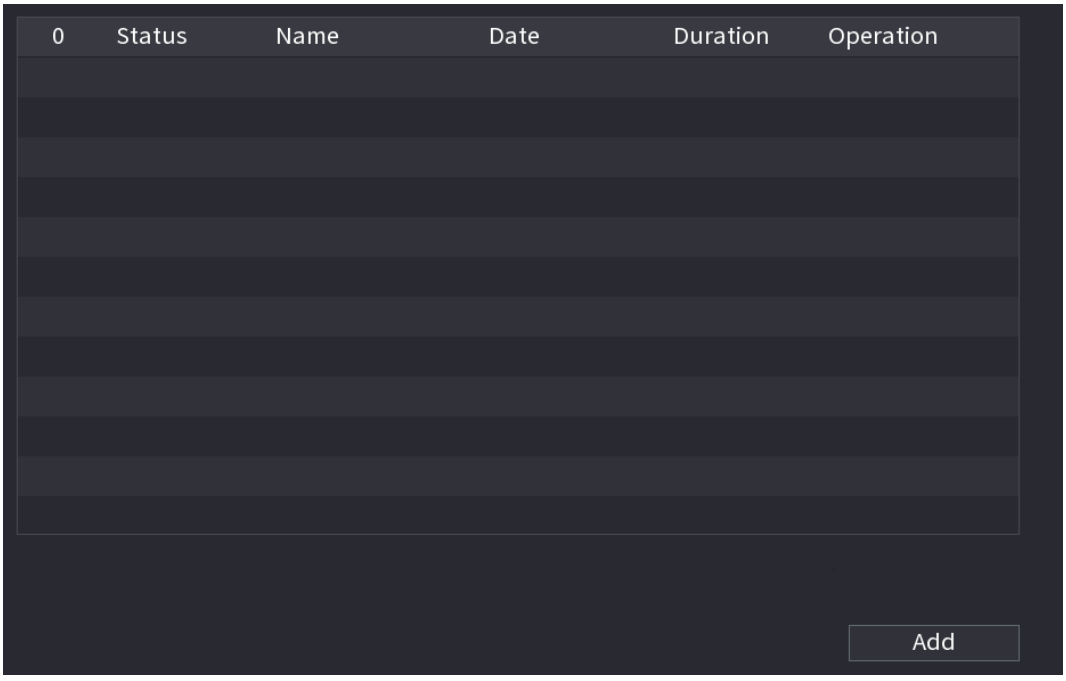
5.15.1.3 Holiday

Here you can add, edit, and delete holiday. After you successfully set holiday information, you can view holiday item on the record and snapshot period.

You can also configure holiday settings by selecting **Main Menu** > **SYSTEM** > **General** > **Holiday**.

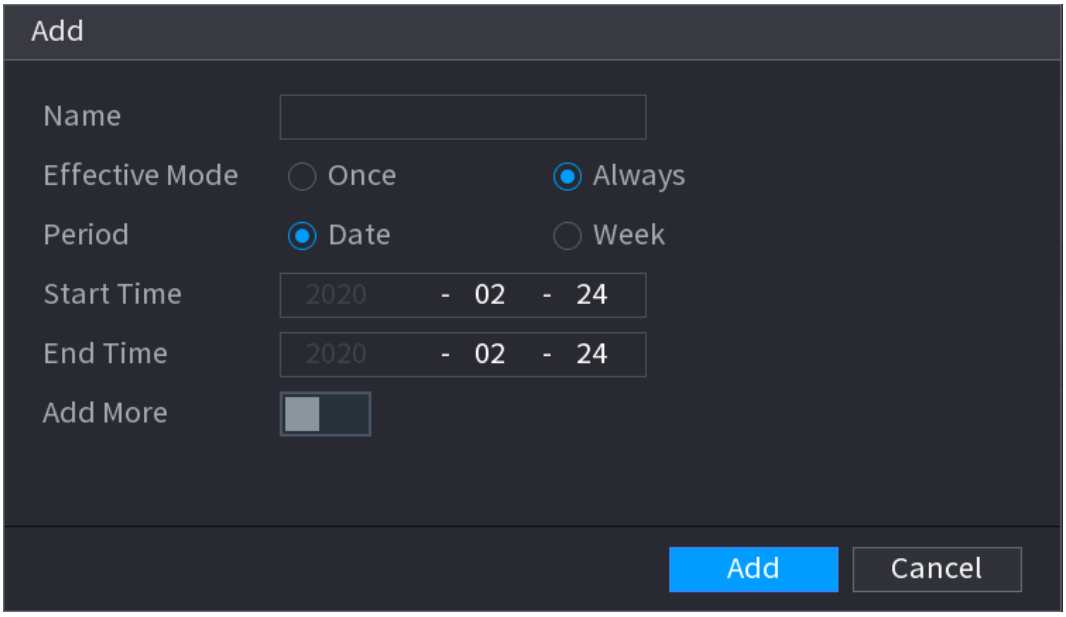
Step 1 Click **Next**.

Figure 5-254 Holiday



Step 2 Click **Add Holidays**.

Figure 5-255 Add holidays



Step 3 Set holiday name, repeat mode and holiday mode.

Click **Add more** to add new holiday information.

Step 4 Click **Add**, you can add current holiday to the list.

- Click the drop-down list of the state; you can enable/disable holiday date.
- Click to change the holiday information. Click to delete current date.

Step 5 Click **Next** to save settings.

5.15.2 Serial Port

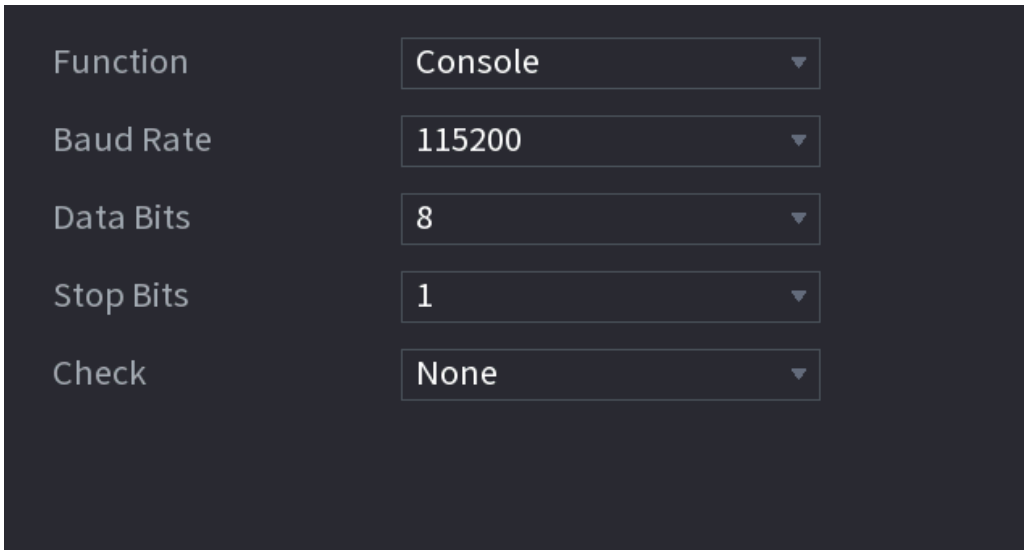
Background Information

After setting RS-232 parameters, the NVR can use the COM port to connect to other device to debug and operate.

Procedure

Step 1 Select **MAIN MENU** > **SYSTEM** > **Serial Port**.

Figure 5-256 Serial port



Step 2 Configure parameters.

Table 5-76 Serial port parameters

Parameter	Description
Function	Select serial port control protocol. • Console: Upgrade the program and debug with the console and mini terminal software. • Keyboard: Control this Device with special keyboard. • Adapter: Connect with PC directly for transparent transmission of data. • Protocol COM: Configure the function to protocol COM, in order to overlay card number. • PTZ Matrix: Connect matrix control Different series products support different RS-232 functions.
Baud Rate	Select baud rate, which is 115200 by default.
Data Bits	It ranges from 5 to 8, which is 8 by default.
Stop Bits	It includes 1 and 2.
Parity	It includes none, odd, even, mark and null.

Step 3 Click **Apply**.

5.16 Output and Display

5.16.1 Display

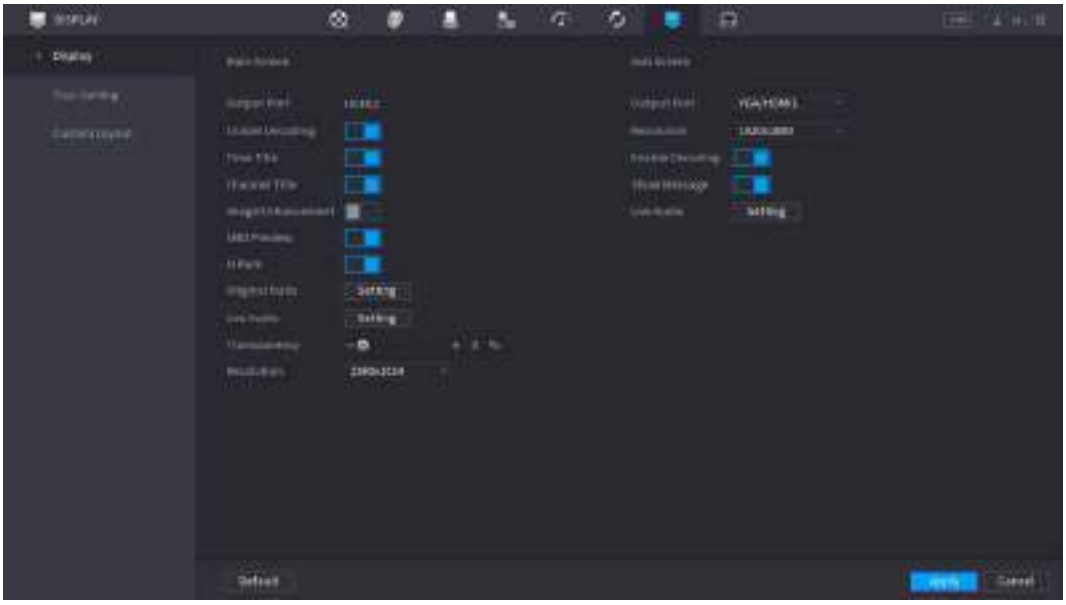
Background Information

You can configure the display effect such as displaying time title and channel title, adjusting image transparency, and selecting the resolution.

Procedure

Step 1 Select **Main Menu** > **DISPLAY** > **Display**.

Figure 5-257 Display



Step 2 Configure the parameters.

Table 5-77 Display parameters

Parameter	Description
Main Screen/Sub Screen	Configure the output port format of both screens. ● When sub screen is disabled, the format of main screen is HDMI/VGA simultaneous output. ● When sub screen is enabled, the format of main screen and sub screen are non-simultaneous outputs. ◇ When output port of sub screen is set to **HDMI**, the output port of main screen is set to **VGA** by the device. ◇ When output port of sub screen is set to **VGA**, the output port of main screen is set to **HDMI** by the device.
Enable Decoding	After it is enabled, the device can normally decode.
Time Title/Channel Title	Select the checkbox and the date and time of the system will be displayed in the preview screen.
Transparency	Set the transparency of the local menu of the NVR device. The higher the transparency, the more transparent the local menu.
Time Title/Channel Title	Select the checkbox and the date and time of the system will be displayed in the preview screen.
Image Enhancement	Select the checkbox to optimize the preview image edges.
SMD Preview	Select the checkbox to display the SMD previews in the live view interface.

Parameter	Description
AI Rule	Select the checkbox to display the AI rules in the live view interface. This function is for some series products only.
Original Ratio	Click **Setting** and select the channel to restore the corresponding channel image to the original scale.
Live Audio	Configure audio input on live view. You can select **Audio 1**, **Audio 2**, and **Mixing**. For example, if you select **Audio 1** for **D1** channel, the sound of audio input port 1 of camera is playing. If you select **Mixing**, the sound of all audio input ports are playing.
Resolution	Support 1920×1080, 1280×1024(default), 1280×720.

Step 3 Click **Apply**.

5.16.2 Tour

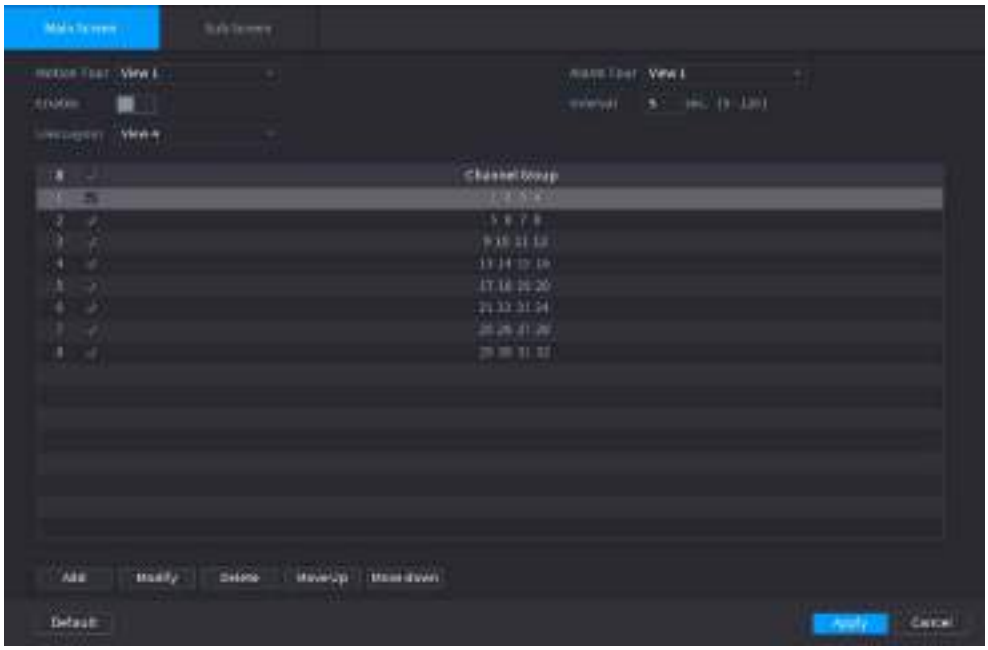
Background Information

You can configure a tour of selected channels to repeat playing videos. The videos display in turn according to the channel group configured in tour settings. The system displays one channel group for a certain period and then automatically changes to the next channel group.

Procedure

Step 1 Select **DISPLAY** > **Tour Setting** > **Main Screen**.

Figure 5-258 Tour



- On the top right of the live view screen, use the left mouse button or press Shift to switch between (image switching is allowed) and (image switching is not allowed) to turn on/off the tour function.
- On the navigation bar, click to enable the tour and click to disable it.

Step 2 Configure the tour setting parameters.

Table 5-78 Tour parameters

Parameter	Description
Enable Tour	Enable tour function.
Interval	Enter the amount of time that you want each channel group displays on the screen. The value ranges from 5 seconds to 120 seconds, and the default value is 5 seconds.
Motion Tour, Alarm Tour	Select the View 1 or View 8 for **Motion Tour** and **Alarm Tour** (system alarm events).
Live Layout	In the **Live Layout** list, select **View 1**, **View 4**, **View 8**, or other modes that are supported by the Device.
Channel Group	Display all channel groups under the current Window Split setting. • Add a channel group: Click **Add**, in the pop-up **Add Group** channel, select the channels to form a group, and then click **Save**. • Delete a channel group: Select the checkbox of any channel group, and then click **Delete**. • Edit a channel group: Select the checkbox of any channel group and then click **Modify**, or double-click on the group. The **Modify Channel Group** dialog box is displayed. You can regroup the channels. • Click **Move up** or **Move down** to adjust the position of channel group.

Step 3 Click **Apply** to save the settings.

5.16.3 Custom Layout

Background Information

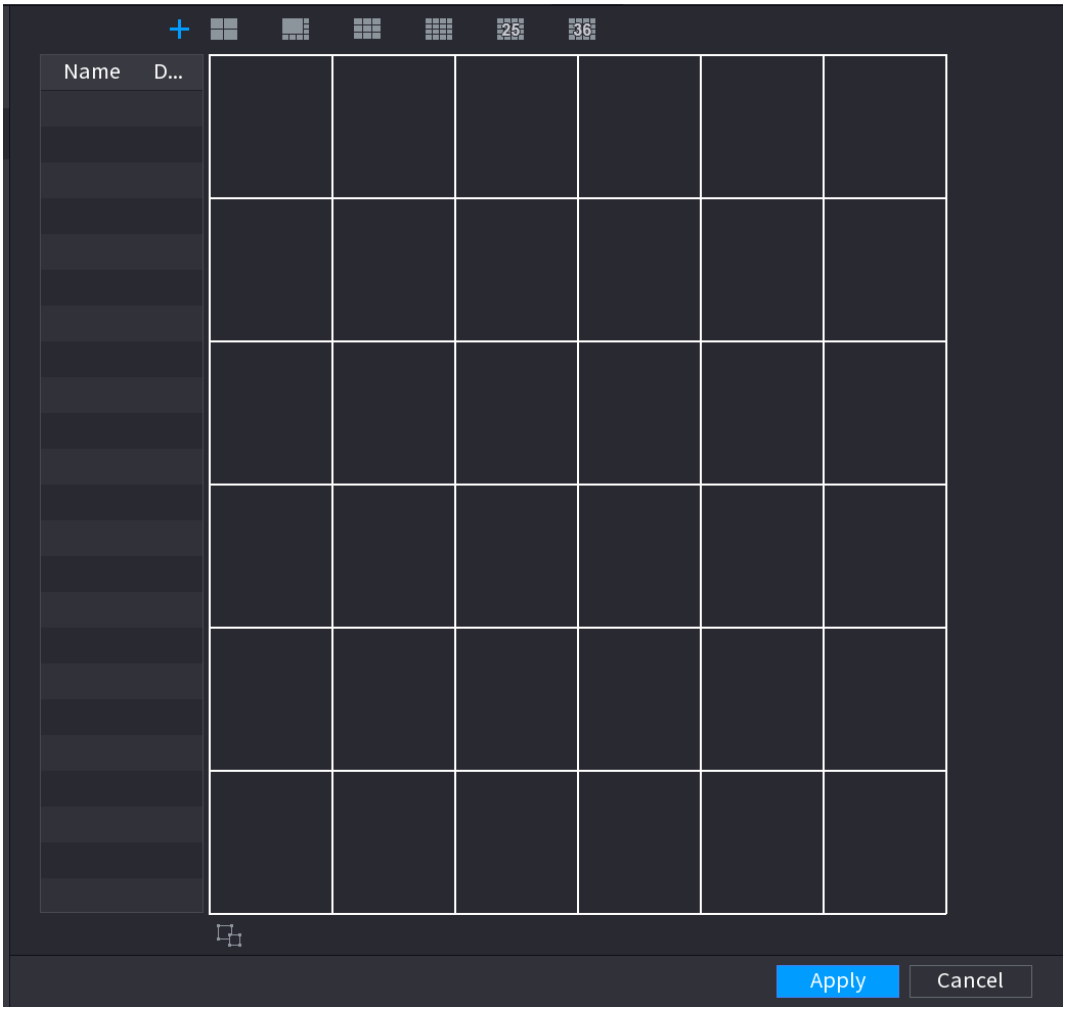
You can set customized video split mode.

- This function is for some series products. See the actual product for detailed information.
- Device max. supports 5 customized videos.

Procedure

Step 1 Select **Main Menu** > **DISPLAY** > **Custom Split**.

Figure 5-259 Custom split

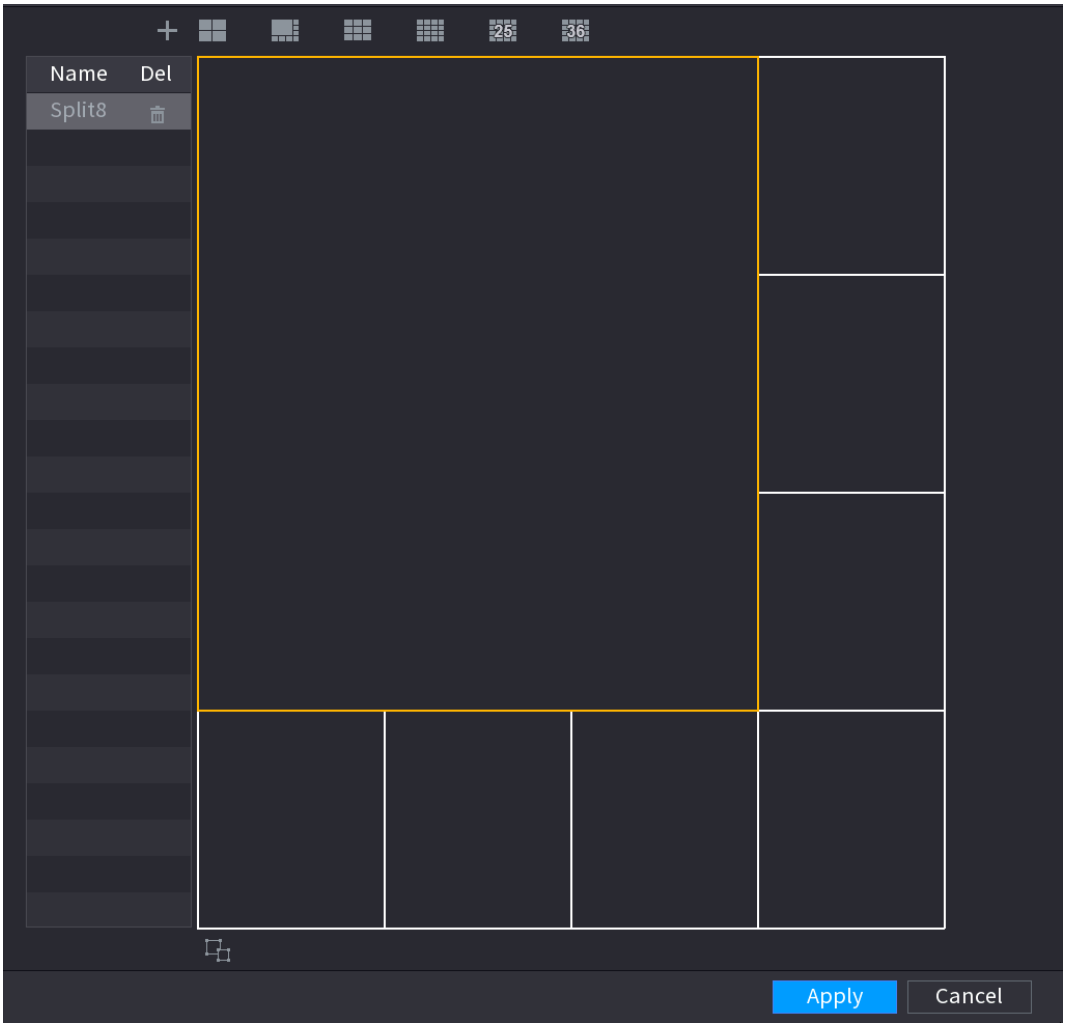


Step 2 Click + and then click [redacted] to select basic mode.

System adopts the basic window mode as the new window name. For example, if you select the 8 display mode, the default name is Split8.In regular mode, drag the mouse in the preview frame; you can merge several small windows to one window so that you can get you desired split mode.

- After merge the window, system adopts the remaining window amount as the new name such as Split6.
- Select the window you want to merge (red highlighted), click [redacted] to cancel the merge to restore the basic mode.
- Click [redacted] to delete the customized window mode.

Figure 5-260 Merged window



Step 3 Click **Apply** to exit.

After the setup, you can go to the preview window, right-click and then select **Live Layout** to select the custom split layout.

5.17 POS

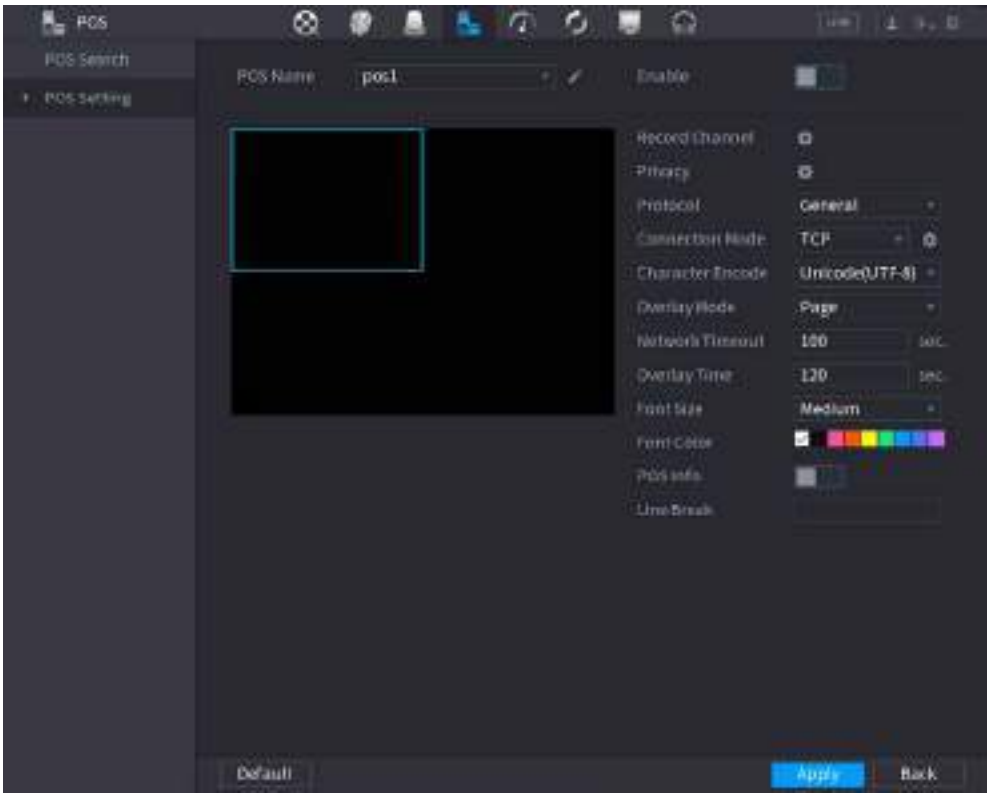
You can connect the Device to the POS (Point of Sale) machine and receive the information from it. This function applies to the scenarios such as supermarket POS machine. After connection is established, the Device can access the POS information and display the overlaid text in the channel window.

5.17.1 Settings

Procedure

Step 1 Select **Main Menu** > **POS** > **POS Setting**.

Figure 5-261 POS setting



Step 2 Configure the POS parameters.

Table 5-79 POS parameters

Parameter	Description
POS Name	In the POS Name list, select the POS machine that you want to configures settings for. Click to modify the POS name. ● The POS name must be unique. ● You can enter up to 21 Chinese characters or 63 English characters.
Enable	Enable the POS function.
Record Channel	Click to select a channel to record.
Privacy	Enter the privacy contents.
Protocol	Select a protocol. Different machines correspond to different protocols.
Connection Mode	Select the connection protocol type. Click , the **IP Address** window is displayed. In the **Source IP** box, enter the IP address (the machine that is connected to the Device) that sends messages.
Character Encode	Select a character encoding mode.

Parameter	Description
Overlay Mode	In the **Overlay Mode** list, Select **Turn** or **ROLL**. • Turn: Once the information is at 16 lines, system displays the next page. • ROLL: Once the information is at 16 lines, system rolls one line after another to delete the first line. When the local preview mode is in 4-split, the turn/ROLL function is based on 8 lines.
Network time out	When the network is not working correctly and cannot be recovered after the entered timeout limit, the POS information will not display normally. After the network is recovered, the latest POS information will be displayed.
Time Display	Enter the time that how long you want to keep the POS information displaying. For example, enter 5, the POS information disappear from the screen after 5 seconds.
Font Size	Select **Small**, **Medium**, or **Big** as the text size of POS information
Font Color	In the color bar, click to select the color for the text size of POS information.
POS Info	Enable the POS Info function, the POS information displays in the live view/WEB.
Line Break	There is no line delimiter by default. After you set the line delimiter (HEX), the overlay information after the delimiter is displayed in the new line. For example, the line delimiter is F and the overlay information is 123F6789, NVR displays overlay information on the local preview interface and Web as: 123 6789

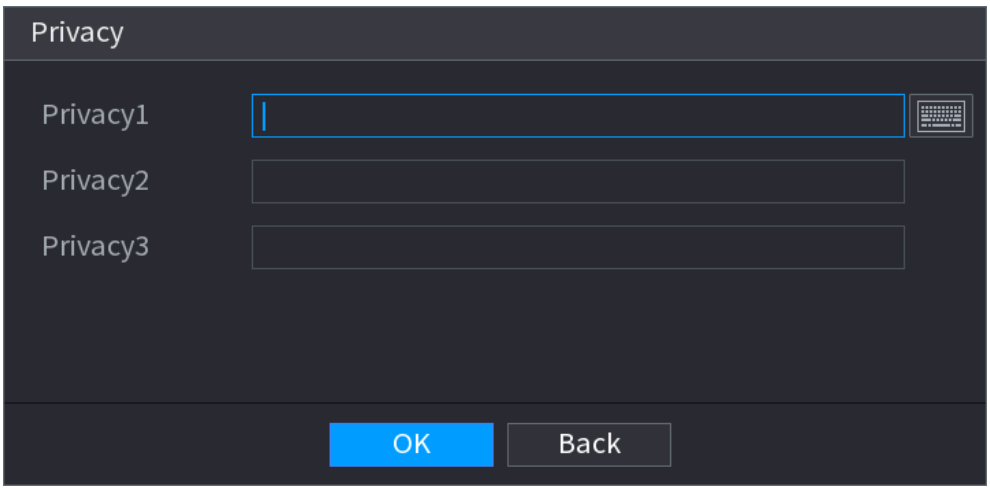
Step 3 Click **Apply**.

5.17.1.1 Privacy Setup

Procedure

Step 1 Click next to **Privacy**.

Figure 5-262 Privacy



Step 2 Set privacy information.

Step 3 Click **OK**.

5.17.1.2 Connection Mode

Background Information

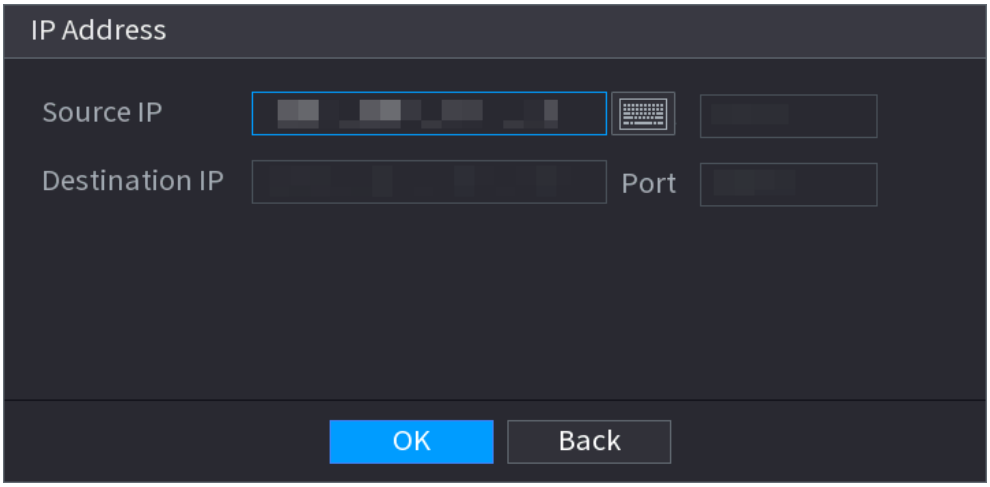
Connection type is UDP or TCP.

Procedure

Step 1 Select **Connection Mode** as **UDP**, **TCP_CLINET** or **TCP**.

Step 2 Click .

Figure 5-263 IP address



Step 3 For **Source IP** and **Port**, enter the POS IP address and port.

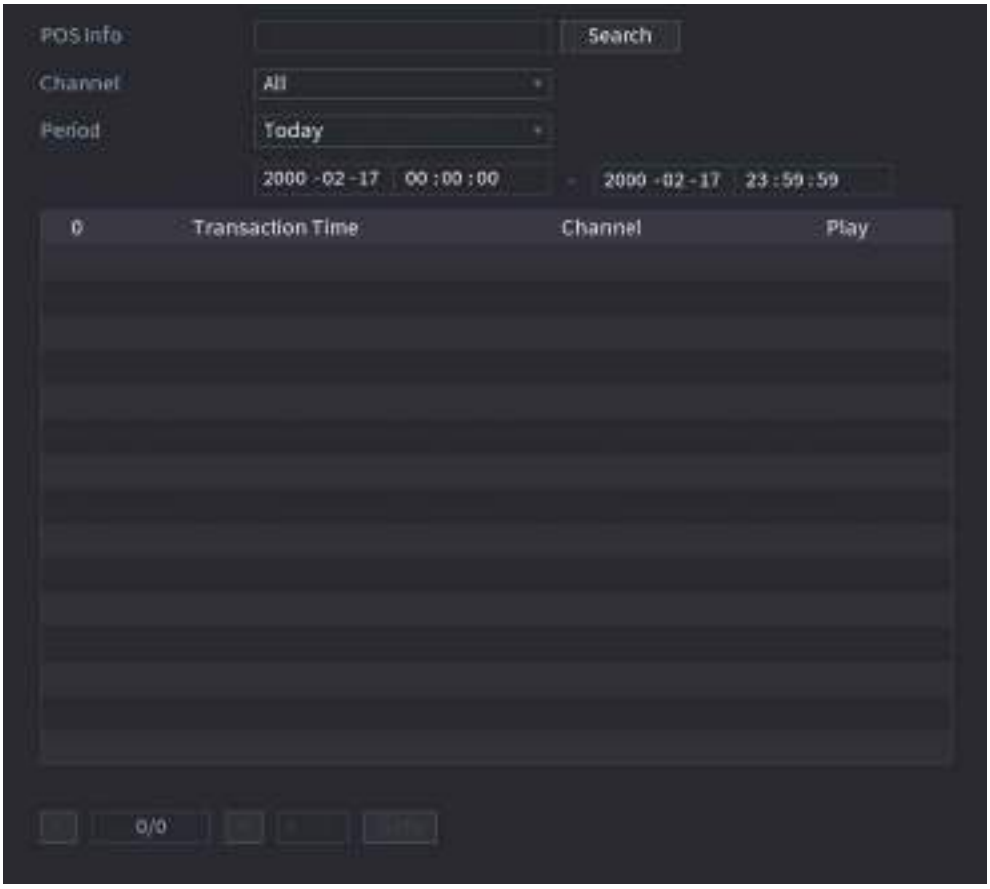
Step 4 Click **OK**.

5.17.2 Search

The system supports fuzzy search.

Step 1 Select **Main Menu** > **POS** > **POS Search**.

Figure 5-264 POS search



Step 2 In the **POS Search** box, enter the information such as transaction number on your receipt, amount, or product name.

Step 3 In the **Start Time** box and **End Time** box, enter the time period that you want to search the POS transaction information.

Step 4 Click **Search**.

The searched transaction results display in the table.

5.18 Audio

The audio function is to manage audio files and set schedule play function. It is to realize audio broadcast activation function.

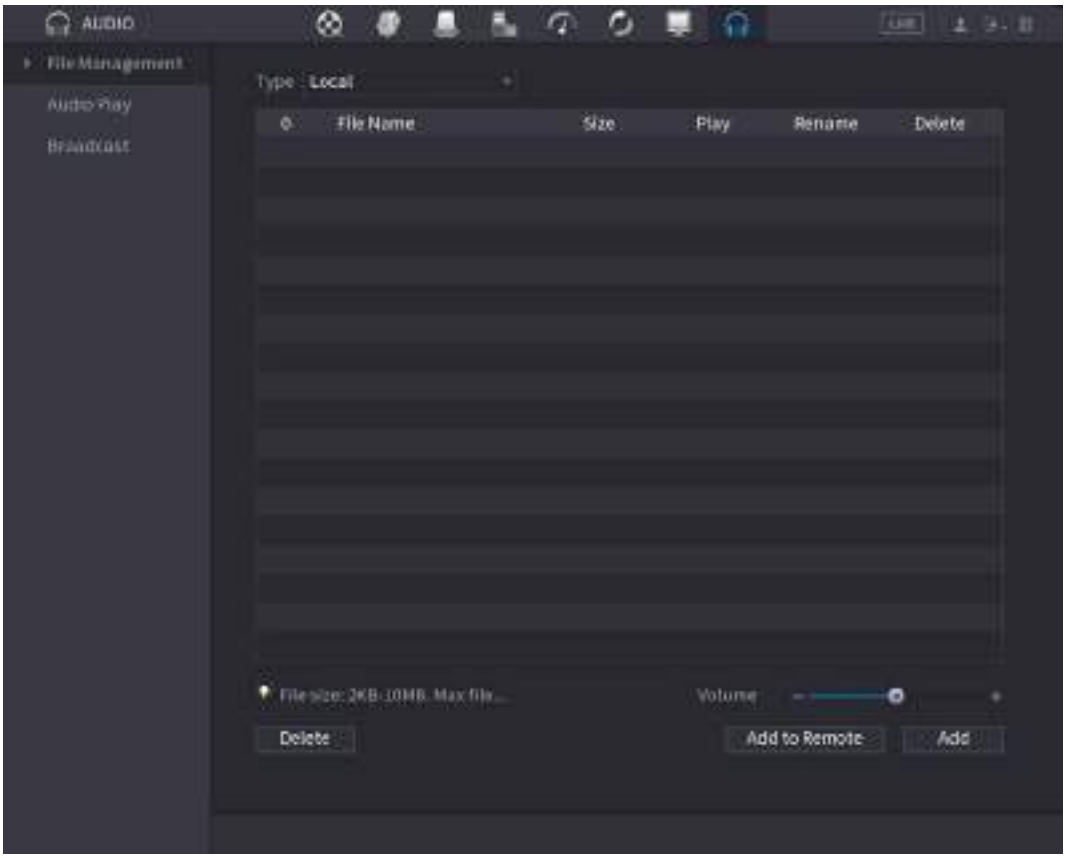
This function is available on select models.

5.18.1 File Management

You can add audio files, listen to audio files, rename and delete audio files, and configure the audio volume.

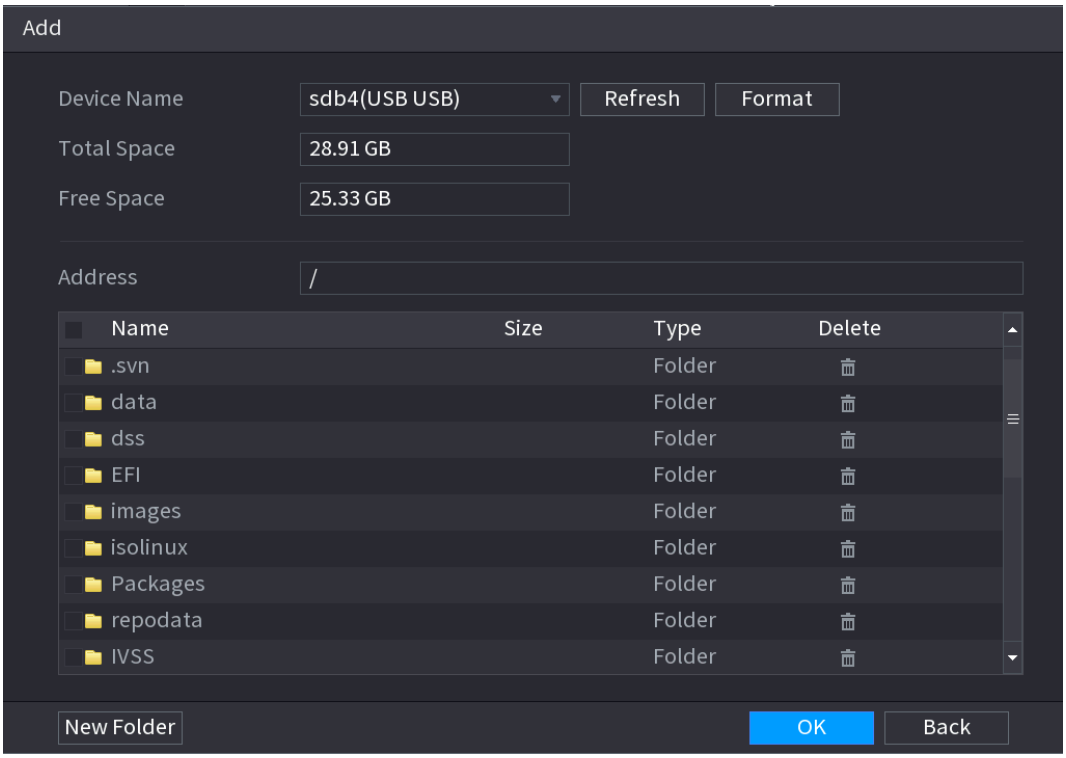
Step 1 Select **Main Menu** > **AUDIO** > **File Management**.

Figure 5-265 File management



Step 2 Click **Add**.

Figure 5-266 Add file



Step 3 Select the audio file and then click **Import**.

System supports MP3 and PCM audio format.

Step 4 Click **OK** to start importing audio files from the USB storage device.

If the importing is successful, the audio files will display in the **File Management** page.

5.18.2 Audio Play

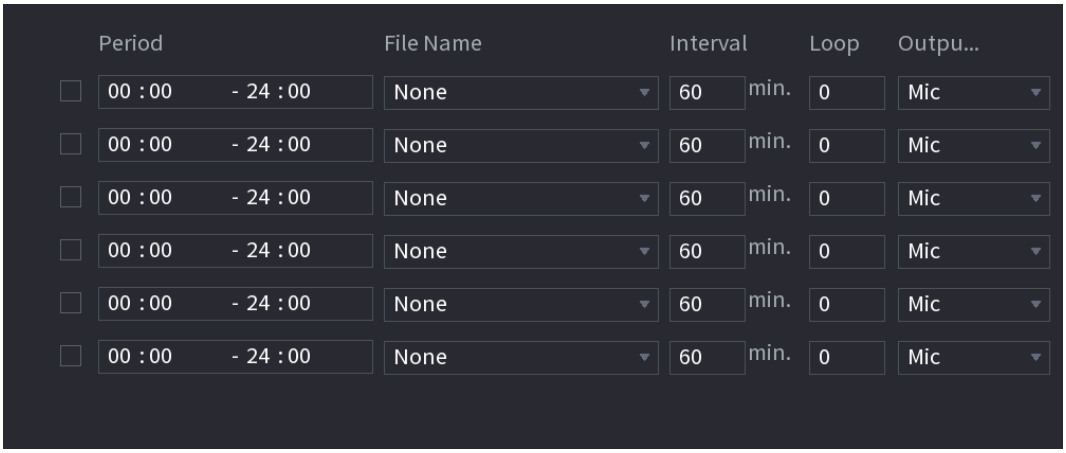
Background Information

You can configure the settings to play the audio files during the defined time period.

Procedure

Step 1 Select **Main Menu** > **AUDIO** > **Schedule**.

Figure 5-267 Schedule



Step 2 Configure the parameters.

Table 5-80 Schedule parameters

Parameter	Description
Period	In the **Period** box, enter the time. Select the checkbox to enable the settings. You can configure up to six periods.
File Name	In the **File Name** list, select the audio file that you want to play for this configured period.
Interval	In the **Interval** box, enter the time in minutes for how often you want to repeat the playing.
Loop	Configure how many times you want to repeat the playing in the defined period.
Output	Includes two options: MIC and Audio. It is MIC by default. The MIC function shares the same port with talkback function and the latter has the priority. Some series products do not have audio port.

- The finish time for audio playing depends on audio file size and the configured interval.
- Playing priority: Alarm event > Audio talk > Trial listening > Schedule audio file.

Step 3 Click **Apply**.

5.18.3 Broadcast

Background Information

System can broadcast to the camera, or broadcast to a channel group.

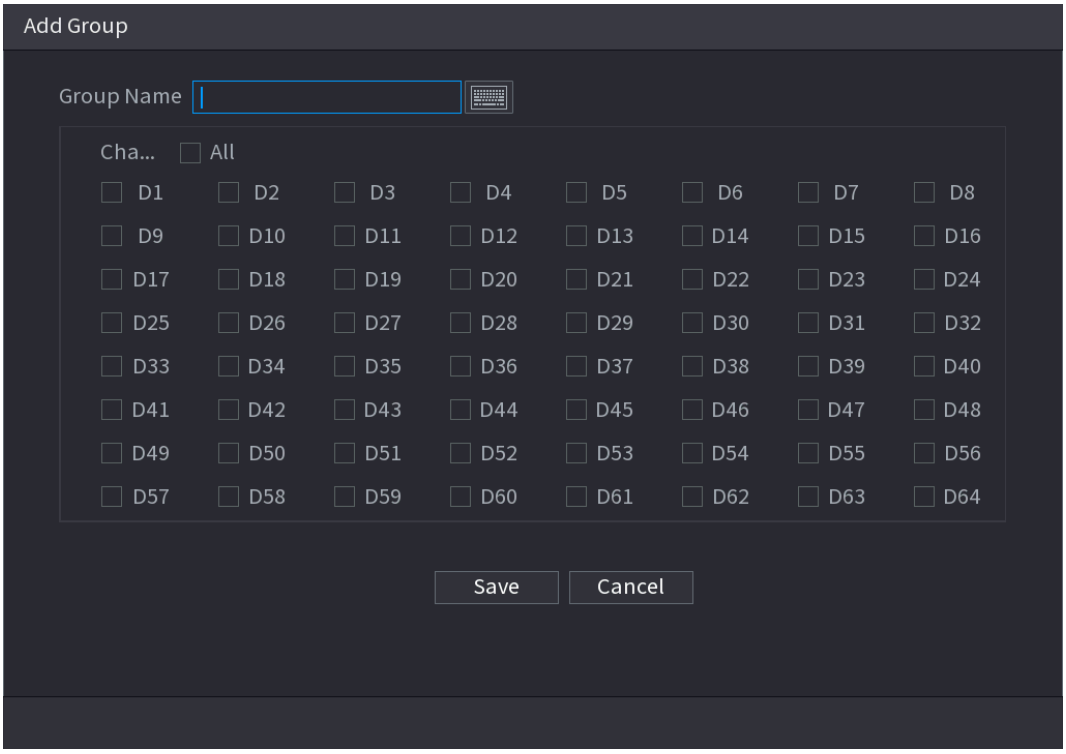
Procedure

Step 1 Select **Mani Menu** > **AUDIO** > **Broadcast**.

Figure 5-268 Broadcast

Step 2 Click **Add Group**.

Figure 5-269 Add group (1)



Step 3 Input group name and select one or more channels.

Step 4 Click **Save** to complete broadcast group setup.

- On the broadcast interface, click to change group setup, click to delete group.
- After complete broadcast setup, on the preview interface and then click on the navigation bar, device pops up broadcast dialogue box. Select a group name and then click to begin broadcast.

Figure 5-270 Add group (2)

5.19 Operation and Maintenance

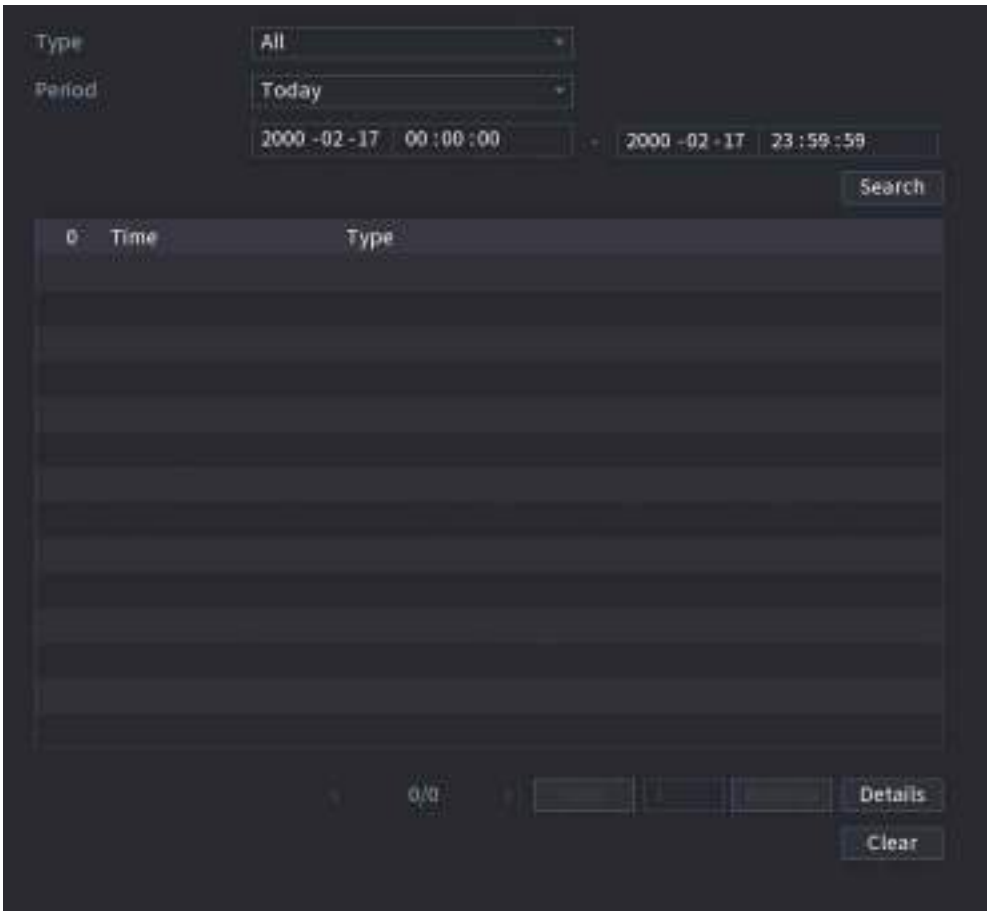
5.19.1 Log

You can view and search for the log information, or back up log to the USB device.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Log**.

Figure 5-271 Log



Step 2 In the **Type** list, select the log type that you want to view (**System**, **Config**, **Storage**, **Record**, **Account**, **Clear Log**, **Playback**, and **Connection**) or select **All** to view all logs.

Step 3 Enter the time period to search, and then click **Search**.

The search results are displayed.

Related Operations

- Click **Details** or double-click the log to view details. Click **Next** or **Previous** to view more log information.
- Click **Backup** to back up the logs to the USB storage device.
- Click **Clear** to remove all logs.

5.19.2 System

5.19.2.1 System Version

Select **Main Menu** > **MAINTAIN** > **System Info** > **Version**.

You can view NVR version information.

5.19.2.2 AI Algorithm Version

Select **Main Menu** > **MAINTAIN** > **System Info** > **Intelligent Algorithm**.

You can view version information for AI functions such as face detection, face recognition, IVS, and

video metadata.

5.19.2.3 HDD Info

You can view the HDD quantity, HDD type, total space, free space, status, and S.M.A.R.T information.

Select **Main Menu** > **MAINTAIN** > **System Info** > **Disk**.

Figure 5-272 Disk information

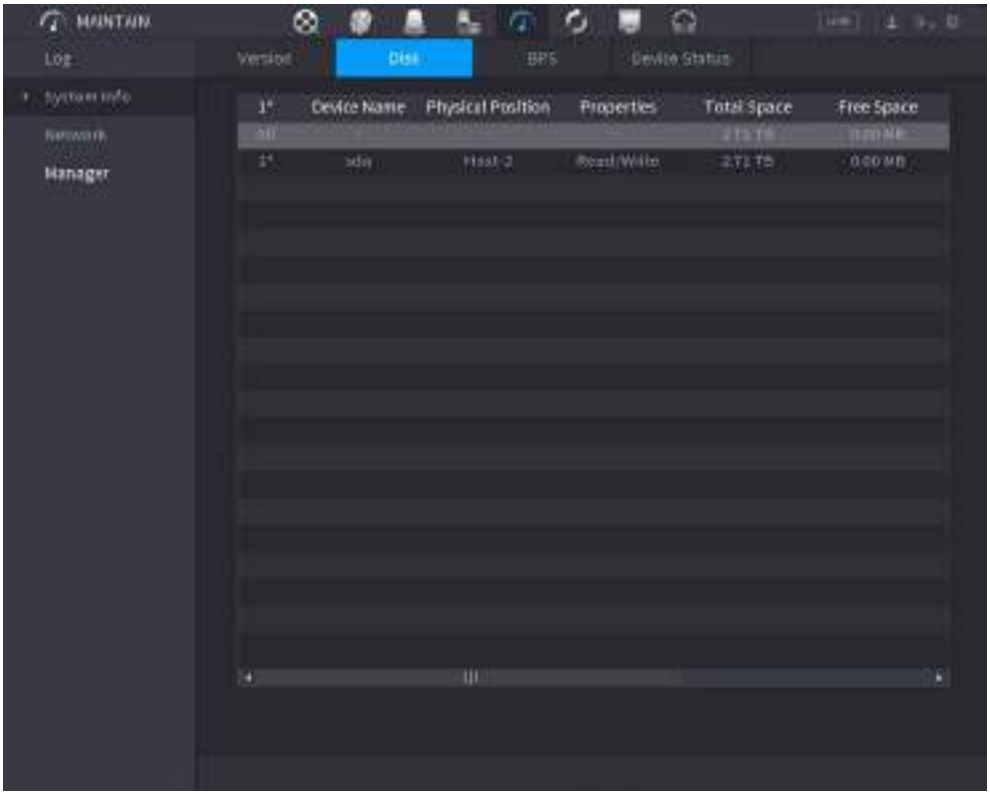


Table 5-81 Disk information

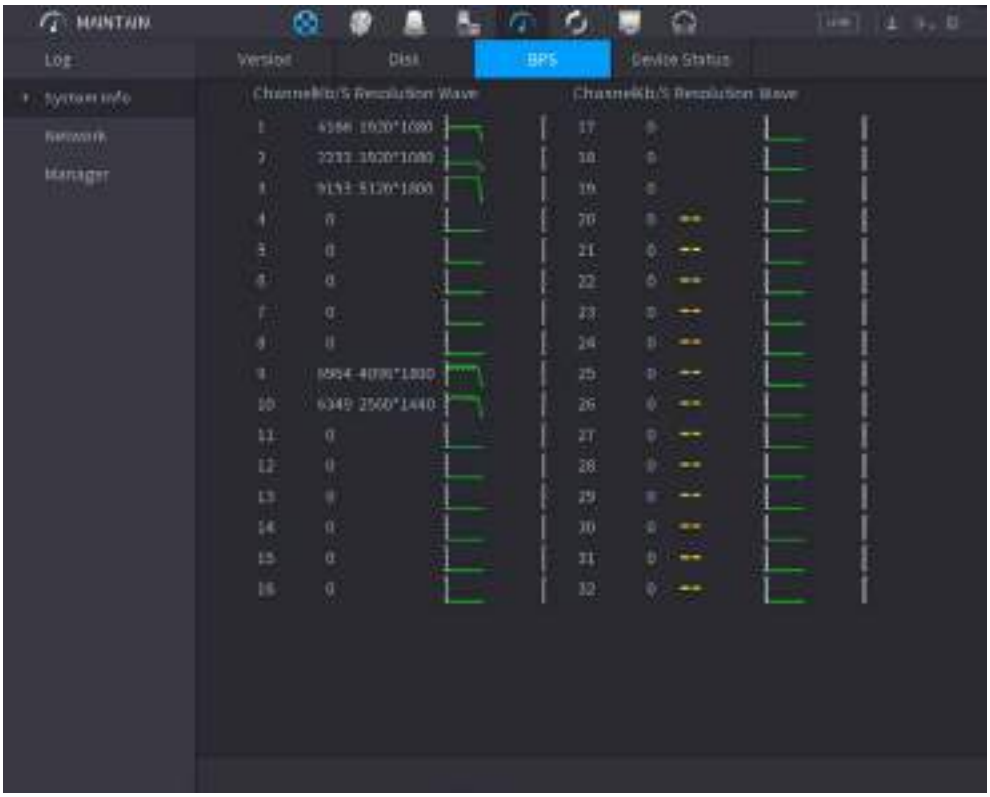
Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Properties	Indicates HDD type.
Total Space	Indicates the total capacity of HDD.
Free Space	Indicates the usable capacity of HDD.
Health Status	Indicates the health status of the HDD.
S.M.A.R.T	View the S.M.A.R.T reports from HDD detecting.
Status	Indicates the status of the HDD to show if it is working normally.

5.19.2.4 BPS

You can view current video bit rate (kb/s) and resolution.

Select **Main Menu** > **MAINTAIN** > **System Info** > **BPS**.

Figure 5-273 BPS

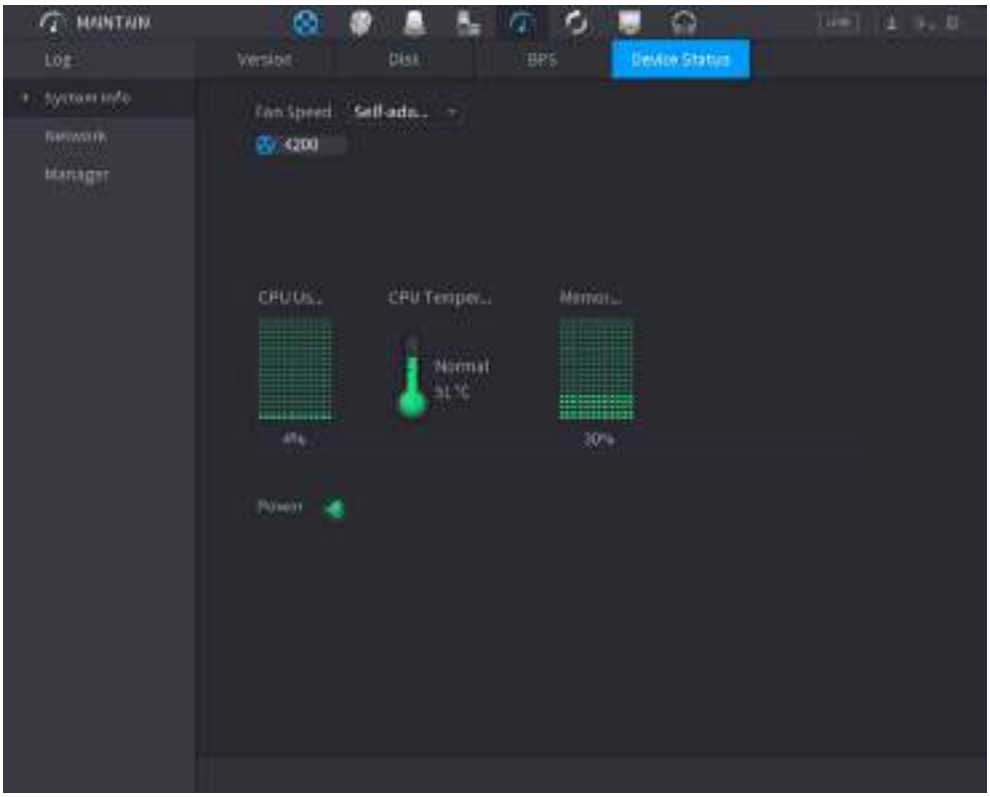


5.19.2.5 Device Status

You can view fan running status such as speed, CPU temperature, and memory.

Select **Main Menu** > **MAINTAIN** > **System Info** > **Device Status**.

Figure 5-274 Device status



5.19.3 Network

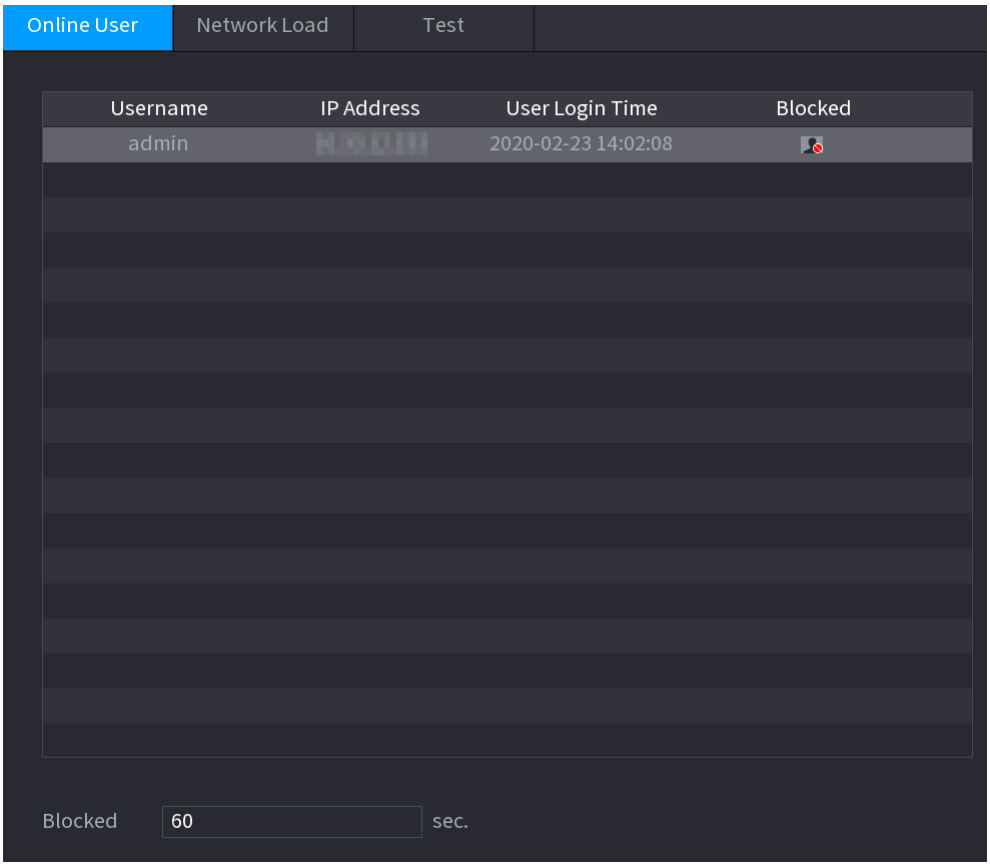
5.19.3.1 Online User

You can view the online user information or block any user for a period of time. To block an online user, click and then enter the time that you want to block this user. The maximum value you can set is 65535.

The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

Select **Main Menu** > **MAINTAIN** > **Network** > **Online User**.

Figure 5-275 Online user



5.19.3.2 Network Load

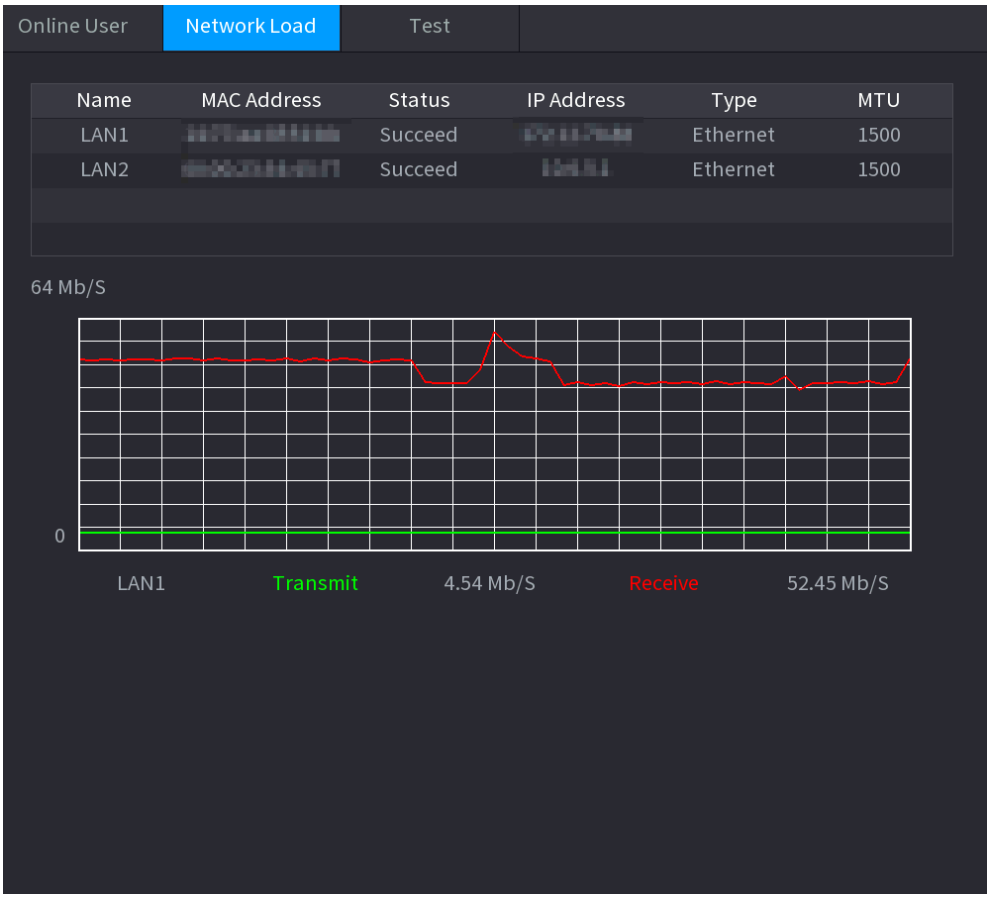
Background Information

Network load means the data flow which measures the transmission capability. You can view the information such as data receiving speed and sending speed.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Network** > **Network Load**.

Figure 5-276 Network load



Step 2 Click the LAN name that you want to view, for example, **LAN1**.

The system displays the information of data sending speed and receiving speed.

- System displays LAN1 load by default.
- Only one LAN load can be displayed at one time.

5.19.3.3 Network Test

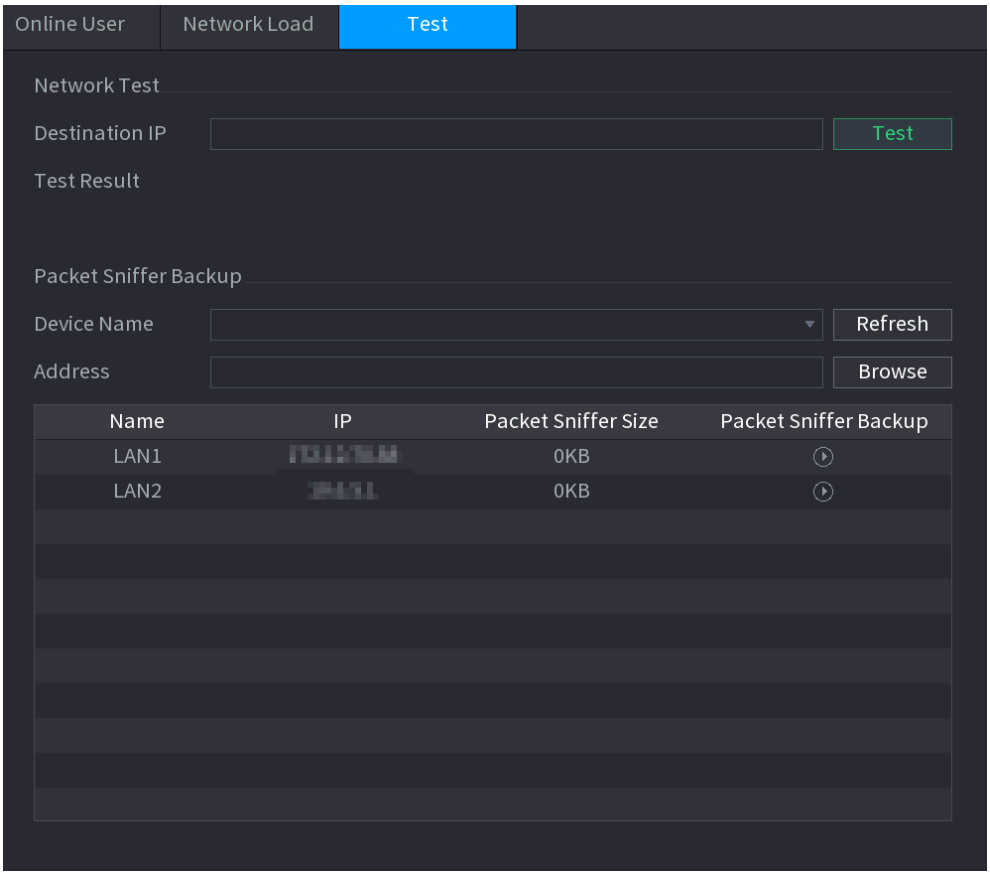
Background Information

You can test the network connection status between the Device and other devices.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Network** > **Test**.

Figure 5-277 Test



Step 2 In the **Destination IP** box, enter the IP address.

Step 3 Click **Test**.

After testing is completed, the test result is displayed. You can check the evaluation for average delay, packet loss, and network status.

5.19.4 Maintenance and Management

5.19.4.1 Device Maintenance

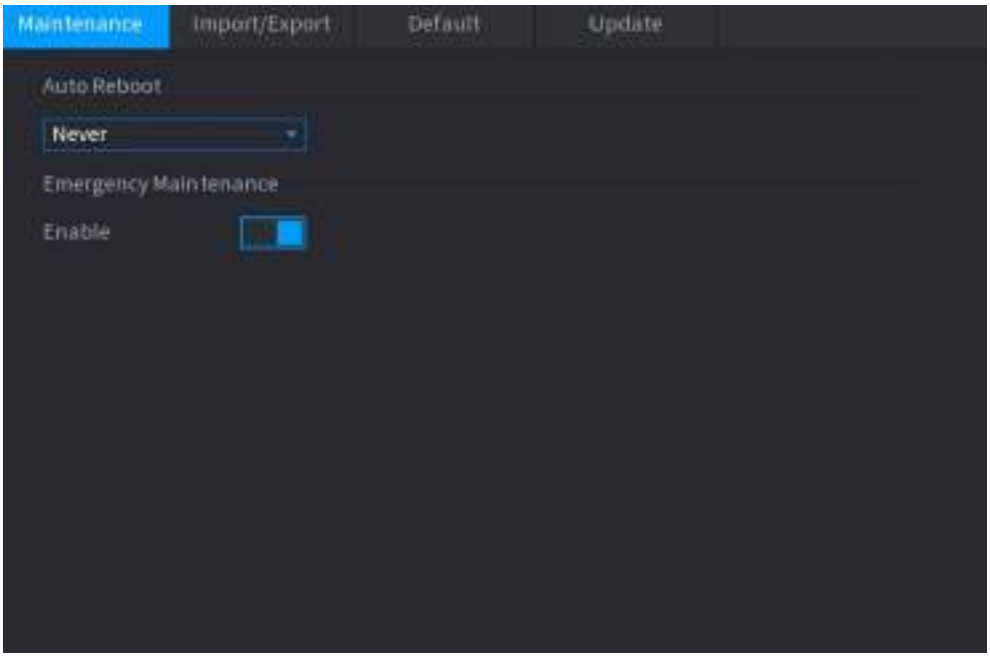
Background Information

When the Device has been running for a long time, you can enable the Device to restart automatically at the idle time. You can also enable emergency maintenance.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Manager** > **Maintenance**.

Figure 5-278 Maintenance



Step 2 Configure the parameters.

- **Auto Reboot**: Enable the Device to restart at the idle time.
- **Emergency Maintenance**: When the Device has an update power outage, running error and other problems, and you cannot log in, then you can use the emergency maintenance function to restart the Device, clear configuration, update the system, and more.

Step 3 Click **Apply**.

5.19.4.2 Exporting System Settings

Background Information

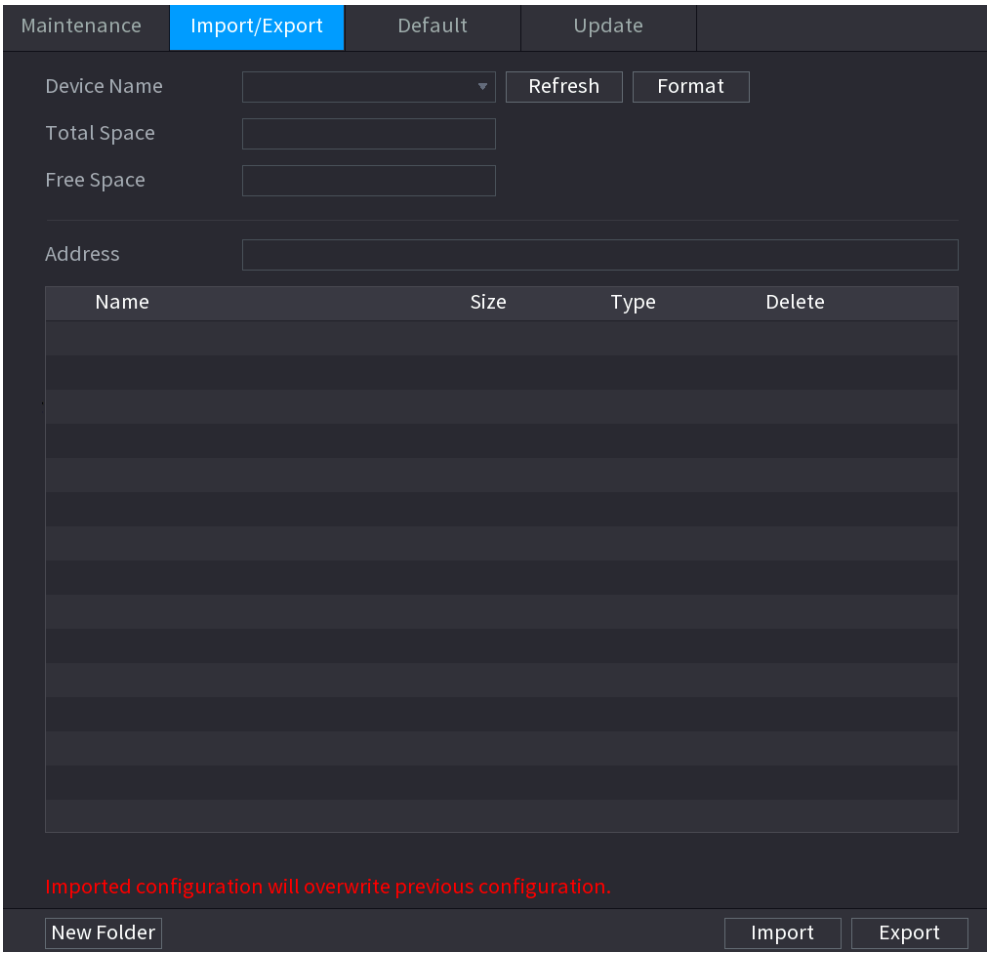
You can export or import the Device system settings if there are several Devices that require the same setup.

- The **Import/Export** interface cannot be opened if the backup operation is ongoing on the other interfaces.
- When you open the **Import/Export** interface, the system refreshes the devices and sets the current directory as the first root directory.
- Click **Format** to format the USB storage device.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Manager** > **Import/Export**.

Figure 5-279 Import and export

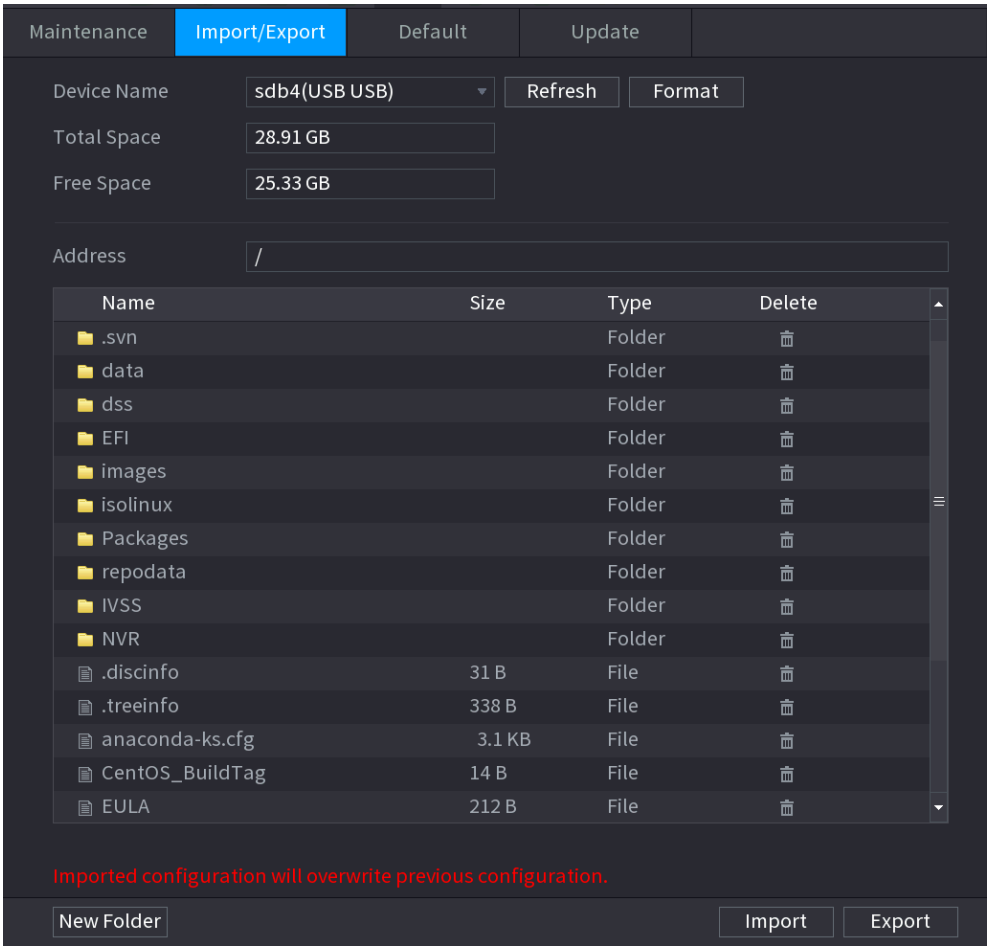


Step 2 Insert a USB storage device into one of the USB ports on the Device.

Step 3 Click **Refresh** to refresh the interface.

The connected USB storage device is displayed.

Figure 5-280 Connected USB device



Step 4 Click **Export**.

There is a folder under the name style of "Config_[YYYYMMDDhhmmss]". Double-click this folder to view the backup files.

5.19.4.3 Restoring Defaults

5.19.4.3.1 Restoring Defaults on the Local Interface

Background Information

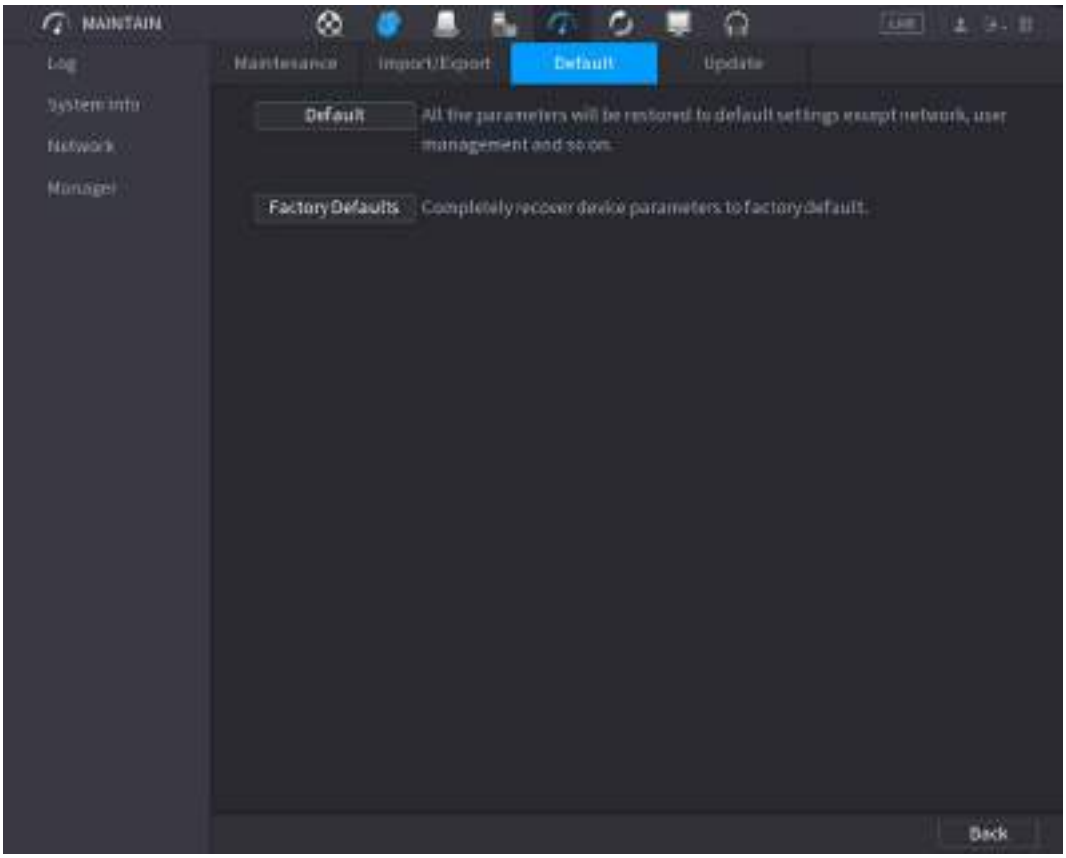
This function is for admin account only.

You can restore the Device to default settings on the local interface.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Manager** > **Default**.

Figure 5-281 Default



Step 2 Restore the settings.

- **Default**: Restore all the configurations except network settings and user management to the default..
- **Factory Default**: Restore all the configurations to the factory default settings.

5.19.4.3.2 Resetting Device through the Reset Button

Background Information

You can use the reset button on the mainboard to reset the Device to the factory default settings.

The reset button is available on select models.

After resetting, all the configurations will be lost.

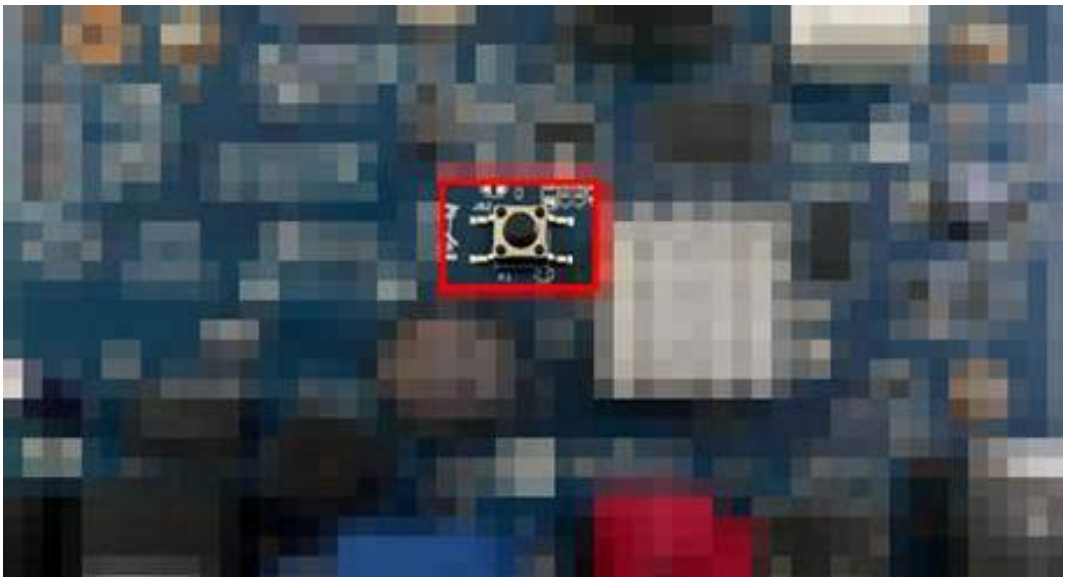
Procedure

Step 1 Disconnect the Device from power source, and then remove the cover panel. For details about removing the cover panel, see "3.3 HDD Installation".

Step 2 Find the reset button on the mainboard, and then connect the Device to the power source again.

Step 3 Press and hold the reset button for 5 seconds to 10 seconds.

Figure 5-282 Reset button



Step 4 Restart the Device.

After the Device restarts, the settings have been restored to the factory default.

5.19.4.4 System Update

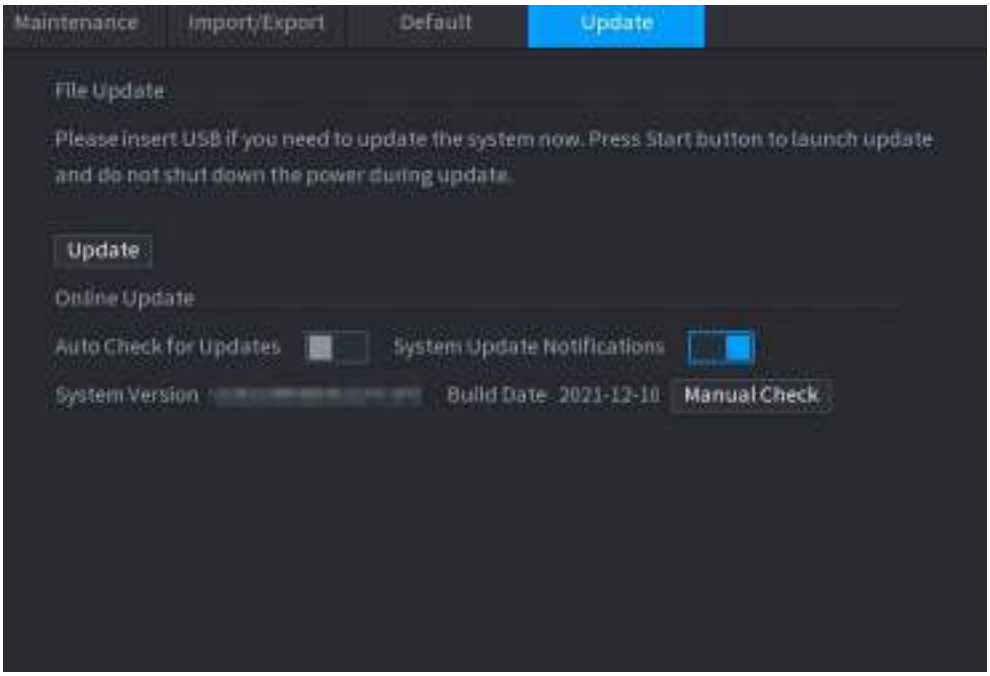
5.19.4.4.1 Upgrading File

Procedure

Step 1 Insert a USB storage device containing the upgrade files into the USB port of the Device.

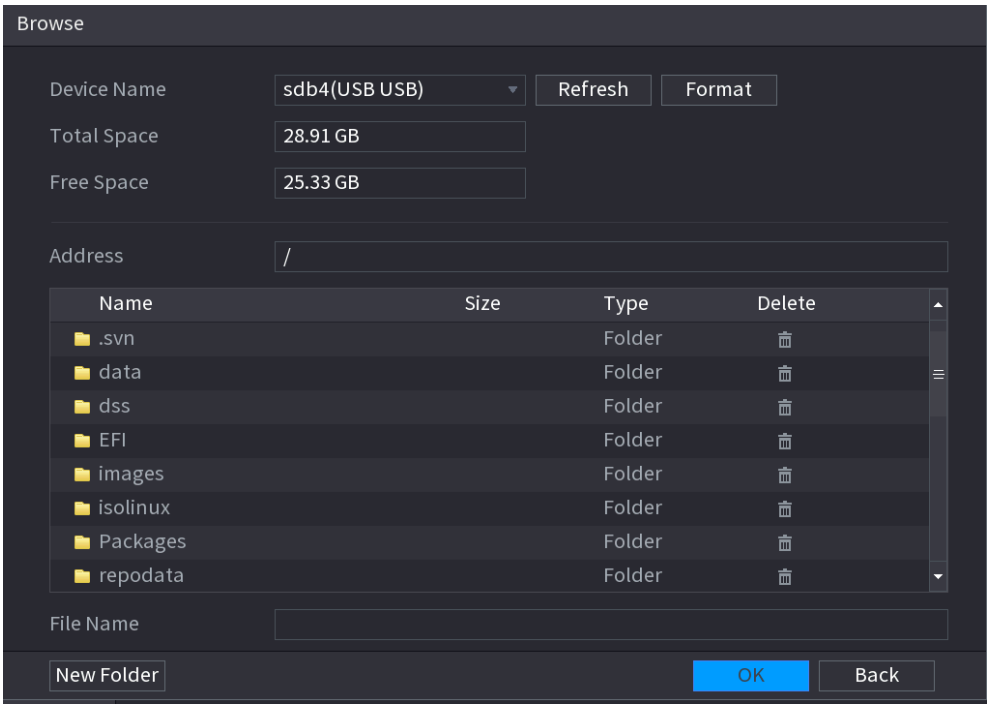
Step 2 Select **Main Menu** > **MAINTAIN** > **Manager** > **Update**

Figure 5-283 Update



Step 3 Click **Update**.

Figure 5-284 Browse



Step 4 Click the file that you want to upgrade.

Step 5 The selected file is displayed in the **Update File** box.

Step 6 Click **Start**.

5.19.4.4.2 Online Upgrade

Background Information

When the Device is connected to Internet, you can use online upgrade function to upgrade the system.

Before using this function, you need to check whether there is any new version by auto check or manual check.

- Auto check: The Device checks if there is any new version available at intervals.
- Manual check: Perform real-time check whether there is any new version available.

⚠

Ensure the correct power supply and network connection during upgrading; otherwise the upgrading might be failed.

Procedure

Step 1 Select **Main Menu** > **MAINTAIN** > **Manager** > **Update**.

Step 2 Check whether there is any new version available.

- Auto-check for updates: Enable Auto-check for updates.
- Manual check: Click **Manual Check**.

The system starts checking the new versions. After checking is completed, the check result is displayed.

- If the "It is the latest version" text is displayed, you do not need to upgrade.
- If the text indicating there is a new version, go to the step 3.

Step 3 Click **Update now** to update the system.

5.19.4.4.3 Uboot Upgrading

- Under the root directory in the USB storage device, there must be "u-boot.bin.img" file and "update.img" file saved, and the USB storage device must be in FAT32 format.
- Make sure the USB storage device is inserted; otherwise the upgrading cannot be performed.

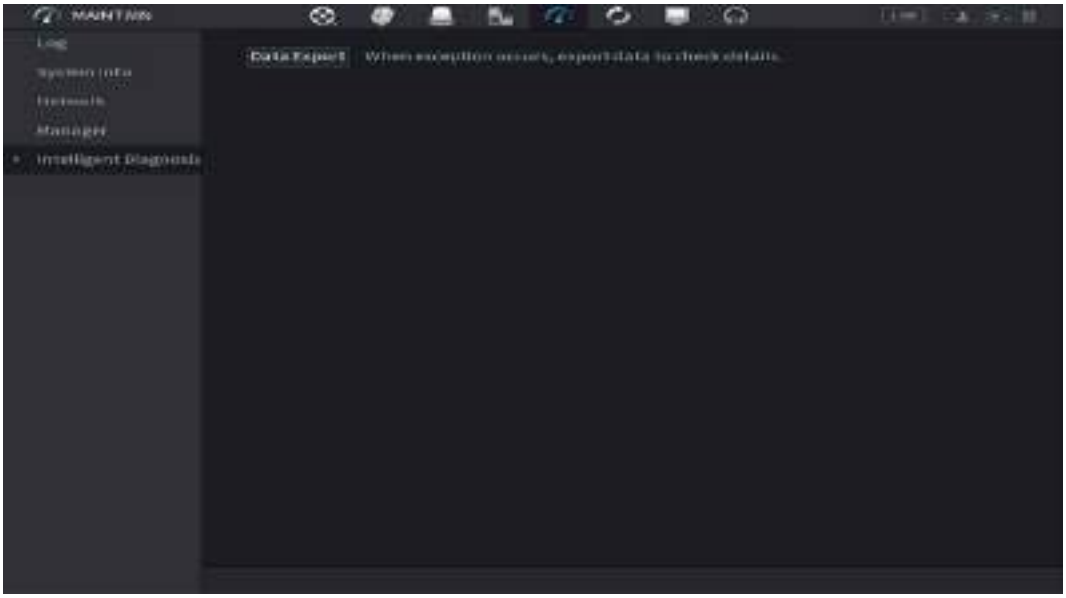
When starting the Device, the system automatically checkswhether there is a USB storage device connected and any upgrade file, and if yes and the check result of the upgrade file is correct, the system will upgrade automatically. The Uboot upgrade can avoid the situation that you have to upgrade through +TFTP when the Device is halted.

5.19.4.5 Intelligent Diagnosis

When exception occurs, export data to check details.

Select **Maintain** > **Intelligent Diagnosis**.

Figure 5-285 Intelligent diagnosis

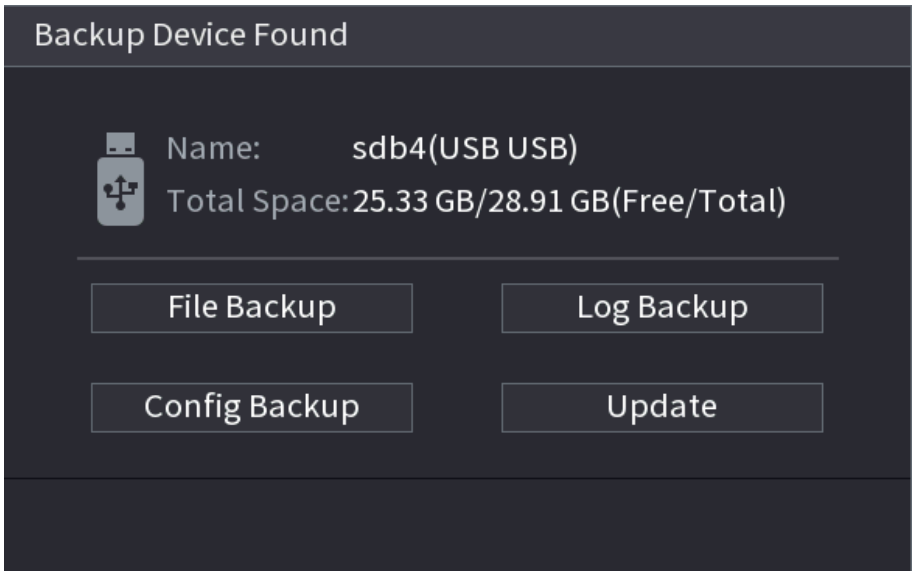


5.20 USB Device Auto Pop-up

After you inserted the USB device, system can auto detect it and pop up the following dialogue box. It allows you to conveniently backup file, log, configuration or update system.

You can add a USB keyboard through USB port, and it can input characters limited to soft keyboard.

Figure 5-286 USB device prompt



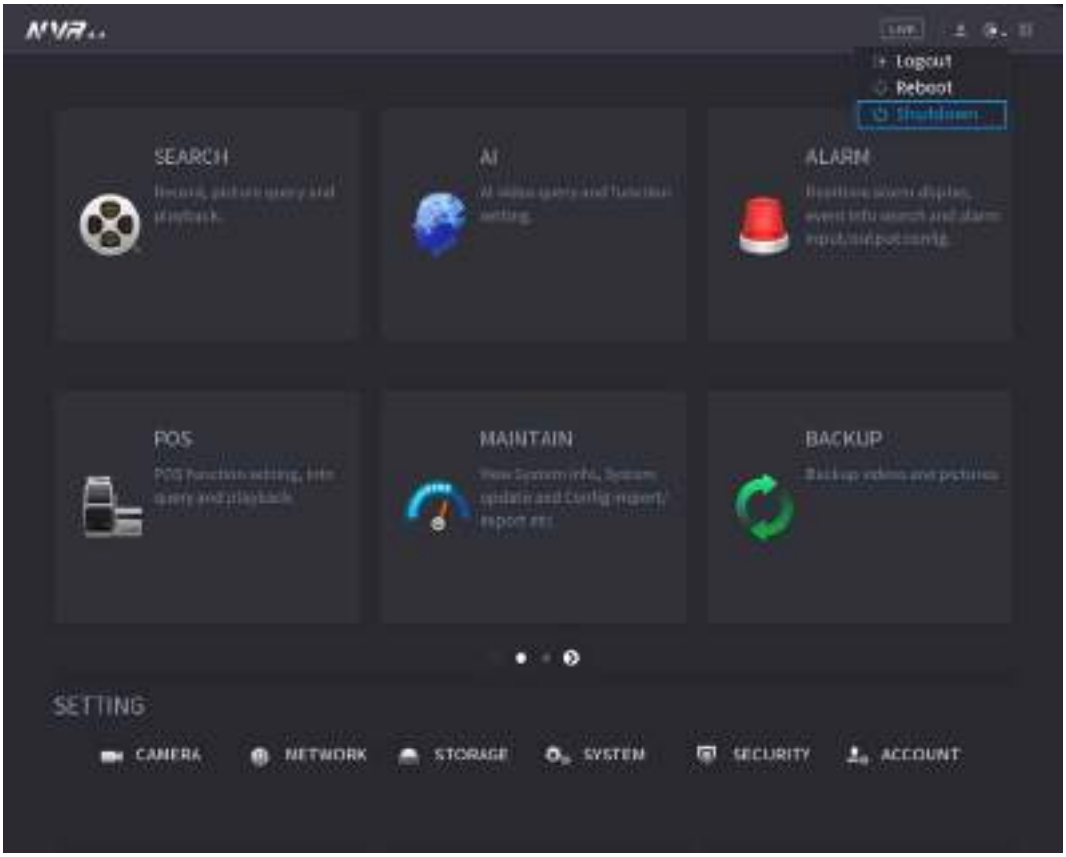
5.21 Shutdown

- When you see corresponding dialogue box "System is shutting down…" Do not click power on-off button directly.
- Do not unplug the power cable or click power on-off button to shutdown device directly when device is running (especially when it is recording.)
- Shut down the device and then unplug the power cable before you replace the HDD.

Procedure

- From the main menu (Recommended)
  1. Click at the upper-right corner.

Figure 5-287 Shutdown (1)



2. Select **Shutdown.**

   Draw the unlock pattern or input password first if you have no authority to shut down.

Figure 5-288 Shutdown (2)

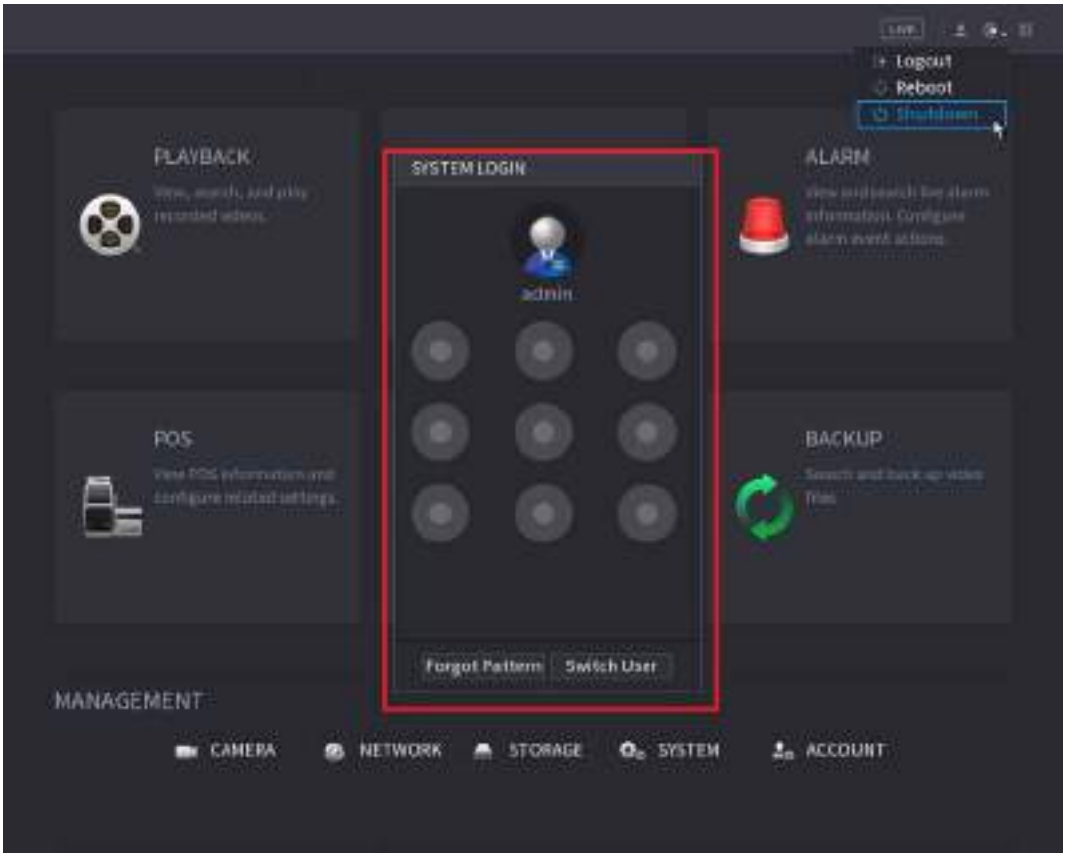
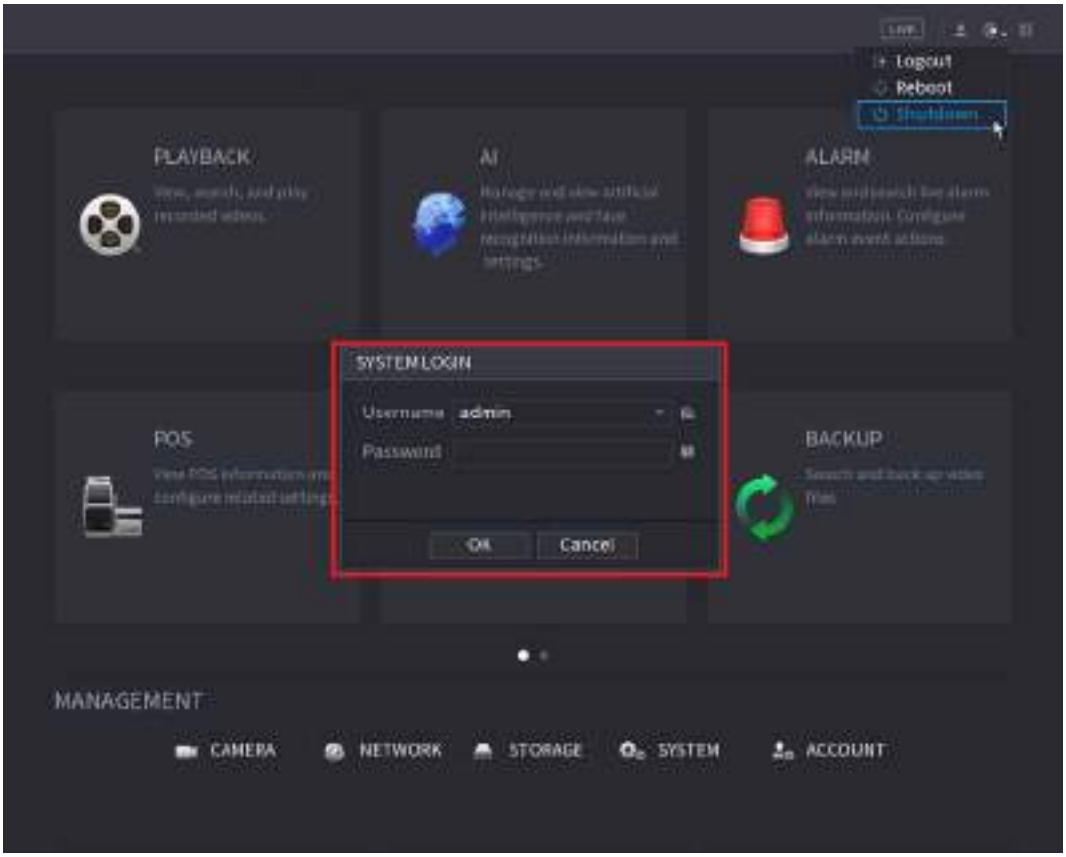


Figure 5-289 Shutdown (3)



- Remote Control

  Press the power button on the remote for at least 3 seconds.

- Press the power button at the rear panel of the device.

Auto Resume after Power Failure

The system can automatically backup video file and resume previous working status after power failure.

6 Web Operation

- The figures in the Manual are used for introducing the operations and only for reference. The actual interface might be different dependent on the model you purchased.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Besides Web, you can use our Smart PSS to login the device. For detailed information, see Smart PSS user's manual.

6.1 Network Connection

Background Information

- The factory default IP of the Device is 192.168.1.108.
- The Device supports monitoring on different browsers such as Safari, Firefox, Google to perform the functions such as multi-channel monitoring, PTZ control, and device parameters configurations.

Procedure

Step 1 Check to make sure the Device has connected to the network.

Step 2 Configure the IP address, subnet mask and gateway for the PC and the Device. For details about network configuration of the Device, see "5.19.3 Network".

Step 3 On your PC, check the network connection of the Device by using "ping ***.***.***.***". Usually the return value of TTL is 255.

6.2 Web Login

Step 1 Open the browser, enter the IP address of the Device, and then press Enter.

Figure 6-1 Login

Step 2 Enter the username and password.

- The default administrator account is **admin**. The password is the one that was configured during initial settings. To ensure your account security, we recommend you keep the password properly and change it regularly.
- Click to display the password.

Step 3 Click **Login**.

6.3 Web Main Menu

After you have logged in to the web, the main menu is displayed.
For detailed operations, see "5 Local Operations".

Figure 6-2 Main menu

Table 6-1 Main menu symbols

No.	Icon	Description
1		Includes configuration menu through which you can configure camera settings, network settings, storage settings, system settings, account settings, and view information.
2	None	Displays system date and time.
3		When you point to , the current user account is displayed.
4		Click , select Logout, Reboot, or Shutdown according to your actual situation.
5		Displays Cell Phone Client and Device SN QR Code. ● Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Cell Phone Client, and then you can start accessing the Device from your cell phone. ● Device SN: Obtain the Device SN by scanning the QR code. Go to the P2P management platform and add the Device SN into the platform. Then you can access and manage the device in the WAN. For details, see the P2P operation manual. You can also configure P2P function in the local configurations, see "5.11.18 P2P".
6		Displays the web main menu.

No.	Icon	Description
7	None	Includes eight function tiles: **LIVE, PLAYBACK, AI, ALARM, POS, OPERATION, BACKUP, DISPLAY, and AUDIO**. Click each tile to open the configuration interface of the tile. • **LIVE**: You can perform the operations such as viewing real-time video, configuring channel layout, setting PTZ controls, and using smart talk and instant record functions if needed. • **PLAYBACK**: Search for and play back the recorded video saved on the Device. • **ALARM**: Search for alarm information and configure alarm event actions. • **AI**: Configure and manage artificial intelligent events. It includes smart search, parameters, and database. • **POS**: View POS information and configure related settings. • **OPERATION**: View system information, import/export system configuration files, or update system. • **BACKUP**: Search and back up the video files to the local PC or external storage device such as USB storage device. • **DISPLAY**: Configure the display effect such as displaying content, image transparency, and resolution, and enable the zero-channel function. • **AUDIO**: Manage audio files and configure the playing schedule. The audio file can be played in response to an alarm event if the voice prompts function is enabled.

7 Glossary

- **DHCP**: DHCP (Dynamic Host Configuration Protocol) is one of the TCP/IP protocol cluster. It is mainly used to assign temporary IP addresses to computers on a network.
- **DDNS**: DDNS (Dynamic Domain Name Server) is a service that maps Internet domain names to IP addresses. This service is useful to anyone who wants to operate a server (web server, mail server, ftp server and more.) connected to the internet with a dynamic IP or to someone who wants to connect to an office computer or server from a remote location with software.
- **eSATA**: eSATA (External Serial AT) is an interface that provides fast data transfer for external storage devices. It is the extension specifications of a SATA interface.
- **GPS**: GPS (Global Positioning System) is a satellite system, protected by the US, safely orbiting thousands of kilometers above the earth.
- **PPPoE**: PPPoE (Point to Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site. Now the popular mode is ADSL and it adopts PPPoE protocol.
- **Wi-Fi**: Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The standard is for wireless local area networks (WLANs). It is like a common language that all the devices use to communicate to each other. It is actually IEEE802.11, a family of standard The IEEE (Institute of Electrical and Electronics Engineers Inc.)
- **3G**: 3G is the wireless network standard. It is called 3G because it is the third generation of cellular telecom standards. 3G is a faster network for phone and data transmission and speed Is over several hundred kbps. Now there are four standards: CDMA2000, WCDMA, TD-SCDMA and WiMAX.
- **Dual-stream**: The dual-stream technology adopts high-rate bit stream for local HD storage such as QCIF/CIF/2CIF/DCIF/4CIF encode and one low-rate bit stream for network transmission such as QCIF/CIF encode. It can balance the local storage and remote network transmission. The dual-stream can meet the difference band width requirements of the local transmission and the remote transmission. In this way, the local transmission using high-bit stream can achieve HD storage and the network transmission adopting low bit stream suitable for the fluency requirements of the 3G network such as WCDMA, EVDO, TD-SCDMA.
- **On-off value**: It is the non-consecutive signal sampling and output. It includes remote sampling and remote output. It has two statuses: 1/0.

8 FAQ

Questions	Reasons
The Device failed to start properly.	• Incorrect input power. • Incorrect connection of the power cord. • Damaged power switch. • Wrong program. • Damaged HDD. • Damaged mainboard.
The Device automatically shuts down or stops running.	• Unstable or insufficient input voltage. • Insufficient button power. • Improper operating environment. • Hardware error.
The Device cannot detect HDD.	• Damaged HDD or HDD ribbon. • Loose connection of HDD cable. • Damaged SATA port.
There is no video output in all channels.	• Program version is not correct. • Brightness is 0. • Hardware error.
I cannot find local records.	• Damaged HDD or HDD ribbon. • Program version is not correct. • The recorded file has been overwritten. • The recording function has been disabled.
Distorted recorded videos.	• Video quality setup is too low. • Program read error, bit data is too small. There is mosaic in the full screen. Restart the NVR to solve this problem. • HDD data ribbon error. • HDD malfunction. • NVR hardware malfunctions.
Time display is not correct.	• Setup is not correct. • Battery contact is not correct or voltage is too low. • Crystal is broken.

Questions	Reasons
NVR cannot control PTZ.	• Front panel PTZ error • PTZ decoder setup, connection or installation is not correct. • Cable connection is not correct. • PTZ setup is not correct. • PTZ decoder and NVR protocol is not compatible. • PTZ decoder and NVR address is not compatible. • When there are several decoders, add 120 Ohm between the PTZ decoder A/B cables furthest end to delete the reverberation or impedance matching. Otherwise the PTZ control is not stable. • The distance is too far.
I cannot log in client-end or web.	• For Windows 98 or Windows ME user, update your system to Windows 2000 sp4. Or you can install client-end software of lower version. Please note right now, our NVR is not compatible with Windows VISTA control. • ActiveX control has been disabled. • No dx8.1 or higher. Upgrade display card driver. • Network connection error. • Network setup error. • Password or username is invalid. • Client-end is not compatible with NVR program.
There is only mosaic no video when preview or playback video file remotely.	• Network fluency is not good. • Client-end resources are limit. • Current user has no right to monitor.
Network connection is not stable.	• Network is not stable. • IP address conflict. • MAC address conflict. • PC or device network card is not good.
Burn error /USB back error.	• Burner and NVR are in the same data cable. • System uses too much CPU resources. Stop record first and then begin backup. • Data amount exceeds backup device capacity. It might result in burner error. • Backup device is not compatible. • Backup device is damaged.
Keyboard cannot control NVR.	• NVR serial port setup is not correct. • Address is not correct. • When there are several switchers, power supply is not enough. • Transmission distance is too far.

Questions	Reasons
Alarm signal cannot be disarmed.	• Alarm setup is not correct. • Alarm output has been open manually. • Input device error or connection is not correct. • Some program versions might have this problem. Upgrade your system.
Alarm function is null.	• Alarm setup is not correct. • Alarm cable connection is not correct. • Alarm input signal is not correct. • There are two loops connect to one alarm device.
Record storage period is not enough.	• Camera quality is too low. Lens is dirty. Camera is installed against the light. Camera aperture setup is not correct. • HDD capacity is not enough. • HDD is damaged.
Cannot playback the downloaded file.	• There is no media player. • No DXB8.1 or higher graphic acceleration software. • There is no DivX503Bundle.exe control when you play the file transformed to AVI via media player. • No DivX503Bundle.exe or ffdshow-2004 1012 .exe in Windows XP OS.
Forgot local menu operation password or network password	Contact your local service engineer or our sales person for help. We can guide you to solve this problem.
There is no video. The screen is in black.	• IPC IP address is not right. • IPC port number is not right. • IPC account (username/password) is not right. • IPC is offline.
The displayed video is not full in the monitor.	Check current resolution setup. If the current setup is 1920*1080, then you need to set the monitor resolution as 1920*1080.
There is no HDMI output.	• Displayer is not in HDMI mode. • HDMI cable connection is not right.
The video is not fluent when I view in multiple-channel mode from the client-end.	• The network bandwidth is not sufficient. The multiple-channel monitor operation needs at least 100M or higher. • Your PC resources are not sufficient. For 16-ch remote monitor operation, the PC shall have the following environment: Quad Core, 2G or higher memory, independent displayer, display card memory 256M or higher.

Questions	Reasons
I cannot connect to the IPC	• Make sure that the IPC has booted up. • IPC network connection is right and it is online • IPC IP is in the blocklist. • The device has connected to the too many IPC. It cannot transmit the video. • Check the IPC port value and the time zone is the same as the NVR. • Make sure current network environment is stable.
After I set the NVR resolution as 1080P, my monitor cannot display.	Shut down the device and then reboot. When you reboot, press the Fn button at the same time and then release after 5 seconds. You can restore NVR resolution to the default setup.
My admin account has been changed and I cannot log in.	Use telnet and then input the following command: cd /mnt/mtd/Config/ rm -rf group rm -rf password Reboot the device to restore the default password.
After I login the Web, I cannot find the remote interface to add the IPC.	Clear the Web controls and load again.
There is IP and gateway, I can access the internet via the router. But I cannot access the internet after I reboot the NVR.	Use command PING to check you can connect to the gateway or not. Use telnet to access and then use command "ifconfig–a" to check device IP address. If you see the subnet mask and the gateway has changed after the reboot. Upgrade the applications and set again.
I use the VGA monitor. I want to know if I use the multiple-window mode, I see the video from the main stream or the sub stream?	• For 32-channel series product, the 9/16-window is using the sub stream. • For 4/8/16 series product, system is using the main stream no matter you are in what display mode.

Daily Maintenance

- Use the brush to clean the board, socket connector and the chassis regularly.
- The device shall be soundly earthed in case there is audio/video disturbance. Keep the device away from the static voltage or induced voltage.
- Unplug the power cable before you remove the audio/video signal cable, RS-232 or RS-485 cable.
- Do not connect the TV to the local video output port (VOUT). It might result in video output circuit.
- Always shut down the device properly. Use the shutdown function in the menu, or you can press the power button in the rear pane for at least three seconds to shut down the device. Otherwise it might result in HDD malfunction.
- Make sure the device is away from the direct sunlight or other heating sources. Keep the sound ventilation.
- Check and maintain the device regularly.

Appendix 1 HDD Capacity Calculation

Calculate the total capacity needed by each device according to video recording (video recording type and video file storage time).

1. According to Formula (1) to calculate storage capacity q_i that is the capacity of each channel needed for each hour, unit Mbyte.

$$q_i = d_i \div 8 \times 3600 \div 1024 \quad (1)$$

In the formula: d_i means the bit rate, unit Kbit/s

2. After video time requirement is confirmed, according to Formula (2) to calculate the storage capacity m_i, which is storage of each channel needed unit Mbyte.

$$m_i = q_i \times h_i \times D_i \quad (2)$$

In the formula:

h_i means the recording time for each day (hour)

D_i means number of days for which the video shall be kept

3. According to Formula (3) to calculate total capacity (accumulation) q_T that is needed for all channels in the device during **scheduled video recording**.

$$q_T = \sum_{i=1}^{c} m_i \quad (3)$$

In the formula:

c means total number of channels in one device

4. According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in device during **alarm video recording (including motion detection)**.

$$q_T = \sum_{i=1}^{c} m_i \times a\% \quad (4)$$

In the formula: $a\%$ means alarm occurrence rate

Appendix 2 Mouse Operation

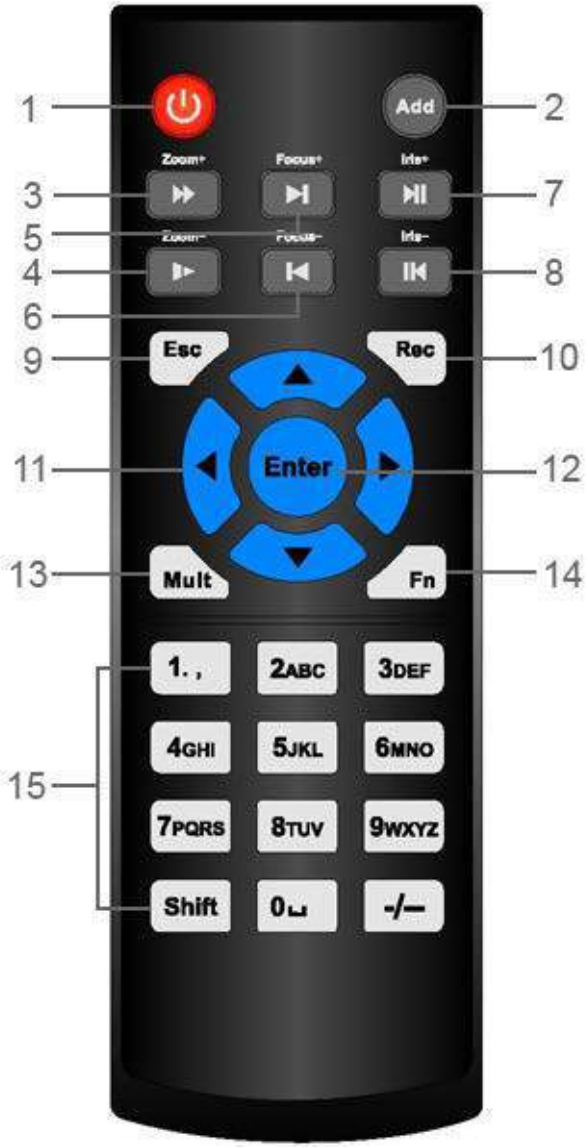
Appendix Table 2-1 Mouse operation

Operation	Description
Left click mouse	When you have selected one menu item, left click mouse to view menu content.
	Modify checkbox or motion detection status.
	Click combo box to pop up drop-down list
	In input box, you can select input methods. Left click the corresponding button on the panel you can input numeral/English character (lower case/upper case). Here← stands for backspace button. __ stands for space button. In English input mode: _ stands for input a backspace icon and← stands for deleting the previous character.  In numeral input mode: _ stands for clear and← stands for deleting the previous numeral.
Double left click mouse	Implement special control operation such as double click one item in the file list to playback the video.
	In multiple-window mode, double left click one channel to view in full-window. Double left click current video again to go back to previous multiple-window mode.
Right click mouse	In real-time monitor mode, pops up shortcut menu.
	Exit current menu without saving the modification.
Press middle button	In numeral input box: Increase or decrease numeral value.
	Switch the items in the checkbox.
	Page up or page down.
Move mouse	Select current control or move control.
Drag mouse	Select motion detection zone.
	Select privacy mask zone.

Appendix 3 Remote Control

Remote control is not our standard accessory and it is not included in the accessory package.

Appendix Figure 3-1 Remote control



No.	Name	Function
1	Power button	Press this button to boot up or shut down the device.
2	Address	Press this button to input device serial number, so that you can control the Device.
3	Forward	Multi-step forward speed and normal speed playback.
4	Slow motion	Multi-step slow motion speed or normal playback.
5	Next record	In playback state, press this button to play back the next video.

No.	Name	Function
6	Previous record	In playback state, press this button to play back the previous video.
7	Play/Pause	• In normal playback state, press this button to pause playback. • In pause state, press this button to resume to normal playback. • In live view window interface, press this button to enter video search menu.
8	Reverse/pause	In the reverse playback state, press this button to pause reverse playback.
		In the reverse playback pause state, press this button to resume to playback reversing state.
9	Esc	Go back to previous menu or cancel current operation (close front interface or control).
10	Record	• Start or stop record manually. • In record interface, use the direction buttons to select the channel that you want to record. • Press this button for at least 1.5 seconds, and the manual record interface will be displayed.
11	Direction keys	Switch between current activated controls by going left or right. In playback state, the keys control the playback progress bar. Aux function (such as operating the PTZ menu).
12	Enter/menu key	• Confirms an operation. • Go to the OK button. • Go to the menu.
13	Multiple-window switch	Switch between multiple-window and one-window.
14	Fn	• In single-channel monitoring mode, press this button to display the PTZ control and color setting functions. • Switch the PTZ control menu in PTZ control interface. • In motion detection interface, press this button with direction keys to complete setup. • In text mode, press and hold this button to delete the last character. To use the clearing function: Long press this button for 1.5 seconds. • In HDD menu, switch HDD recording time and other information as indicated in the pop-up message.

No.	Name	Function
15	Alphanumeric keys	• Input password, numbers. • Switch channel. • Press Shift to switch the input method.

Appendix 4 Compatible Network Camera List

Please note all the models in the following list for reference only. For those products not included in the list, please contact your local retailer or technical supporting engineer for detailed information.

Appendix Table 4-1 Compatible network camera list

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
AXIS	P1346	5.40.9.2	H264	√	ONVIF/Private
	P3344/P3344-E	5.40.9.2	H264	√	ONVIF/Private
	P5512	—	H264	√	ONVIF/Private
	Q1604	5.40.3.2	H264	√	ONVIF/Private
	Q1604-E	5.40.9	H264	√	ONVIF/Private
	Q6034E	—	H264	√	ONVIF/Private
	Q6035	5.40.9	H264	√	ONVIF/Private
	Q1755	—	H264	√	ONVIF/Private
	M7001	—	H264	√	Private
	M3204	5.40.9.2	H264	√	Private
	P3367	HEAD LFP4_0130220	H264	√	ONVIF
	P5532-P	HEAD LFP4_0130220	H264	√	ONVIF
ACTi	ACM-3511	A1D-220-V3.12.15-AC	MPEG4	√	Private
	ACM-8221	A1D-220-V3.13.16-AC	MPEG4	√	Private
Arecont	AV1115	65246	H264	√	Private
	AV10005DN	65197	H264	√	Private
	AV2115DN	65246	H264	√	Private
	AV2515DN	65199	H264	√	Private
	AV2815	65197	H264	√	Private
	AV5115DN	65246	H264	√	Private
	AV8185DN	65197	H264	√	Private
Bosch	NBN-921-P	—	H264	√	ONVIF
	NBC-455-12P	—	H264	√	ONVIF
	VG5-825	9500453	H264	√	ONVIF
	NBN-832	66500500	H264	√	ONVIF

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	VEZ-211-IWTEIVA	—	H264	√	ONVIF
	NBC-255-P	15500152	H264	√	ONVIF
	VIP-X1XF	—	H264	√	ONVIF
Brikcom	B0100	—	H264	√	ONVIF
	D100	—	H264	√	ONVIF
	GE-100-CB	—	H264	√	ONVIF
	FB-100A	v1.0.3.9	H264	√	ONVIF
	FD-100A	v1.0.3.3	H264	√	ONVIF
Cannon	VB-M400	—	H264	√	Private
CNB	MPix2.0DIR	XNETM11201 11229	H264	√	ONVIF
	VIPBL1.3MI RVF	XNETM21001 11229	H264	√	ONVIF
	IGC-2050F	XNETM21001 11229	H264	√	ONVIF
CP PLUS	CP-NC9-K	6.E.2.7776	H264	√	ONVIF/Private
	CP-NC9W-K	6.E.2.7776	H264	√	Private
	CP-ND10-R	cp20111129 ANS	H264	√	ONVIF
	CP-ND20-R	cp20111129 ANS	H264	√	ONVIF
	CP-NS12W-CR	cp20110808 NS	H264	√	ONVIF
	VS201	cp20111129 NS	H264	√	ONVIF
	CP-NB20-R	cp20110808B NS	H264	√	ONVIF
	CP-NT20VL3-R	cp20110808B NS	H264	√	ONVIF
	CP-NS36W-AR	cp20110808 NS	H264	√	ONVIF
	CP-ND20VL2-R	cp20110808B NS	H264	√	ONVIF
	CP-RNP-1820	cp20120821 NSA	H264	√	Private
	CP-RNC-TP20FL3C	cp20120821 NSA	H264	√	Private
	CP-RNP-12D	cp20120828 ANS	H264	√	Private

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	CP-RNC-DV10	cp20120821NSA	H264	√	Private
	CP-RNC-DP20FL2C	cp20120821NSA	H264	√	Private
Dynacolor	ICS-13	d20120214NS	H264	√	ONVIF/Private
	ICS-20W	vt20111123NSA	H264	√	ONVIF/Private
	NA222	—	H264	√	ONVIF
	MPC-IPVD-0313	k20111208ANS	H264	√	ONVIF/Private
	MPC-IPVD-0313AF	k20111208BNS	H264	√	ONVIF/Private
Honeywell	HIDC-1100PT	h.2.2.1824	H264	√	ONVIF
	HIDC-1100P	h.2.2.1824	H264	√	ONVIF
	HIDC-0100P	h.2.2.1824	H264	√	ONVIF
	HIDC-1300V	2.0.0.21	H264	√	ONVIF
	HICC-1300W	2.0.1.7	H264	√	ONVIF
	HICC-2300	2.0.0.21	H264	√	ONVIF
	HDZ20HDX	H20130114NSA	H264	√	ONVIF
LG	LW342-FP	—	H264	√	Private
	LNB5100	—	H264	√	ONVIF
Imatek	KNC-B5000	—	H264	√	Private
	KNC-B5162	—	H264	√	Private
	KNC-B2161	—	H264	√	Private
Panasonic	NP240/CH	—	MPEG4	√	Private
	WV-NP502	—	MPEG4	√	Private
	WV-SP102H	1.41	H264	√	ONVIF/Private
	WV-SP105H	—	H264	√	ONVIF/Private
	WV-SP302H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SP306H	1.4	H264, MPEG4	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	WV-SP508H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP509H	—	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW316H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW355H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW352H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW152E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW558H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW559H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP105H	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW155E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF336H	1.44	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF132E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF135E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF346H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF342H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SC385H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SC386H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SP539	1.66	H264, MPEG4	√	ONVIF
	DG-SC385	1.66	H264, MPEG4	√	ONVIF

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
PELCO	IXSOLW	1.8.1-20110912-1.9082-A1.6617	H264	√	Private
	IDE20DN	1.7.41.9111-O3.6725	H264	√	Private
	D5118	1.7.8.9310-A1.5288	H264	√	Private
	IM10C10	1.6.13.9261-O2.4657	H264	√	Private
	DD4N-X	01.02.0015	MPEG4	√	Private
	DD423-X	01.02.0006	MPEG4	√	Private
	D5220	1.8.3-FC2-20120614-1.9320-A1.8035	H264	√	Private
Samsung	SNB-3000P	2.41	H264, MPEG4	√	ONVIF/Private
	SNP-3120	1.22_110120_1	H264, MPEG4	√	ONVIF/Private
	SNP-3370	1.21_110318	MPEG4	√	Private
	SNB-5000	2.10_111227	H264, MPEG4	√	ONVIF/Private
	SND-5080	—	H264, MPEG4	√	Private
	SNZ-5200	1.02_110512	H264, MPEG4	√	ONVIF/Private
	SNP-5200	1.04_110825	H264, MPEG4	√	ONVIF/Private
	SNB-7000	1.10_110819	H264	√	ONVIF/Private
	SNB-6004	V1.0.0	H264	√	ONVIF
Sony	SNC-DH110	1.50.00	H264	√	ONVIF/Private
	SNC-CH120	1.50.00	H264	√	ONVIF/Private
	SNC-CH135	1.73.01	H264	√	ONVIF/Private
	SNC-CH140	1.50.00	H264	√	ONVIF/Private
	SNC-CH210	1.73.00	H264	√	ONVIF/Private
	SNC-DH210	1.73.00	H264	√	ONVIF/Private
	SNC-DH240	1.50.00	H264	√	ONVIF/Private
	SNC-DH240-T	1.73.01	H264	√	ONVIF/Private
	SNC-CH260	1.74.01	H264	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	SNC-CH280	1.73.01	H264	√	ONVIF/Private
	SNC-RH-124	1.73.00	H264	√	ONVIF/Private
	SNC-RS46P	1.73.00	H264	√	ONVIF/Private
	SNC-ER550	1.74.01	H264	√	ONVIF/Private
	SNC-ER580	1.74.01	H264	√	ONVIF/Private
	SNC-ER580	1.78.00	H264	√	ONVIF
	SNC-VM631	1.4.0	H264	√	ONVIF
	WV-SP306	1.61.00	H264, MPEG4	√	SDK
	WV-SP306	1.61.00	H264	√	ONVIF
	SNC-VB600	1.5.0	H264	√	Private
	SNC-VM600	1.5.0	H264	√	Private
	SNC-VB630	1.5.0	H264	√	Private
	SNC-VM630	1.5.0	H264	√	Private
SANYO	VCC-HDN4000PC	—	H264	√	ONVIF

Appendix 5 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (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 device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
10. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
12. **Network Log**
    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
13. **Construct a Safe Network Environment**
    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

More information

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883