- ◇ 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.

5.9.5.5.3 Report Query

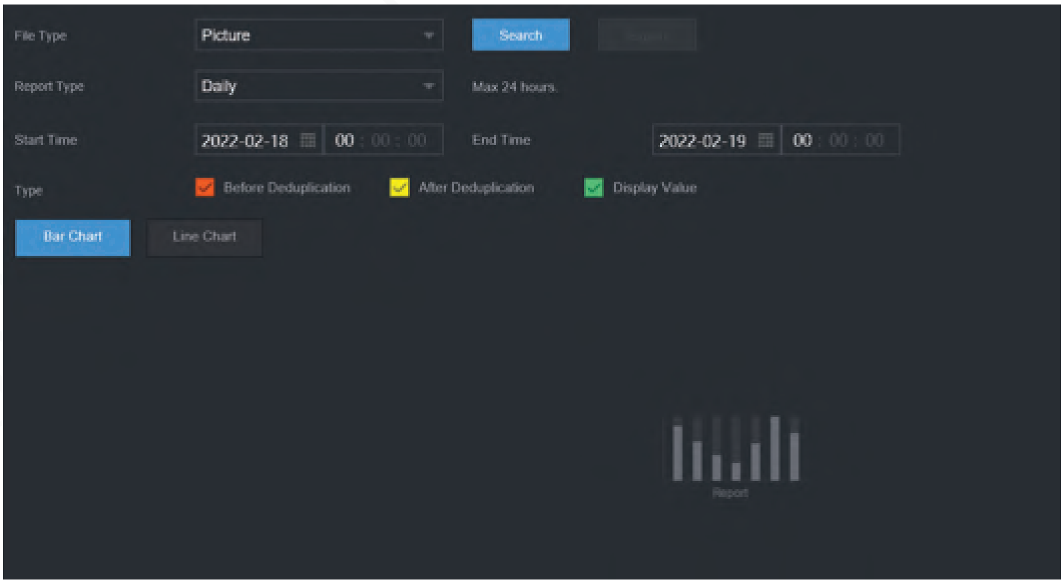
You can search for and export face statistics.

- 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** > **Face Statistics**.

Figure 5-102 Face statistics



File Type: Picture

Report Type: Daily

Max 24 hours.

Start Time: 2022-02-18 00 : 00 : 00

End Time: 2022-02-19 00 : 00 : 00

Type: ☑ Before Deduplication ☑ After Deduplication ☑ Display Value

Step 2 Select the 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 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".

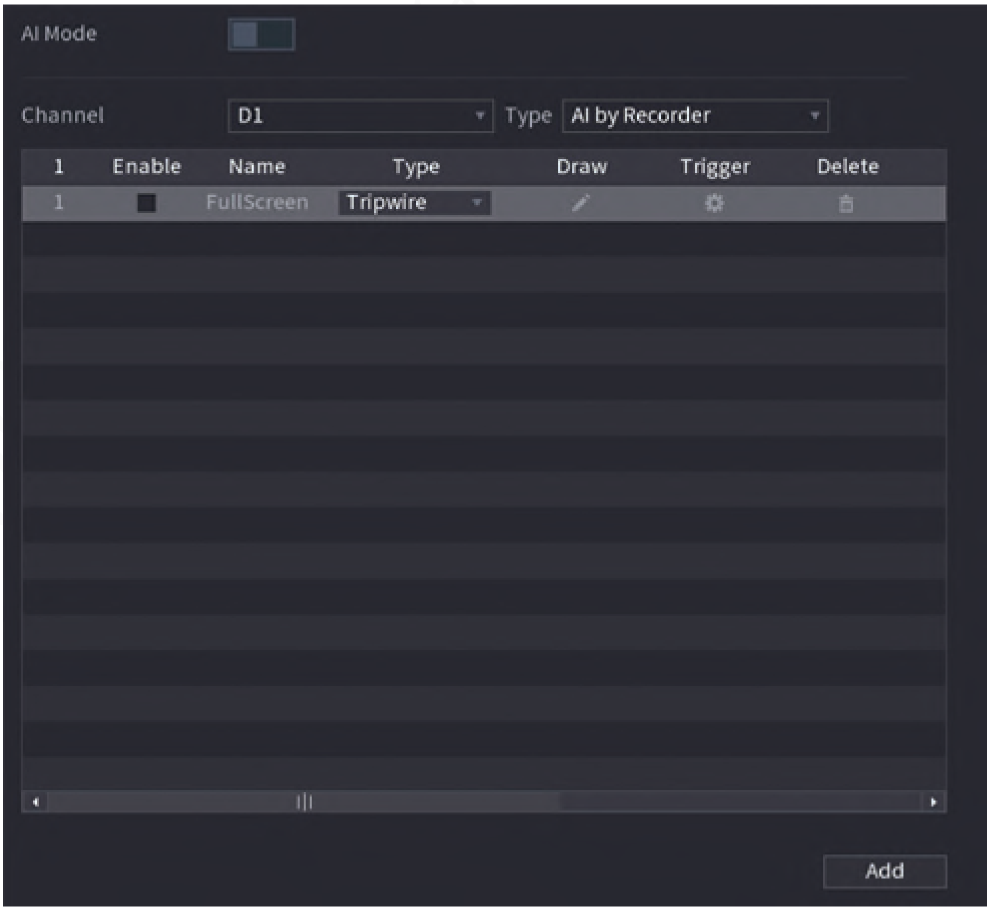
5.9.6.2 Configuring IVS

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



AI Mode

Channel: D1 Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

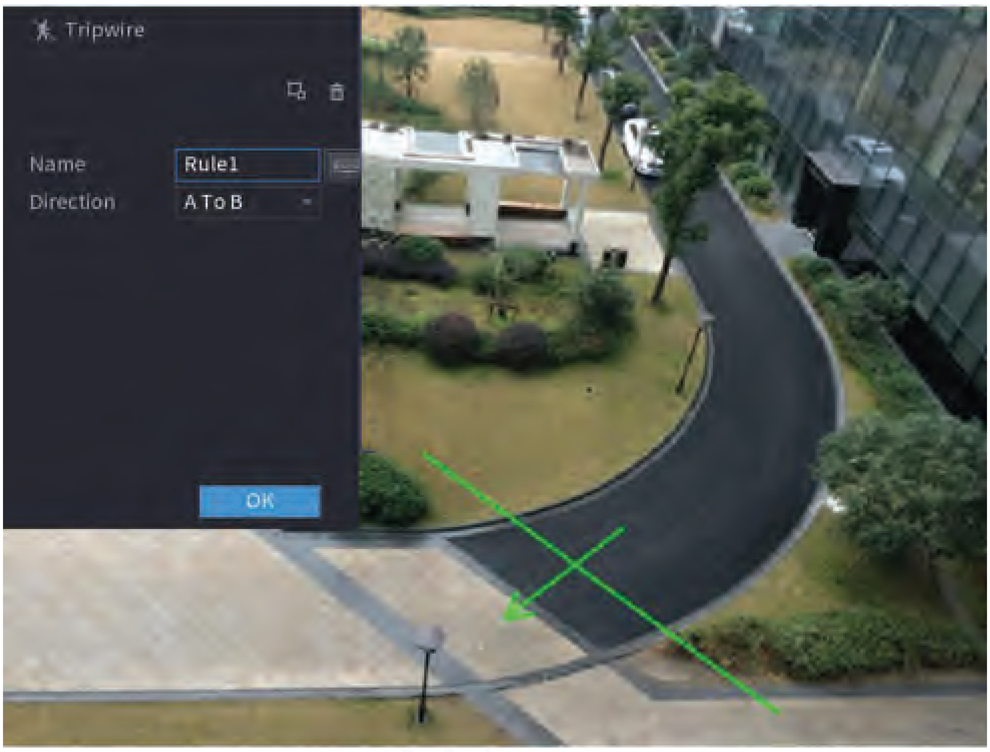
Step 3 Click **Add** to add a rule.

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)

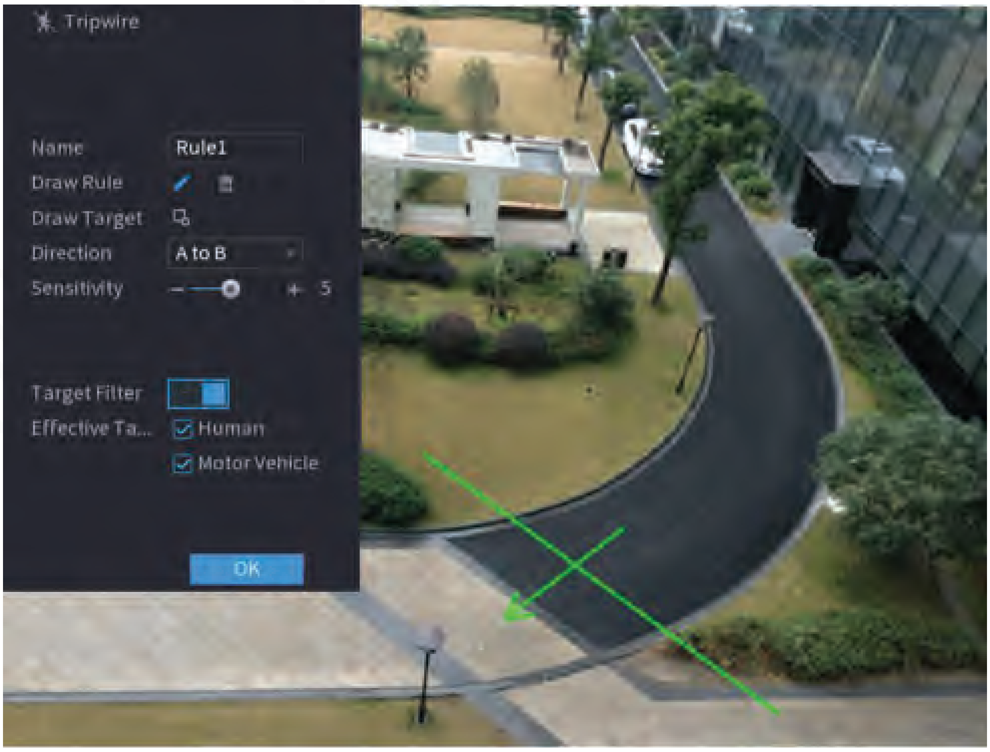


Tripwire

Name: Rule1

Direction: A To B

Figure 5-105 Tripwire (AI by recorder)



Tripwire

Name: Rule1

Draw Rule

Draw Target

Direction: A to B

Sensitivity: 5

Target Filter

Effective Ta...: ☑ Human ☑ Motor Vehicle

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.

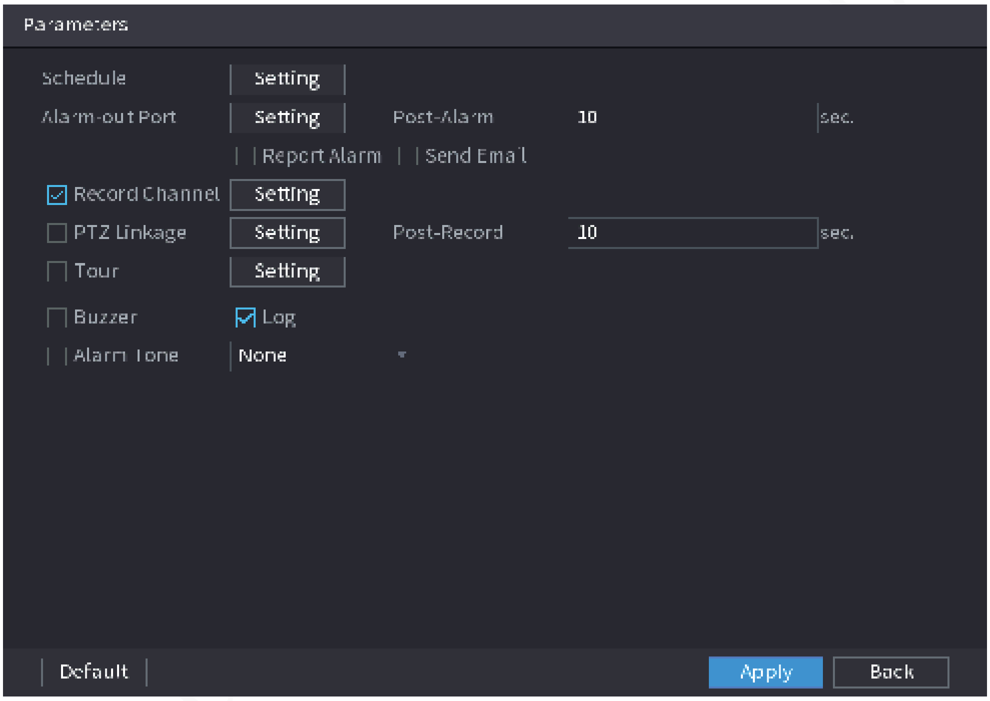
Table 5-27 Tripwire parameters

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



Parameters

Schedule: Setting

Alarm-out Port: Setting Post-Alarm: 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel: Setting

□ PTZ Linkage: Setting Post-Record: 10 sec.

□ Tour: Setting

□ Buzzer ☑ Log

□ Alarm Tone: None

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**.

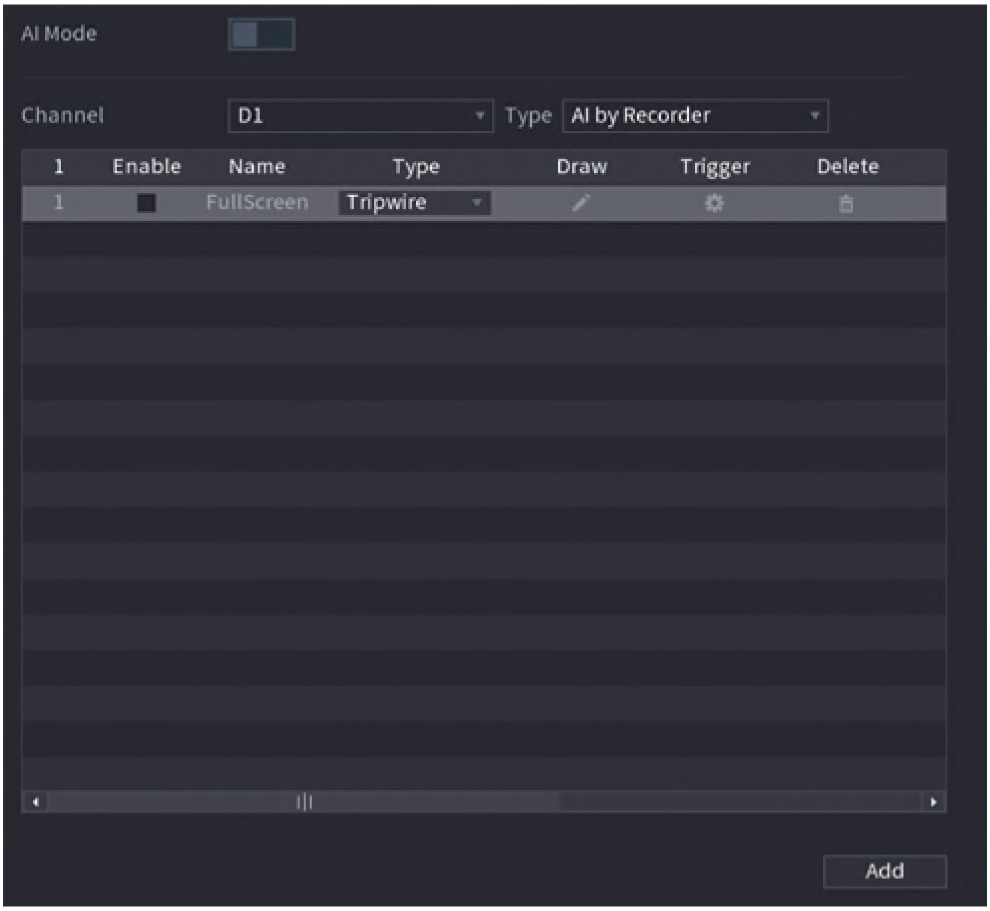
Step 7 Select the **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1

Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

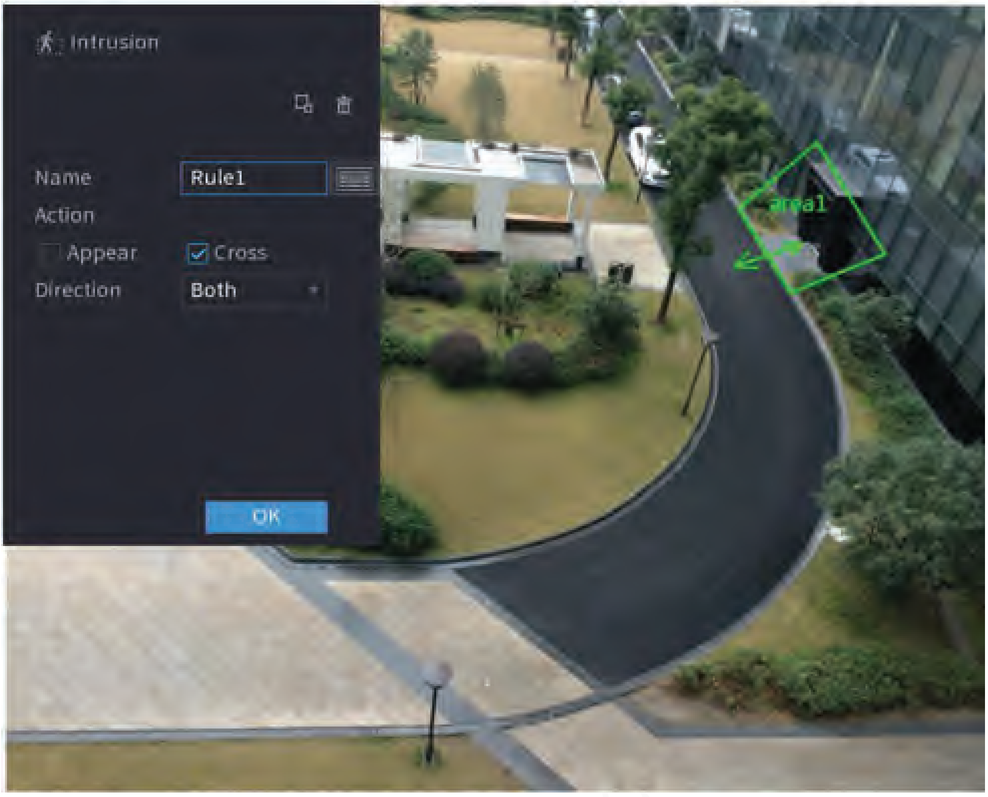
Step 3 Click **Add** to add a rule.

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)



Intrusion

Name: Rule1

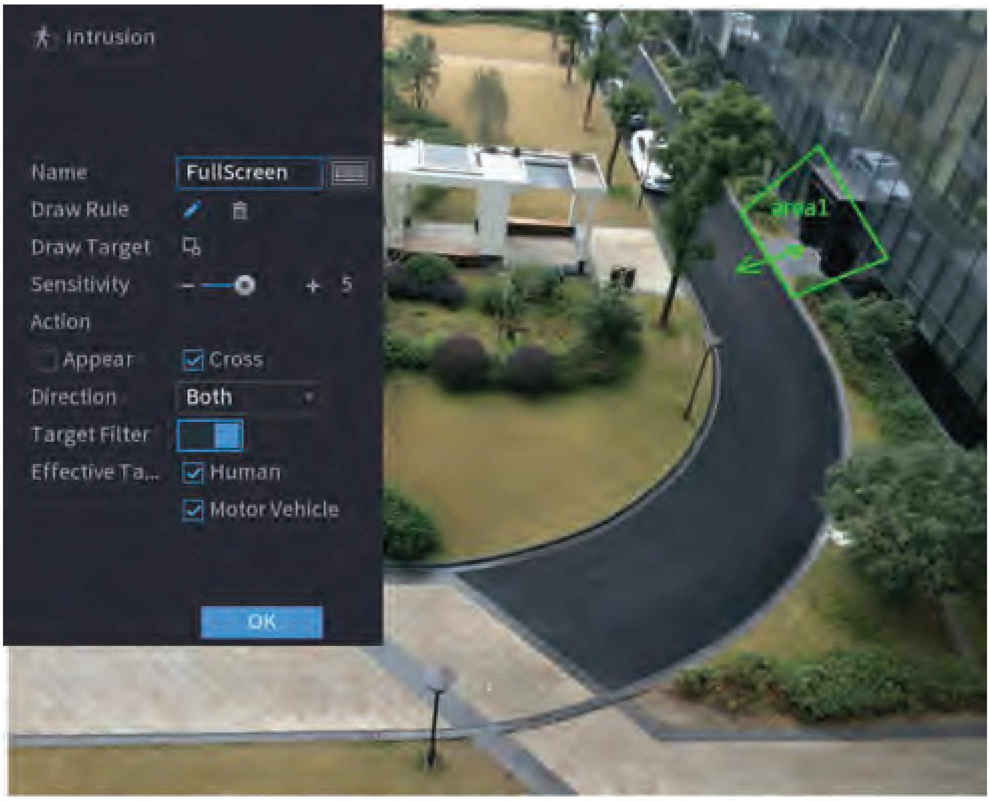
Action

□ Appear ☑ Cross

Direction: Both

OK

Figure 5-109 Intrusion (AI by recorder)



Intrusion

Name: FullScreen

Draw Rule

Draw Target

Sensitivity: 5

Action

□ Appear ☑ Cross

Direction: Both

Target Filter

Effective Ta... ☑ Human ☑ Motor Vehicle

OK

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.

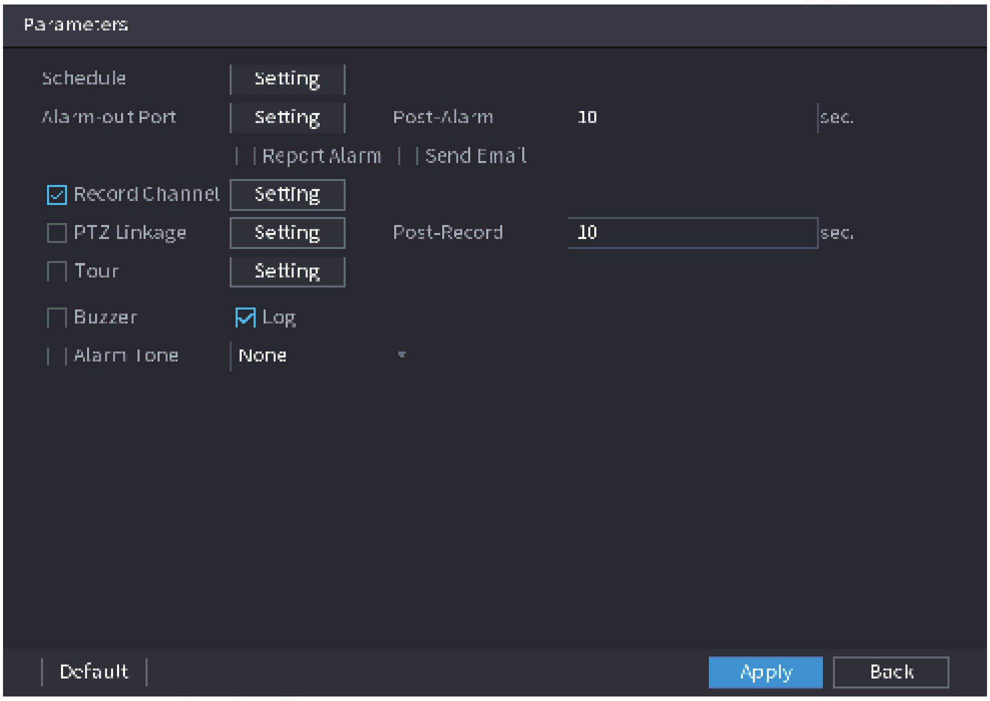
Table 5-28 Intrusion parameters

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

Default Apply Back

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**.

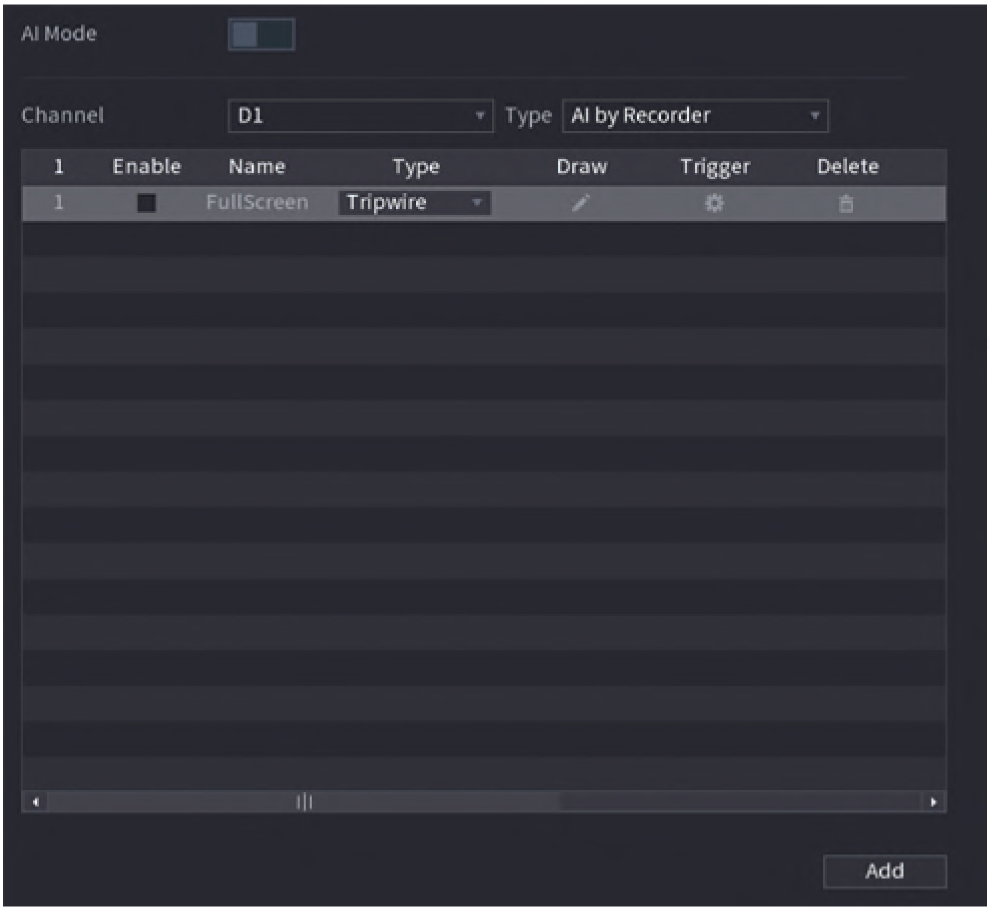
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel D1 Type AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

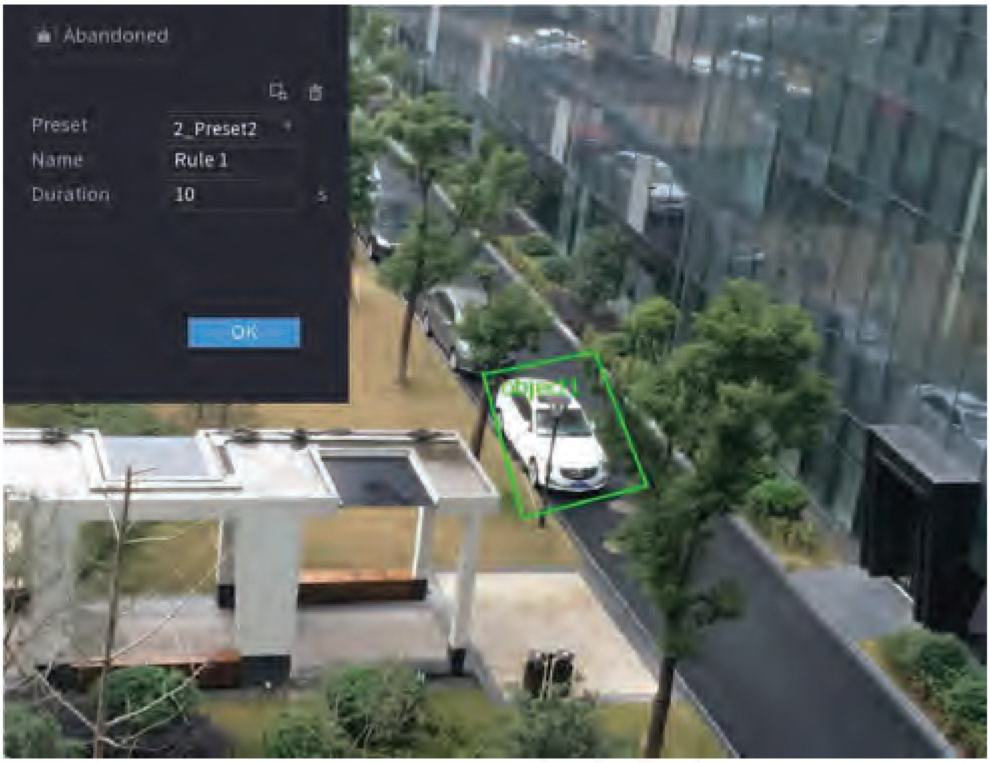
Step 3 Click **Add** to add a rule.

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



Abandoned

Preset: 2_Preset2

Name: Rule 1

Duration: 10 s

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.

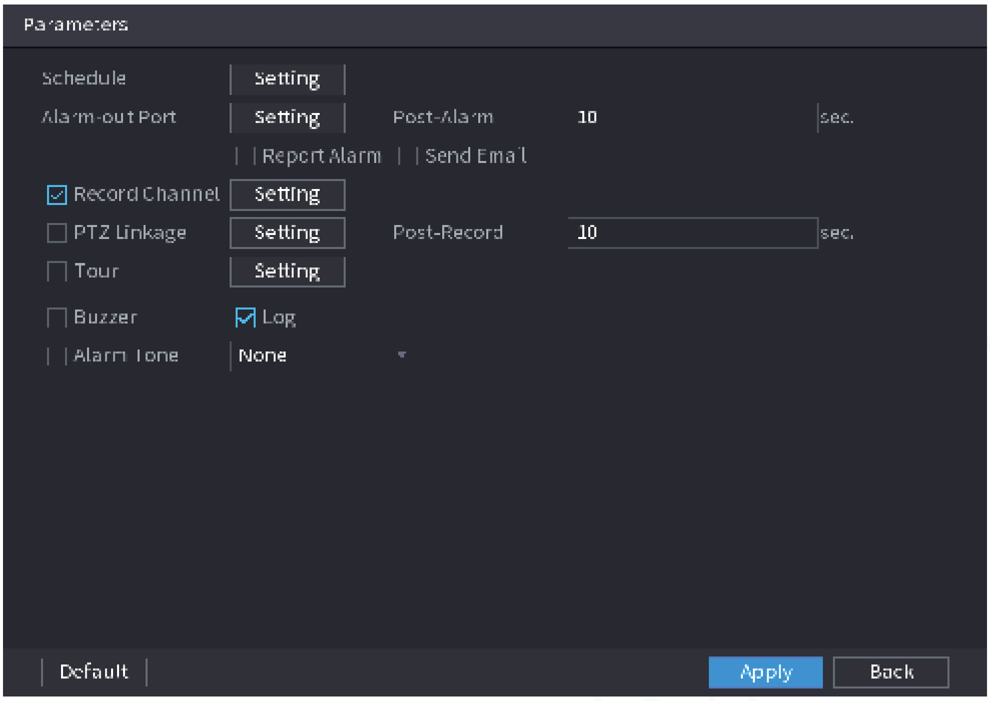
Table 5-29 Parameters of abandoned object detection

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



Schedule: Setting

Alarm-out Port: Setting — Post-Alarm: 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel: Setting

□ PTZ Linkage: Setting — Post-Record: 10 sec.

□ Tour: Setting

□ Buzzer ☑ Log

□ Alarm Tone: None

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**.

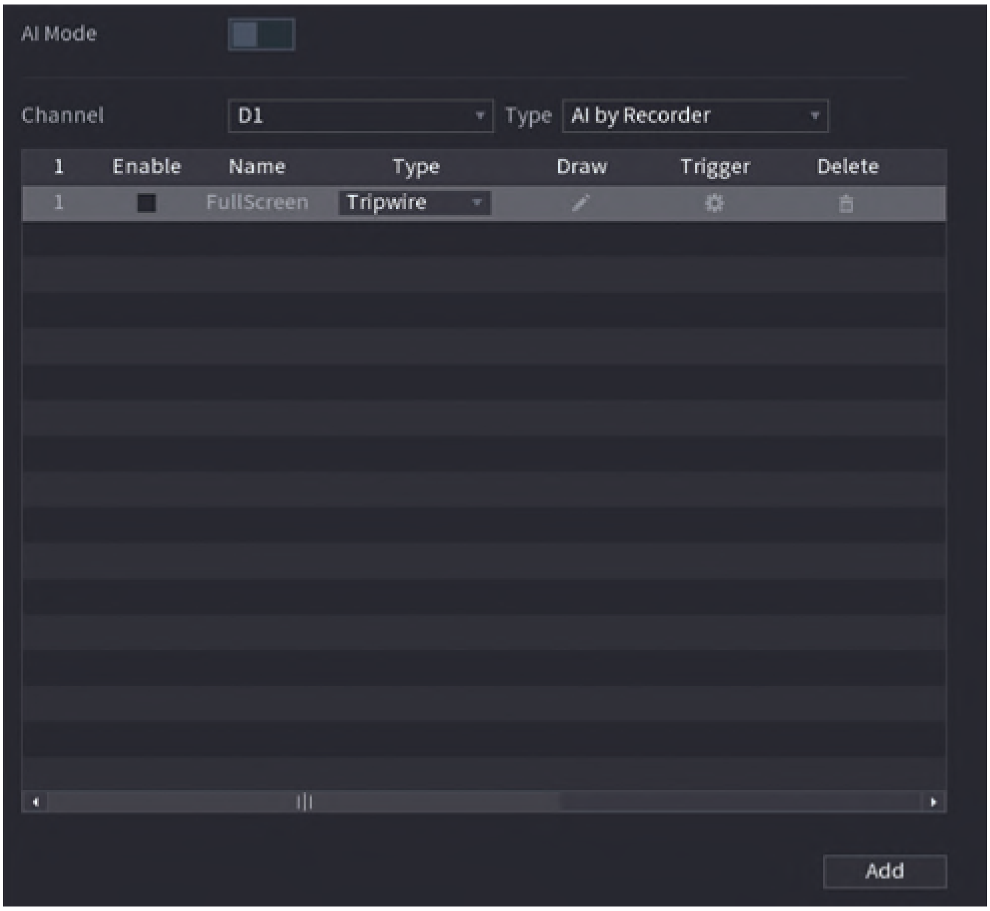
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1 Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

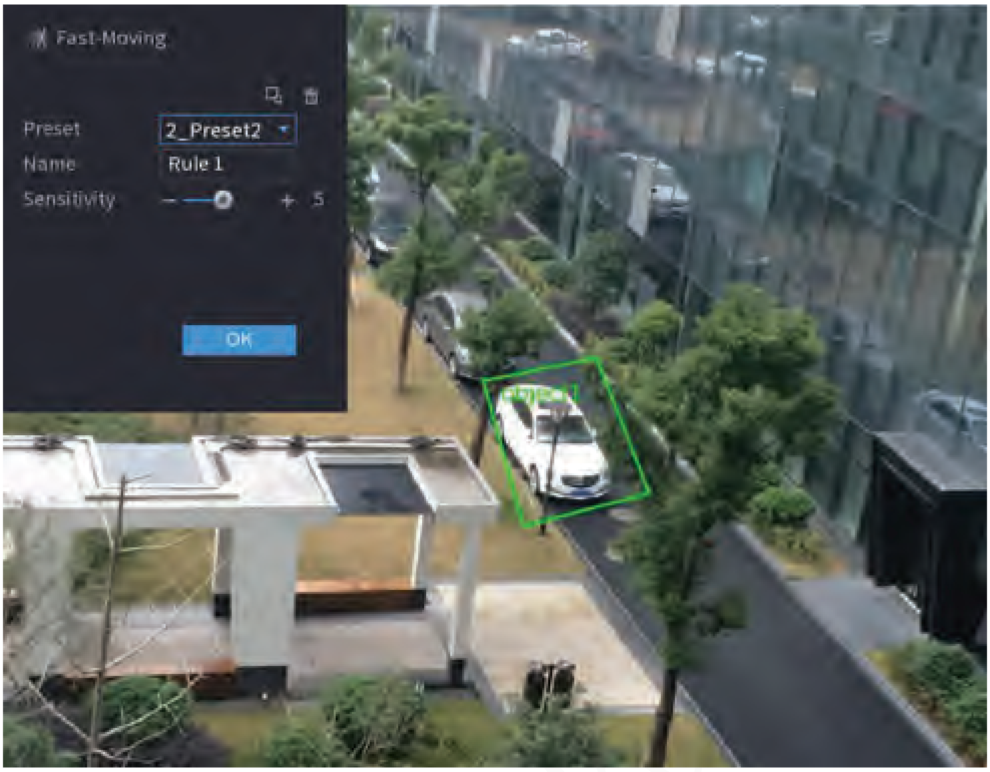
Step 3 Click **Add** to add a rule.

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



Fast-Moving

Preset: 2_Preset2

Name: Rule 1

Sensitivity: 5

OK

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.

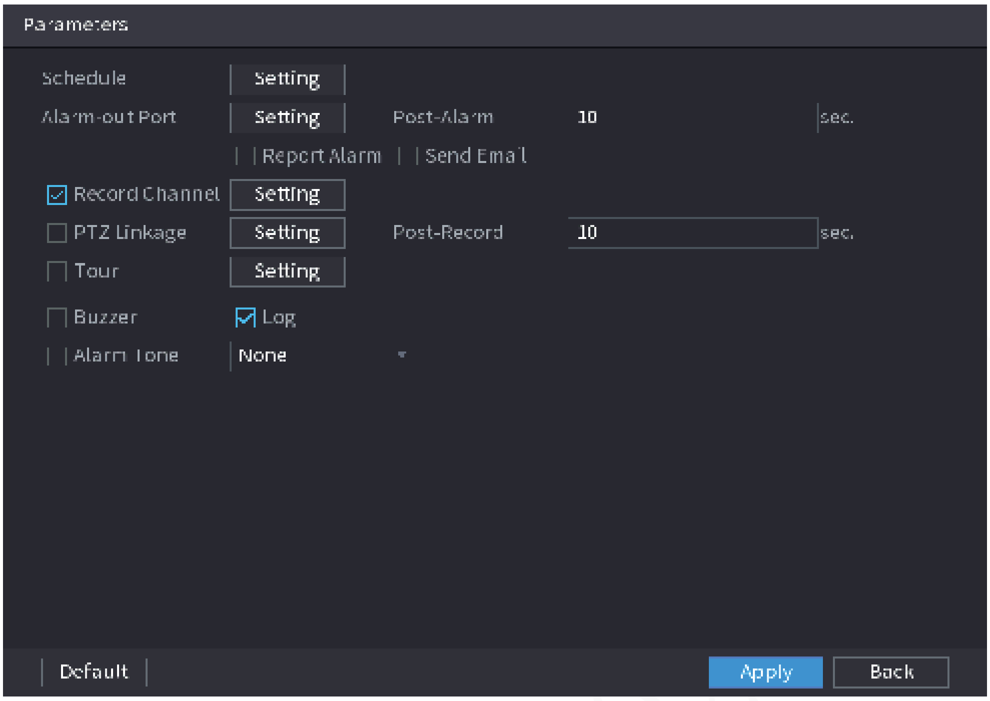
Table 5-30

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

Default Apply Back

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**.

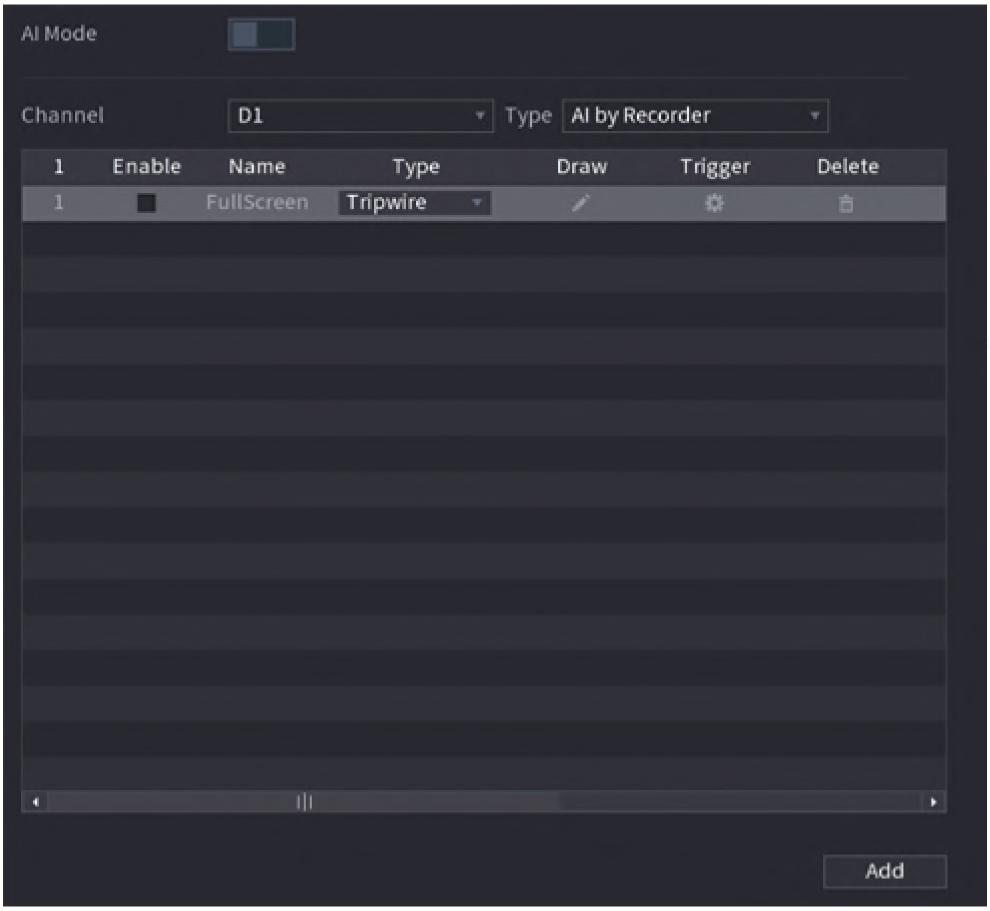
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1 | Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

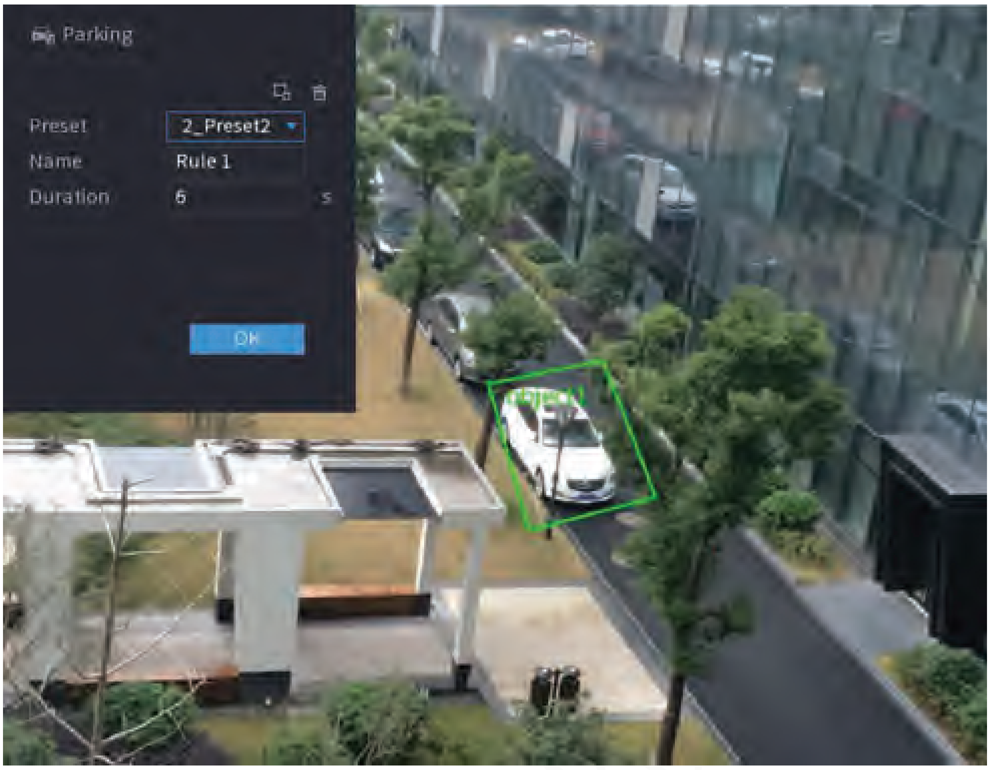
Step 3 Click **Add** to add a rule.

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



Parking

Preset	2_Preset2
Name	Rule 1
Duration	6 s

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.

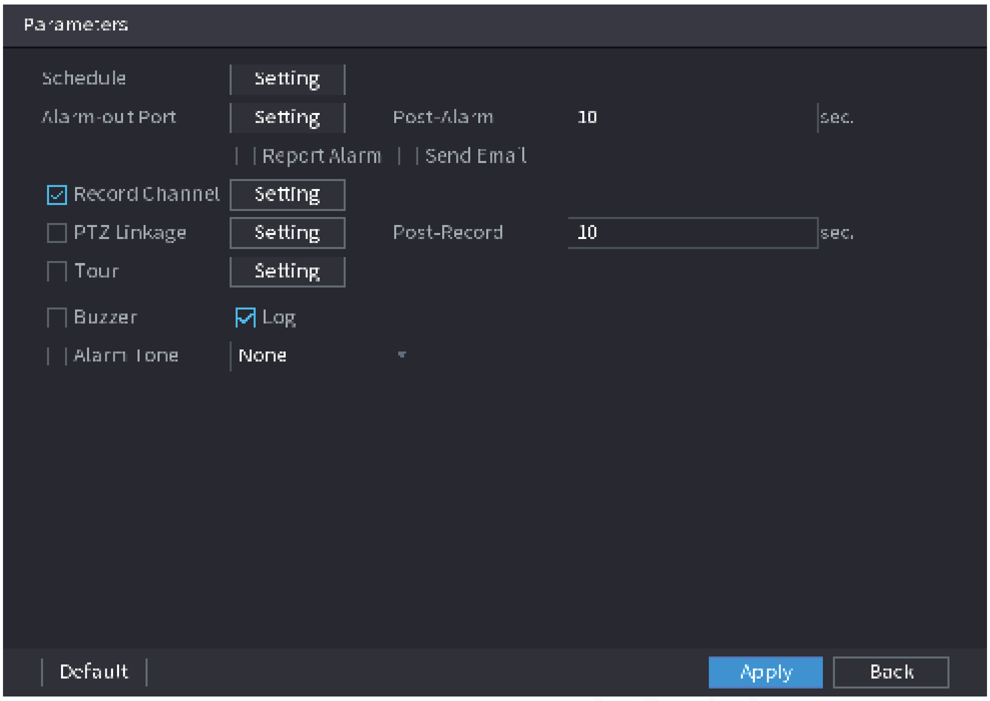
Table 5-31

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



Schedule: Setting

Alarm-out Port: Setting — Post-Alarm: 10 sec.

☐ Report Alarm ☐ Send Email

☑ Record Channel: Setting

☐ PTZ Linkage: Setting — Post-Record: 10 sec.

☐ Tour: Setting

☐ Buzzer ☑ Log

☐ Alarm Tone: None

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**.

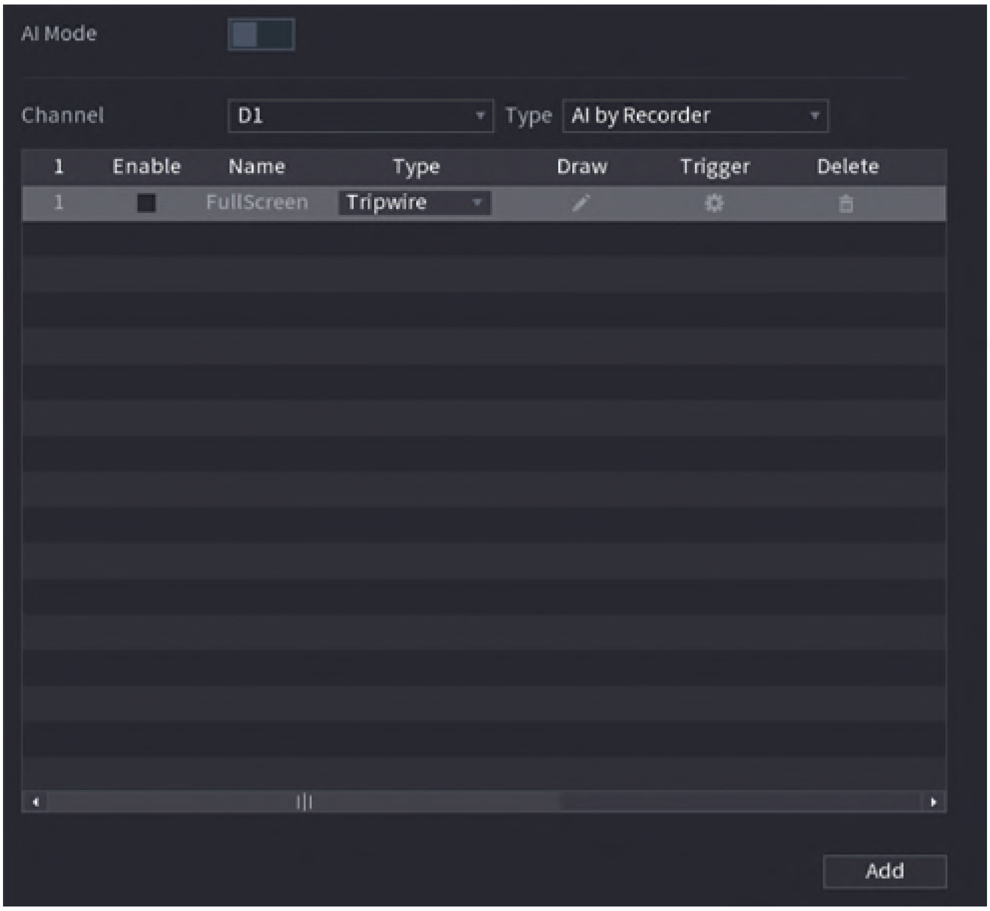
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1

Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

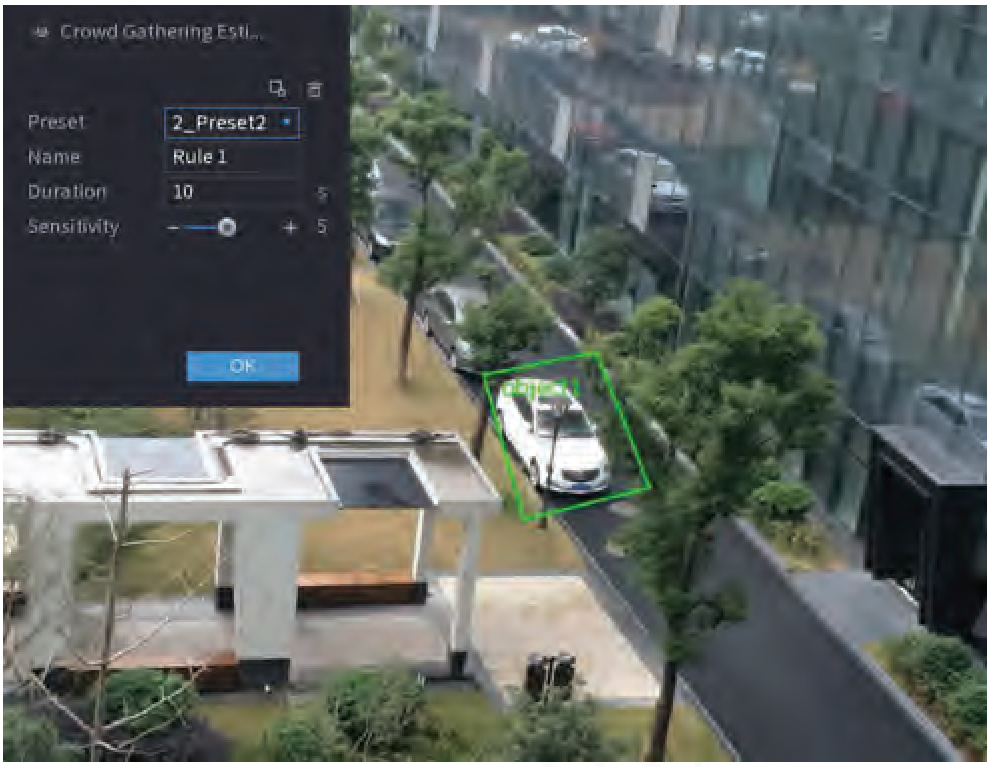
Step 3 Click **Add** to add a rule.

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



Crowd Gathering Esti...

Preset 2_Preset2

Name Rule 1

Duration 10 s

Sensitivity 5

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.

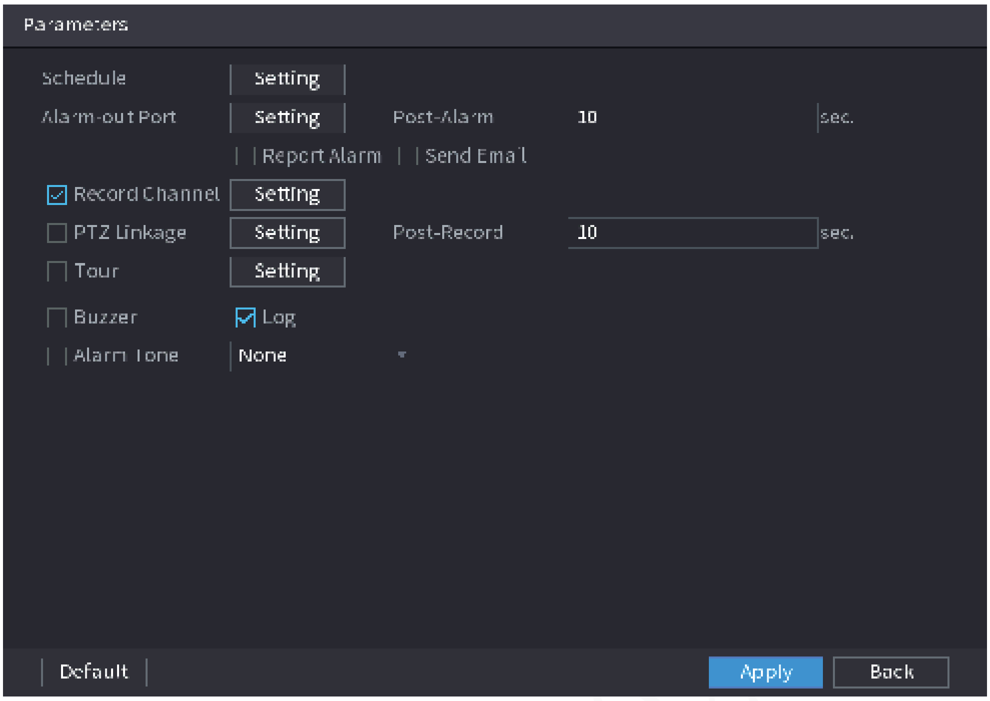
Table 5-32 Crowd gathering parameters

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


Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

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**.

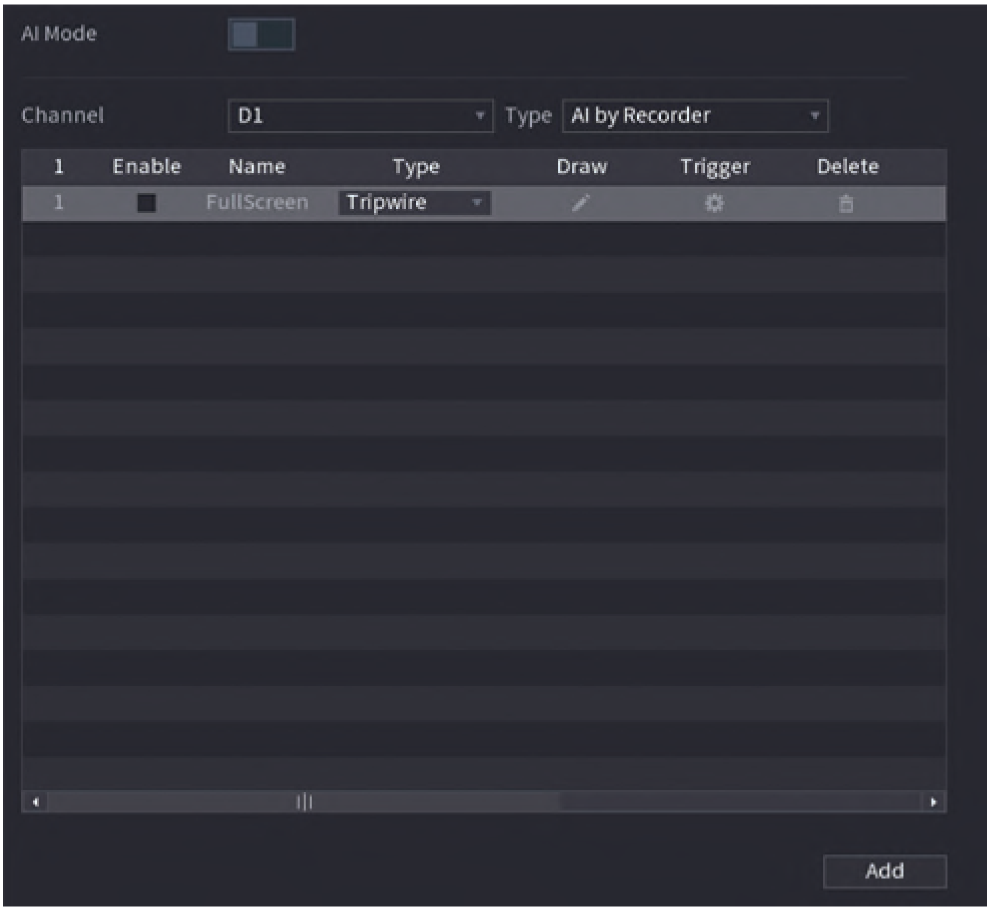
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1 Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

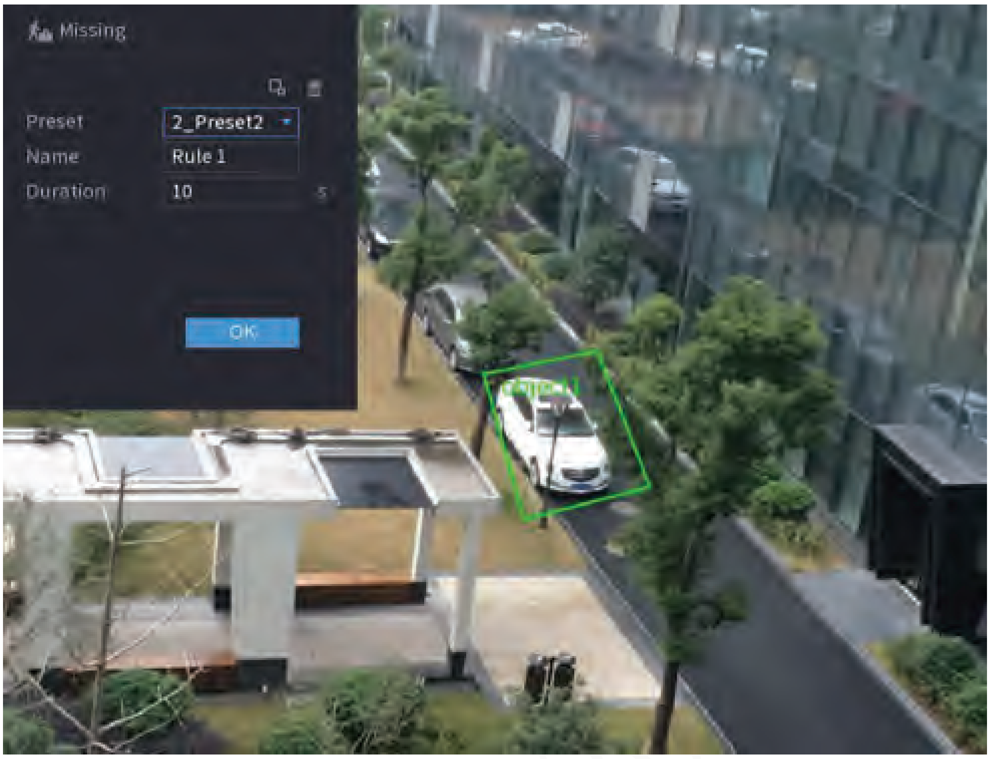
Step 3 Click **Add** to add a rule.

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



Preset 2_Preset2

Name Rule 1

Duration 10 s

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.

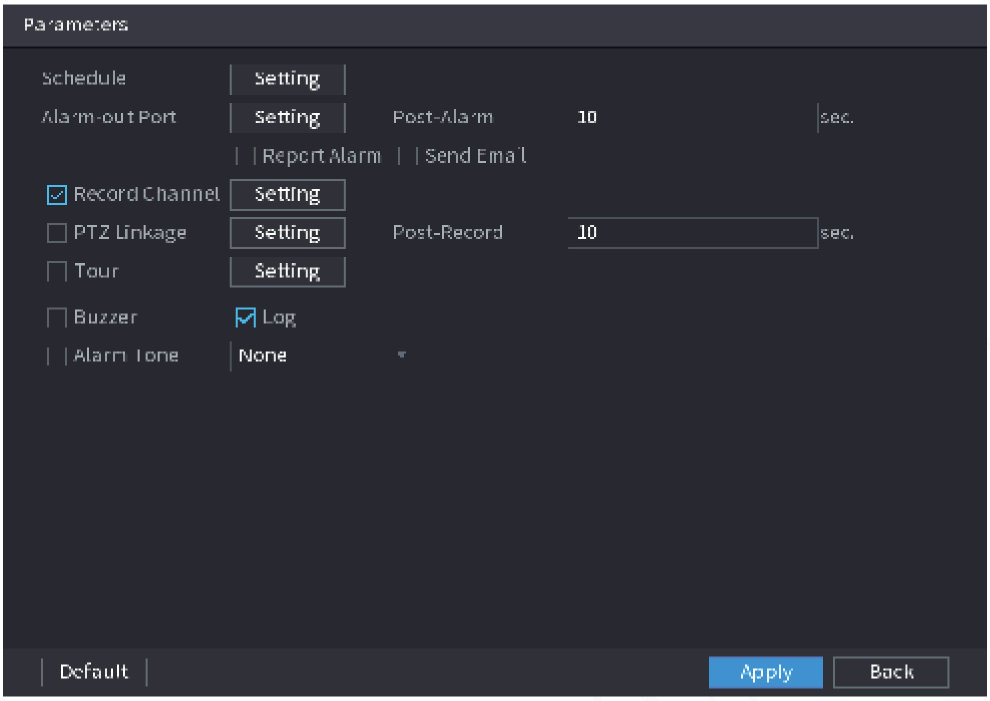
Table 5-33 Parameters of missing object detection

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

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**.

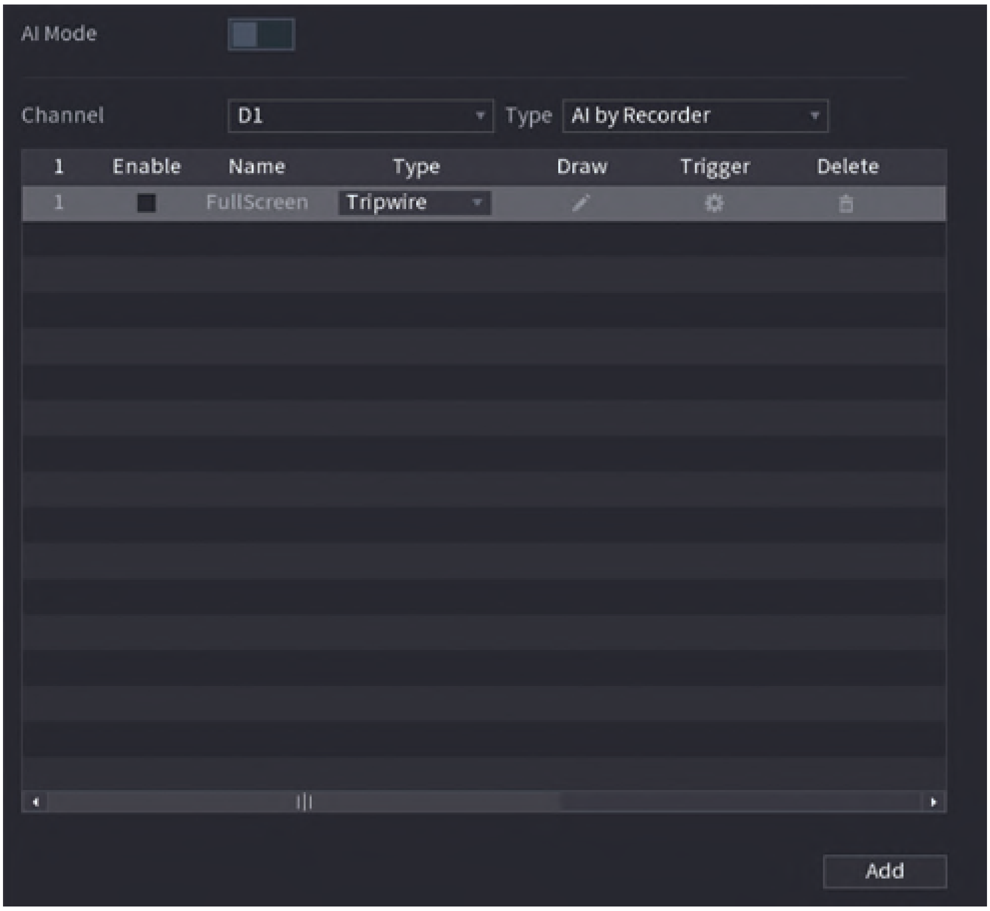
Step 7 Select **Enable** checkbox and then click **Apply**.

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



AI Mode

Channel: D1

Type: AI by Recorder

1	Enable	Name	Type	Draw	Trigger	Delete
1	■	FullScreen	Tripwire	✎	⚙	🗑

Step 2 Select channel and AI type.

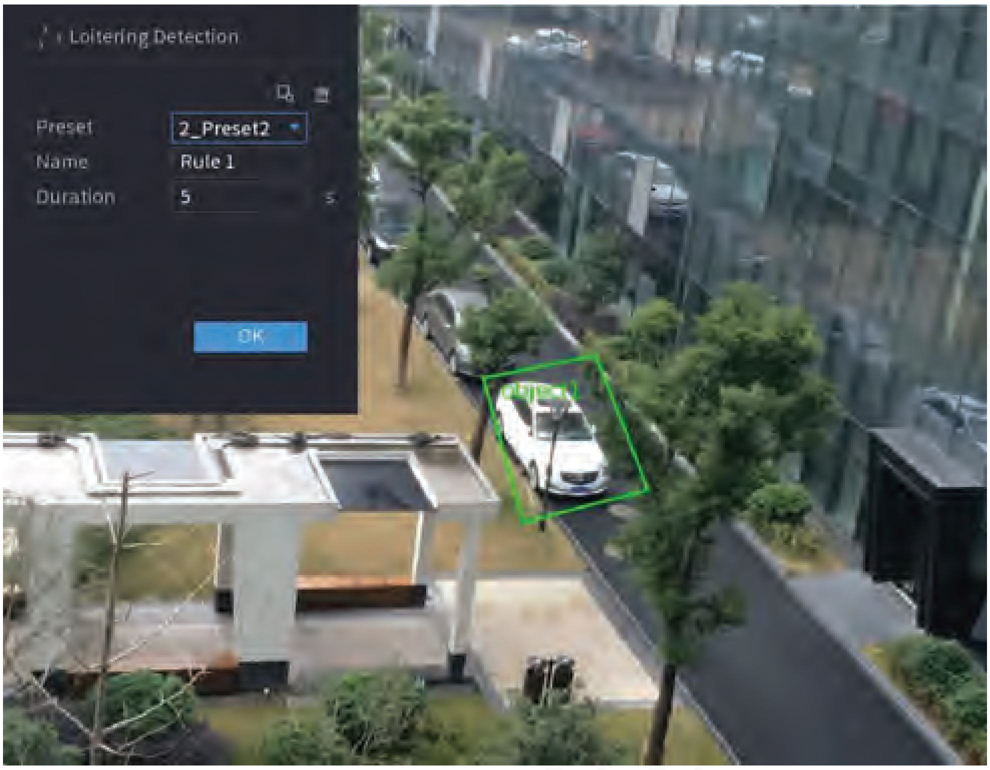
Step 3 Click **Add** to add a rule.

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



Loitering Detection

Preset: 2_Preset2

Name: Rule 1

Duration: 5 s

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.

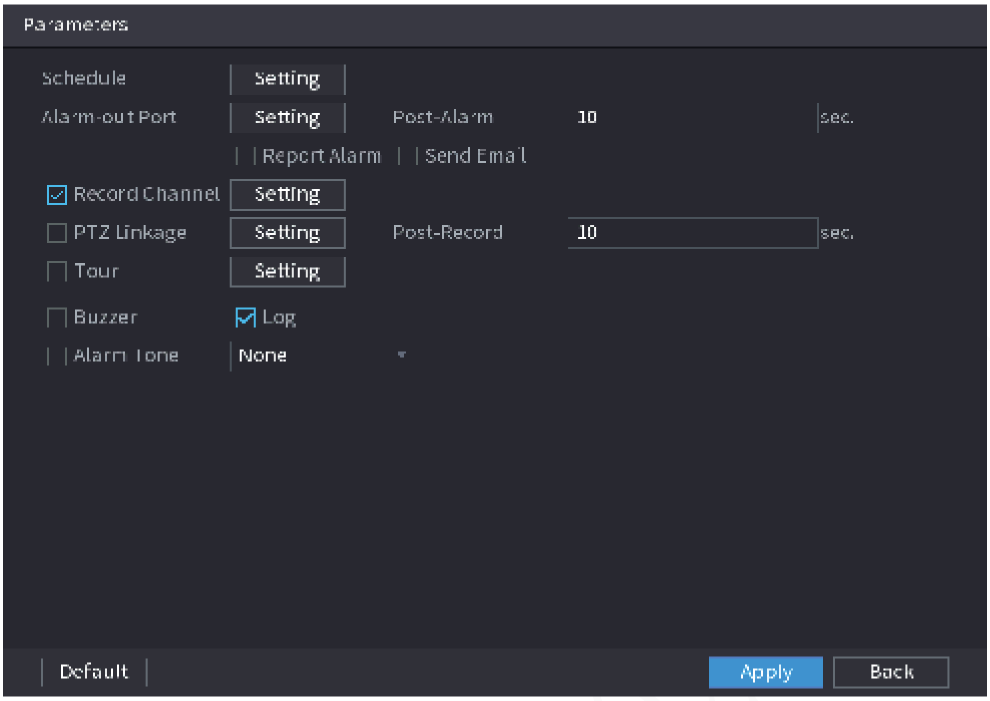
Table 5-34 Loitering detection parameters

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

☐ Report Alarm ☐ Send Email

☑ Record Channel Setting

☐ PTZ Linkage Setting Post-Record 10 sec.

☐ Tour Setting

☐ Buzzer ☑ Log

☐ Alarm Tone None

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**.

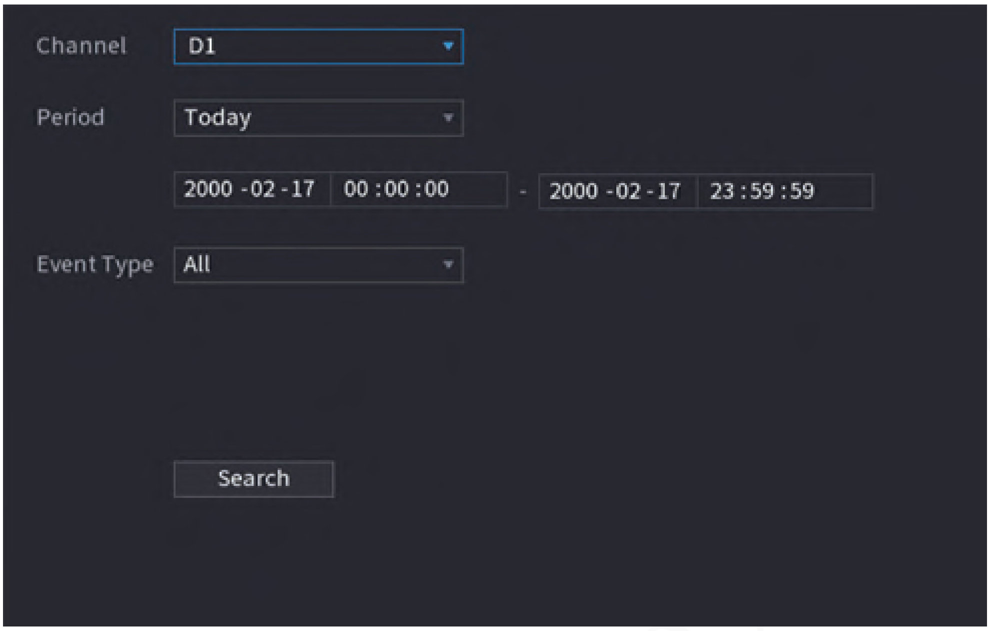
5.9.6.3 AI Search (IVS)

You can search for IVS detection results.

Procedure

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

Figure 5-129 IVS search



Channel: D1

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

Event Type: All

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.

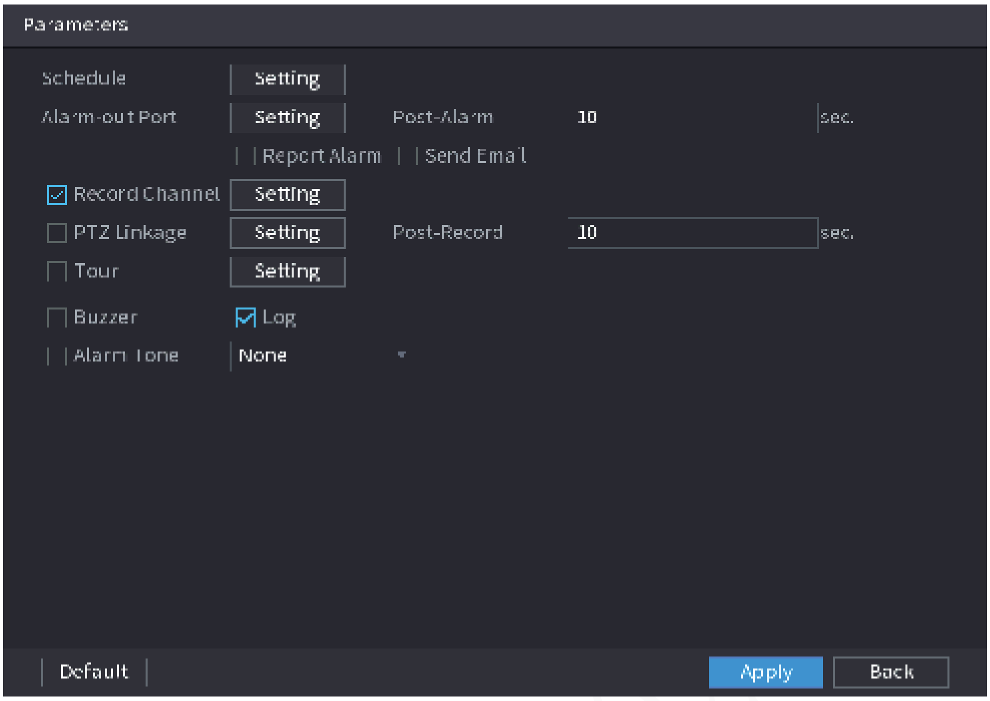
Table 5-35 Parameters of people approach detection

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

Default Apply Back

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.

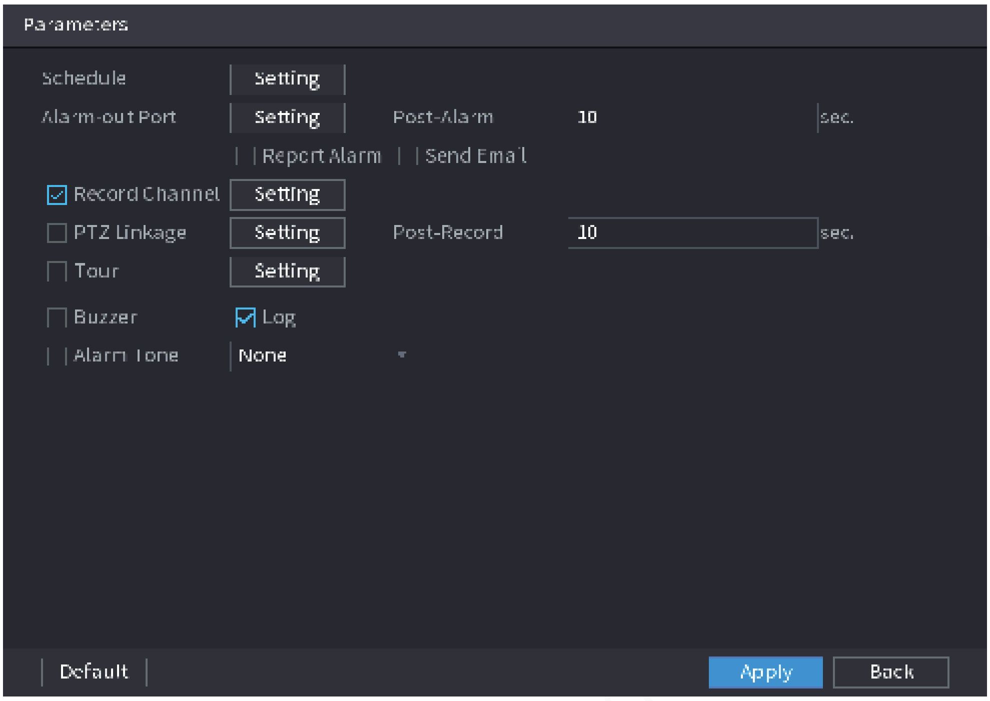
Table 5-36 Parameters of fall detection

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



Parameters

Schedule	Setting			
Alarm-out Port	Setting	Post-Alarm	10	sec.
	□ Report Alarm □ Send Email			
☑ Record Channel	Setting			
□ PTZ Linkage	Setting	Post-Record	10	sec.
□ Tour	Setting			
□ Buzzer	☑ Log			
□ Alarm Tone	None			

Default Apply Back

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.

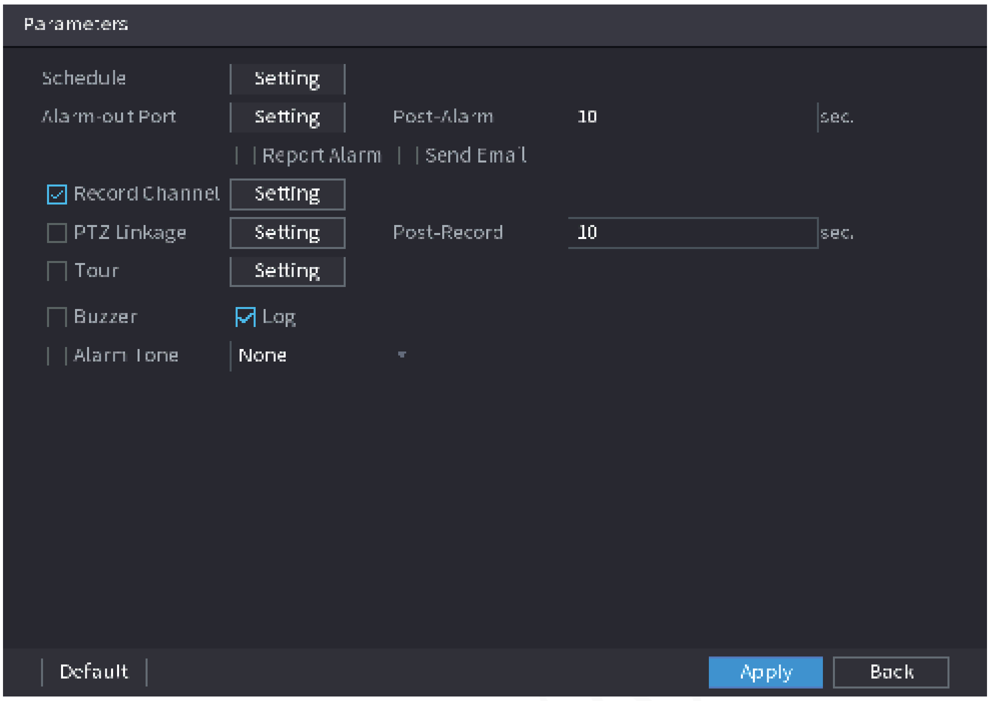
Table 5-37 Parameters of violence detection

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



Parameters

Schedule	Setting			
Alarm-out Port	Setting	Post-Alarm	10	sec.
	□ Report Alarm	□ Send Email		
☑ Record Channel	Setting			
□ PTZ Linkage	Setting	Post-Record	10	sec.
□ Tour	Setting			
□ Buzzer	☑ Log			
□ Alarm Tone	None			

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

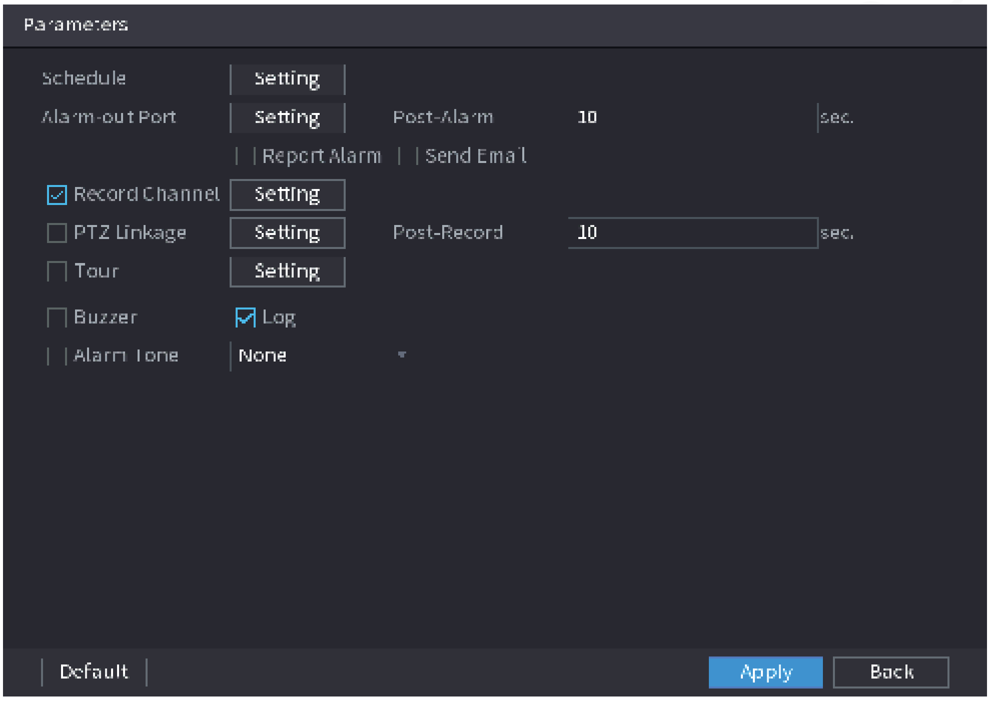
Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.

Parameter	Description
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



Parameters

Schedule	Setting			
Alarm-out Port	Setting	Post-Alarm	10	sec.
	□ Report Alarm □ Send Email			
☑ Record Channel	Setting			
□ PTZ Linkage	Setting	Post-Record	10	sec.
□ Tour	Setting			
□ Buzzer	☑ Log			
□ Alarm Tone	None			

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.

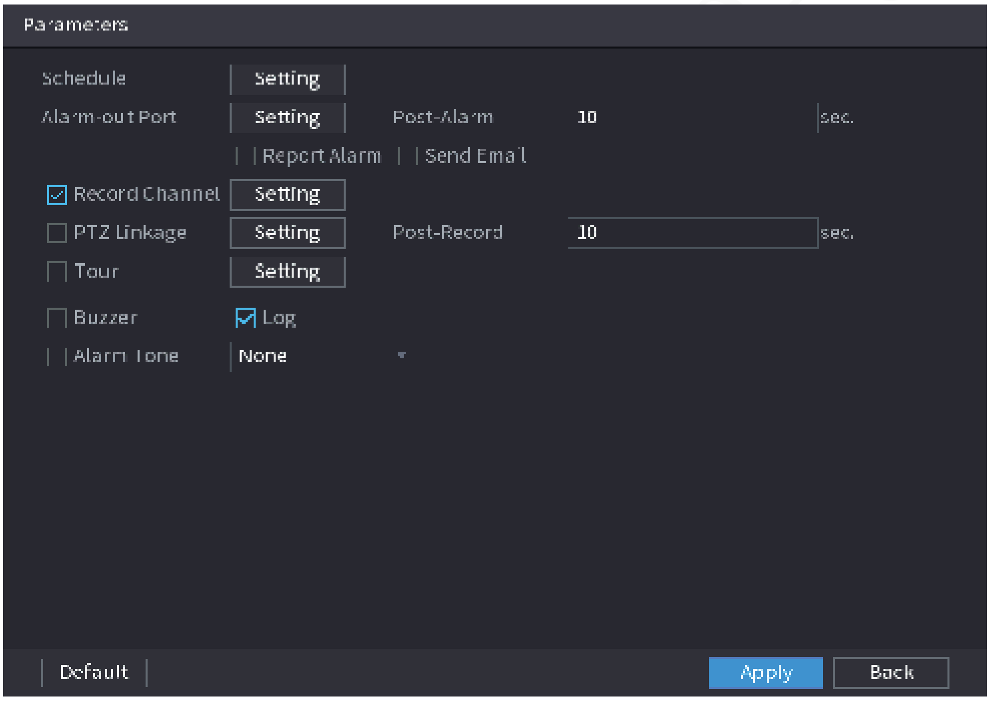
Table 5-39 Parameters of people stay detection

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



Parameters

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Report Alarm □ Send Email

☑ Record Channel Setting

□ PTZ Linkage Setting Post-Record 10 sec.

□ Tour Setting

□ Buzzer ☑ Log

□ Alarm Tone None

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**.

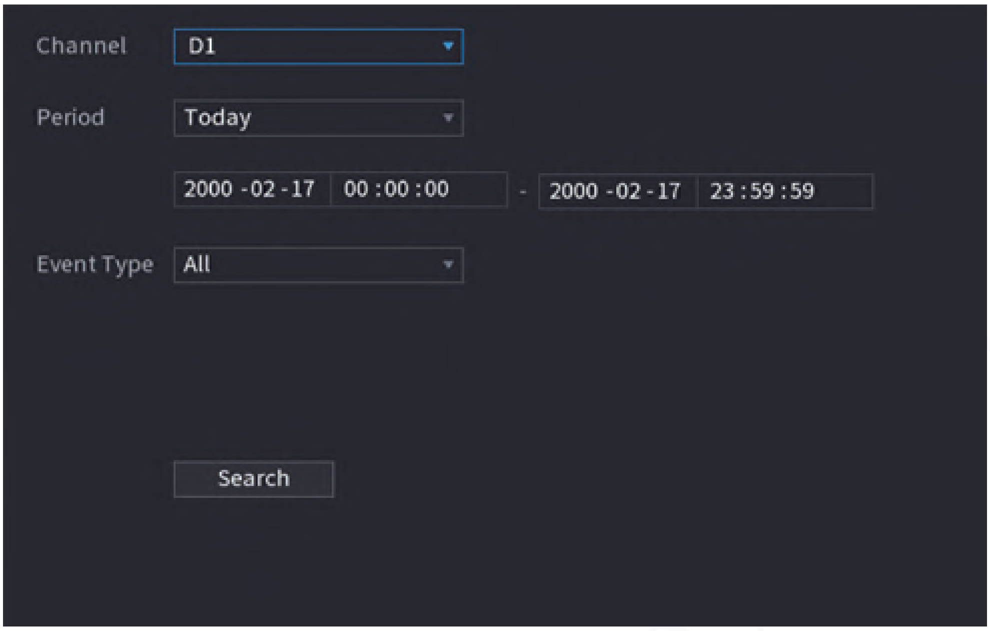
5.9.7.3 AI Search (Stereo Analysis)

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



Channel: D1

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

Event Type: All

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

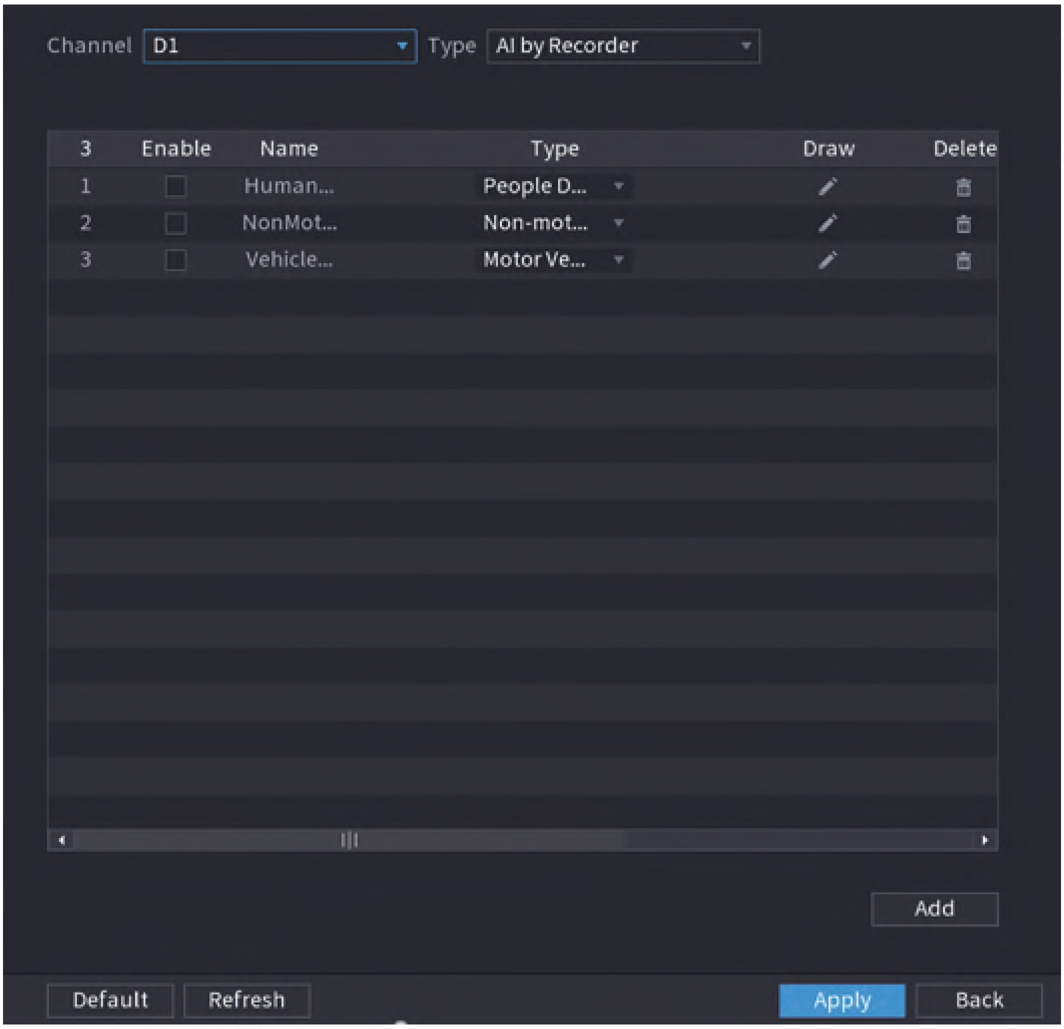
To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

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



Channel: D1

Type: AI by Recorder

3	Enable	Name	Type	Draw	Delete
1	□	Human...	People D...	✎	🗑
2	□	NonMot...	Non-mot...	✎	🗑
3	□	Vehicle...	Motor Ve...	✎	🗑

Step 2 Select a channel and AI type.

AI by Recorder is available on select models.

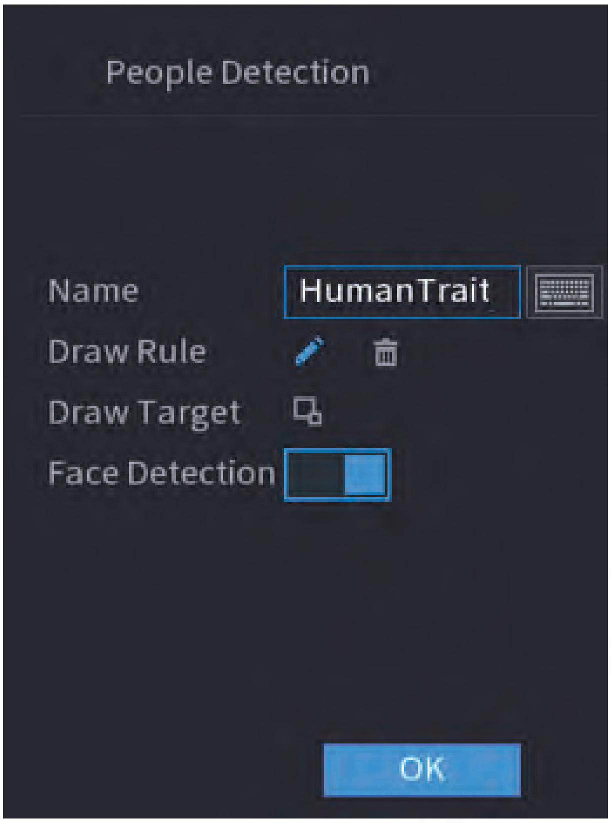
Step 3 Click **Add** to add a rule.

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



People Detection

Name: HumanTrait

Draw Rule

Draw Target

Face 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)

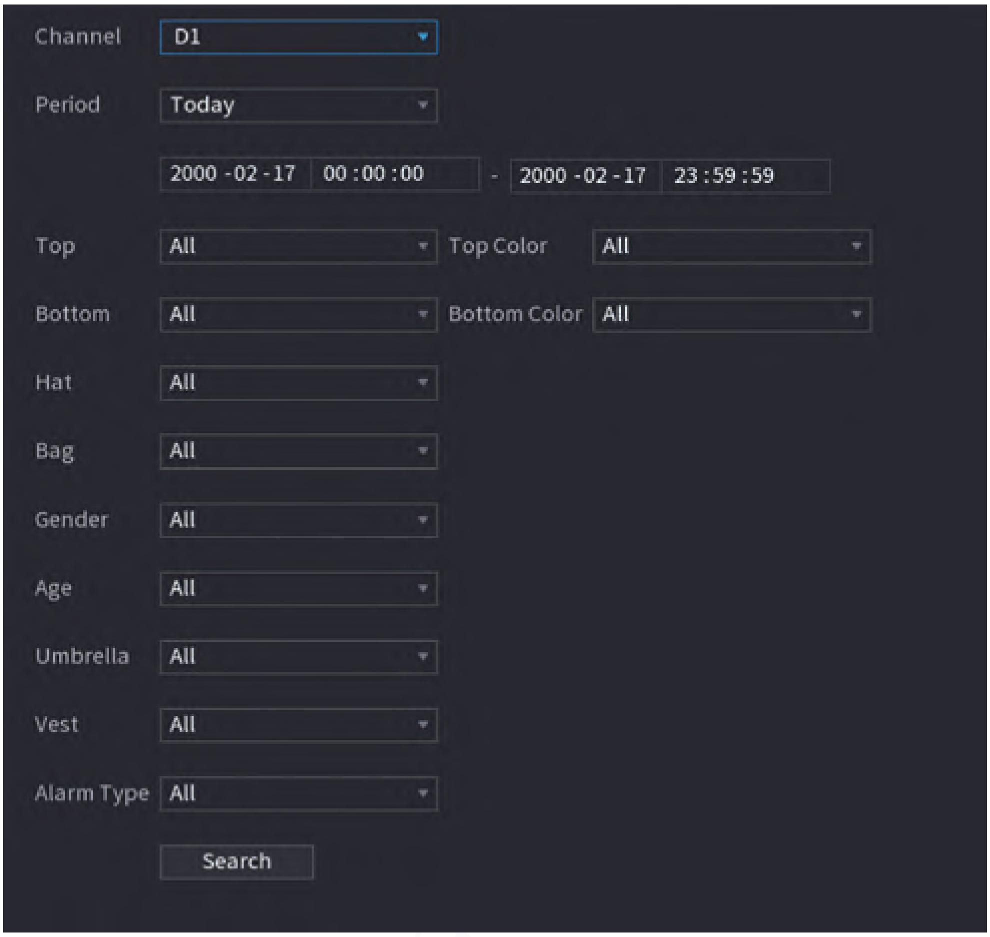
You can search for the video metadata detection results and play back related videos.

5.9.8.3.1 Human Detection

Procedure

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

Figure 5-138 Human detection



Channel: D1

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

Top: All

Top Color: All

Bottom: All

Bottom Color: All

Hat: All

Bag: All

Gender: All

Age: All

Umbrella: All

Vest: All

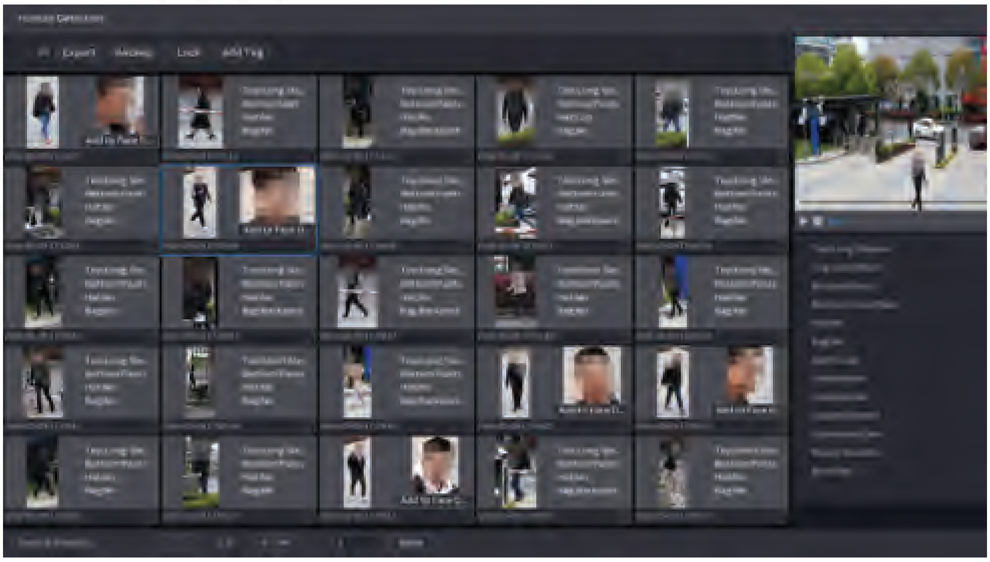
Alarm Type: All

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.

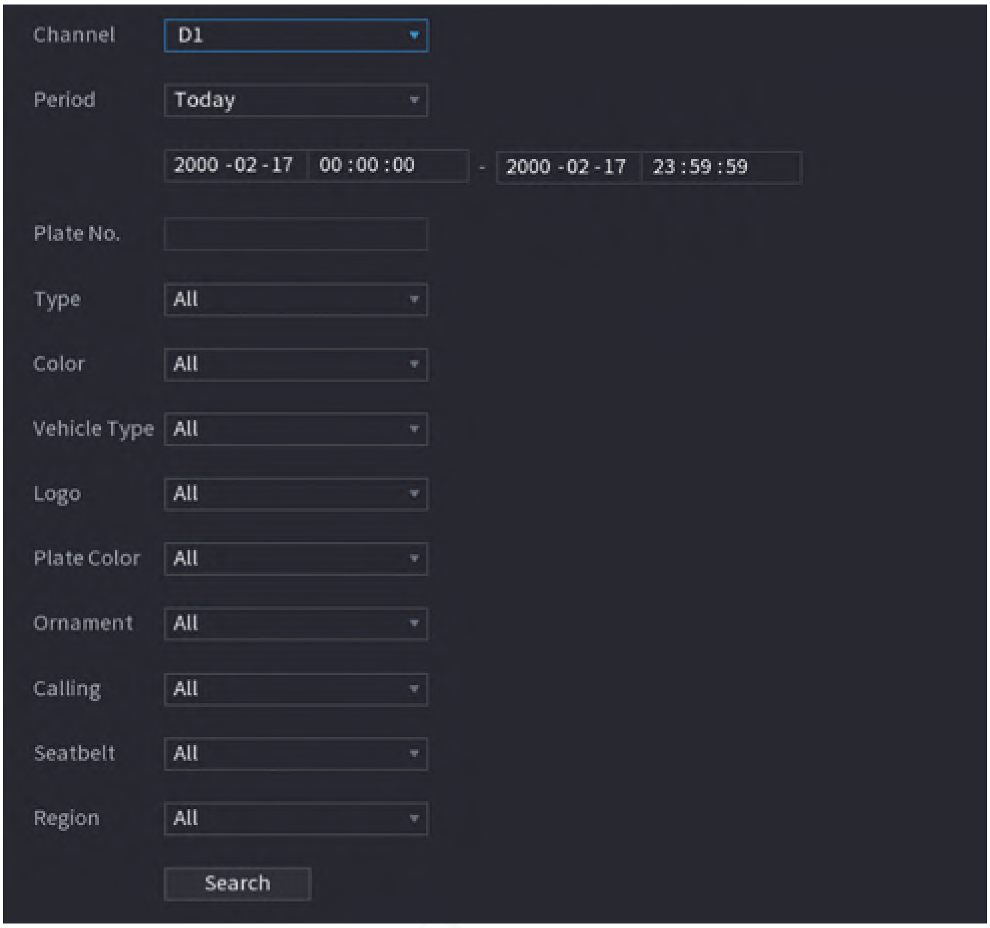
📖

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



Channel	D1
Period	Today
	2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59
Plate No.	
Type	All
Color	All
Vehicle Type	All
Logo	All
Plate Color	All
Ornament	All
Calling	All
Seatbelt	All
Region	All

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

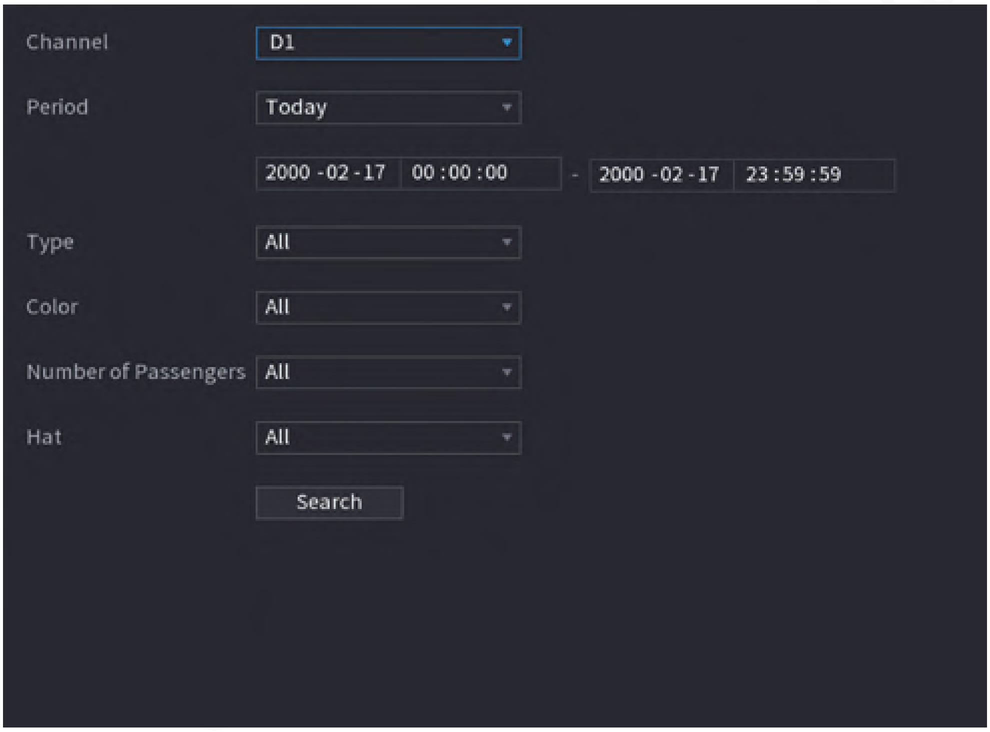
You can search for non-motor vehicle detection results according to the non-motor vehicle parameters.

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



Channel: D1

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

Type: All

Color: All

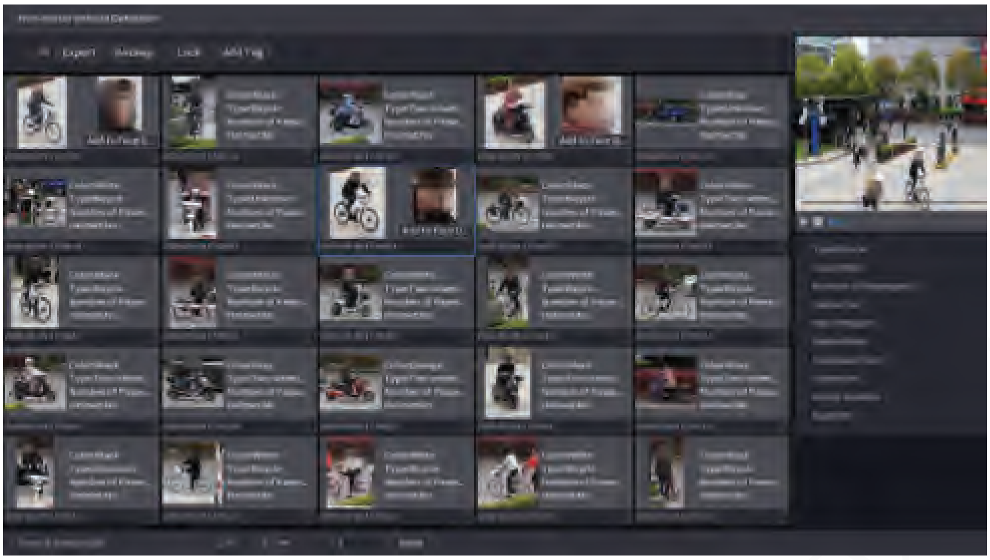
Number of Passengers: All

Hat: All

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

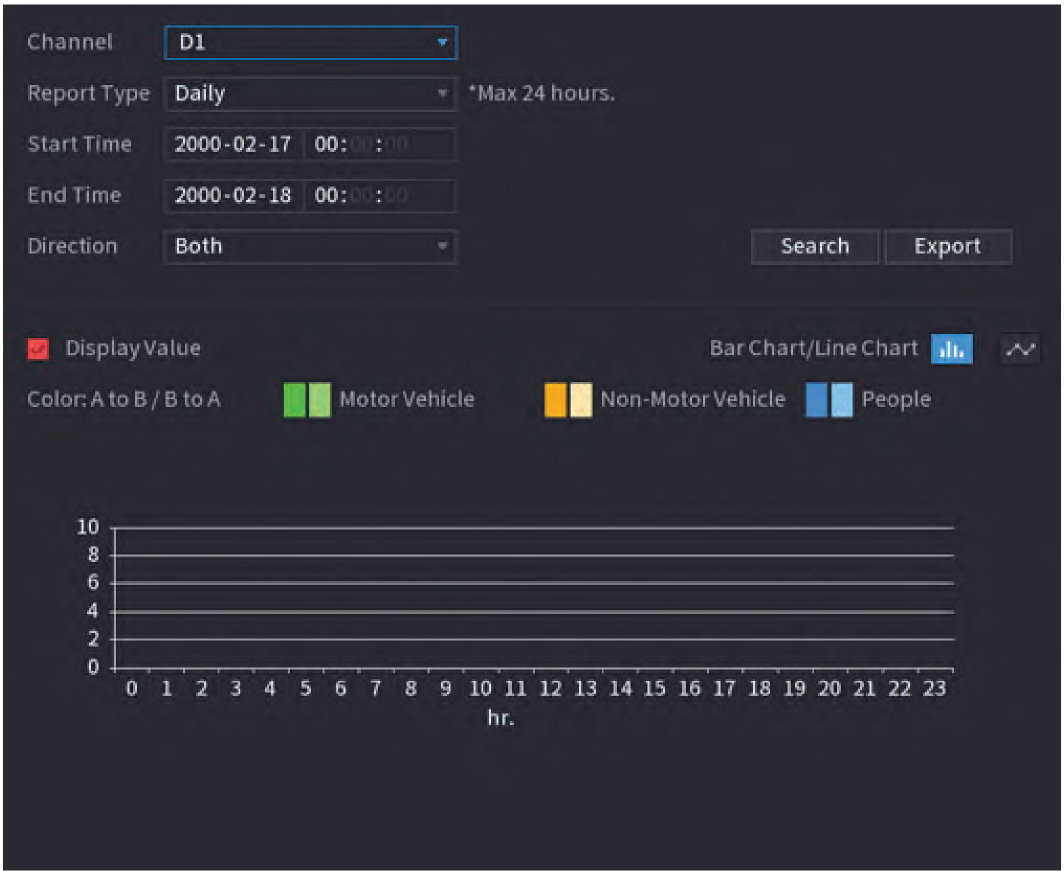
You can search for and export video metadata statistics.

- 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



Channel: D1
Report Type: Daily *Max 24 hours.
Start Time: 2000-02-17 00:00:00
End Time: 2000-02-18 00:00:00
Direction: Both

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

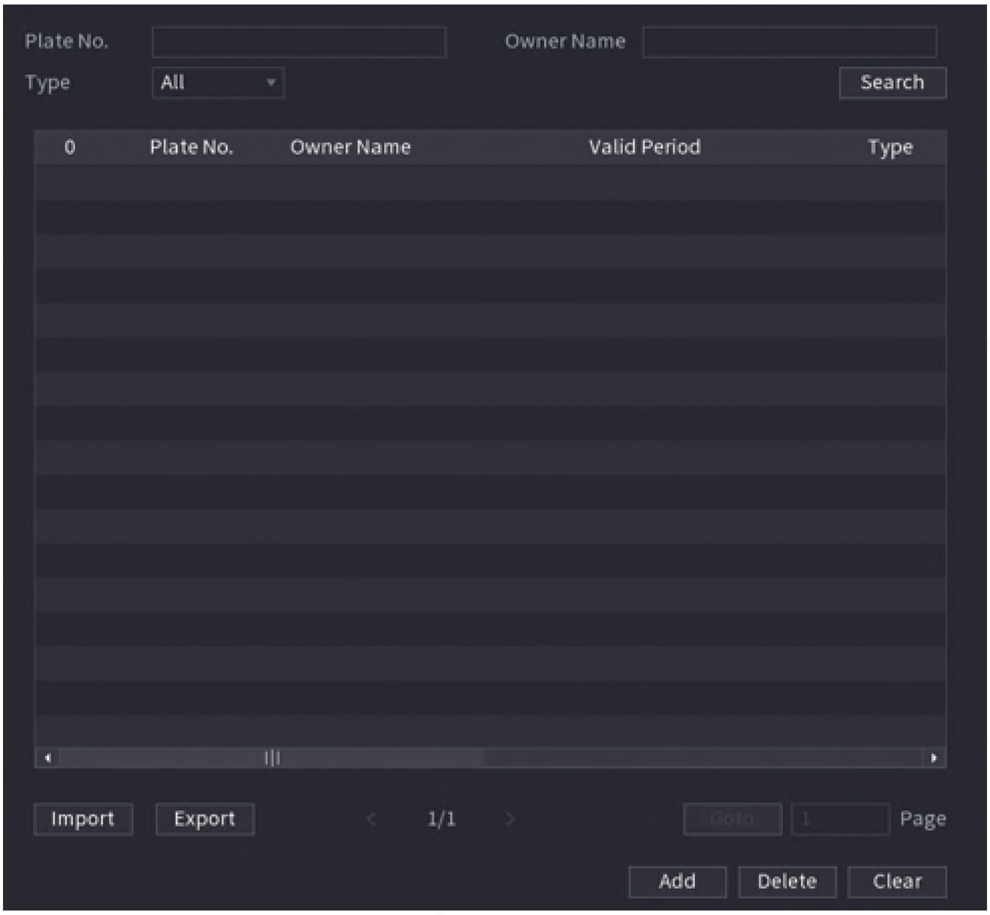
To facilitate vehicle management, you can add the plate numbers to the blocklist or allowlist. The system can compare the detected plate information with the plate on the blocklist and allowlist and then trigger the corresponding alarm linkage.

- 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**.

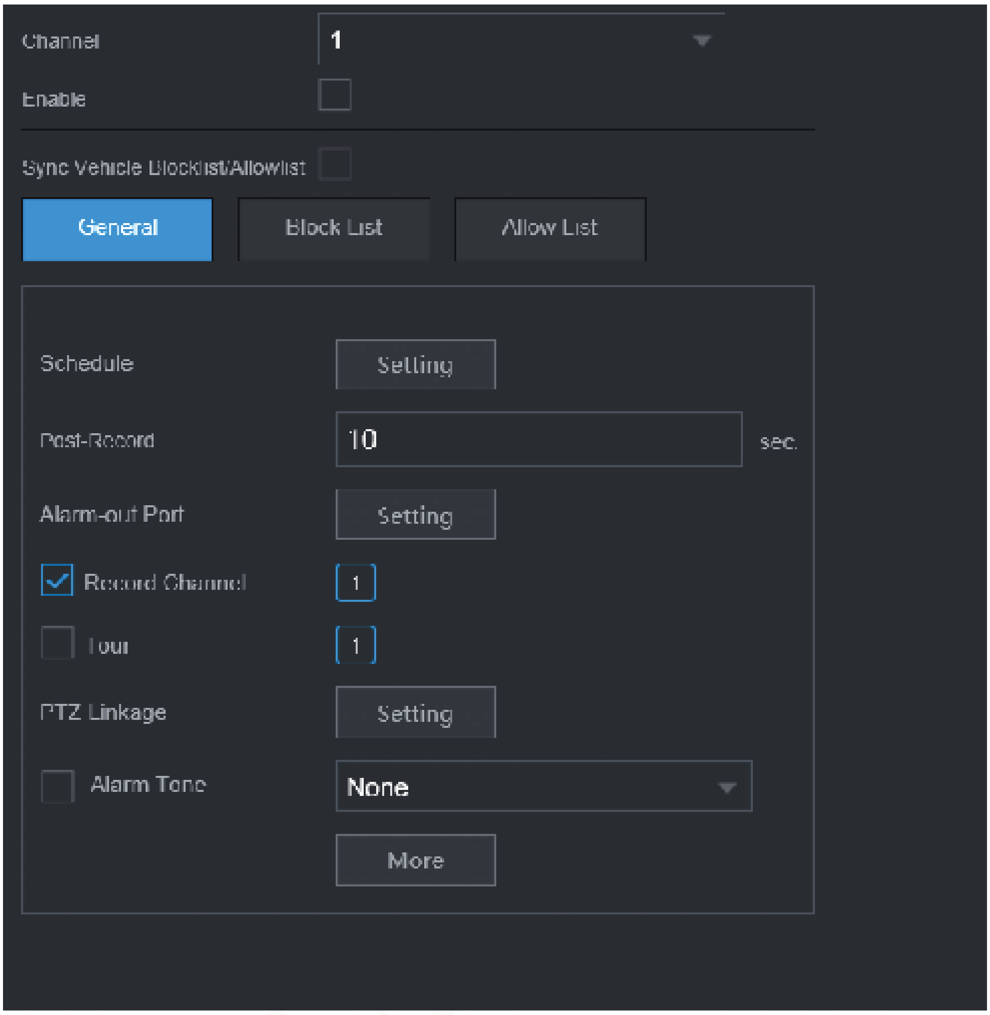
5.9.9.2 Configuring ANPR

Configure the ANPR alarm rules.

Procedure

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

Figure 5-145 ANPR



Channel: 1

Enable □

Sync Vehicle Blocklist/Allowlist □

Schedule: Setting

Post-Record: 10 sec.

Alarm-out Port: Setting

☑ Record Channel: 1

□ Tour: 1

PTZ Linkage: Setting

□ Alarm Tone: None

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.

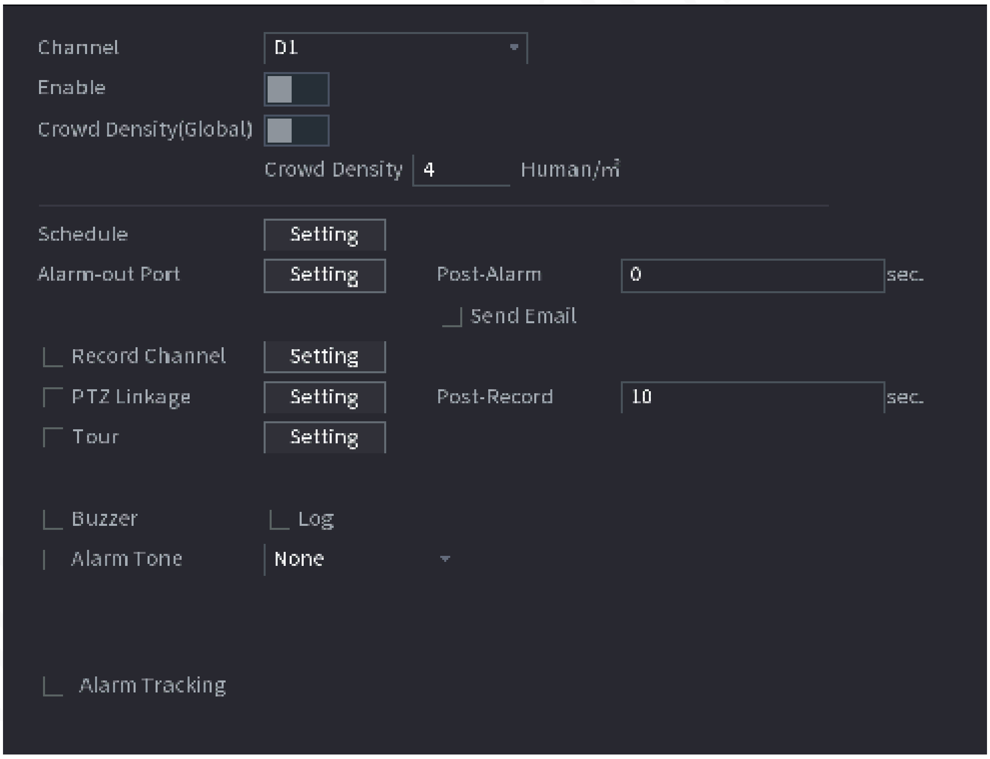
Prerequisites

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



Channel: D1
Enable
Crowd Density(Global)
Crowd Density: 4 Human/㎡
Schedule: Setting
Alarm-out Port: Setting
Post-Alarm: 0 sec.
□ Send Email
□ Record Channel: Setting
□ PTZ Linkage: Setting
Post-Record: 10 sec.
□ Tour: Setting
□ Buzzer
□ Log
Alarm Tone: None
□ Alarm Tracking

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

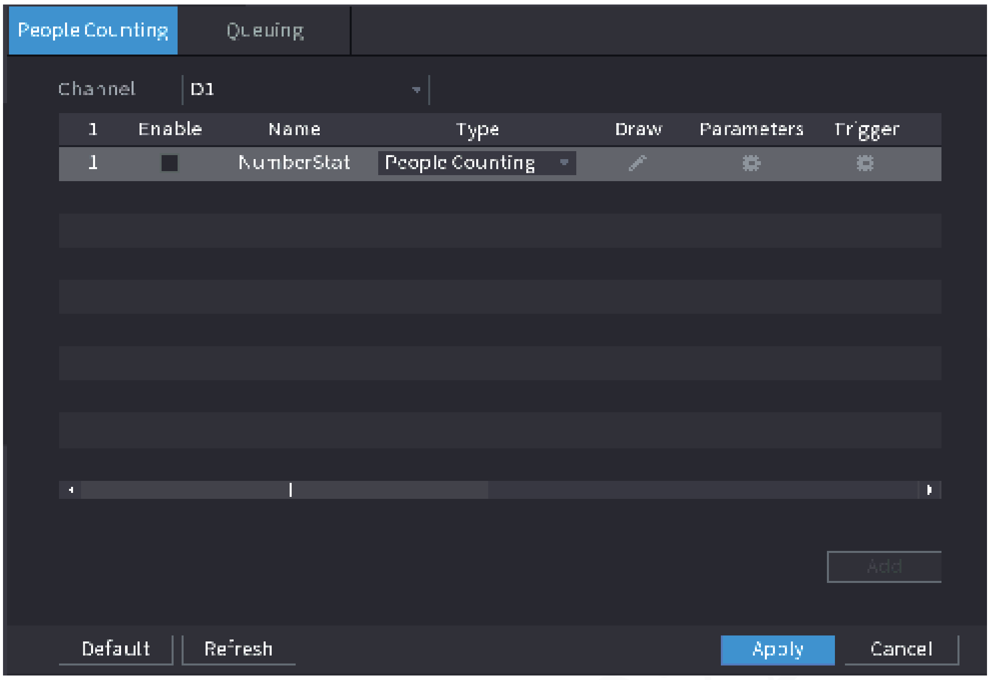
To use AI by camera, you need to enable the smart plan first. For details, see "5.9.2 Smart Plan".

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



Channel: D1

1	Enable	Name	Type	Draw	Parameters	Trigger
1	■	NumberStat	People Counting	✎	⚙	⚙

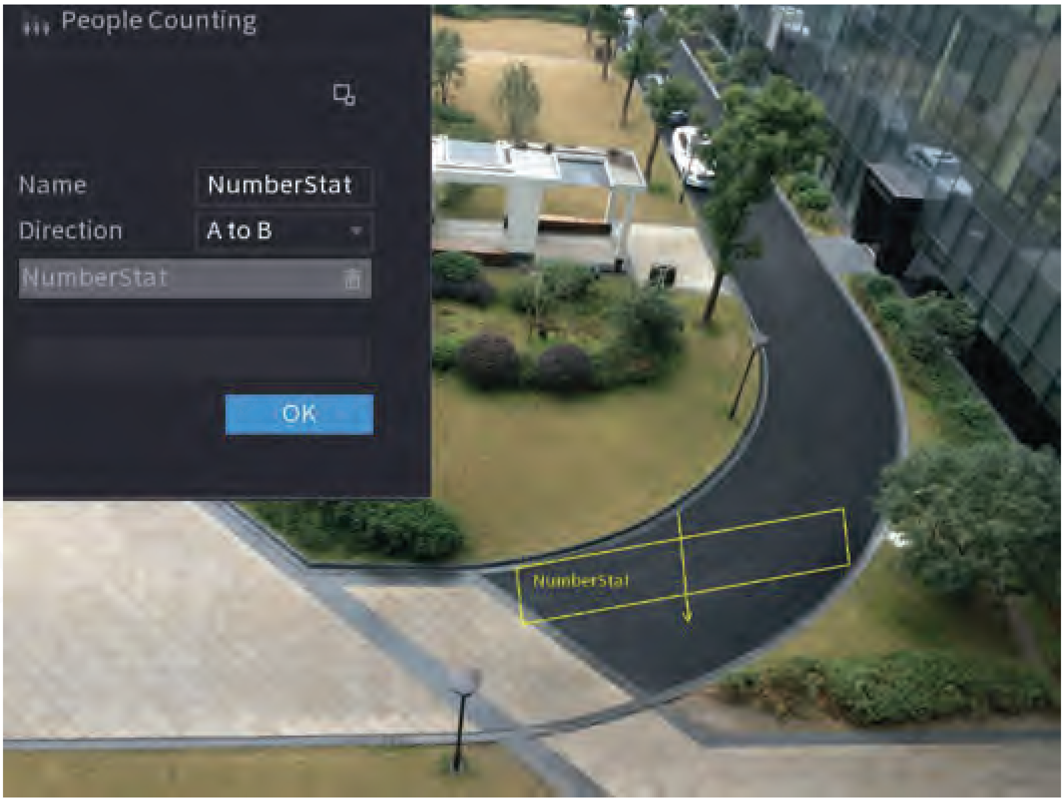
<u>Step 2</u> Select a channel and then click **Add**.

<u>Step 3</u> Select the **Enable** checkbox and then set **Type** to **People Counting**.

<u>Step 4</u> Draw people counting rule.

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

Figure 5-148 People counting rule



Name: NumberStat

Direction: A to B

NumberStat

2) Customize the rule name and then select direction.

3) Click **OK**.

<u>Step 5</u> 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.

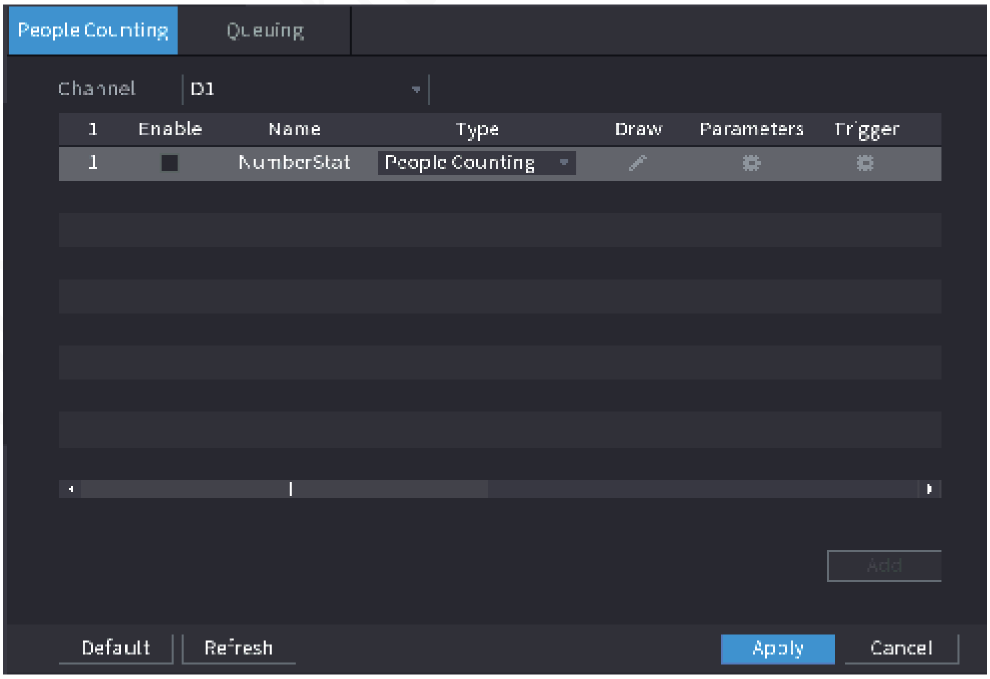
Step 7 Click **Apply**.

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



Channel: D1

1	Enable	Name	Type	Draw	Parameters	Trigger
1	■	NumberStat	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

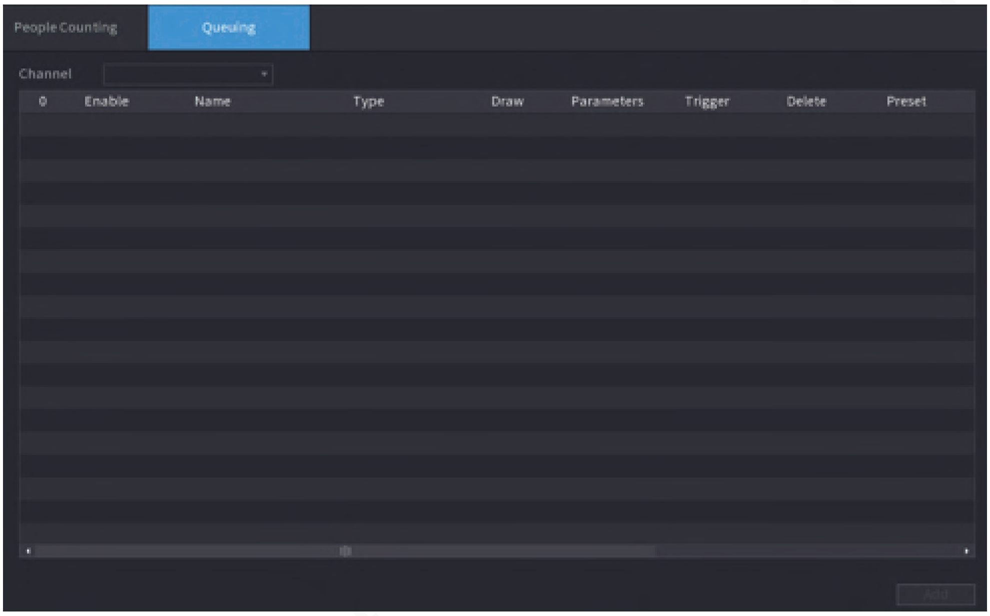
Step 7 Click **Apply**.

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

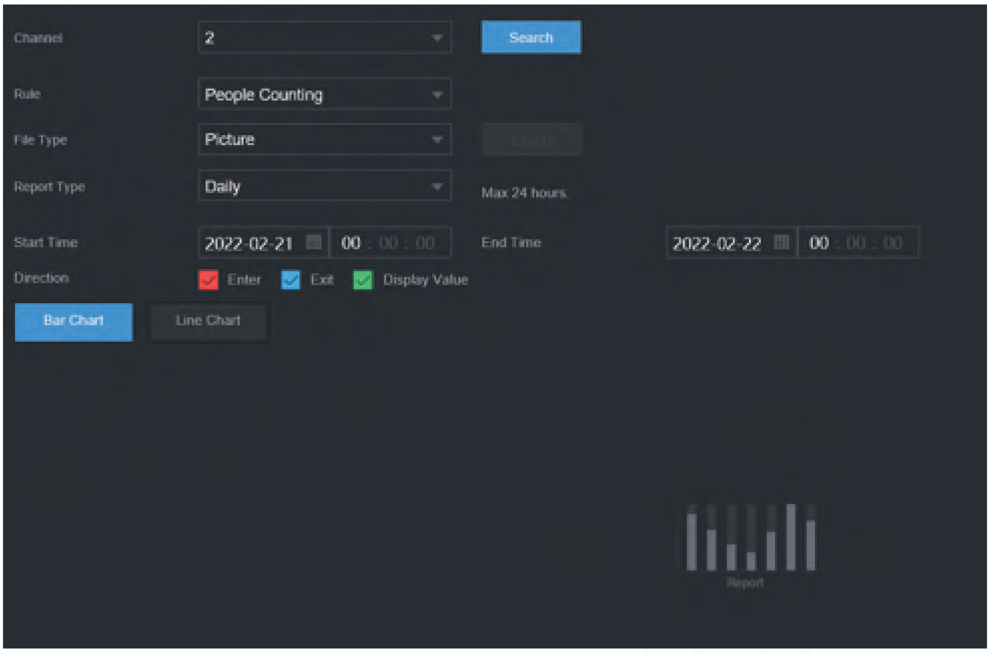
You can search for and export the people counting statistics.

- 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



Channel: 2

Search

Rule: People Counting

File Type: Picture

Export

Report Type: Daily

Max 24 hours.

Start Time: 2022-02-21 00 : 00 : 00

End Time: 2022-02-22 00 : 00 : 00

Direction: ☑ Enter ☑ Exit ☑ Display Value

Bar Chart

Line Chart

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

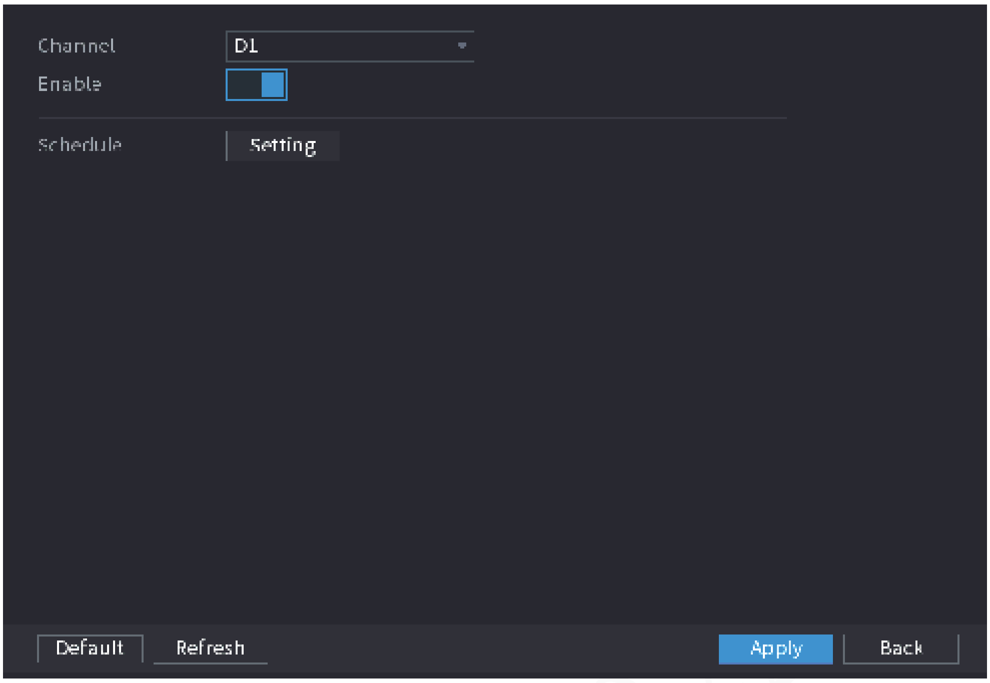
Background Information

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**.

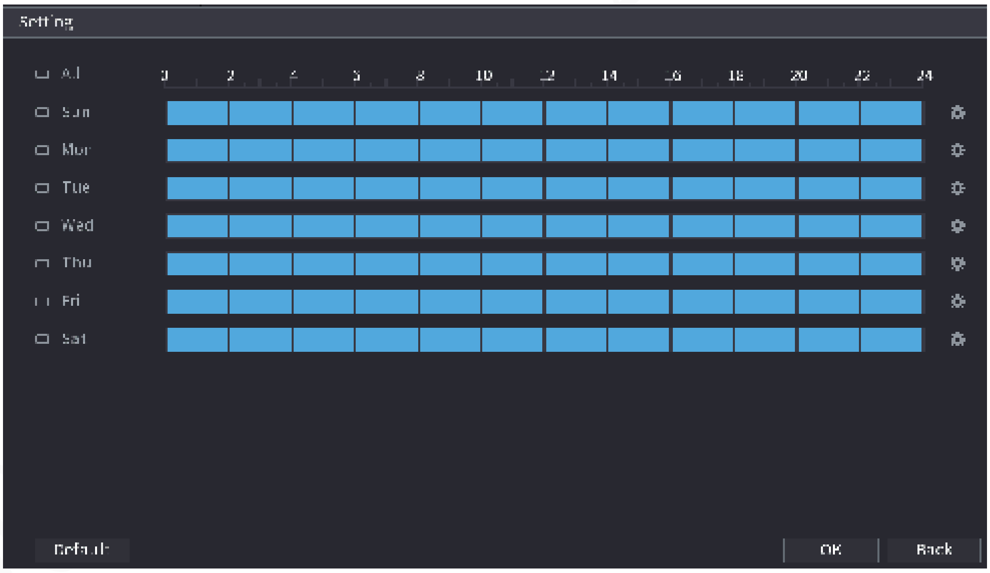
Figure 5-152 Heat map


Channel: D1

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**.

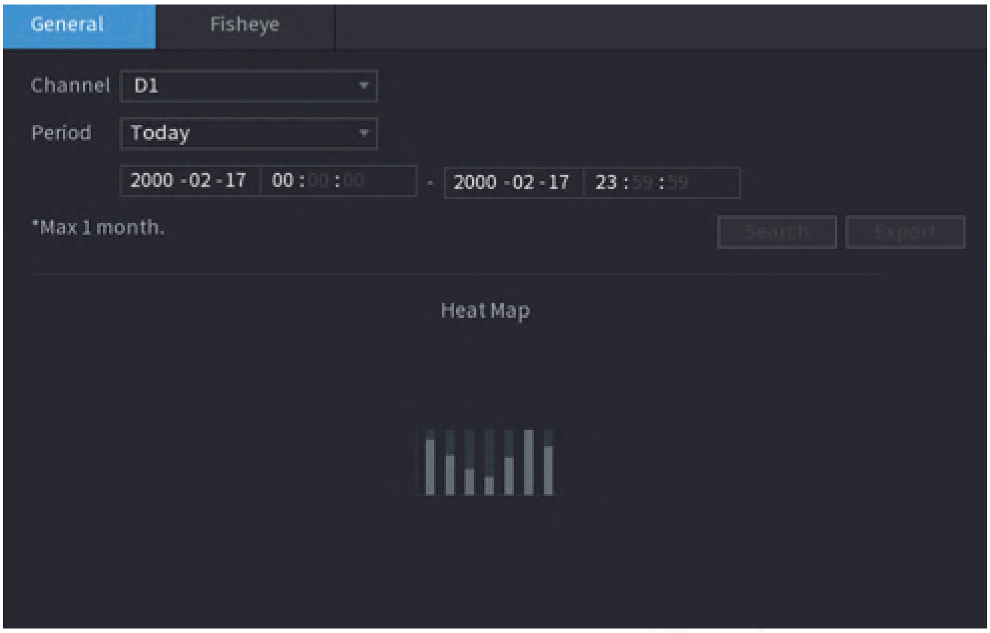
5.9.12.3 Report Query

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



Channel D1

Period Today

2000 -02 -17 00 : 00 : 00 - 2000 -02 -17 23 : 59 : 59

*Max 1 month.

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

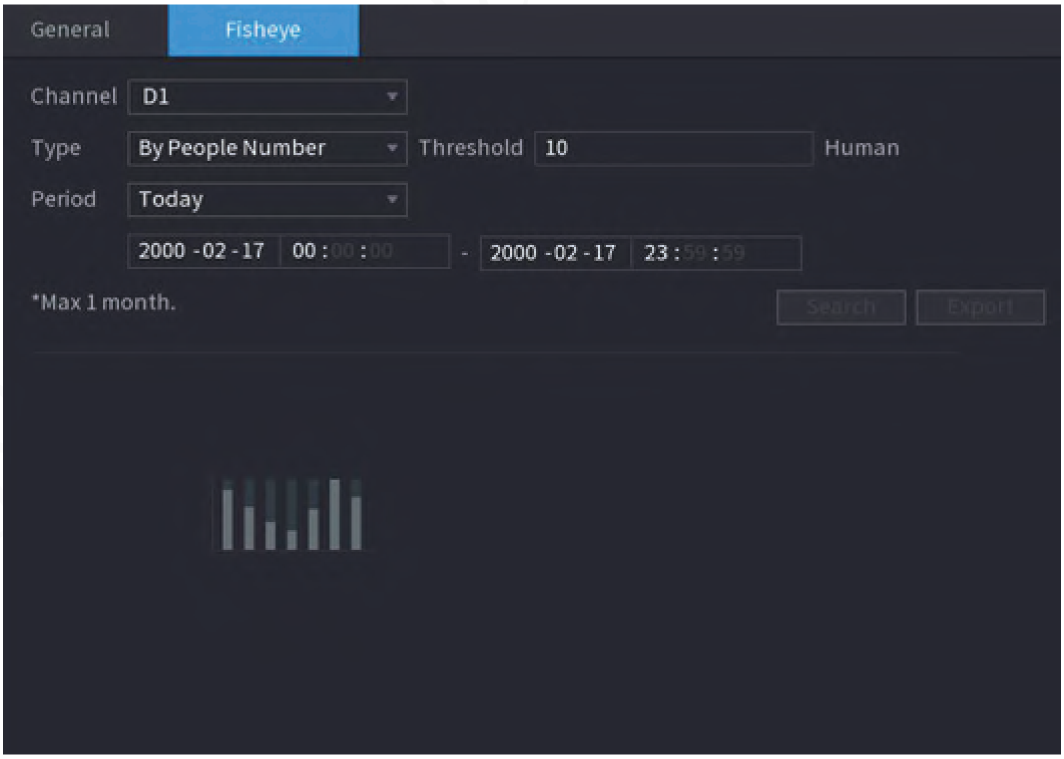
Step 3 Click **Search**.

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



Channel D1

Type By People Number Threshold 10 Human

Period Today

2000 -02 -17 00 : 00 : 00 - 2000 -02 -17 23 : 59 : 59

*Max 1 month.

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.

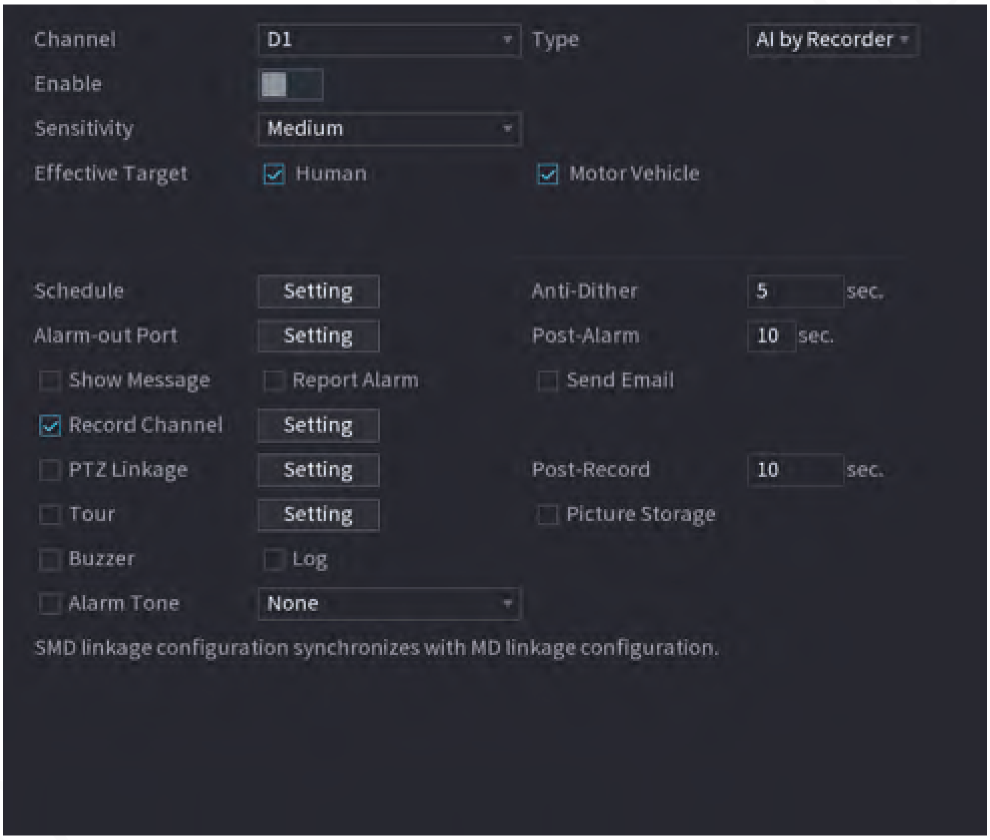
5.9.13.1 Enabling Smart Plan

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



Channel: D1 | Type: AI by Recorder

Enable

Sensitivity: Medium

Effective Target: ☑ Human ☑ Motor Vehicle

Schedule: Setting | Anti-Dither: 5 sec.

Alarm-out Port: Setting | Post-Alarm: 10 sec.

□ Show Message □ Report Alarm □ Send Email

☑ Record Channel: Setting

□ PTZ Linkage: Setting | Post-Record: 10 sec.

□ Tour: Setting | □ Picture Storage

□ Buzzer □ Log

□ Alarm Tone: None

SMD linkage configuration synchronizes with MD linkage configuration.

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.

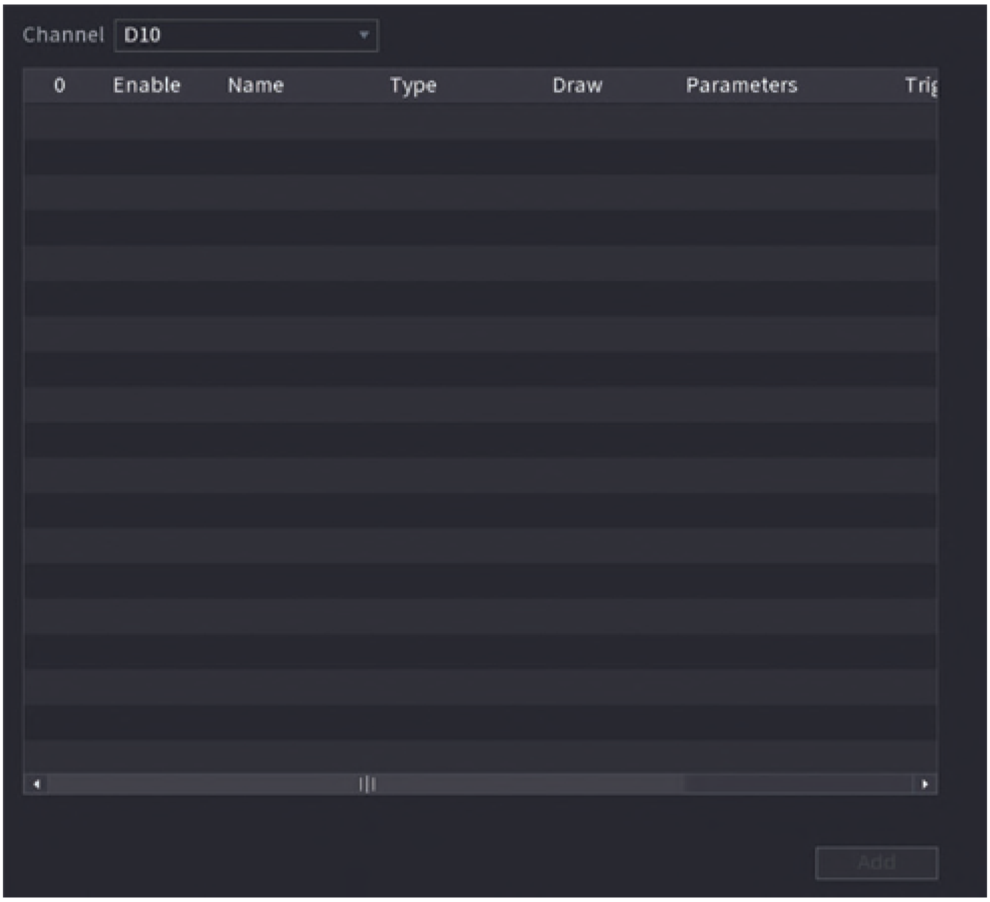
5.9.14.1 Enabling Smart Plan

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



Channel D10

0	Enable	Name	Type	Draw	Parameters	Trig

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

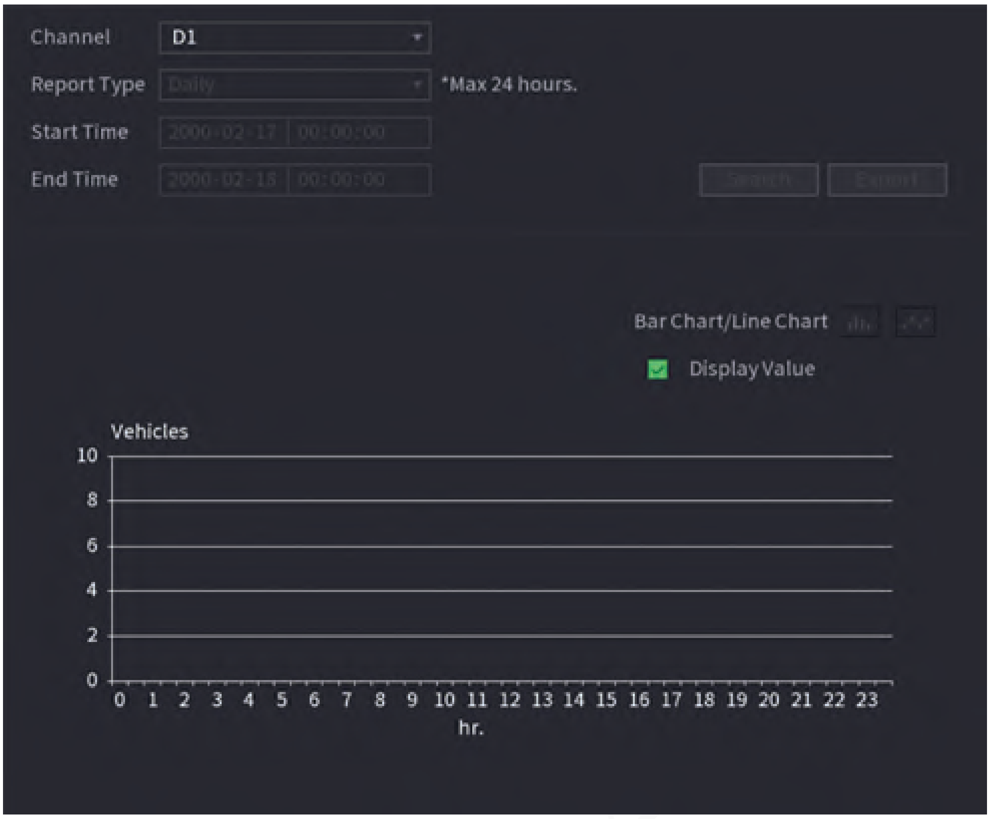
You can search for and export statistics on vehicle density.

- 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



Channel: D1

Report Type: Daily *Max 24 hours.

Start Time: 2000-02-17 | 00:00:00

End Time: 2000-02-18 | 00:00:00

Search Export

Bar Chart/Line Chart

☑ Display Value

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.

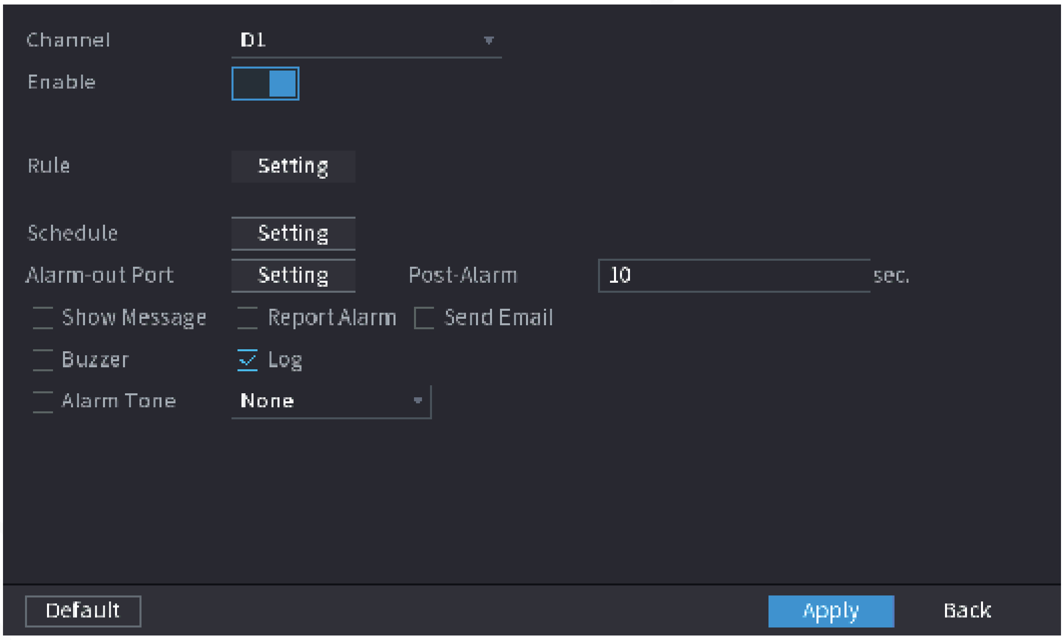
- This function takes effect only when the remote IPC supports video quality analytics.
- This function is available on select models.

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



Channel D1

Enable ●

Rule Setting

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Show Message □ Report Alarm □ Send Email

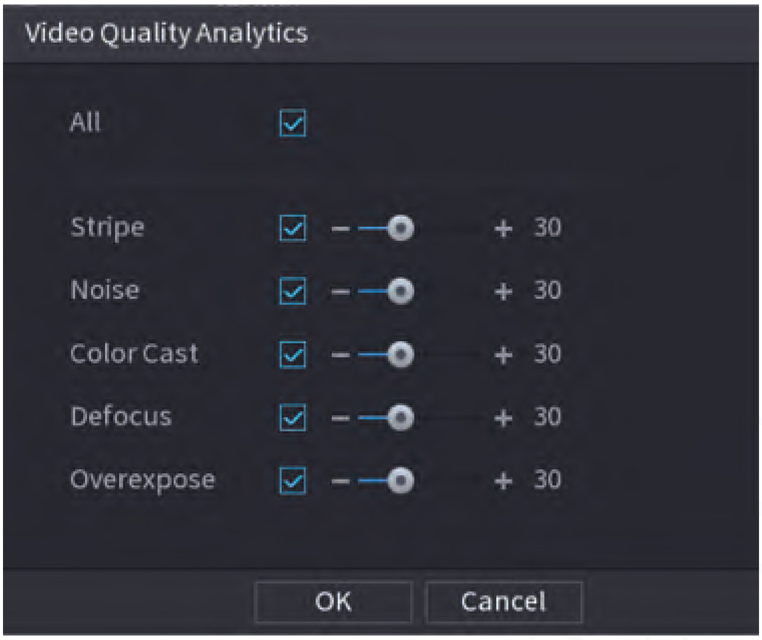
□ Buzzer ☑ Log

□ Alarm Tone None

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

Step 4 Select items and set thresholds as needed.

Figure 5-160 Video quality analytics settings



Video Quality Analytics

All ☑

Stripe ☑ − + 30

Noise ☑ − + 30

Color Cast ☑ − + 30

Defocus ☑ − + 30

Overexpose ☑ − + 30

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.

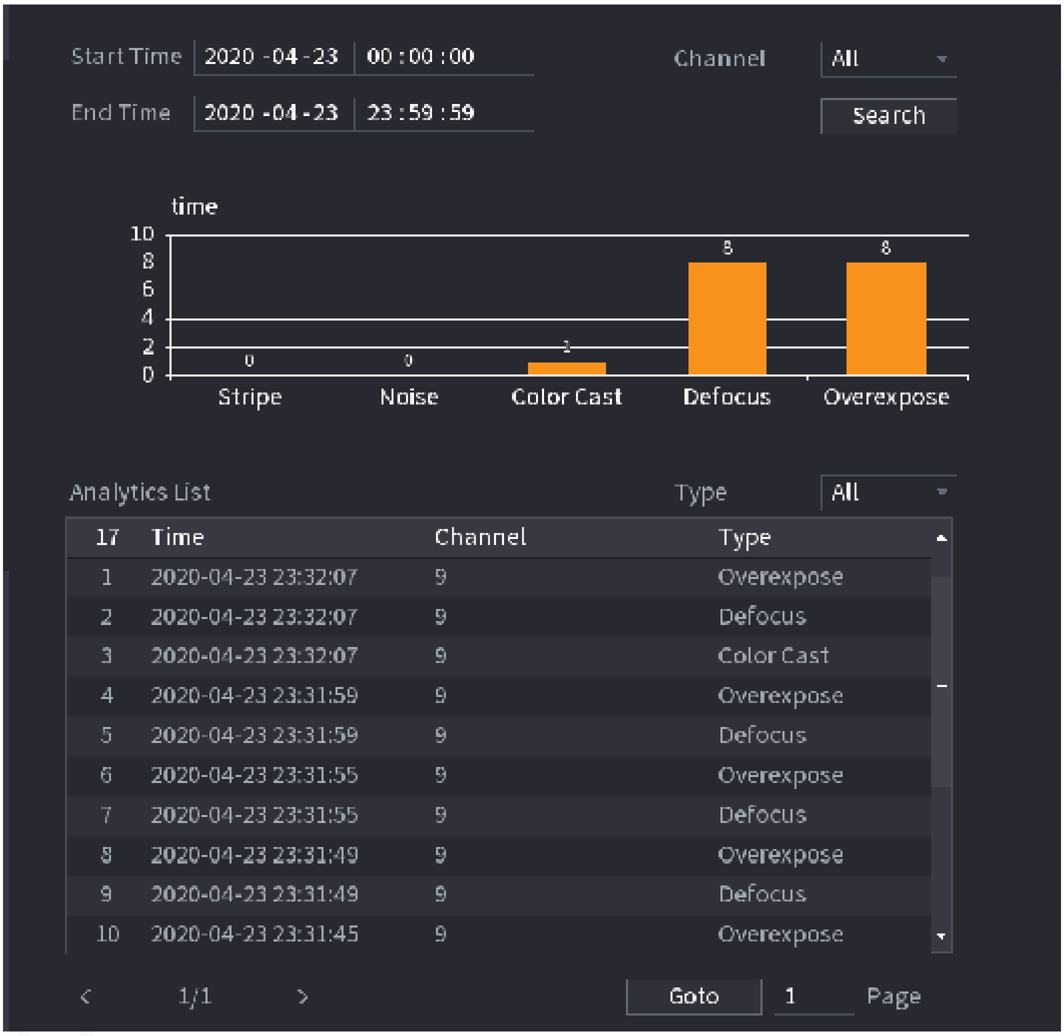
Step 1 Select **Main Menu** > **AI** > **AI Search** > **Analytics List**.

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



Start Time 2020 -04 -23 00 :00 :00

End Time 2020 -04 -23 23 :59 :59

Channel All

Analytics List

Type All

17	Time	Channel	Type
1	2020-04-23 23:32:07	9	Overexpose
2	2020-04-23 23:32:07	9	Defocus
3	2020-04-23 23:32:07	9	Color Cast
4	2020-04-23 23:31:59	9	Overexpose
5	2020-04-23 23:31:59	9	Defocus
6	2020-04-23 23:31:55	9	Overexpose
7	2020-04-23 23:31:55	9	Defocus
8	2020-04-23 23:31:49	9	Overexpose
9	2020-04-23 23:31:49	9	Defocus
10	2020-04-23 23:31:45	9	Overexpose

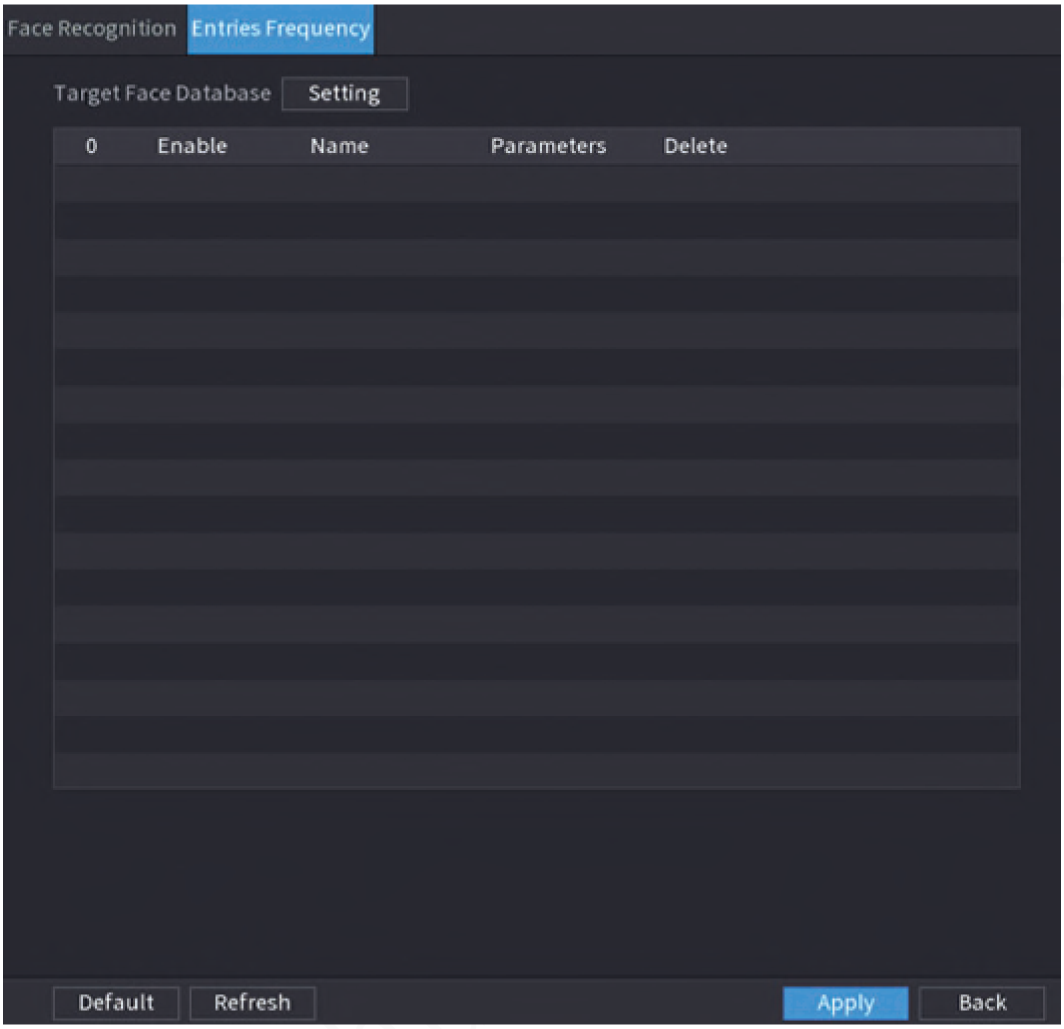
5.9.17 Entries Frequency

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**.

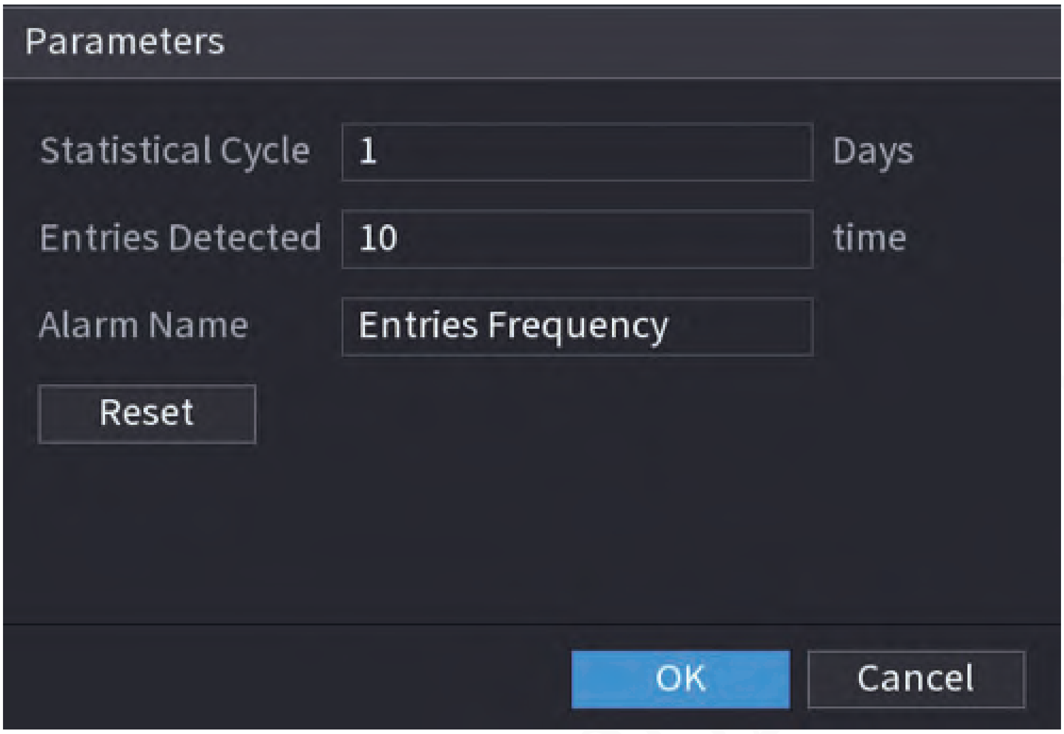
Figure 5-162 Entries frequency



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



Statistical Cycle: 1 Days

Entries Detected: 10 time

Alarm Name: 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

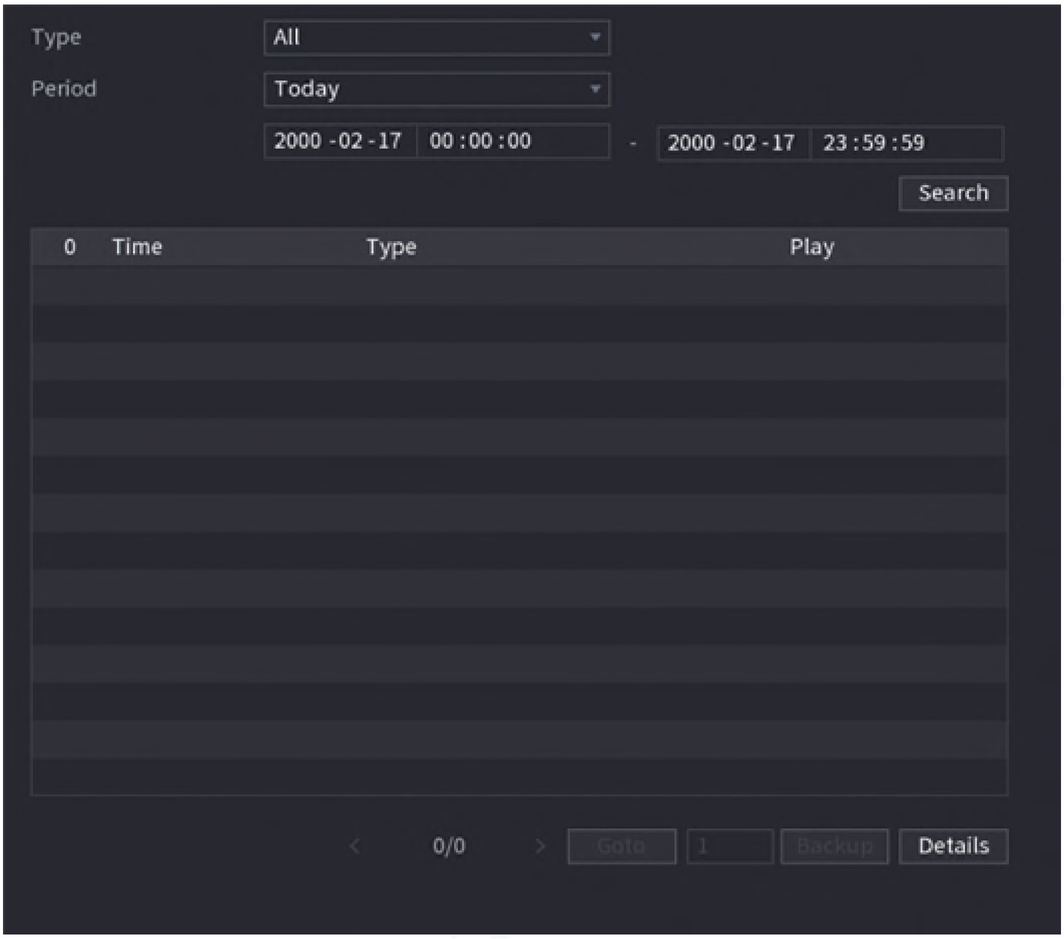
5.10.1 Alarm Information

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



Type: All

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

Search

0	Time	Type	Play

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.

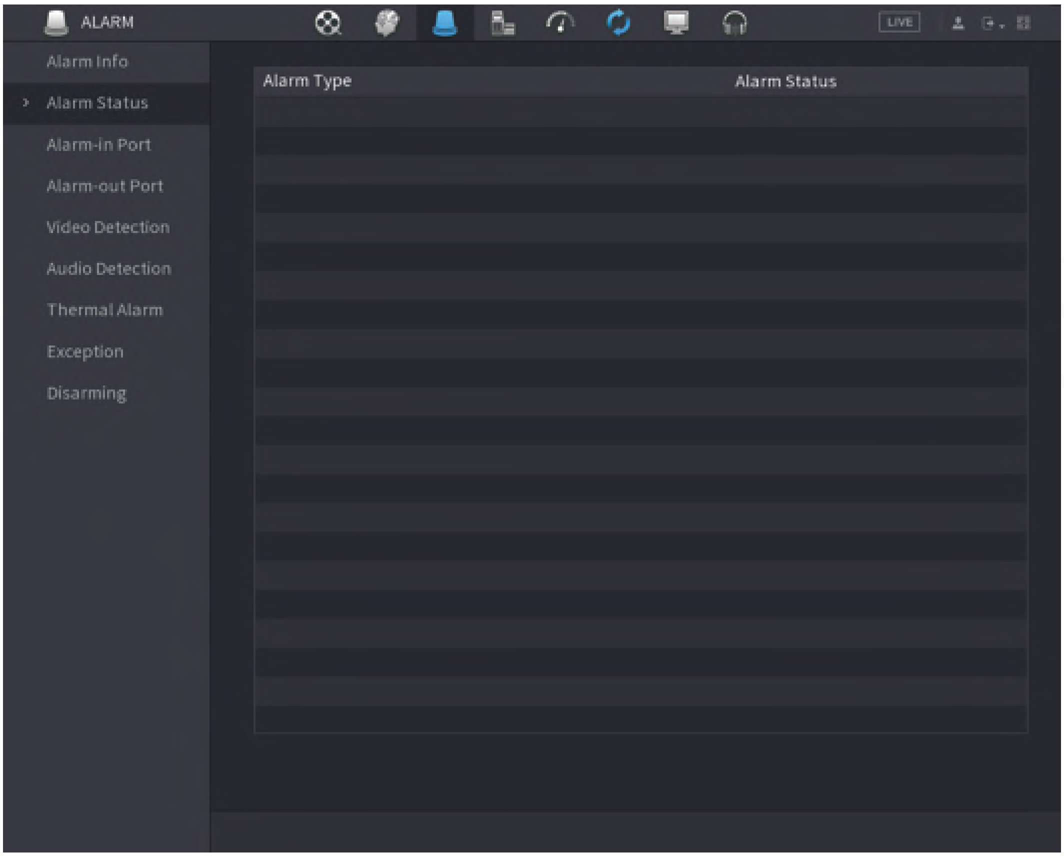
  Double-click a log or click **Details** to view the detailed information of the event.

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



Alarm Type	Alarm Status

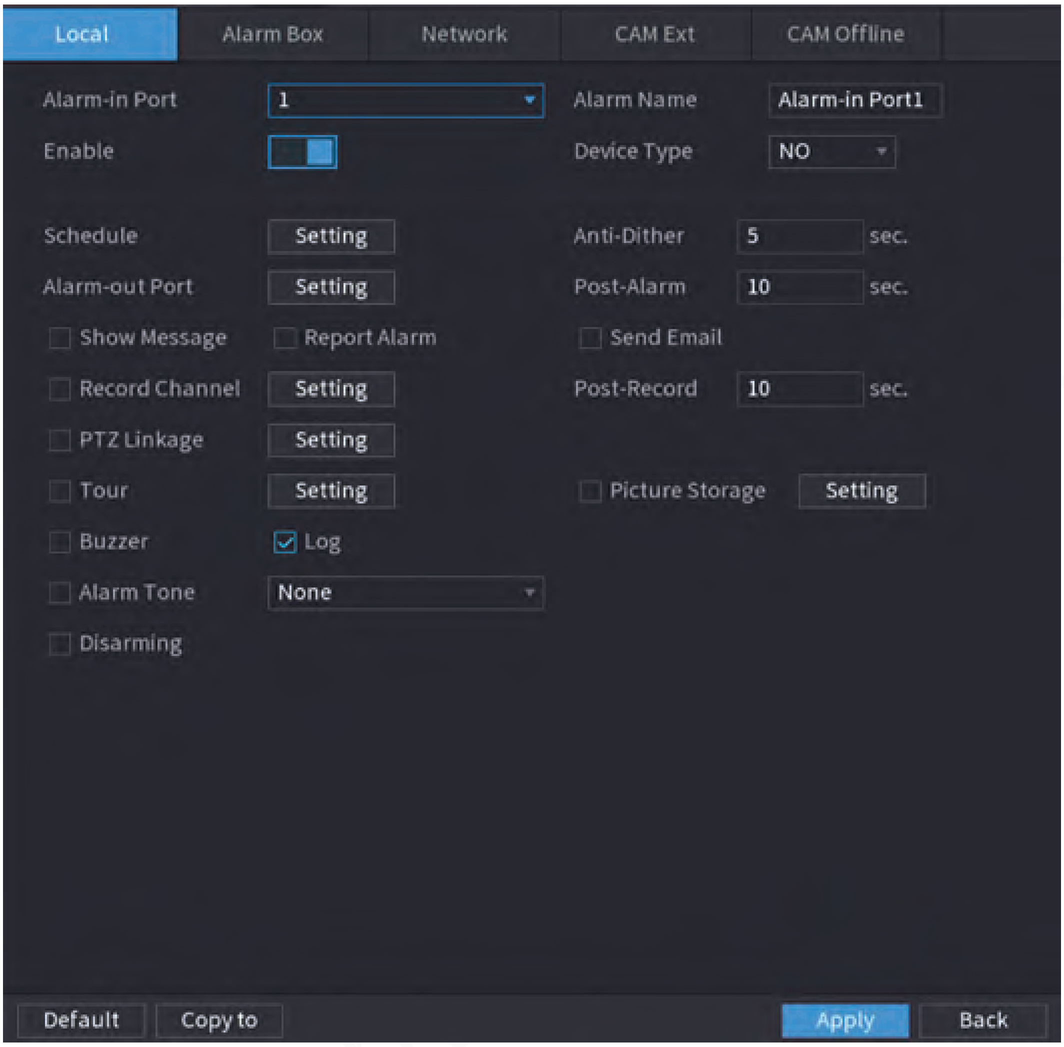
5.10.3 Alarm Input

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



Alarm-in Port: 1
Alarm Name: Alarm-in Port1
Enable: on
Device Type: NO
Schedule: Setting
Anti-Dither: 5 sec.
Alarm-out Port: Setting
Post-Alarm: 10 sec.
☐ Show Message
☐ Report Alarm
☐ Send Email
☐ Record Channel: Setting
Post-Record: 10 sec.
☐ PTZ Linkage: Setting
☐ Tour: Setting
☐ Picture Storage: Setting
☐ Buzzer
☑ Log
☐ Alarm Tone: None
☐ Disarming

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**.

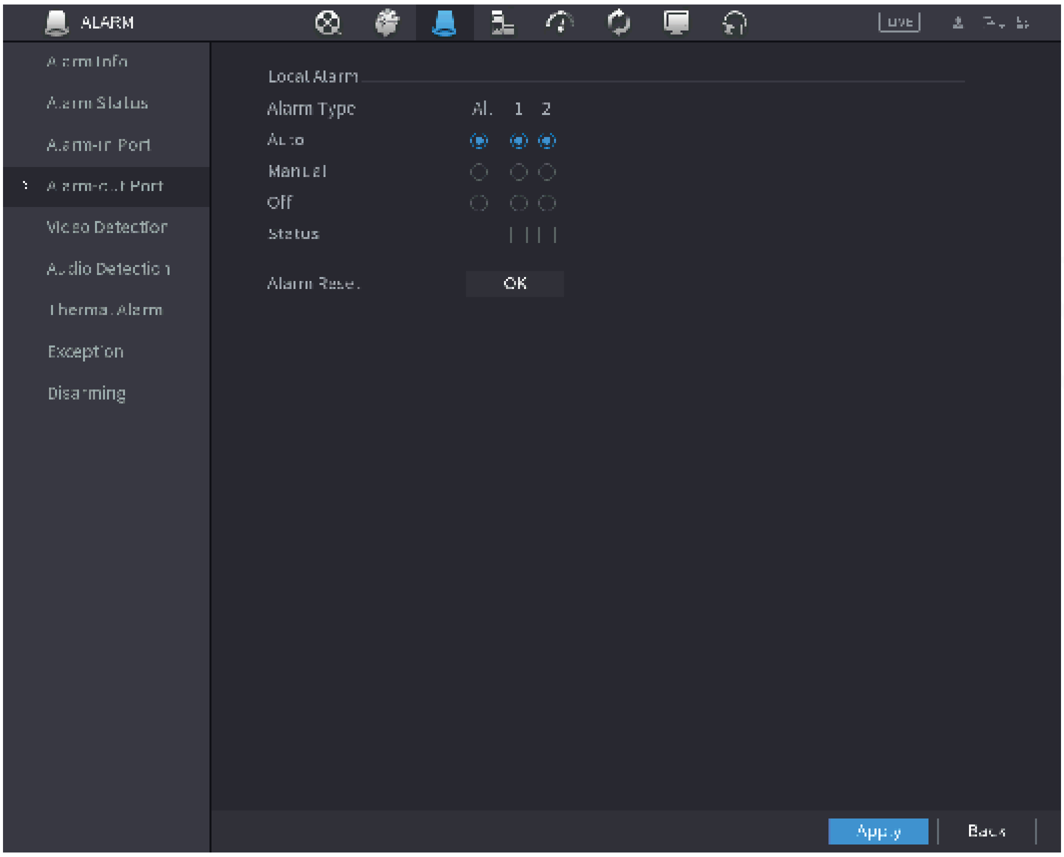
5.10.4 Alarm Output

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



Local Alarm

Alarm Type	All	1	2
Auto	●	●	●
Manual	○	○	○
Off	○	○	○
Status			

Alarm Reset OK

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

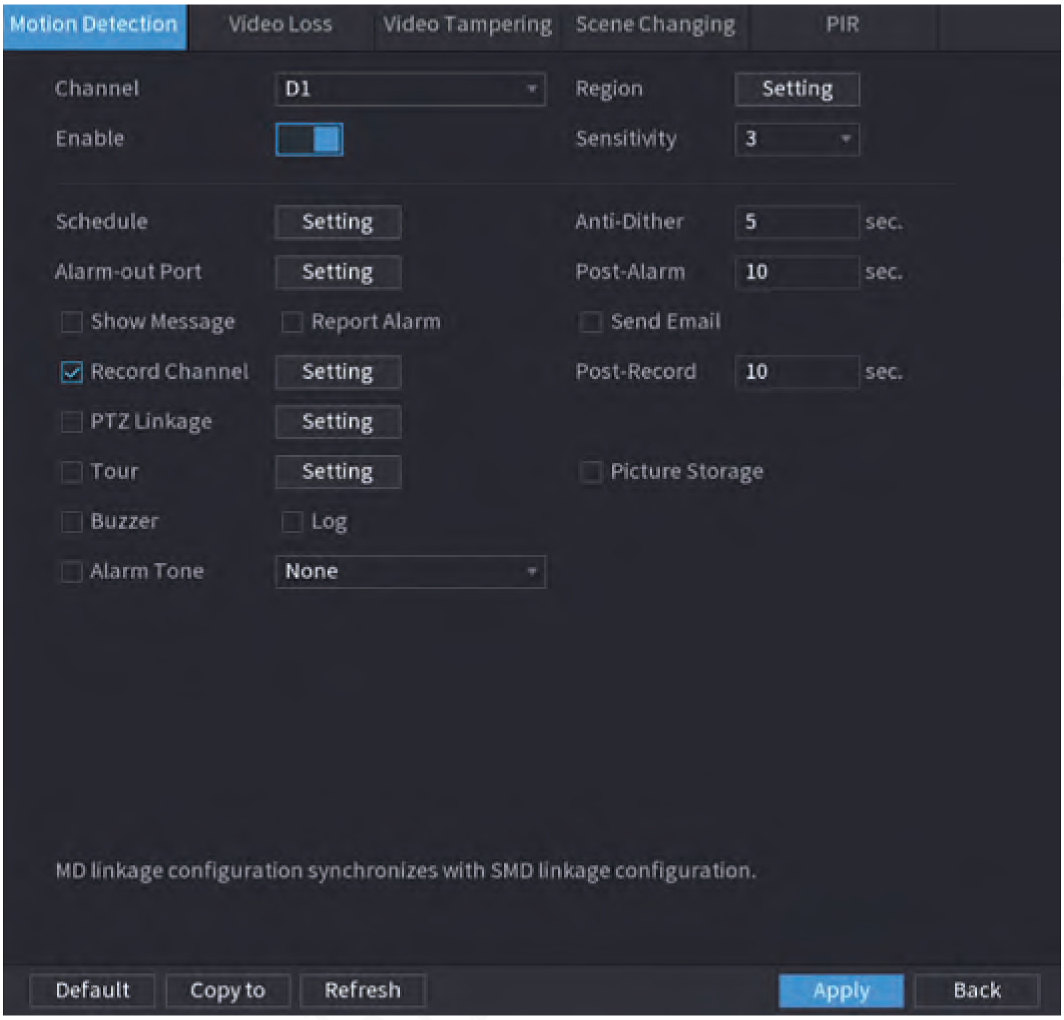
Background Information

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



Motion Detection | Video Loss | Video Tampering | Scene Changing | PIR

Channel: D1
Region: Setting
Enable: ●
Sensitivity: 3

Schedule: Setting
Anti-Dither: 5 sec.
Alarm-out Port: Setting
Post-Alarm: 10 sec.
□ Show Message
□ Report Alarm
□ Send Email
☑ Record Channel: Setting
Post-Record: 10 sec.
□ PTZ Linkage: Setting
□ Tour: Setting
□ Picture Storage
□ Buzzer
□ Log
□ Alarm Tone: None

MD linkage configuration synchronizes with SMD linkage configuration.

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.

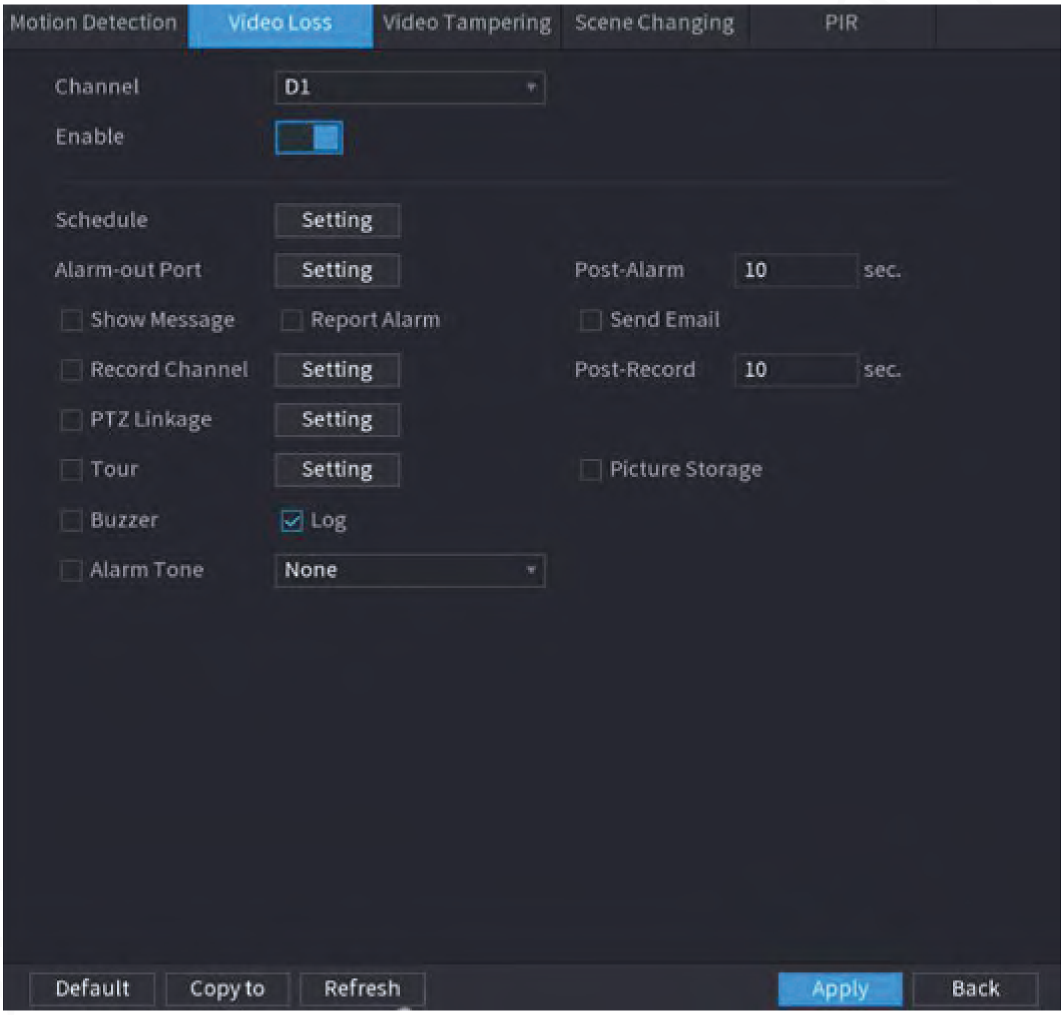
Step 7 Click **Apply**.

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



Channel D1

Enable

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

☐ Show Message ☐ Report Alarm ☐ Send Email

☐ Record Channel Setting Post-Record 10 sec.

☐ PTZ Linkage Setting

☐ Tour Setting ☐ Picture Storage

☐ Buzzer ☑ Log

☐ Alarm Tone None

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.

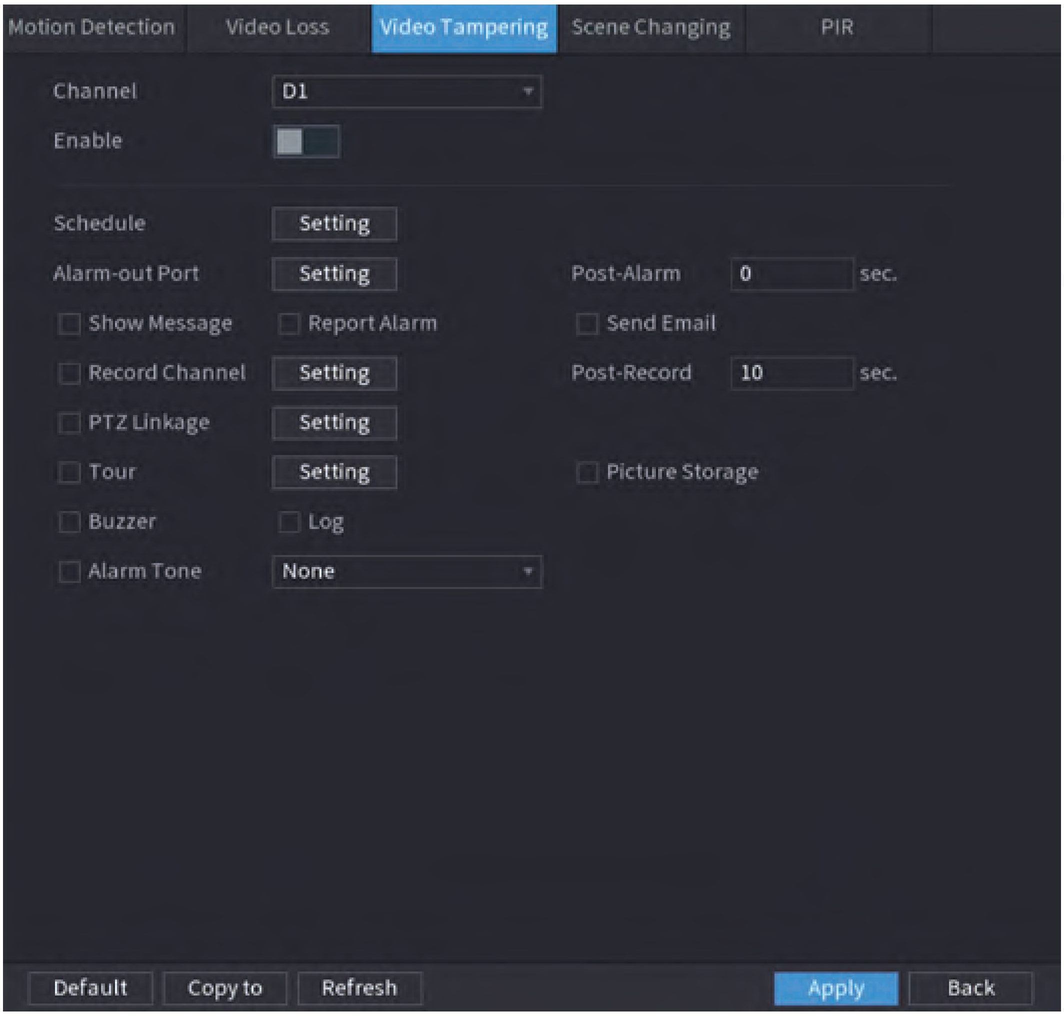
Step 5 Click **Apply**.

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



Channel: D1

Enable

Schedule: Setting

Alarm-out Port: Setting

Post-Alarm: 0 sec.

□ Show Message

□ Report Alarm

□ Send Email

□ Record Channel: Setting

Post-Record: 10 sec.

□ PTZ Linkage: Setting

□ Tour: Setting

□ Picture Storage

□ Buzzer

□ Log

□ Alarm Tone: None

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

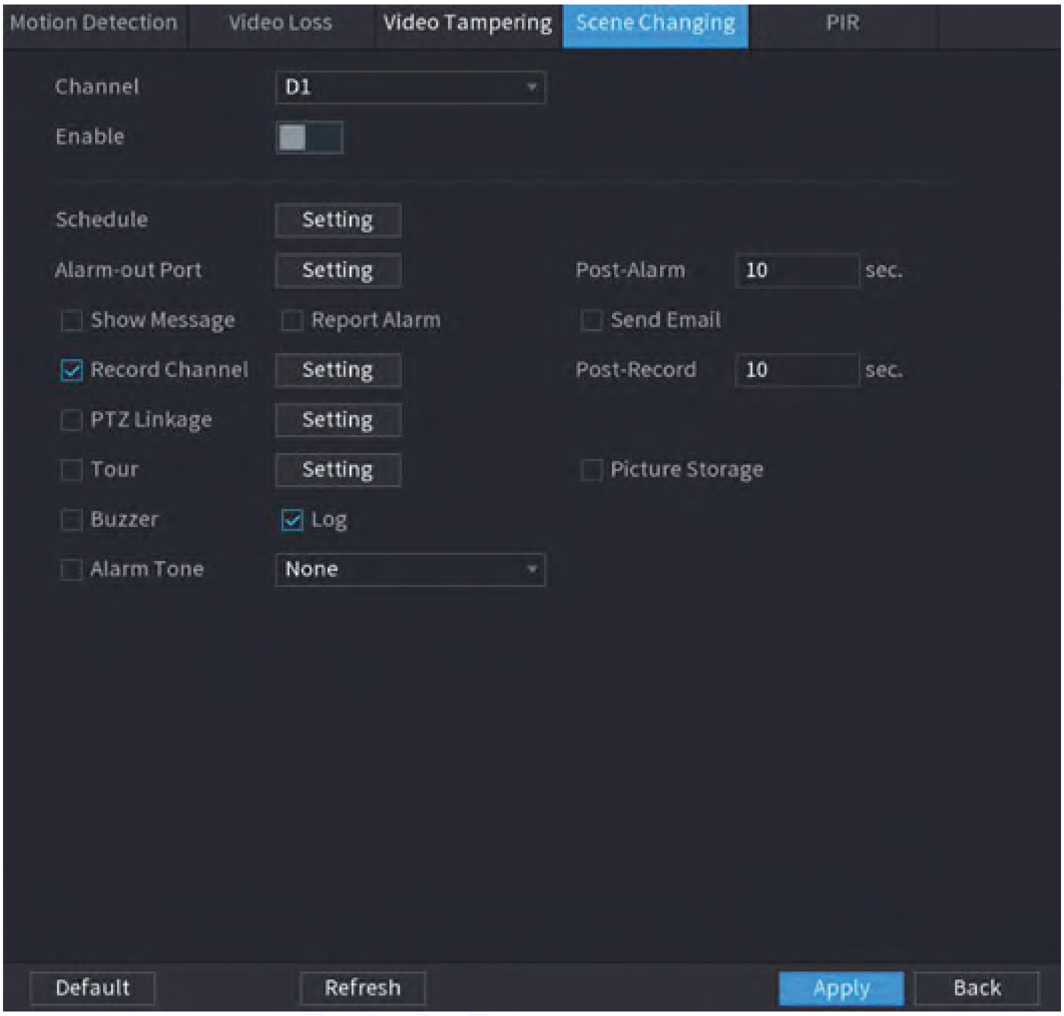
Background Information

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



Channel D1

Enable

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Show Message □ Report Alarm □ Send Email

☑ Record Channel Setting Post-Record 10 sec.

□ PTZ Linkage Setting

□ Tour Setting □ Picture Storage

□ Buzzer ☑ Log

□ Alarm Tone None

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**.

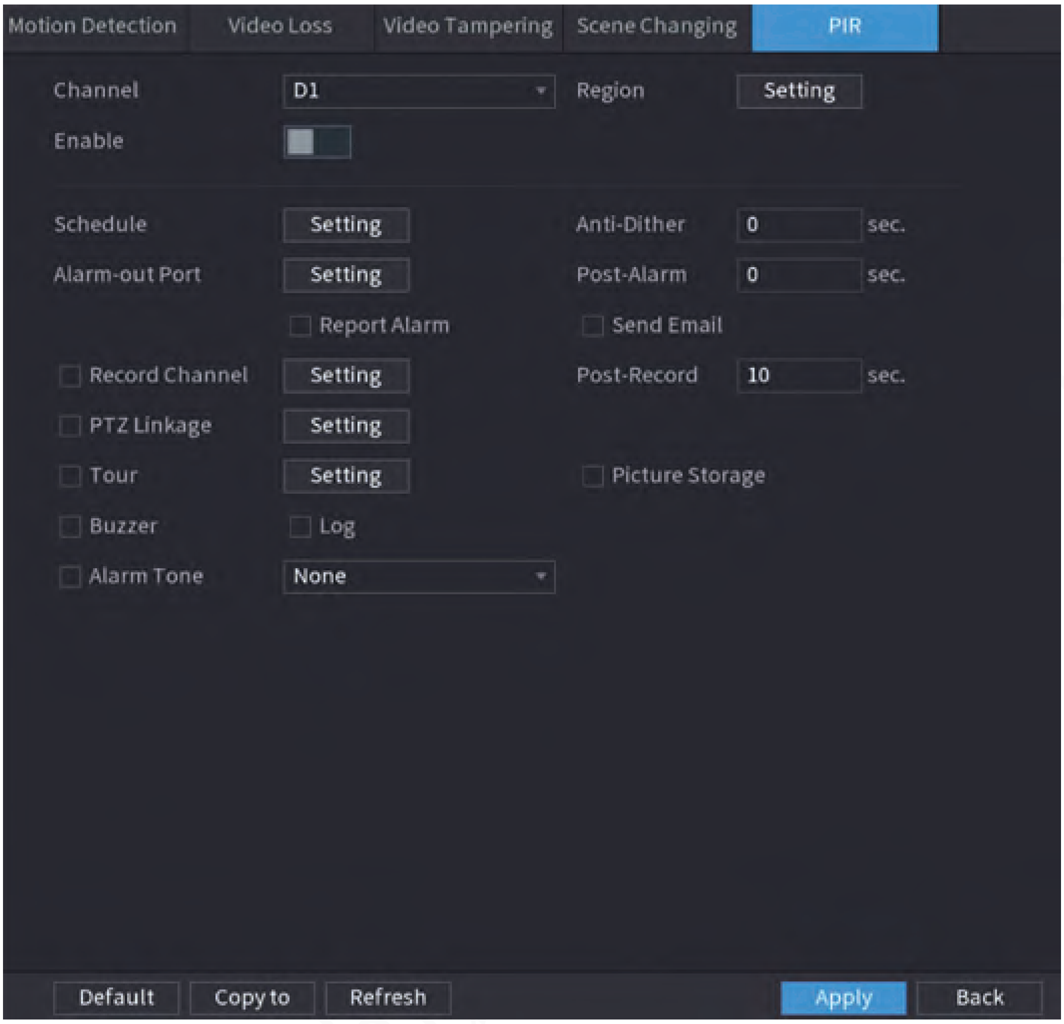
5.10.5.5 PIR Alarm

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



Channel: D1

Region: Setting

Enable

Schedule: Setting

Anti-Dither: 0 sec.

Alarm-out Port: Setting

Post-Alarm: 0 sec.

□ Report Alarm

□ Send Email

□ Record Channel: Setting

Post-Record: 10 sec.

□ PTZ Linkage: Setting

□ Tour: Setting

□ Picture Storage

□ Buzzer

□ Log

□ Alarm Tone: None

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.

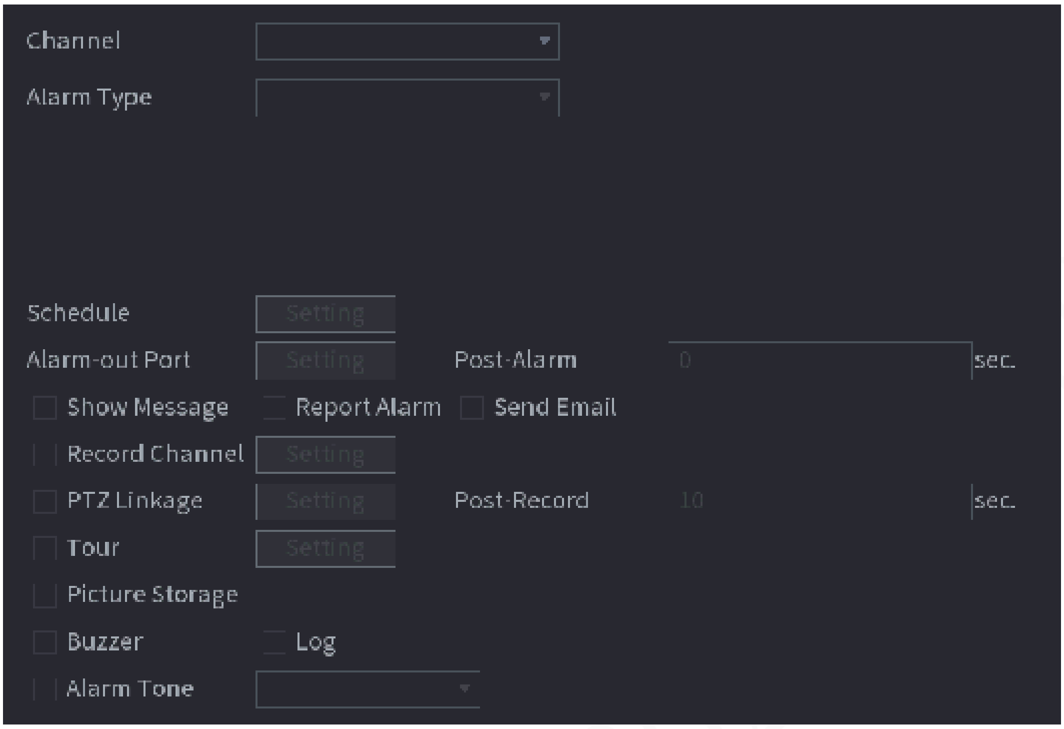
The system supports heat alarm, temperature (temperature difference) and cold/hot alarm.

- 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



Post-Alarm 0 sec.

Post-Record 10 sec.

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.

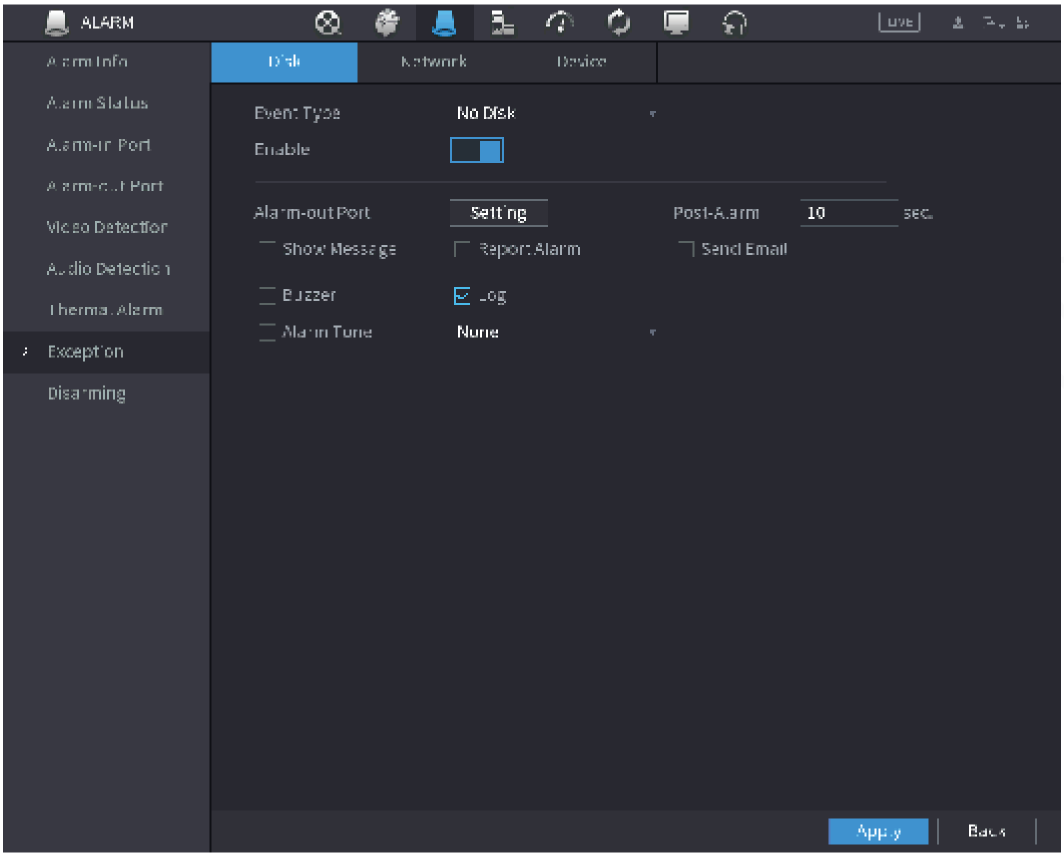
Step 5 Click **Apply**.

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



Event Type: No Disk

Enable

Alarm-out Port: Setting Post-Alarm: 10 sec.

☐ Show Message ☐ Report Alarm ☐ Send Email

☐ Buzzer ☑ Log

☐ Alarm Tone: None

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**.

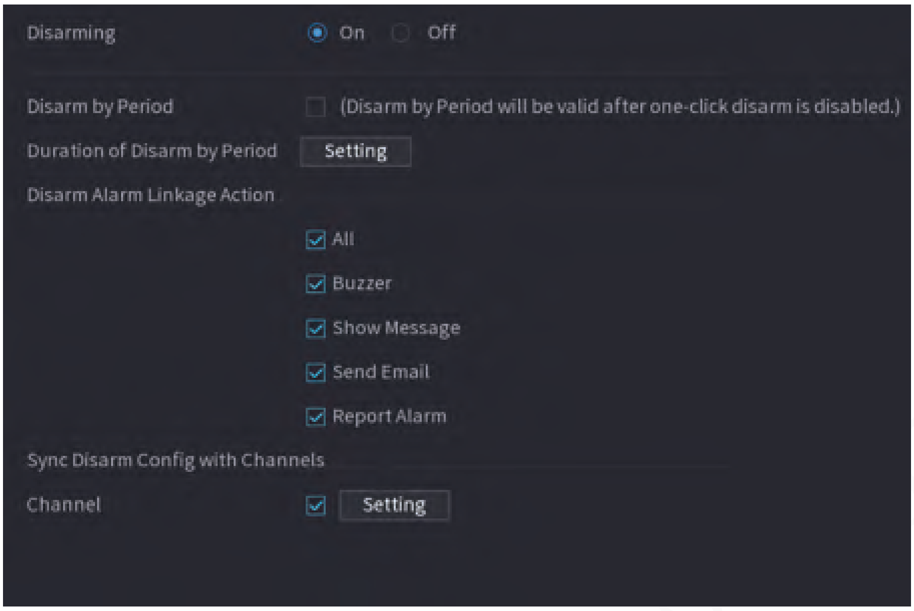
5.10.9 Disarming

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



Disarming ● On ○ Off

Disarm by Period □ (Disarm by Period will be valid after one-click disarm is disabled.)

Duration of Disarm by Period Setting

Disarm Alarm Linkage Action

☑ All

☑ Buzzer

☑ Show Message

☑ Send Email

☑ Report Alarm

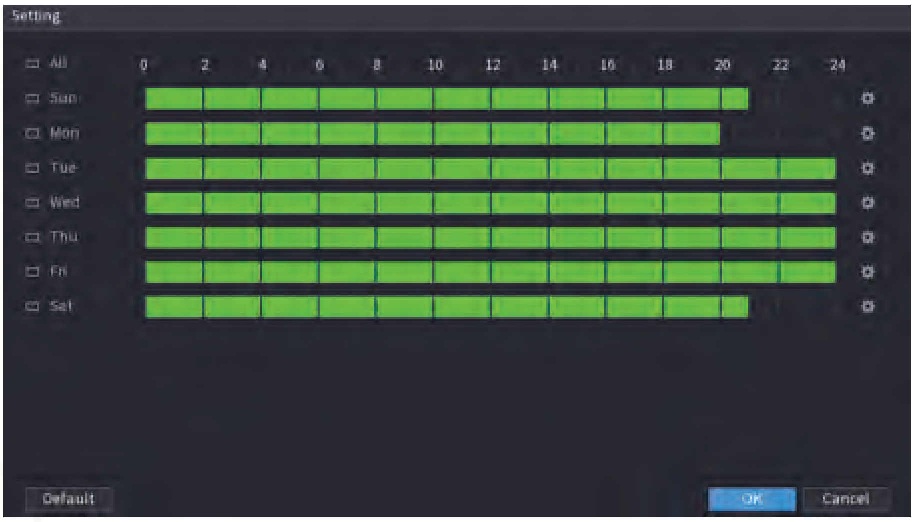
Sync Disarm Config with Channels

Channel ☑ Setting

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

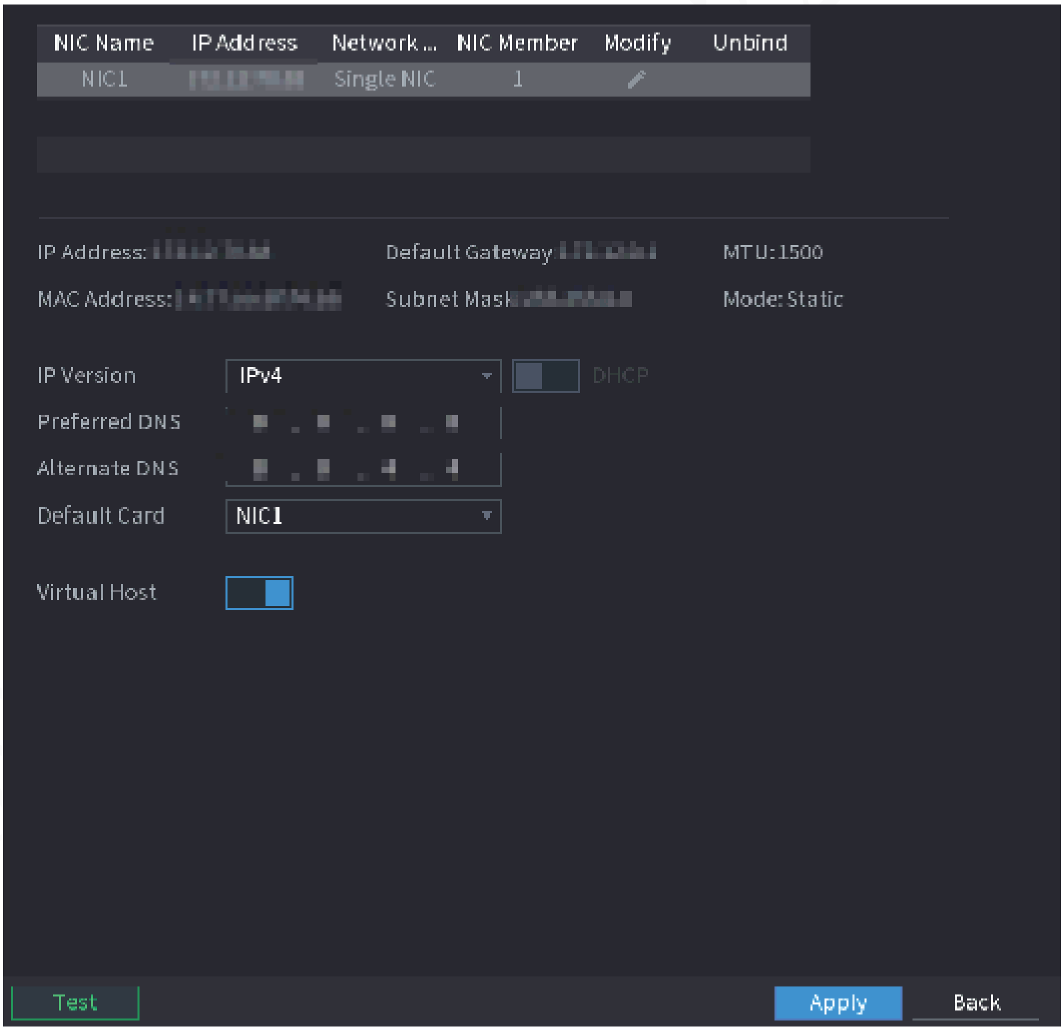
Configure the network settings to ensure the Device can communicate with other devices on the same LAN.

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



NIC Name	IP Address	Network ...	NIC Member	Modify	Unbind
NIC1	[redacted]	Single NIC	1	✎	

IP Address: [redacted]

Default Gateway [redacted]

MTU:1500

MAC Address: [redacted]

Subnet Mask [redacted]

Mode: Static

IP Version: IPv4

DHCP: ○

Preferred DNS: [redacted]

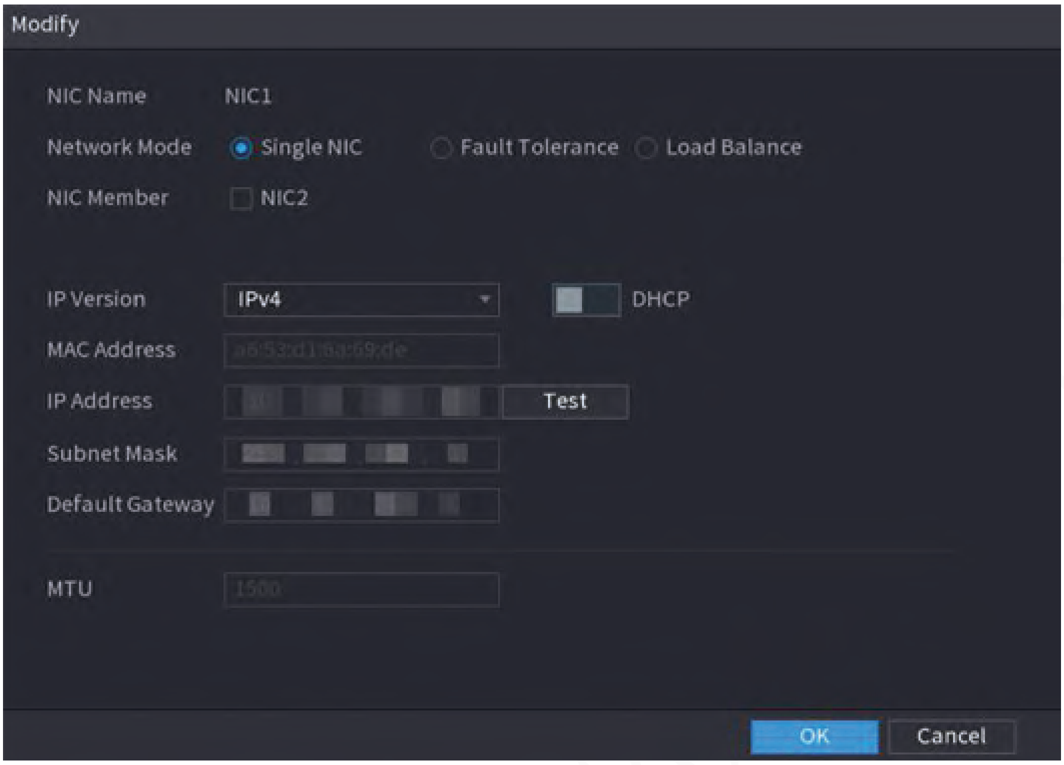
Alternate DNS: [redacted]

Default Card: NIC1

Virtual Host: ●

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

Figure 5-178 TCP/IP



Modify

NIC Name NIC1

Network Mode ● Single NIC ○ Fault Tolerance ○ Load Balance

NIC Member □ NIC2

IP Version IPv4

DHCP

MAC Address a6:53:d1:6a:69:de

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

MTU 1500

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.
MAC Address	Displays the MAC address of the Device.

Parameter	Description
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.

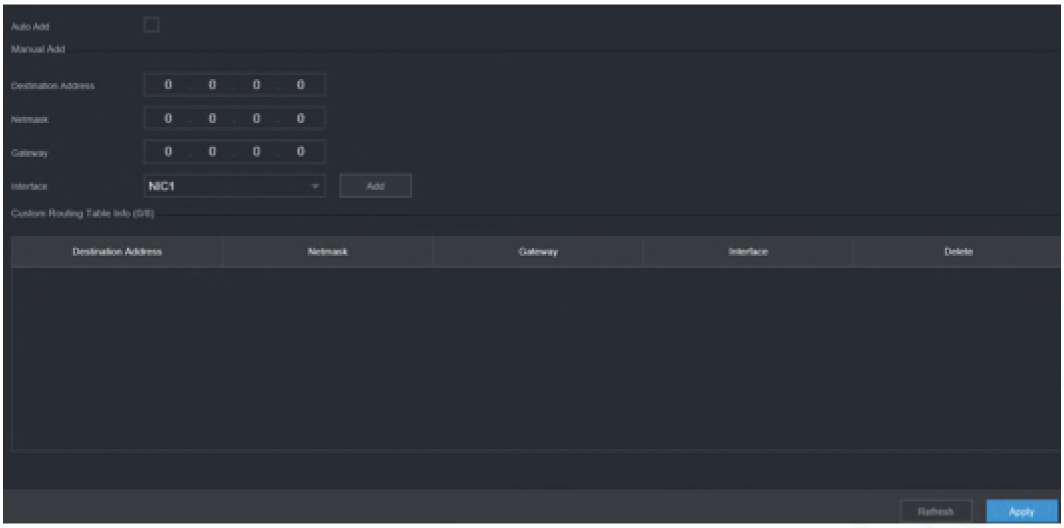
Step 5 Click **Apply**.

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



Auto Add □

Manual Add

Destination Address 0 . 0 . 0 . 0

Netmask 0 . 0 . 0 . 0

Gateway 0 . 0 . 0 . 0

Interface NIC1

Custom Routing Table Info (0/8)

Destination Address	Netmask	Gateway	Interface	Delete

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.

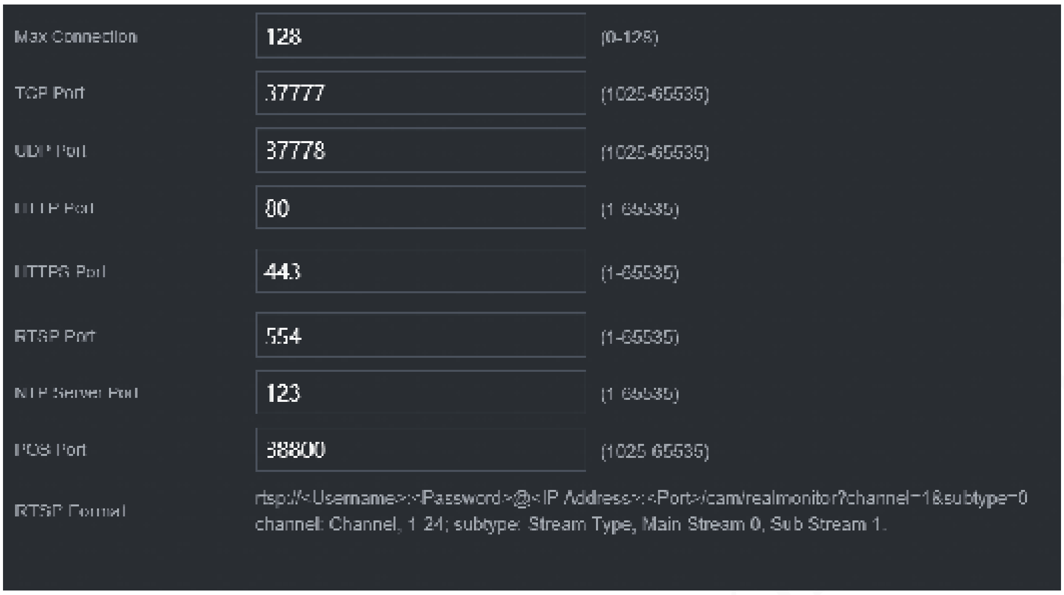
Step 3 Click **Apply**.

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



```
Max Connection     128      (0-128)
TCP Port           37777    (1025-65535)
UDP Port           37778    (1025-65535)
HTTP Port          80       (1-65535)
HTTPS Port         443      (1-65535)
RTSP Port          554      (1-65535)
NTP Server Port    123      (1-65535)
POS Port           38800    (1025-65535)
RTSP Format        rtsp://<Username>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel=1&subtype=0
                   channel: Channel, 1-24; subtype: Stream Type, Main Stream 0, Sub Stream 1.
```

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.

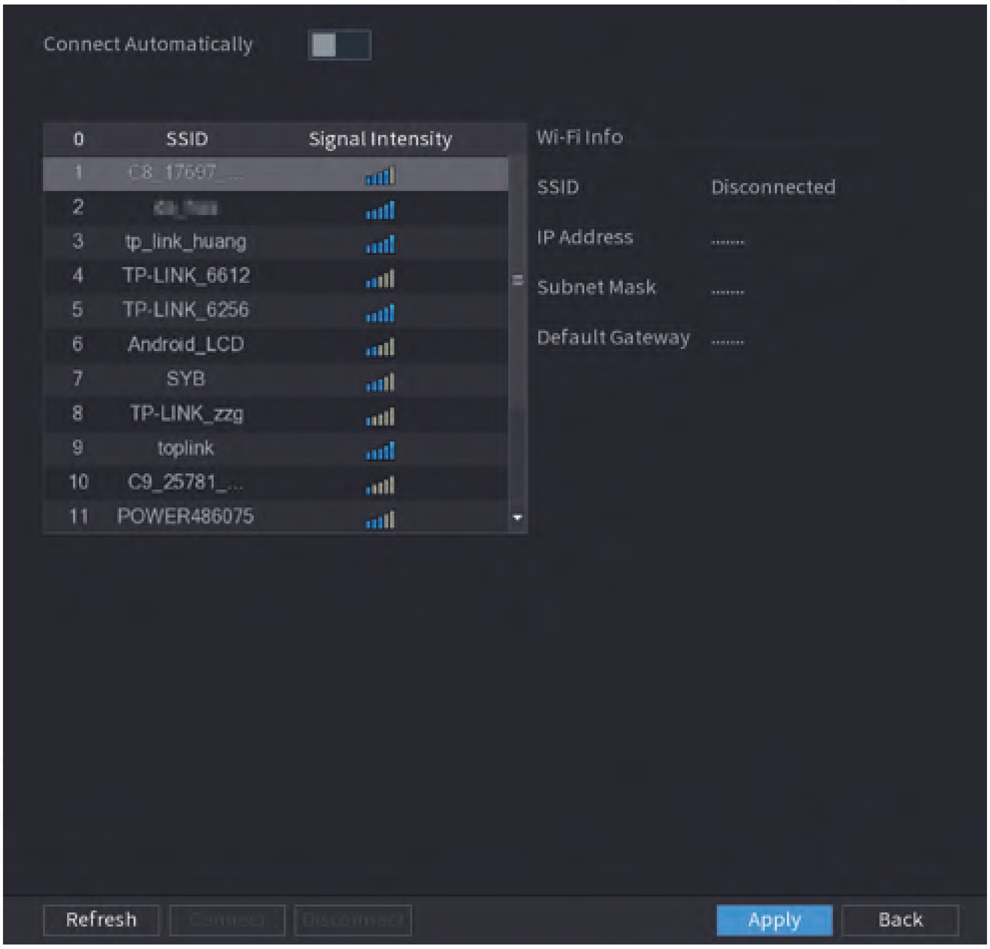
Background Information

This function is available on select models.

Procedure

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

Figure 5-181 Wi-Fi



Connect Automatically

0	SSID	Signal Intensity
1	C8_17697_...	
2	[illegible]	
3	tp_link_huang	
4	TP-LINK_6612	
5	TP-LINK_6256	
6	Android_LCD	
7	SYB	
8	TP-LINK_zzg	
9	toplink	
10	C9_25781_...	
11	POWER486075	

Wi-Fi Info

SSID Disconnected

IP Address ....

Subnet Mask ....

Default Gateway ....

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.
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.

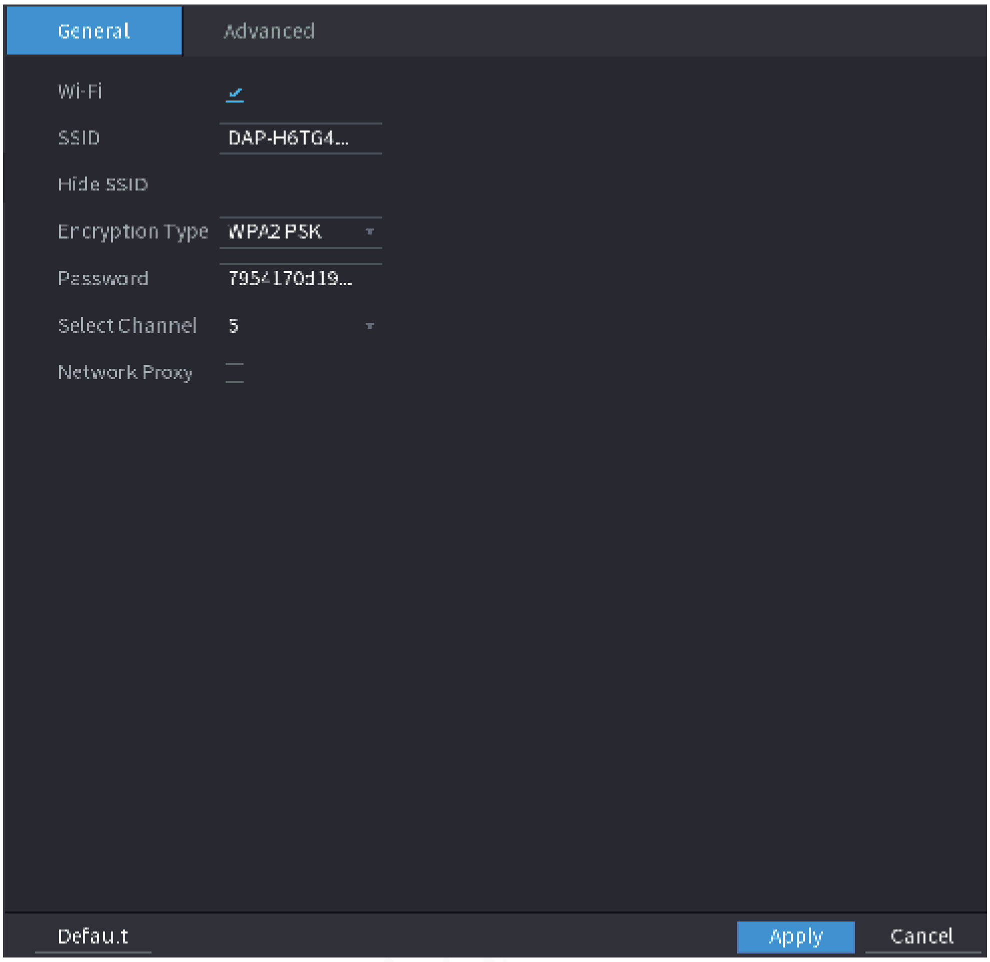
5.11.5.1 General Settings

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



Wi-Fi ☑

SSID DAP-H6TG4...

Hide SSID

Encryption Type WPA2 PSK

Password 7954170d19...

Select Channel 5

Network Proxy □

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**.

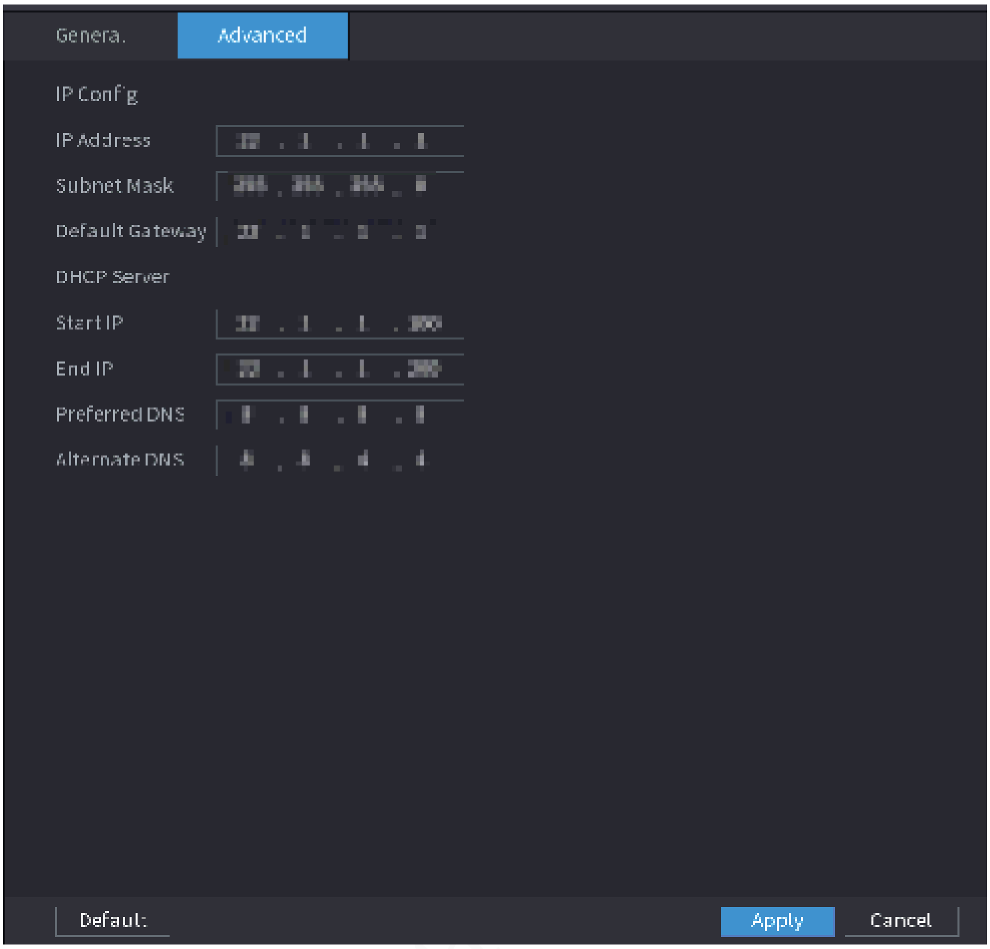
5.11.5.2 Advanced Settings

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



IP Config

IP Address: [redacted]

Subnet Mask: [redacted]

Default Gateway: [redacted]

DHCP Server

Start IP: [redacted]

End IP: [redacted]

Preferred DNS: [redacted]

Alternate DNS: [redacted]

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.

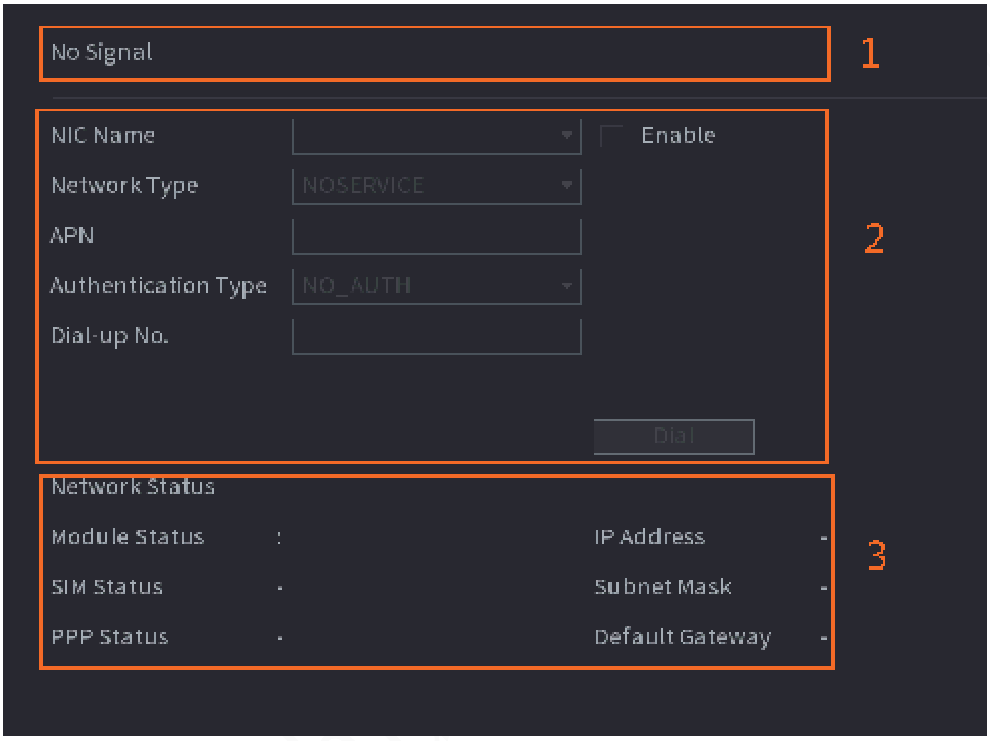
Background Information

This function is available on select models.

Procedure

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

Figure 5-184 3G/4G



No Signal

NIC Name ☐ Enable

Network Type NOSERVICE

APN

Authentication Type NO_AUTH

Dial-up No.

Dial

Network Status

Module Status : IP Address -

SIM Status - Subnet Mask -

PPP Status - Default Gateway -

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.

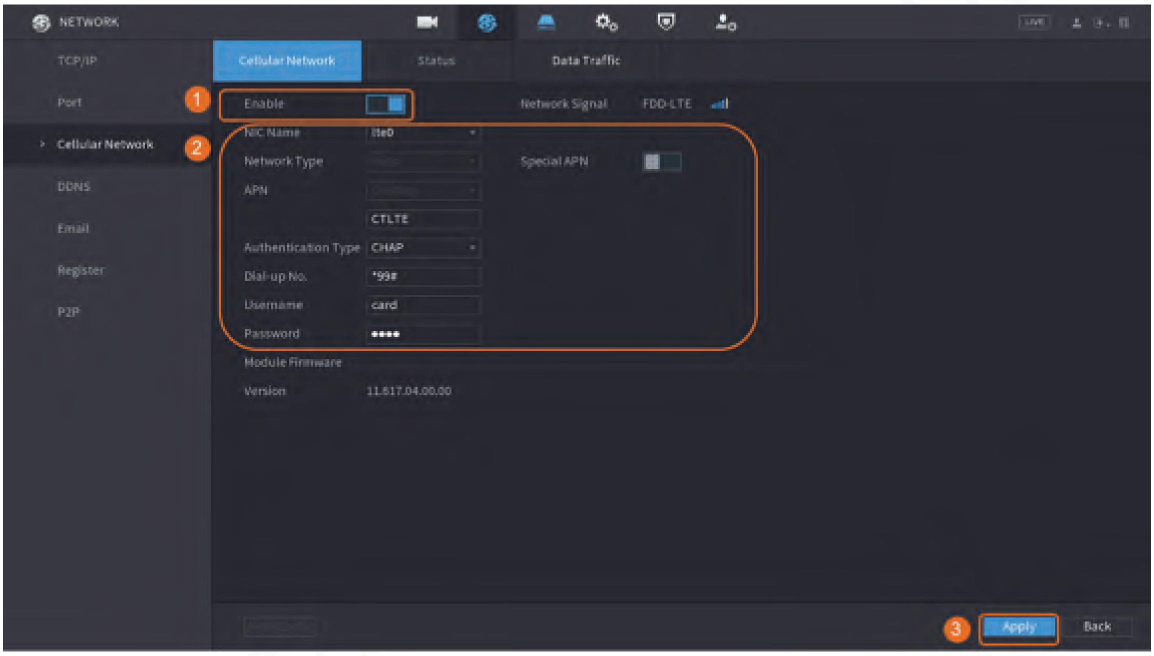
This function is available on select models.

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



Enable
Network Signal FDD-LTE
NIC Name lte0
Network Type
Special APN
APN
CTLTE
Authentication Type CHAP
Dial-up No. *99#
Username card
Password ●●●●
Module Firmware
Version 11.617.04.00.00

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.

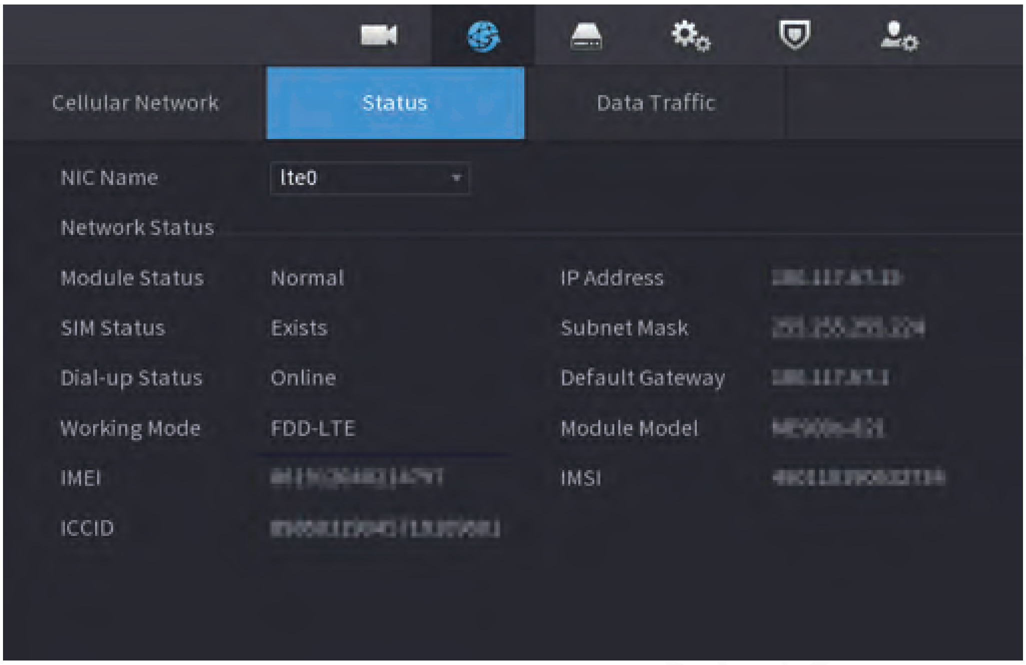
Step 3 Click **Apply**.

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.

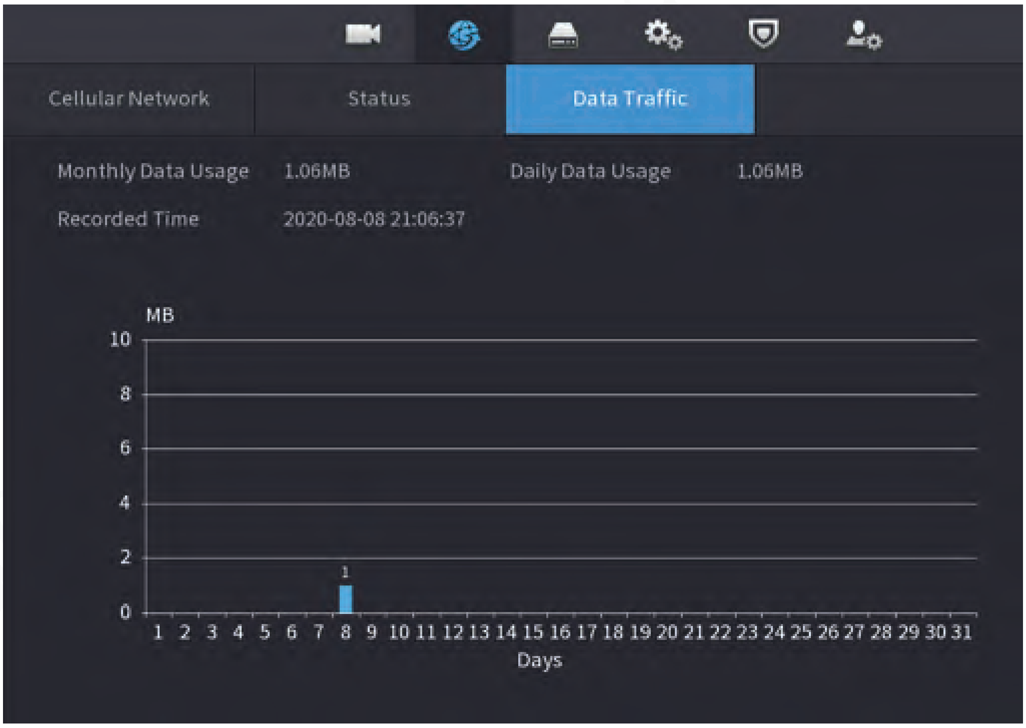
Figure 5-186 Network status



NIC Name	lte0		
Network Status			
Module Status	Normal	IP Address	[redacted]
SIM Status	Exists	Subnet Mask	[redacted]
Dial-up Status	Online	Default Gateway	[redacted]
Working Mode	FDD-LTE	Module Model	[redacted]
IMEI	[redacted]	IMSI	[redacted]
ICCID	[redacted]		

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

Figure 5-187 Cellular data usage



Monthly Data Usage	1.06MB	Daily Data Usage	1.06MB
Recorded Time	2020-08-08 21:06:37		

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.

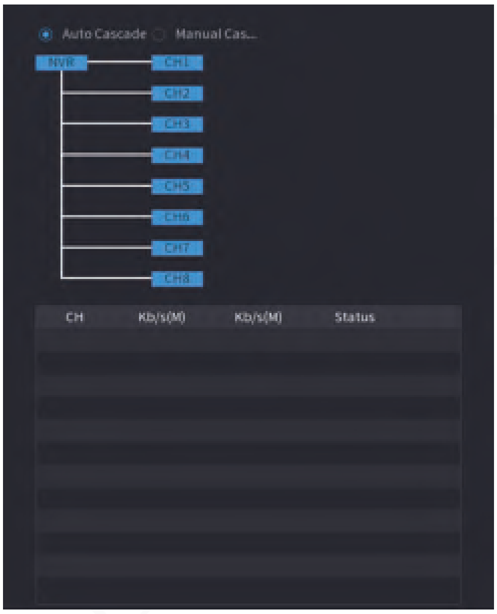
Procedure

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



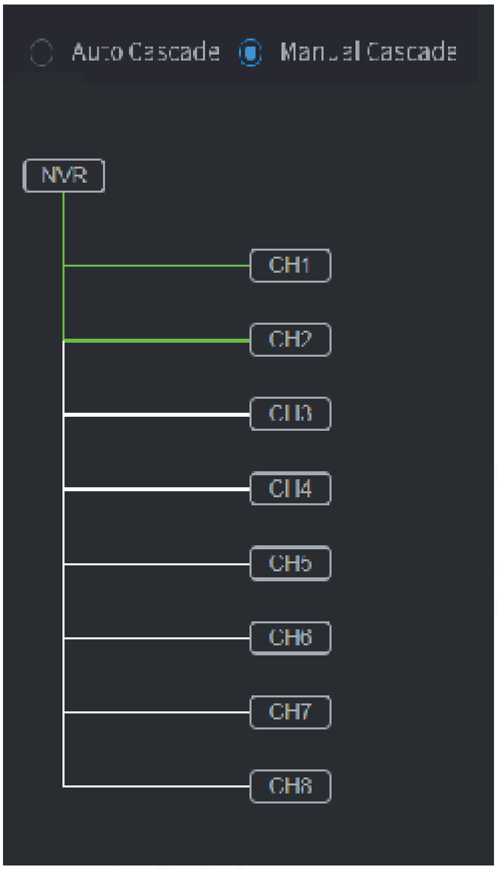
● Auto Cascade ○ Manual Cas...

CH	Kb/s(M)	Kb/s(M)	Status

Step 3 Select **Manual Cascade**.

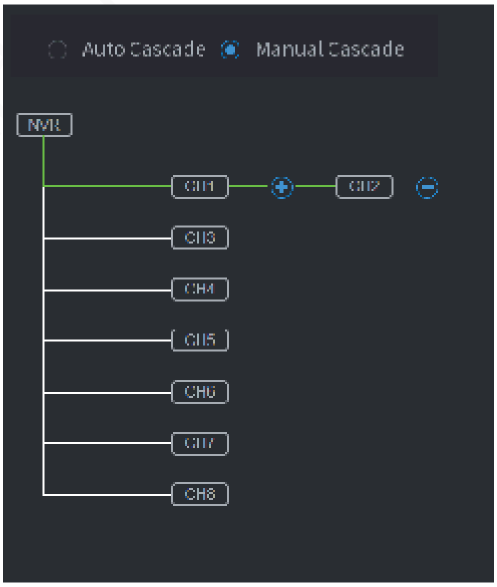
You can use manual cascade when there are at least two IPCs on the network.

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

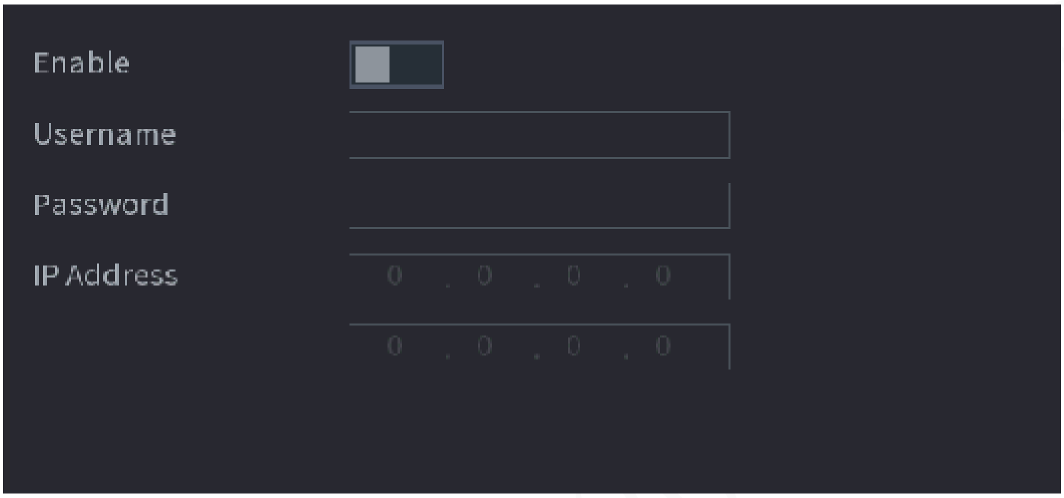
PPPoE is another way for the Device to access the network. You can establish network connection by configuring PPPoE settings to give the Device a dynamic IP address on the WAN.

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



Enable

Username

Password

IP Address 0 . 0 . 0 . 0

0 . 0 . 0 . 0

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.

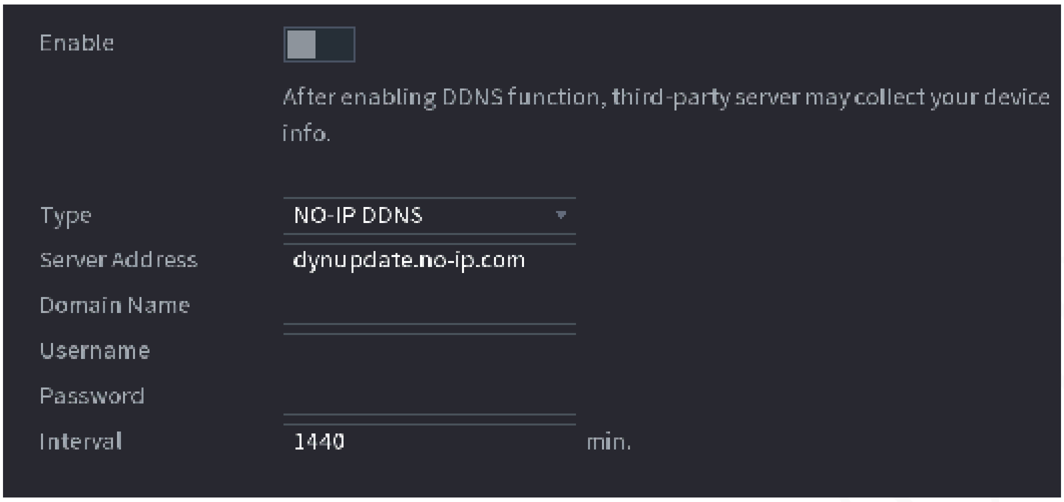
Check the type of DDNS that the Device supports and then log in to the website provided by the DDNS service provider to register domain and other information.

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



Enable

After enabling DDNS function, third-party server may collect your device info.

Type: NO-IP DDNS

Server Address: dynupdate.no-ip.com

Domain Name

Username

Password

Interval: 1440 min.

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.

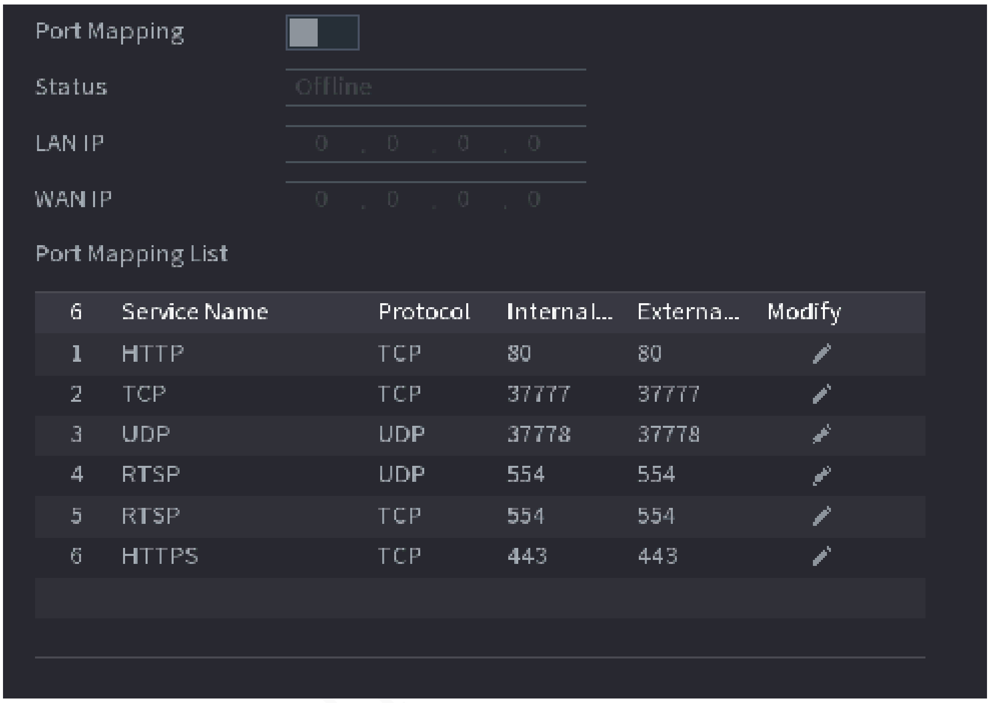
Step 4 Select **Main Menu** > **NETWORK** > **TCP/IP**, configure the IP address into the router IP address range, or enable the DHCP function to obtain an IP address automatically.

5.11.11.2 Configuring UPnP

Procedure

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

Figure 5-193 UPnP



Port Mapping □

Status Offline

LAN IP 0 . 0 . 0 . 0

WAN IP 0 . 0 . 0 . 0

Port Mapping List

6	Service Name	Protocol	Internal...	Externa...	Modify
1	HTTP	TCP	80	80	✎
2	TCP	TCP	37777	37777	✎
3	UDP	UDP	37778	37778	✎
4	RTSP	UDP	554	554	✎
5	RTSP	TCP	554	554	✎
6	HTTPS	TCP	443	443	✎

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

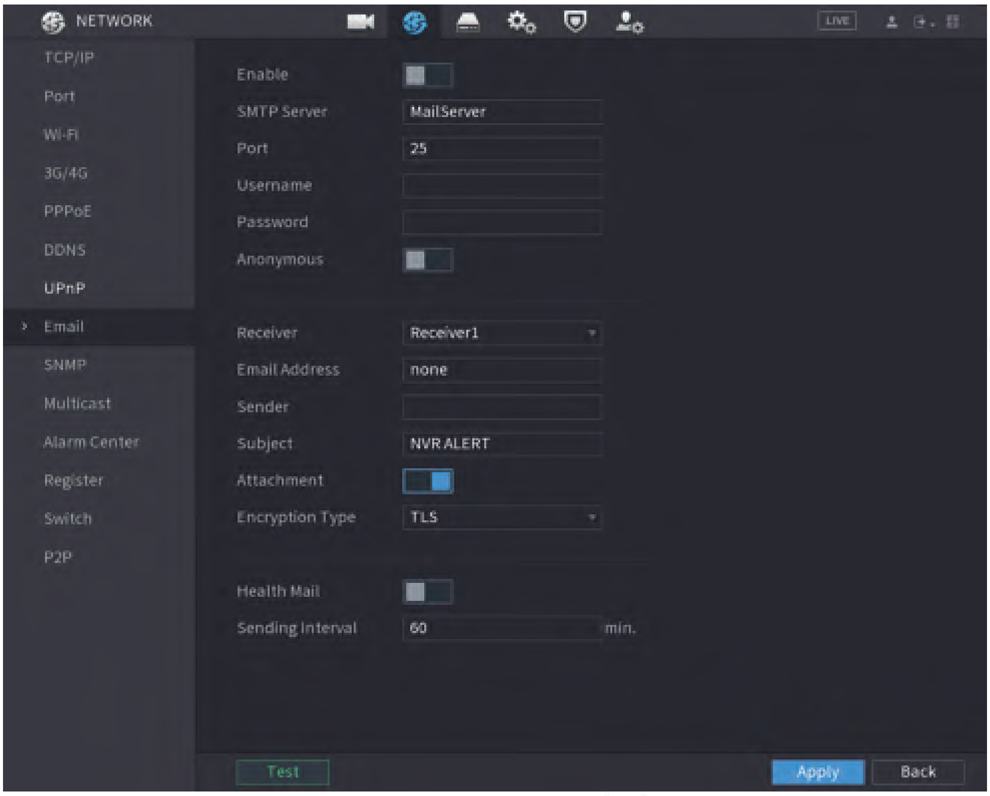
Background Information

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



Enable
SMTP Server: MailServer
Port: 25
Username
Password
Anonymous
Receiver: Receiver1
Email Address: none
Sender
Subject: NVR ALERT
Attachment
Encryption Type: TLS
Health Mail
Sending Interval: 60 min.

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

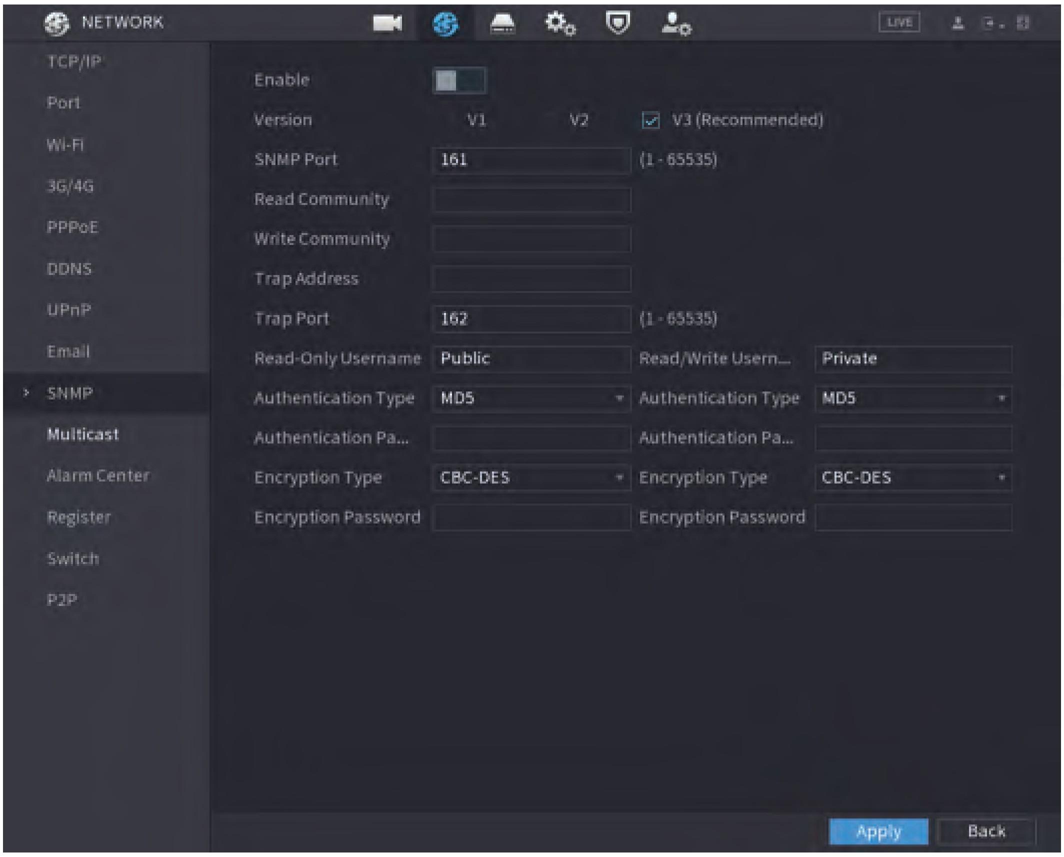
- Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser
- Obtain the MIB files that correspond to the current version from the technical support.

This function is available on select models.

Procedure

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

Figure 5-195 SNMP



Enable □

Version: V1 V2 ☑ V3 (Recommended)

SNMP Port: 161 (1 - 65535)

Read Community:

Write Community:

Trap Address:

Trap Port: 162 (1 - 65535)

Read-Only Username: Public | Read/Write Usern...: Private

Authentication Type: MD5 | Authentication Type: MD5

Authentication Pa...: | Authentication Pa...:

Encryption Type: CBC-DES | Encryption Type: CBC-DES

Encryption Password: | Encryption Password:

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.
Encryption Type	Select an encryption type. The default setting is CBC-DES.

Parameter	Description
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

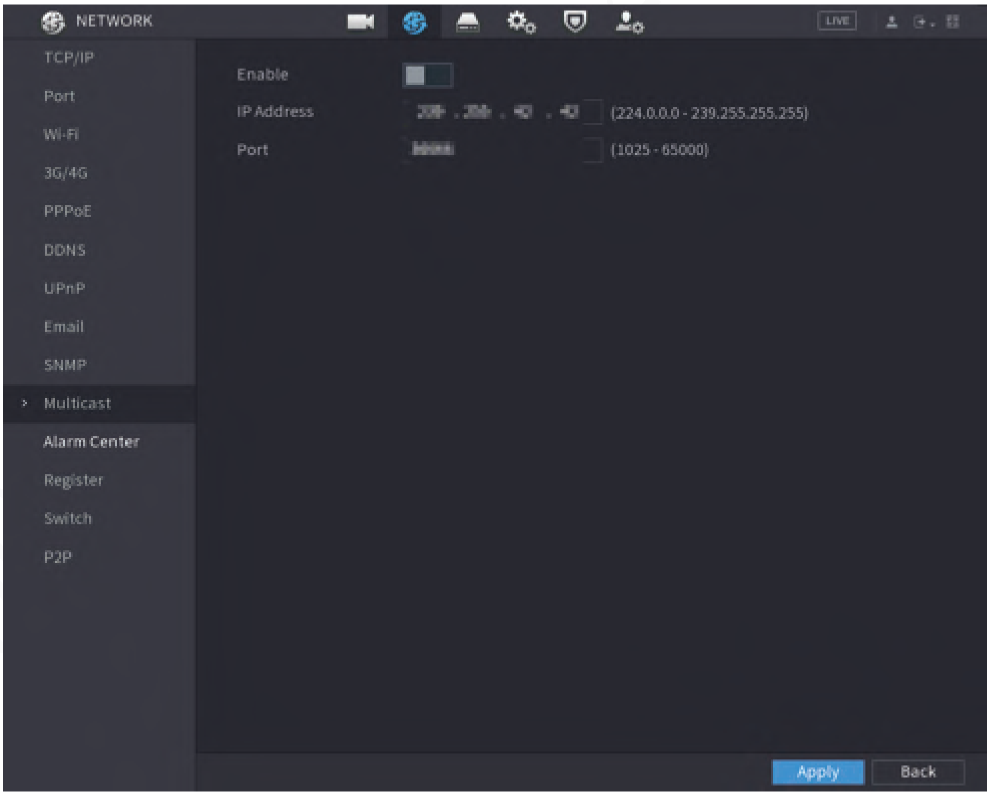
Background Information

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



Enable
IP Address [illegible] (224.0.0.0 - 239.255.255.255)
Port [illegible] (1025 - 65000)

Step 2 Configure the parameters.

Table 5-60

Parameter	Description
Enable	Enable the multicast function.
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.

Parameter	Description
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

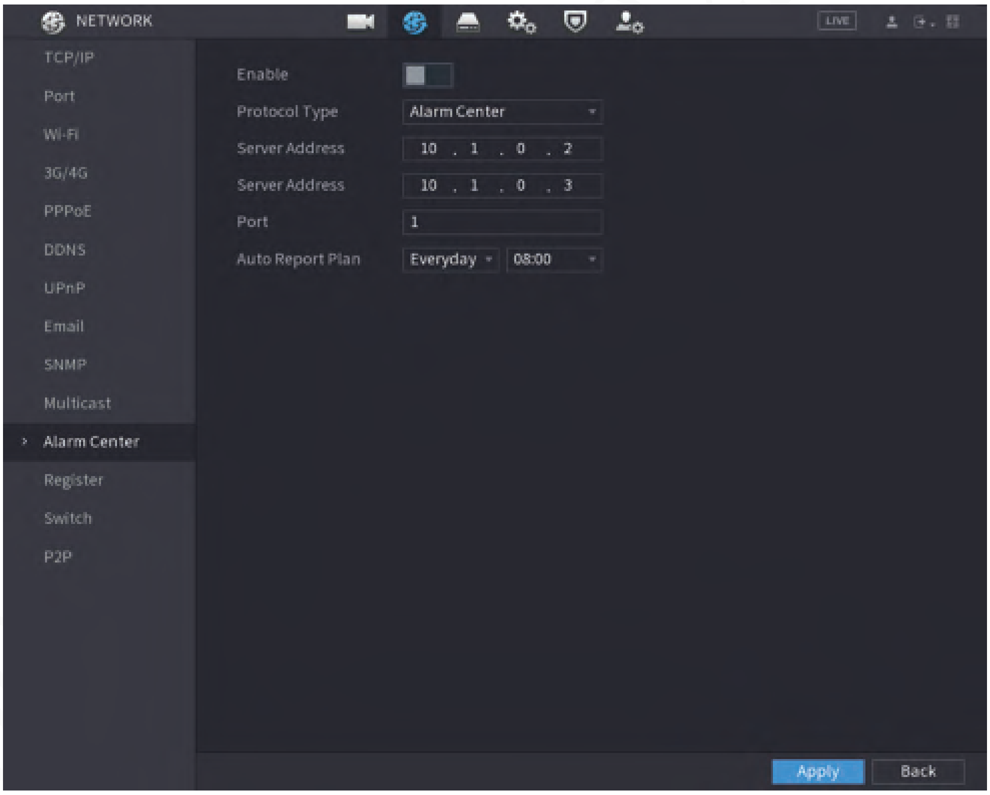
Background Information

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



Enable
Protocol Type: Alarm Center
Server Address: 10 . 1 . 0 . 2
Server Address: 10 . 1 . 0 . 3
Port: 1
Auto Report Plan: Everyday 08:00

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.
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

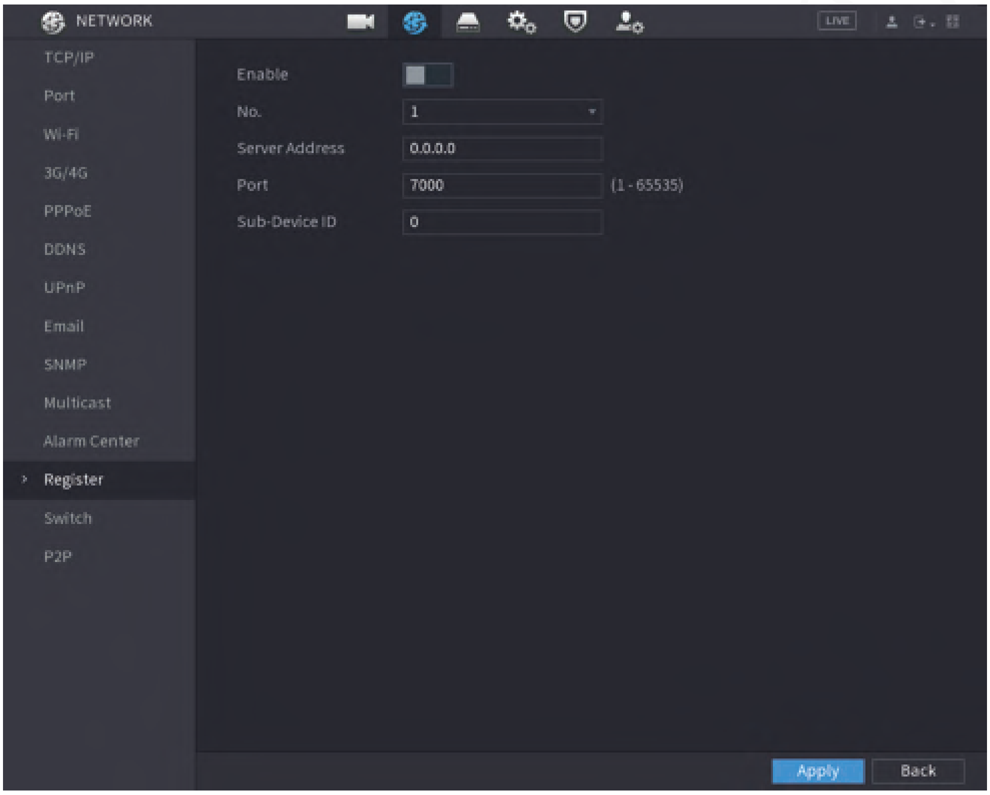
You can register the Device into the specified proxy server which acts as the transit to enable the client software to access the Device

- 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



Enable
No. 1
Server Address 0.0.0.0
Port 7000 (1 - 65535)
Sub-Device ID 0

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.
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

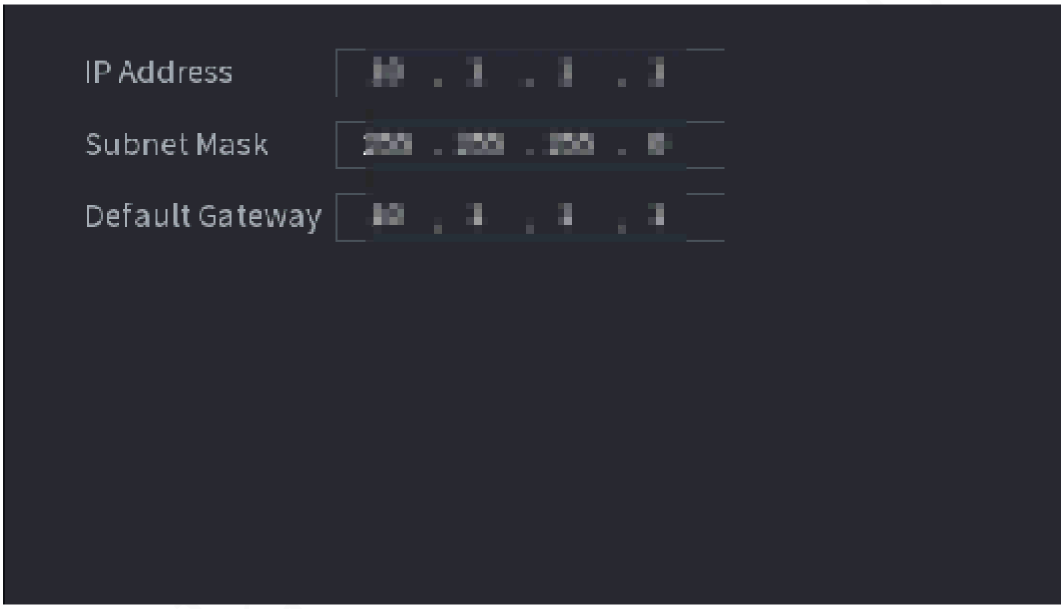
IP address to the IPC according to the defined IP segment, and the NVR will automatically connect to the IPC.

- 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



IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

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

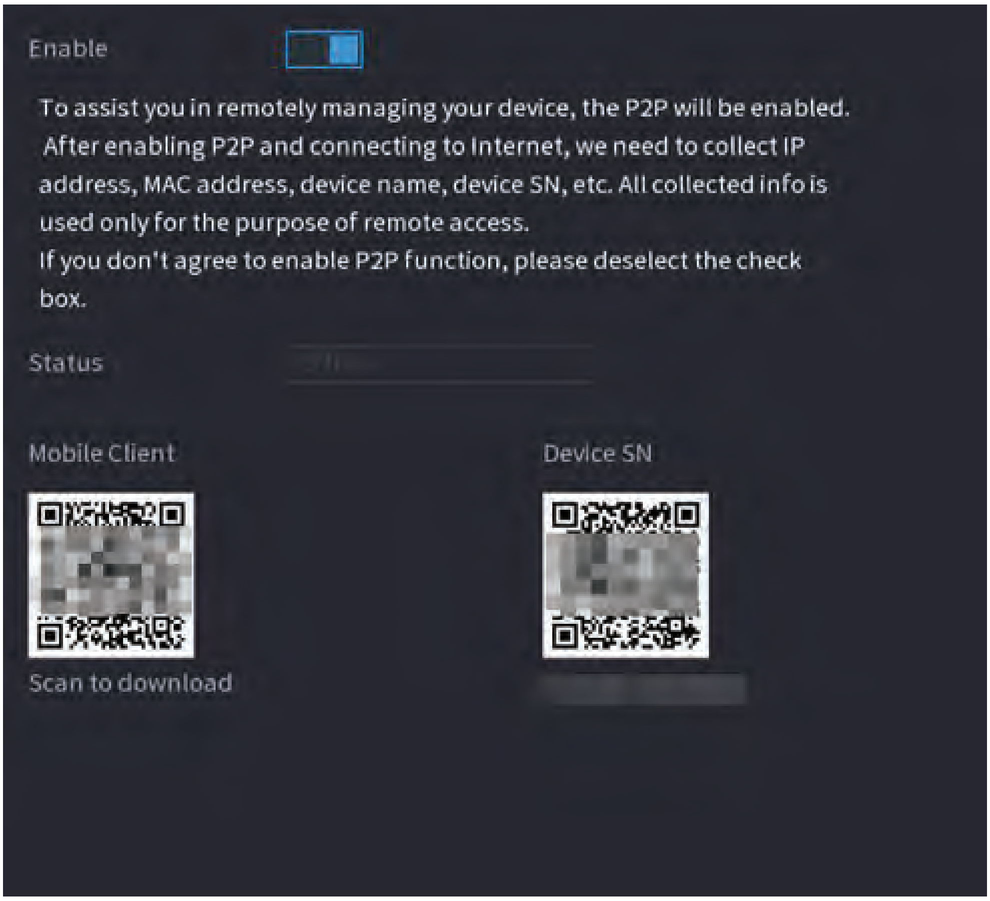
PoE operation	Description
Connect to PoE port	When an IPC is connected to the PoE port, the system automatically assigns the IP address to the IPC according to the set IP segment. The NVR will try the method of arp ping to assign the IP address. If DHCP is enabled on the NVR, the NVR will use DHCP to 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



Enable

To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access.
If you don't agree to enable P2P function, please deselect the check box.

Status

Mobile Client

Scan to download

Device SN

[redacted]

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

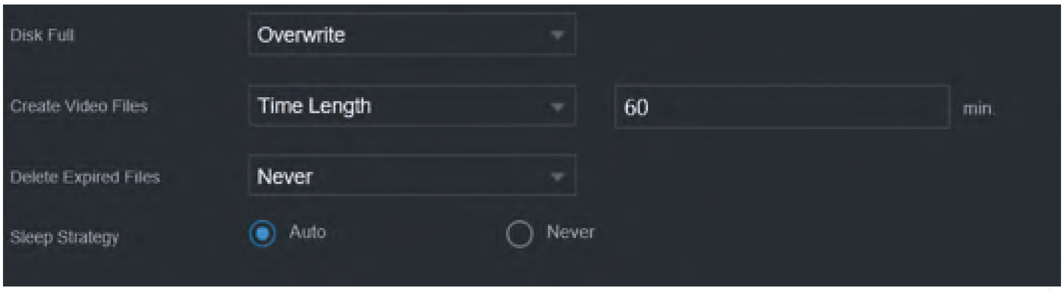
Background Information

You can set basic storage parameters.

Procedure

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

Figure 5-201 Basic storage



Disk Full: Overwrite

Create Video Files: Time Length, 60 min

Delete Expired Files: Never

Sleep Strategy: ● Auto ○ Never

Step 2 Set parameters.

Table 5-64 Basic storage parameters

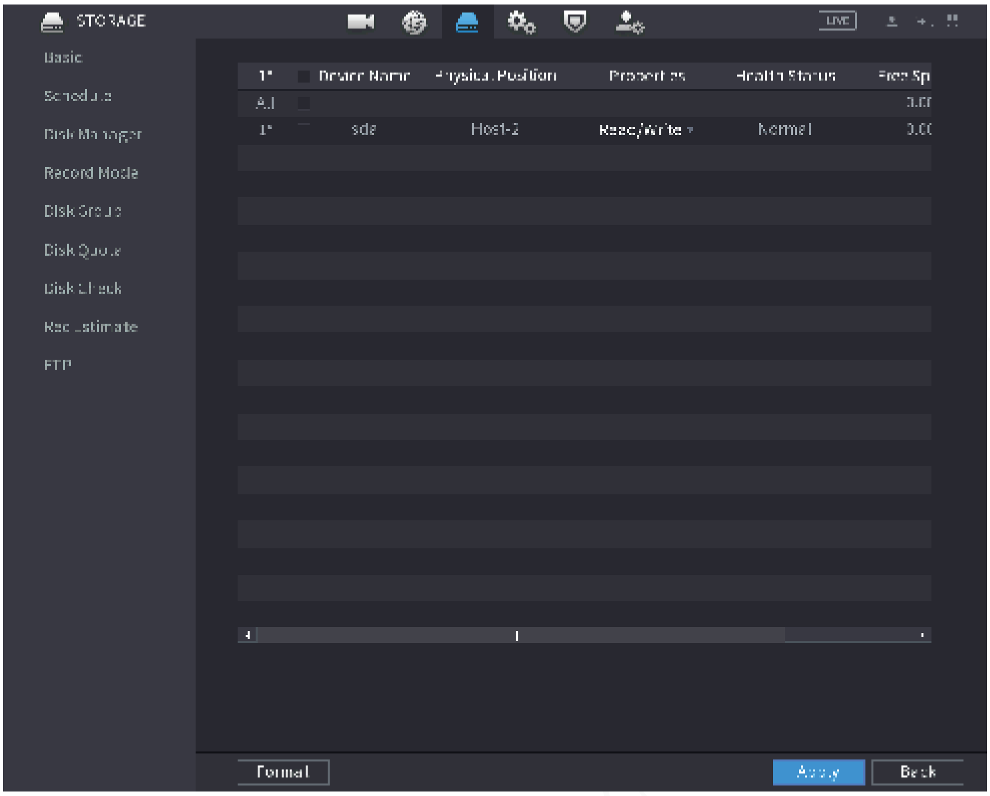
Parameter	Description
Disk Full	Configure the storage strategy to be used when no more storage space is available ● **Stop**: Stop recording ● **Overwrite**: The newest files overwrite the oldest ones.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired 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



1*	☐	Device Name	Physical Position	Properties	Health Status	Free Sp
All	☐					0.00
1*		sda	Host-2	Read/Write ▾	Normal	0.00

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.

⚠

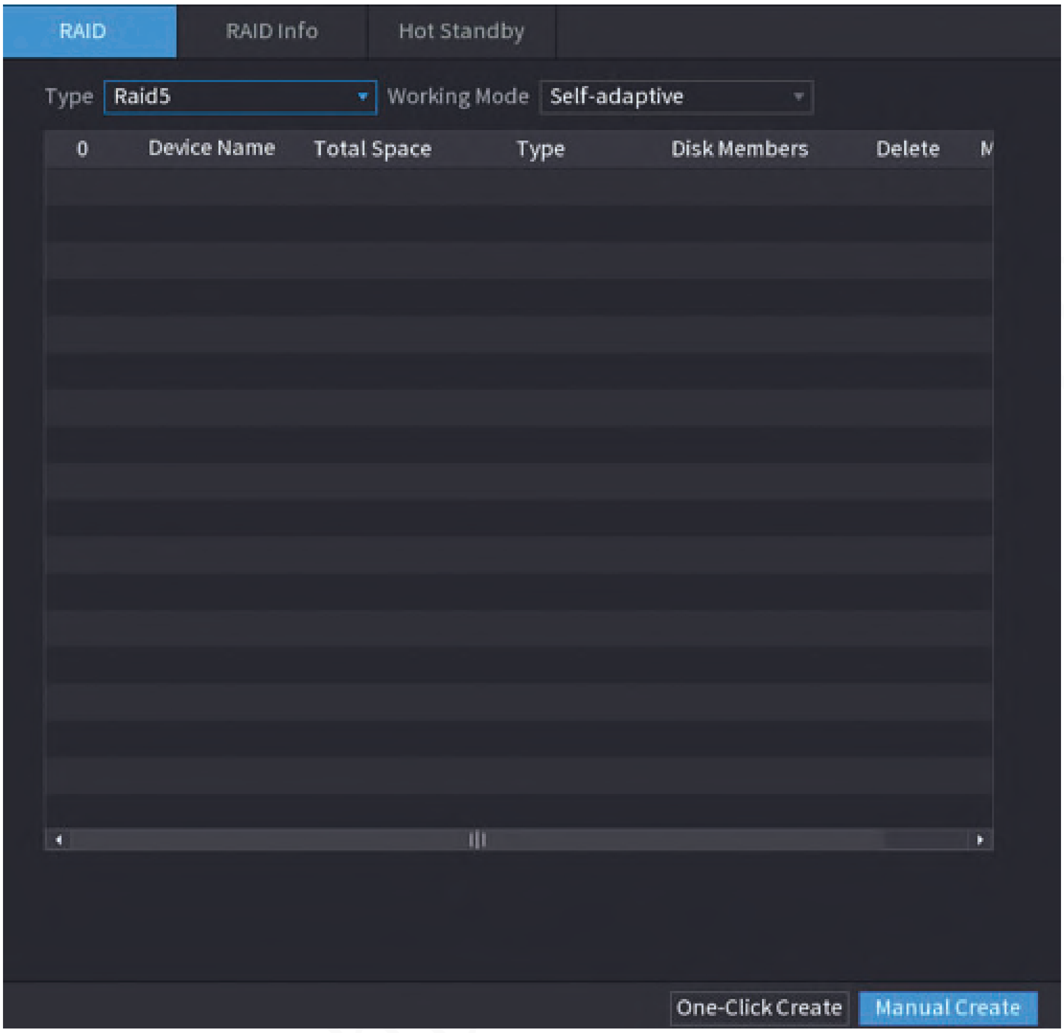
When you create RAID, the disks in the RAID group will be formatted. Back up data in time.

You can create different types of RAID as needed.

Procedure

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

Figure 5-203 RAID



Type Raid5 Working Mode Self-adaptive

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

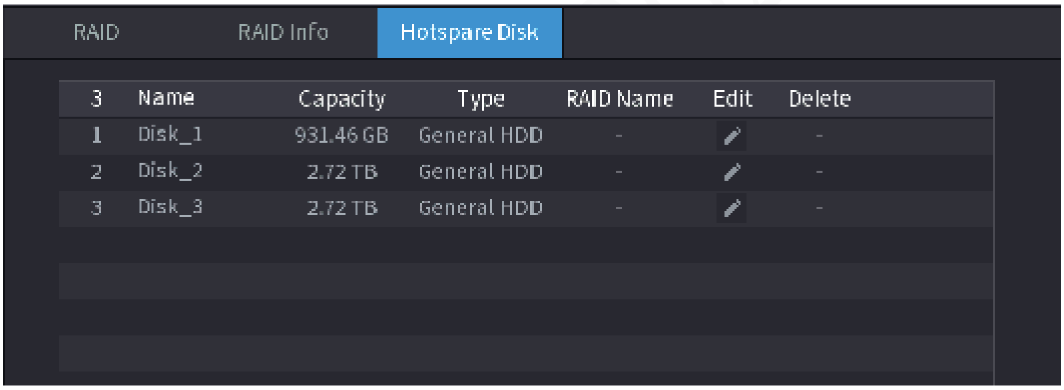
Select **Main Menu** > **STORAGE** > **RAID** > **RAID Info**. You can view the RAID information, including type, disk space, hot spare, and status.

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**.

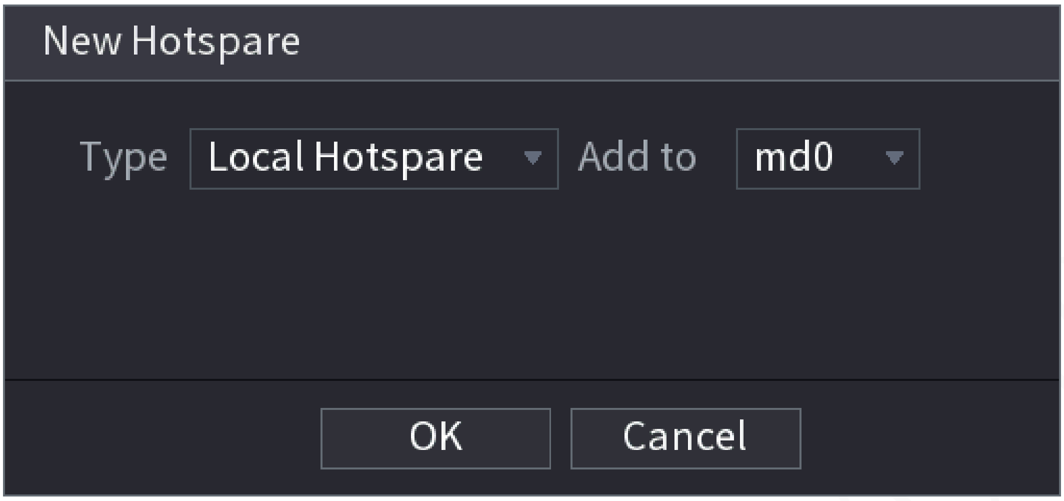
Figure 5-204 Hotspare disk



3	Name	Capacity	Type	RAID Name	Edit	Delete
1	Disk_1	931.46 GB	General HDD	-	✎	-
2	Disk_2	2.72 TB	General HDD	-	✎	-
3	Disk_3	2.72 TB	General HDD	-	✎	-

Step 2 Click ✎.

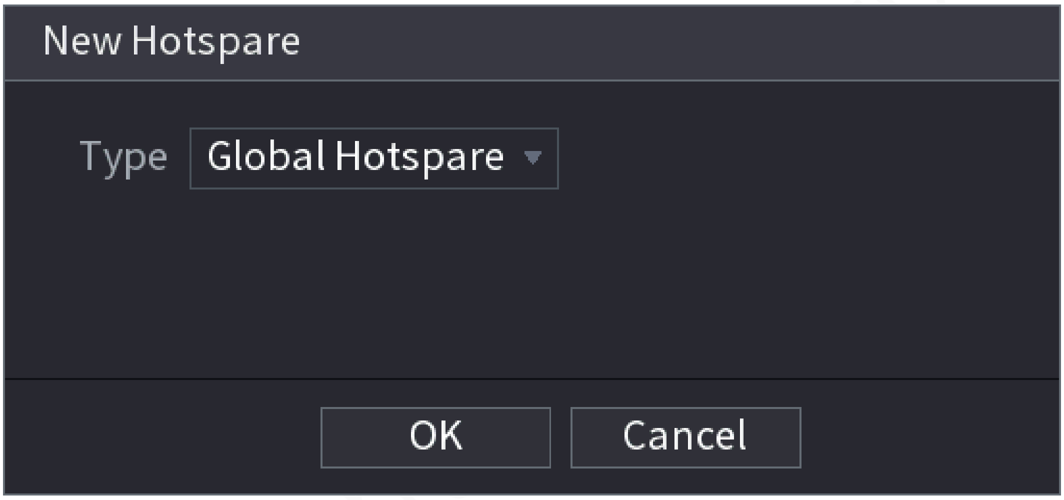
Figure 5-205 Local hotspare



New Hotspare

Type: Local Hotspare ▾ Add to: md0 ▾

Figure 5-206 Global hotspare



New Hotspare

Type: 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**.

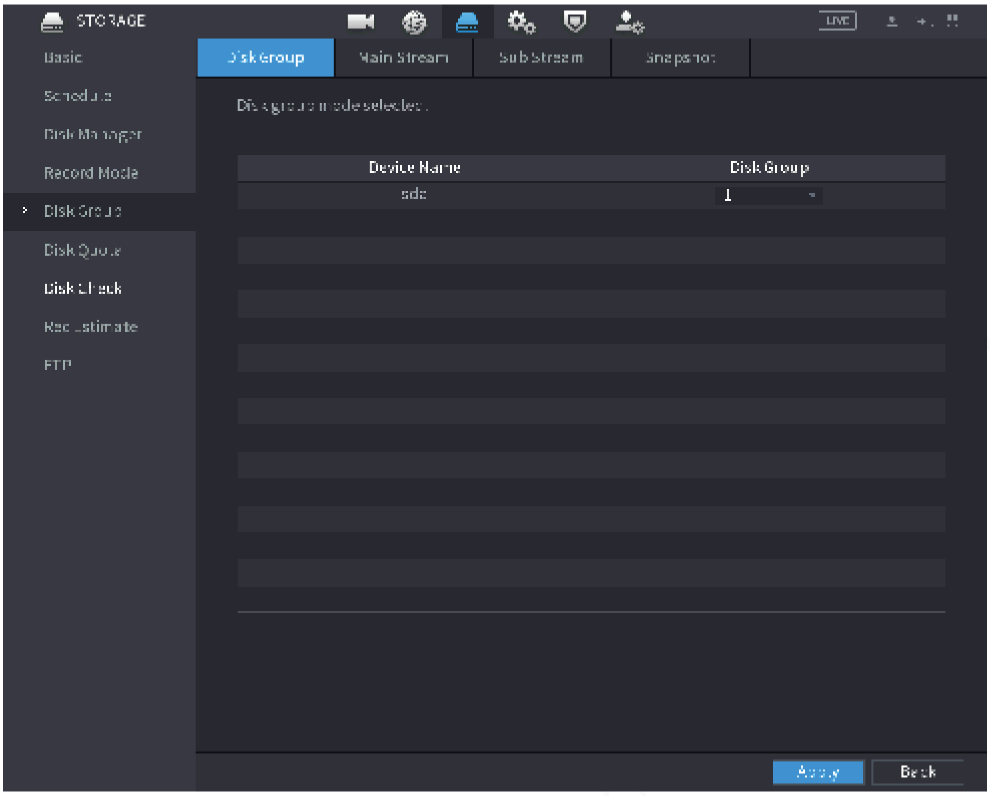
Click ▣ to delete a hot spare disk.

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



Disk group mode selected.

Device Name	Disk Group
sdc	1

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

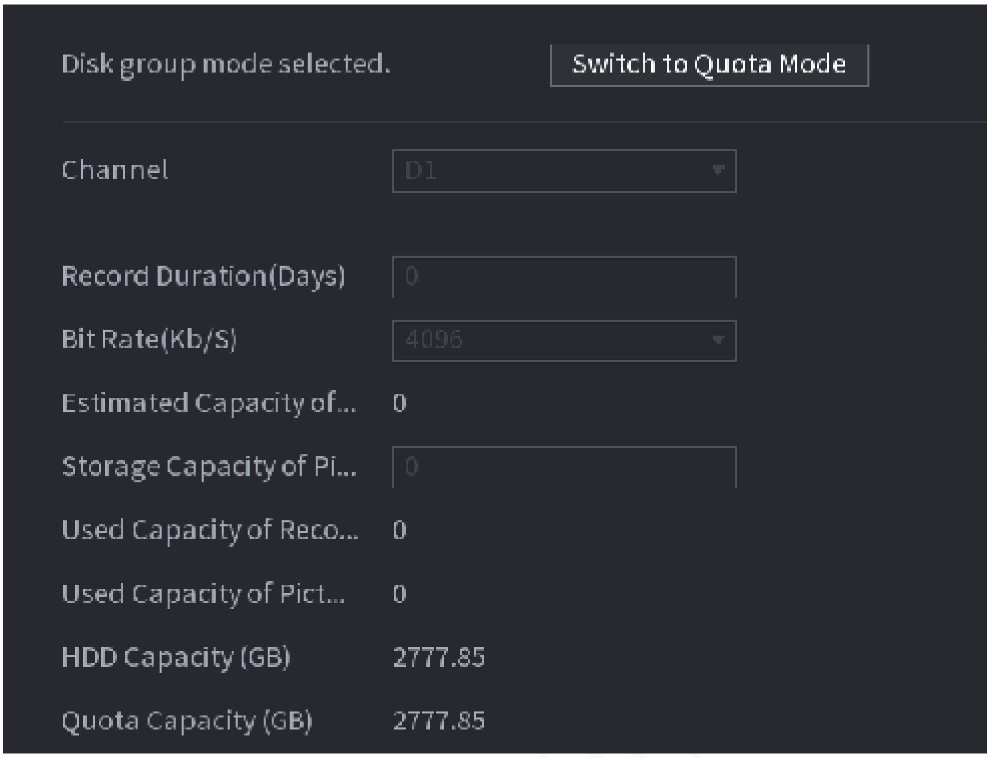
You can allocate a certain storage capacity for each channel to manage the storage space properly.

- 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



Disk group mode selected. Switch to Quota Mode

Channel	D1
Record Duration(Days)	0
Bit Rate(Kb/S)	4096
Estimated Capacity of...	0
Storage Capacity of Pi...	0
Used Capacity of Reco...	0
Used Capacity of Pict...	0
HDD Capacity (GB)	2777.85
Quota Capacity (GB)	2777.85

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**.

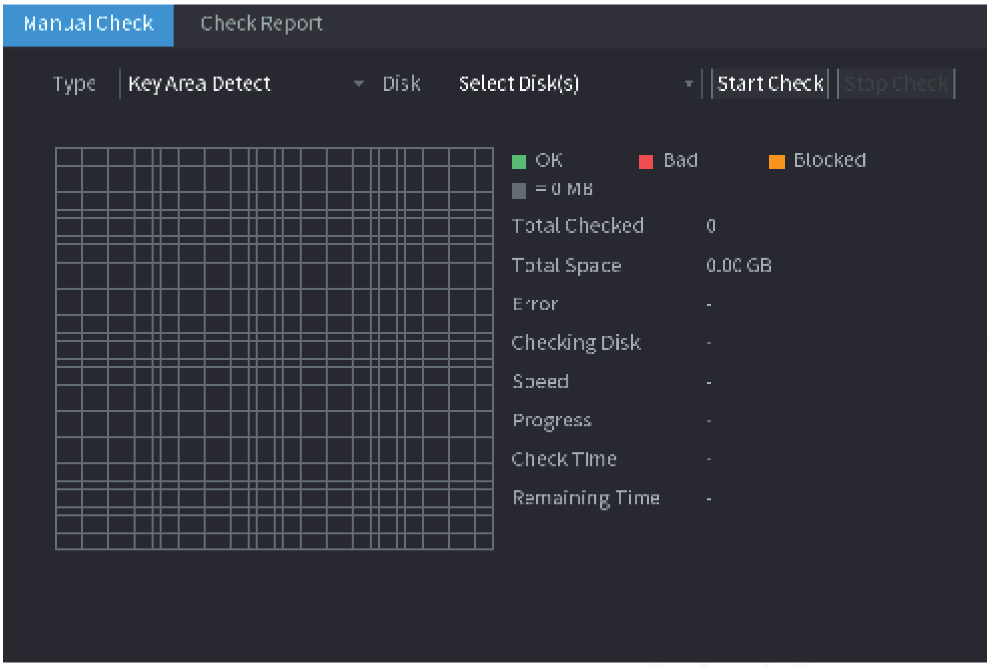
5.12.6 Disk Check

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



Type: Key Area Detect

Disk: Select Disk(s)

Total Checked	0
Total Space	0.00 GB
Error	-
Checking Disk	-
Speed	-
Progress	-
Check Time	-
Remaining Time	-

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

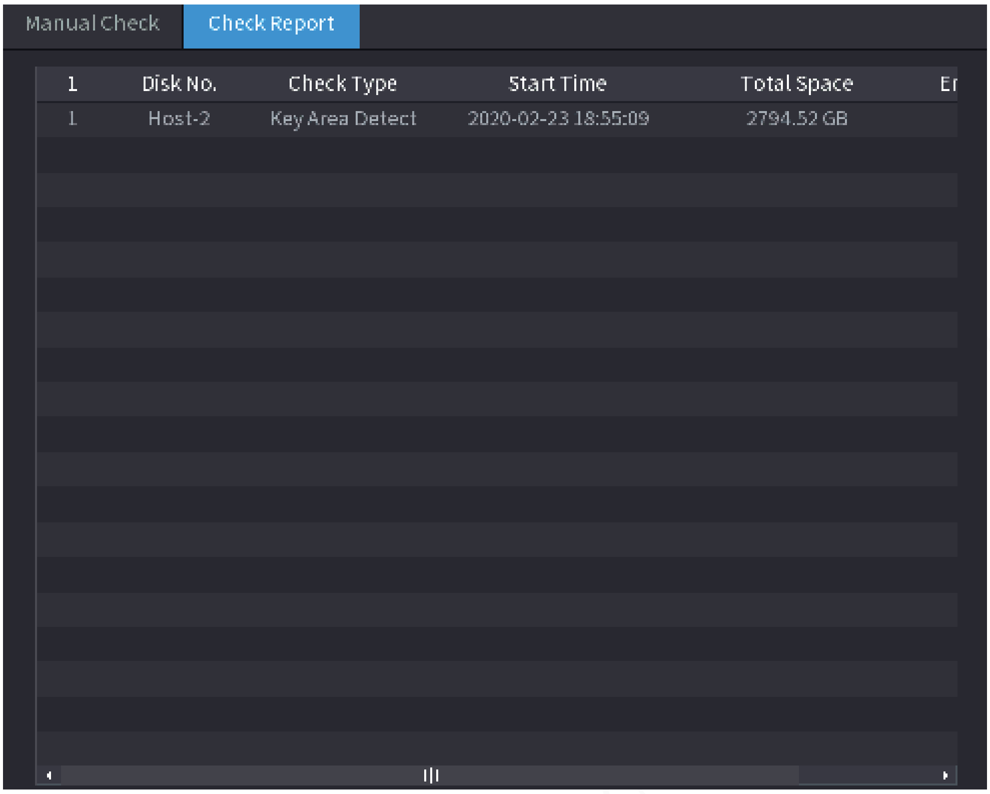
Background Information

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

Procedure

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

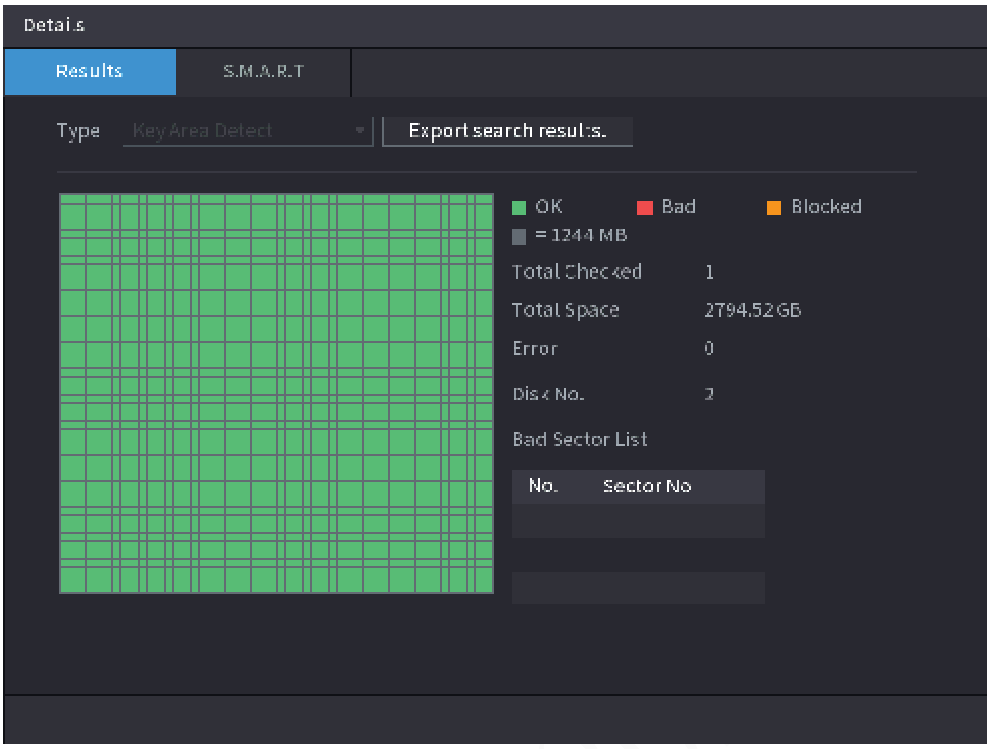
Figure 5-210 Check report



1	Disk No.	Check Type	Start Time	Total Space	Er
1	Host-2	Key Area Detect	2020-02-23 18:55:09	2794.52 GB	

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

Figure 5-211 Results



Details

Results | S.M.A.R.T

Type: Key Area Detect

Export search results.

🟩 OK 🟥 Bad 🟧 Blocked

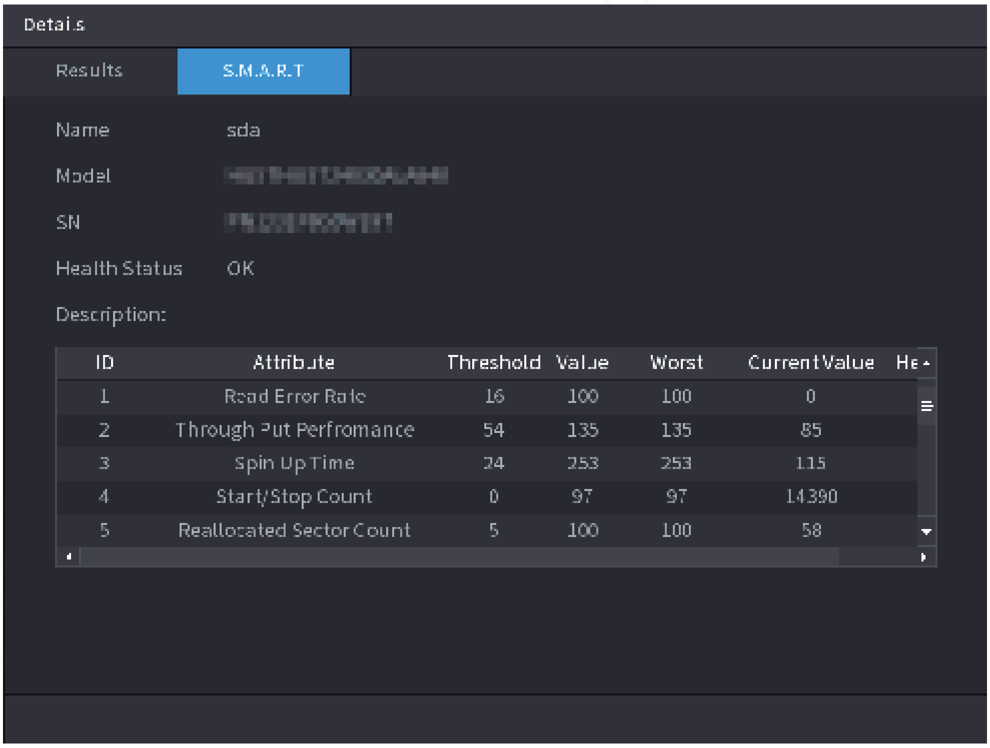
▪ = 1244 MB

Total Checked	1
Total Space	2794.52GB
Error	0
Disk No.	2

Bad Sector List

No.	Sector No

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



Details

Results | S.M.A.R.T

Name	sda
Model	[redacted]
SN	[redacted]
Health Status	OK

Description:

ID	Attribute	Threshold	Value	Worst	Current Value	He
1	Read Error Rate	16	100	100	0	
2	Through Put Perfromance	54	135	135	85	
3	Spin Up Time	24	253	253	115	
4	Start/Stop Count	0	97	97	14390	
5	Reallocated Sector Count	5	100	100	58	

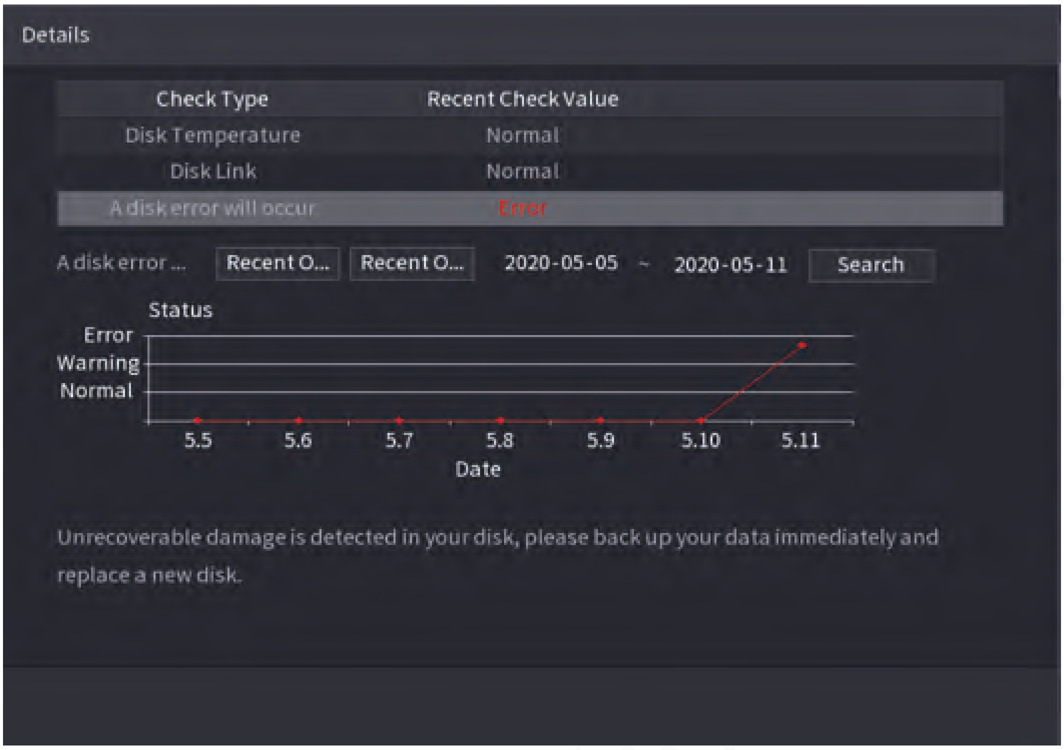
5.12.6.3 Disk Health Monitoring

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



Details

Check Type	Recent Check Value
Disk Temperature	Normal
Disk Link	Normal
A disk error will occur	Error

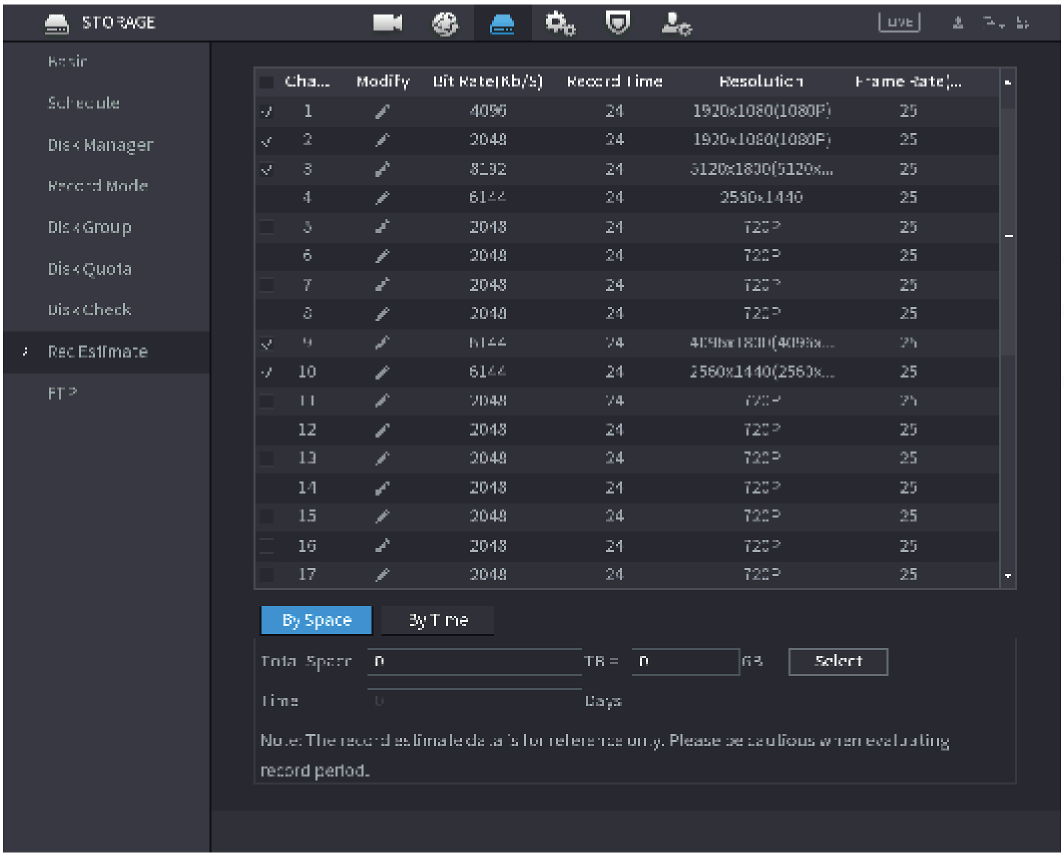
Unrecoverable damage is detected in your disk, please back up your data immediately and replace a new disk.

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



☐	Cha...	Modify	Bit Rate(Kb/S)	Record Time	Resolution	Frame Rate(...
☑	1	✎	4096	24	1920x1080(1080P)	25
☑	2	✎	2048	24	1920x1080(1080P)	25
☑	3	✎	8192	24	5120x1800(5120x...	25
☐	4	✎	6144	24	2560x1440	25
☐	5	✎	2048	24	720P	25
☐	6	✎	2048	24	720P	25
☐	7	✎	2048	24	720P	25
☐	8	✎	2048	24	720P	25
☑	9	✎	6144	24	4096x1800(4096x...	25
☑	10	✎	6144	24	2560x1440(2560x...	25
☐	11	✎	2048	24	720P	25
☐	12	✎	2048	24	720P	25
☐	13	✎	2048	24	720P	25
☐	14	✎	2048	24	720P	25
☐	15	✎	2048	24	720P	25
☐	16	✎	2048	24	720P	25
☐	17	✎	2048	24	720P	25

By Space | By Time

Total Space 0 TB = 0 GB Select

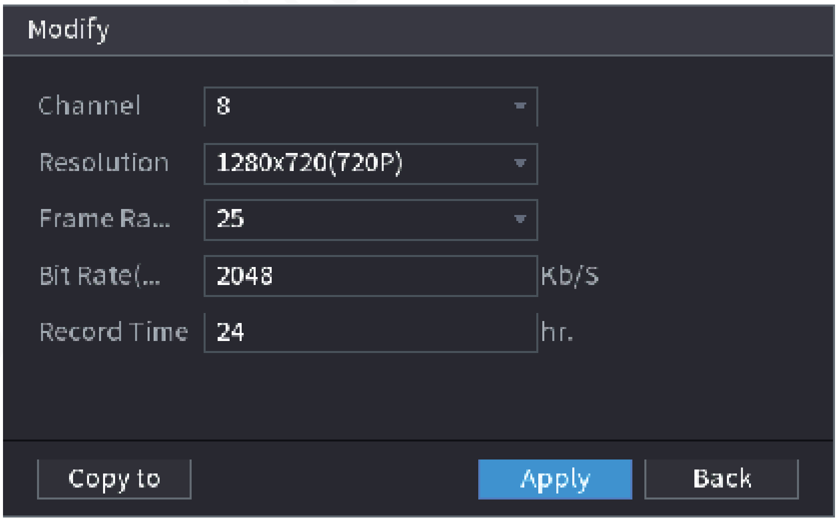
Time 0 Days

Note: The record estimate data is for reference only. Please be cautious when evaluating record period.

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



Modify

Channel: 8

Resolution: 1280x720(720P)

Frame Ra...: 25

Bit Rate(...: 2048 Kb/S

Record Time: 24 hr.

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.

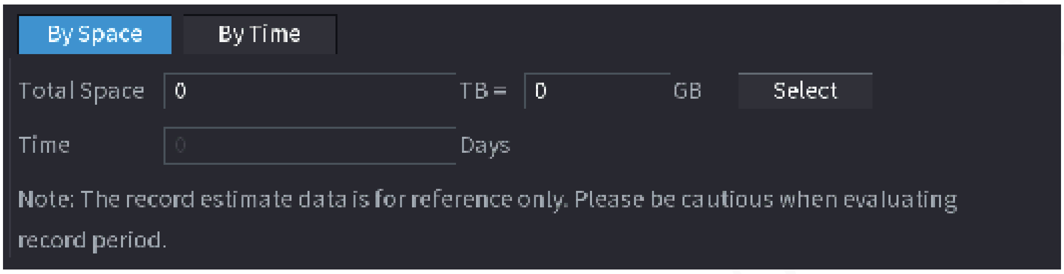
Click **Copy to** to copy the settings to other channels.

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



Total Space 0 TB = 0 GB

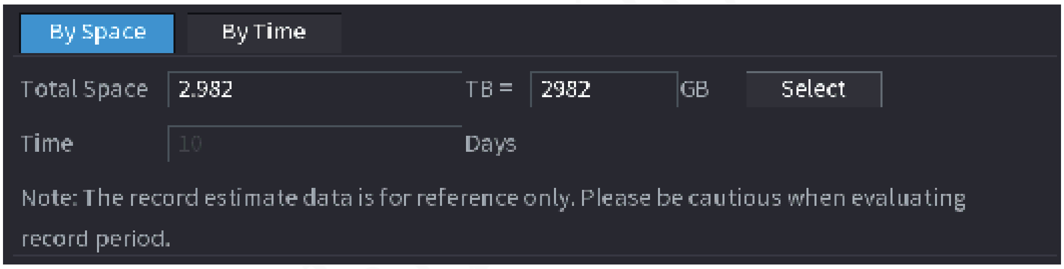
Time 0 Days

Note: The record estimate data is for reference only. Please be cautious when evaluating record period.

Step 2 Click **Select**.

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

Figure 5-217 Recording time



Total Space 2.982 TB = 2982 GB

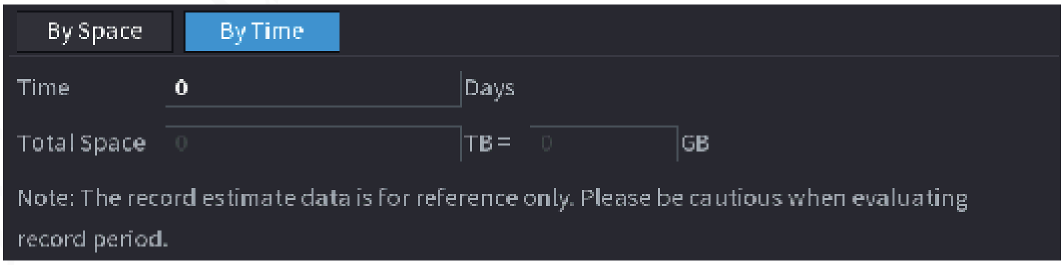
Time 10 Days

Note: The record estimate data is for reference only. Please be cautious when evaluating record period.

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



Time 0 Days

Total Space 0 TB = 0 GB

Note: The record estimate data is for reference only. Please be cautious when evaluating record period.

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

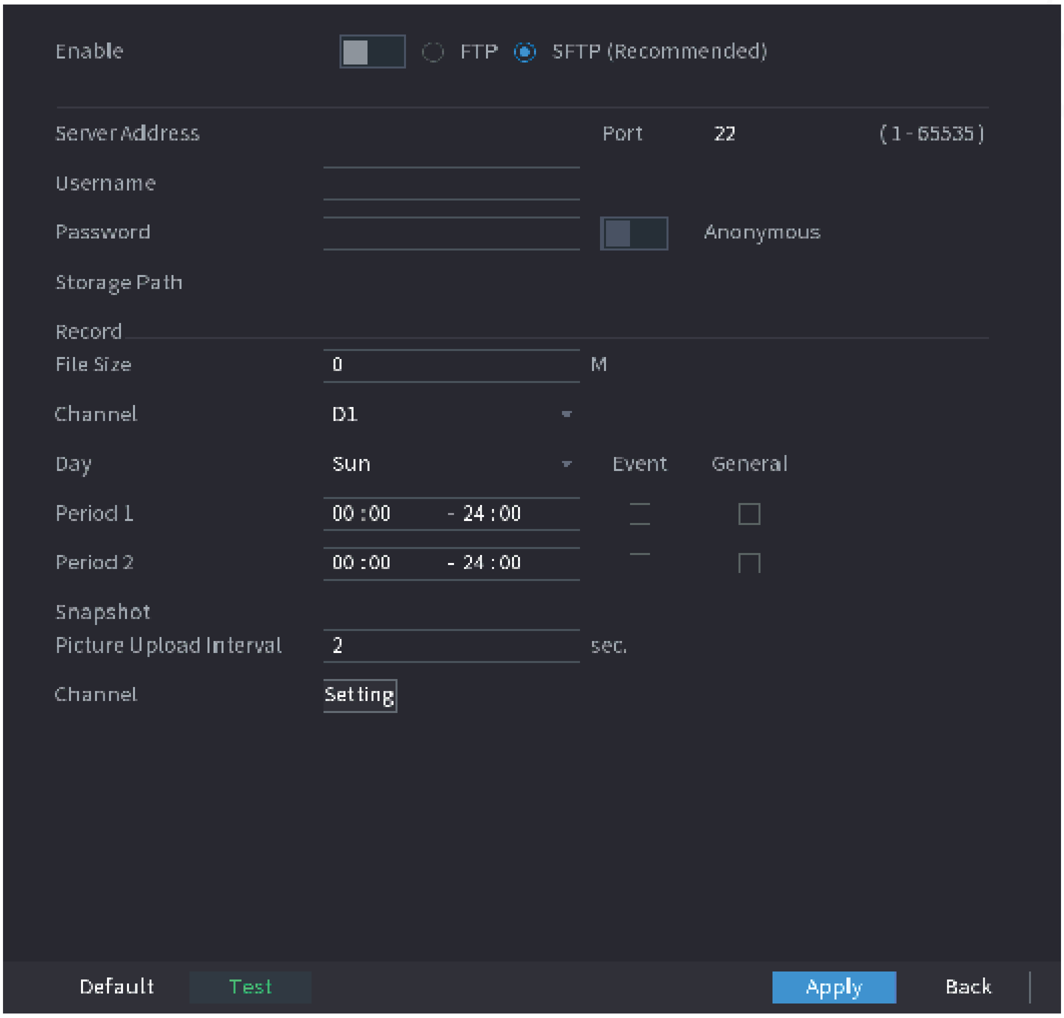
Purchase or download a FTP (File Transfer Protocol) server and install it on your PC.

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



Enable ○ FTP ● SFTP (Recommended)

Server Address Port 22 (1 - 65535)

Username

Password Anonymous

Storage Path

Record

File Size 0 M

Channel D1

Day Sun Event General

Period 1 00 :00 - 24 :00 □

Period 2 00 :00 - 24 :00 □

Snapshot

Picture Upload Interval 2 sec.

Channel Setting

Step 2 Configure the parameters.

Table 5-66 FTP parameters

Parameter	Description
Enable	Enable the FTP upload function.
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.

Parameter	Description
Password	If you enable the anonymity function, you can log in anonymously without entering the username and 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**.

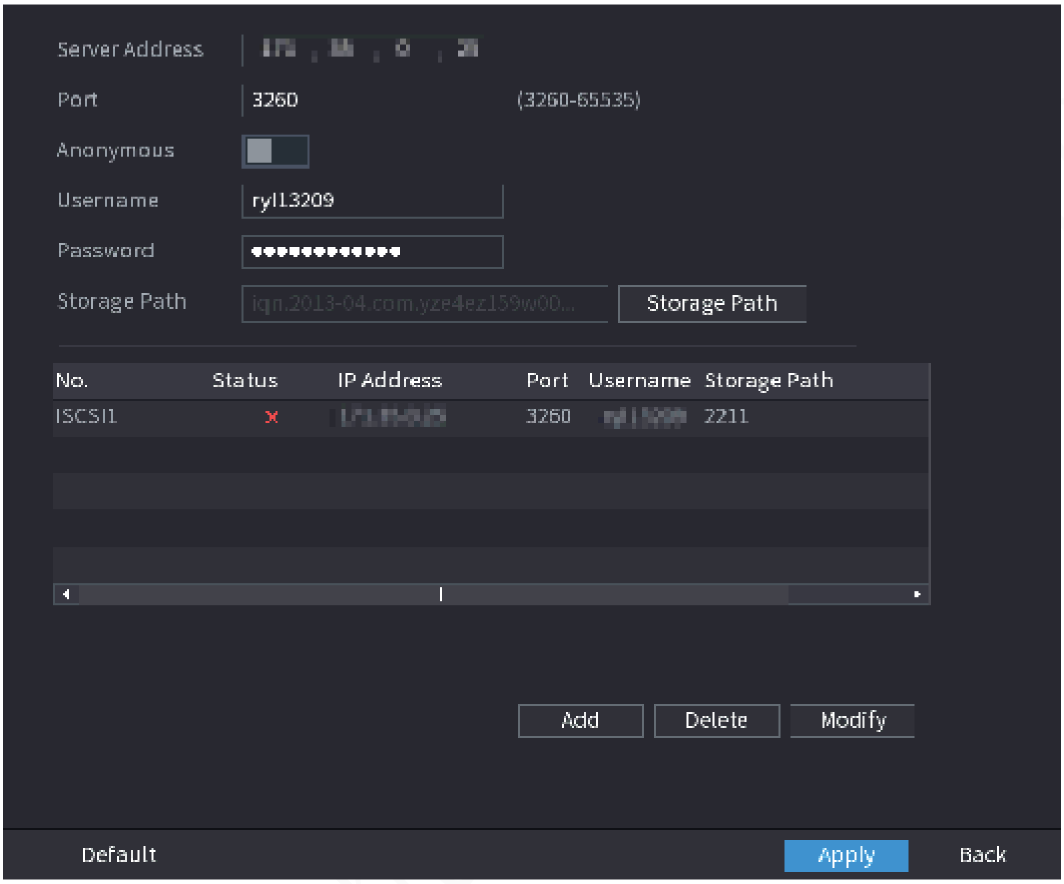
5.12.9 iSCSI

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



Server Address [redacted]

Port 3260 (3260-65535)

Anonymous

Username ryl13209

Password ●●●●●●●●●●●●●

Storage Path iqn.2013-04.com.yze4ez159w00...

No.	Status	IP Address	Port	Username	Storage Path
ISCSI1	×	[redacted]	3260	[redacted]	2211

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.

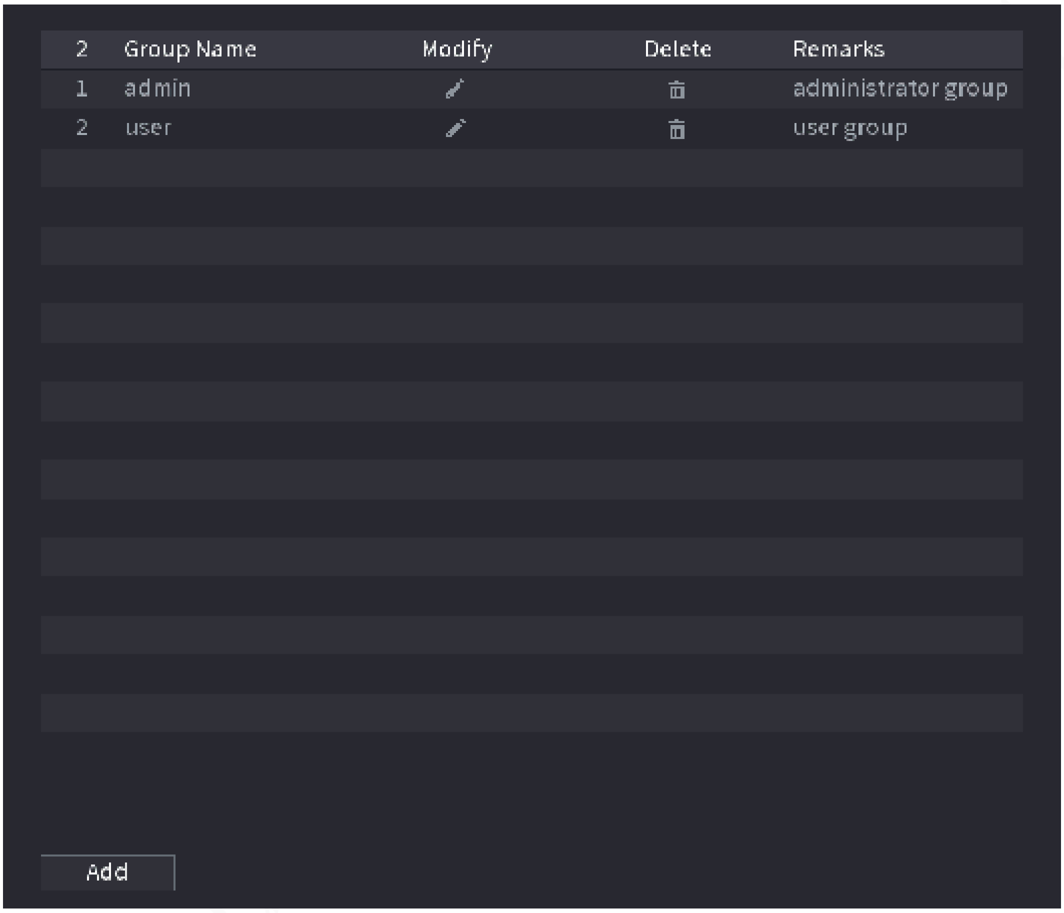
5.13.1 Group

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

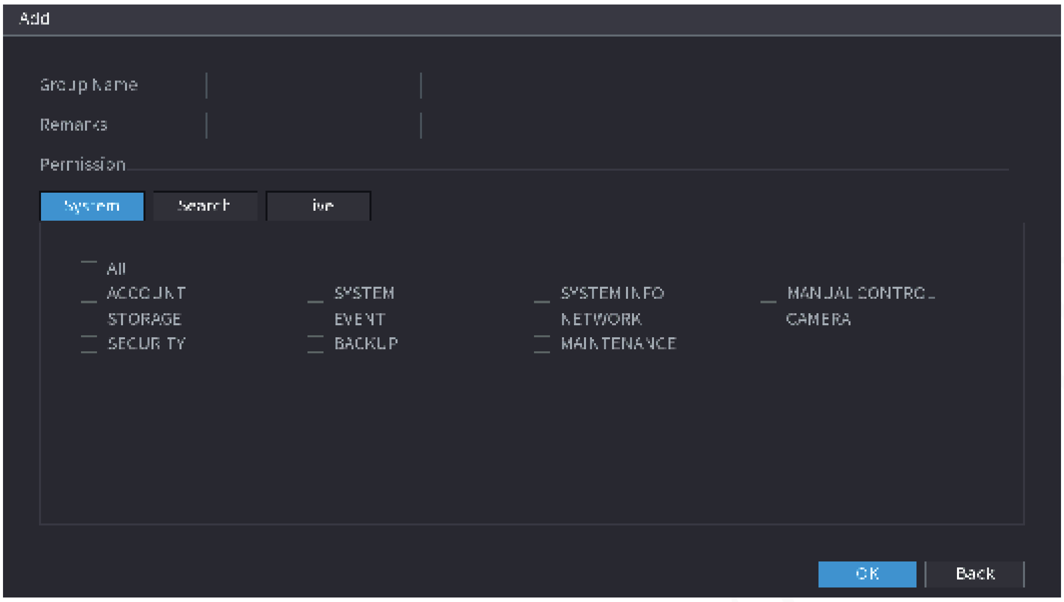


2	Group Name	Modify	Delete	Remarks
1	admin	✎	🗑	administrator group
2	user	✎	🗑	user group

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.

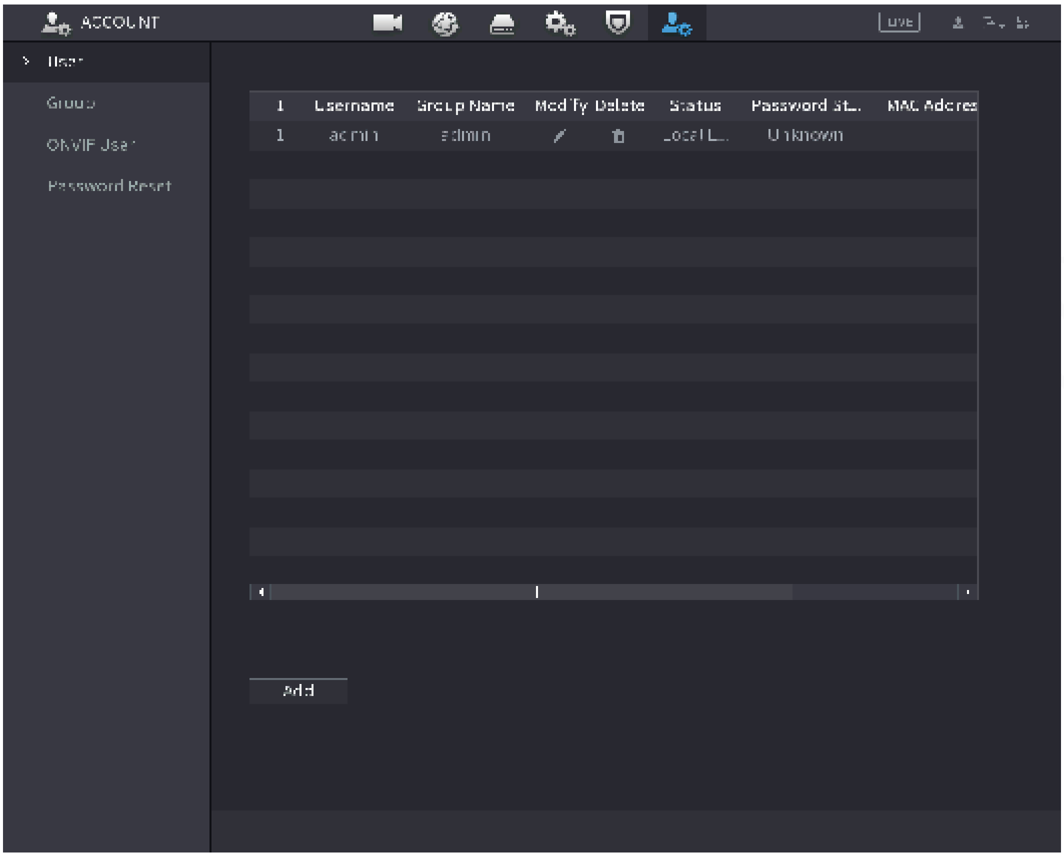
5.13.2 User

5.13.2.1 Adding User

Procedure

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

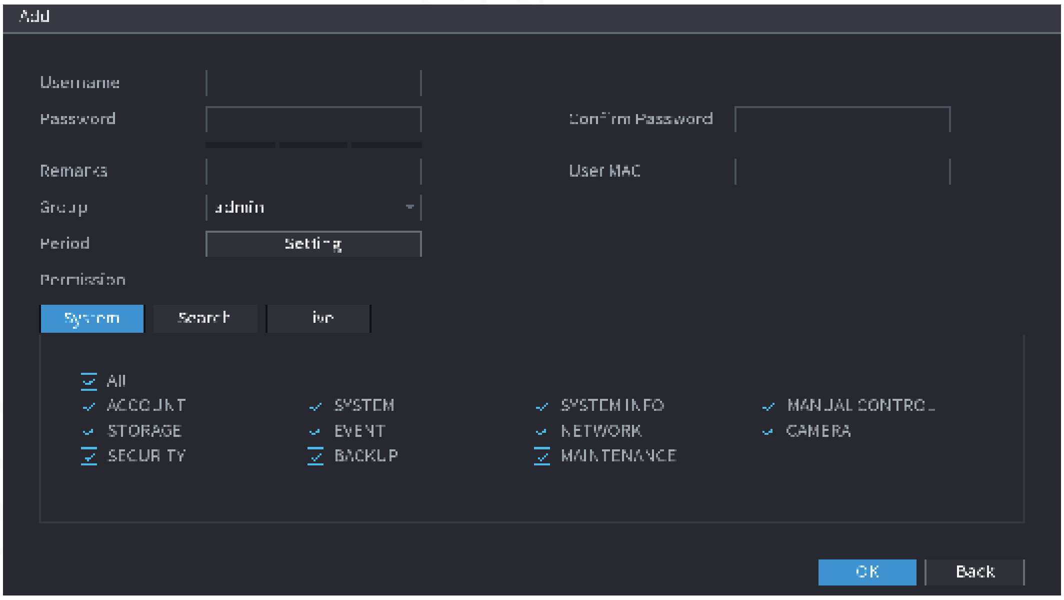
Figure 5-223 User



1	Username	Group Name	Modify	Delete	Status	Password St...	MAC Addres
1	admin	admin	✎	🗑	Local L...	Unknown	

Step 2 Click **Add**.

Figure 5-224 Add user



Group: admin

☑ All
☑ ACCOUNT ☑ SYSTEM ☑ SYSTEM INFO ☑ MANUAL CONTROL
☑ STORAGE ☑ EVENT ☑ NETWORK ☑ CAMERA
☑ SECURITY ☑ BACKUP ☑ MAINTENANCE

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.

Parameter	Description
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.

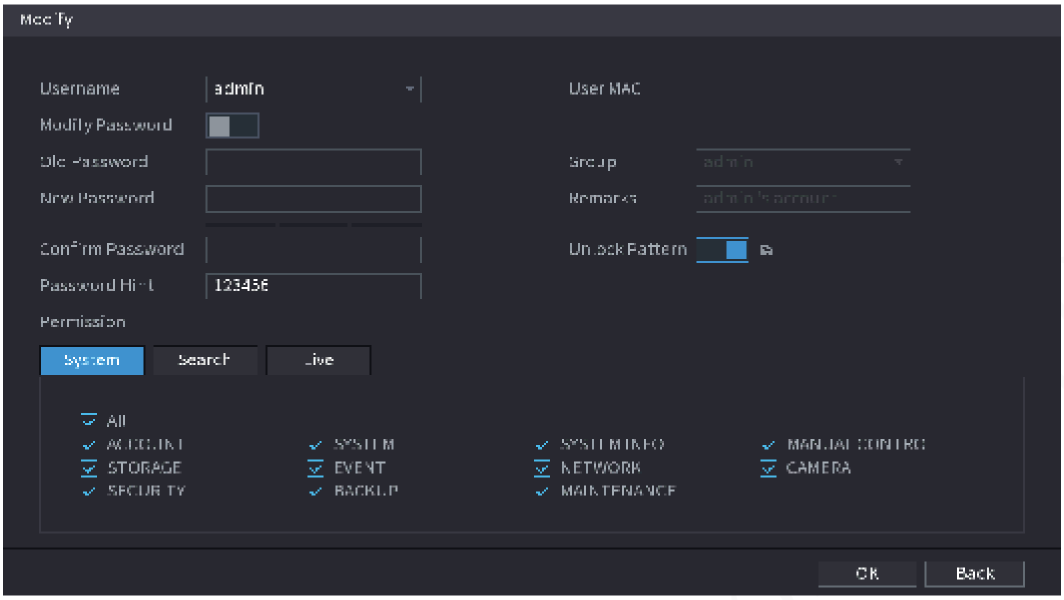
Users with account permissions can change the password of other users.

Procedure

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

Step 2 Click ✎ of the corresponding user.

Figure 5-225 Change password



Modify

Username: admin

Modify Password: ☐

Old Password:

New Password:

Confirm Password:

Password Hint: 123456

User MAC

Group: admin

Remarks: admin 's account

Unlock Pattern: ☑

Permission

System | Search | Live

☑ All

✓ ACCOUNT	✓ SYSTEM	✓ SYSTEM INFO	✓ MANUAL CONTROL
☑ STORAGE	☑ EVENT	☑ NETWORK	☑ CAMERA
✓ SECURITY	✓ BACKUP	✓ MAINTENANCE	

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 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 5-226 Pattern login

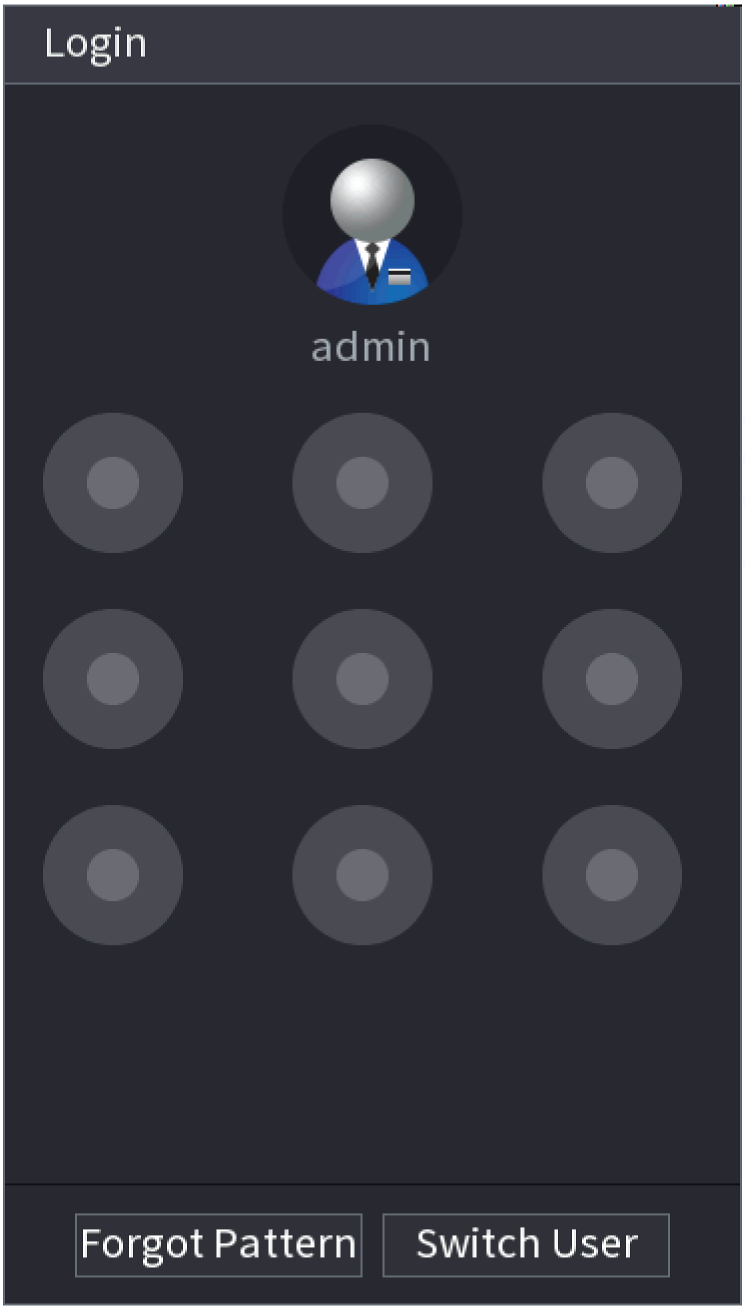
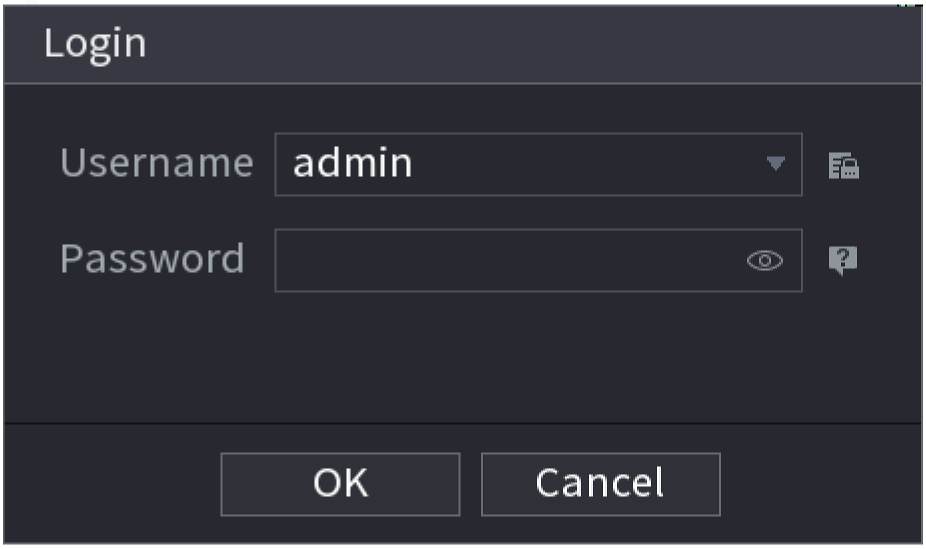


Figure 5-227 Password login



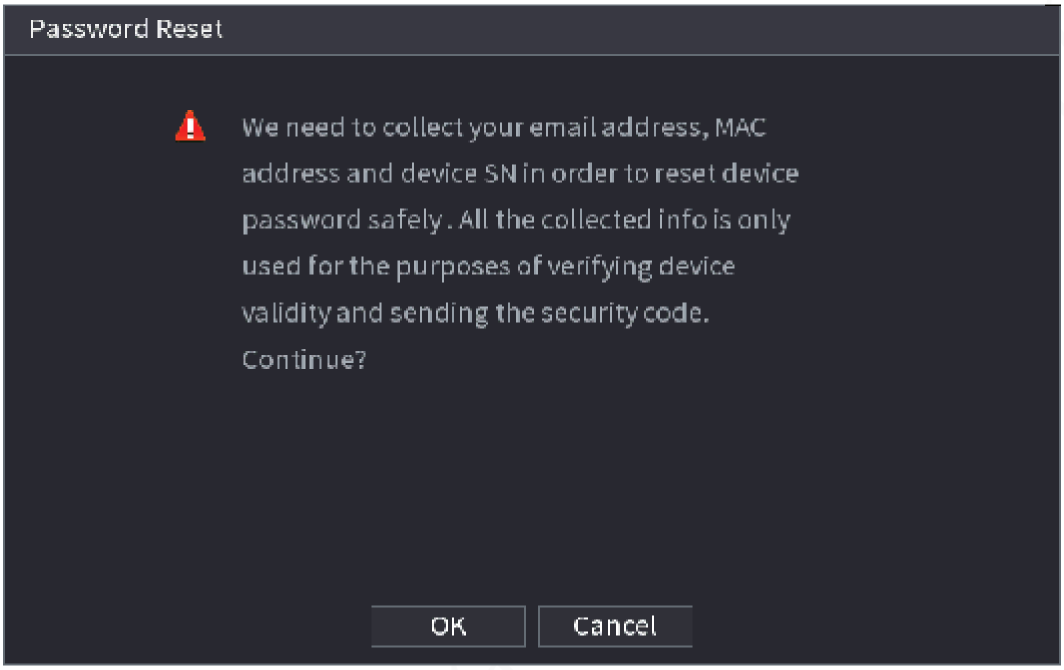
Username: admin

Password:

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 5-228 Notification on data colleciton



Password Reset

We need to collect your email address, MAC address and device SN in order to reset device password safely . All the collected info is only used for the purposes of verifying device validity and sending the security code. Continue?

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.

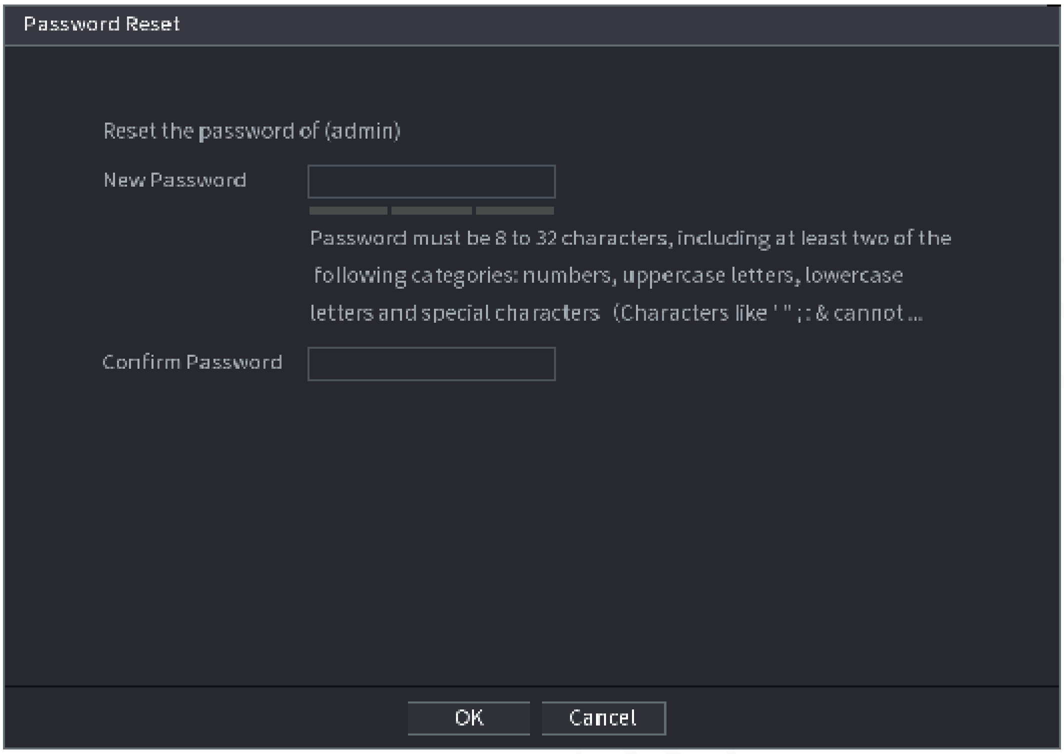
- Email.
  Select **Email** as the reset mode, and then follow the on-screen instructions to get the security code in your linked email address. After that, enter the security code in the **Security Code** box.
- Security question
  Select **Security Question** as reset mode and then answer the security 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 5-229 Enter new password



Password Reset

Reset the password of (admin)

New Password

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters （Characters like ' " ; : & cannot ...

Confirm 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

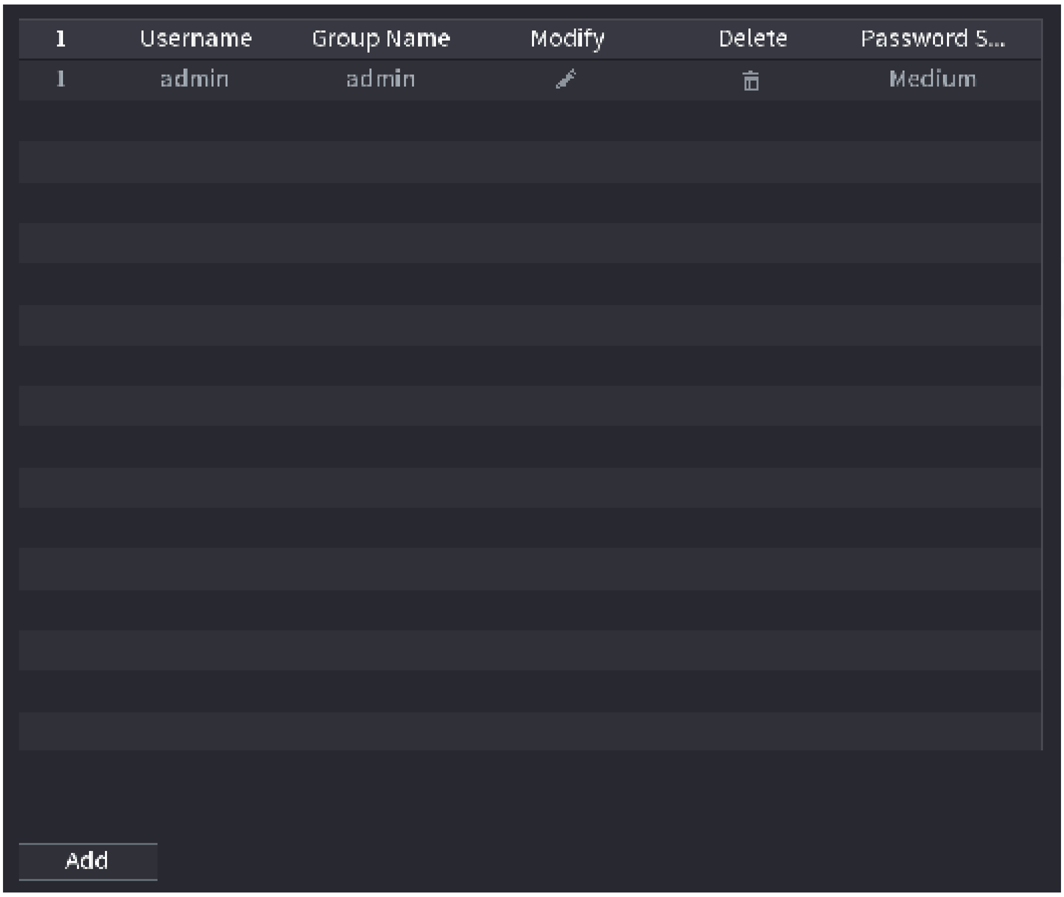
To connect the camera from the third party to the NVR via the ONVIF protocol, you need to use a verified ONVIF account.

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 5-230 ONVIF user

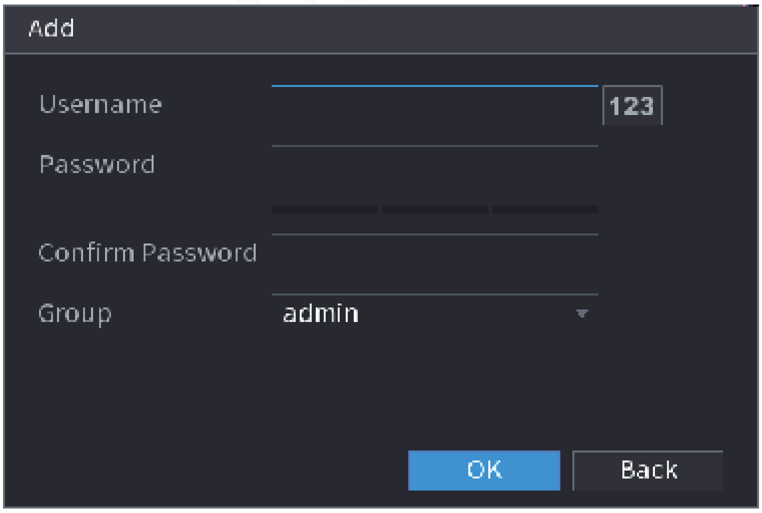


1	Username	Group Name	Modify	Delete	Password S...
1	admin	admin	✎	🗑	Medium

Add

Step 2 Click **Add**.

Figure 5-231 Add ONVIF user



Add

Username	123
Password	
Confirm Password	
Group	admin ▾

OK Back

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

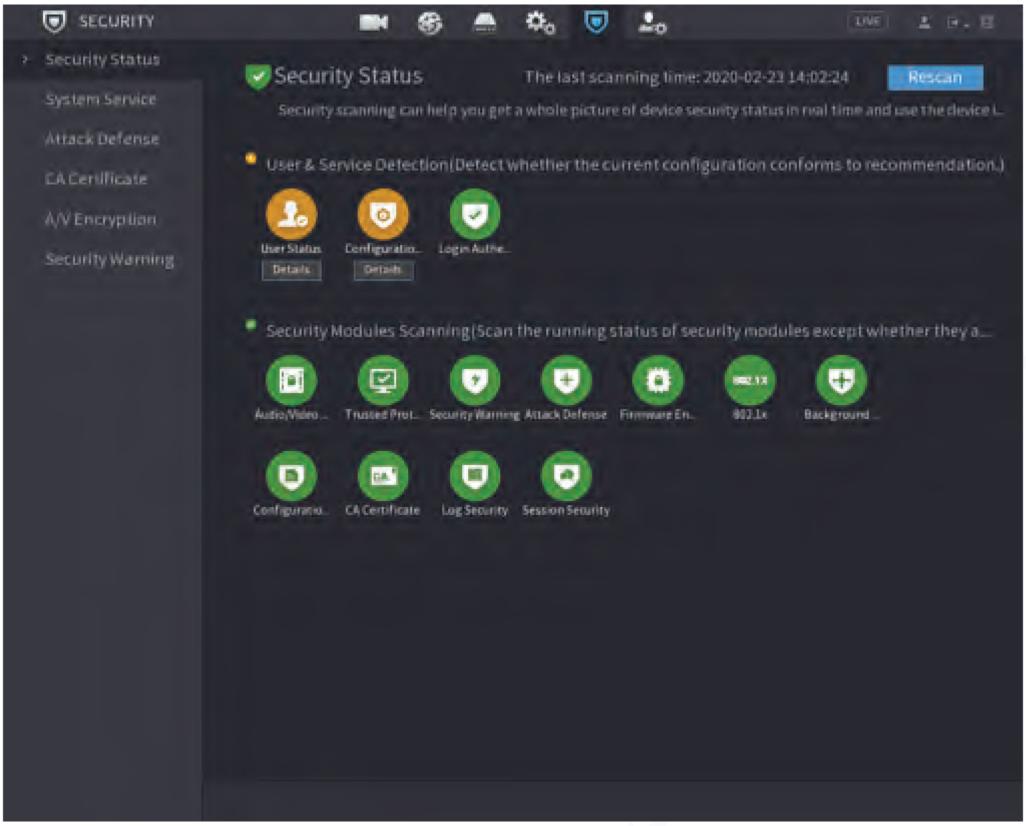
Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information on the security status of the device.

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 5-232 Security status



Security Status

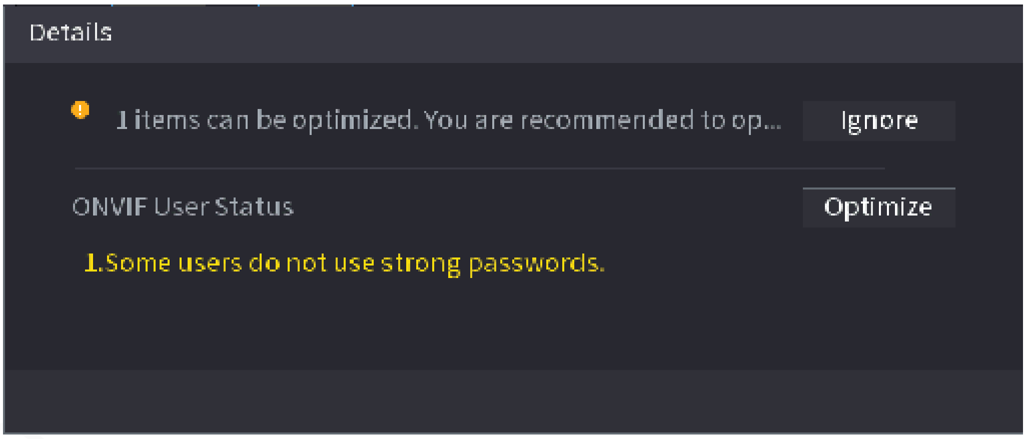
The last scanning time: 2020-02-23 14:02:24

Security scanning can help you get a whole picture of device security status in real time and use the device i...

User & Service Detection(Detect whether the current configuration conforms to recommendation.)

Security Modules Scanning(Scan the running status of security modules except whether they a...

Figure 5-233 Details (1)



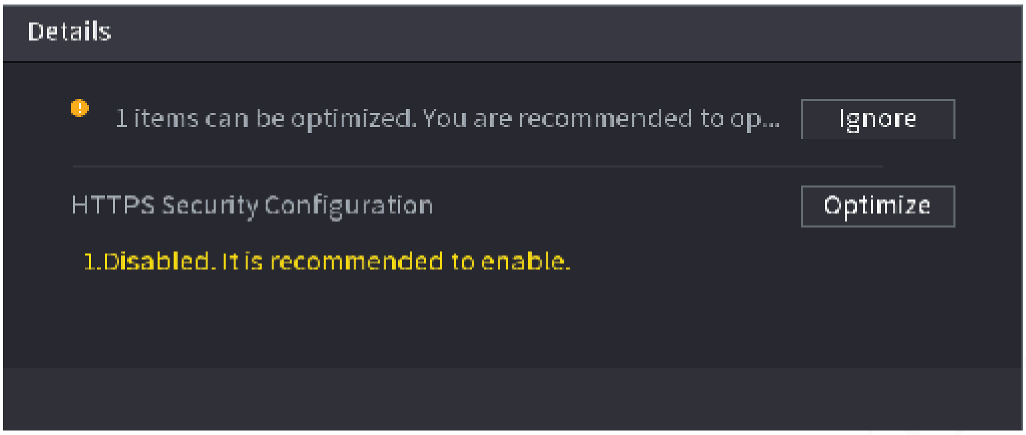
1 items can be optimized. You are recommended to op...

ONVIF User Status

1.Some users do not use strong passwords.

- 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 5-234 Details (2)



Details

1 items can be optimized. You are recommended to op...

HTTPS Security Configuration

1.Disabled. It is recommended to enable.

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

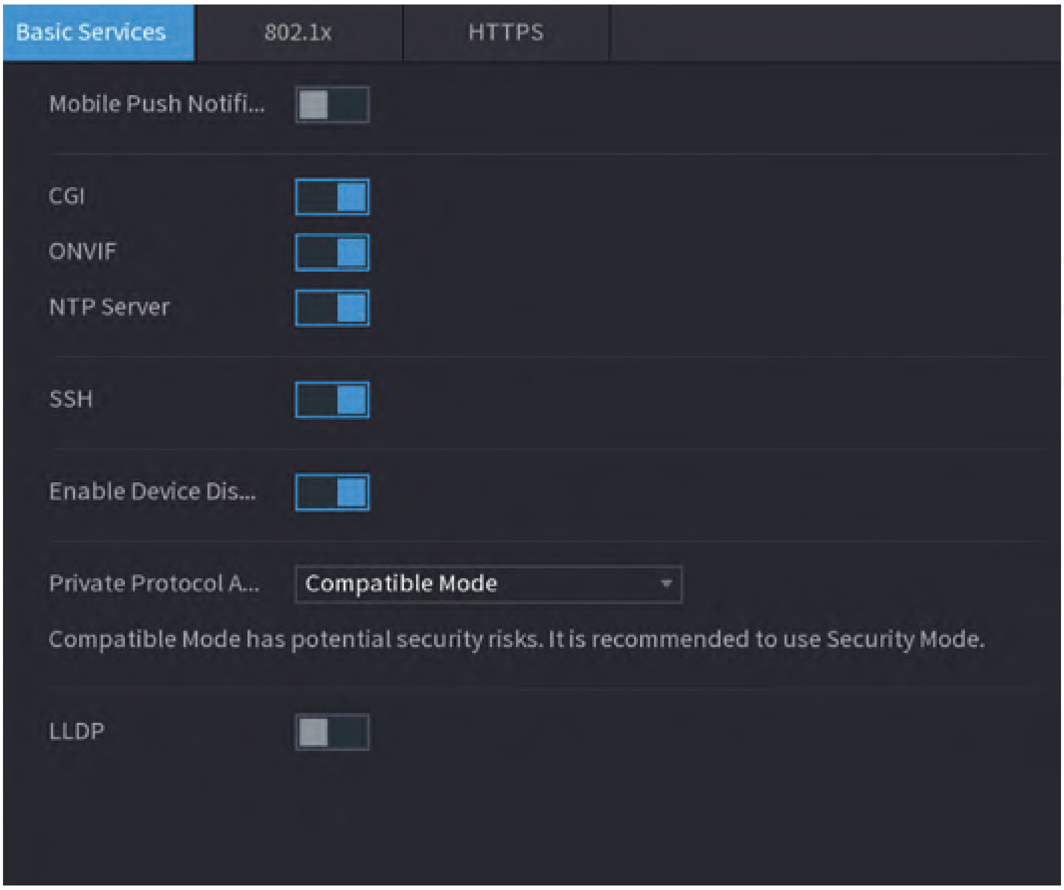
You can set NVR basic information such as basic services, 802.1x and HTTPS.

5.14.2.1 Basic Services

Procedure

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

Figure 5-235 Basic services



Mobile Push Notifi... ○
CGI ●
ONVIF ●
NTP Server ●
SSH ●
Enable Device Dis... ●
Private Protocol A... Compatible Mode
Compatible Mode has potential security risks. It is recommended to use Security Mode.
LLDP ○

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.
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.

Parameter	Description
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**.

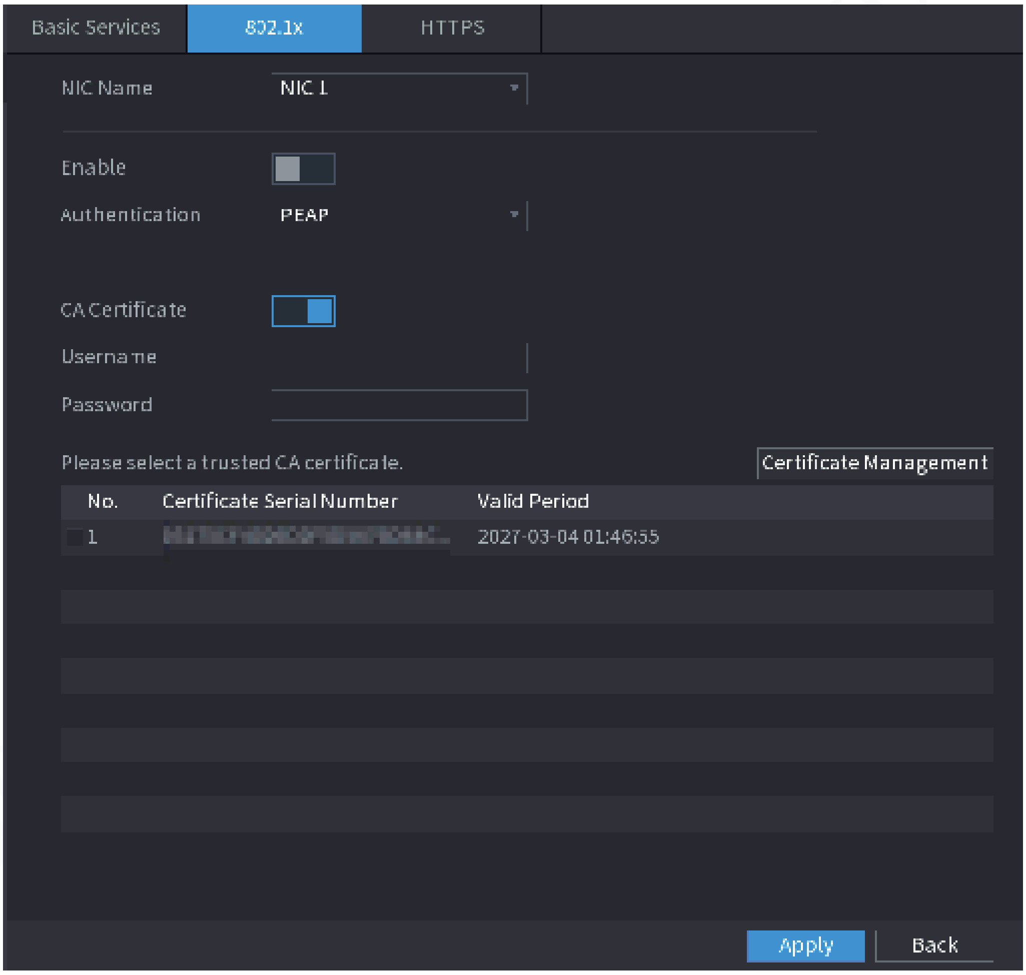
5.14.2.2 802.1x

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

Procedure

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

Figure 5-236 802.1x



NIC Name: NIC 1

Enable

Authentication: PEAP

CA Certificate

Username

Password

Please select a trusted CA certificate.

Certificate Management

No.	Certificate Serial Number	Valid Period
1	[redacted]	2027-03-04 01:46:55

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.

Parameter	Description
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

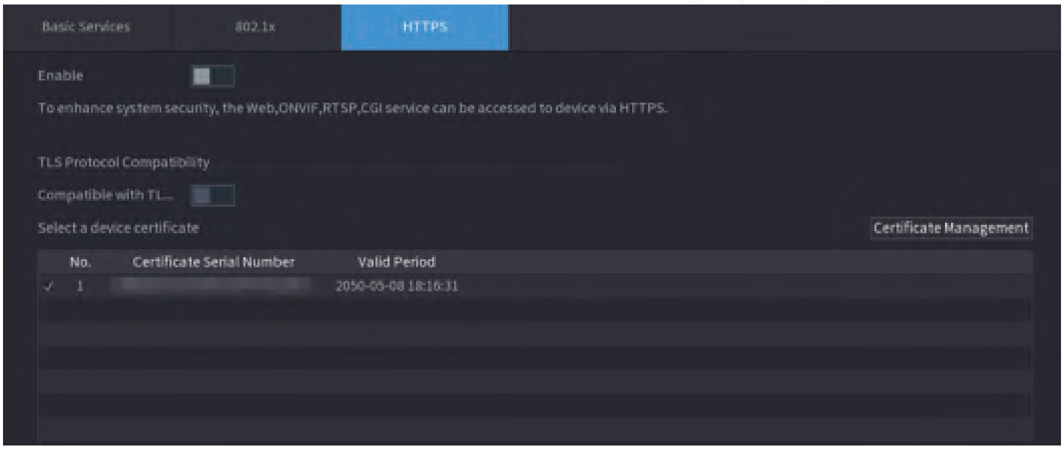
Background Information

We recommend you enable HTTPS function to enhance system security.

Procedure

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

Figure 5-237 HTTPS



Enable

To enhance system security, the Web,ONVIF,RTSP,CGI service can be accessed to device via HTTPS.

TLS Protocol Compatibility

Compatible with TL...

Select a device certificate

	No.	Certificate Serial Number	Valid Period
✓	1	[redacted]	2050-05-08 18:16:31

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**.

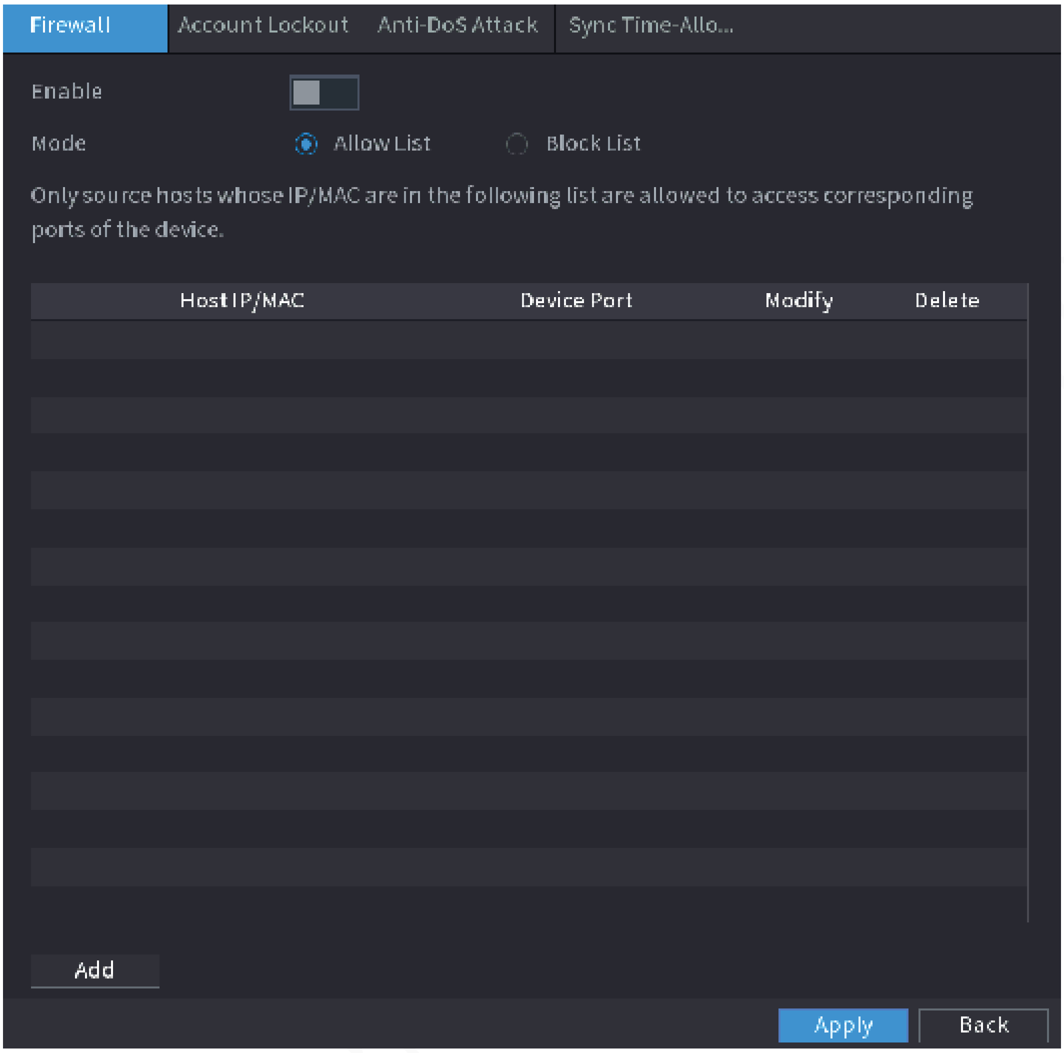
5.14.3 Attack Defense

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 5-238 Firewall



Enable

Mode ● Allow List ○ Block List

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

Host IP/MAC	Device Port	Modify	Delete

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.

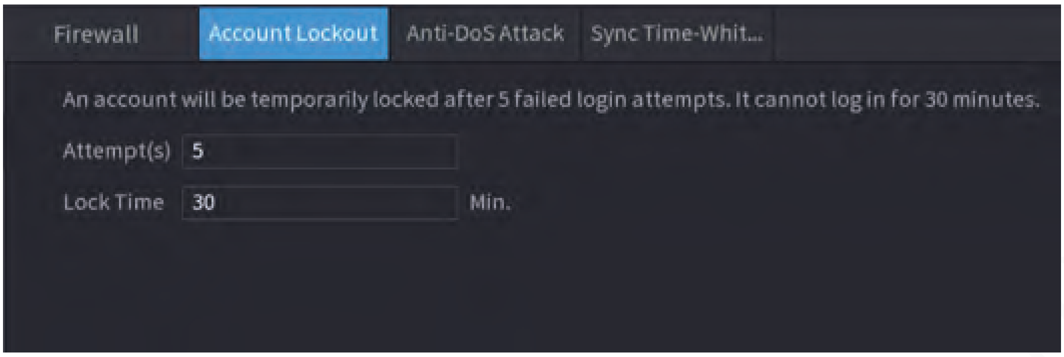
  Enter the MAC address, and then click **OK**.

Step 5 Click **Apply**.

5.14.3.2 Account Lockout

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

Figure 5-239 Account lockout



An account will be temporarily locked after 5 failed login attempts. It cannot log in for 30 minutes.

Attempt(s) 5

Lock Time 30 Min.

Step 2 Set parameters.

Table 5-71 Account lockout parameters

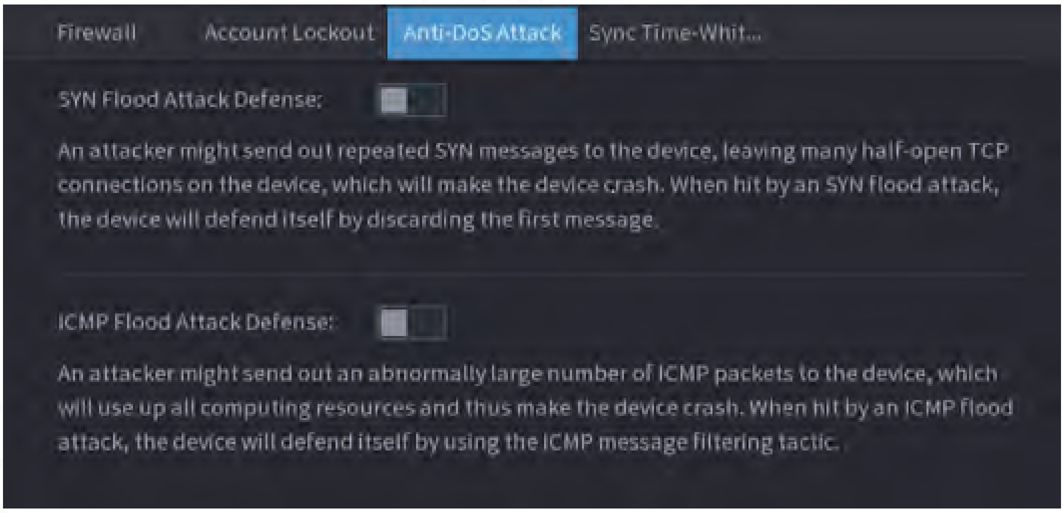
Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number.
Lock Time	Set how long the account is locked for.

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 5-240 Anti-Dos Attack



SYN Flood Attack Defense:

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense:

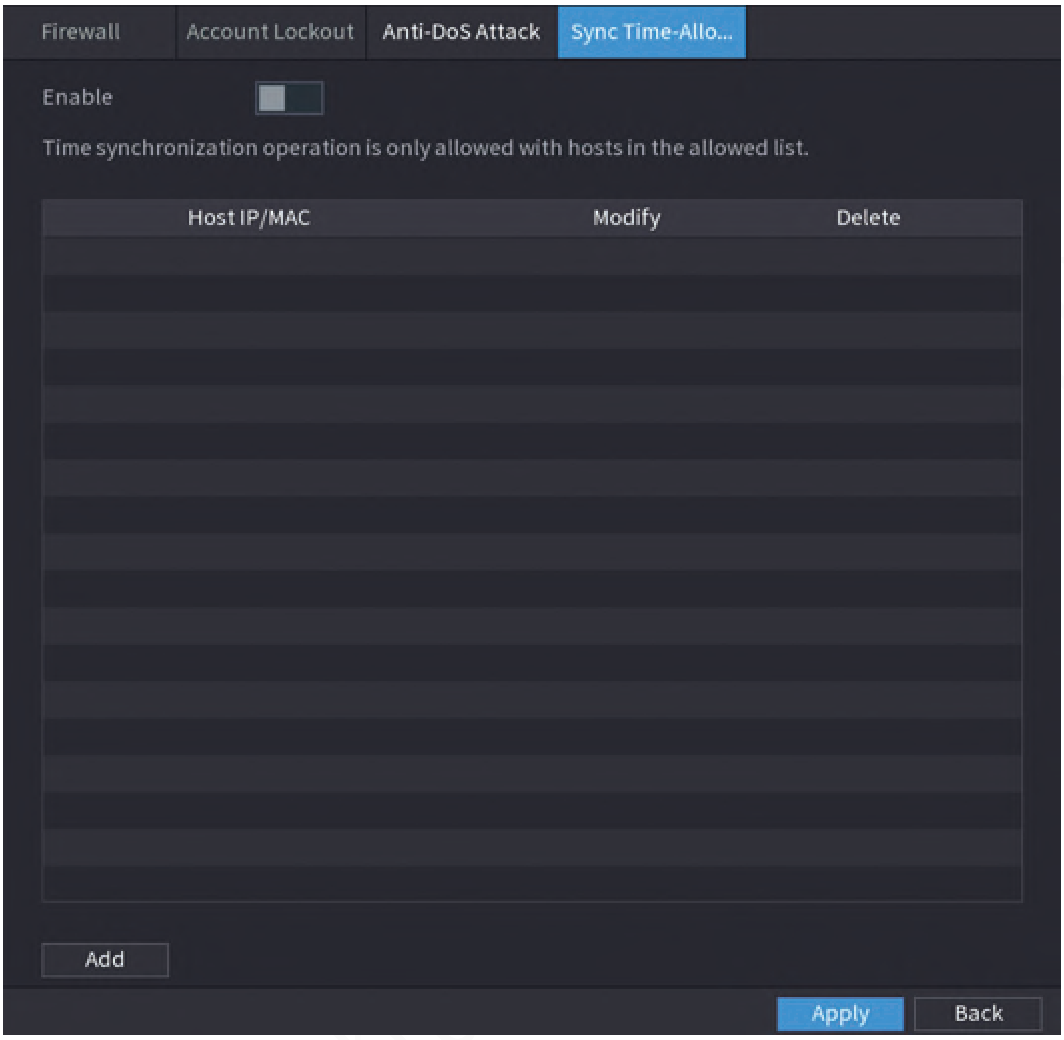
An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

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 5-241 Sync Time-Allowlist



Time synchronization operation is only allowed with hosts in the allowed list.

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**.

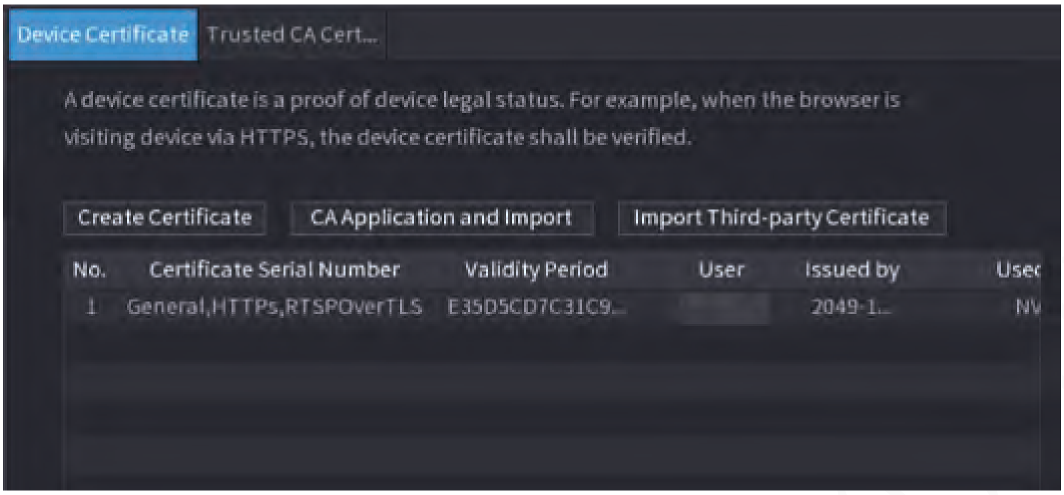
5.14.4 CA Certificate

5.14.4.1 Device Certificate

Create Certificate

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

Figure 5-242 Device certificate

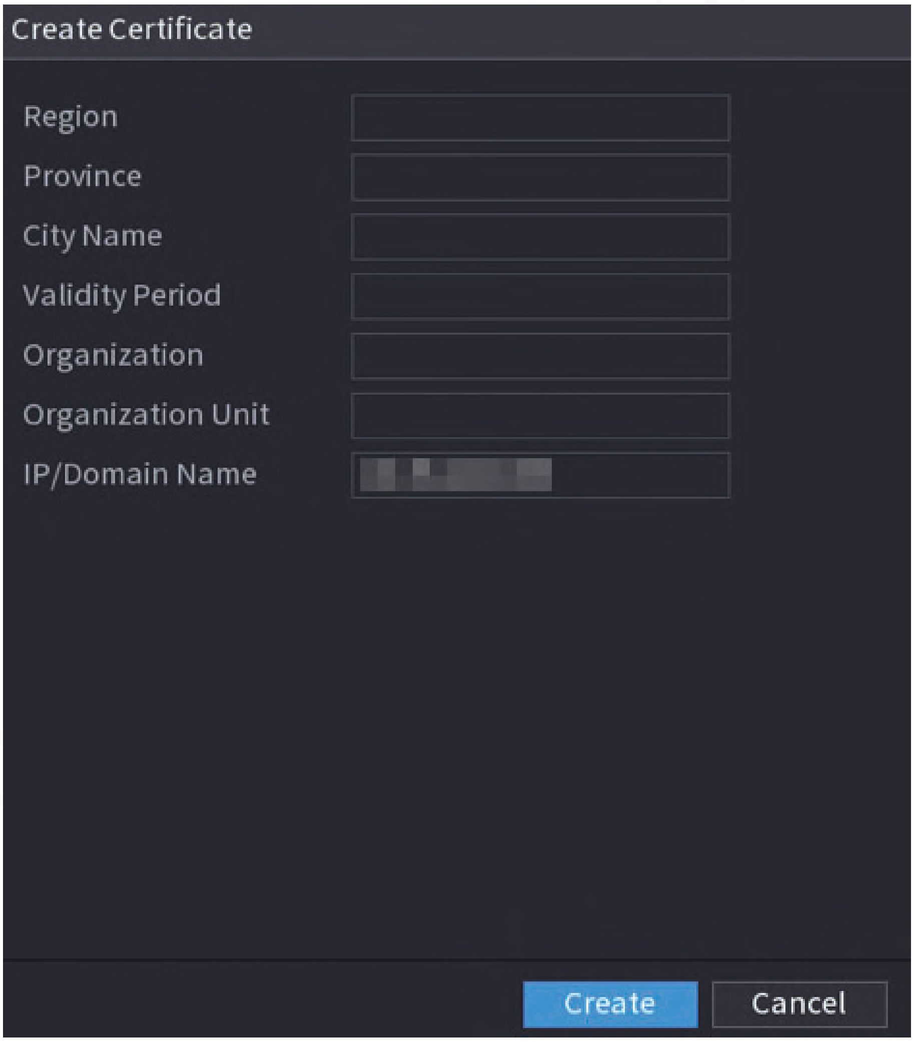


A device certificate is a proof of device legal status. For example, when the browser is visiting device via HTTPS, the device certificate shall be verified.

No.	Certificate Serial Number	Validity Period	User	Issued by	Usec
1	General,HTTPs,RTSPOverTLS	E35D5CD7C31C9...	[redacted]	2049-1...	NV

2. Click **Create Certificate**.

Figure 5-243 Create certificate



Create Certificate

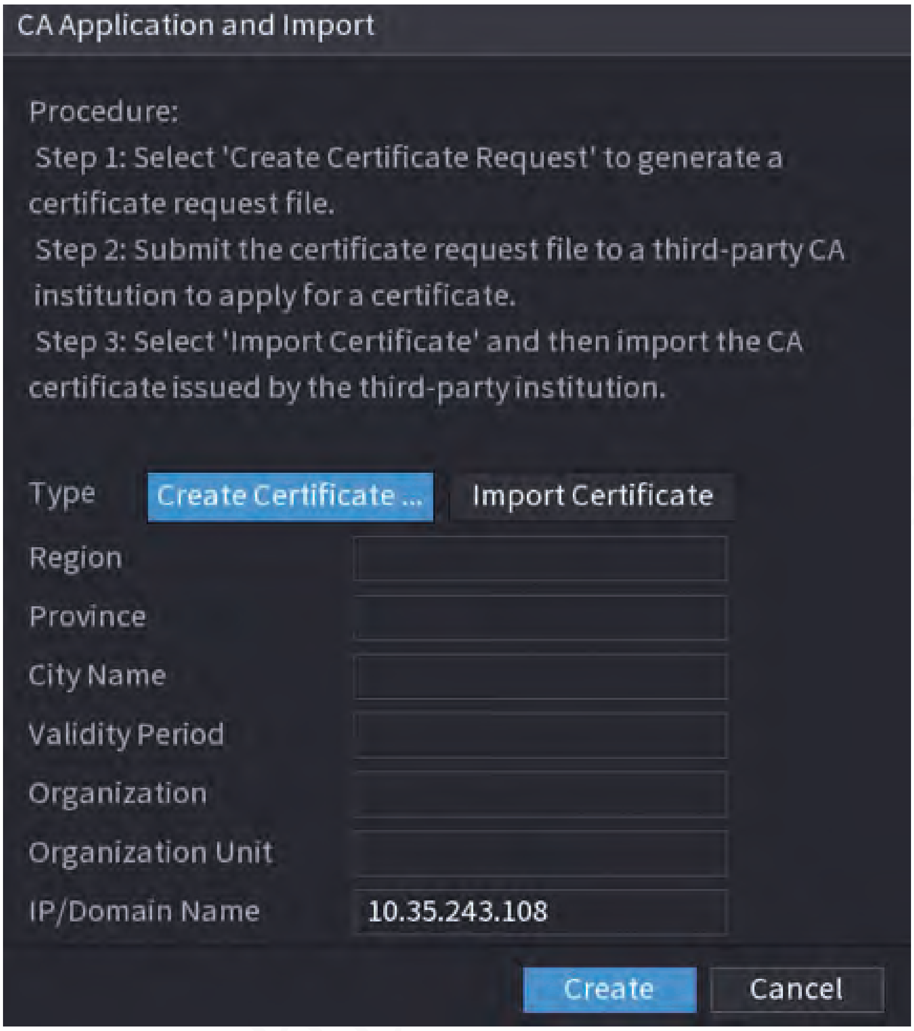
Region	
Province	
City Name	
Validity Period	
Organization	
Organization Unit	
IP/Domain Name	[redacted]

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 5-244 CA application and import



CA Application and Import

Procedure:

Step 1: Select 'Create Certificate Request' to generate a certificate request file.

Step 2: Submit the certificate request file to a third-party CA institution to apply for a certificate.

Step 3: Select 'Import Certificate' and then import the CA certificate issued by the third-party institution.

Type: Create Certificate ... | Import Certificate

Region:

Province:

City Name:

Validity Period:

Organization:

Organization Unit:

IP/Domain Name: 10.35.243.108

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.

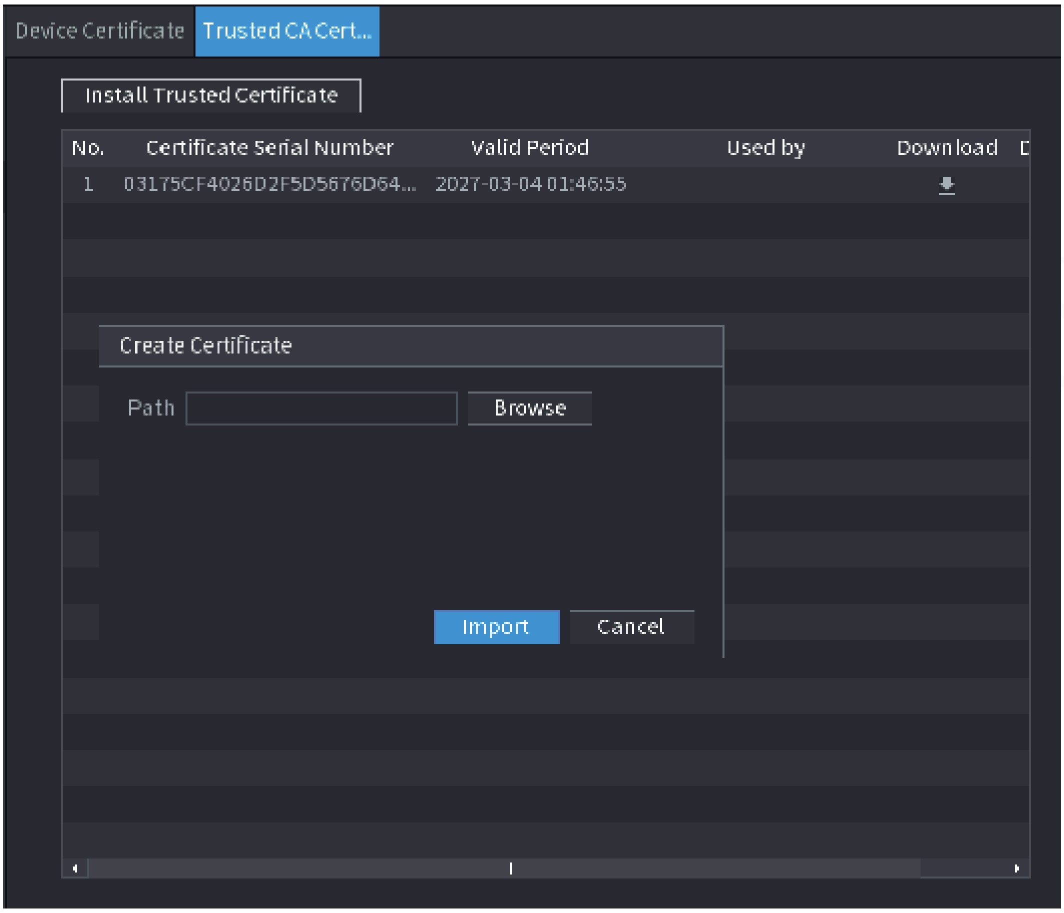
3. Click **Create**.

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 5-245 Create certificate



No.	Certificate Serial Number	Valid Period	Used by	Download	D
1	03175CF4026D2F5D5676D64...	2027-03-04 01:46:55		⬇	

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

Step 4 Click **Import**.

5.14.5 Audio/Video Encryption

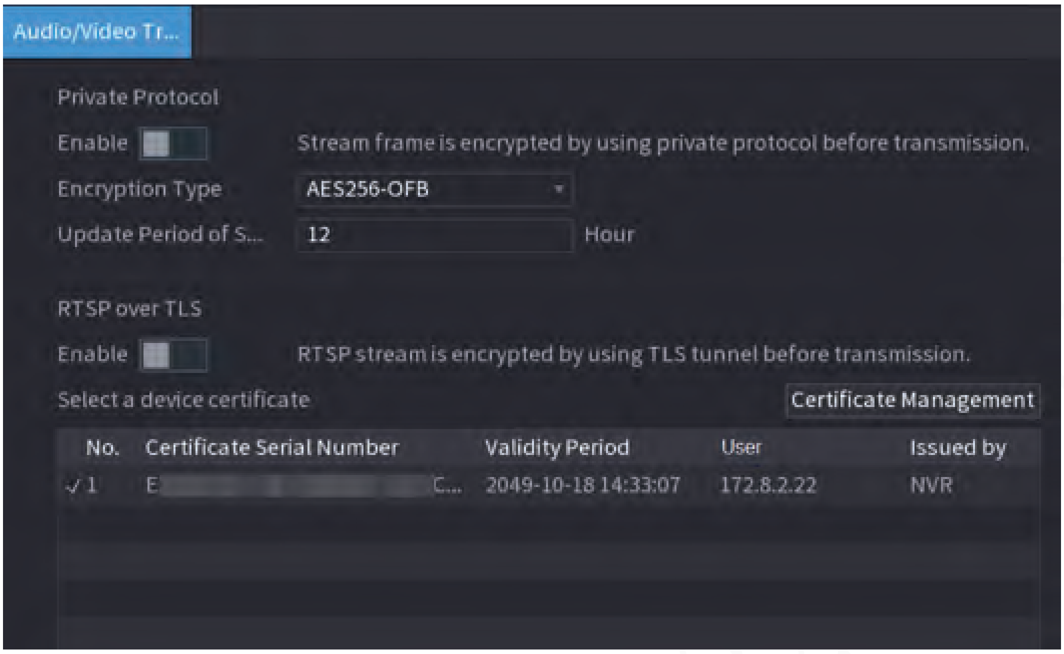
Background Information

The Device supports audio and video encryption during data transmission.

Procedure

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

Figure 5-246 Audio and video transmission



Private Protocol

Enable — Stream frame is encrypted by using private protocol before transmission.

Encryption Type: AES256-OFB

Update Period of S...: 12 Hour

RTSP over TLS

Enable — RTSP stream is encrypted by using TLS tunnel before transmission.

Select a device certificate — Certificate Management

No.	Certificate Serial Number	Validity Period	User	Issued by
✓ 1	E[redacted]C...	2049-10-18 14:33:07	172.8.2.22	NVR

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**.

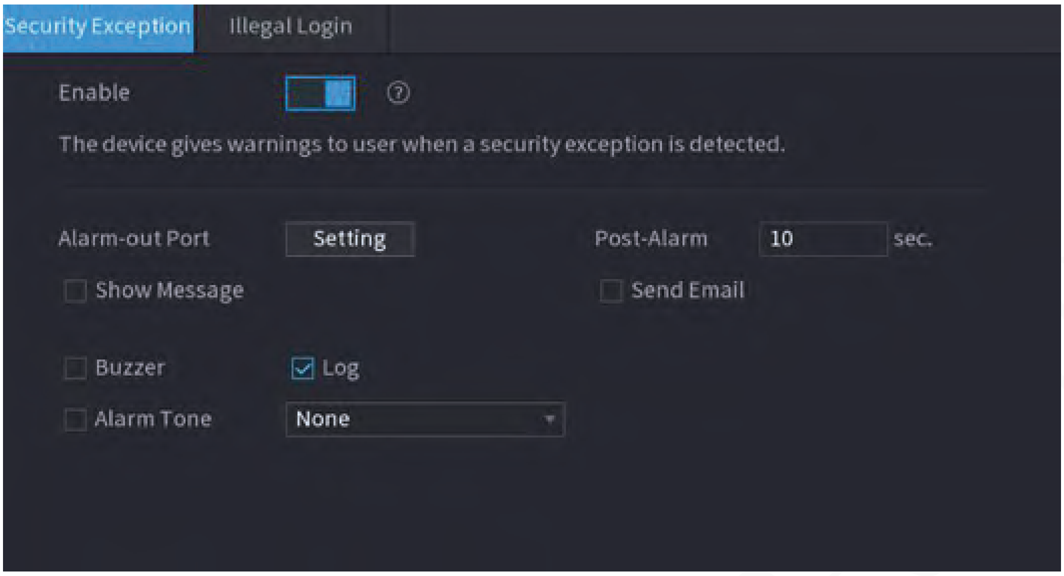
5.14.6 Security Warning

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 5-247 Security exception



Enable ▭ ?

The device gives warnings to user when a security exception is detected.

Alarm-out Port: Setting

Post-Alarm: 10 sec.

□ Show Message

□ Send Email

□ Buzzer

☑ Log

□ Alarm Tone: None

Step 2 Click ▭ to enable the function.

Click ● to view the list of security exception events.

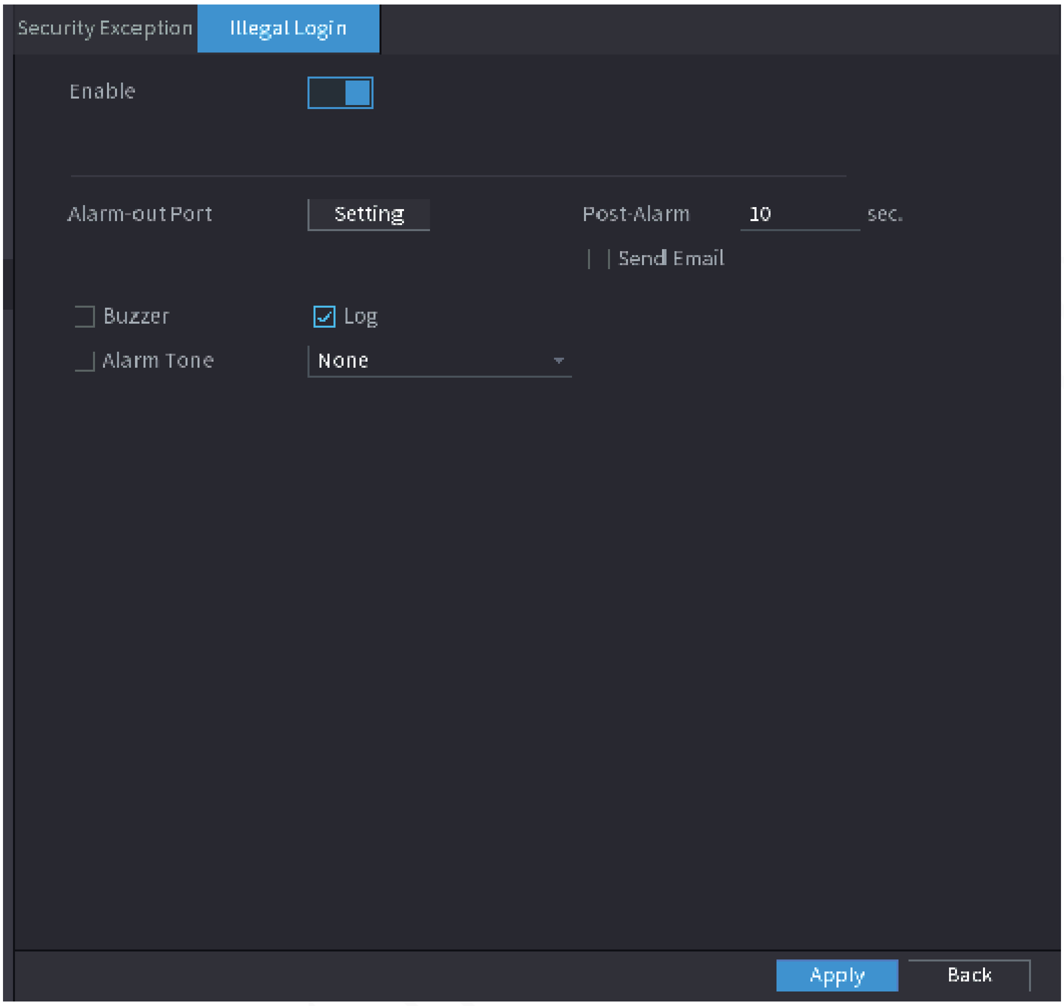
Step 3 Configure alarm linkage actions. For details, see Table 5-42.

Step 4 Click **Apply**.

5.14.6.2 Illegal Login

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

Figure 5-248 Illegal login



Enable ■

Alarm-out Port Setting

Post-Alarm 10 sec.

□ Send Email

□ Buzzer

☑ Log

□ Alarm Tone None

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.

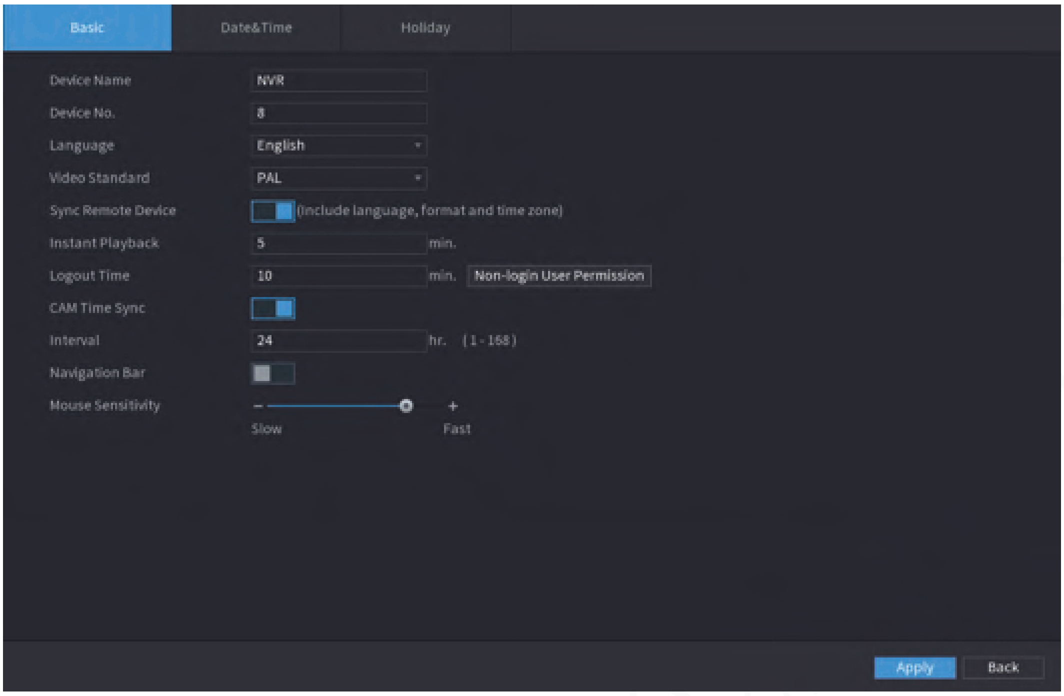
5.15.1.1 General

Background Information

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

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

Figure 5-249 Basic settings



Device Name NVR

Device No. 8

Language English

Video Standard PAL

Sync Remote Device (Include language, format and time zone)

Instant Playback 5 min.

Logout Time 10 min. Non-login User Permission

CAM Time Sync

Interval 24 hr. (1-168)

Navigation Bar

Mouse Sensitivity – + Slow Fast

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.
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.

Parameter	Description
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

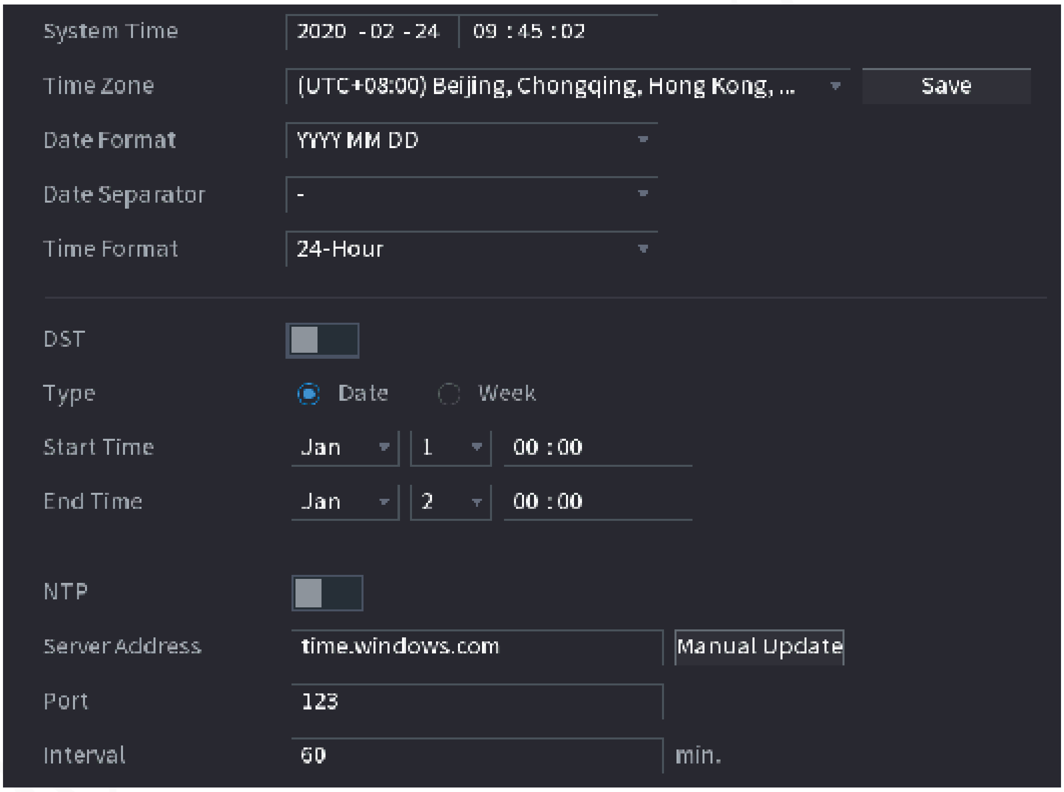
Background Information

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 5-250 Date and time



System Time 2020 - 02 - 24 09 : 45 : 02

Time Zone (UTC+08:00) Beijing, Chongqing, Hong Kong, ...

Date Format YYYY MM DD

Date Separator -

Time Format 24-Hour

DST

Type ● Date ○ Week

Start Time Jan 1 00 : 00

End Time Jan 2 00 : 00

NTP

Server Address time.windows.com

Port 123

Interval 60 min.

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.

Parameter	Description
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	
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.

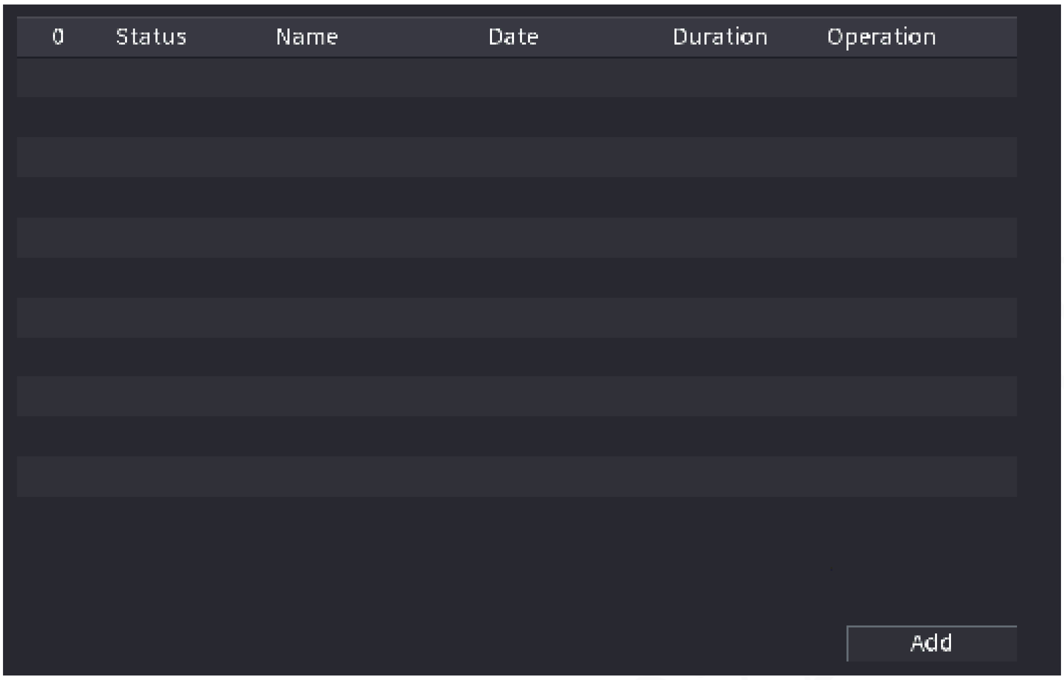
5.15.1.3 Holiday

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**.

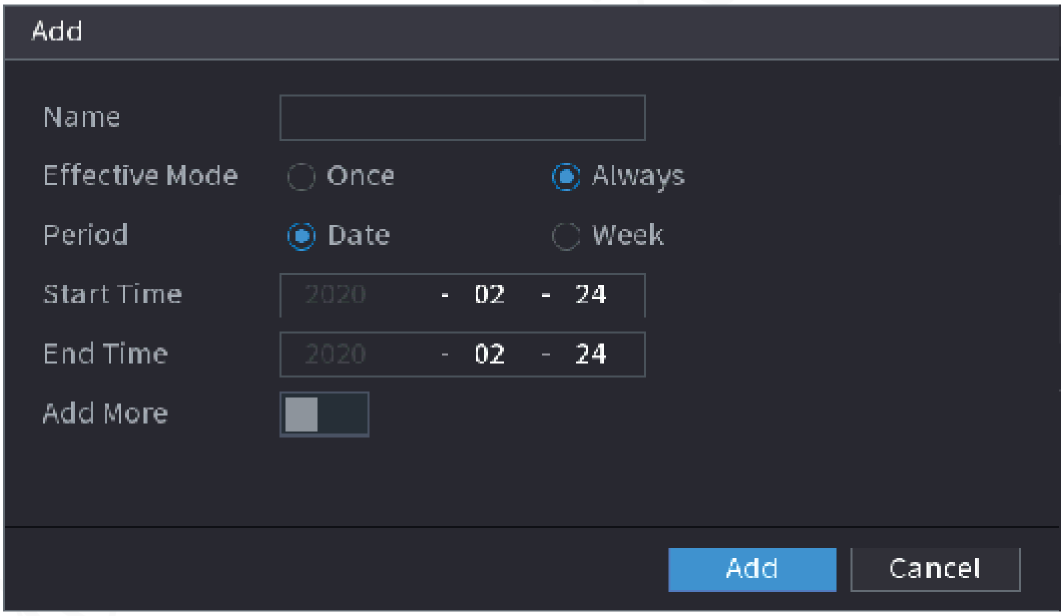
Figure 5-251 Holiday



0	Status	Name	Date	Duration	Operation

Step 2 Click **Add Holidays**.

Figure 5-252 Add holidays



Add

Name		
Effective Mode	○ Once	● Always
Period	● Date	○ Week
Start Time	2020 - 02 - 24	
End Time	2020 - 02 - 24	
Add More		

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

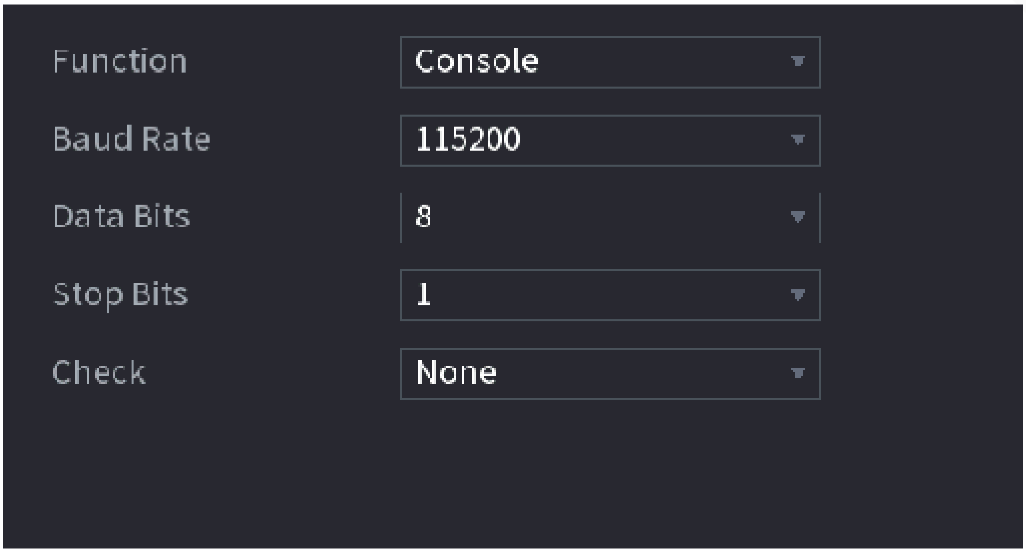
Background Information

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 5-253 Serial port



Function: Console

Baud Rate: 115200

Data Bits: 8

Stop Bits: 1

Check: None

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

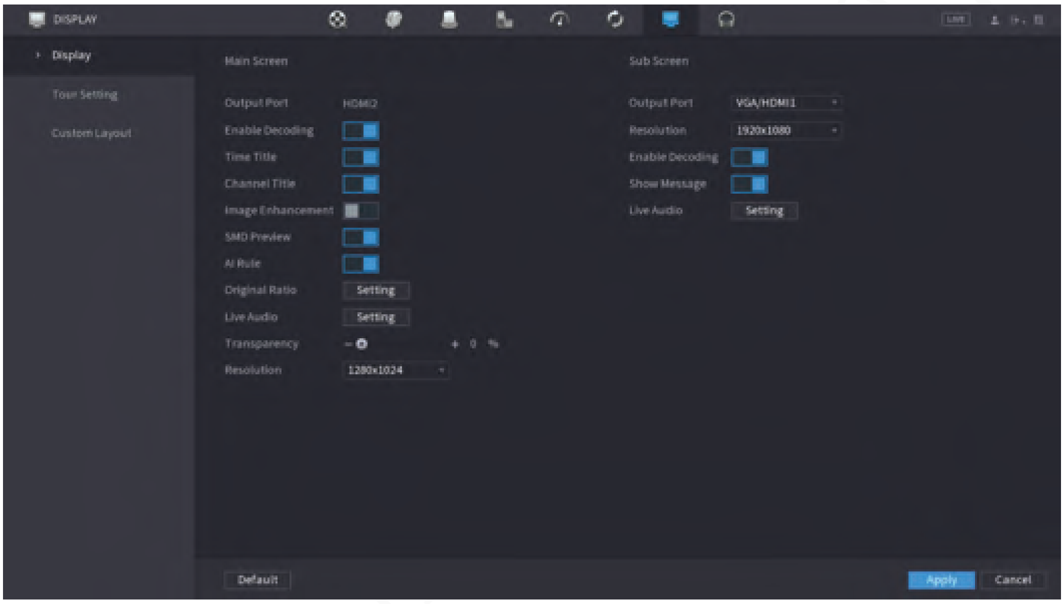
Background Information

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 5-254 Display



Main Screen

Output Port: HDMI2
Enable Decoding: on
Time Title: on
Channel Title: on
Image Enhancement: off
SMD Preview: on
AI Rule: on
Original Ratio: Setting
Live Audio: Setting
Transparency: − + 0 %
Resolution: 1280x1024

Sub Screen

Output Port: VGA/HDMI1
Resolution: 1920x1080
Enable Decoding: on
Show Message: on
Live Audio: Setting

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.

Parameter	Description
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.
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

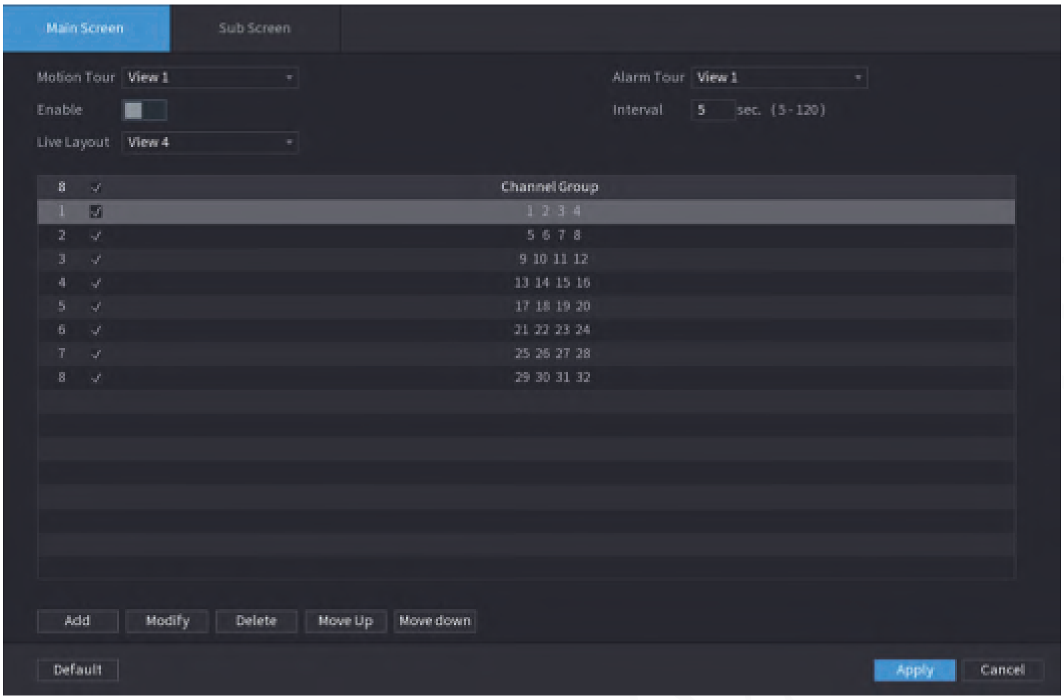
Background Information

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 5-255 Tour



Motion Tour: View 1

Enable: □

Live Layout: View 4

Alarm Tour: View 1

Interval: 5 sec. (5 - 120)

8	✓	Channel Group
1	☑	1 2 3 4
2	✓	5 6 7 8
3	✓	9 10 11 12
4	✓	13 14 15 16
5	✓	17 18 19 20
6	✓	21 22 23 24
7	✓	25 26 27 28
8	✓	29 30 31 32

- 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

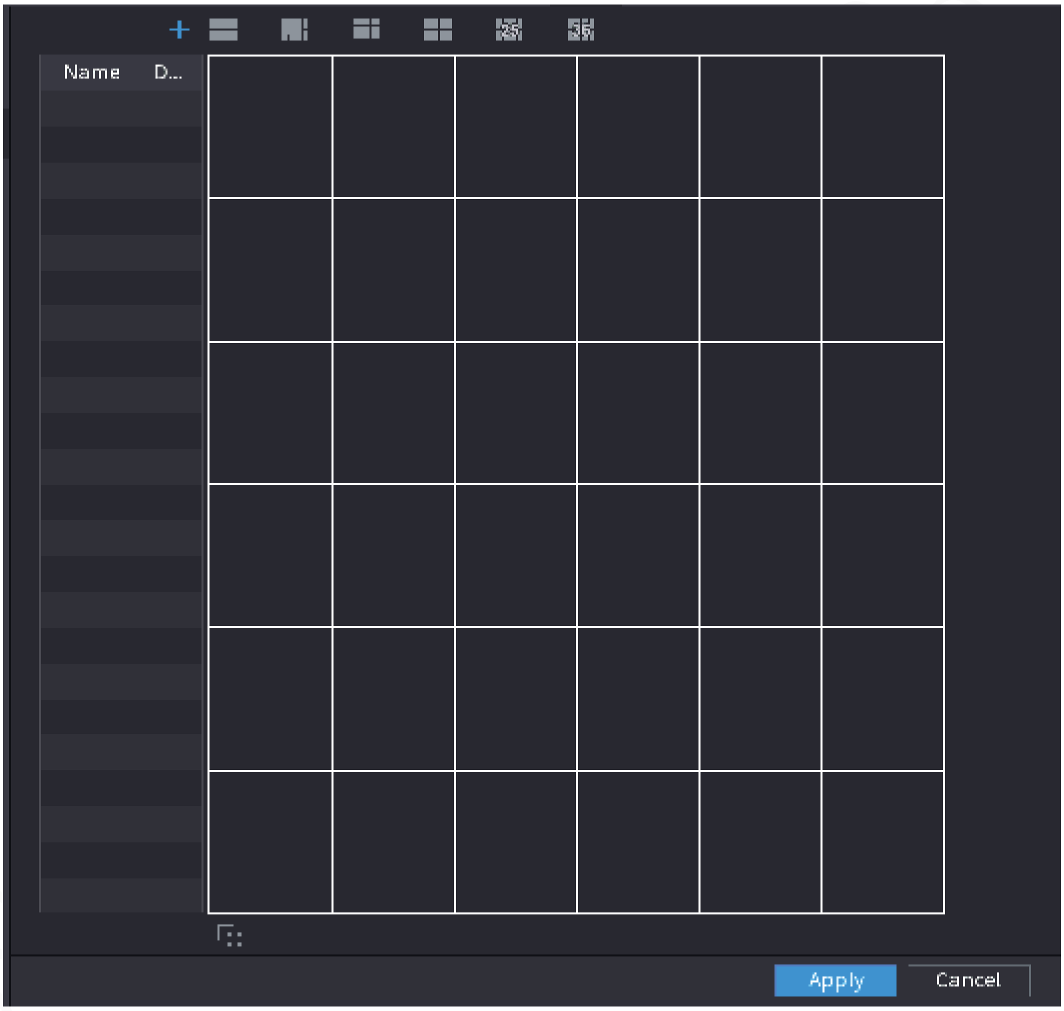
You can set customized video split mode.

- 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 5-256 Custom split

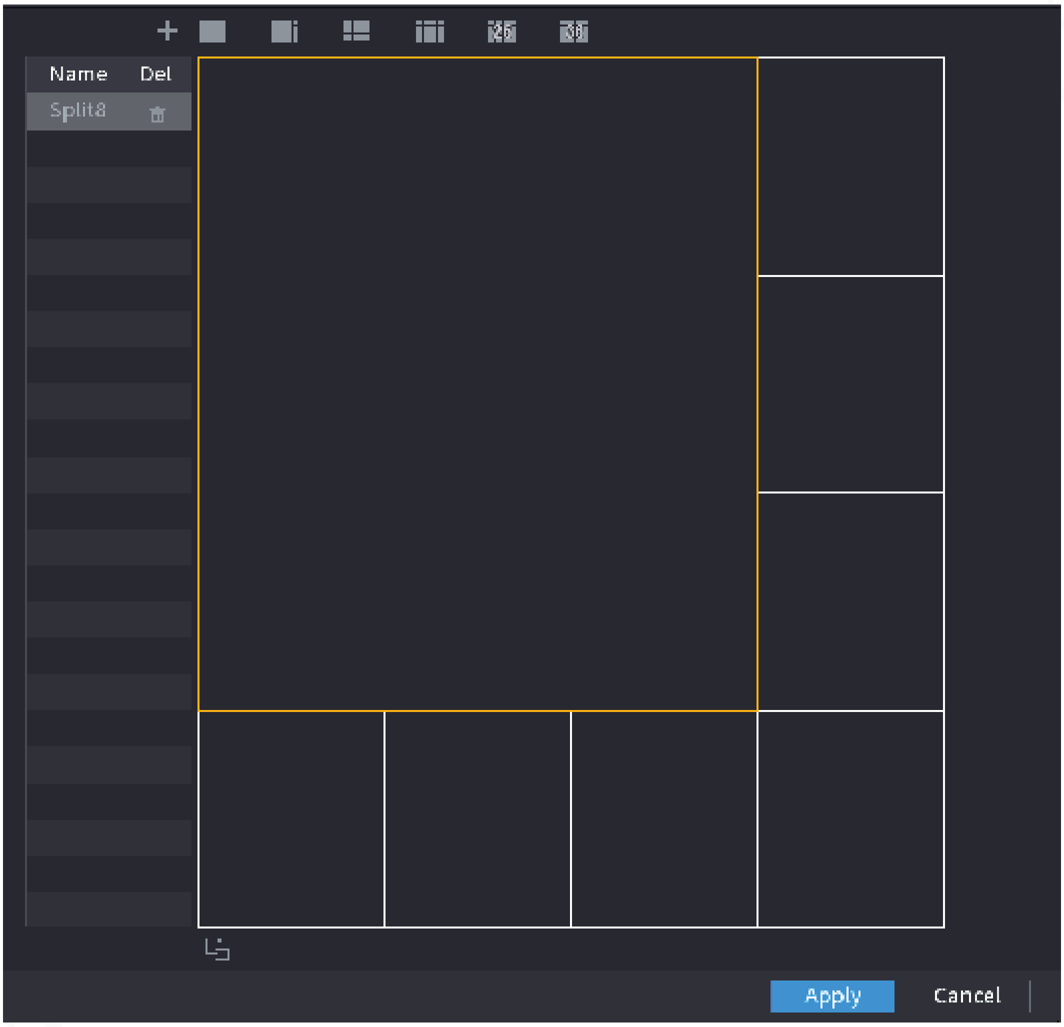


Step 2 Click + and then click ▤ ▦ ▦ ▦ ▦ ▦ to select basic mode.

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 ⊞ to cancel the merge to restore the basic mode.
- Click 🗑 to delete the customized window mode.

Figure 5-257 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

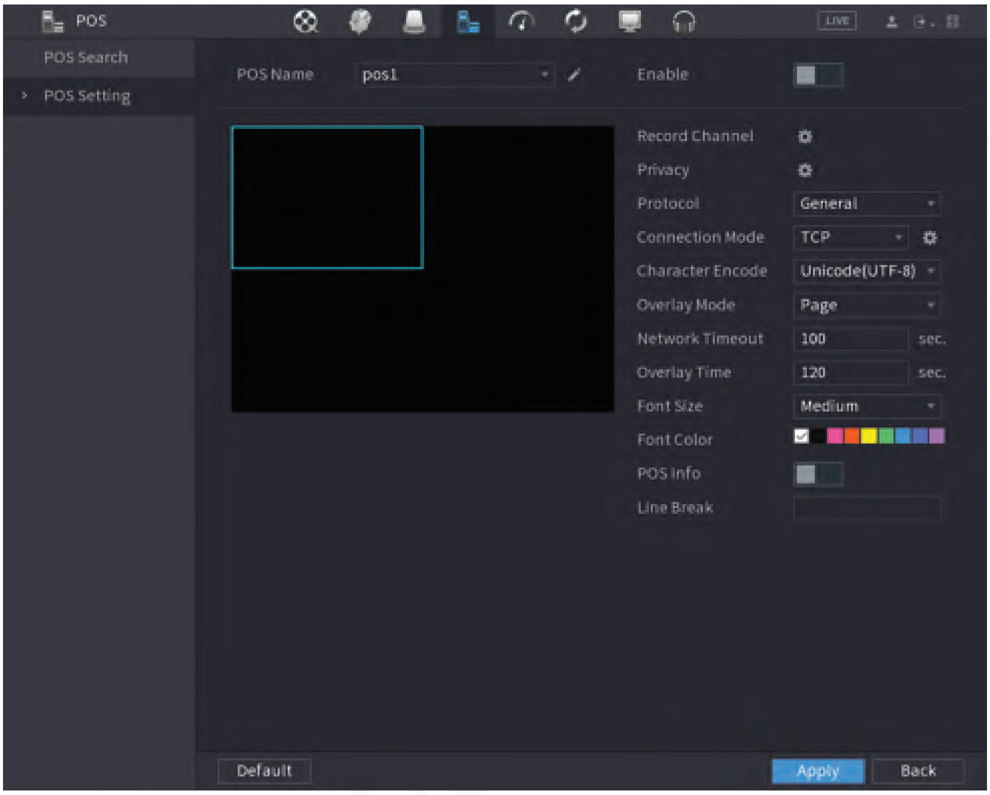
You can connect the Device to the POS (Point of Sale) machine and receive the information from it. This function applies to the scenarios such as supermarket POS machine. After connection is established, the Device can access the POS information and display the overlaid text in the channel window.

5.17.1 Settings

Procedure

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

Figure 5-258 POS setting



POS Name: pos1

Enable

Record Channel

Privacy

Protocol: General

Connection Mode: TCP

Character Encode: Unicode(UTF-8)

Overlay Mode: Page

Network Timeout: 100 sec.

Overlay Time: 120 sec.

Font Size: Medium

Font Color

POS Info

Line Break

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

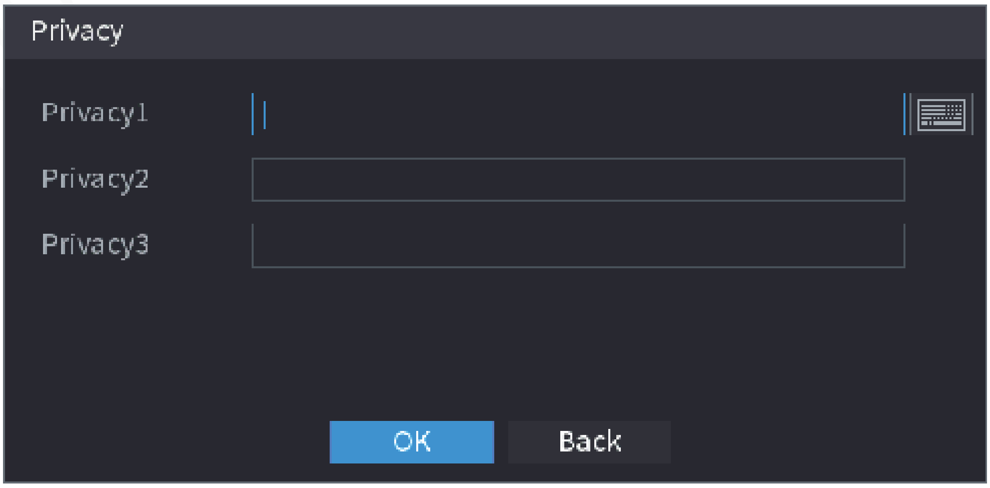
Step 3 Click **Apply**.

5.17.1.1 Privacy Setup

Procedure

Step 1 Click ⚙ next to **Privacy**.

Figure 5-259 Privacy



Step 2 Set privacy information.

Step 3 Click **OK**.

5.17.1.2 Connection Mode

Background Information

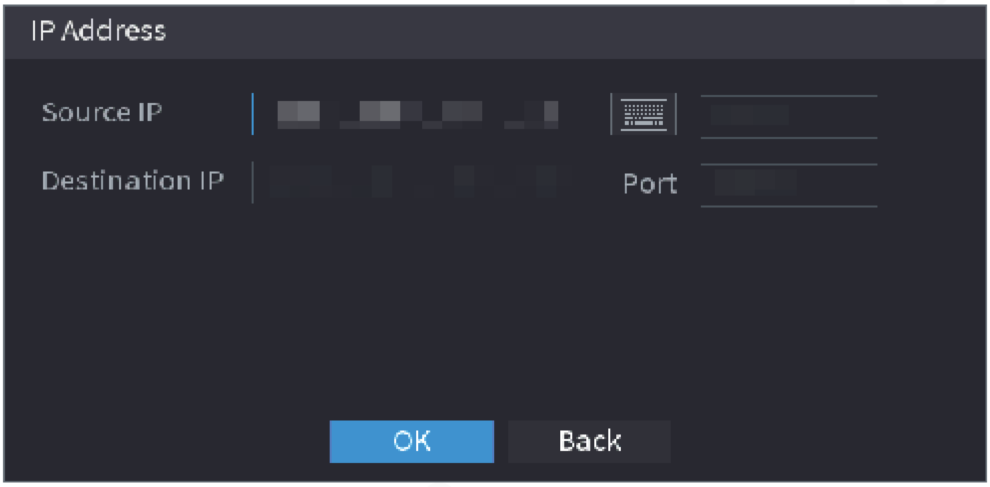
Connection type is UDP or TCP.

Procedure

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

Step 2 Click ⚙.

Figure 5-260 IP address



IP Address

Source IP [redacted] [redacted]

Destination IP [redacted] Port [redacted]

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

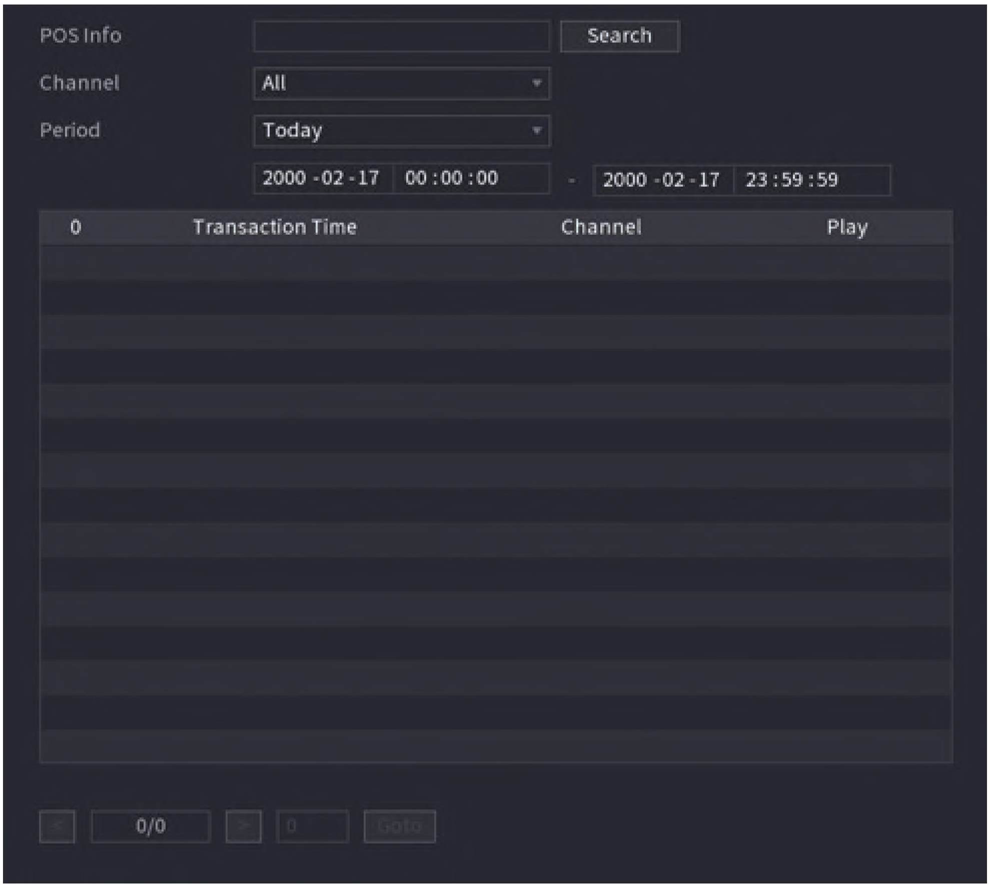
Step 4 Click **OK**.

5.17.2 Search

The system supports fuzzy search.

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

Figure 5-261 POS search



POS Info

Search

Channel: All

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

0	Transaction Time	Channel	Play

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.

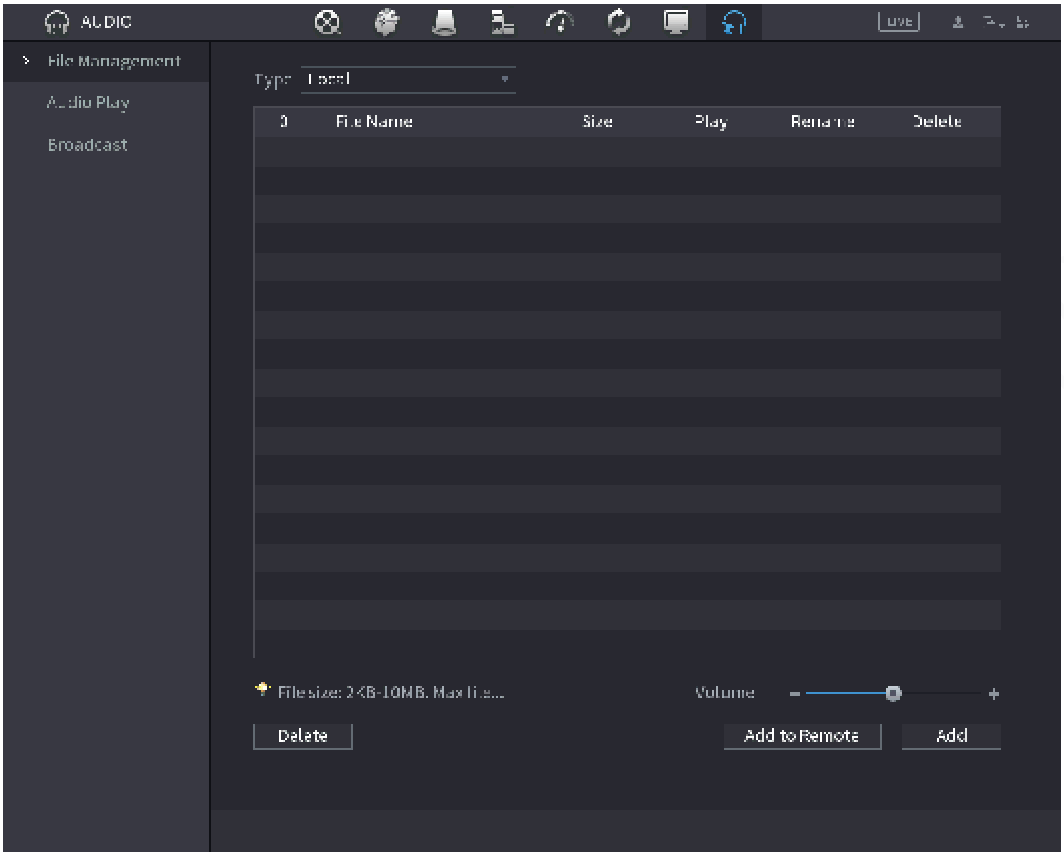
This function is available on select models.

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 5-262 File management



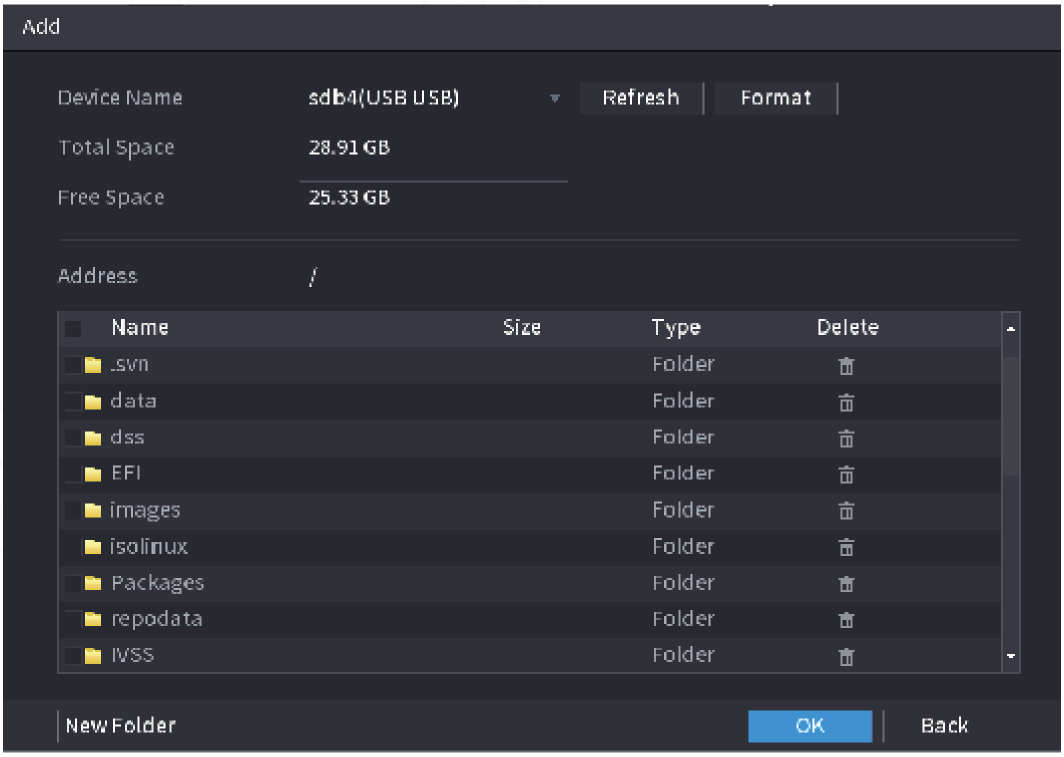
Type: Local

0	File Name	Size	Play	Rename	Delete

File size: 2KB-10MB. Max li...

Step 2 Click **Add**.

Figure 5-263 Add file



Device Name: sdb4(USB USB)

Total Space: 28.91 GB

Free Space: 25.33 GB

Address: /

Name	Size	Type	Delete
.svn		Folder	🗑
data		Folder	🗑
dss		Folder	🗑
EFI		Folder	🗑
images		Folder	🗑
isolinux		Folder	🗑
Packages		Folder	🗑
repodata		Folder	🗑
IVSS		Folder	🗑

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

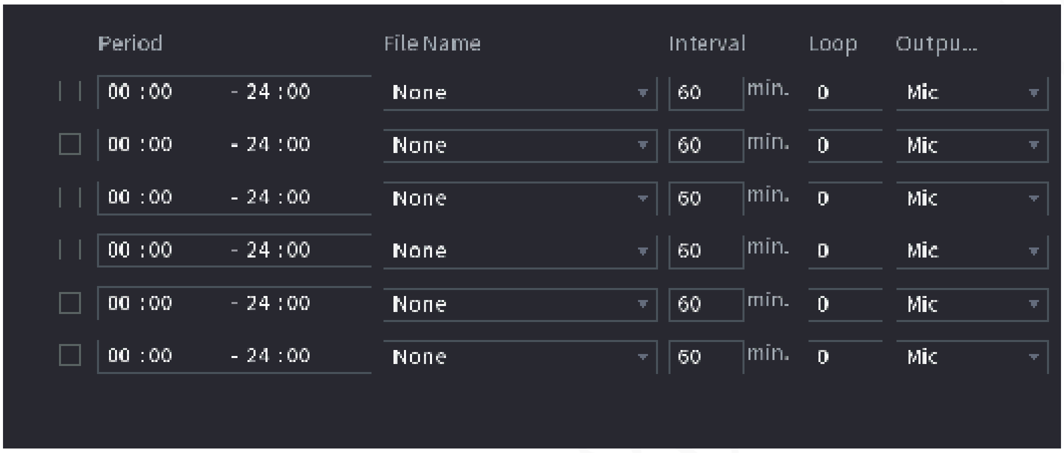
Background Information

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

Procedure

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

Figure 5-264 Schedule



	Period	File Name	Interval		Loop	Outpu...
□	00 :00 - 24 :00	None	60	min.	0	Mic
□	00 :00 - 24 :00	None	60	min.	0	Mic
□	00 :00 - 24 :00	None	60	min.	0	Mic
□	00 :00 - 24 :00	None	60	min.	0	Mic
□	00 :00 - 24 :00	None	60	min.	0	Mic
□	00 :00 - 24 :00	None	60	min.	0	Mic

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

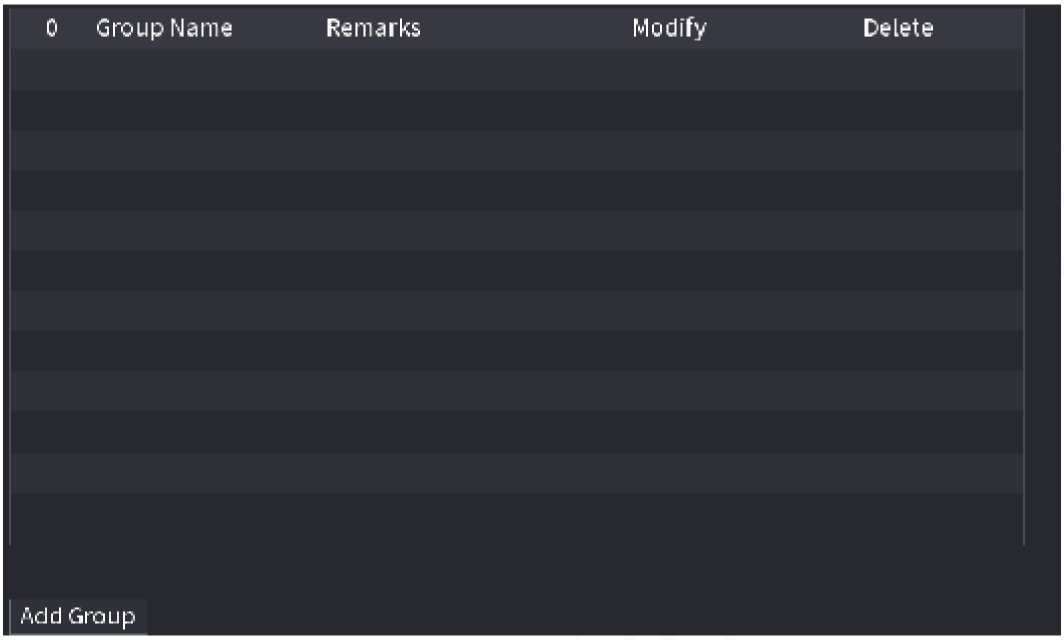
Background Information

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

Procedure

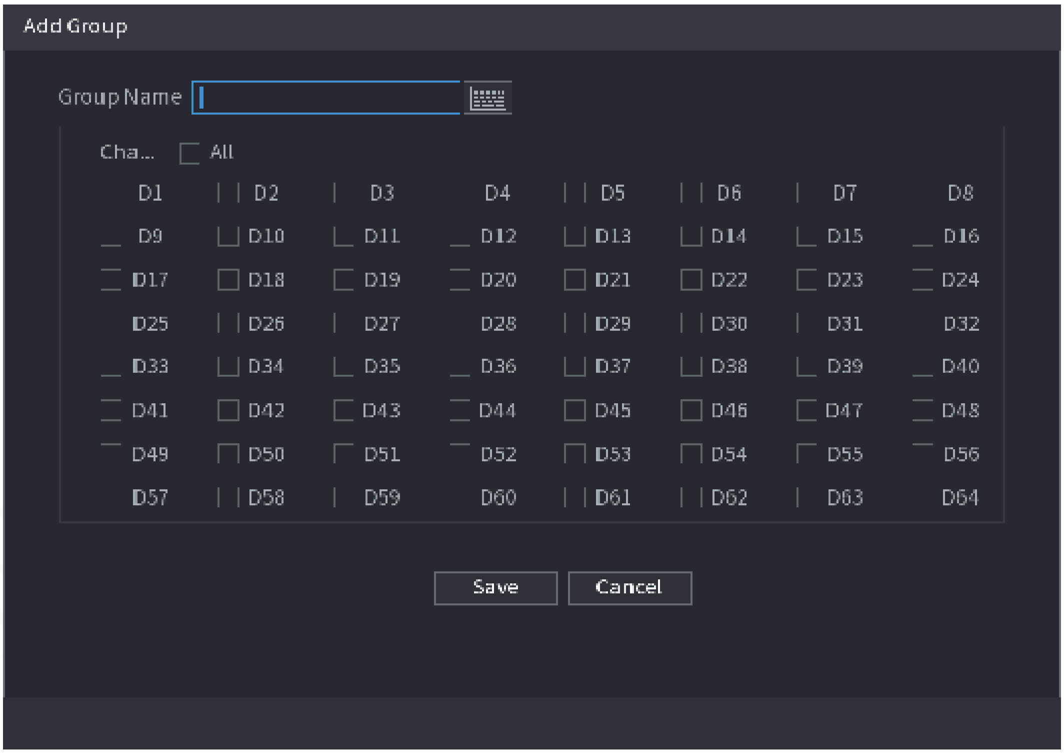
Step 1 Select **Mani Menu** > **AUDIO** > **Broadcast**.

Figure 5-265 Broadcast



Step 2 Click **Add Group**.

Figure 5-266 Add group (1)

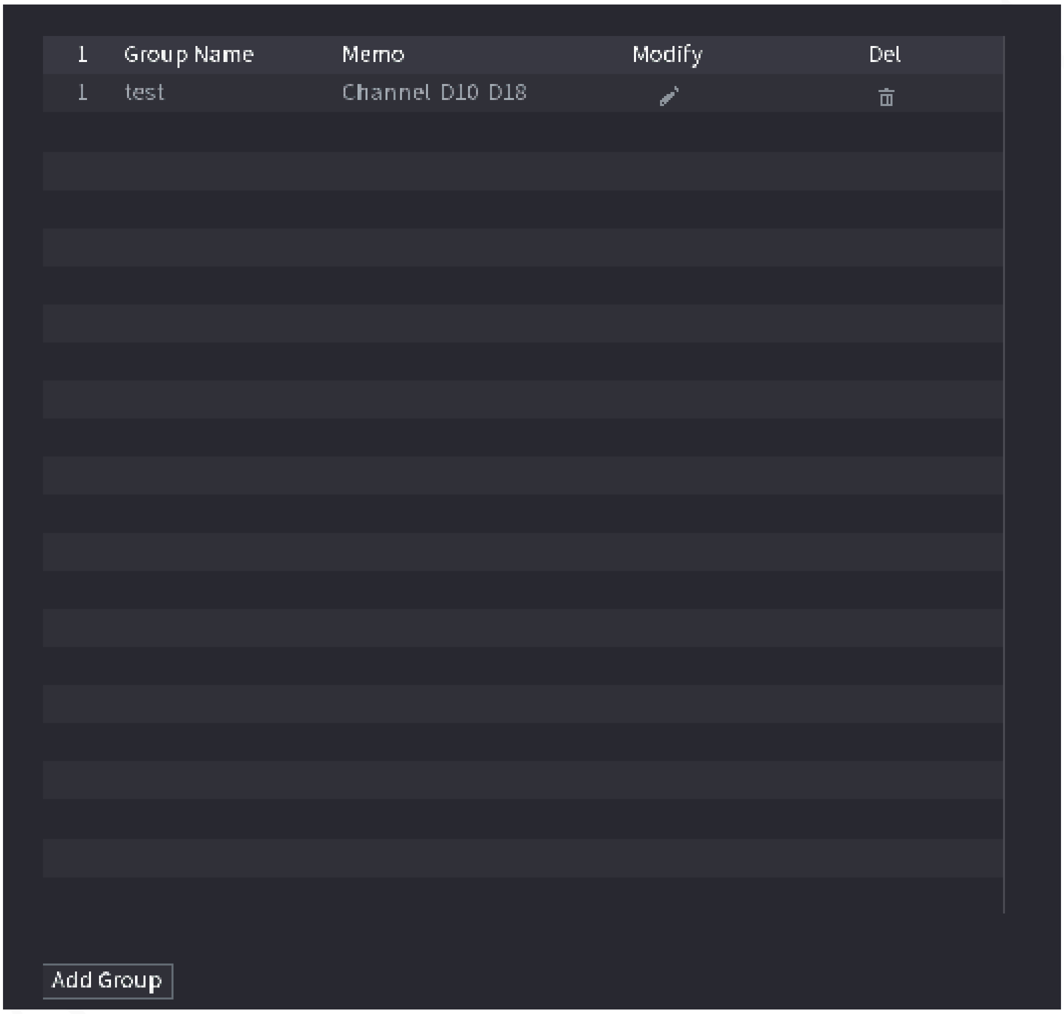

Add Group
Group Name
Cha... □ All
D1 D2 D3 D4 D5 D6 D7 D8
D9 D10 D11 D12 D13 D14 D15 D16
D17 D18 D19 D20 D21 D22 D23 D24
D25 D26 D27 D28 D29 D30 D31 D32
D33 D34 D35 D36 D37 D38 D39 D40
D41 D42 D43 D44 D45 D46 D47 D48
D49 D50 D51 D52 D53 D54 D55 D56
D57 D58 D59 D60 D61 D62 D63 D64
Save
Cancel

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 5-267 Add group (2)



1	Group Name	Memo	Modify	Del
1	test	Channel D10 D18	✎	🗑

5.19 Operation and Maintenance

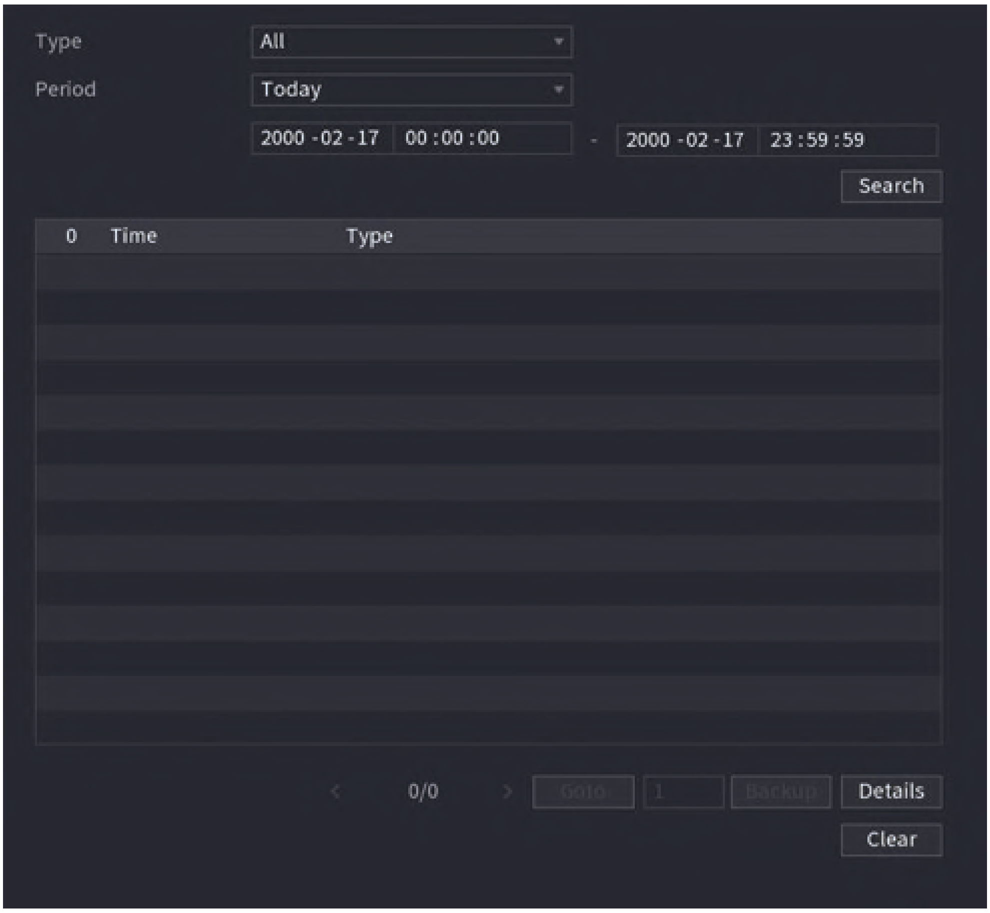
5.19.1 Log

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 5-268 Log



Type: All

Period: Today

2000 -02 -17 00 :00 :00 - 2000 -02 -17 23 :59 :59

0	Time	Type

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

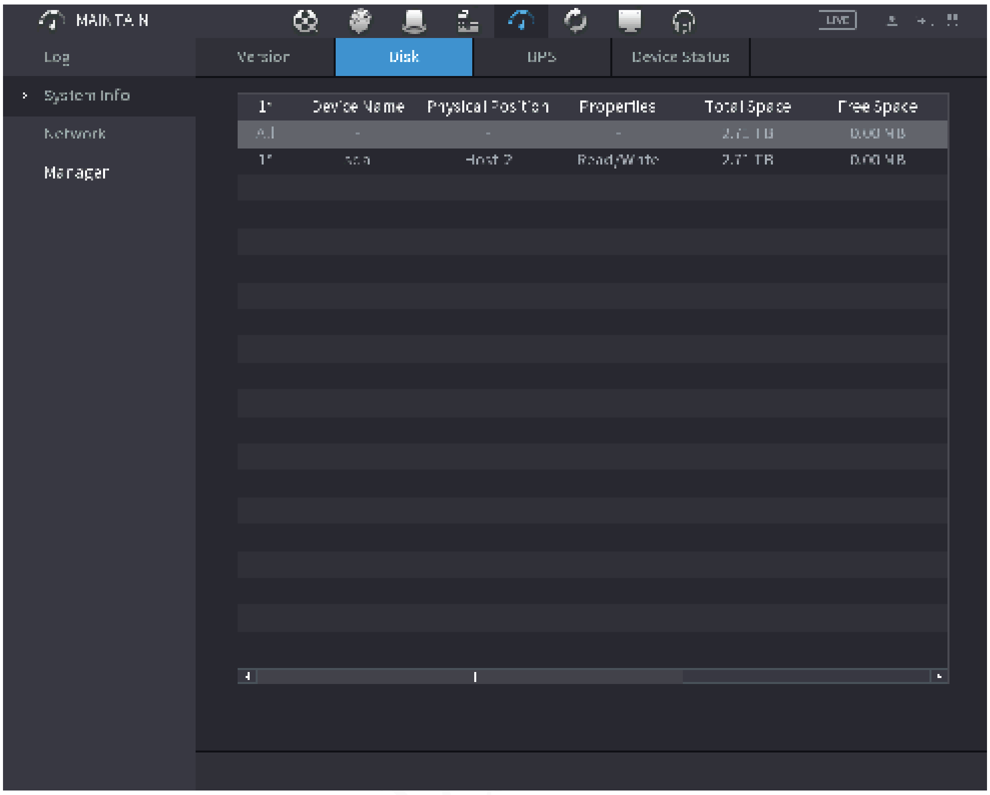
Select **Main Menu** > **MAINTAIN** > **System Info** > **Intelligent Algorithm**.

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 5-269 Disk information



1*	Device Name	Physical Position	Properties	Total Space	Free Space
All	-	-	-	2.72 TB	0.00 MB
1*	sda	Host 2	Read/Write	2.72 TB	0.00 MB

Table 5-81 Disk information

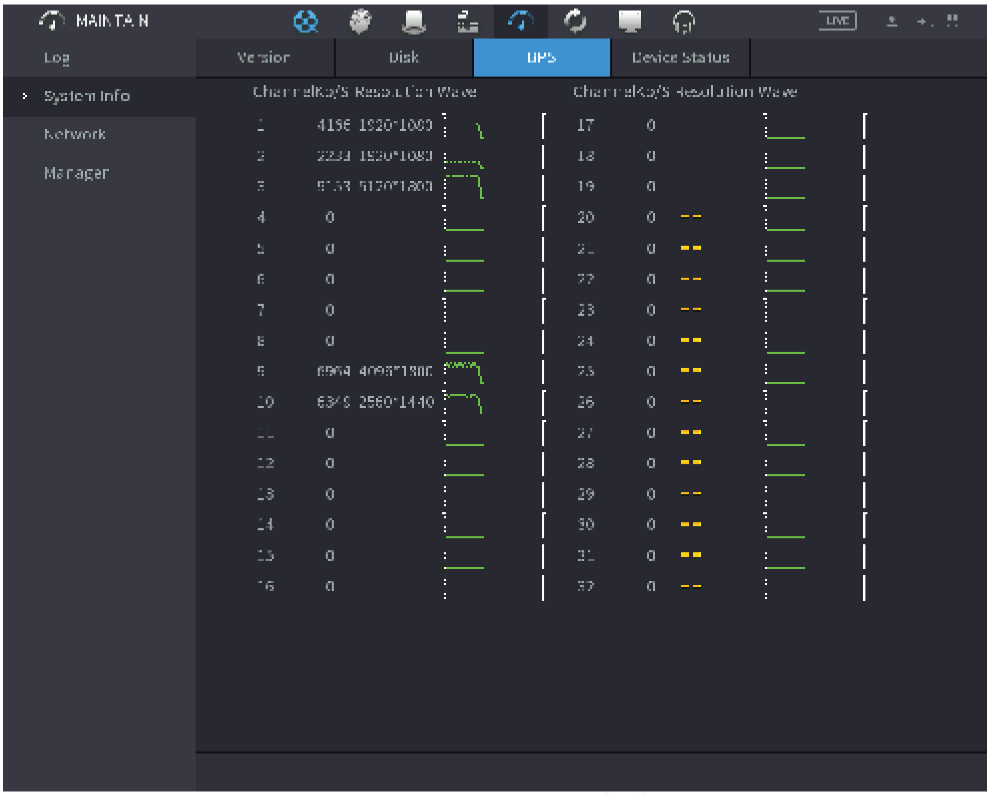
Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Properties	Indicates HDD type.
Total Space	Indicates the total capacity of HDD.
Free 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 5-270 BPS



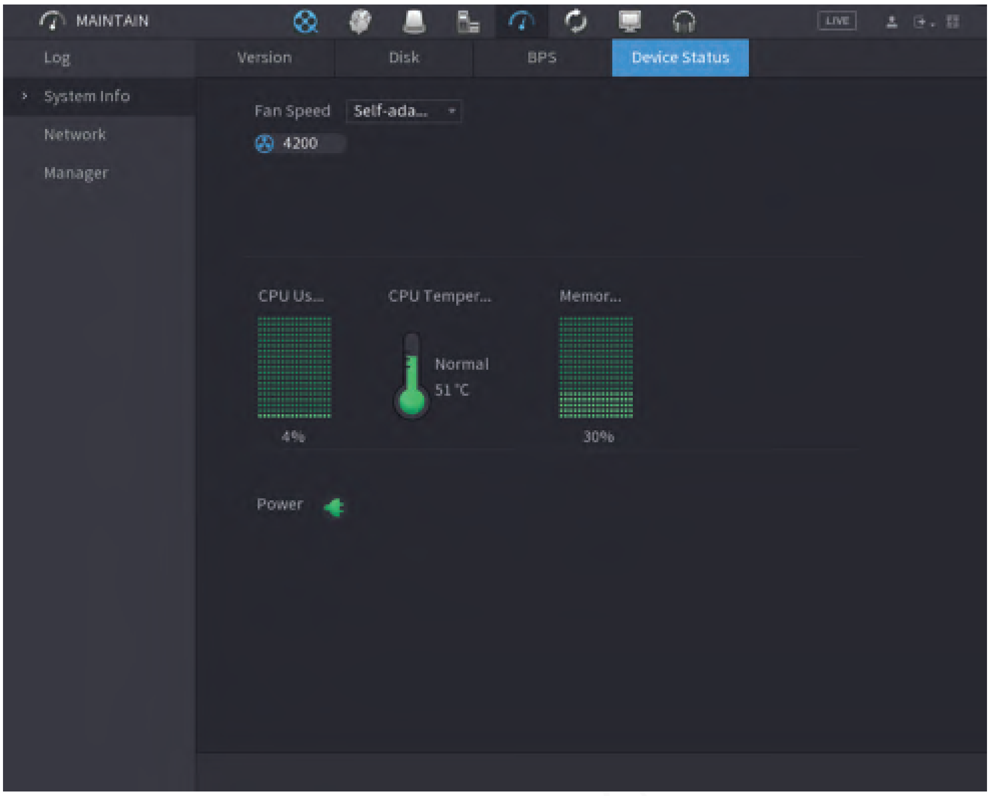
Channel	Kb/S	Resolution	Wave	Channel	Kb/S	Resolution	Wave
1	4196	1920*1080		17	0		
2	2233	1920*1080		18	0		
3	5153	5120*1800		19	0		
4	0			20	0	--	
5	0			21	0	--	
6	0			22	0	--	
7	0			23	0	--	
8	0			24	0	--	
9	6964	4096*1800		25	0	--	
10	6348	2560*1440		26	0	--	
11	0			27	0	--	
12	0			28	0	--	
13	0			29	0	--	
14	0			30	0	--	
15	0			31	0	--	
16	0			32	0	--	

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 5-271 Device status



Fan Speed: Self-ada...

4200

CPU Us... 4%

CPU Temper... Normal 51 ℃

Memor... 30%

Power

5.19.3 Network

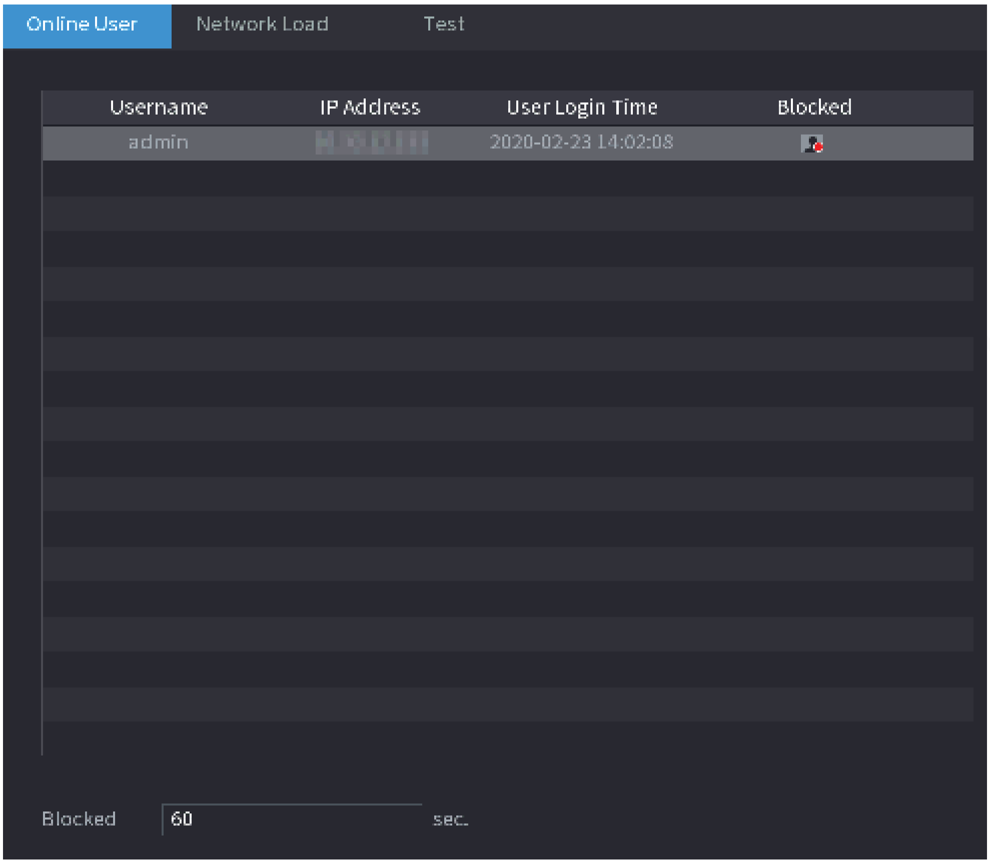
5.19.3.1 Online User

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 5-272 Online user



Username	IP Address	User Login Time	Blocked
admin	[redacted]	2020-02-23 14:02:08	

Blocked 60 sec.

5.19.3.2 Network Load

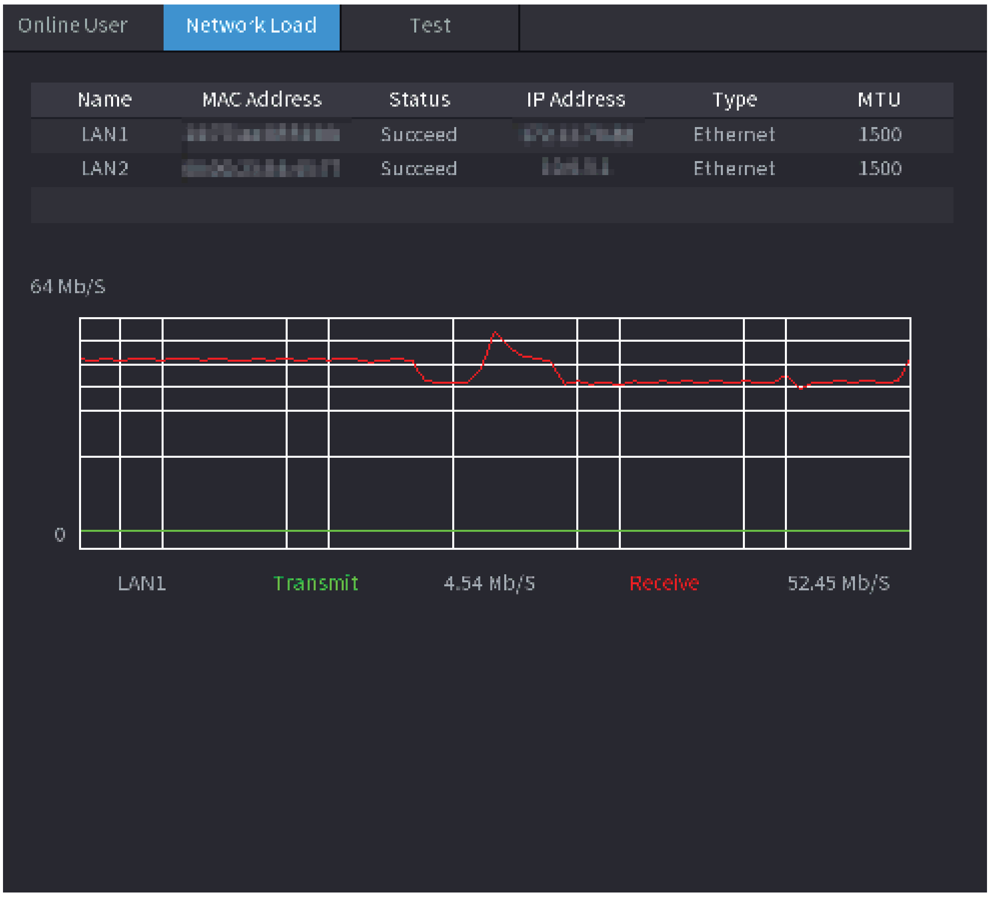
Background Information

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 5-273 Network load



Name	MAC Address	Status	IP Address	Type	MTU
LAN1	[redacted]	Succeed	[redacted]	Ethernet	1500
LAN2	[redacted]	Succeed	[redacted]	Ethernet	1500

LAN1 Transmit 4.54 Mb/S Receive 52.45 Mb/S

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

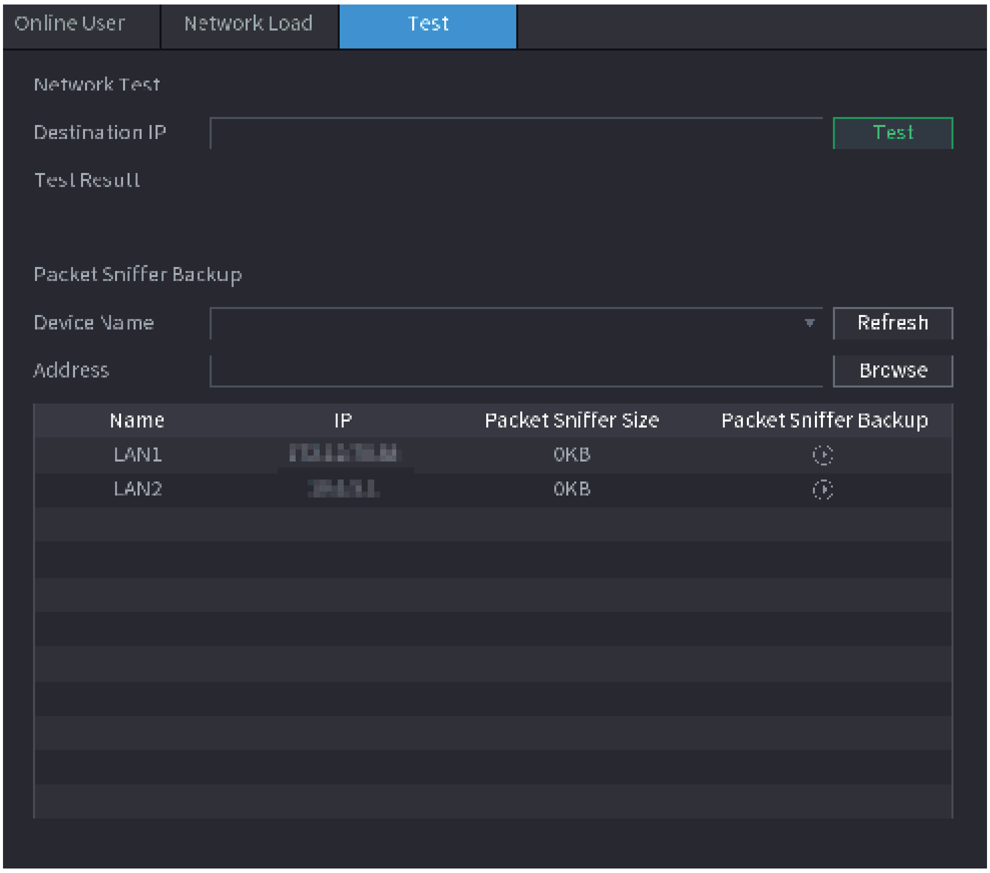
Background Information

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

Procedure

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

Figure 5-274 Test



Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	[redacted]	0KB	⊙
LAN2	[redacted]	0KB	⊙

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

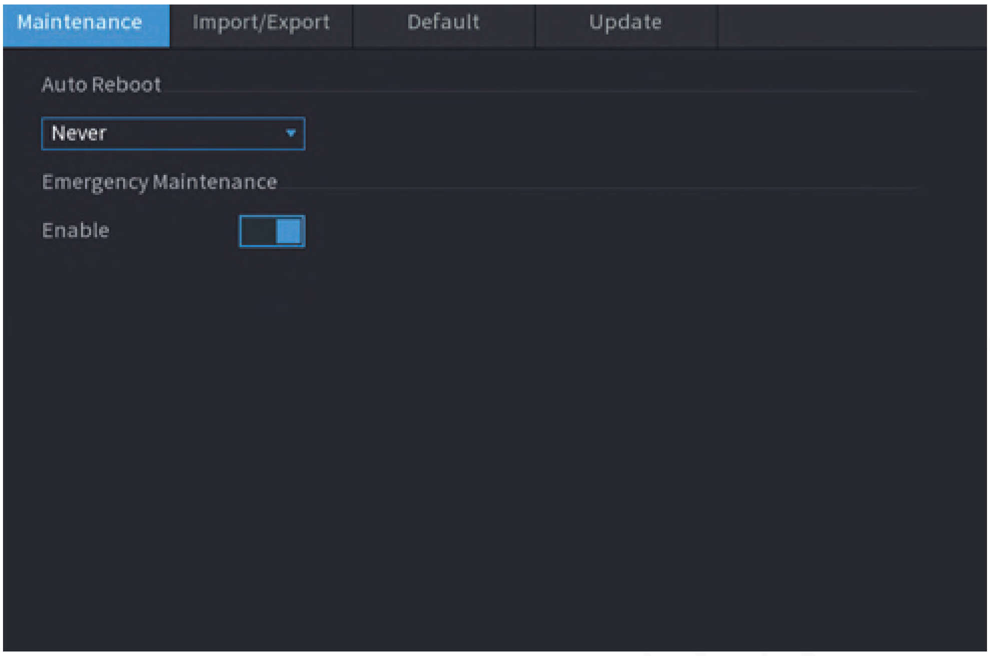
Background Information

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 5-275 Maintenance



Auto Reboot

Never

Emergency Maintenance

Enable

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

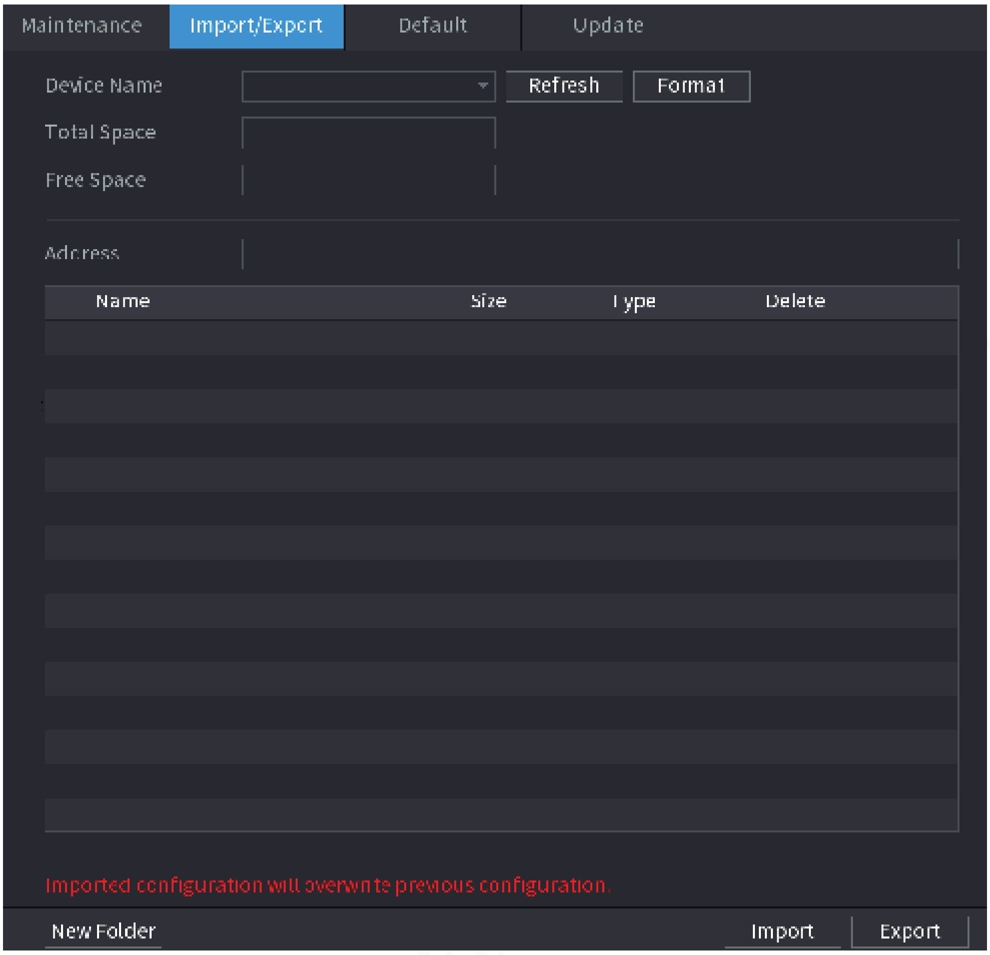
You can export or import the Device system settings if there are several Devices that require the same setup.

- 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 5-276 Import and export



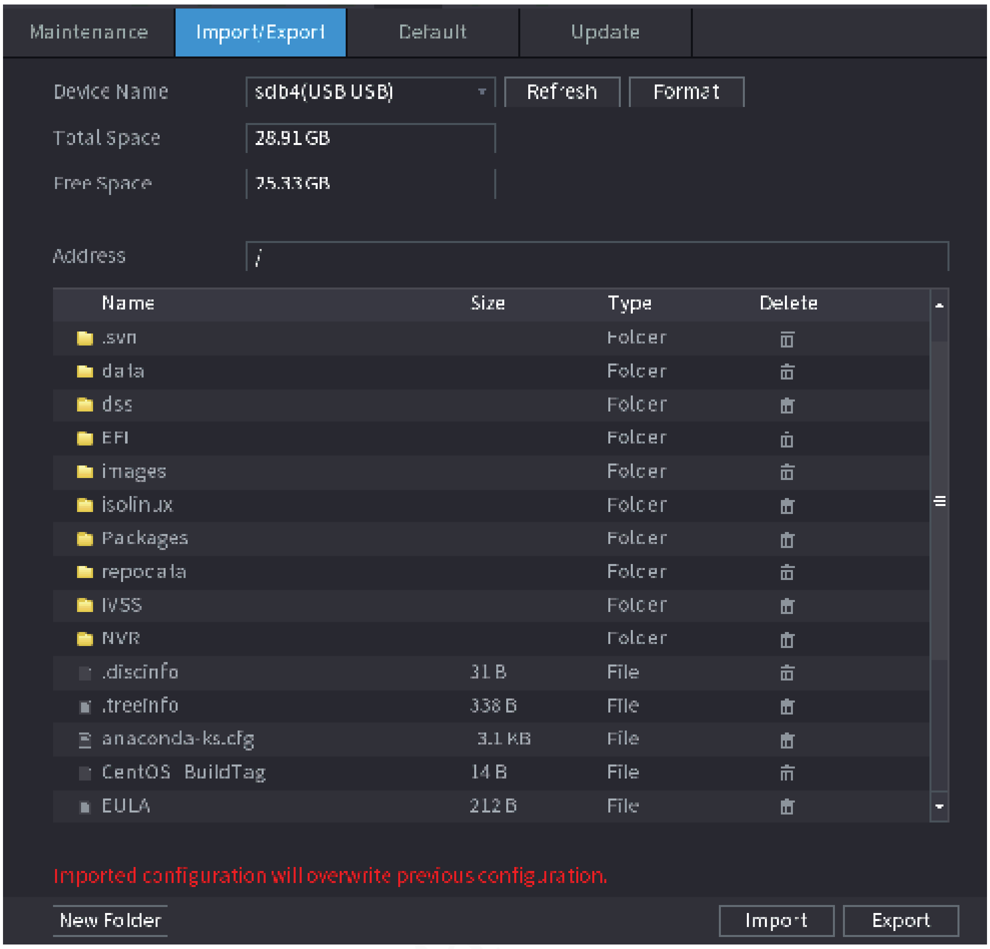
Imported configuration will overwrite previous configuration.

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 5-277 Connected USB device



Device Name: sdb4(USB USB)

Total Space: 28.91 GB

Free Space: 25.33 GB

Address: /

Name	Size	Type	Delete
.svn		Folder	🗑
data		Folder	🗑
dss		Folder	🗑
EFI		Folder	🗑
images		Folder	🗑
isolinux		Folder	🗑
Packages		Folder	🗑
repodata		Folder	🗑
IVSS		Folder	🗑
NVR		Folder	🗑
.discinfo	31 B	File	🗑
.treeinfo	338 B	File	🗑
anaconda-ks.cfg	3.1 KB	File	🗑
CentOS_BuildTag	14 B	File	🗑
EULA	212 B	File	🗑

Imported configuration will overwrite previous configuration.

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

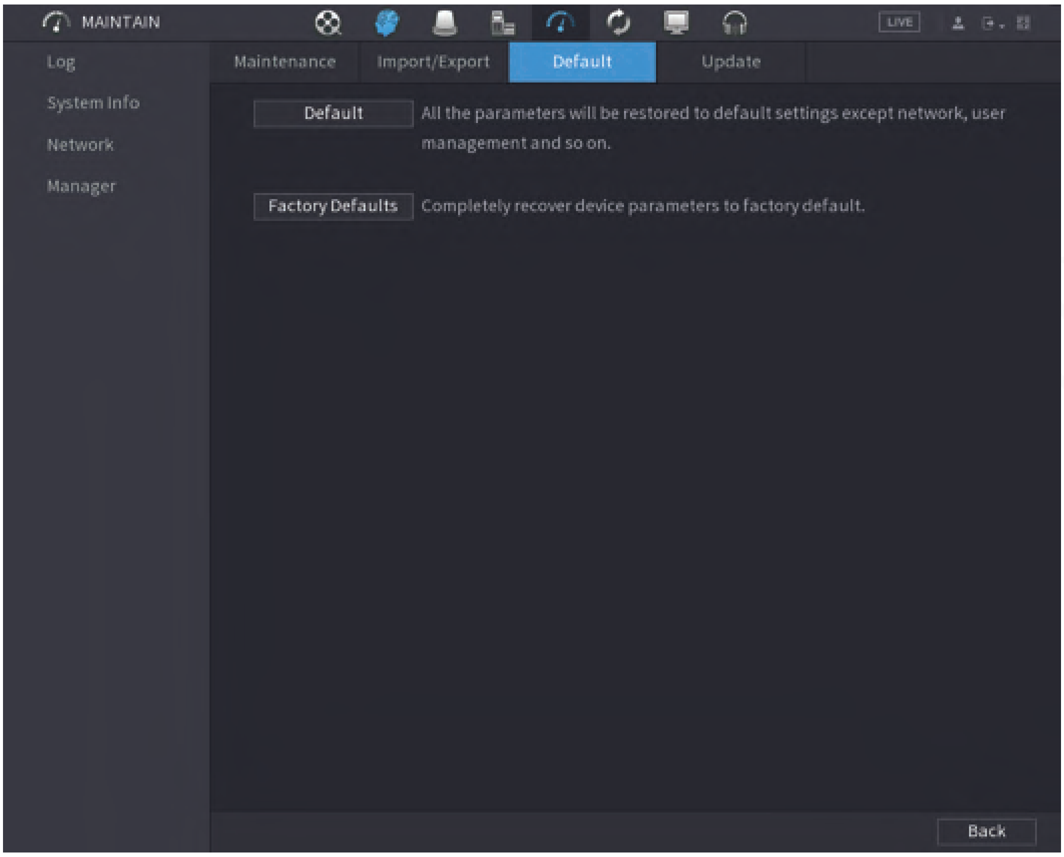
This function is for admin account only.

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

Procedure

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

Figure 5-278 Default



All the parameters will be restored to default settings except network, user management and so on.

Completely recover device parameters to factory 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.

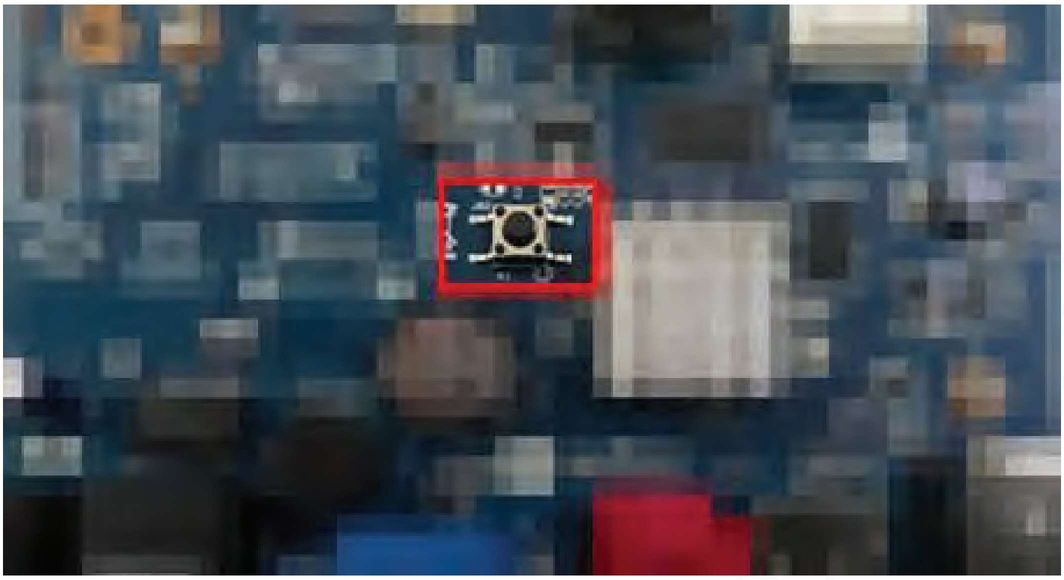
Procedure

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 5-279 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

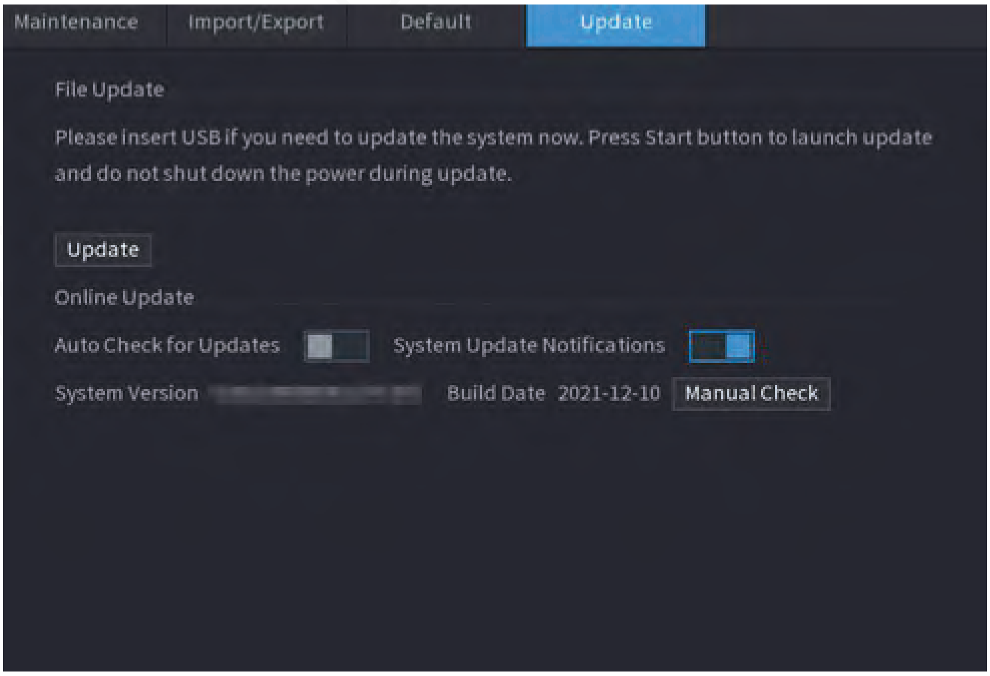
5.19.4.4.1 Upgrading File

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 5-280 Update



File Update

Please insert USB if you need to update the system now. Press Start button to launch update and do not shut down the power during update.

Online Update

Auto Check for Updates ○

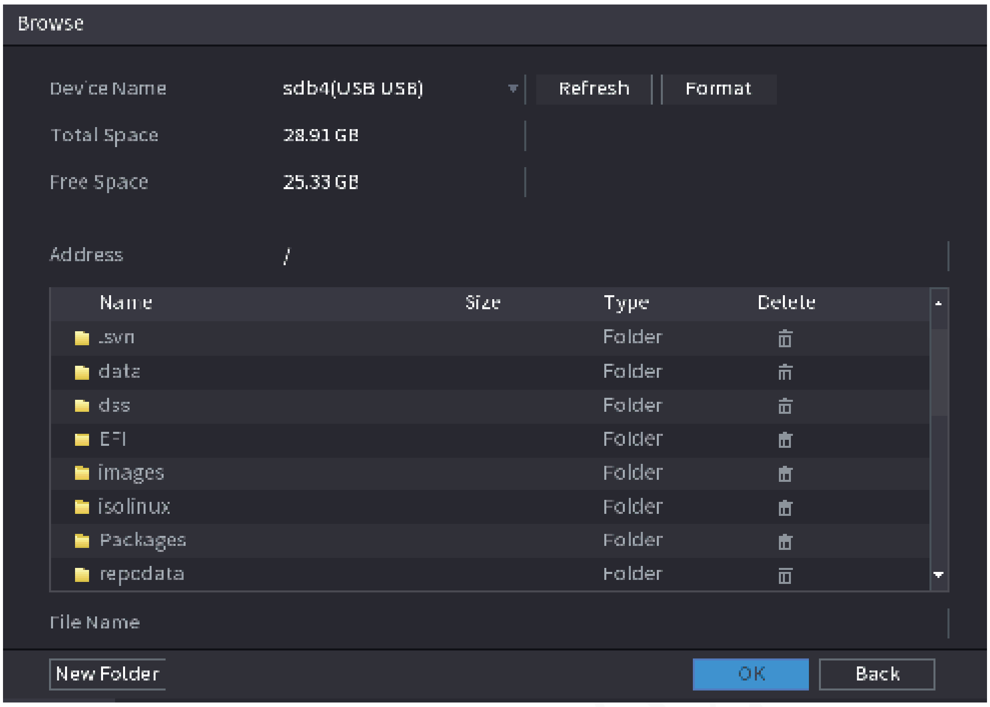
System Update Notifications ●

System Version [redacted]

Build Date 2021-12-10

Step 3 Click **Update**.

Figure 5-281 Browse



Device Name sdb4(USB USB)

Total Space 28.91 GB

Free Space 25.33 GB

Address /

Name	Size	Type	Delete
.svn		Folder	🗑
data		Folder	🗑
dss		Folder	🗑
EFI		Folder	🗑
images		Folder	🗑
isolinux		Folder	🗑
Packages		Folder	🗑
repodata		Folder	🗑

File Name

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.

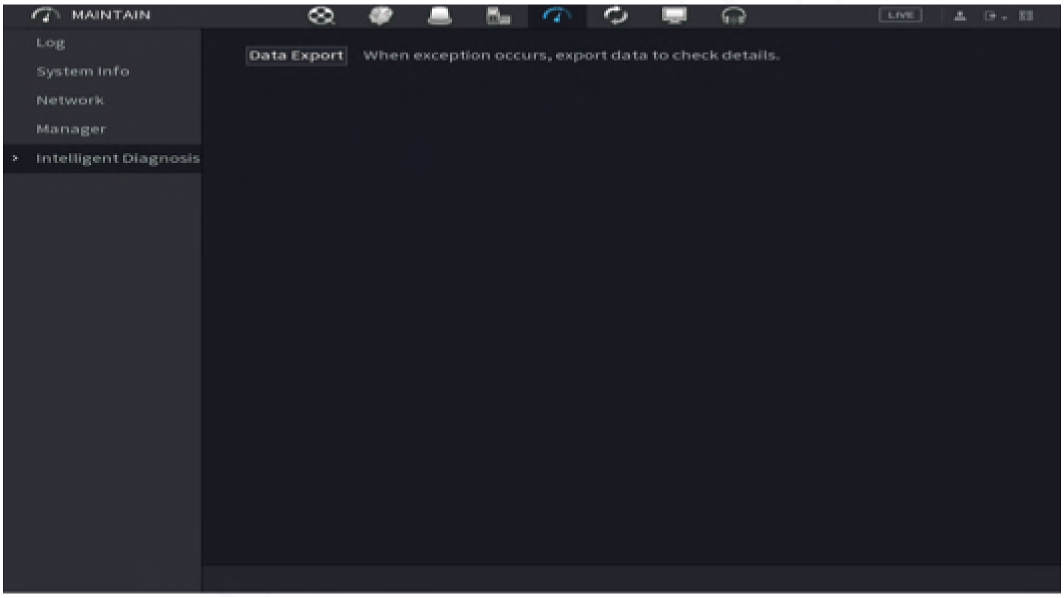
When starting the Device, the system automatically checkswhether there is a USB storage device connected and any upgrade file, and if yes and the check result of the upgrade file is correct, the system will upgrade automatically. The Uboot upgrade can avoid the situation that you have to upgrade through +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 5-282 Intelligent diagnosis



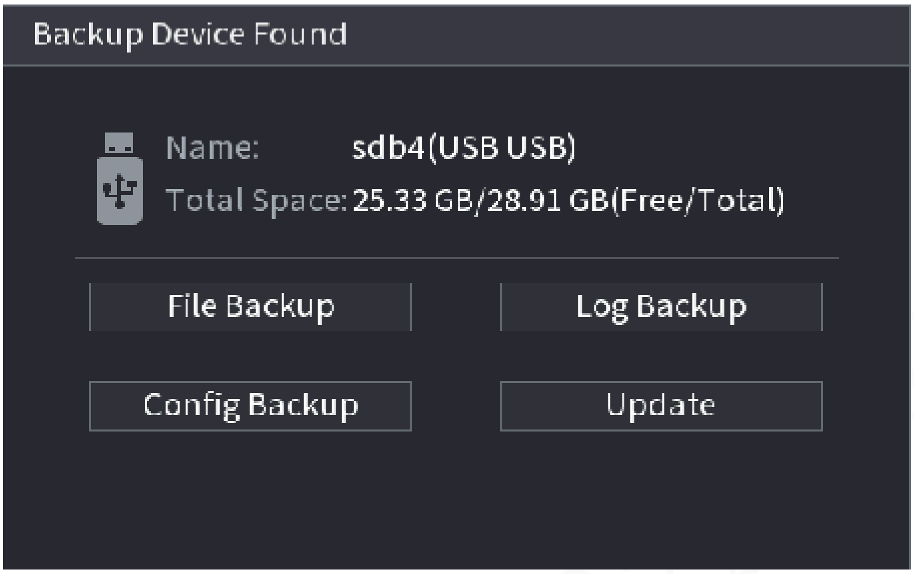
When exception occurs, export data to check details.

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 5-283 USB device prompt



Backup Device Found

Name: sdb4(USB USB)

Total Space: 25.33 GB/28.91 GB(Free/Total)

5.21 Shutdown

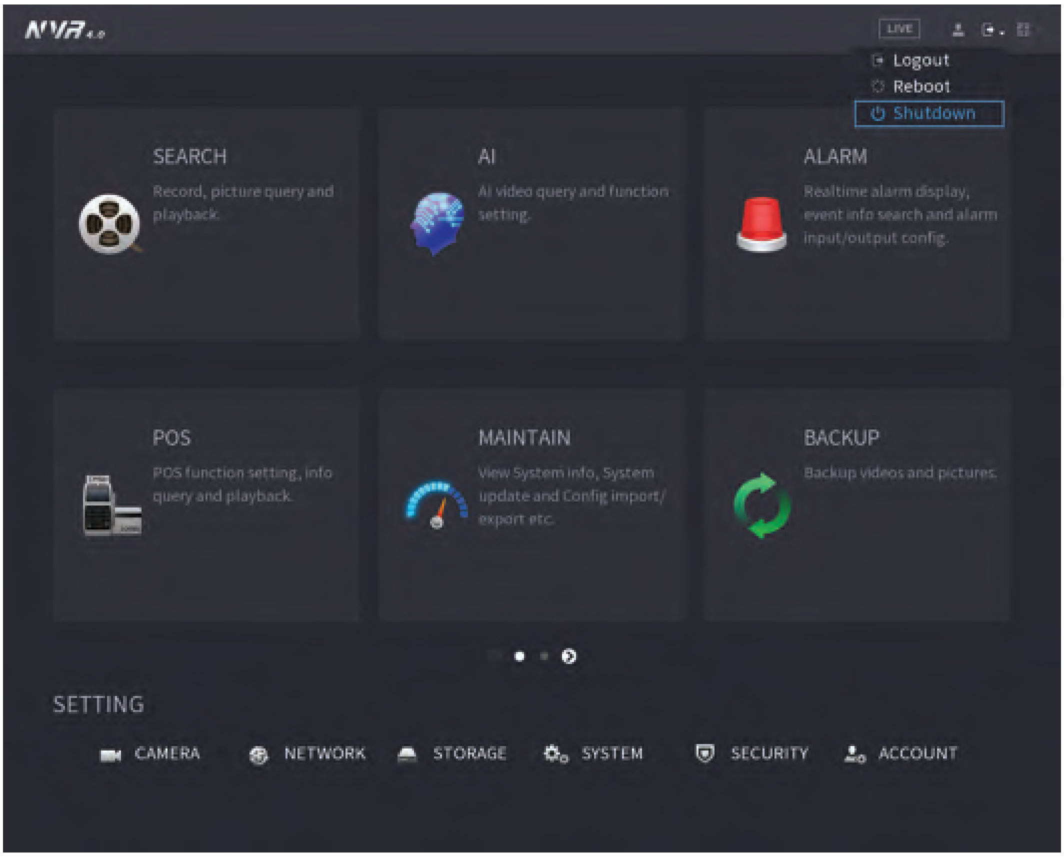
- When you see corresponding dialogue box "System is shutting down…" Do not click power on-off button directly.
- Do not unplug the power cable or click power on-off button to shutdown device directly when device is running (especially when it is recording.)
- Shut down the device and then unplug the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

Procedure

- From the main menu (Recommended)

1. Click ⏏ at the upper-right corner.

Figure 5-284 Shutdown (1)


NVR 4.0
LIVE
Logout
Reboot
Shutdown
SEARCH
Record, picture query and playback.
AI
AI video query and function setting.
ALARM
Realtime alarm display, event info search and alarm input/output config.
POS
POS function setting, info query and playback.
MAINTAIN
View System info, System update and Config import/ export etc.
BACKUP
Backup videos and pictures.
SETTING
CAMERA
NETWORK
STORAGE
SYSTEM
SECURITY
ACCOUNT

2. Select **Shutdown.**

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

Figure 5-285 Shutdown (2)

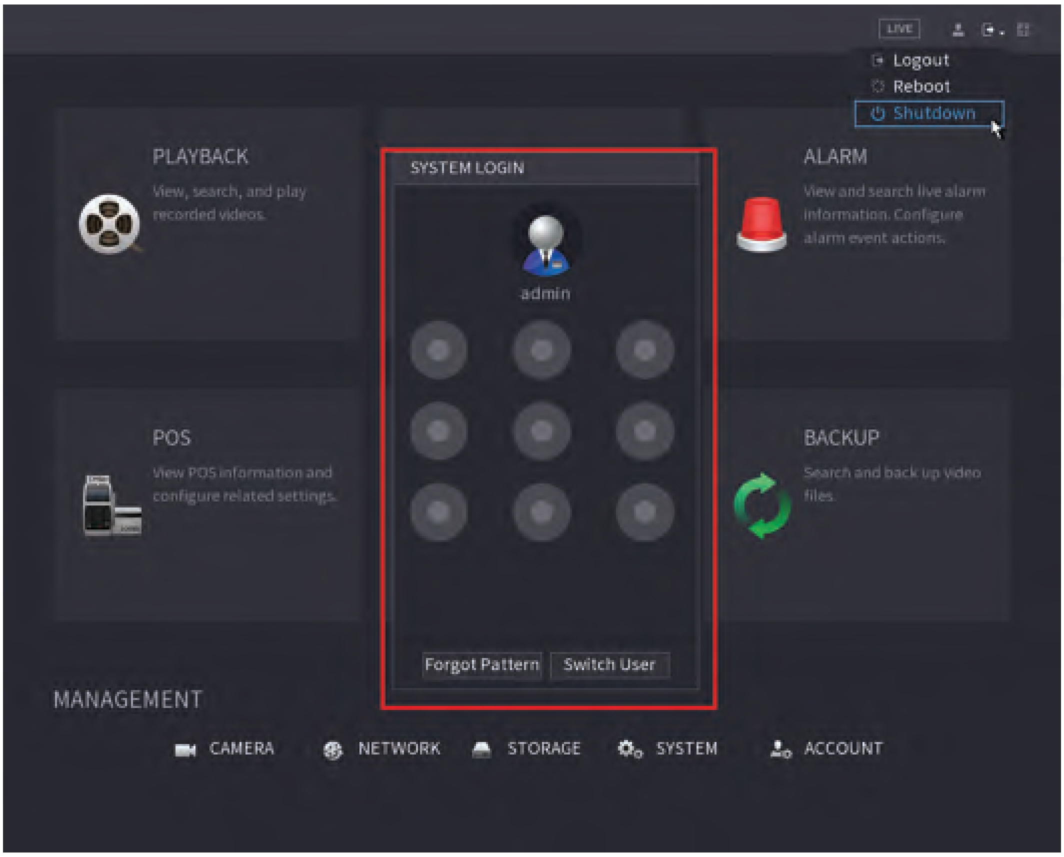
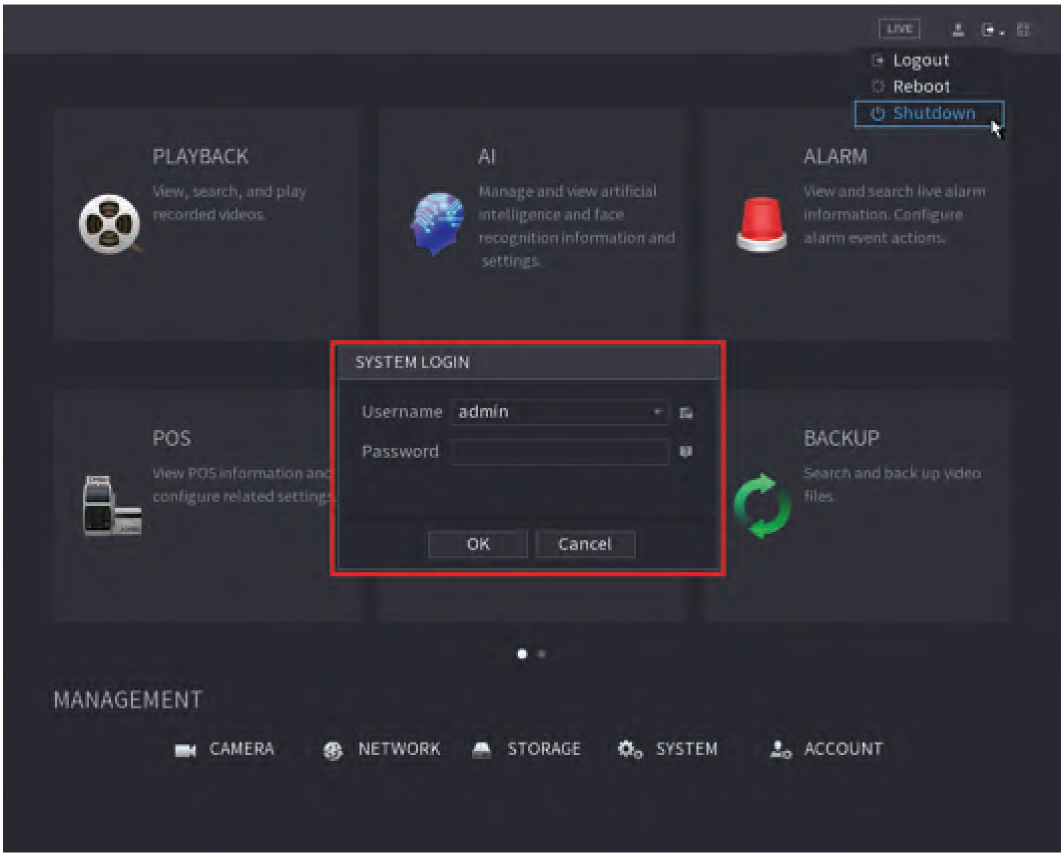

LIVE
Logout
Reboot
Shutdown
PLAYBACK
View, search, and play recorded videos.
SYSTEM LOGIN
admin
Forgot Pattern
Switch User
ALARM
View and search live alarm information. Configure alarm event actions.
POS
View POS information and configure related settings.
BACKUP
Search and back up video files.
MANAGEMENT
CAMERA
NETWORK
STORAGE
SYSTEM
ACCOUNT

Figure 5-286 Shutdown (3)


LIVE
Logout
Reboot
Shutdown
PLAYBACK
View, search, and play recorded videos.
AI
Manage and view artificial intelligence and face recognition information and settings.
ALARM
View and search live alarm information. Configure alarm event actions.
SYSTEM LOGIN
Username admin
Password
OK
Cancel
POS
View POS information and configure related settings.
BACKUP
Search and back up video files.
MANAGEMENT
CAMERA
NETWORK
STORAGE
SYSTEM
ACCOUNT

- 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.

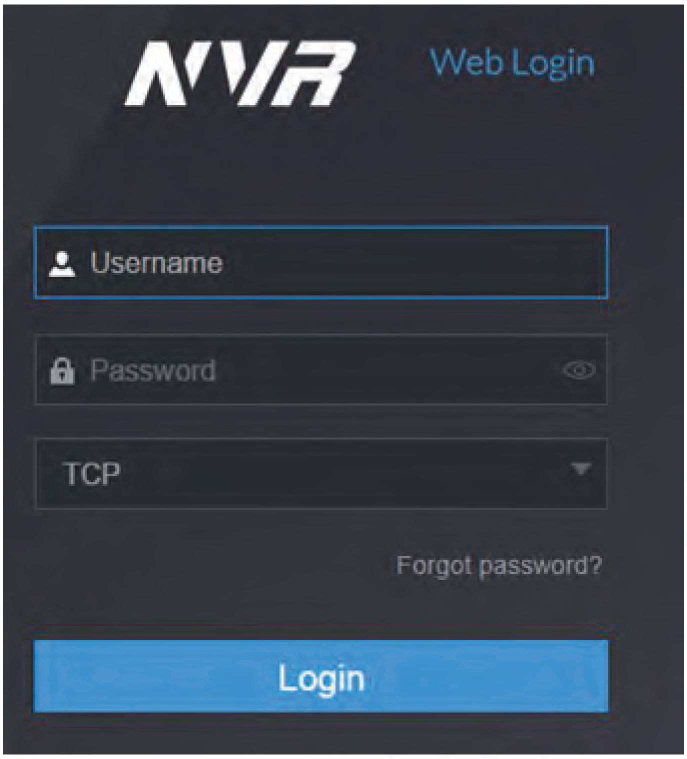
Step 2 Configure the IP address, subnet mask and gateway for the PC and the Device. For details about network configuration of the Device, see "5.19.3 Network".

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

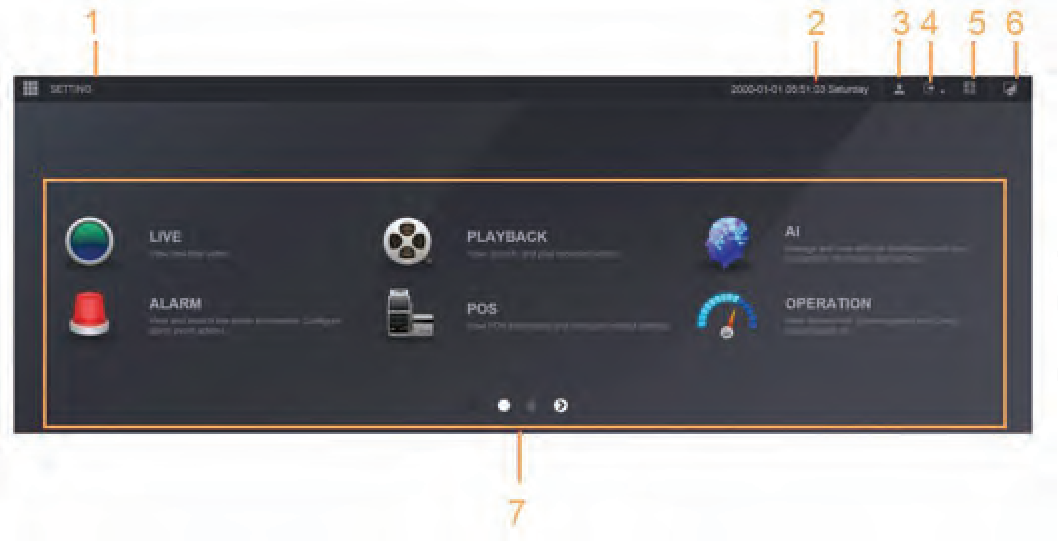


Table 6-1 Main menu symbols

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.

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

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.

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

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**.

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

In the formula:

c means total number of channels in one device

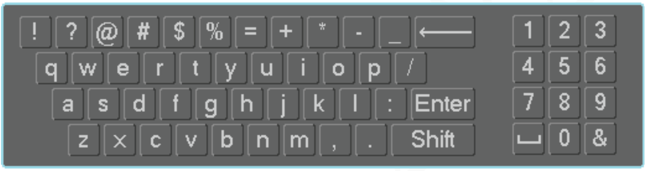
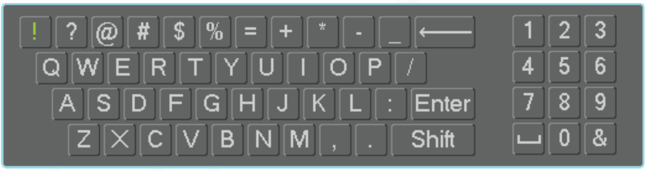
4. According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in device during **alarm video recording (including motion detection)**.

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

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

Appendix 2 Mouse Operation

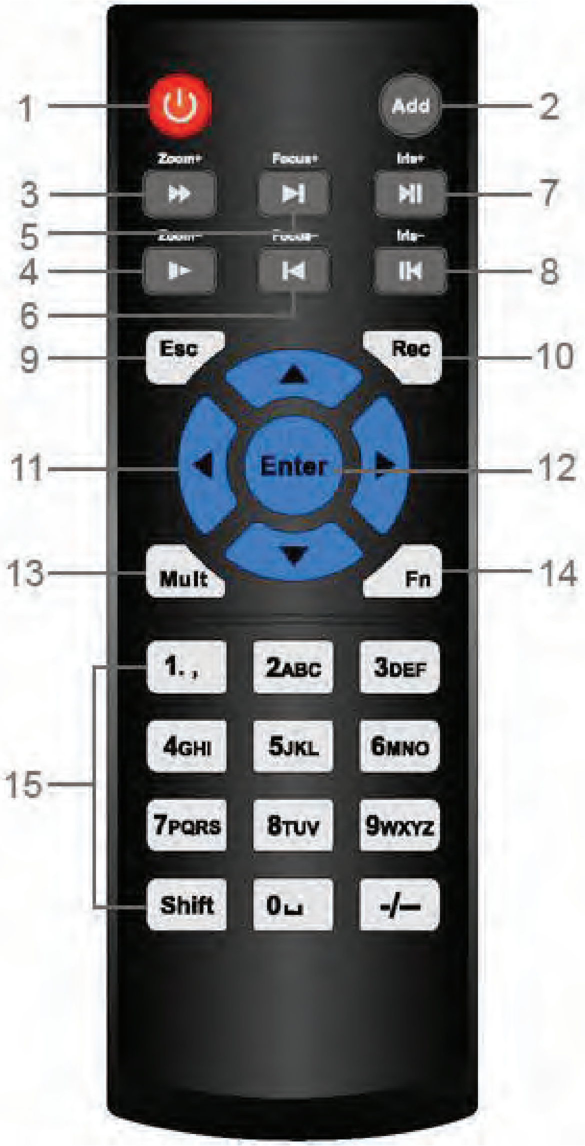
Appendix Table 2-1 Mouse operation

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.  ! ? @ # $ % = + * - _ ⟵ 1 2 3 q w e r t y u i o p / 4 5 6 a s d f g h j k l : Enter 7 8 9 z x c v b n m , . Shift ␣ 0 &  ! ? @ # $ % = + * - _ ⟵ 1 2 3 Q W E R T Y U I O P / 4 5 6 A S D F G H J K L : Enter 7 8 9 Z X C V B N M , . Shift ␣ 0 & 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.
6	Previous record	In playback state, press this button to play back the previous video.

No.	Name	Function
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.
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_0 130220	H264	√	ONVIF
	P5532-P	HEAD LFP4_0 130220	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

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	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
	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	XNETM1120111229	H264	√	ONVIF
	VIPBL1.3MIRVF	XNETM2100111229	H264	√	ONVIF
	IGC-2050F	XNETM2100111229	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	cp20111129ANS	H264	√	ONVIF
	CP-ND20-R	cp20111129ANS	H264	√	ONVIF
	CP-NS12W-CR	cp20110808NS	H264	√	ONVIF
	VS201	cp20111129NS	H264	√	ONVIF
	CP-NB20-R	cp20110808BNS	H264	√	ONVIF
	CP-NT20VL3-R	cp20110808BNS	H264	√	ONVIF
	CP-NS36W-AR	cp20110808NS	H264	√	ONVIF

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	CP-ND20VL2-R	cp20110808BNS	H264	√	ONVIF
	CP-RNP-1820	cp20120821NSA	H264	√	Private
	CP-RNC-TP20FL3C	cp20120821NSA	H264	√	Private
	CP-RNP-12D	cp20120828ANS	H264	√	Private
	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

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	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
	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

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	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
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

Manufacturer	Model	Version	Video Encode	Audio/Video	Protocol
	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
	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

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.

Legal and Regulatory Information

Legal Considerations

Video surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

Disclaimer

Every care has been taken in the preparation of this document. Please inform your nearest Dahua office of any inaccuracies or omissions. Dahua Technology shall not be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Dahua Technology makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Dahua Technology shall not be liable or responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights

Dahua Technology retains all intellectual property rights relating to technology embodied in the product described in this document.

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Trademark Acknowledgments

dahua , dahua TECHNOLOGY , HDCVI , imou are registered trademarks or trademark applications of Dahua Technology in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.

Regulatory Information

European Directives Compliance

CE This product complies with the applicable CE marking directives and standards:

- Low Voltage (LVD) Directive 2014/35/EU.
- Electromagnetic Compatibility (EMC) Directive 2014/30/EU.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU and its amending Directive (EU) 2015/863.

A copy of the original declaration of conformity may be obtained from Dahua

Technology.

The most up to date copy of the signed EU Declaration of Conformity (DoC) can be downloaded from: www.dahuasecurity.com/support/notice/

CE-Electromagnetic Compatibility (EMC)

This digital equipment is compliant with Class A according to EN 55032.

⚠Warning:

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

CE-Safety

This product complies with IEC/EN/UL 60950-1 or IEC/EN/UL 62368-1, Safety of Information Technology Equipment.

Declaration of Conformity CE

(Only for the product has RF function)

Hereby, Dahua Technology declares that the radio equipment is compliant with Radio Equipment Directive (RED) 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.dahuasecurity.com/support/notice/

USA Regulatory Compliance

FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

Attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC SDOC Statement can be downloaded from: https://us.dahuasecurity.com/support/notices/

RF exposure warning

(Only for the product has RF communication function)

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Canada Regulatory Compliance

ICES-003

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la Classe A est conforme à la norme NMB-003 du Canada.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF exposure warning

(Only for the product has RF communication function)

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Japan Regulatory Compliance

VCCI

These products comply with the requirements of VCCI Class A Information

Technology Equipment.

⚠**CAUTION**

This is a Class A equipment. Operation of this equipment in a residential environment could cause radio interference. In such a case, the user may be required to take corrective actions.

Batteries

Correct disposal of batteries in this product

This marking on the battery indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in Directive 2006/66/EC and its amending Directive 2013/56/EU. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.

⚠**CAUTION**

Do not ingest battery. Chemical Burn Hazard.

This product contains a coin cell battery. If the coin cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.

Keep new and used batteries away from children.

If the battery compartment does not close securely, stop using the product and keep it away from children.

If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.

⚠**CAUTION**

Risk of explosion if the battery is replaced by an incorrect type.

Do not throw or immerse into water, heat to more than 100℃(212℉), repair or disassemble, leave in an extremely low air pressure environment or extremely high-temperature environment, crush, puncture, cut or incinerate.

Dispose of the battery as required by local ordinances or regulations.

Safety

The product complies with IEC/EN/UL 60950-1, Information Technology Equipment – Safety – Part 1: General Requirements; or complies with IEC/EN/UL 62368-1, Audio/video, information and communication technology equipment – Part 1: Safety requirements.

If the power supply to the product is from external power adaptor without connecting to AC Mains, and the product is not shipped with power adaptor, customers are required to use the external power adaptor that must fulfill the requirements for Safety Extra Low Voltage (SELV) and Limited Power Source (LPS).

Waste Electrical and Electronic Equipment (WEEE) statements

Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.

This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should contact the product supplier for information about how to dispose of this product correctly.

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures, including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related jurisdictions. For detailed information, refer to the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Support

Should you require any technical assistance, please contact your Dahua distributor. If your questions cannot be answered immediately, your distributor will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:

- Download user documentation and software updates.
- Search by product, category, or phrase.
- Report problems to Dahua support staff by logging in to your private support area.
- Chat with Dahua support staff.
- Visit Dahua Support at www.dahuasecurity.com/support

Contact Information

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com

English

Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep it well for future reference.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Safety Requirement

- Abide by local electrical safety standards to ensure that the voltage is stable and complies with the power supply requirement of the device.
- Transport, use, and store the device under the allowed humidity and temperature conditions. Refer to the corresponding technical specifications of

device for specific working temperature and humidity.

- Do not place the device in a location exposed to dampness, dust, extreme hot or cold, strong electronic radiation, or unstable lighting condtions.
- Do not install the device in a place near the heat source, such as radiator, heater, furnace, or other heat generating device to avoid fire.
- Prevent liquid from flowing into the device to avoid damge to internal components.
- Install the device horizontally or install on the stable place to prevent it from falling.
- Install the device in a well-ventilated place, and do not block the ventilation of the device.
- Do not disassemble the device arbitrarily.
- Avoid heavy stress, violent vibration, and soaking during during transportation, storage, and installation. Complete package is necessary during the transportation.
- Use the factory package or the equivalent for transportation.

Battery

Low battery power affects the operation of the RTC, causing it to reset at every power-up. When the battery needs replacing, a log message will appear in the product’s server report. For more information about the server report, see the product´s setup pages or contact Dahua support.

⚠ WARNING

- Risk of explosion if the battery is incorrectly replaced.
- Replace only with an identical battery or a battery which is recommended by Dahua.
- Dispose of used batteries according to local regulations or the battery manufacturer's instructions.

Polski

Ważne środki ostrożności i ostrzeżenia

Niniejszy rozdział opisuje właściwe sposoby korzystania z urządzenia, sposoby zapobiegania zagrożeniom, a także sposoby zapobiegania uszkodzeniu mienia. Przed rozpoczęciem korzystania z urządzenia zapoznaj się dokładnie z tymi informacjami i zachowaj je na przyszłość do celów referencyjnych.

Instrukcje dot. bezpieczeństwa

W podręczniku mogą pojawić się następujące symbole. Ich znaczenie wyjaśnia poniższa tabela.

Symbol	Znaczenie
⚠ ZAGROŻENIE	Oznacza potencjalne zagrożenie wysokiego stopnia, którego nieuniknięcie może skutkować poważnymi urazami lub śmiercią.
⚠ OSTRZEŻENIE	Oznacza potencjalne zagrożenie średniego lub niskiego stopnia, którego nieuniknięcie może skutkować pomniejszymi lub średnimi urazami.
⚠ UWAGA	Oznacza potencjalne zagrożenie, którego nieuniknięcie może skutkować zniszczeniem mienia, utratą danych, spadkiem wydajności lub mieć inne nieprzewidziane skutki.

Symbol	Znaczenie
WSKAZÓWKI	Oznacza wskazówki pozwalające na rozwiązanie problemu lub oszczędność czasu.
UWAGA	Oznacza informacje uzupełniające tekst główny.

Wymogi dot. Bezpieczeństwa

- Przestrzegaj lokalnych standardów bezpieczeństwa elektrycznego celem upewnienia się, że źródło napięcia jest stabilne i zgodne z wymogami określonymi dla urządzenia.
- Urządzenie należy transportować, używać i przechowywać w warunkach o dozwolonym poziomie wilgotności i temperatury. Szczegółowe informacje na temat wilgotności i temperatury roboczej znaleźć można w odpowiedniej specyfikacji technicznej urządzenia.
- Nie umieszczaj urządzenia w miejscach narażonych na wilgoć, kurz, ekstremalne temperatury, silne promieniowanie elektroniczne oraz niestabilne warunki oświetleniowe.
- Nie instaluj urządzenia w pobliżu źródeł ciepła, takich jak kaloryfery, grzałki, piece bądź inne urządzenia generujące ciepło, aby zapobiegać wystąpieniu pożaru.
- Zabezpiecz urządzenie przed dostaniem się do jego wnętrza cieczy, ponieważ może to spowodować uszkodzenie komponentów wewnętrznych.
- Zamontuj urządzenie poziomo lub wybierz stabilne miejsce, tak aby wyeliminować ryzyko upadku.
- Zamontuj urządzenie w dobrze wentylowanym miejscu i upewnij się, że jego otwory wentylacyjne nie są zablokowane.
- Nie rozmontowuj urządzenia samodzielnie.
- Chroń urządzenie przed dużymi obciążeniami i naprężeniami, silnymi wibracjami oraz zalaniem zarówno podczas transportu, przechowywania, jak i montażu. Na potrzeby transportu wymagane jest korzystanie z kompletnego opakowania.
- Do transportu używaj oryginalnego opakowania lub innego zapewniającego podobny poziom ochrony.

Akumulator

Niski poziom naładowania akumulatora wpływa na działanie zegara czasu rzeczywistego, powodując jego resetowanie przy każdym włączeniu. Gdy akumulator wymaga wymiany, w raporcie serwerowym dla produktu pojawi się stosowna wiadomość. Aby uzyskać więcej informacji na temat raportu serwerowego, zapoznaj się z instrukcjami konfiguracji urządzenia lub skontaktuj się z personelem pomocy technicznej firmy Dahua.

⚠ OSTRZEŻENIE

- W przypadku niewłaściwej wymiany akumulatora występuje zagrożenie wybuchem.
- Akumulator należy zastępować wyłącznie takim samym typem lub innym typem zalecanym przez firmę Dahua.
- Akumulatory należy utylizować zgodnie z lokalnymi regulacjami lub instrukcjami producenta akumulatora.

Dansk

Vigtige sikkerhedsanvisninger og advarsler

Kapitlet beskriver korrekt håndtering af produktet, undgåelse af risici og undgåelse af skader på ejendom. Læs kapitlet omhyggeligt, før du bruger produktet, overhold alle anvisninger og advarsler under brugen, og gem kapitlet til senere brug.

Sikkerhedsanvisninger

Følgende signalord med beskrivelse kan forekomme i vejledningen.

Signalord	Beskrivelse
⚠ FARE	Angiver høj risiko, som, hvis den ikke undgås, kan medføre død eller alvorlig personskade.
⚠ ADVARSEL	Angiver middel eller lav risiko, som, hvis den ikke undgås, kan medføre lettere til moderat personskade.
⚠ FORSIGTIG	Angiver mulig risiko, som hvis den ikke undgås, kan resultere i skade på ejendom, tab af data, reduceret ydelse eller uforudsigelige resultater.
TIPS	Indeholder forslag, som hjælper dig med at løse et problem eller sparer tid.
BEMÆRK	Indeholder yderligere oplysninger, som understreger og supplerer teksten.

Sikkerhedskrav

- Følg lokale standarder for elsikkerhed for at sikre, at spændingen er stabil og i overensstemmelse med produktets krav til strømforsyning.
- Transportér, brug og opbevar produktet i henhold til de tilladte klimatiske forhold (temperatur og luftfugtighed). Se produktets tekniske specifikationer for specifik temperatur og luftfugtighed ved drift.
- Placér ikke produktet et sted med fugt, støv, stærk varme eller kulde, stærk elektronisk udstråling eller ustabile lysforhold.
- Installér ikke produktet i nærheden af en varmekilde, såsom en radiator, et varmeapparat, et centralfyr eller andre varmeafgivende enheder, for at undgå ildebrand.
- Undgå, at væske løber ind i produktet og dermed forårsager skade på de indvendige komponenter.
- Installér produktet vandret, eller installér det et stabilt sted for at undgå, at det falder ned.
- Installér produktet et sted med god udluftning, og blokér ikke produktets ventilationsåbninger.
- Adskil ikke produktet.
- Undgå stærkt tryk, kraftige vibrationer og gennemblødning under transport, opbevaring og installation. Produktet skal være fuldt emballeret under transport.
- Brug fabriksemballagen eller tilsvarende til transporten.

Batteri

Lav batterispænding påvirker driften af realtidsuret og får uret til at nulstille, hver gang produktet tændes. Der vises en logbesked i produktets serverrapport, når batteriet skal udskiftes. Se konfigurationssiderne til produktet, eller kontakt Dahuas supportteam for at få flere oplysninger om serverrapporten.

⚠ **ADVARSEL**

- Der er risiko for eksplosion, hvis batteriet udskiftes forkert.
- Udskift kun med et tilsvarende batteri eller et batteri, der anbefales af Dahua.

- Bortskaf brugte batterier i overensstemmelse med lokale bestemmelser eller batteriproducentens anvisninger.

Suomi

Tärkeitä varotoimenpiteitä ja varoituksia

Tässä luvussa kuvataan laitteen asianmukainen käsittely, vaarojen torjunta ja omaisuusvahinkojen estäminen. Lue tämä sisältö huolellisesti ennen laitteen käyttämistä ja noudata näitä ohjeita, kun käytät laitetta. Säilytä ohjeet tulevia tarpeita varten.

Turvallisuusohje

Seuraavat luokitellut huomiosanat kuvatulla merkityksellä saattavat esiintyä oppaassa.

Huomiosanat	Merkitys
⚠VAARA	Ilmaisee suuren potentiaalisen vaaran, joka johtaa kuolemaan tai vakavaan loukkaantumiseen, jos sitä ei vältetä.
⚠VAROITUS	Ilmaisee keskisuuren tai pienen potentiaalisen vaaran, joka saattaa johtaa lievään tai kohtalaiseen loukkaantumiseen, jos sitä ei vältetä.
⚠HUOMIO	Ilmaisee mahdollisen vaarallisen tilanteen, joka saattaa johtaa omaisuusvahinkoon, tietojen menetykseen, suoritustehon heikkenemiseen tai odottamattomiin tuloksiin, jos sitä ei vältetä.
🔑VINKIT	Tarjoavat apua ongelmien ratkaisemiseen tai säästävät aikaa.
📖HUOMAUTUS	Tarjoaa lisätietoa, joka korostaa tai täydentää tekstiä.

Turvallisuusvaatimus

- Noudata paikallisia sähköturvallisuusstandardeja varmistaaksesi, että jännite on vakaa ja vastaa laitteen virtalähteelle asetettuja vaatimuksia.
- Kuljeta, käytä ja säilytä laitetta sallituissa kosteus- ja lämpötilaolosuhteissa. Katso laitteen erityinen käyttölämpötila ja -kosteus laitteen vastaavista teknisistä tiedoista.
- Älä sijoita laitetta paikkaan, jossa se altistuu kosteudelle, pölylle, erittäin kuumalle tai kylmälle lämpötilalle, voimakkaalle sähkösäteilylle tai epävakaille valaistusolosuhteille.
- Älä asenna laitetta lähelle lämmönlähdettä, kuten lämpöpatteria, lämmitintä, uunia tai muuta lämpöä tuottavaa laitetta, tulipalon välttämiseksi.
- Vältä nesteen pääsemistä laitteen sisälle sisäisten komponenttien vahingoittumisen estämiseksi.
- Asenna laite vaakasuoraan tai asenna se vakaaseen paikkaan estääksesi sen kaatumisen.
- Asenna laite hyvin ilmastoituun paikkaan äläkä peitä laitteen tuuletusaukkoja.
- Älä pura laitetta omavaltaisesti.
- Vältä kovaa rasitusta, voimakasta tärinää ja kosteutta kuljetuksen, säilytyksen ja asennuksen aikana. Kuljetus vaatii täydellisen pakkaamisen.
- Käytä tehtaan pakkausta tai vastaavaa kuljetuksen aikana.

Paristo

Alhainen pariston varaustaso vaikuttaa tosiaikakellon (RTC:n) toimintaan nollaten sen jokaisella käynnistyskerralla. Lokiviesti ilmestyy tuotteen palvelinraporttiin, kun paristo on vaihdettava. Lisätietoa palvelinraportista saat tuotteen asetussivuilta tai ottamalla yhteyttä Dahuan tukeen.

⚠ **VAROITUS**

- Räjähdysvaara, jos paristo asetetaan väärin paikalleen.
- Vaihda vain samanlaiseen paristoon tai Dahuan suosittelemaan paristoon.
- Hävitä käytetyt paristot ja akut paikallisten määräysten tai valmistajan ohjeiden mukaisesti.

Magyar

Fontos óvintézkedések és figyelmeztetések

A jelen Fejezet leírja az Eszköz megfelelő kezelését, a veszélyek megelőzését és a vagyoni károk megelőzését. Az Eszköz használata előtt olvassa el figyelmesen, a használata során tartsa be, és őrizze meg jól jövőbeni hivatkozás céljára.

Biztonsági utasítások

Az Útmutatóban az alábbi meghatározott jelentéssel bíró kategorizált figyelmeztetések jelenhetnek meg.

Figyelmeztetés	Jelentés
⚠ **VESZÉLY**	Nagy potenciális veszélyt jelez, amely, ha nem kerüli el, halált vagy súlyos sérülést okoz.
⚠ **FIGYELEM**	Közepes vagy kis potenciális veszélyt jelez, amely, ha nem kerüli el, enyhe vagy mérsékelt sérülést okozhat.
⚠ **VIGYÁZAT**	Olyan potenciális kockázatot jelez, amely, ha nem kerüli el, vagyoni kárt, adatvesztést, alacsonyabb teljesítményt vagy kiszámíthatatlan eredményt okozhat.
🔑 **TIPPEK**	Olyan módszereket biztosít, amelyek segítenek megoldani a problémáját vagy időt takarítanak meg.
📖 **MEGJEGYZÉSEK**	További információkat biztosít a szöveg kiemelésével és kiegészítésével.

Biztonsági követelmények

- Tartsa be a helyi elektromos biztonsági szabványokat annak biztosítása érdekében, hogy a feszültség stabil és az eszköz áramellátási követelményének megfelelő legyen.
- Az eszközt a megengedett páratartalom és hőmérséklet viszonyok között szállítsa, használja, és tárolja. A konkrét üzemi hőmérsékletet és páratartalmat megtalálja az eszköz műszaki leírásában.
- Ne tegye az eszközt olyan helyre, ahol nedvességnek, pornak, rendkívüli melegnek vagy hidegnek, erős elektronikus sugárzásnak, vagy instabil fényviszonyoknak van kitéve.

- A tűz elkerülése érdekében ne telepítse az eszközt hőforrás, mint például radiátor, hősugárzó, kemence, vagy más hőtermelő eszköz közelében lévő helyre.
- A belső alkatrészek károsodásának elkerülése érdekében akadályozza meg, hogy folyadék folyjon az eszközbe.
- A leesésének megakadályozása érdekében az eszközt vízszintesen telepítse, vagy stabil helyre telepítse.
- Az eszközt jól szellőző helyre telepítse, és ne blokkolja az eszköz szellőzését.
- Önkényesen ne szerelje szét az eszközt.
- A szállítás, tárolás és telepítés során kerülje a nagy igénybevételt, erős rezgést, és az eláztatást. A szállítás során a teljes csomagolásra szükség van.
- A szállításhoz gyári csomagolást vagy azzal egyenértékűt használjon.

Elem

Az alacsony elem töltöttségi szint hatással van az RTC működésére, minden bekapcsoláskor alaphelyzetbe áll. Amikor az elemet cserélni kell, egy napló üzenet jelenik meg a termék szerver jelentésében. A szerver jelentésről további információkat talál a termék beállítási oldalain, vagy forduljon a Dahua támogatáshoz.

⚠ **FIGYELEM**

- Robbanásveszély, ha az elemet nem megfelelőre cseréli.
- Csak ugyanolyan elemre vagy a Dahua által ajánlott elemre cserélje.
- A használt elemet a helyi előírások vagy az elemgyártó utasításai szerint ártalmatlanítsa.

Български

Важни предпазни мерки и предупреждения

Тази глава описва инструкциите за правилна експлоатация на устройството, за предотвратяване на опасностите и материалните щети. Прочетете внимателно тези инструкции, преди да използвате устройството, спазвайте ги при използването на устройството, и ги запазете за бъдещи справки.

Инструкции за безопасност

Ръководството съдържа следните определени сигнални думи.

Сигнални думи	Значение
⚠ **ОПАСНОСТ**	Показва висока потенциална опасност, която, ако не бъде избегната, ще доведе до смърт или сериозно нараняване.
⚠ **ПРЕДУПРЕЖДЕНИЕ**	Показва средна или ниска потенциална опасност, която, ако не бъде избегната, може да доведе до леки или умерени наранявания.
⚠ **ВНИМАНИЕ**	Посочва потенциален риск, който, ако не бъде избегнат, може да доведе до материални щети, загуба на данни, по-ниска производителност или непредсказуем резултат.

Сигнални думи	Значение
СЪВЕТИ	Обозначава начини, които да ви помогнат да разрешите проблем или да спестите време.
ЗАБЕЛЕЖКА	Предоставя допълнителна информация като акцент и допълнение към основния текст.

Изисквания за безопасност

- Спазвайте местните стандарти за електрическа безопасност, за да осигурите стабилно напрежение, отговарящо на изискването за захранване на устройството.
- Транспортирайте, използвайте и съхранявайте устройството при указаните условия на влажност и температура. Направете справка в съответните технически спецификации на устройството за конкретната работна температура и влажност.
- Не поставяйте устройството на място, изложено на влага, прах, много висока или ниска температура, със силно електронно излъчване или на място с променливо осветление.
- Не поставяйте устройството близо до източник на топлина, като радиатор, нагревател, пещ или друго устройство за генериране на топлина, за да избегнете пожар.
- Не допускайте в устройството да попадне течност, за да не се повредят вътрешните компоненти.
- Монтирайте устройството хоризонтално или го поставете на стабилно място, за да не падне.
- Монтирайте устройството на добре проветриво място и не блокирайте вентилацията на устройството.
- Не разглобявайте устройството произволно.
- Избягвайте силно натоварване, вибрации и намокряне по време на транспортиране, съхранение и монтаж. При транспортиране следва да се опакова напълно.
- Използвайте за транспортиране фабричната опаковка или подобна.

Батерия

Ниската мощност на батерията влияе на работата на часовника в реално време (RTC), което води до нулиране при всяко включване. Когато батерията трябва да бъде сменена, в отчета на сървъра на продукта ще се покаже съобщение. За повече информация относно отчета на сървъра вижте страниците за настройка на продукта или се свържете с екипа на Dahua.

⚠ **ПРЕДУПРЕЖДЕНИЕ**

- Ако батерията е неправилно подменена, има риск от експлозия.
- Сменяйте само със същата или батерия, препоръчана от Dahua.
- Изхвърляйте използваните батерии в съответствие с местните разпоредби или инструкциите на производителя на батерията.

Românesc

Masuri de siguranta si Atentionari

Acest capitol descrie indicatiile de utilizare corecta a Dispozitivului , prevenirea pericolului si prevenirea distrugerii proprietatii.Cititi aceste randuri inaintea folosirii

Dispozitivului

Instructiuni de siguranta

Urmatoarele semne categorizate pot aparea in Ghid.

Signal Words	Meaning
PERICOL	Indică un risc potențial ridicat care, dacă nu este evitat, va duce la deces sau vătămări grave.
AVERTIZARE	Indică un pericol potențial mediu sau scăzut care, dacă nu este evitat, poate duce la răni ușoare sau moderate.
ATENTIE	Indică un risc potențial care, dacă nu este evitat, ar putea duce la daune materiale, pierderi de date, performanțe mai scăzute sau rezultate imprevizibile.
SFATURI	Oferă metode care să vă ajute să rezolvați o problemă sau să economisiți timp.
NOTA	Oferă informații suplimentare ca accent și supliment la text.

Cerinte de siguranta

- Respectați standardele locale de siguranță electrică pentru a vă asigura că tensiunea este stabilă și respectă cerințele de alimentare ale dispozitivului.
- Transportați, utilizați și depozitați dispozitivul sub condițiile de umiditate și temperatură admise. Consultați specificațiile tehnice corespunzătoare ale dispozitivului pentru temperatură și umiditate specifice de lucru.
- Nu așezați dispozitivul într-o locație expusă la umezeală, praf, extrem de caldă sau rece, de radiații electronice puternice sau de condiții de iluminare instabile.
- Nu instalați dispozitivul într-un loc în apropierea sursei de căldură, cum ar fi radiatorul, încălzitorul, cuptorul sau alt dispozitiv generator de căldură, pentru a evita incendiul.
- Împiedicați curgerea lichidului în dispozitiv pentru a evita deteriorarea componentelor interne.
- Instalați dispozitivul în poziție orizontală sau instalați-l pe un loc stabil pentru a preveni căderea acestuia.
- Instalați aparatul într-un loc bine ventilat și nu blocați ventilația aparatului.
- Nu dezasamblați dispozitivul voit.
- Evitați loviturile puternice, vibrațiile violente și umiditatea în timpul transportului, depozitării și instalării. Este necesar un pachet complet în timpul transportului.
- Utilizati pachetul de fabrica sau echvalent in timpul transportului.

Bateriile

Puterea redusă a bateriei afectează funcționarea RTC, determinând resetarea la fiecare pornire. Când bateria are nevoie de înlocuire, în raportul serverului produsului va apărea un mesaj de jurnal. Pentru mai multe informații despre raportul serverului, consultați paginile de configurare ale produsului sau contactați asistența Dahua.

⚠ **AVERTIZARE**

- Risc de explozie dacă bateria este înlocuită incorect.
- Înlocuiți numai cu o baterie identică sau cu o baterie recomandată de Dahua.
- Aruncați bateriile uzate în conformitate cu reglementările locale sau cu instrucțiunile producătorului bateriei.

Čeština

Důležitá bezpečnostní opatření a varování

Tato kapitola popisuje obsah vztahující se na správnou manipulaci se zařízením, prevenci nebezpečí a prevenci škod na majetku. Pečlivě si tyto informace pročtěte před použitím zařízení, během používání zařízení je dodržujte a uschovejte je pro budoucí použití.

Bezpečnostní pokyny

Tato příručka může obsahovat následující kategorie signálních slov.

Signální slova	Význam
⚠ NEBEZPEČÍ	Označuje možnost závažného nebezpečí, které, pokud by mu nebylo zamezeno, může mít za následek smrt nebo vážné zranění.
⚠ VAROVÁNÍ	Označuje možnost středně nebo málo závažného nebezpečí, které, pokud by mu nebylo zamezeno, může mít za následek lehké nebo nepříliš závažné zranění.
⚠ UPOZORNĚNÍ	Označuje možné riziko, které, pokud by mu nebylo zamezeno, může mít za následek škodu na majetku, ztrátu dat, snížení výkonu nebo neočekávaný výsledek.
TIPY	Uvádí metody, které vám pomohou vyřešit problém nebo vám ušetří čas.
POZNÁMKA	Poskytuje dodatečné informace formou důrazu a doplnění textu.

Bezpečnostní požadavek

- Dodržujte místní normy pro elektrickou bezpečnost pro zajištění stabilního napětí a dodržení požadavků na napájení zařízení.
- Zařízení přepravujte, používejte a skladujte při odpovídající teplotě a vlhkosti. Konkrétní pracovní teplotu a vlhkost naleznete v příslušných technických specifikacích zařízení.
- Neumísťujte zařízení tam, kde bude vystaveno vlhkosti, prachu, extrémnímu horku nebo chladu, silnému elektronickému záření nebo nestabilním světelným podmínkám.
- Neinstalujte zařízení v blízkosti zdrojů tepla, jako je radiátor, ohřívač, kotel nebo jiné zařízení generující teplo, aby nedošlo k požáru.
- Zamezte proniknutí kapalin do zařízení, aby nedošlo k poškození jeho vnitřních součástí.
- Zařízení instalujte vodorovně nebo je instalujete na stabilním místě, aby bylo chráněno před pádem.

- Zařízení instalujte na dobře větraném místě a neblokujte odvětrávání zařízení.
- Zařízení svévolně nedemontujte.
- Během přepravy, skladování a instalace zamezte silnému tlaku, prudkým vibracím a namočení. Při přepravě je nezbytné úplné zabalení.
- Při přepravě použijte obal z výroby nebo obdobný obal.

Baterie

Nízké nabití baterie ovlivňuje fungování hodin ve skutečném čase a způsobuje, že se při každém spuštění resetují. V případě, že je třeba baterii vyměnit, se v serverové zprávě produktu zobrazí zpráva protokolu. Další informace o serverové zprávě naleznete na stránkách o nastavení produktu, případně kontaktujte podporu společnosti Dahua.

⚠ **VAROVÁNÍ**

- Nebezpečí výbuchu v případě nesprávné výměny baterie.
- Vyměňte pouze za totožnou baterii nebo baterii doporučenou společností Dahua.
- Použité baterie likvidujte v souladu s místními předpisy nebo pokyny výrobce baterie.

Ελληνικά

Σημαντικές Διασφαλίσεις και Προειδοποιήσεις

Αυτό το Κεφάλαιο περιγράφει το περιεχόμενο που καλύπτει το σωστό χειρισμό της Συσκευής, την πρόληψη των κινδύνων και την πρόληψη της καταστροφής της ιδιοκτησίας. Διαβάστε προσεκτικά τα αναγραφόμενα πριν χρησιμοποιήσετε τη Συσκευή, τηρήστε τα κατά τη χρήση και κρατήστε τα καλά για μελλοντική χρήση.

Οδηγίες Ασφαλείας

Τα ακόλουθα κατηγοριοποιημένα σήματα με λέξεις έχουν καθορισμένη σημασία και ενδέχεται να εμφανίζονται στις Οδηγίες Χρήσης.

Σήματα με λέξεις	**Σημασία**
⚠ ΚΙΝΔΥΝΟΣ	Δείχνει έναν υψηλό δυνητικό κίνδυνο, ο οποίος, εάν δεν αποφευχθεί, θα έχει ως αποτέλεσμα θάνατο ή σοβαρό τραυματισμό.
⚠ ΠΡΟΕΙΔΟΠΟΙΗΣΗ	Υποδεικνύει έναν μεσαίο ή χαμηλό δυνητικό κίνδυνο, ο οποίος, αν δεν αποφευχθεί, θα μπορούσε να προκαλέσει ελαφρύ ή μέτριο τραυματισμό.
⚠ ΠΡΟΣΟΧΗ	Δείχνει έναν πιθανό κίνδυνο, ο οποίος, εάν δεν αποφευχθεί, θα μπορούσε να προκαλέσει ζημιά στην ιδιοκτησία, απώλεια δεδομένων, χαμηλότερη απόδοση ή απρόβλεπτο αποτέλεσμα.

Σήματα με λέξεις	Σημασία
ΣΥΜΒΟΥΛΕΣ	Παρέχει μεθόδους που θα σας βοηθήσουν να επιλύσετε ένα πρόβλημα ή να εξοικονομήσετε χρόνο.
ΣΗΜΕΙΩΣΗ	Παρέχει πρόσθετες πληροφορίες δίνοντας έμφαση και συμπληρώνοντας το κείμενο.

Απαιτήσεις ασφαλείας

- Τηρήστε τα τοπικά πρότυπα ηλεκτρικής ασφάλειας για να βεβαιωθείτε ότι η τάση είναι σταθερή και συμμορφώνεται με την απαίτηση τροφοδοσίας της συσκευής.
- Μεταφέρετε, χρησιμοποιήστε και αποθηκεύστε τη συσκευή υπό τις επιτρεπόμενες συνθήκες υγρασίας και θερμοκρασίας. Ανατρέξτε στις αντίστοιχες τεχνικές προδιαγραφές της συσκευής για τη συγκεκριμένες συνθήκες λειτουργίας θερμοκρασίας και υγρασίας.
- Μην τοποθετείτε τη συσκευή σε θέση που είναι εκτεθειμένη σε υγρασία, σκόνη, ακραία ζέστη ή κρύο, ισχυρή ηλεκτρονική ακτινοβολία ή ασταθές φωτισμό.
- Μην τοποθετείτε τη συσκευή σε μέρος κοντά στην πηγή θερμότητας, όπως καλοριφέρ, θερμάστρα, κλίβανο ή άλλη συσκευή παραγωγής θερμότητας για να αποφύγετε τη φωτιά.
- Αποφύγετε να ρέει υγρό μέσα στη συσκευή για να αποφύγετε την αποδυνάμωση των εσωτερικών εξαρτημάτων.
- Εγκαταστήστε τη συσκευή οριζόντια ή εγκαταστήστε την στο σταθερό μέρος για να μην πέσει.
- Τοποθετήστε τη συσκευή σε καλά αεριζόμενο μέρος και μην εμποδίζετε τον εξαερισμό της συσκευής.
- Μην αποσυναρμολογείτε αυθαίρετα τη συσκευή.
- Αποφύγετε την υψηλή συμπίεση, το υψηλό βάρος, τη βίαιη δόνηση και τη διαβροχή κατά τη διάρκεια της μεταφοράς, της αποθήκευσης και της εγκατάστασης. Το πλήρες πακέτο είναι απαραίτητο κατά τη μεταφορά.
- Χρησιμοποιήστε το εργοστασιακό πακέτο ή το αντίστοιχο για μεταφορά.

Μπαταρία

Η χαμηλή ισχύς της μπαταρίας επηρεάζει τη λειτουργία του RTC, προκαλώντας την επαναφορά του σε κάθε επανεκκίνηση. Όταν η μπαταρία χρειάζεται αντικατάσταση, ένα μήνυμα συμβάντος θα εμφανιστεί στην αναφορά συμβάντων του διακομιστή. Για περισσότερες πληροφορίες σχετικά με την αναφορά διακομιστή, ανατρέξτε στις σελίδες εγκατάστασης του προϊόντος ή επικοινωνήστε με την υποστήριξη Dahua.

⚠ ΠΡΟΕΙΔΟΠΟΙΗΣΗ

- Κίνδυνος έκρηξης σε περίπτωση λανθασμένης αντικατάστασης της μπαταρίας.
- Αντικαταστήστε μόνο με πανομοιότυπη μπαταρία ή μπαταρία που συνιστάται από τη Dahua.
- Απορρίψτε τις χρησιμοποιημένες μπαταρίες σύμφωνα με τους τοπικούς κανονισμούς ή τις οδηγίες του κατασκευαστή της μπαταρίας.

hrvatski

Važne zaštitne mjere i upozorenja

Ovo poglavlje opisuje sadržaj koji obuhvaća pravilno rukovanje uređajem, sprječavanje opasnosti i sprečavanje oštećenja imovine. Pažljivo pročitajte ove sadržaje prije korištenja Uređaja, pridržavajte ih se pri upotrebi i sačuvajte ih za buduću uporabu.

Sigurnosne upute

U vodiču se mogu pojaviti sljedeće kategorizirane signalne riječi s definiranim značenjem.

Signal Words	Meaning
⚠ **OPASNOST**	Označava veliku potencijalnu opasnost koja će, ako se ne izbjegne, rezultirat smrću ili ozbiljnim ozljedama.
⚠ **UPOZORENJE**	Označava srednju ili malu potencijalnu opasnost koja, ako se ne izbjegne, može rezultirati malom ili umjerenom ozljedom.
⚠ **OPREZ**	Ukazuje na potencijalni rizik koji, ako se ne izbjegne, može rezultirati oštećenjem imovine, gubitkom podataka, manjom učinkovitošću ili nepredvidivim rezultatom.
🔑 **SAVJETI**	Pruža vam metode kojim vam pomaže riješiti problem ili će vam uštedjeti vrijeme.
📖 **BILJEŠKA**	Pruža dodatne informacije kao naglasak i dopunu teksta.

Sigurnosni zahtjevi

- Avoid heavy stress, violent vibration, and soaking during during transportation, storage, and installation. Complete package is necessary during the transportation.
- Pridržavajte se lokalnih električnih sigurnosnih standarda kako biste osigurali da je napon stabilan i da udovoljava zahtjevima napajanja uređaja.
- Prijenosite, upotrebljavajte i pohranjujte uređaj pod dopuštenim uvjetima vlage i temperature. Pogledajte odgovarajuće tehničke specifikacije uređaja za određenu radnu temperaturu i vlagu.
- Nemojte postavljati uređaj na mjesto izloženo vlazi, prašini, ekstremno vrućoj ili hladnoj okolini, jakom elektronskom zračenju ili nestabilnim uvjetima osvjetljenja.
- Kako biste izbjegli požar nemojte postavljati uređaj na mjesto u blizini izvora topline, kao što su radijator, grijač, peć ili neki drugi uređaj za stvaranje topline.
- Spriječite da tekućina teče u uređaj kako bi se izbjegla šteta na unutarnjim dijelovima.
- Ugradite uređaj vodoravno ili ga postavite na stabilno mjesto kako biste spriječili padanje.
- Ugradite uređaj na dobro prozračeno mjesto i ne blokirajte ventilaciju uređaja.
- Nemojte rastavljati uređaj samovoljno.
- Izbjegavajte teški stres, nasilne vibracije i natapanje tijekom prijevoza, skladištenja i instalacije. Prilikom prijevoza potrebno je koristiti tvorničko

zaštitno pakiranje.
- Koristite tvorničko pakiranje ili ekvivalent za transport.

Baterija

Niska baterija utječe na rad RTC, uzrokujući da se resetira pri svakom uključivanju. Kad bateriju treba zamijeniti, pojaviti će se poruka u izvješću poslužitelja (server). Dodatne informacije o izvješću poslužitelja (server) potražite na stranicama priručnika proizvoda ili se obratite Dahua podršci.

⚠ **UPOZORENJE**

- Rizik od eksplozije ako se baterija nepravilno zamijeni.
- Zamijeniti samo sa jednakom baterijom ili sa baterijom koja je preporučena od strane Dahua Technology.
- instructions. Dotrajale baterije trba zbrinuti u skladu sa lokalnim propisima ili u skladu s uputama proizvođača baterije.

Slovenčina

Dôležité bezpečnostné pokyny a varovania

Táto kapitola obsahuje informácie týkajúce sa správnej manipulácie so zariadením, prevencie pred nebezpečenstvom a prevencie poškodenia majetku. Pred používaním zariadenia si pozorne prečítajte tieto informácie, dodržiavajte ich pri používaní a uchovajte ich na budúce použitie.

Bezpečnostné pokyny

V príručke sa môžu nachádzať nasledujúce kategorizované signálne výrazy s definovaným významom.

Signálne výrazy	Význam
⚠ **NEBEZPEČENSTVO**	Označuje vysoké potenciálne nebezpečenstvo, ktoré spôsobí smrť alebo vážne zranenie, ak sa mu nevyhnete.
⚠ **VAROVANIE**	Označuje stredné alebo nízke potenciálne nebezpečenstvo, ktoré môže mať za následok mierne alebo stredne ťažké zranenie, ak sa mu nevyhnete.
⚠ **POZOR**	Označuje potenciálne riziko, ktoré môže viesť k poškodeniu majetku, strate údajov, zníženiu výkonu alebo nepredvídateľnému výsledku, ak sa mu nevyhnete.
🔑 **TIPY**	Poskytuje metódy, ktoré vám pomôžu vyriešiť problém alebo ušetriť čas.
📖 **POZNÁMKA**	Poskytuje ďalšie informácie ako zdôraznenie a doplnenie textu.

Požiadavky na bezpečnosť

- Dodržujte miestne elektrické bezpečnostné normy, aby ste zabezpečili, že napätie je stabilné a zodpovedá požiadavkám na napájanie zariadenia.
- Zariadenie prepravujte, používajte a uchovávajte pri povolených podmienkach

vlhkosti a teploty. Prečítajte si príslušné technické špecifikácie zariadenia pre špecifickú pracovnú teplotu a vlhkosť.

- Zariadenie neumiestňujte na miesto vystavené vlhkosti, prachu, extrémnemu teplu alebo chladu, silnému elektronickému žiareniu alebo nestabilným podmienkam osvetlenia.
- Zariadenie neinštalujte na miesto, ktoré sa nachádza blízko zdroja tepla, ako je napríklad radiátor, ohrievač, pec alebo iné zariadenie na tvorbu tepla. Predídete tak vzniku požiaru.
- Zabráňte vnikaniu kvapaliny do zariadenia, aby nedošlo k poškodeniu vnútorných komponentov.
- Zariadenie nainštalujte horizontálne alebo ho nainštalujte na stabilné miesto, aby ste zabránili pádu.
- Zariadenie nainštalujte na dobre vetranom mieste a neblokujte ventiláciu zariadenia.
- Zariadenie svojvoľne nerozoberajte.
- Počas prepravy, skladovania a inštalácie sa vyhnite silnému namáhaniu, prudkým vibráciám a namáčaniu. Počas prepravy je potrebne prepravovať kompletné balenie.
- Na prepravu použite továrenské balenie alebo jeho ekvivalent.

Batéria

Nízka kapacita batérie ovplyvňuje prevádzku RTC, čo spôsobí jeho vynulovanie pri každom zapnutí. Keď je batériu potrebné vymeniť, v správe servera produktu sa zobrazí hlásenie. Ďalšie informácie o hlásení servera nájdete na stránkach s nastaveniami produktu alebo sa obráťte na podporu spoločnosti Dahua.

⚠ **VAROVANIE**

- Nebezpečenstvo výbuchu, ak je batéria nesprávne vymenená.
- Vymeňte iba za tú istú batériu alebo batériu, ktorú odporúča spoločnosť Dahua.
- Použité batérie zlikvidujte v súlade s miestnymi predpismi alebo pokynmi výrobcu batérie.

Српски

Važne Zaštitne mere i Upozorenja

Ovo poglavlje opisuje sadržaj koji pokriva pravilno rukovanje uređajem, sprečavanje opasnosti i sprečavanje oštećenja imovine. Pažljivo pročitajte ove sadržaje pre korišćenja uređaja, poštujte ih kada koristite i čuvajte ga za buduću referencu.

Bezbednosna Uputstva

Sledeće kategorije reči sa definisanim značenjem mogu se pojaviti u „Vodiču“.

Oznaka	Značenje
⚠ **OPASNOST**	Označava visoku potencijalnu opasnost koja će, ako se i ne izbegne, rezultirati smrću ili ozbiljnim povredama.

Oznaka	Značenje
⚠ **UPOZORENJE**	Označava opasnost srednje ili niske potencijale koja bi, ukoliko se ne izbegne, mogla dovesti do blagih ili umerenih povreda.
⚠ **OPREZ**	Označava potencijalni rizik koji bi, ukoliko se to ne izbegne, mogao dovesti do oštećenja imovine, gubitka podataka, niže performanse ili nepredvidivog rezultata.
🔑 **PREPORUKE**	Pruža metode za pomoć u rešavanju problema ili uštede vremena.
📖 **BELEŠKA**	Pruža dodatne informacije kao naglasak i dodatak tekstu.

Bezbednosna Uputstva

- Pridržavajte se lokalnih standarda električne sigurnosti kako biste bili sigurni da je napon stabilan i da odgovara zahtevu za napajanje uređaja.
- Prevoz, korišćenje i skladištenje uređaja treba da budu u skladu sa dozvoljenim uslovima vlage i temperaturnim uslovima. Pogledajte odgovarajuće tehničke specifikacije uređaja koji se odnose na specifičnu radnu temperaturu i vlažnost vazduha.
- Nemojte postavljati uređaj na mesto izloženo vlazi, prašini, ekstremnom vrućem ili hladnom vazduhu, jakom elektronskom zračenju ili nestabilnim uslovima osvetljenja.
- Ne postavljajte uređaj na mesto blizu izvora toplote, kao što je radijator, grejač, peć ili drugi uređaj za proizvodnju toplote kako biste izbegli požar.
- Sprečite tečnost da teče u uređaj kako bi se izbeglo oštećenje unutrašnjih komponenti.
- Instalirajte uređaj horizontalno ili postavite na stabilno mesto kako biste sprečili padanje.
- Ugradite uređaj na dobro provetreno mesto i ne blokirajte ventilaciju uređaja.
- Nemojte rastavljati uređaj proizvoljno.
- Izbegavajte jak pritisak, nasilne vibracije i usisavanje tokom transporta, skladištenja i instalacije. Kompletan paket je neophodan tokom transporta.
- Koristite fabričko pakovanje ili ekvivalent u toku transporta.

Baterija

Baterija male snage utiče na rad RTC-a, dovodeći do reseta pri svakom uključivanju. Kada se baterija mora zameniti, logovna poruka će se pojaviti u izveštaju servera proizvoda. Za više informacija o izveštaju servera, pogledajte stranice za podešavanje proizvoda ili kontaktirajte Dahua podršku.

⚠ **UPOZORENJE**

- Opasnost od eksplozije ako se baterija nepravilno zameni.
- Zamenite je samo sa identičnom baterijom ili sa baterijom koju preporučuje Dahua.
- Odložite iskorišćene baterije u skladu sa lokalnim propisima ili uputstvima proizvođača baterije.

Türkçe

Önemli Kurallar ve Uyarılar

Bu Bölüm, Cihazın doğru kullanımını, tehlike önlemeyi ve mal zararının önlenmesini kapsayan içerikleri anlatmaktadır. Cihazı kullanmadan önce bu içerikleri dikkatli şekilde okuyun, kullanırken bunlara uyun ve ileride başvurmak üzere saklayın.

Güvenlik Talimatları

Aşağıda, belirtilen açıklamaya sahip kategorize edilmiş uyarı sözcüklerini Kılavuzda görebilirsiniz.

Uyarı Sözcükleri	Anlamı
⚠ **TEHLİKE**	Kaçınılmaması durumunda ölüm veya ciddi yaralanmalara neden olacak yüksek potansiyelli bir tehlikeyi belirtir.
⚠ **UYARI**	Kaçınılmaması durumunda hafif veya orta dereceli yaralanmaya neden olabilecek orta veya düşük potansiyelli bir tehlikeyi belirtir.
⚠ **DİKKAT**	Kaçınılmaması durumunda mal hasarına, veri kaybına, düşük performansa veya tahmin edilemeyen sonuca neden olabilecek potansiyel bir riski belirtir.
🔑 **İPUÇLARI**	Bir problemi çözmenize veya zamandan tasarruf etmenize yardımcı olmak için yöntemler sunar.
📖 **NOT**	Metne pekiştirme ve ek olarak ilave bilgiler sağlar.

Güvenlik Gereksinimi

- Voltajın is istikrarlı olduğundan ve cihazın güç kaynağı gereksinimine uygun olduğundan emin olmak için yerel elektrik güvenliği standartlarına uyun.
- Cihazı izin verilen nem ve sıcaklık şartları altında nakledin, kullanın ve saklayın. Belirli çalışma sıcaklığı ve nem değerleri için cihazın ilgili teknik özelliklerine bakın.
- Cihazı rutubete, toza, aşırı sıcağa veya soğuğa, güçlü elektronik radyasyona veya değişken aydınlatma şartlarına maruz kalan bir yere yerleştirmeyin.
- Yangını önlemek için cihazı radyatör, ısıtıcı, fırın veya başka ısı üreten cihazlar gibi ısı kaynağına yakın bir yere monte etmeyin.
- İçerisindeki parçaların hasar görmesini önlemek için cihazın içerisine sıvıların girmesini önleyin.
- Cihazın düşmesini önlemek için yatay olarak veya dayanıklı bir yere monte edin.

- Cihazı iyi havalandırılan bir yere monte edin ve cihazın hava sirkülasyonunu engellemeyin.
- Cihazın parçalarını gelişigüzel sökmeyin.
- Cihazın nakliyesi, saklanması ve montajı esnasında ağır baskılardan, şiddetli sarsıntılardan ve sıvıya batmalardan kaçının. Cihazın nakliyesi esnasında ambalajın tamamı gereklidir.
- Nakliye için fabrikasyon ambalajı ya da eş değerini kullanın.

Pil

Düşük pil gücü, her güç açma esnasında sıfırlanmasına neden olarak RTC'nin çalışmasını etkiler. Pillerin değiştirilmesi gerektiğinde ürünün sunucu raporunda bir günlük iletisi görüntülenir. Sunucu raporu hakkında daha fazla bilgi için ürünün kurulum sayfalarına bakın veya Dahua destek merkeziyle iletişime geçin.

⚠ **UYARI**

- Pil yanlış şekilde takılırsa patlama tehlikesi.
- Sadece aynı türde veya Dahua tarafından önerilen bir pil takın.
- Eski pilleri, yerel yönetmeliklere veya pil üreticisinin talimatlarına göre elden çıkarın.

עִבְרִית

חשיבות בעלי ואזהרות זהירות אמצעי

יש .רכוש נזקי ומניעת בעיות מניעת ,במכשיר נאות טיפול בנושא התכנים את מתאר זה פרק
המכשיר הפעלת בעת לאורם לפעול ,במכשיר שימוש לפני לב בתשומת אלה תכנים לקרוא
.עתידי לעיון אותם ולשמור

הנחיות בטיחות

.במדריך להופיע עשויות המוגדרים הפירושים עם הבאות המסווגות הסימון מילות

מילות סימון	משמעות
⚠ **סכנה**	לגרום עשויה ,תימנע לא שאם ,גבוהה בסבירות סכנה מציינת .קשה לפציעה או מוות
⚠ **אזהרה**	עשויה ,תימנע לא שאם ,נמוכה או בינונית בסבירות סכנה מציינת .בינונית או קלה לפציעה לגרום
⚠ **זהירות**	אובדן ,לנזק לגרום עשויה ,תימנע לא שאם לסכנה סבירות מציינת .צפויות לא לתוצאות או הביצועים ברמת הפחתה ,מידע
🔑 **עצות**	.זמן לך שיחסכו או בעיות לפתור לך שיסייעו שיטות מספקות

משמעות	סימון מילות
ולהשלמתו לטקסט להדגשה נוסף מידע מספקת.	📖 הערה

בטיחות דרישת

- ותואם יציב שהמתח להבטיח מנת על בחשמל לבטיחות המקומיים התקנים לכל לציית יש
  המכשיר של החשמל אספקת לדרישות.
- המותרים והלחות הטמפרטורה לתנאי בהתאם יעשו המוצר של ואחסון שימוש ,הובלה.
  המוגדרים וללחות לטמפרטורה המכשיר של המקבילים הטכניים למפרטים להתייחס יש
  עבודה לביצוע.
- קרינה ,קיצוניים חום או קור תנאי ,אבק ,לרטיבות חשוף במקום המכשיר את למקם אין
  יציבים לא תאורה תנאי או חזקה חשמלית.
- מכשיר או כבשן ,תנור ,מקרן כגון ,חום מקור בקרבת המכשיר את להתקין אין מנת על
  חום שפולט אחר.
- הפנימיים למרכיביו נזק למנוע מנת על המכשיר על נוזל משפיכת להימנע יש.
- יציב במקום או מאוזנת בצורה המכשיר את להתקין יש ,לייפו שלא מנת על.
- למכשיר האוויר מעבר את לחסום ולא היטב מאוורר במקום המכשיר את להתקין יש.
- עצמך בכוחות המכשיר את לפרק אין.
- אחסונו ,המכשיר הובלת במהלך הרטבתו או חזק טלטול ,כבד משקל מהצבת להימנע יש
  המלאה באריזתו להשתמש שי המכשיר העברת לשם .התקנתו או.
- במקבילה או היצרן ידי על המסופקת באריזה להשתמש יש המכשיר העברת לשם.

סוללה

צורך יש כאשר .שלו הדלקה בכל להתאפס לו ותגרום ה-RTC פעולת על תשפיע חלשה סוללה
ח"דו אודות נוסף למידע .המוצר של השרת ח"בדו אירועים יומן הודעת תופיע ,הסוללה בהחלפת
השרת, יש לעיין בדפי ההגדרה של המוצר או ליצור קשר עם התמיכה של Dahua.

⚠ אזהרה

- לפיצוץ לגרום עלולה הסוללה של נכונה לא החלפה.
- ידי על שמומלצת כזו או זהה בסוללה ורק אך להחליף יש Dahua.
- היצרן של להנחיותיו או המקומיות לתקנות בהתאם משומשות סוללות לסלק יש.

Français

Précautions et avertissements importants

Le contenu de ce chapitre aborde la bonne manipulation de l’appareil, la prévention des risques et la prévention des dommages matériels. Lisez ce contenu soigneusement avant d’utiliser l’appareil, respectez-le lorsque vous l’utilisez, et conservez-le pour vous y référer ultérieurement.

Précautions d’emploi

Les mentions d’avertissement catégorisées suivantes ayant un sens défini sont susceptibles d’apparaître dans le manuel.

Mentions d’avertissement	Signification
⚠ DANGER	Indique un danger à risque élevé qui entraînera la mort ou des blessures graves si les instructions données ne sont pas respectées.
⚠ AVERTISSEMENT	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
⚠ AVERTISSEMENT	Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées.
🔑 ASTUCES	Fournit des instructions qui vous permettront de résoudre un problème ou de vous faire gagner du temps.
📖 REMARQUE	Fournit des informations supplémentaires pour mettre en évidence et compléter le texte.

Exigences de sécurité

- Respectez les normes de sécurité électrique locales pour vous assurer que la tension est stable et conforme aux exigences d’alimentation de l’appareil.
- Transportez, utilisez et stockez l’appareil dans les conditions d’humidité et de température autorisées. Consultez les spécifications techniques correspondantes de l’appareil pour connaître la température et l’humidité de fonctionnement spécifiques.
- Ne placez pas l’appareil dans un lieu exposé à l’humidité, à la poussière, à une chaleur ou un froid extrême, à de forts rayonnements électroniques, ou à des conditions d’éclairage instables.
- N’installez pas l’appareil près d’une source de chaleur telle qu’un radiateur, un chauffage, une chaudière, ou tout autre dispositif générant de la chaleur afin d’éviter les risques d’incendie.
- Empêchez aux liquides de couler sur l’appareil afin d’éviter d’endommager les composants internes.
- Installez l’appareil horizontalement ou sur une surface stable afin de l’empêcher de tomber.
- Installez l’appareil dans un lieu bien ventilé et ne bloquez pas la ventilation de l’appareil.
- Ne démontez pas l’appareil de façon arbitraire.
- Au cours du transport, du stockage et de l’installation de l’appareil, évitez de le soumettre à de fortes contraintes, à des vibrations violentes ou à une immersion. L’emballage complet est nécessaire au cours du transport.
- Utilisez l’emballage d’usine ou équivalent pour le transport.

Batterie

Un niveau de batterie faible affecte le fonctionnement du RTC, qui se réinitialisera à chaque redémarrage. Lorsque la batterie doit être remplacée, un message de journal apparaît dans le rapport du serveur du produit. Pour plus d’informations sur le rapport du serveur, consultez les pages de configuration du produit ou contactez l’assistance Dahua.

⚠ **AVERTISSEMENT**

- Risque d’explosion si la batterie est remplacée de façon incorrecte.
- Remplacez la batterie uniquement par une batterie recommandée par Dahua.
- Éliminez les batteries usagées conformément aux réglementations locales ou aux instructions du fabricant de la batterie.

Español(España)

Advertencias y precauciones de seguridad importantes

En este capítulo se describe el contenido que cubre la manipulación correcta del dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea detenidamente este contenido antes de usar el dispositivo, sígalo cuando lo utilice y consérvelo para consultas futuras.

Instrucciones de seguridad

Las siguientes palabras de advertencia con un significado definido podrían aparecer en la guía.

Palabras de advertencia	Significado
⚠ PELIGRO	Indica un riesgo potencial alto que, si no se evita, resultará en muerte o lesiones graves.
⚠ ADVERTENCIA	Indica un riesgo potencial medio o bajo que, si no se evita, podría resultar en lesiones leves o moderadas.
⚠ PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría resultar en daños materiales, pérdida de datos, rendimiento menor o resultados impredecibles.
CONSEJOS	Ofrece métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como hincapié y complemento para el texto.

Requisitos de seguridad

- Cumpla las normas locales de seguridad eléctrica para garantizar que la tensión sea estable y cumpla los requisitos de alimentación eléctrica del dispositivo.
- Transporte, utilice y almacene el dispositivo bajo las condiciones de humedad y temperatura permitidas. Consulte las especificaciones técnicas

correspondientes del dispositivo para la temperatura y humedad operativas específicas.

- No coloque el dispositivo en un lugar expuesto a humedad, polvo, calor o frío extremos, radiaciones electrónicas fuertes o condiciones de iluminación inestables.
- No instale el dispositivo en un lugar cerca de fuentes de calor, como radiadores, calentadores, hornos u otros dispositivos generadores de calor, para evitar un incendio.
- No deje que entre líquido en el dispositivo para evitar daños en los componentes internos.
- Instale el dispositivo horizontalmente o instálelo sobre un lugar estable para evitar que caiga.
- Instale el dispositivo en un lugar bien ventilado y no obstruya la ventilación.
- No desmonte de forma arbitraria el dispositivo.
- Evite las presiones excesivas, las vibraciones violentas y mojar el dispositivo durante el transporte, almacenamiento e instalación. Es necesario utilizar el embalaje completo durante el transporte.
- Utilice el embalaje de fábrica o uno equivalente para transportarlo.

Pilas

La baja batería afecta al funcionamiento del RTC, provocando que se restablezca cada vez que recibe alimentación. Cuando sea necesario sustituir las pilas, aparecerá un mensaje de registro en el informe de servidor del producto. Para más información acerca del informe de servidor, consulte las páginas de configuración del producto o póngase en contacto con el departamento de soporte de Dahua.

⚠ **ADVERTENCIA**

- Riesgo de explosión si se sustituyen incorrectamente las pilas.
- Sustitúyalas únicamente por pilas idénticas o pilas recomendadas por Dahua.
- Elimine las pilas gastadas en conformidad con la normativa local o las instrucciones del fabricante de las pilas.

Deutsch

Wichtige Sicherheits- und Warnhinweise

Dieses Kapitel beschreibt die Inhalte zum richtigen Umgang mit dem Gerät, zur Verhütung von Gefahren und zur Vermeidung von Sachschäden. Lesen Sie dieses Kapitel sorgfältig durch, bevor Sie das Gerät verwenden, halten Sie die Anweisungen bei der Verwendung ein und bewahren Sie diese Anleitung zum späteren Nachlesen gut auf.

Sicherheitshinweise

Die folgenden kategorisierten Signalwörter mit definierter Bedeutung können in der Kurzanleitung verwendet werden.

Signalwörter	Bedeutung
⚠ **GEFAHR**	Weist auf ein hohes Gefahrenpotential hin, das, wenn es nicht vermieden wird, zum Tod oder zu schweren Verletzungen führt.

Signalwörter	Bedeutung
⚠ **WARNUNG**	Weist auf eine mittlere oder geringe potentielle Gefahr hin, die, wenn sie nicht vermieden wird, zu leichten oder mittelschweren Verletzungen führen kann.
⚠ **VORSICHT**	Weist auf ein potenzielles Risiko hin, das, wenn es nicht vermieden wird, zu Sachschäden, Datenverlust, geringerer Leistung oder unvorhersehbaren Ergebnis führen kann.
🔑 **TIPPS**	Stellt Methoden bereit, mit denen Sie ein Problem lösen oder Zeit sparen können.
📖 **HINWEIS**	Bietet zusätzliche Informationen als Schwerpunkt und Ergänzung zum Text.

Sicherheitsanforderungen

- Halten Sie sich an die örtlichen elektrischen Sicherheitsnormen, um sicherzustellen, dass die Spannung stabil ist und den Anforderungen an die Stromversorgung des Geräts entspricht.
- Transportieren, verwenden und lagern Sie das Gerät unter den zulässigen Feuchtigkeits- und Temperaturbedingungen. Die entsprechenden technischen Spezifikationen des Geräts für die jeweilige Betriebstemperatur und Luftfeuchtigkeit sind zu beachten.
- Stellen Sie das Gerät nicht an Orten auf, an denen es Feuchtigkeit, Staub, extremer Hitze oder Kälte, starker elektronischer Strahlung oder instabilen Lichtverhältnissen ausgesetzt ist.
- Installieren Sie das Gerät nicht in der Nähe einer Wärmequelle, z. B. einem Heizkörper, Heizlüfter, Ofen oder anderen Wärme erzeugenden Geräten, um Feuer zu vermeiden.
- Verhindern Sie, dass Flüssigkeit in das Gerät fließt, um Schäden an internen Bauteilen zu vermeiden.
- Installieren Sie das Gerät waagerecht oder an einem stabilen Ort, damit es nicht herunterfällt.
- Installieren Sie das Gerät an einem gut belüfteten Ort und blockieren Sie die Belüftung des Geräts nicht.
- Nehmen Sie das Gerät nicht eigenmächtig auseinander.
- Vermeiden Sie starke Belastungen, Vibrationen und eindringende Nässe während des Transports, der Lagerung und der Installation. Das Gerät sollte immer vollständig verpackt transportiert werden.
- Verwenden Sie die ab Werk verwendete Verpackung oder eine gleichwertige Verpackung für den Transport.

Batterie

Eine niedrige Batterieleistung beeinträchtigt den Betrieb der Echtzeituhr, wodurch sie bei jedem Einschalten zurückgesetzt wird. Wenn die Batterie ausgetauscht werden muss, wird eine Protokollmeldung im Serverbericht des Produkts angezeigt. Weitere Informationen zum Serverbericht finden Sie auf den Einrichtungsseiten des Produkts oder wenden Sie sich an den Support von Dahua.

⚠ **WARNUNG**

- Bei nicht ordnungsgemäßem Austausch der Batterie besteht

Explosionsgefahr.

- Ersetzen Sie die Batterie nur durch eine identische Batterie oder eine Batterie, die von Dahua empfohlen wird.
- Entsorgen Sie leere Batterien entsprechend den örtlichen Vorschriften oder den Anweisungen des Batterieherstellers.

Italiano

Norme di sicurezza e avvertenze importanti

Il presente capitolo descrive le procedure per una corretta manipolazione del dispositivo, per la prevenzione dei rischi e per la prevenzione di danni materiali. Leggere attentamente queste informazioni prima di utilizzare il dispositivo, attenersi alle istruzioni fornite durante l’uso e conservarle come futuro riferimento.

Istruzioni di sicurezza

I seguenti indicatori di pericolo, aventi i significati indicati, possono apparire nella presente guida.

Indicatori di pericolo	Significato
⚠ **PERICOLO**	Indica una situazione ad alto rischio che, se non viene evitata, può causare il decesso o gravi lesioni.
⚠ **AVVERTENZA**	Indica una situazione a medio o basso rischio che, se non viene evitata, può causare lesioni di leggera o moderata entità.
⚠ **ATTENZIONE**	Indica un rischio potenziale che, se non evitato, può causare danni materiali, perdite di dati, riduzione delle prestazioni o altre conseguenze imprevedibili.
🔑 **CONSIGLI**	Spiegano metodi utili per risolvere un problema o per aiutarvi a risparmiare tempo.
📖 **NOTA**	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Requisiti di sicurezza

- Attenersi alle leggi locali sulla sicurezza elettrica per garantire una tensione stabile e soddisfare i requisiti di alimentazione del dispositivo.
- Trasportare, utilizzare e conservare il dispositivo alle condizioni di umidità e temperatura consentite. Fare riferimento alle specifiche tecniche del dispositivo per conoscere i valori specifici della temperatura di esercizio e dell’umidità.
- Non posizionare il dispositivo in un ambiente esposto ad una eccessiva umidità, a polvere, a condizioni di caldo e freddo estremi, a forti radiazioni elettroniche o a condizioni di illuminazione non stabile.
- Non installare il dispositivo vicino ad una fonte di calore, quali ad esempio radiatori, apparecchi di riscaldamento, forni o altri dispositivi di generazione del calore, per evitare il rischio di incendio.
- Evitare di versare liquido sul dispositivo per non danneggiare i componenti interni.
- Installare il dispositivo in posizione orizzontale, oppure in una zona stabile, per evitare che possa cadere.

- Installare il dispositivo in un ambiente adeguatamente ventilato e non ostruire la circolazione dell'aria.
- Non smontare il dispositivo in modo casuale.
- Evitare forte sollecitazioni, violente vibrazioni e non bagnare il prodotto durante il trasporto, lo stoccaggio e l'installazione. Trasportare il prodotto utilizzando un imballaggio adeguato.
- Utilizzare l'imballaggio standard previsto o un imballaggio equivalente.

Batteria

L'uso di una batteria scarica può compromettere il funzionamento del dispositivo RTC, che si resetterà ad ogni avvio. Quando è necessario sostituire la batteria, nel report del server del prodotto viene visualizzato un messaggio di log. Per ulteriori informazioni sul report del server, leggere le pagine di configurazione del prodotto, oppure contattare il servizio assistenza di Dahua.

AVVERTENZA

- Se la batteria non viene sostituita correttamente, può generare il rischio di esplosione.
- Sostituire solo con una batteria identica o una batteria raccomandata da Dahua.
- Smaltire le batterie usate in conformità con le normative locali o attenendosi alle istruzioni del produttore della batteria.

Nederlands

Belangrijke voorzorgsmaatregelen en waarschuwingen

Dit hoofdstuk beschrijft de inhoud die de juiste omgang met het apparaat behandelt, het voorkomen van gevaren alsmede het voorkomen van materiële schade. Lees deze inhoud zorgvuldig door voordat u het apparaat gebruikt, houdt u eraan tijdens het gebruik, en bewaar ze goed voor toekomstige referentie.

Veiligheidsinstructies

De volgende gecategoriseerde signaalwoorden met gedefinieerde betekenis staan in de handleiding vermeld.

Signaalwoorden	Betekenis
GEVAAR	Geeft een hoog potentieel gevaar aan dat, indien niet voorkomen, kan leiden tot overlijden of ernstig.
WAARSCHUWING	Geeft een gemiddeld of laag potentieel gevaar aan dat, indien niet voorkomen, kan leiden tot licht of matig letsel.
LET OP	Geeft een potentieel risico aan dat, indien niet voorkomen, kan leiden tot materiële schade, gegevensverlies, lagere prestaties of onvoorspelbaar resultaat.
TIPS	Biedt methodes om u te helpen een probleem op te lossen of tijd te besparen.
OPMERKING	Biedt aanvullende informatie als nadruk op en aanvulling van de tekst.

Veiligheidsvereiste

- Houdt u aan plaatselijke veiligheidsstandaarden om ervoor te zorgen dat het voltage stabiel is en voldoet aan de vereiste stroomvoorziening van het apparaat.
- Transporteer, gebruik en bewaar het apparaat onder de toegestane relatieve luchtvochtigheid en temperatuuromstandigheden. Zie de overeenkomstige technische specificaties van het apparaat voor specifieke werktemperatuur en relatieve luchtvochtigheid.
- Plaats het apparaat niet op een locatie die blootgesteld is aan vocht, stof, extreme hitte of koude, sterke elektronische straling of onstabiele verlichtingsomstandigheden.
- Installeer het apparaat niet op een plek vlakbij de warmtebron, zoals een radiator, verwarming, fornuis of ander warmte-genererend apparaat om brand te voorkomen.
- Voorkom dat er vloeistof in het apparaat loopt om schade aan interne componenten te vermijden.
- Installeer het apparaat horizontaal of installeer het op een stabiele plek om te voorkomen dat het valt.
- Installeer het apparaat in een goed geventileerde ruimte en blokkeer de ventilatie van het apparaat niet.
- Haal het apparaat niet willekeurig uit elkaar.
- Vermijd zware druk, hevige trilling en nat worden tijdens het transport, de opslag en de installatie. De complete verpakking is noodzakelijk tijdens het transport.
- Gebruik de fabrieksverpakking of gelijkwaardig voor het transport.

Batterij

Lage batterijstroom beïnvloedt de bediening van de RTC, waardoor deze bij iedere stroominschakeling reset. Als de batterij vervangen moet worden, verschijnt een logbericht in het serverrapport van het product. Zie voor meer informatie over het serverrapport de setuppagina's van het product of neem contact op met Dahua Support.

⚠ **WAARSCHUWING**

- Gevaar op ontploffing als de batterij onjuist wordt vervangen.
- Vervang alleen met een identieke batterij die wordt aanbevolen door Dahua.
- Verwerk de gebruikte batterijen volgens de plaatselijke regelgeving of de instructies van de batterijfabrikant.

Portugués

Instruções e advertências importantes

Este capítulo descreve os conteúdos relativos ao manuseamento correto do dispositivo, à prevenção de riscos e à prevenção de danos materiais. Leia estes conteúdos atentamente antes de utilizar o dispositivo, respeite as instruções durante a utilização e guarde-as em boas condições para consulta futura.

Instruções de segurança

As seguintes palavras-sinal categorizadas, com um significado definido, poderão surgir no Guia.

Palavras-sinal	Significado
⚠ PERIGO	Indica um risco potencial elevado que, se não for evitado, resultará em morte ou ferimentos graves.
⚠ AVISO	Indica um risco potencial médio ou baixo que, se não for evitado, poderá resultar em ferimentos ligeiros ou moderados.
⚠ ATENÇÃO	Indica um risco potencial que, se não for evitado, pode resultar em danos materiais, perda de dados, desempenho inferior ou resultados imprevisíveis.
SUGESTÕES	Disponibiliza métodos para o ajudar a resolver um problema ou a poupar o seu tempo.
NOTA	Disponibiliza informações adicionais como destaque e complemento ao texto.

Requisitos em termos de segurança

- Respeite as normas locais de segurança elétrica de forma a garantir que a tensão é estável e respeita os requisitos da fonte de alimentação do dispositivo.
- Transporte, utilize e armazene o dispositivo nas condições de humidade e temperatura permitidas. Consulte as respetivas especificações técnicas do dispositivo para conhecer a temperatura e humidade de funcionamento específicas.
- Não coloque o dispositivo num local exposto a humidade, poeira, condições de calor ou frio extremas, radiação eletrónica intensa ou condições de iluminação instáveis.
- Não instale o dispositivo num local próximo de uma fonte de calor, como, por exemplo, um radiador, aquecedor, fornalha ou outro dispositivo de geração de calor de forma a evitar incêndios.
- Não permita o escorrimento de líquidos para o dispositivo, evitando, assim, danos nos componentes internos.
- Instale o dispositivo numa posição horizontal ou num local estável, prevenindo possíveis quedas.
- Instale o dispositivo num local bem ventilado e não bloqueie a ventilação do dispositivo.
- Não desmonte o dispositivo de forma arbitrária.
- Evite pressões intensas, vibrações violentas e a imersão do dispositivo durante o transporte, armazenamento e instalação. Para o transporte, é necessária a embalagem completa.
- Utilize a embalagem de fábrica ou equivalente para efetuar o transporte.

Bateria

Uma bateria fraca afeta a operação do RTC, fazendo com que este reinicie sempre que é ligado. Quando a bateria tiver de ser substituída, surgirá uma mensagem de registo no relatório do servidor do produto. Para mais informações sore o relatório do servidor, consulte as páginas de configuração do produto ou contacte a Dahua para obter assistência.

⚠ AVISO

- Risco de explosão se a bateria não for corretamente colocada.
- Substitua apenas por uma bateria idêntica ou por uma bateria recomendada pela Dahua.
- Elimine as baterias usadas de acordo com os regulamentos locais ou com as instruções do fabricante da bateria.