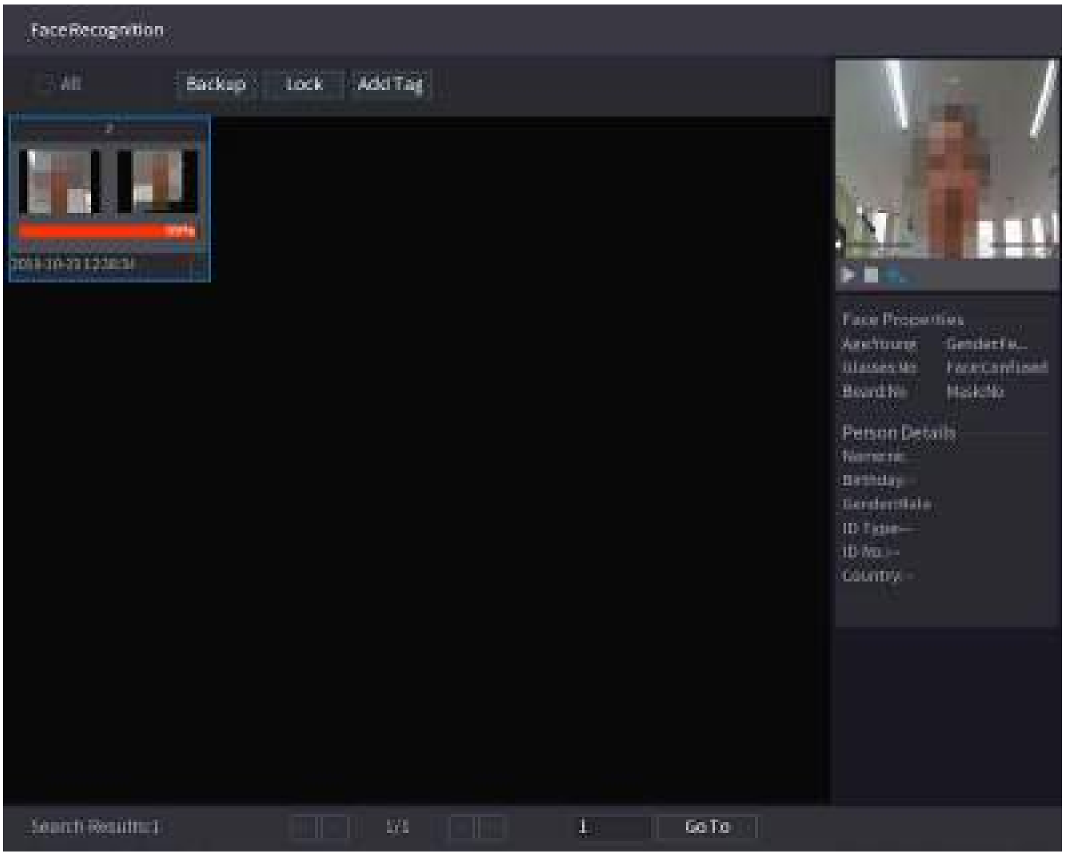
Step 4 Click the picture that you want to play back.

Figure 5-167 Registered information



Face Properties
Age:Young Gender:Fe...
Glasses:No Face:Confused
Beard:No Mask:No

Person Details
Name:nr...
Birthday:--
Gender:Male
ID Type:--
ID No.:--
Country:--

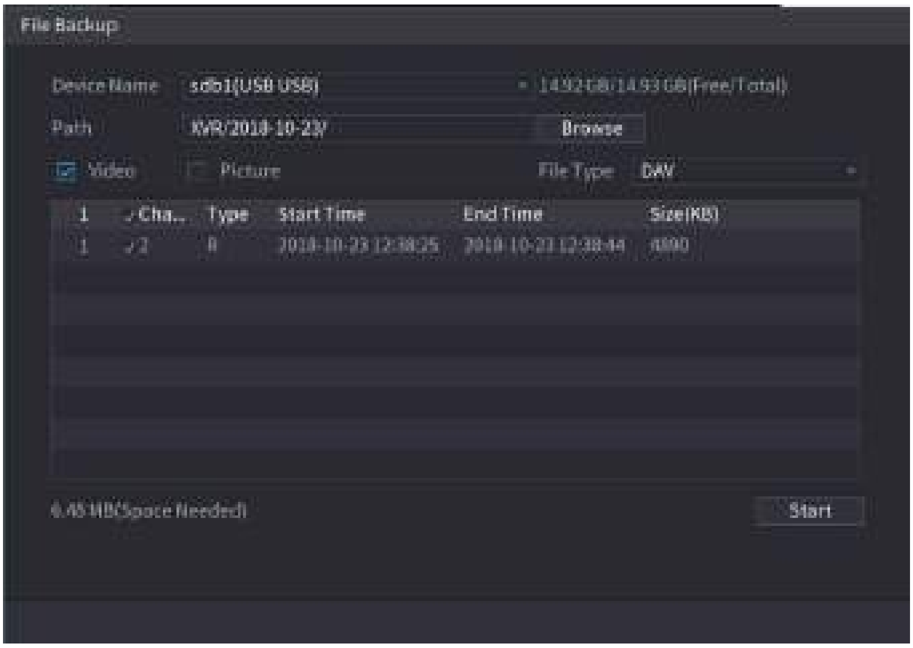
Step 5 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-168 Backup



File Backup

Device Name: sdb1(USB USB) — 14.92 GB/14.93 GB(Free/Total)

Path: KVR/2018-10-23/

☑ Video □ Picture File Type: DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	4890

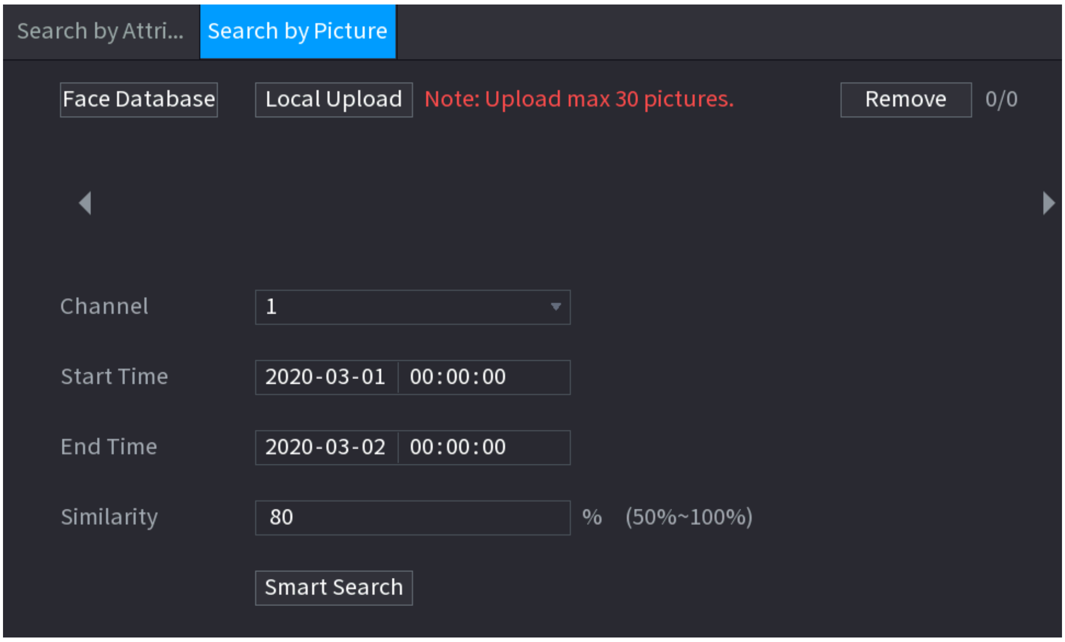
6.48 MB(Space Needed)

- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

Search by Picture

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Face Recognition** > **Search by Picture**.

Figure 5-169 Search by picture



Note: Upload max 30 pictures.

Channel: 1

Start Time: 2020-03-01 00:00:00

End Time: 2020-03-02 00:00:00

Similarity: 80 % (50%~100%)

Step 2 Upload face pictures from **Face Database** or **Local Upload**.

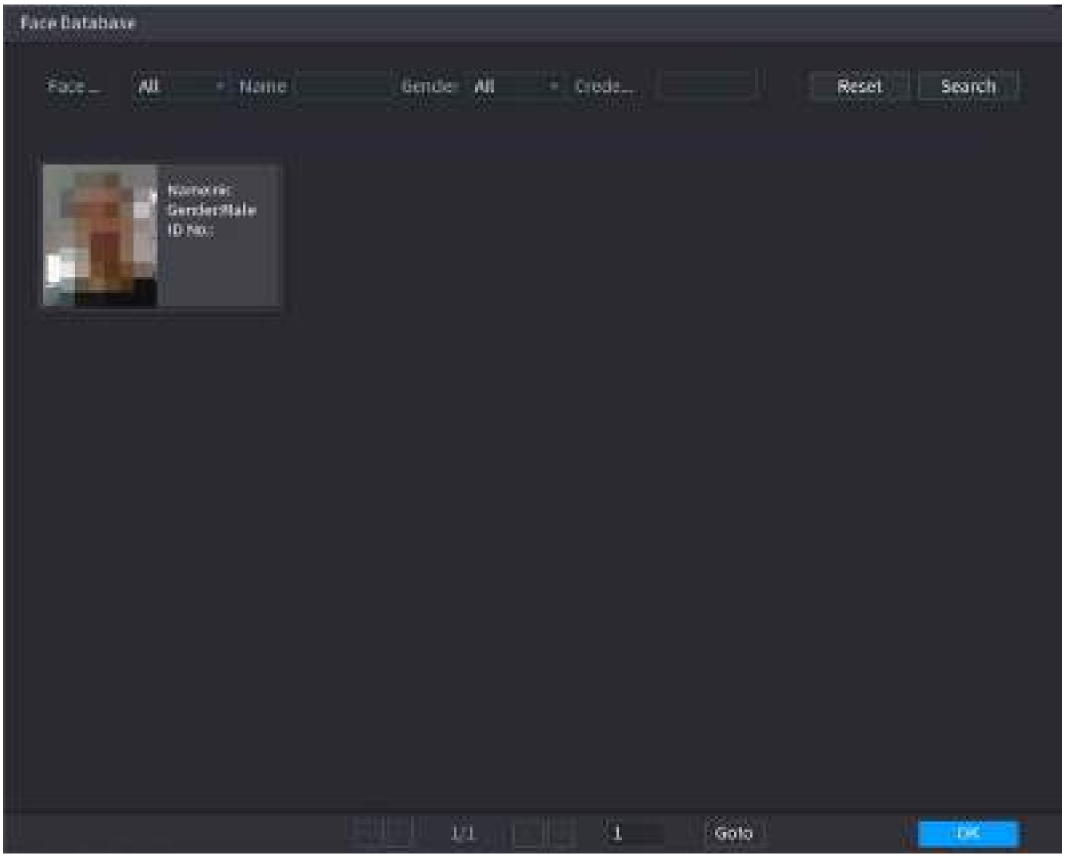
NOTE

Maximum 30 pictures can be uploaded at one time, and the system support searching 8 pictures at one time.

- Face Database

1) Click **Face Database**.

Figure 5-170 Face database



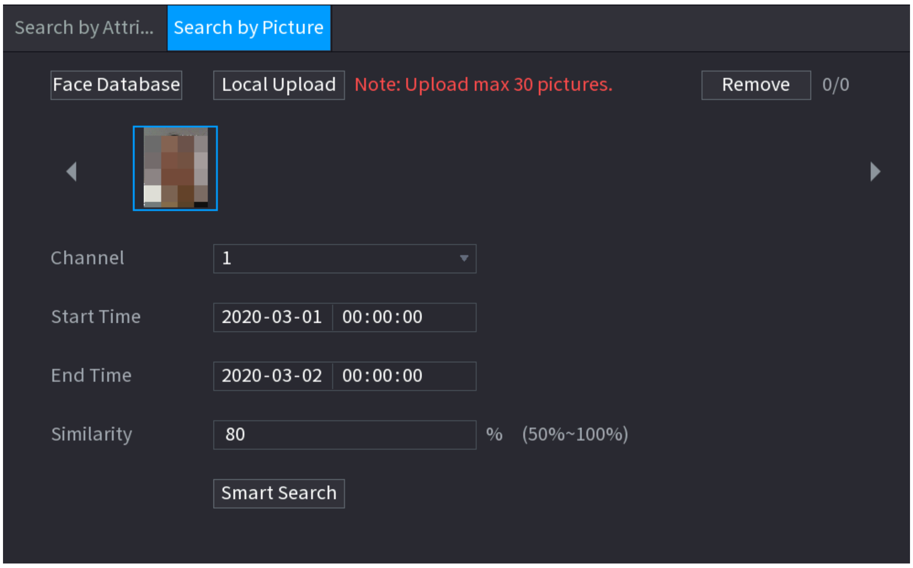
2) Set the searching parameters by selecting the face database and gender, and entering name and ID No. according to your actual requirement.

3) Click **Search** to display the results that satisfy the requirement.

Click **Reset** to clear the searching parameters.

4) Select the picture and then click **OK**.

Figure 5-171 Uploaded picture



Note: Upload max 30 pictures.

Channel: 1

Start Time: 2020-03-01 00:00:00

End Time: 2020-03-02 00:00:00

Similarity: 80 % (50%~100%)

- Local Upload

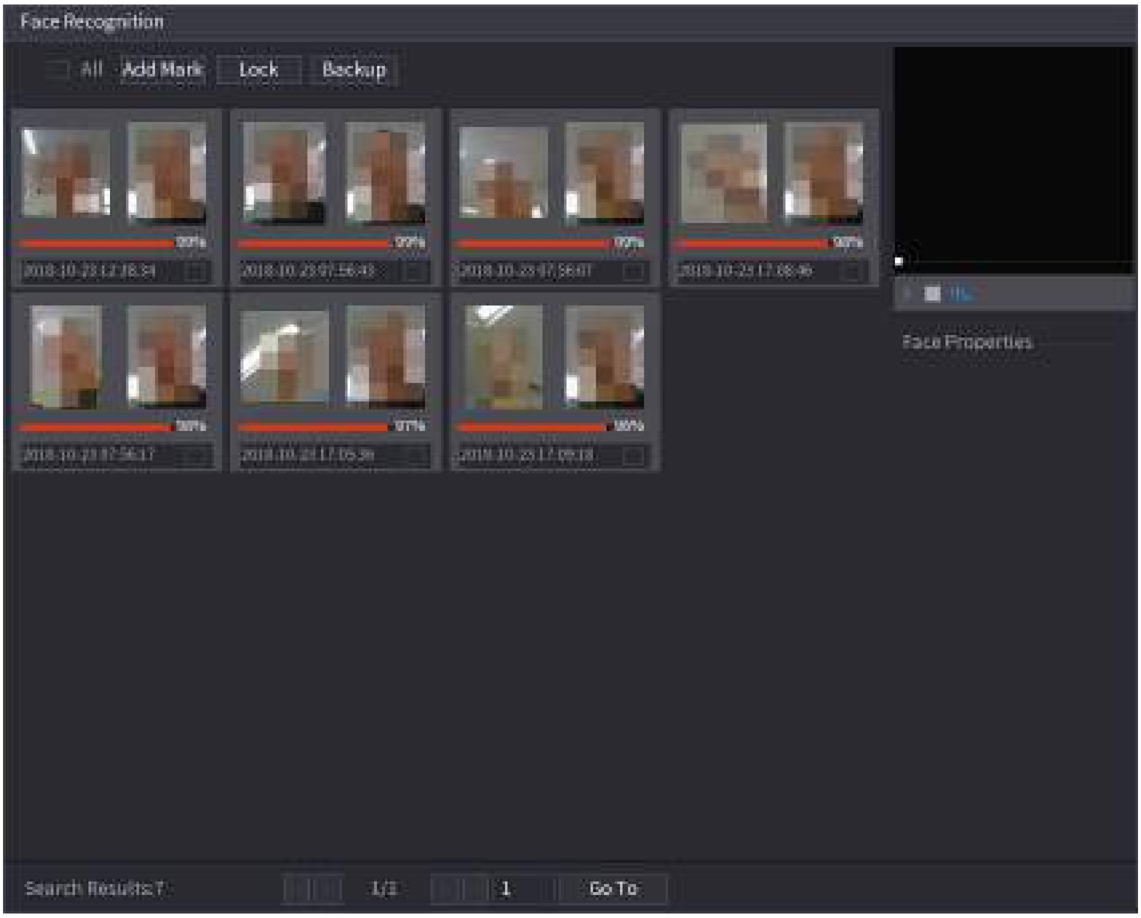
Plug the USB storage device (with face pictures) to the Device, and then click **Local Upload**. Then select the picture from the USB storage device, and then click **OK**. The selected face pictures are uploaded.

Step 3 After the face pictures are uploaded, continue to configure other parameters (channel, start time, end time, and similarity).

Step 4 Click **Smart Search**.

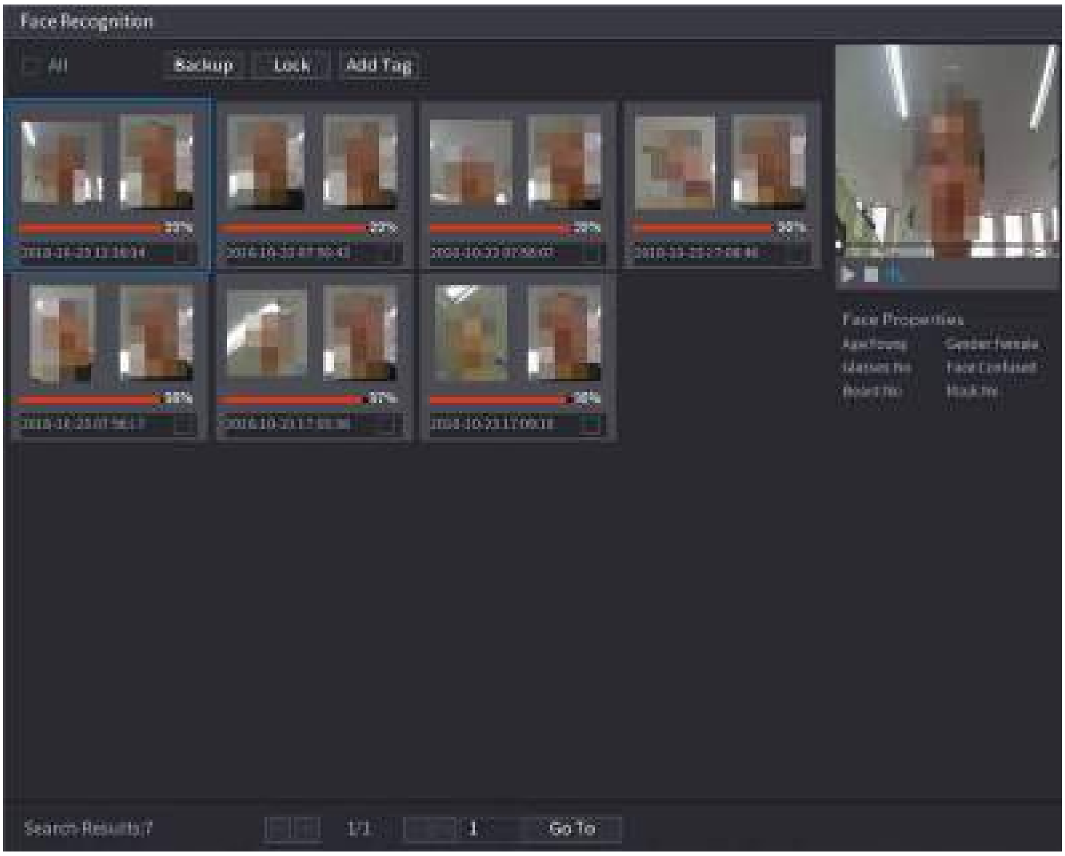
The searching results are displayed.

Figure 5-172 Search results



Step 5 Select the face picture that you want to play back.

Figure 5-173 Playback



Age:Young Gender:Female
Glasses:No Face:Confused
Beard:No Mask:No

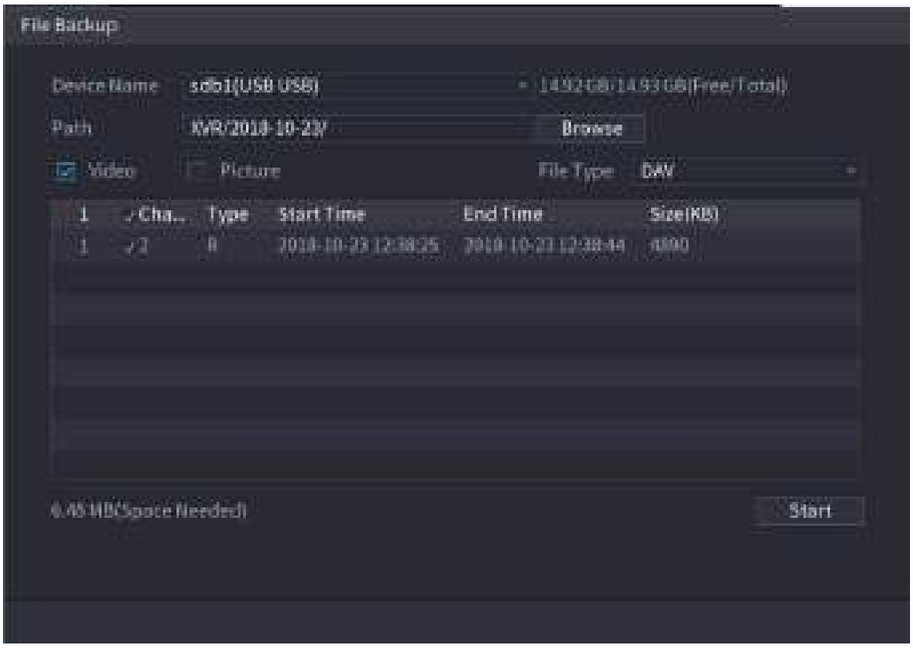
Step 6 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To add a mark to the file, select the files and then click **Add Tag**.
- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-174 Backup



File Backup

Device Name sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path KVR/2018-10-23/ Browse

☑ Video □ Picture File Type DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	4890

6.48 MB(Space Needed) Start

5.11.2.3 IVS Function

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

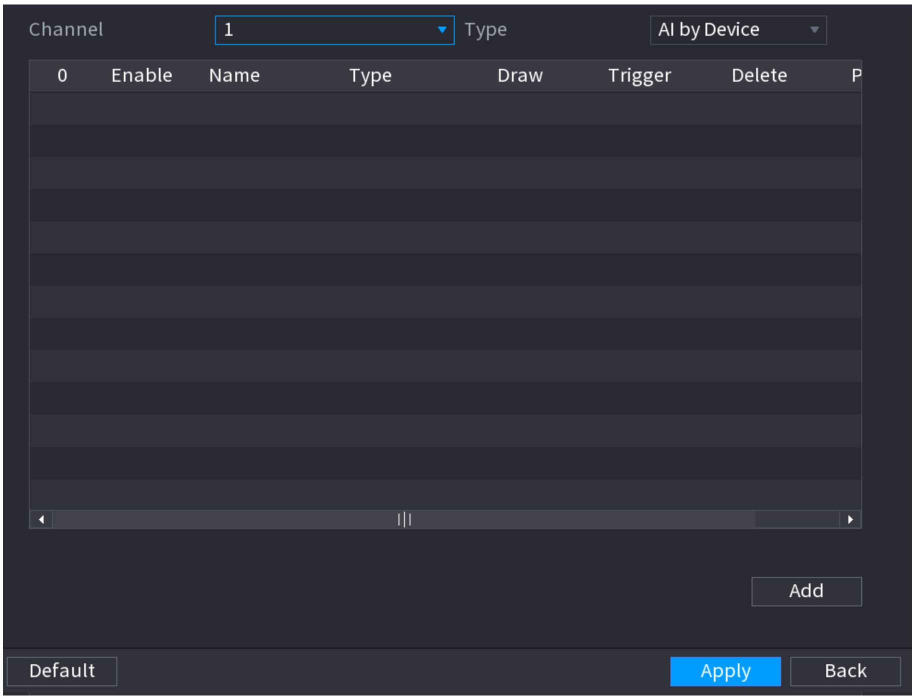
If you select AI by device, then among face detection and recognition, IVS function, and video structuring, you can use one of them at the same time for the same channel.

5.11.2.3.1 Configuring IVS Parameters

The alarms are generated according to the configured parameters.

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

Figure 5-175 IVS



Channel: 1 | Type: AI by Device

0	Enable	Name	Type	Draw	Trigger	Delete	P

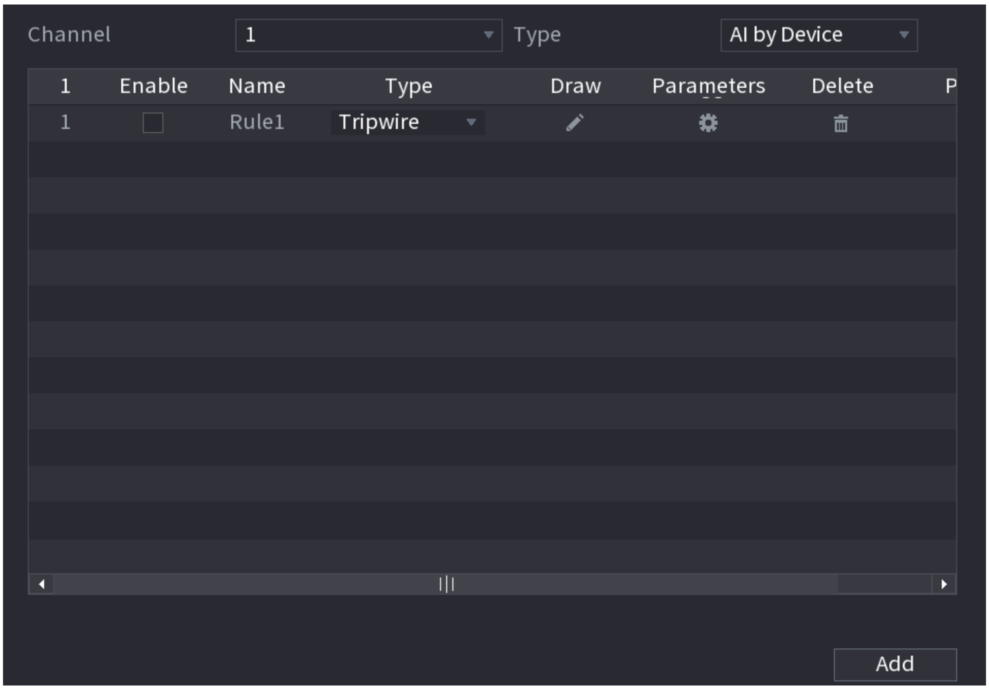
Step 2 In the **Channel** list, select the channel number that you want to configure the IVS function.

Step 3 At **Type**, you can select from **AI by Camera** and **AI by Device**.

- **AI by Camera:** This option requires certain AI cameras. The camera will do all the AI analysis, and then give the results to the DVR.
- **AI by Device:** The camera only transmits normal video stream to the DVR, and then the DVR will do all the AI analysis.

Step 4 Click **Add**.

Figure 5-176 Added rule



Channel: 1 | Type: AI by Device

1	Enable	Name	Type	Draw	Parameters	Delete	P
1	□	Rule1	Tripwire	✎	⚙	🗑	

Step 5 Configure the parameters for the rule that you selected.

Step 6 Select the checkbox of the rule to enable it.

Step 7 Click **Apply** to complete the settings.

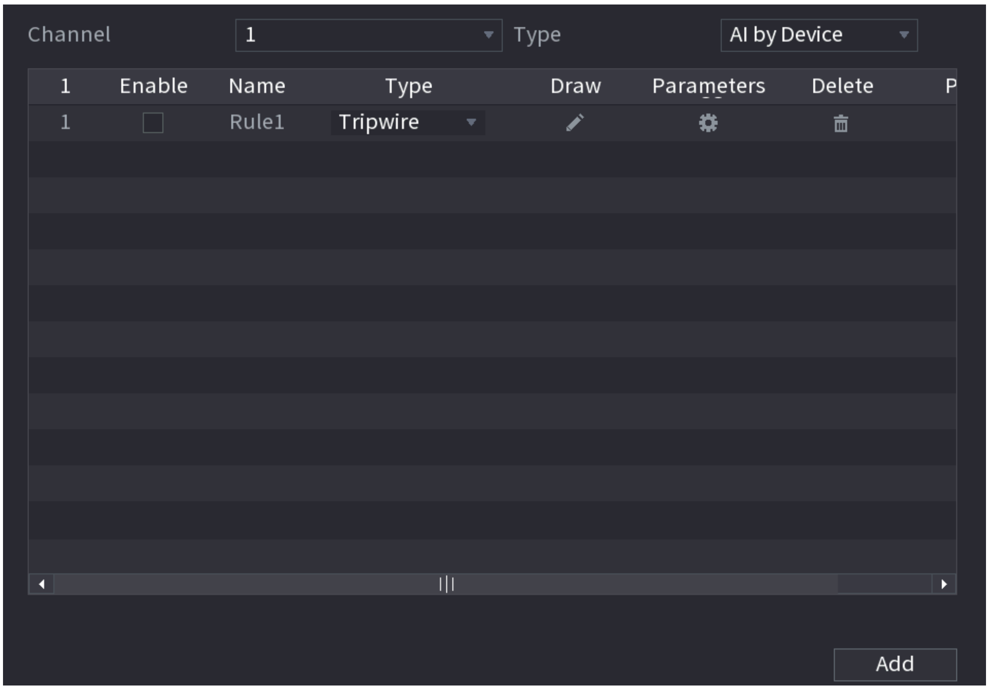
Configuring Tripwire Rules

When the target object crosses the tripwire in the defined direction, the system activates alarms.

- The tripwire can be configured as a straight line or broken line.
- Supports detecting one-way or two-way tripwire crossing.
- Supports multiple tripwires in the same scenario to meet the complexity.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Tripwire**.

Figure 5-177 Tripwire



Channel: 1 Type: AI by Device

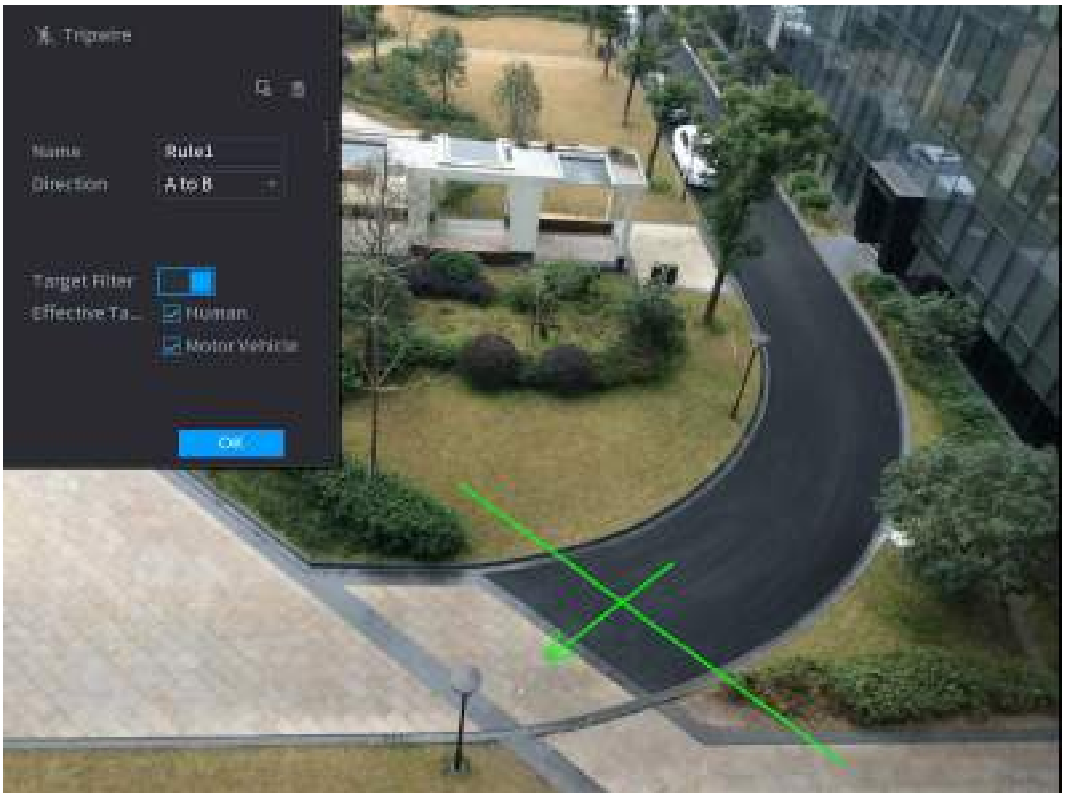
1	Enable	Name	Type	Draw	Parameters	Delete	P
1	☐	Rule1	Tripwire	✎	⚙	🗑	

Step 2 Draw a tripwire.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click ✎.

Figure 5-178 Tripwire rule



Tripwire

Name: Rule1

Direction: A to B

Target Filter

Effective Ta... ☑ Human ☑ Motor Vehicle

OK

3) Configure the settings for the parameters of drawing rules.

Figure 5-179 Tripwire parameters

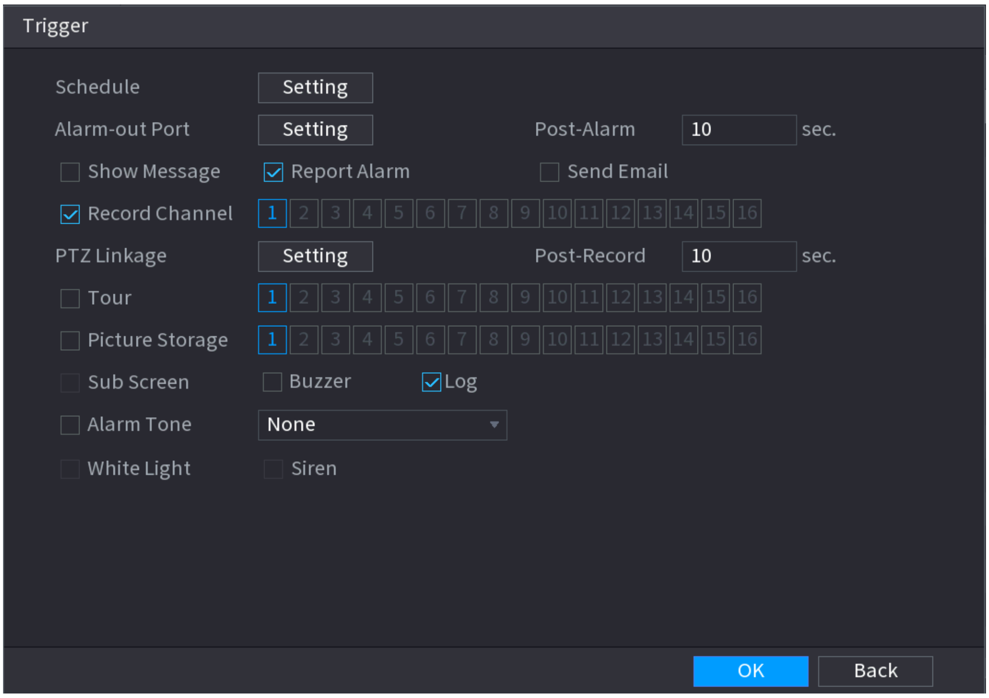
Parameter	Description
Name	Enter the customized rule name.
Direction	Set the direction of the tripwire. You can choose **A to B** (left to right), **B to A** (right to left), and **Both**.
Target Filter	Click ⧉ to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (●). By default, **Human** and **Motor Vehicle** are selected for alarm object.

4) Drag to draw a tripwire. The tripwire can be a straight line, broken line or polygon.

5) Click **OK** to save the settings.

Step 3 Click ⚙ to set the actions to be triggered.

Figure 5-180 Trigger



Trigger

Schedule: Setting

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

□ Show Message ☑ Report Alarm □ Send Email

☑ Record Channel: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

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

□ Tour: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Picture Storage: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Sub Screen □ Buzzer ☑ Log

□ Alarm Tone: None

□ White Light □ Siren

Step 4 Configure the triggering parameters.

Figure 5-181 Triggering parameters

Parameter	Description
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable general alarm and select the alarm output port. ● Ext. Alarm: Connect the alarm box to the Device and then enable it. ● Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the **Show Message** checkbox to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the **Report Alarm** checkbox to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs. ● Not all models support this function. ● The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."

Parameter	Description
Send Email	Select the **Send Email** checkbox to enable the system to send an email notification when an alarm event occurs. 📖 To use this function, make sure the email function is enabled in **Main Menu > NETWORK > EMAIL**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs. 📖 The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs. 📖 To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post-Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.
Tour	Select the **Tour** checkbox to enable a tour of the selected channels. 📖 ● To use this function, the tour setting must be configured. ● After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the **Picture Storage** checkbox to take a snapshot of the selected channel. 📖 To use this function, make sure the snapshot function is enabled for **Intel** in **Main Menu > STORAGE > Schedule > Picture Storage**.
Video Matrix	Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "**Main Menu > DISPLAY > Tour > Sub Screen**." 📖 ● Not all models support this function. ● The extra screen must be enabled to support this function.
Buzzer	Select the checkbox to activate a buzzer noise at the Device.
Log	Select the checkbox to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.

Step 5 Click **OK** to save the settings.

Step 6 Select the **Enable** checkbox, and then click **Apply**.

The tripwire detecting function is active. When the target object crosses the tripwire in the defined direction, the system activates alarms.

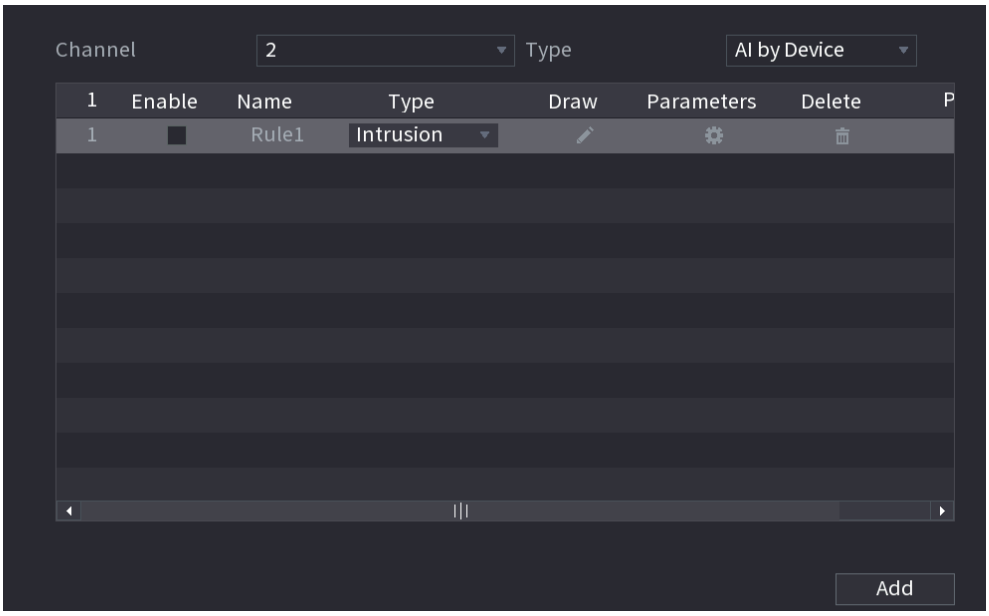
Configuring Intrusion Rules

When the target enters and leaves the defined detection area, or the target appears in the defined area, the system activates alarms.

- You can define the shape and quantity of intrusion areas.
- Supports detecting the behaviors that enter and leave the intrusion areas.
- Supports detecting the behaviors that are moving in the intrusion areas. The quantity of areas and lasting time can be configured.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Intrusion**.

Figure 5-182 Intrusion



Channel: 2
Type: AI by Device

1	Enable	Name	Type	Draw	Parameters	Delete	P
1	■	Rule1	Intrusion	✎	⚙	🗑	

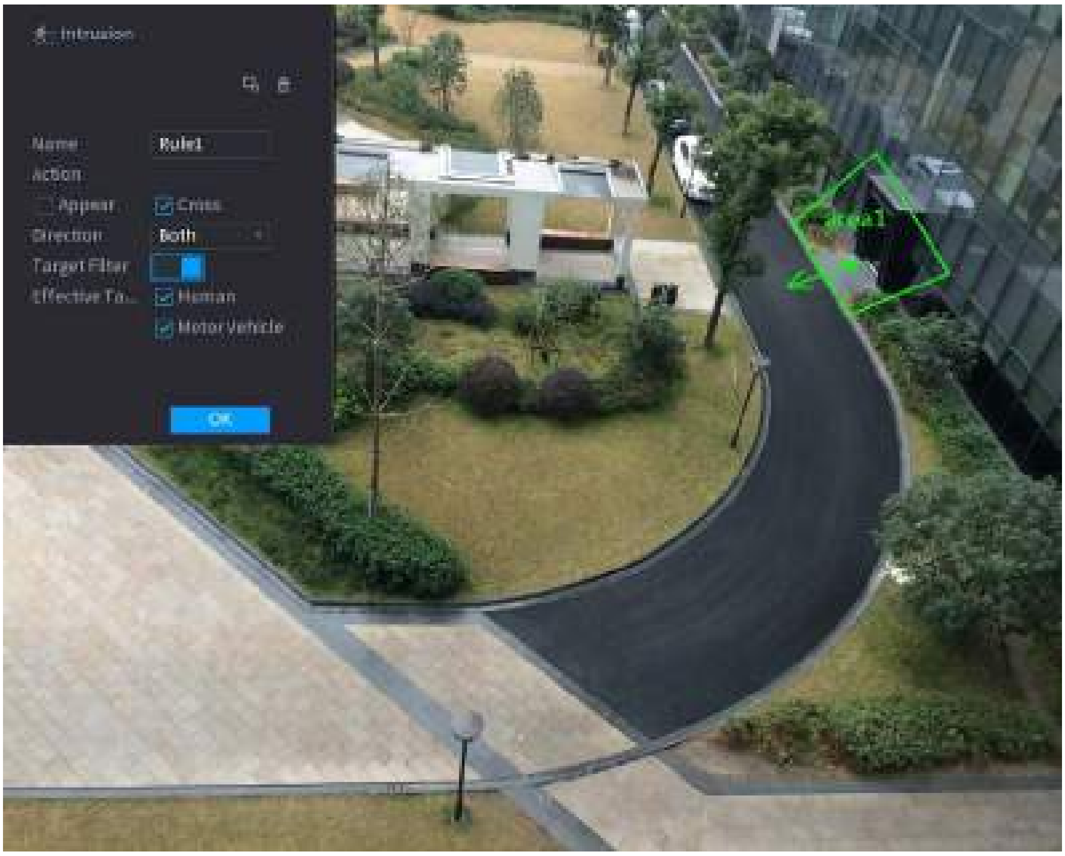
Add

Step 2 Draw an area.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click ✎.

Figure 5-183 Intrusion rule



Intrusion

Name: Rule1

Action

□ Appear ☑ Cross

Direction: Both

Target Filter

Effective Ta... ☑ Human

☑ Motor Vehicle

3) Configure the settings for the parameters of drawing rules.

Figure 5-184 Intrusion parameters

Parameter	Description
Name	Enter the customized rule name.
Action	Configure the actions that are defined as intrusion. You can select the **Appear** checkbox and the **Cross** checkbox.
Direction	In the **Direction** list, select the direction of crossing the configured area. You can select **Enter&Exit**, **Enter**, and **Exit**.
Target Filter	Click ⧉ to draw areas to filter the target. 📖 You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (▭). By default, **Human** and **Motor Vehicle** are selected for alarm object.

4) Drag to draw an area.

5) Click **OK** to save the settings.

Step 3 Click ⚙ to set the actions to be triggered.

Step 4 Select the **Enable** checkbox, and then click **Apply**.

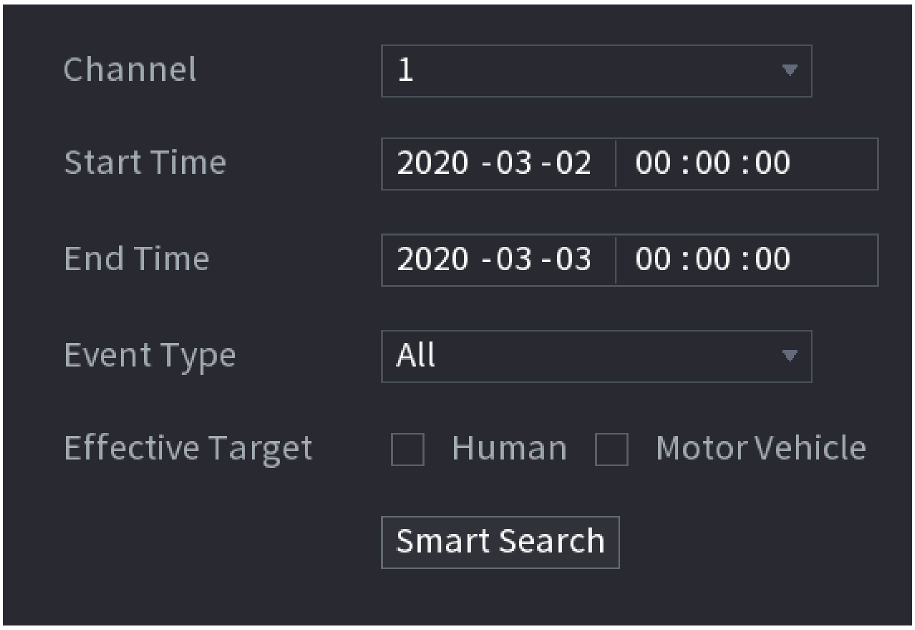
The intrusion detecting function is active. When the target enters and leaves the area, or the target appears in the defined area, the system activates alarms.

5.11.2.3.2 Smart Search for IVS Function

You can search for the intelligent events and play back.

Step 1 Select **Main Menu** > **AI** > **SMART SEARCH** > **IVS**.

Figure 5-185 IVS



Channel: 1

Start Time: 2020 -03 -02 00 :00 :00

End Time: 2020 -03 -03 00 :00 :00

Event Type: All

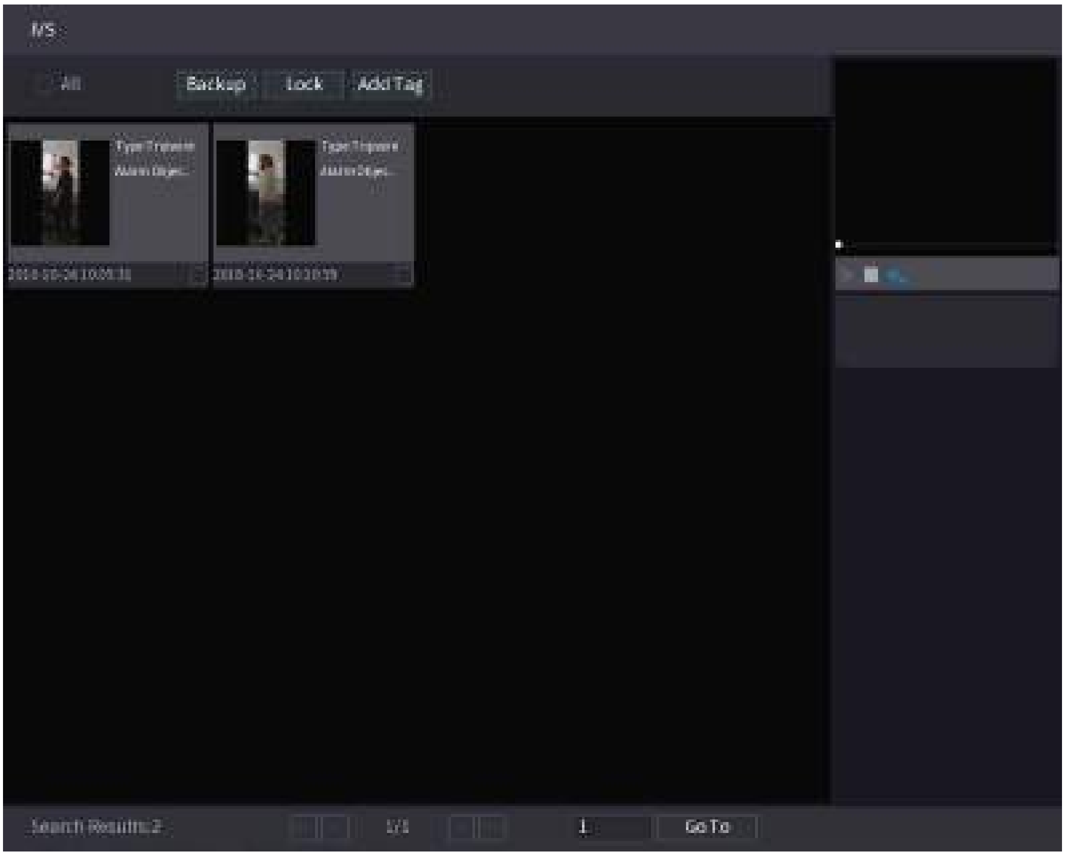
Effective Target: □ Human □ Motor Vehicle

Step 2 In the **Channel** list, select the channel that you want to search for the events, and then set other parameters such as start time, end time, event type, and alarm object.

Step 3 Click **Smart Search**.

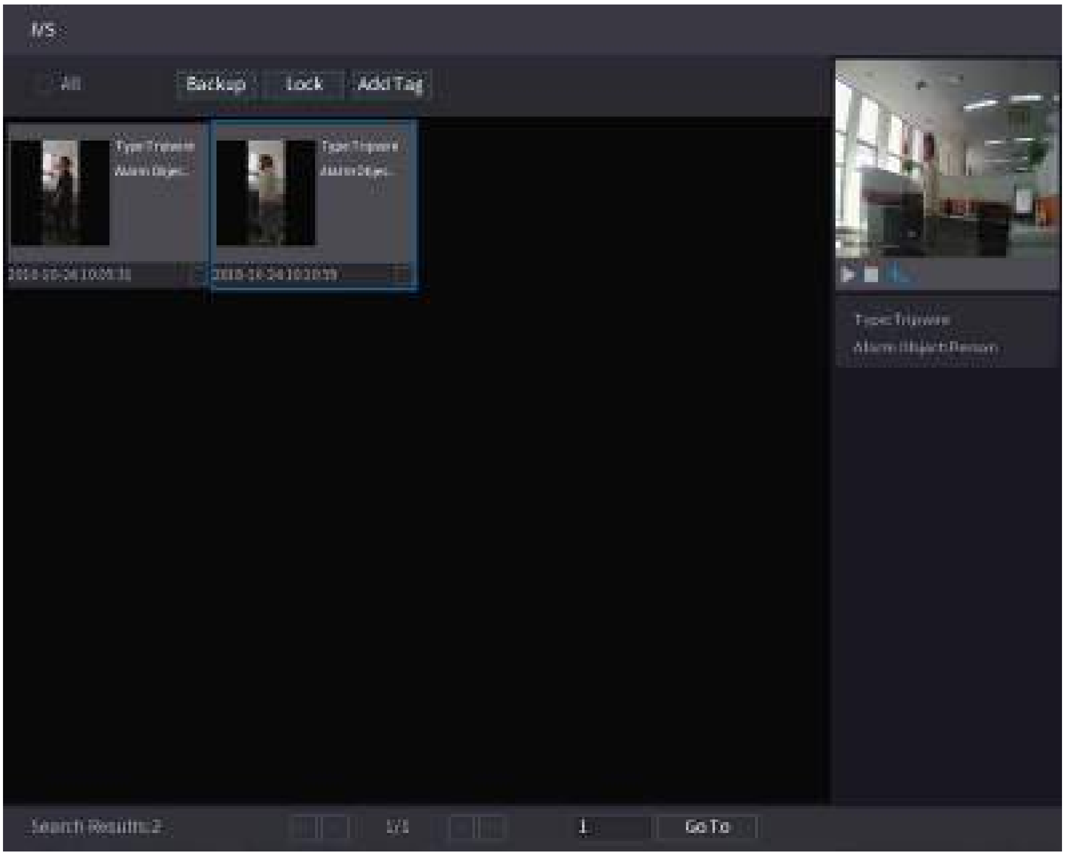
The results that satisfy the searching conditions are displayed.

Figure 5-186 Search results



Step 4 Click the picture that you want to play back.

Figure 5-187 Playback



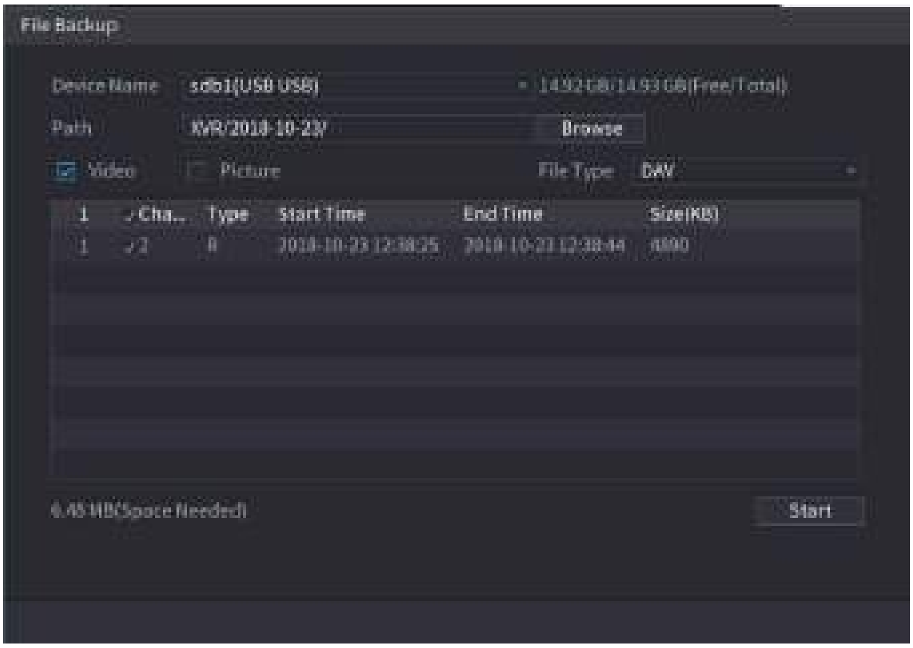
Step 5 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-188 Backup



File Backup

Device Name sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path KVR/2018-10-23/ Browse

☑ Video □ Picture File Type DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	4890

6.48 MB(Space Needed)

Start

- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

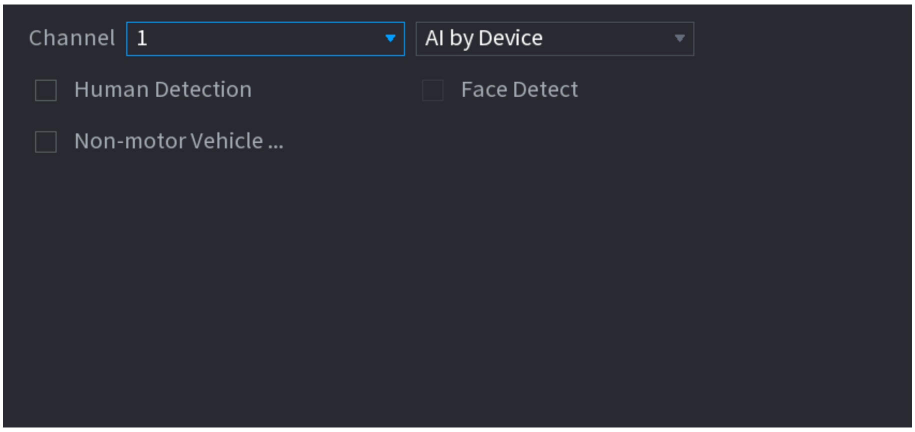
5.11.2.4 Video Structuring

The device can detect and extract key features from the human bodies and non-motor vehicles in the video, and then build a structured database. You can search any target you need with these features.

5.11.2.4.1 Configuring Video Structuring

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

Figure 5-189 Video structuring



Channel 1 | AI by Device

□ Human Detection

□ Face Detect

□ Non-motor Vehicle ...

Step 2 In the **Channel** list, select a channel that you want to configure video structuring function, and then enable it.

Step 3 At **Type**, you can select from **AI by Camera** and **AI by Device**.

- **AI by Camera**: This option requires certain AI cameras. The camera will do all the AI analysis, and then give the results to the DVR.
- **AI by Device:** The camera only transmits normal video stream to the DVR, and then the DVR will do all the AI analysis.

Step 4 You can select from **Human Detection, Face Detect**, and **Non-motor Vehicle**.

- **Human Detection**: Select this option, and then the device will analyze all the human body features in the video, including Top, Top Color, Bottom, Bottom Color, Hat, Bag, Gender, Age, and Umbrella. You can search the target you need with these features. See "Human Body Detection" in "5.11.1.4.2 Smart Search for Video Structuring."
- **Face Detect**: You need to select **Human Detection** first, and then you can select this option. If you select this option, and there is any human face appears in the video, then there will be an extra face image and some extra face features in the human body detection results, including Glasses, Expression, Mask, and Beard. You can search the target you need with these features. See "Human Body Detection" in "5.11.1.4.2 Smart Search for Video Structuring."
- **Non-motor Vehicle**: Select this option, and then the device will analyze all the non-motor vehicle features in the video, including Type, Vehicle Color, People Number, and Helmet. You can search the target you need with these features. See " Non-motor Vehicle Detection" in "5.11.1.4.2 Smart Search for Video Structuring."

Step 5 Click **Apply**.

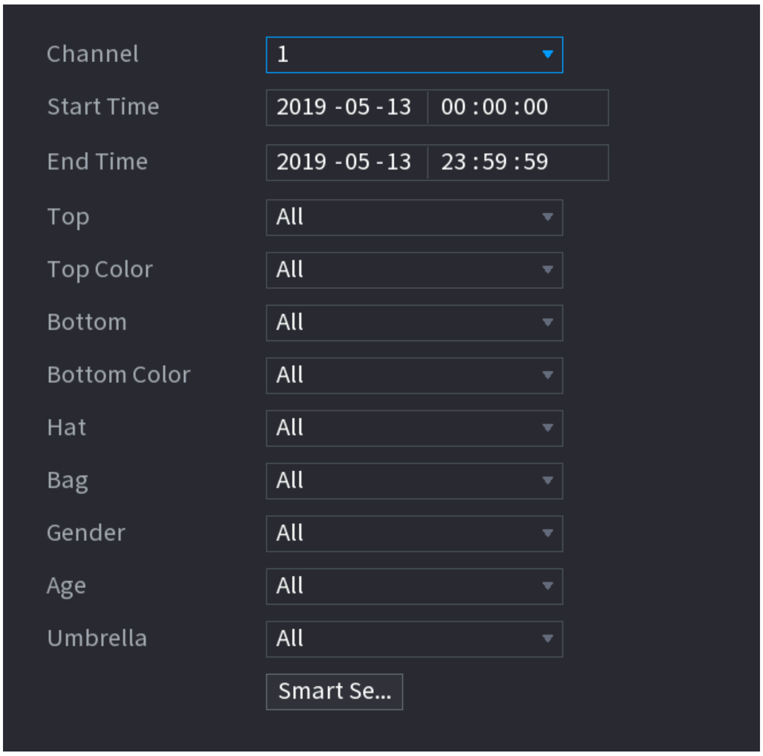
5.11.2.4.2 Smart Search for Video Structuring

You can search the target you need with human body features or non-motor vehicle features

Human Body Detection

Step 1 Select **Main Menu > AI > SMART SEARCH > Human Body Detection**.

Figure 5-190 Human body detection



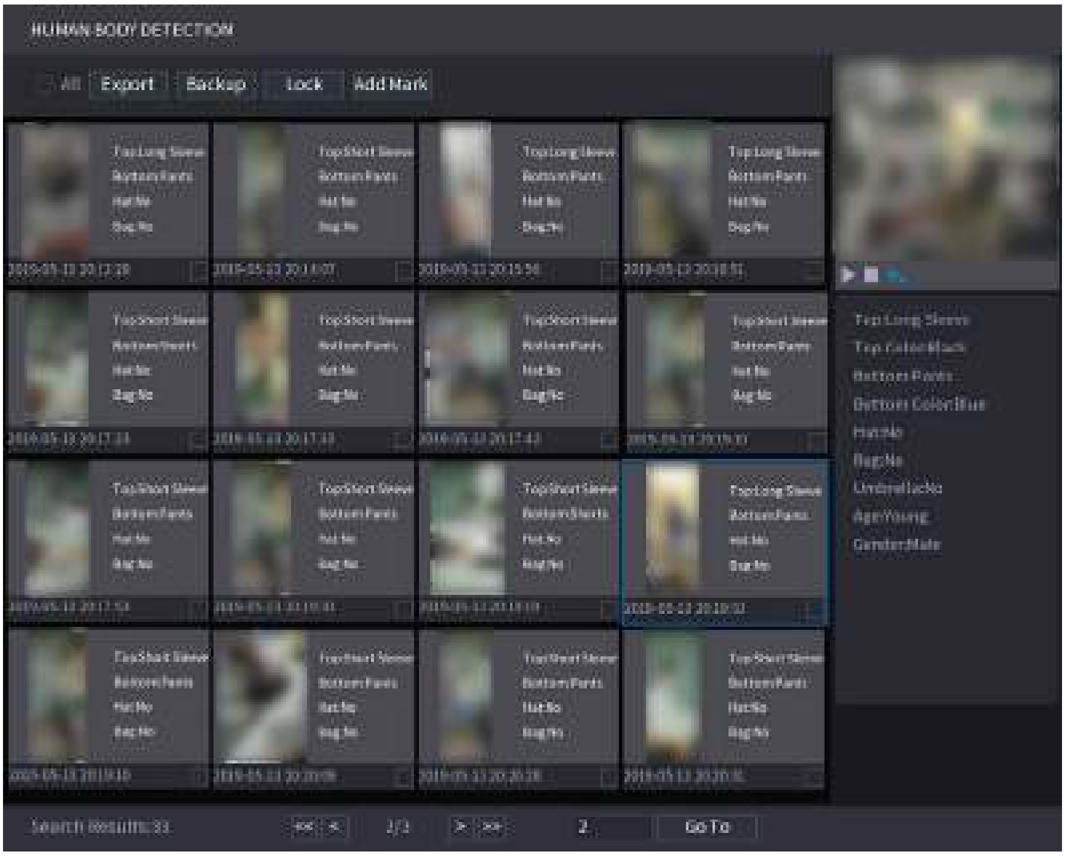
Channel	1
Start Time	2019 -05 -13 00 :00 :00
End Time	2019 -05 -13 23 :59 :59
Top	All
Top Color	All
Bottom	All
Bottom Color	All
Hat	All
Bag	All
Gender	All
Age	All
Umbrella	All

Step 2 Select the channel and the time, and then select one or multiple features from **Top**, **Top Color**, **Bottom**, **Bottom Color**, **Hat**, **Bag**, **Gender**, **Age**, or **Umbrella**.

Step 3 Click **Smart Search**.

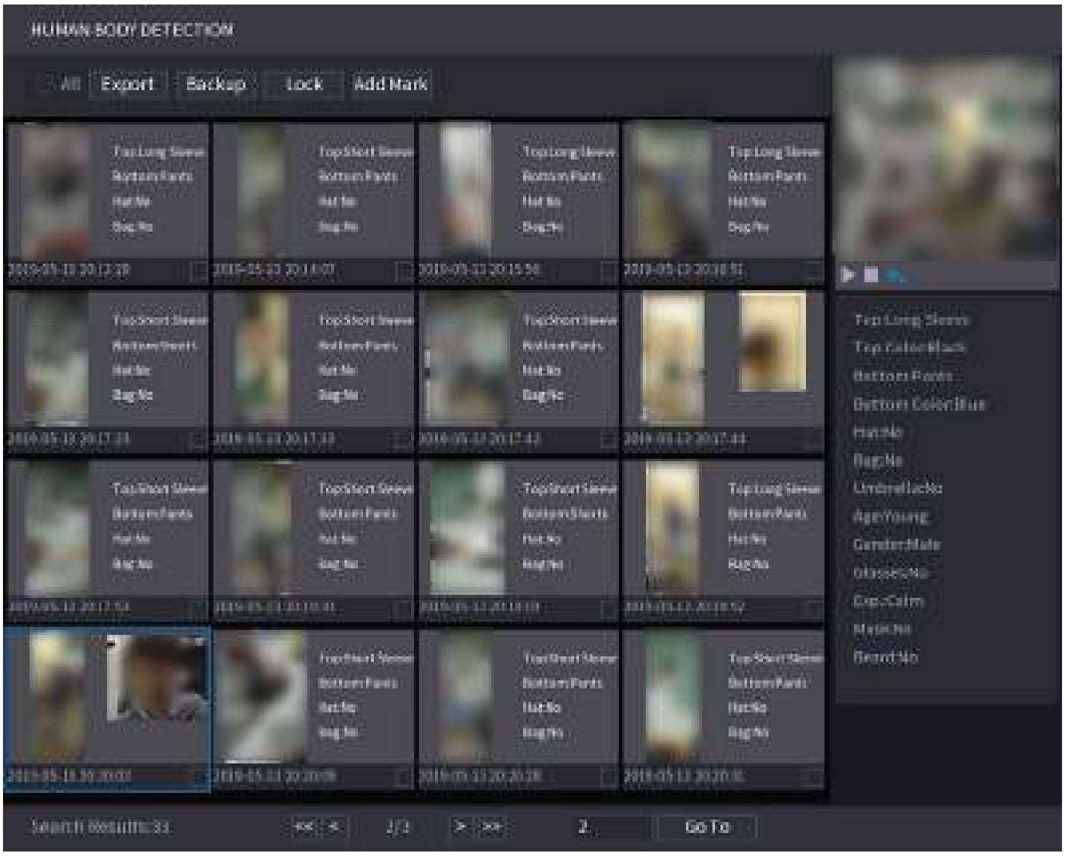
- If you only selected **Human Body Detection** and did not select **Face Detection** in "5.11.1.4.1 Configuring Video Structuring", there will be only human body features displayed in the results.

Figure 5-191 Human body detection



- If you selected **Human Body Detection** and **Face Detection** in "5.11.1.4.1 Configuring Video Structuring", and there is any human face appears in the video, there will be extra face features displayed in the results.

Figure 5-192 Extra face features



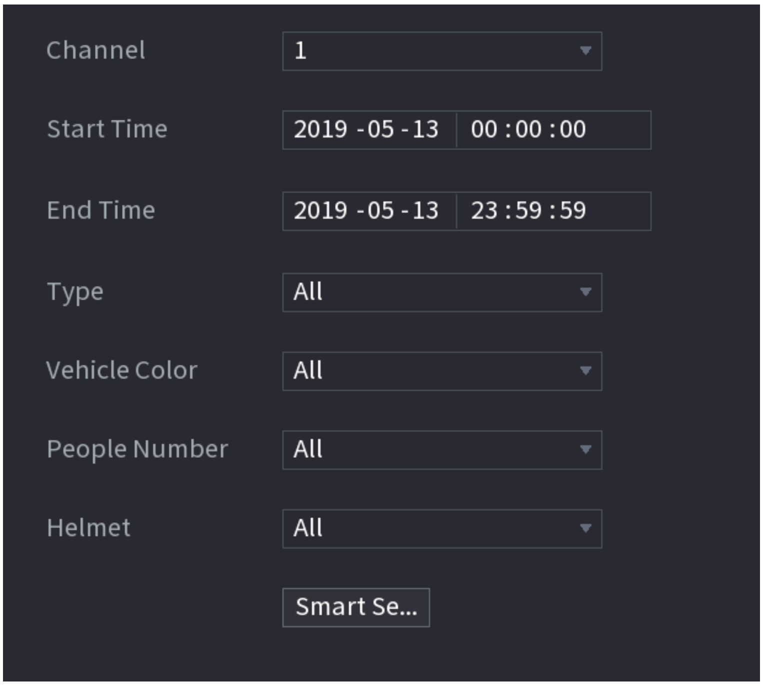
Step 4 Select one or multiple results, and then you can

- Click **Export** to export them to the USB device
- Click **Backup** to make backup in the DVR
- Click **Lock** so that they don't get overwritten or deleted
- Click **Add Tag** to name them as needed.

Non-motor Vehicle Detection

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

Figure 5-193 Non-motor vehicle detection

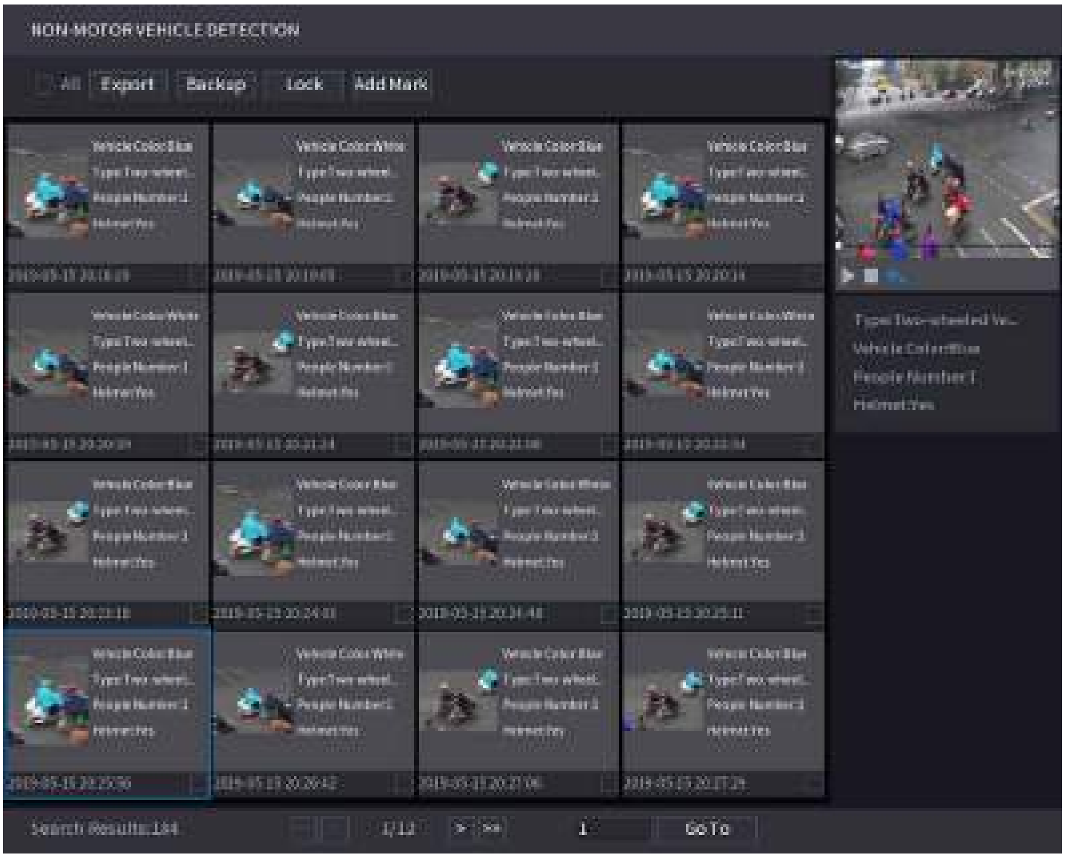


Channel	1
Start Time	2019 -05 -13 00 :00 :00
End Time	2019 -05 -13 23 :59 :59
Type	All
Vehicle Color	All
People Number	All
Helmet	All

Step 2 Select the channel and the time, and then select one or multiple features from **Type**, **Vehicle Color**, **People Number**, or **Helmet**.

Step 3 Click **Smart Search**.

Figure 5-194 Search results



NON-MOTOR VEHICLE DETECTION

Type:Two-wheeled Ve...
Vehicle Color:Blue
People Number:1
Helmet:Yes

Search Results:184

Step 4 Select one or multiple results, and then you can

- Click **Export** to export them to the USB device

- Click **Backup** to make backup in the DVR
- Click **Lock** so that they don't get overwritten or deleted
- Click **Add Tag** to name them as needed.

5.11.3 For Lite AI Series

AI module provides SMD (Smart Motion Detection) and IVS functions. These functions take effect after they are configured and enabled. It adopts deep learning and can realize precision alarms. You can only enable one of them to the same channel at the same time.

- SMD: The device can detect and classify humans and vehicles in the image.
- IVS: The IVS function processes and analyzes the human and vehicle images to extract the key information to match with the preset rules. When the detected behaviors match with the rules, the system activates alarms. The IVS function can avoid wrong alarms by filtering the factors such as rains, light, and animals.
- Face detection: The Device can analyze the faces captured by the camera and link the configured alarms. This function is available for XVR5X-I and XVR 7X-I series only.
- Face recognition: The Device can compare the captured faces with the face database and then link the configured alarms. This function is available for XVR 7X-I series only.

📖

SMD, face detection, face recognition and IVS cannot be enabled simultaneously on select models. For details, see 5.1.4.2 Configuring General Settings.

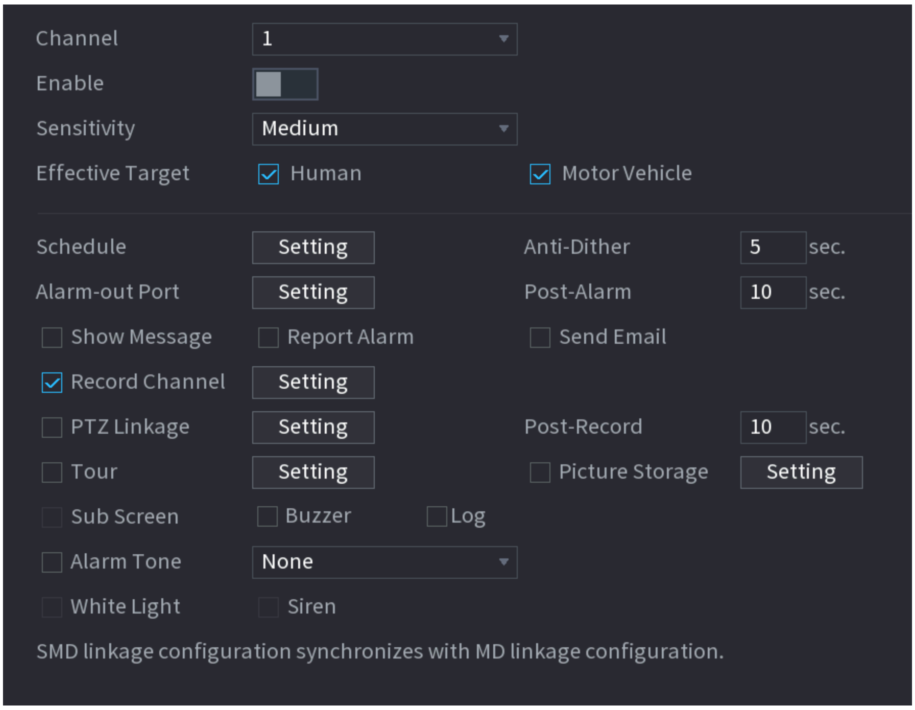
5.11.3.1 SMD

The device can detect and classify humans and vehicles in the image.

5.11.3.1.1 Configuring SMD Parameters

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

Figure 5-195 SMD



Channel 1

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 Setting

□ Sub Screen □ Buzzer □ Log

□ Alarm Tone None

□ White Light □ Siren

SMD linkage configuration synchronizes with MD linkage configuration.

Step 2 In the **Channel** list, select a channel that you want to configure face detection function, and then enable it.

Step 3 Configure the parameters.

Figure 5-196 SMD parameters

Parameter	Description
Channel	In the **Channel** list, select a channel to set the motion detection.
Enable	Enable or disable the motion detection function.
Sensitivity	Set the sensitivity for smart motion detection.
Effective Target	Select human or motor vehicle or both.
Schedule	Define a period during which the motion detection is active.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. ● External Alarm: Enable alarm activation through the connected alarm box. ● Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Show Message	Select the **Show Message** checkbox to enable a pop-up message in your local host PC.

Parameter	Description
Report Alarm	Select the **Report Alarm** checkbox to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs.
Send Email	Select the **Send Email** checkbox to enable the system to send an email notification when an alarm event occurs. 📖 To use this function, make sure the email function is enabled in **Main Menu** > **NETWORK** > **Email**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs. 📖 The recording for motion detection and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs. 📖 Motion Detect can only activate PTZ preset.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Tour	Select the **Tour** checkbox to enable a tour of the selected channels.
Picture Storage	Select the **Snapshot** checkbox to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu** > **CAMERA** > **Encode** > **Snapshot**, in the **Type** list, select **Event**.
Sub Screen	Select the checkbox to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in **Main Menu** > **DISPLAY** > **Tour** > **Sub Screen.** 📖 ● Not all models support this function. ● To use this function, extra screen shall be enabled.
Video Matrix	Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in **Main Menu** > **DISPLAY** > **Tour**. 📖 Not all models support this function.
Buzzer	Select the checkbox to activate a buzzer noise at the Device.
Log	Select the checkbox to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a motion detection event.
White Light	Select the checkbox to enable white light alarm of the camera.

Parameter	Description
Siren	Select the checkbox to enable sound alarm of the camera.

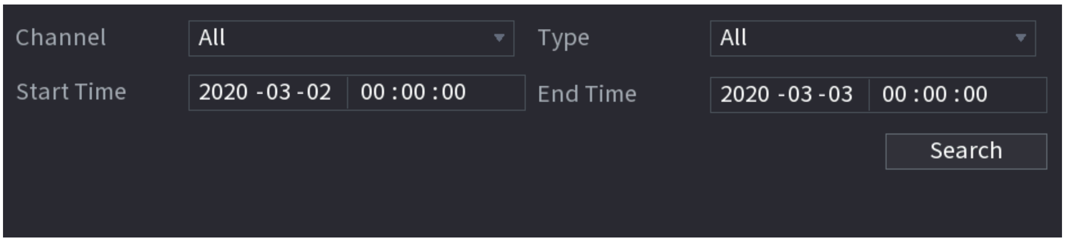
Step 4 Click **Apply** to complete the settings.

5.11.3.1.2 Searching for SMD Reports

You can search the detection history by channel, object type, and time.

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

Figure 5-197 SMD



Channel: All
Type: All
Start Time: 2020 -03 -02 00 :00 :00
End Time: 2020 -03 -03 00 :00 :00

Step 2 Select the channel, enter the start time and end time, and select the object type you need.

Step 3 Click **Search**.

The results are displayed.

5.11.3.2 Configuring IVS Function

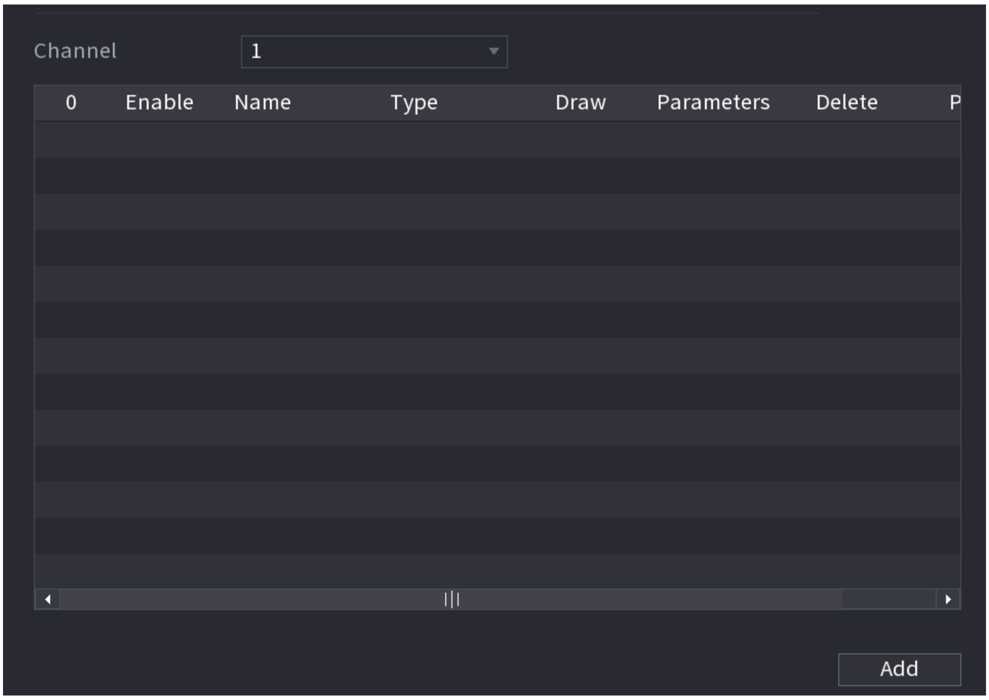
The IVS function processes and analyzes the images to extract the key information to match with the preset rules. When the detected behaviors match with the rules, the system activates alarms.

5.11.3.2.1 Configuring IVS Parameters

The alarms are generated according to the configured parameters.

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

Figure 5-198 IVS



Channel: 1

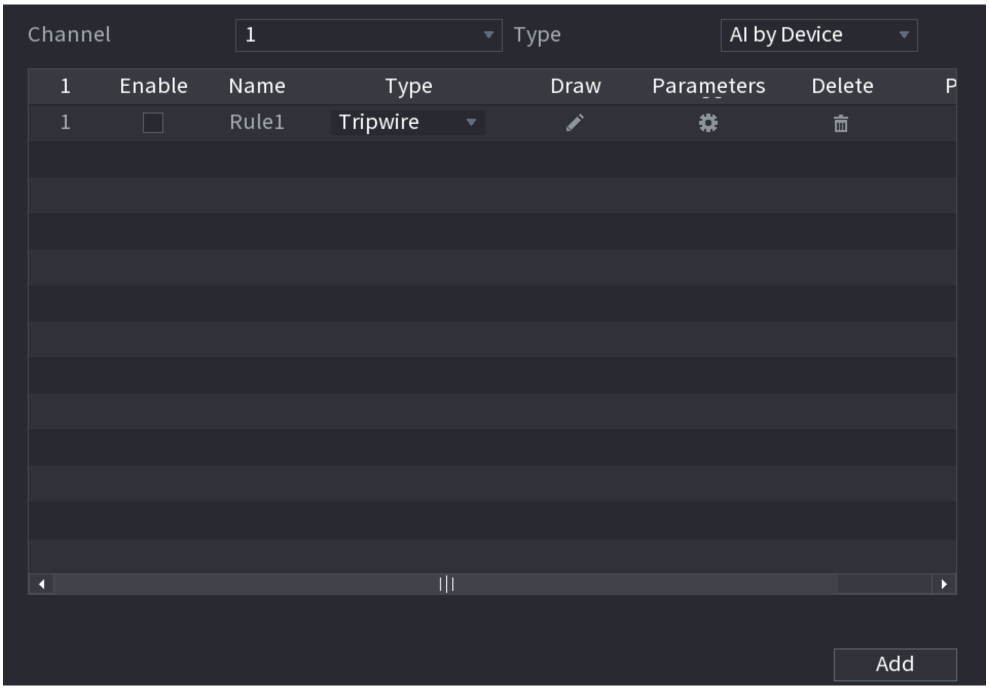
0	Enable	Name	Type	Draw	Parameters	Delete	P

You can enable the AI Mode, and then the detection accuracy would be improved, but the video stream quantity that the DVR can process will reduce.

Step 2 In the **Channel** list, select the channel number that you want to configure the IVS function.

Step 3 Click **Add**.

Figure 5-199 Added rule



Channel: 1 Type: AI by Device

1	Enable	Name	Type	Draw	Parameters	Delete	P
1	□	Rule1	Tripwire	✎	⚙	🗑	

Step 4 Configure the parameters for the rule that you selected.

Step 5 Select the checkbox of the rule to enable it.

Step 6 Click **Apply** to complete the settings.

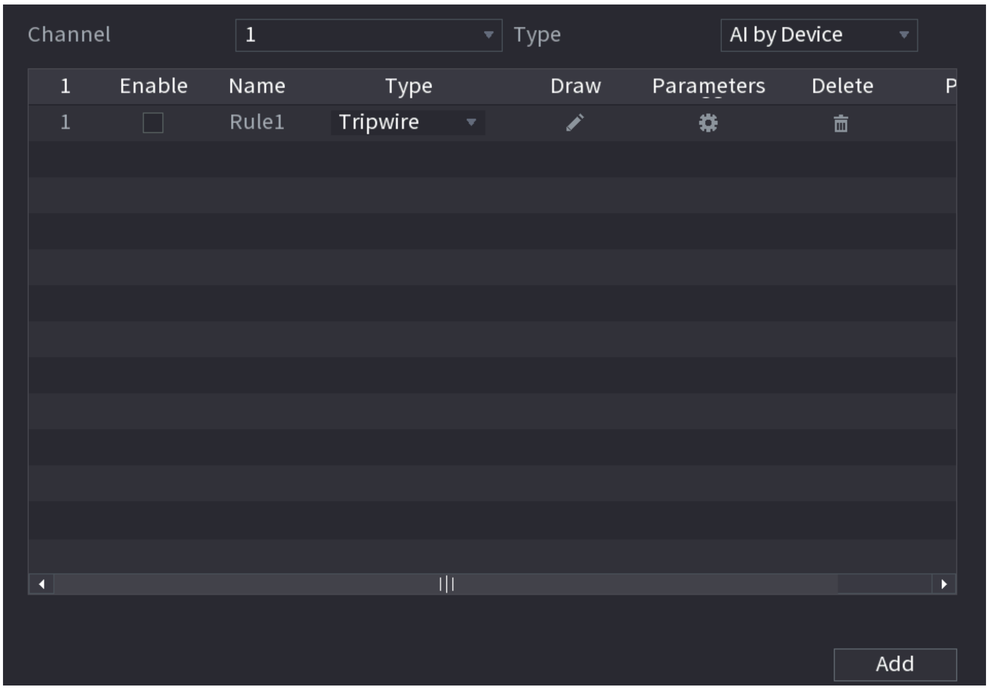
Configuring Tripwire Rules

When the target object crosses the tripwire in the defined direction, the system activates alarms.

- The tripwire can be configured as a straight line or broken line.
- Supports detecting one-way or two-way tripwire crossing.
- Supports multiple tripwires in the same scenario to meet the complexity.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Tripwire**.

Figure 5-200 Tripwire



Channel: 1 Type: AI by Device

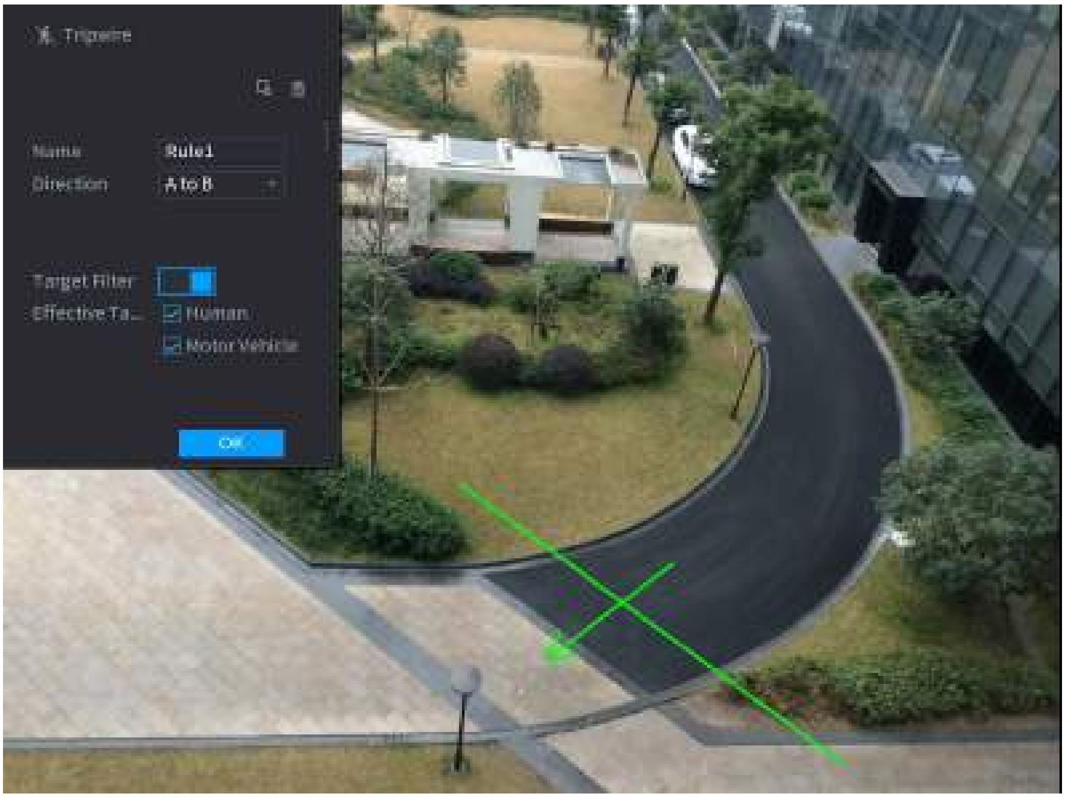
1	Enable	Name	Type	Draw	Parameters	Delete	P
1	□	Rule1	Tripwire	✎	⚙	🗑	

Step 2 Draw a tripwire.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click ✎.

Figure 5-201 Tripwire rule



Tripwire

Name: Rule1

Direction: A to B

Target Filter

Effective Ta...: ☑ Human ☑ Motor Vehicle

3) Configure the settings for the parameters of drawing rules.

Table 5-37 Tripwire parameters

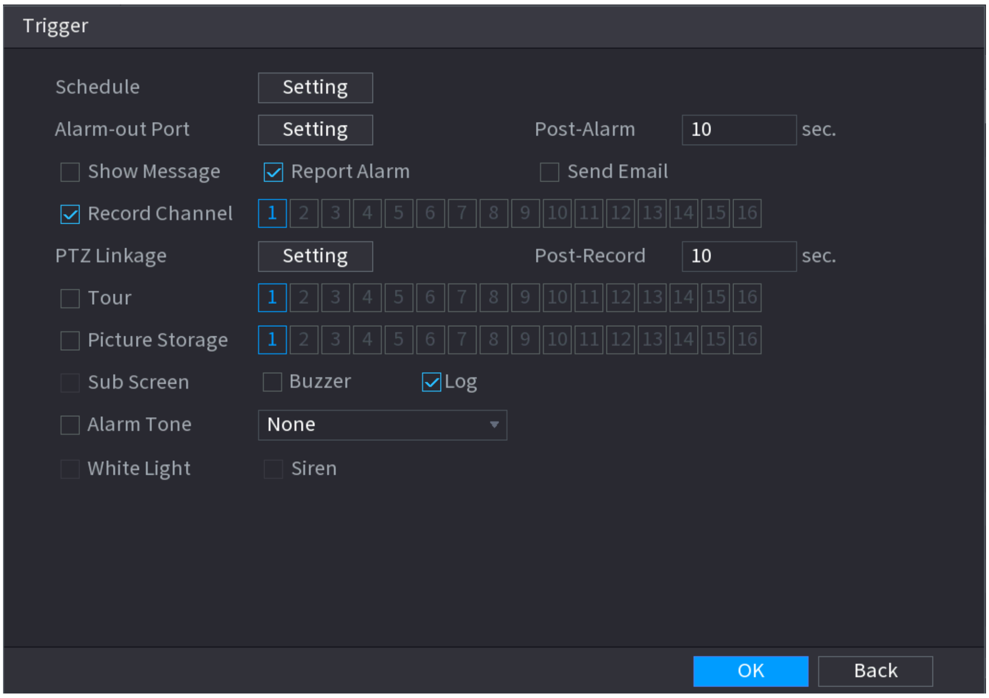
Parameter	Description
Name	Enter the customized rule name.
Direction	Set the direction of the tripwire. You can choose **A to B** (left to right), **B to A** (right to left), and **Both**.
Target Filter	Click ⧉ to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (●). By default, **Human** and **Motor Vehicle** are selected for alarm object.

4) Drag to draw a tripwire. The tripwire can be a straight line, broken line or polygon.

5) Click **OK** to save the settings.

Step 3 Click ⚙ to set the actions to be triggered.

Figure 5-202 Trigger



Trigger

Schedule: Setting

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

□ Show Message   ☑ Report Alarm   □ Send Email

☑ Record Channel: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

PTZ Linkage: Setting   Post-Record: 10 sec.

□ Tour: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Picture Storage: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Sub Screen   □ Buzzer   ☑ Log

□ Alarm Tone: None

□ White Light   □ Siren

OK   Back

Step 4 Configure the triggering parameters.

Table 5-38 Triggering parameters

Parameter	Description
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."

Parameter	Description
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable general alarm and select the alarm output port. ● Ext. Alarm: Connect the alarm box to the Device and then enable it. Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the **Show Message** checkbox to enable a pop-up alarm message in your local host PC.
Report Alarm	Select the **Report Alarm** checkbox to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs. 📖 ● Not all models support this function. ● The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."
Send Email	Select the **Send Email** checkbox to enable the system to send an email notification when an alarm event occurs. 📖 To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs. 📖 The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs. 📖 To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post-Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.

Parameter	Description
Tour	Select the **Tour** checkbox to enable a tour of the selected channels. 📖 ● To use this function, the tour setting must be configured. ● After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the **Snapshot** checkbox to take a snapshot of the selected channel. 📖 To use this function, make sure the snapshot function is enabled for **Intel** in **Main Menu > STORAGE > Schedule > Snapshot**.
Video Matrix	Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "**Main Menu > DISPLAY > Tour > Sub Screen**." 📖 ● Not all models support this function. ● The extra screen must be enabled to support this function.
Buzzer	Select the checkbox to activate a buzzer noise at the Device.
Log	Select the checkbox to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.

Step 5 Click **OK** to save the settings.

Step 6 Select the **Enable** checkbox, and then click **Apply**.

The tripwire detecting function is active. When the target object crosses the tripwire in the defined direction, the system activates alarms.

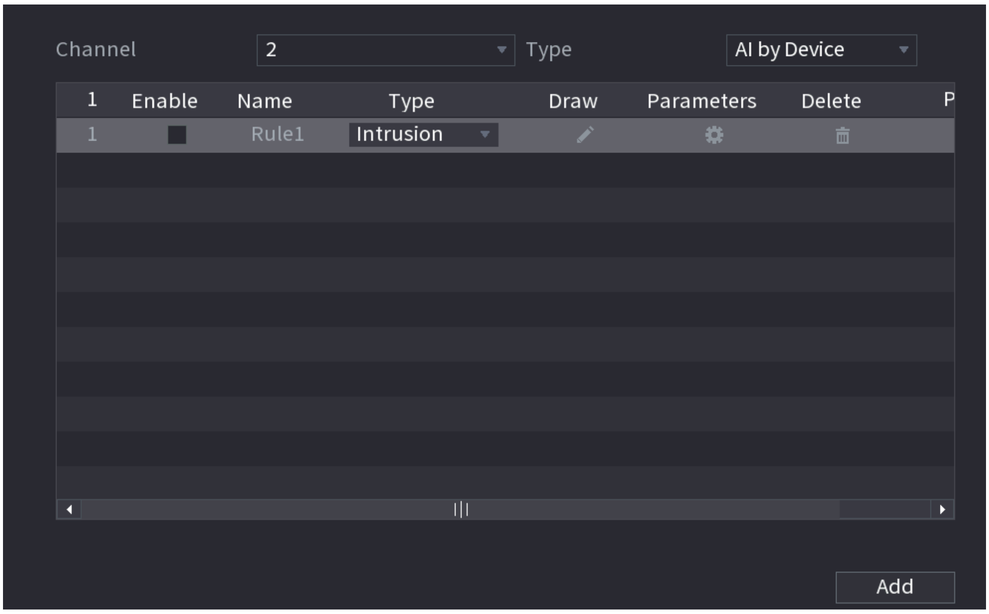
Configuring Intrusion Rules

When the target enters and leaves the defined detection area, or the target appears in the defined area, the system activates alarms.

- You can define the shape and quantity of intrusion areas.
- Supports detecting the behaviors that enter and leave the intrusion areas.
- Supports detecting the behaviors that are moving in the intrusion areas. The quantity of areas and lasting time can be configured.
- Supports size filtering for target.

Step 1 On the rule line that you added, in the **Type** list, select **Intrusion**.

Figure 5-203 Intrusion



Channel 2 Type AI by Device

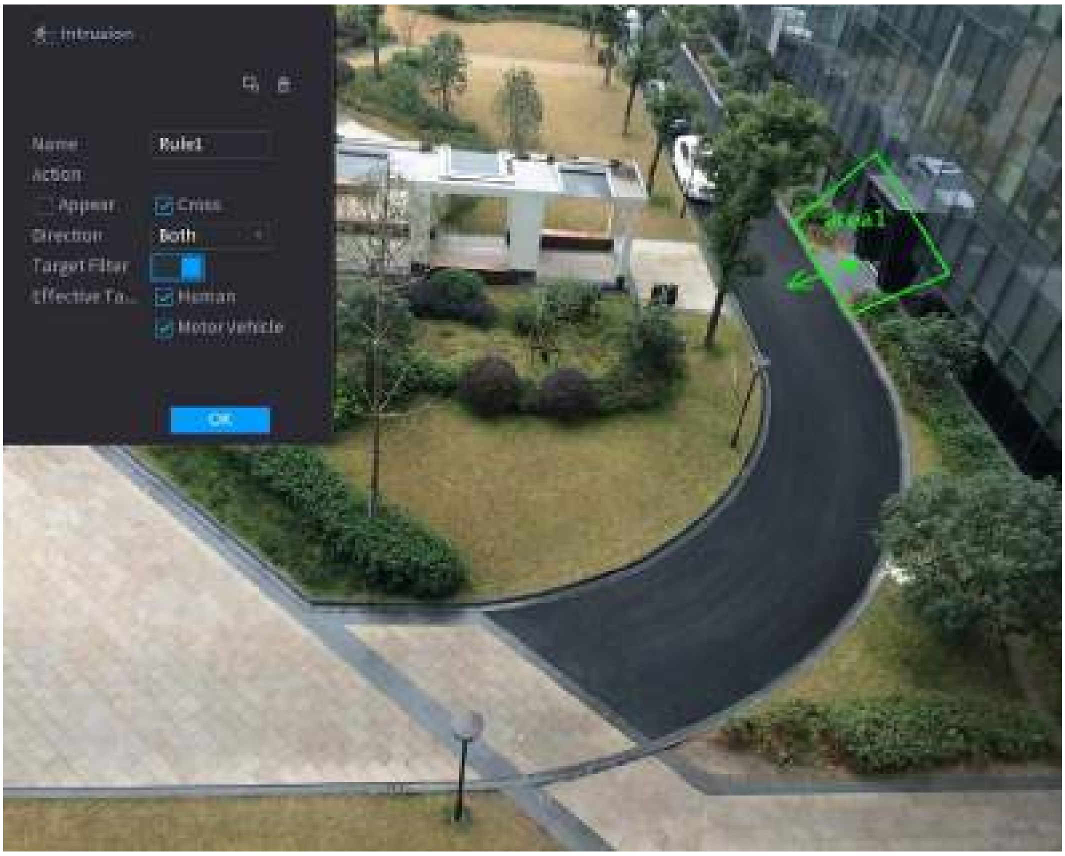
1	Enable	Name	Type	Draw	Parameters	Delete	P
1	■	Rule1	Intrusion	✎	⚙	🗑	

Step 2 Draw an area.

1) In the **Channel** list, select the channel that you want to configure the rules for.

2) Click ✎.

Figure 5-204 Intrusion rule



Intrusion

Name: Rule1

Action

□ Appear ☑ Cross

Direction: Both

Target Filter: ●

Effective To...: ☑ Human ☑ Motor Vehicle

3) Configure the settings for the parameters of drawing rules.

Table 5-39 Intrusion parameters

Parameter	Description
Name	Enter the customized rule name.
Action	Configure the actions that are defined as intrusion. You can select the **Appear** checkbox and the **Cross** checkbox.
Direction	In the **Direction** list, select the direction of crossing the configured area. You can select **Enter&Exit**, **Enter**, and **Exit**.
Target Filter	Click to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target that is crossing the tripwire is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Effective Target	Enable the AI Recognition function (). By default, **Human** and **Motor Vehicle** are selected for alarm object.

4) Drag to draw an area.

5) Click **OK** to save the settings.

Step 3 Click to set the actions to be triggered.

Step 4 Select the **Enable** checkbox, and then click **Apply**.

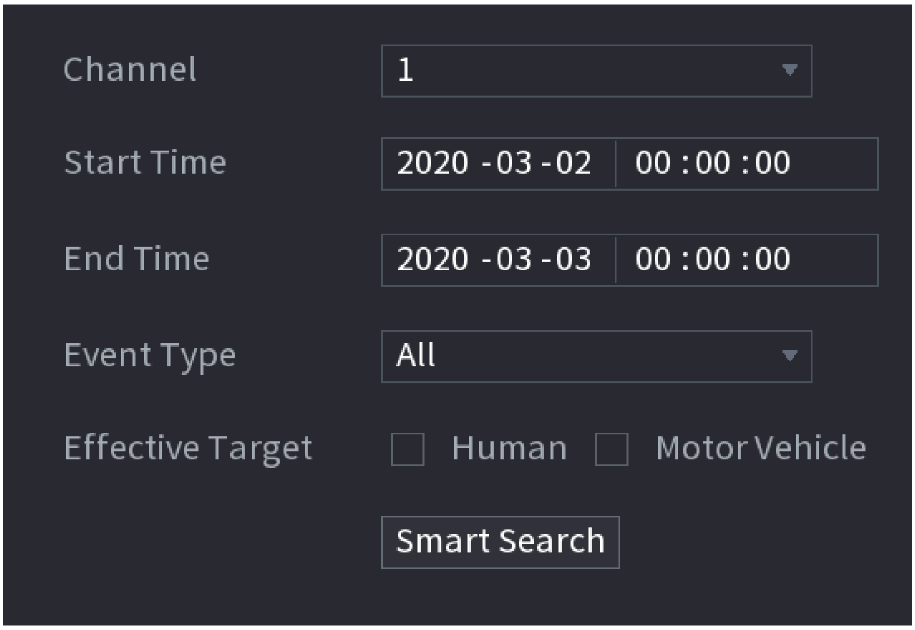
The intrusion detecting function is active. When the target enters and leaves the area, or the target appears in the defined area, the system activates alarms.

5.11.3.2.2 Smart Search for IVS Function

You can search for the intelligent events and play back.

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

Figure 5-205 IVS



Channel: 1

Start Time: 2020 -03 -02 00 :00 :00

End Time: 2020 -03 -03 00 :00 :00

Event Type: All

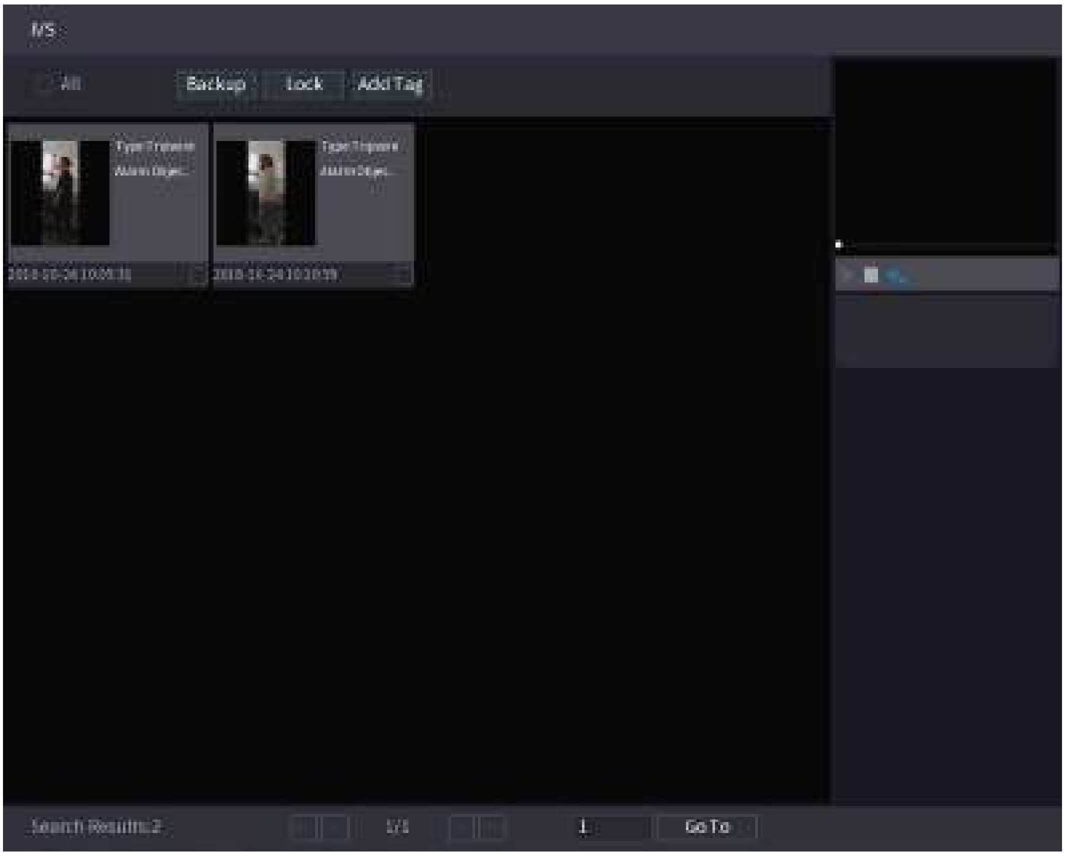
Effective Target: □ Human □ Motor Vehicle

Step 2 In the **Channel** list, select the channel that you want to search for the events, and then set other parameters such as start time, end time, event type, and alarm object.

Step 3 Click **Smart Search**.

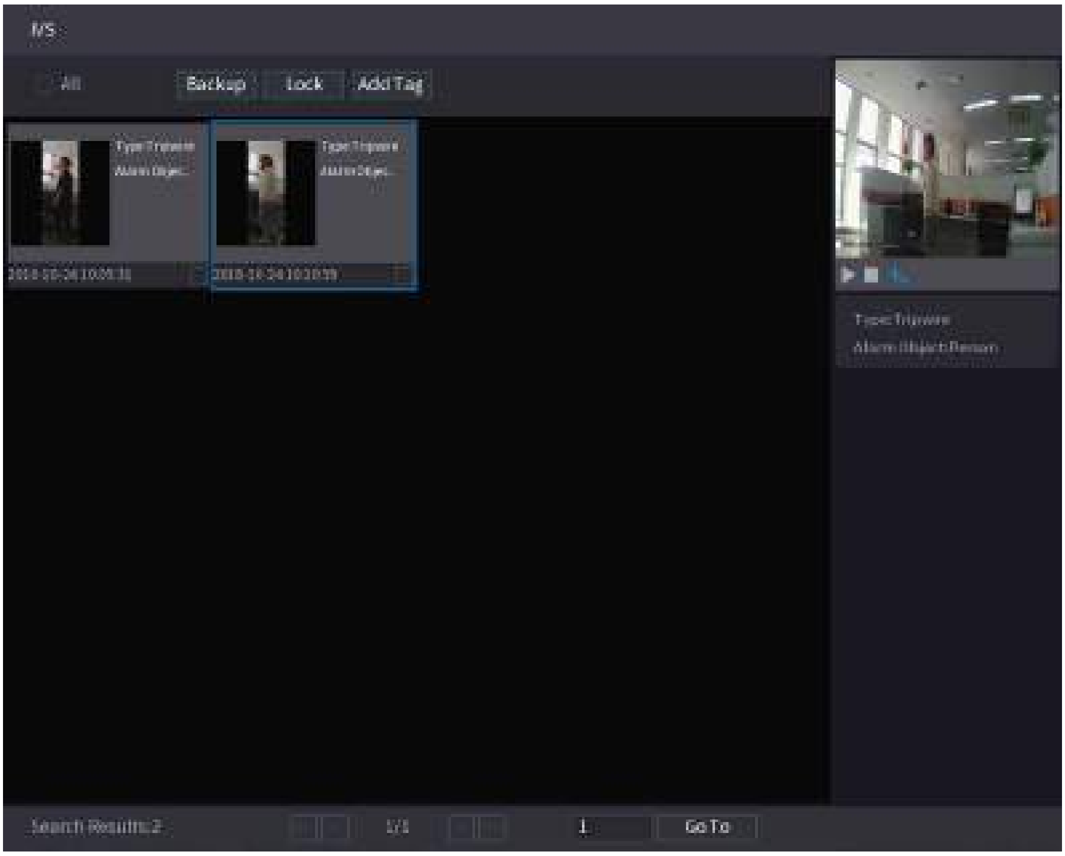
The results that satisfy the searching conditions are displayed.

Figure 5-206 Search results



Step 4 Click the picture that you want to play back.

Figure 5-207 Playback



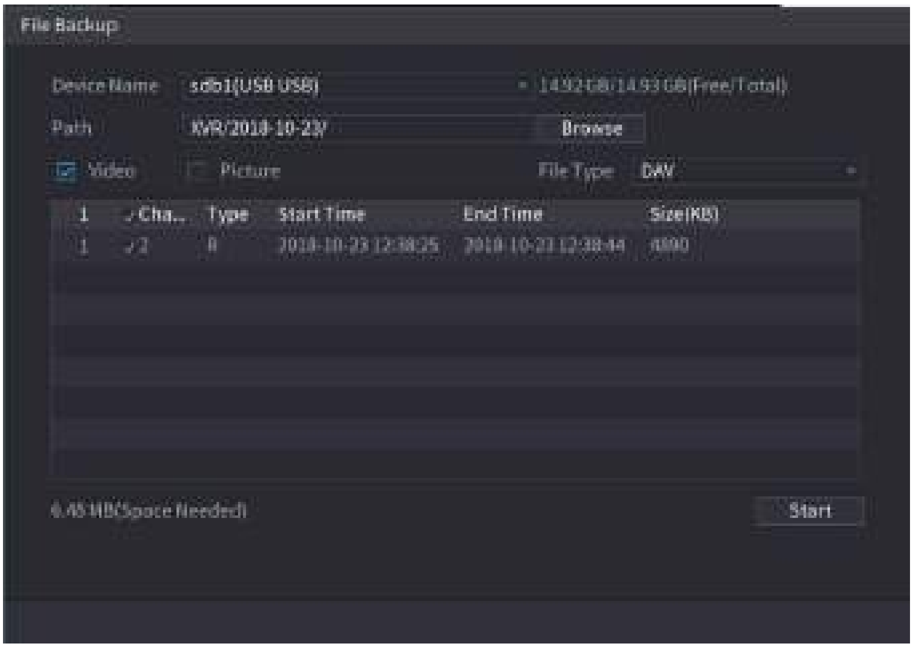
Step 5 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-208 Backup



File Backup

Device Name: sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path: XVR/2018-10-23/ Browse

☑ Video ☐ Picture File Type: DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	4890

6.48 MB(Space Needed)

Start

- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.3.3 Face Detection (For XVR5X-I and XVR7X-I series only)

Some series of devices can analyze the pictures captured by the camera to detect whether the faces are on the pictures. You can search and filter the recorded videos the faces and play back.

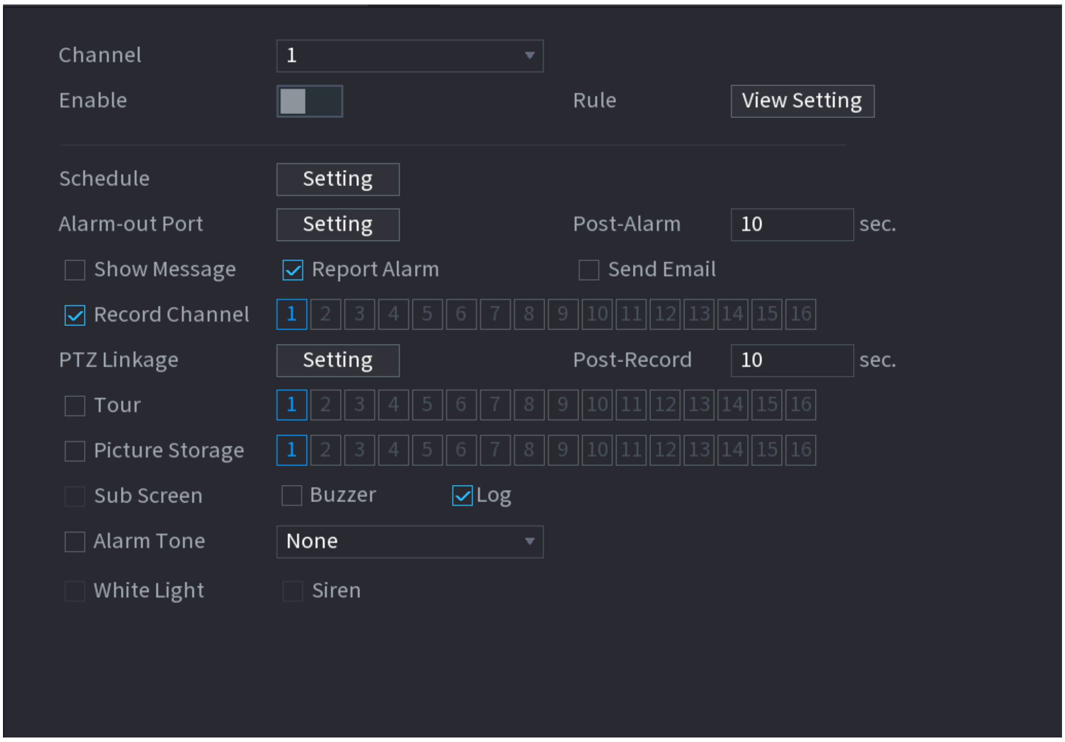
If you select AI by device, then among face detection and recognition, IVS function, you can use one of them at the same time for the same channel.

5.11.3.3.1 Configuring Face Detection Parameters

The alarms are generated according to the configured parameters.

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Face Detection**.

Figure 5-209 Face detection



Channel 1

Enable □ Rule View Setting

Schedule Setting

Alarm-out Port Setting Post-Alarm 10 sec.

□ Show Message ☑ Report Alarm □ Send Email

☑ Record Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

PTZ Linkage Setting Post-Record 10 sec.

□ Tour 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Picture Storage 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

□ Sub Screen □ Buzzer ☑ Log

□ Alarm Tone None

□ White Light □ Siren

Step 2 In the **Channel** list, select a channel that you want to configure face detection function, and then enable it.

Step 3 Configure the parameters.

Table 5-40 Face detection parameters

Parameter	Description
Rule	Click **View Setting** to draw areas to filter the target. You can configure two filtering targets (maximum size and minimum size). When the target is smaller than the minimum size or larger than the maximum size, no alarms will be activated. The maximum size should be larger than the minimum size.
Schedule	Define a period during which the detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable general alarm and select the alarm output port. ● Ext. Alarm: Connect the alarm box to the Device and then enable it. ● Wireless Siren: Connect the wireless gateway to the Device and then enable it. For details, see "5.12 IoT Function." When an alarm event occurs, the system links the peripheral alarm devices connected to the selected output port.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds. If you enter 0, there will be no delay.
Show Message	Select the **Show Message** checkbox to enable a pop-up alarm message in your local host PC.

Parameter	Description
Report Alarm	Select the **Report Alarm** checkbox to enable the system to upload the alarm signal to the network (including alarm center) when an alarm event occurs. 📖 ● Not all models support this function. ● The corresponding parameters in the alarm center should be configured. For details, see "5.15.1.12 Configuring Alarm Center Settings."
Send Email	Select the **Send Email** checkbox to enable the system to send an email notification when an alarm event occurs. 📖 To use this function, make sure the email function is enabled in **Main Menu** > **NETWORK** > **Email**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs. 📖 The recording for intelligence event and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs. 📖 To use this function, the PTZ operations must be configured. For details, see "5.4 Controlling PTZ Cameras."
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds.
Tour	Select the **Tour** checkbox to enable a tour of the selected channels. 📖 ● To use this function, the tour setting must be configured." ● After the tour is ended, the live view screen returns to the view layout before tour started.
Picture Storage	Select the **Picture Storage** checkbox to take a snapshot of the selected channel. 📖 To use this function, make sure the snapshot function is enabled for **Intel** in **Main Menu** > **STORAGE** > **Schedule** > **Snapshot**.
Video Matrix	Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in **Main Menu** > **DISPLAY** > **TOUR** > **Extra Screen**. 📖 ● Not all models support this function. ● The extra screen must be enabled to support this function.

Parameter	Description
Buzzer	Select the checkbox to activate a buzzer noise at the Device.
Log	Select the checkbox to enable the Device to record a local alarm log.
Alarm Tone	Select to enable audio broadcast in response to a face detection event.
White Light	Select the checkbox to enable the white light alarm of the camera.
Siren	Select the checkbox to enable the sound alarm of the camera.

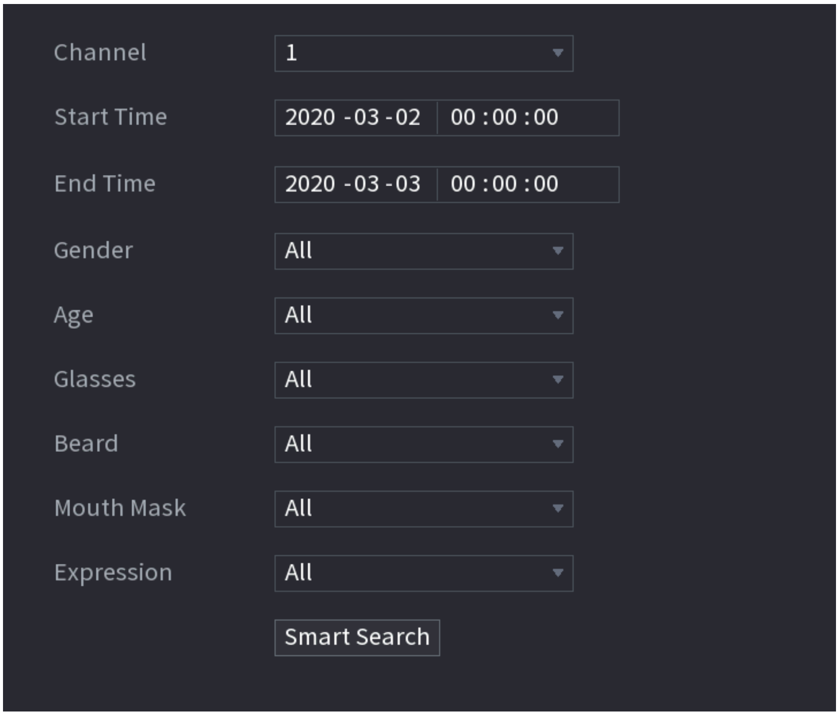
Step 4 Click **Apply** to complete the settings.

5.11.3.3.2 Searching for and Playing Detected Faces

You can search the detected faces and play back.

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

Figure 5-210 Face detection



Channel: 1

Start Time: 2020 -03 -02 00 :00 :00

End Time: 2020 -03 -03 00 :00 :00

Gender: All

Age: All

Glasses: All

Beard: All

Mouth Mask: All

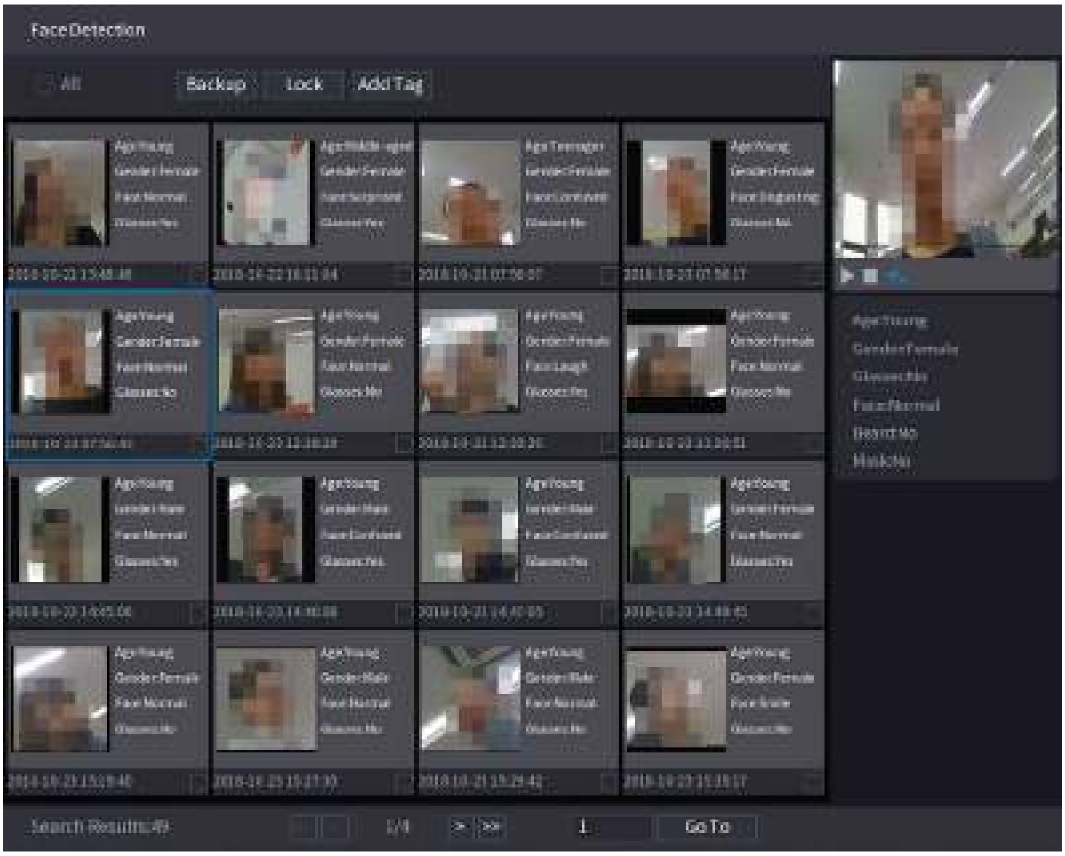
Expression: All

Step 2 Select the channel, enter the start time and end time, and set for the gender, age, glasses, beard, and mask.

Step 3 Click **Smart Search**.

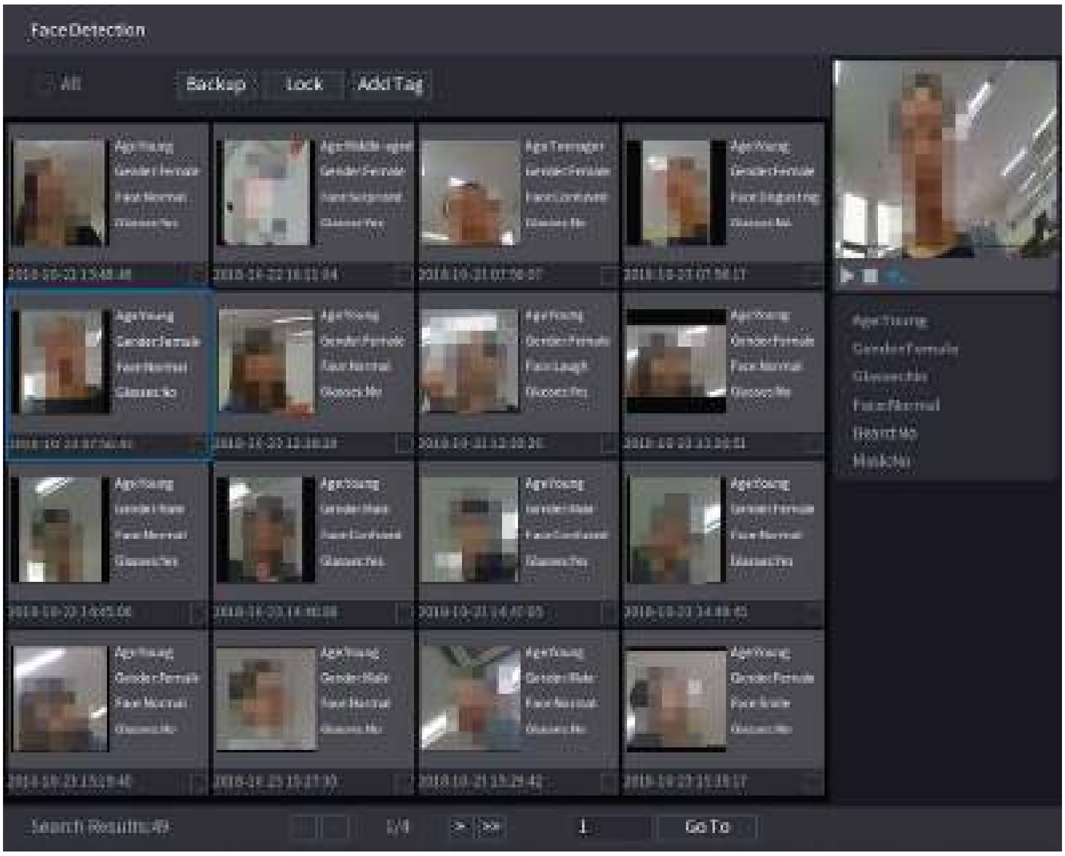
The results are displayed.

Figure 5-211 Search results



Step 4 Select the face that you want to play back.

Figure 5-212 Registered information



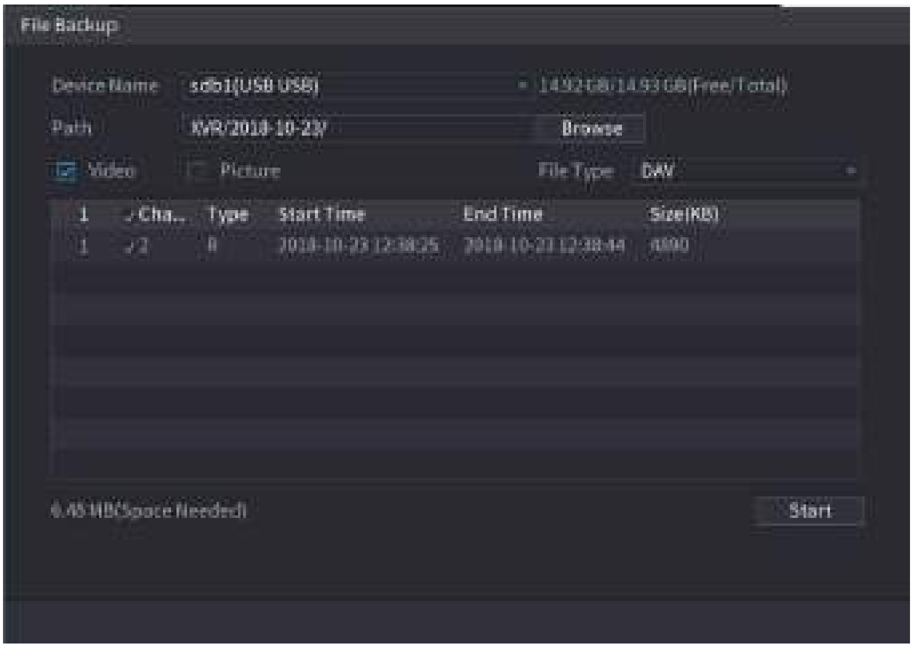
Step 5 And then click ▶ to start playing back the recorded detected face snapshots.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-213 Backup



File Backup

Device Name: sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path: XVR/2018-10-23/ Browse

☑ Video □ Picture File Type: DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	6890

6.45 MB(Space Needed)

Start

- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Tag**.

5.11.3.4 Face Recognition (For XVR7X-I series only)

Face recognition applies to AI preview mode and smart search.

- AI preview mode: Supports comparing the detected faces with the face database, and display the comparison results.
- Smart search: Supports faces searching by faces attributes or portraits.

- If you select AI by device, then among face detection and recognition, IVS function, you can use one of them at the same time for the same channel.
- Before enabling face recognition function for a channel, the face detection must be enabled first for this channel.

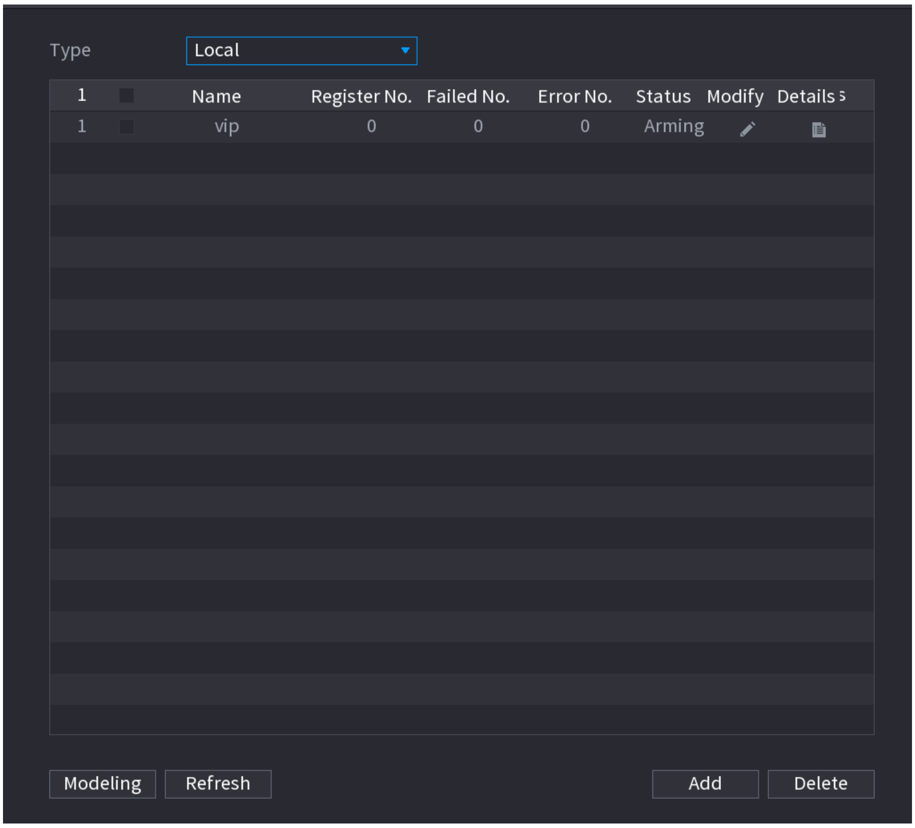
5.11.3.4.1 Face Database Management

You should create a face database for comparing the detected faces and the faces in the database. The Device supports creating maximum 20 databases and registering 100,000 faces.

Creating a Face Database

Step 1 Select **Main Menu > AI > Database > Face Database Config**.

Figure 5-214 Face database configuration



Type: Local

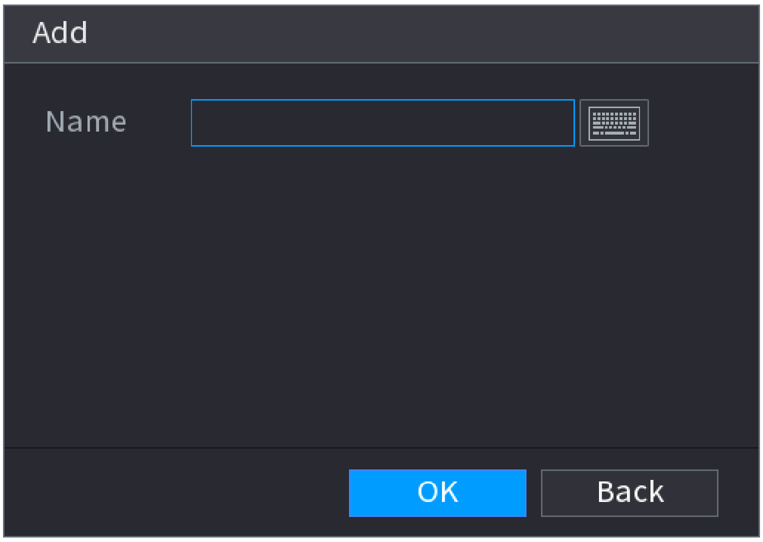
1	□	Name	Register No.	Failed No.	Error No.	Status	Modify	Details
1	□	vip	0	0	0	Arming	✎	🗎

Step 2 At **Type**, you can select **Local** or **Remote**.

- **Local**: Viewing the existing face databases or adding new one on the DVR.
- **Remote**: If you have face recognition camera, you can select this to view the existing face databases or adding new one on the camera.

Step 3 Click **Add**.

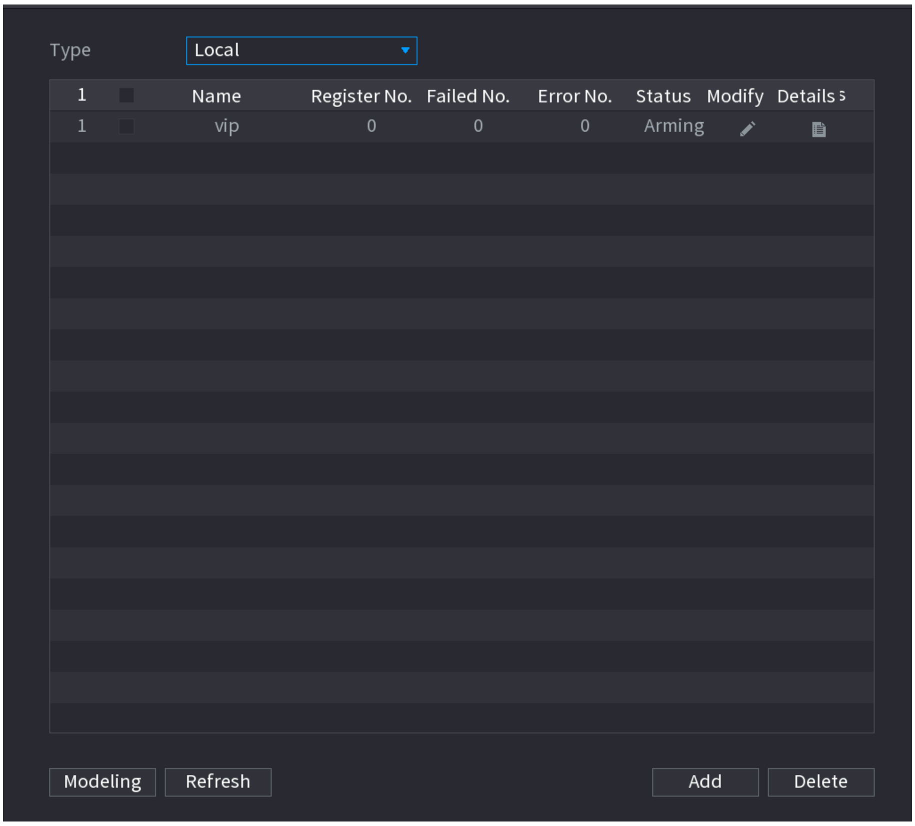
Figure 5-215 Add face database



Step 4 Enter the face database name, and then click **Save**.

- Click ✏ to modify database name.
- Click 📄 to view the database details and add new faces to the database. For details, see "Adding Face Pictures."
- Select the database, and then click **Modeling**. The system will extract the attributes of face pictures in the database for the future comparison.
- Select the database, and then click **Delete** to delete the database.

Figure 5-216 Configure face database



Type: Local

1	□	Name	Register No.	Failed No.	Error No.	Status	Modify	Details
1	□	vip	0	0	0	Arming	✏	📄

Adding Face Pictures

You can add face pictures to the existing databases one by one or by batch, or add from the detected faces.

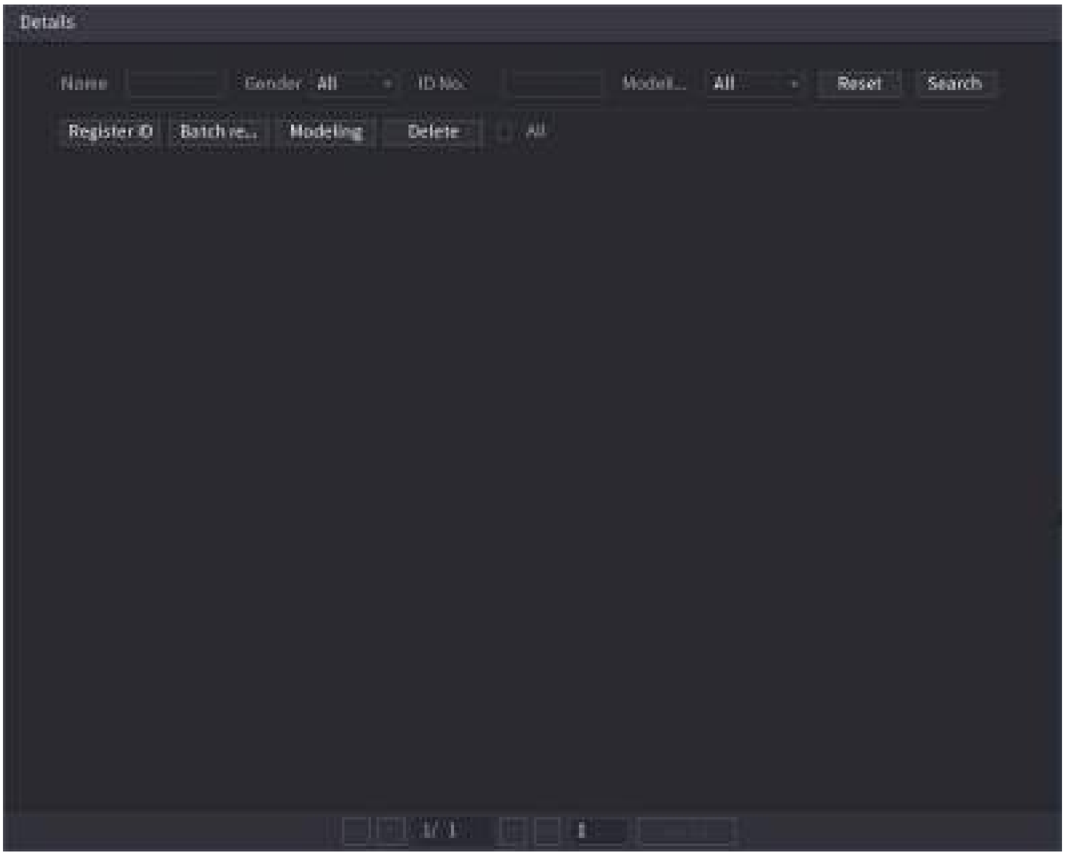
To add face pictures one by one or by batch, you need to get the pictures from the USB storage device. The picture size should be smaller than 256K with resolution between 200×200–6000×5000.

Adding One Face Picture

Step 1 Select **Main Menu > AI > Database > Face Database Config**.

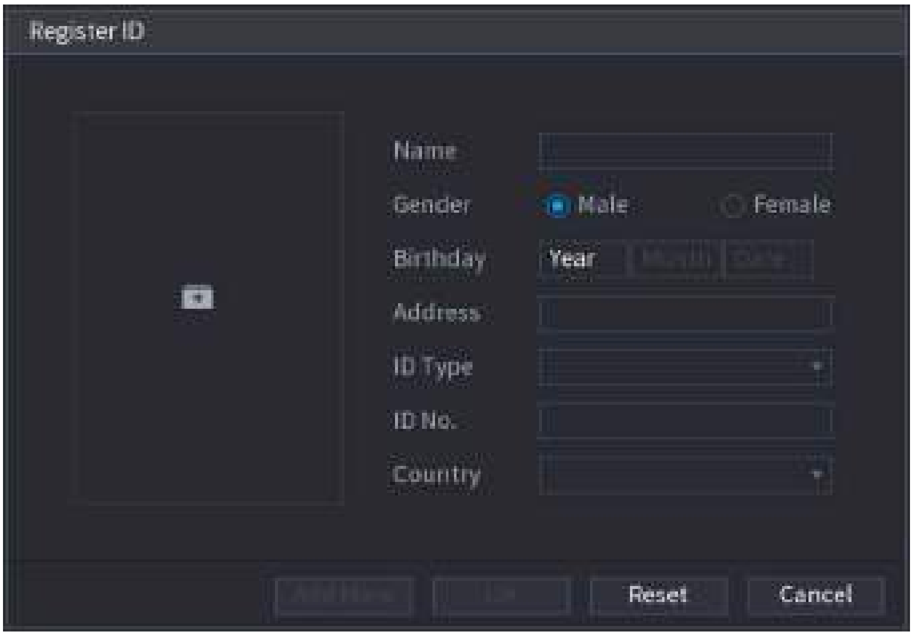
Step 2 Click 📄 of the database that you want to configure.

Figure 5-217 Details



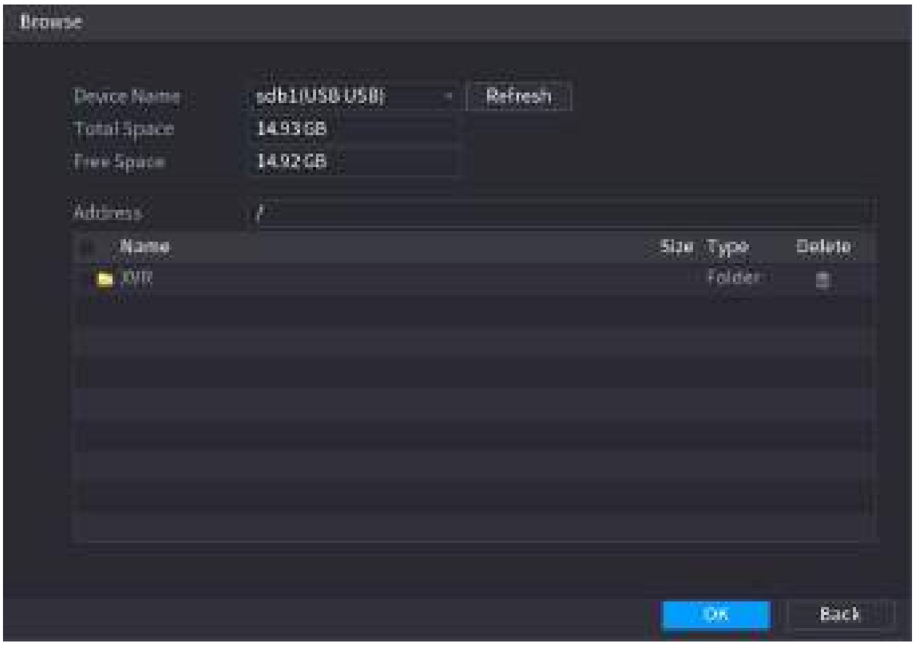
Step 3 Click **Register ID**.

Figure 5-218 Register ID



Step 4 Click + to add a face picture.

Figure 5-219 Browse



Browse

Device Name: sdb1(USB USB) Refresh

Total Space: 14.93 GB

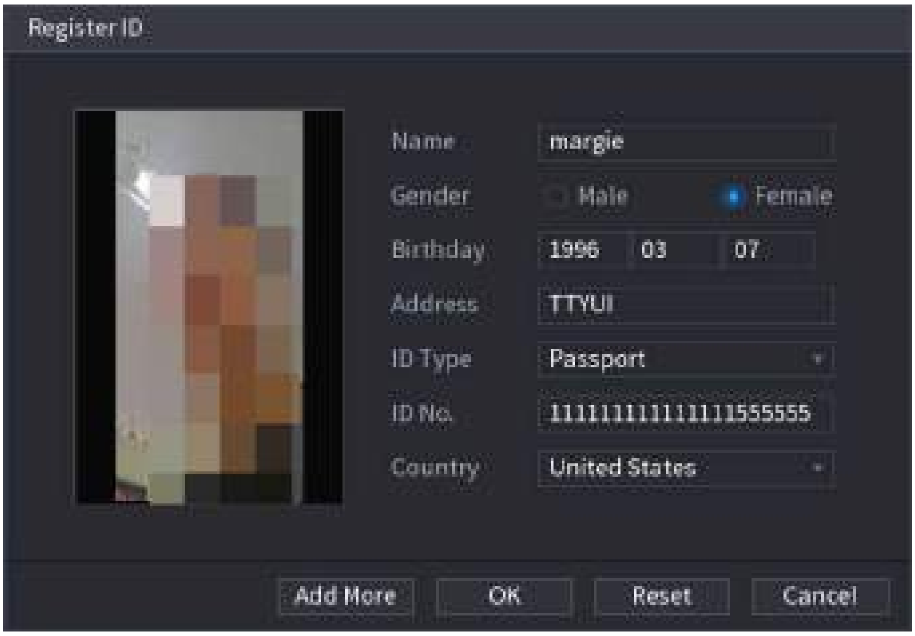
Free Space: 14.92 GB

Address: /

Name	Size	Type	Delete
DVR		Folder	🗑

Step 5 Select a face picture and enter the registration information.

Figure 5-220 Register ID



Register ID

Name: margie

Gender: ○ Male ● Female

Birthday: 1996 03 07

Address: TTYUI

ID Type: Passport

ID No.: 11111111111111555555

Country: United States

Step 6 Click **OK**.

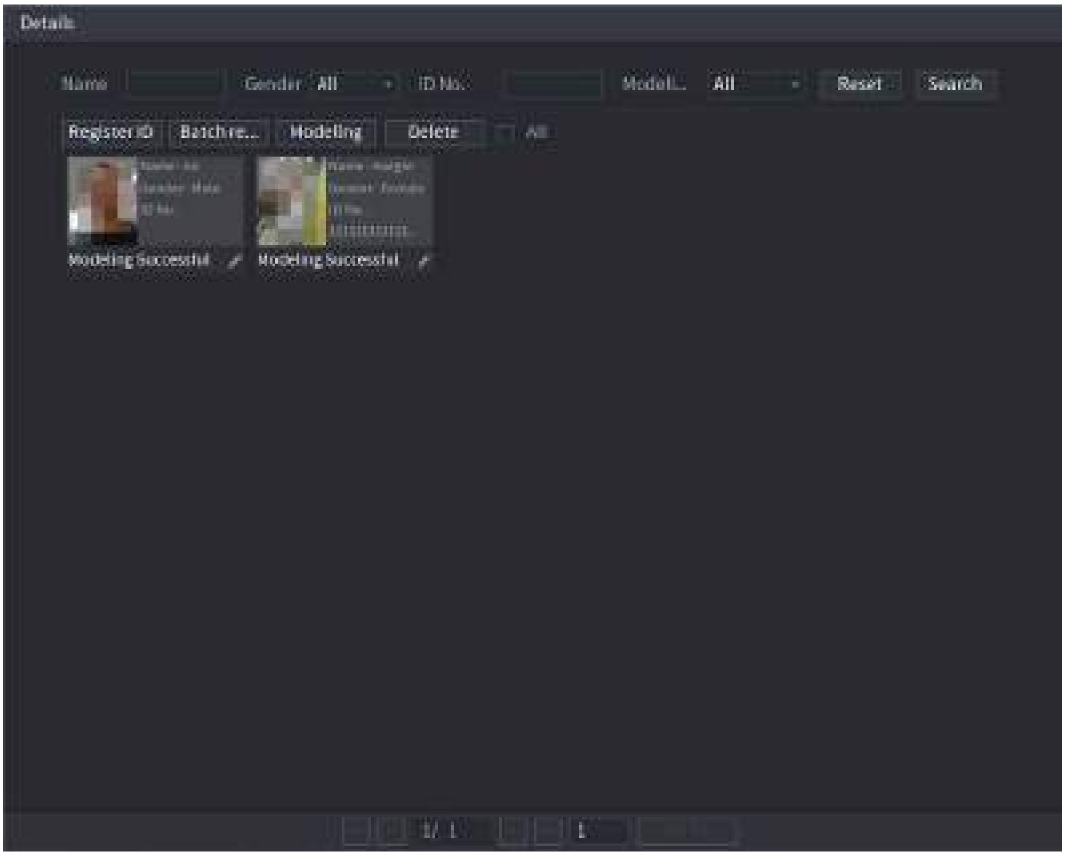
The system prompts the registration is successful.

Step 7 On the **Details** page, click **Search**.

The system prompts modeling is successful.

If the system prompts the message indicating modeling is in process, wait a while and then click **Search** again. If modeling is failed, the registered face picture cannot be used for face recognition.

Figure 5-221 Details



Adding Face Pictures in Batches

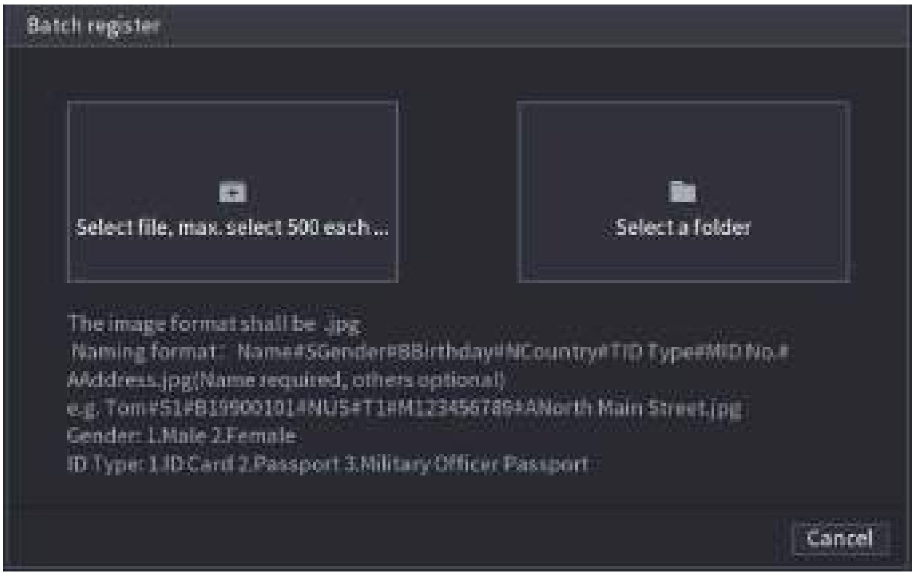
Step 1 Give a name to the face picture.

Figure 5-222 Register ID

Naming format	Description
Name	Enter the name.
Gender	Enter 1 or 2. 1 represents male, and 2 represents female.
Birthday	Enter numbers in the format of yyyy-mm-dd.
Country	Enter the abbreviation of country. For example, CN for China.
ID Type	1 represents ID card; 2 represents passport; 3 represents officer password.
ID No.	Enter the ID number.
Address	Enter the address.

Step 2 On the **Details** page, click **Batch register**.

Figure 5-223 Batch register



Batch register

Select file, max. select 500 each...

Select a folder

The image format shall be .jpg
Naming format: Name#SGender#BBirthday#NCountry#TID Type#MID No.#AAddress.jpg(Name required, others optional)
e.g. Tom#S1#B19900101#NUS#T1#M123456789#ANorth Main Street.jpg
Gender: 1.Male 2.Female
ID Type: 1.ID Card 2.Passport 3.Military Officer Passport

Cancel

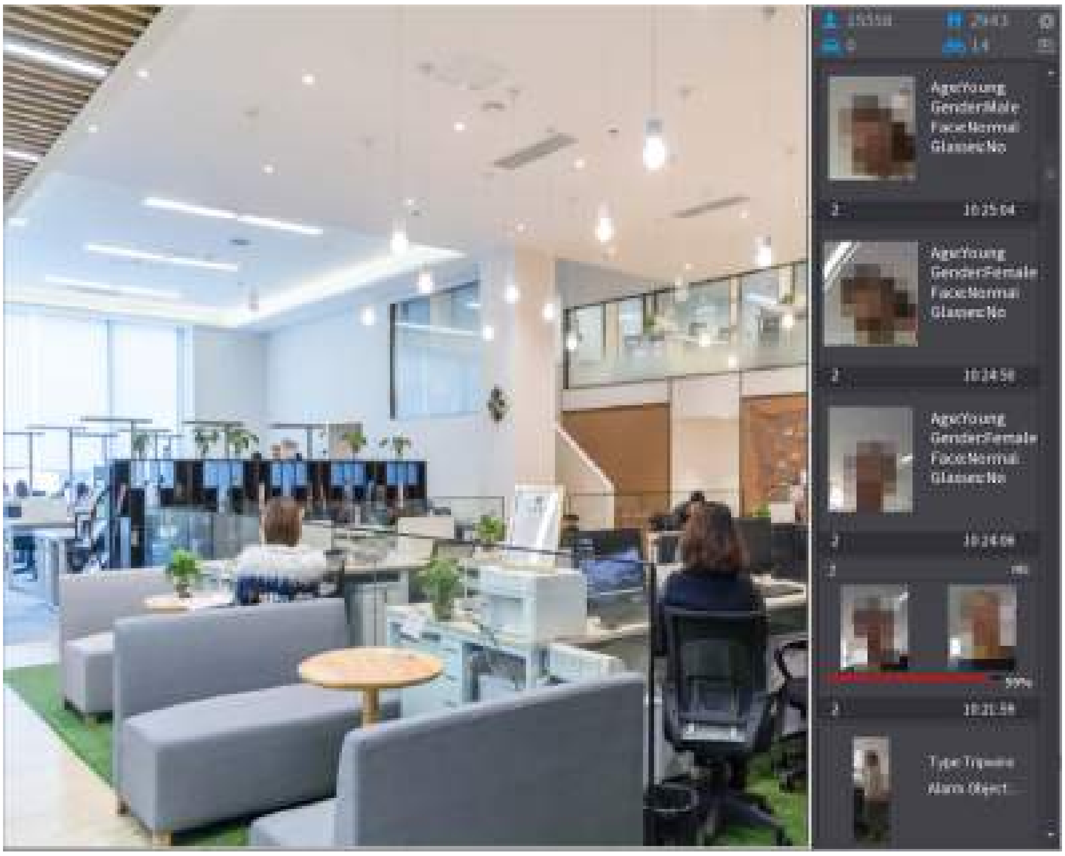
Step 3 Click **Select file, max select 500 each time** or **Select a folder** to import face pictures.

Step 4 Click **OK** to complete batch registration.

Adding the Detected Faces

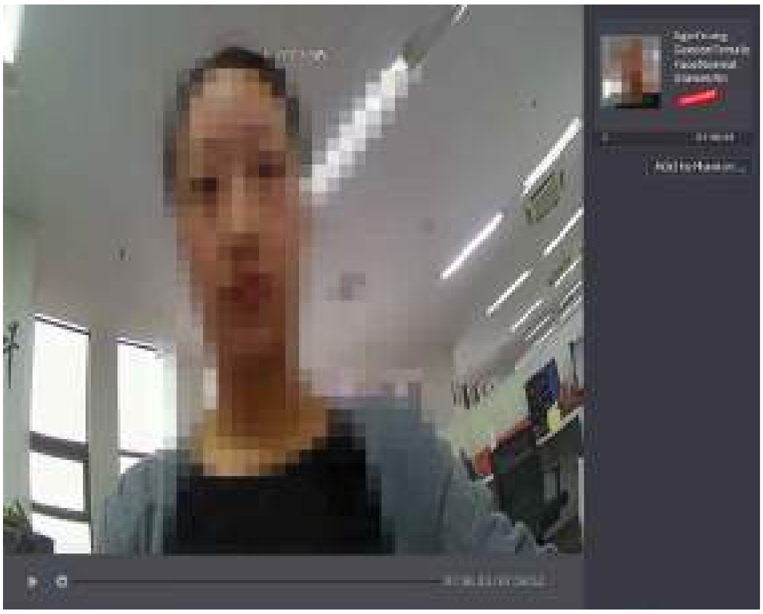
Step 1 Right-click on the live view screen, and then select **Live Mode** > **AI Mode**.

Figure 5-224 AI mode live view



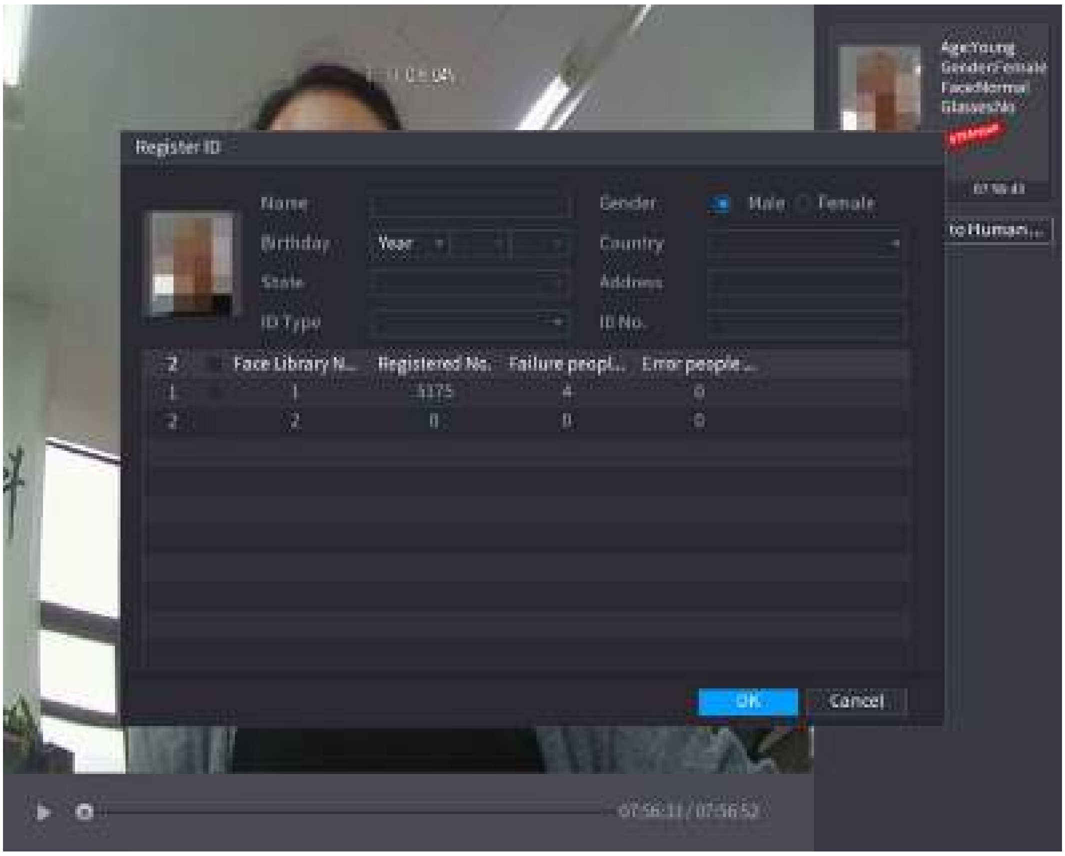
Step 2 Double-click the detected face snapshot that you want to add.

Figure 5-225 Playback



Step 3 Click **Add to Human Face Database**.

Figure 5-226 Register ID



Register ID

Name

Gender ● Male ○ Female

Birthday Year

Country

State

Address

ID Type

ID No.

2		Face Library N...	Registered No.	Failure peopl...	Error people ...
1		1	3175	4	0
2		2	0	0	0

Step 4 Select the face database and enter the ID information.

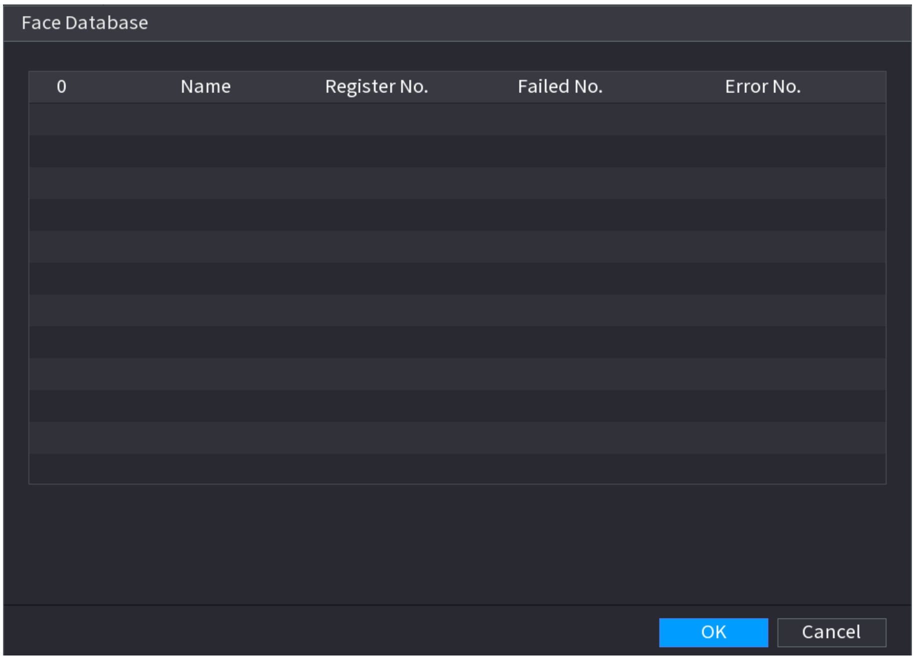
Step 5 Click **OK** to complete registration.

5.11.3.4.2 Face Recognition Configuration

You can compare the detected faces with the faces in the database to judge if the detected face belongs to the database. The comparison result will be displayed on the AI mode live view screen and smart search page, and link the alarms.

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

Figure 5-227 Face recognition



Face Database

0	Name	Register No.	Failed No.	Error No.

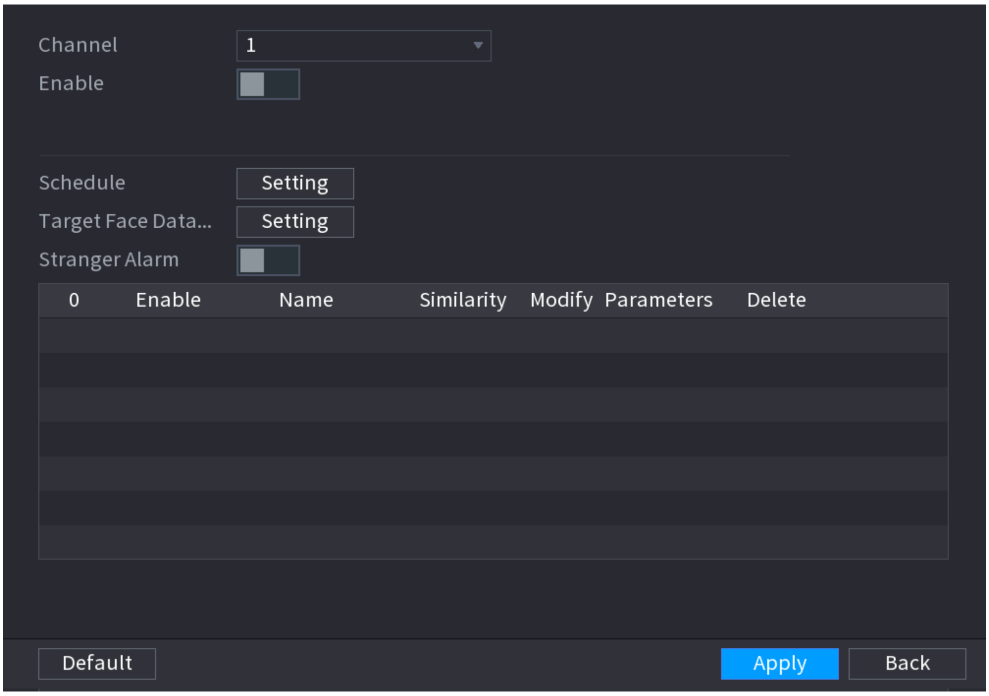
Step 2 In the **Channel** list, select a channel that you want to configure face recognition function, and then enable it.

Step 3 Set the **Period**. For details, see "5.10.4.1 Configuring Motion Detection Settings."

Step 4 Set the **Target Face Database**.

1) Click **Setting**.

Figure 5-228 Face database



Channel: 1
Enable
Schedule: Setting
Target Face Data...: Setting
Stranger Alarm

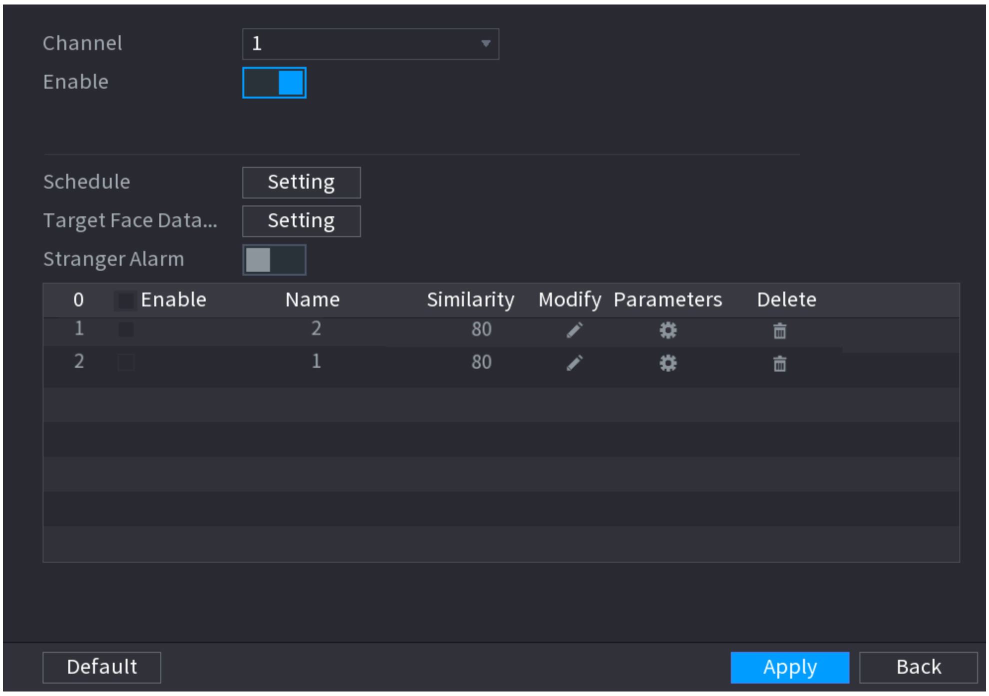
0	Enable	Name	Similarity	Modify	Parameters	Delete

2) Select one or multiple face databases.

3) Click **OK**.

The selected face database is listed.

Figure 5-229 Database list



Channel: 1

Enable: ■

Schedule: Setting

Target Face Data...: Setting

Stranger Alarm: □

0	Enable	Name	Similarity	Modify	Parameters	Delete
1	□	2	80	✎	⚙	🗑
2	□	1	80	✎	⚙	🗑

Step 5 Configure the added face database.

- Click ✎ to modify the similarity. The lower the number is, the easier the alarm linkage will trigger.
- Click 🗑 to delete the face database.
- Click ⚙ to set the alarm linkage.

  After setting is completed, click **OK**.

Step 6 (Optional) Enable the **Stranger Mode**.

1) Enable the Stranger mode (■). When the detected faces do not belong to the face database, the system remarks the face as "Stranger."

2) Click **Setting** to set the alarm linkage.

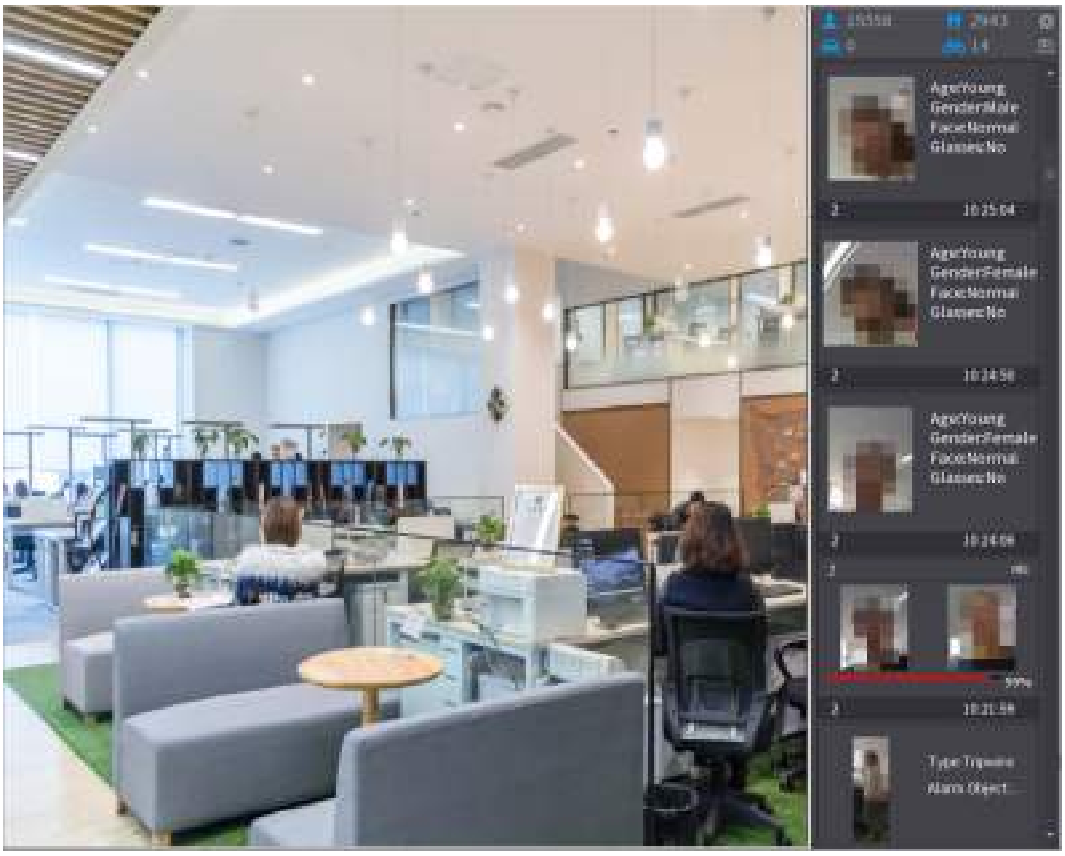
3) After setting is completed, click **OK**.

Step 7 Click **Apply** to complete the settings.

After the face recognition function is enabled, right-click on the live view screen, and then select **Preview Mode > AI Mode**. The AI mode live view screen is displayed.

- If the detected face belongs to the enabled face database, the similarity result is displayed.
- If the detected face does not belong to the enabled face database, the face will be remarked as "Stranger."

Figure 5-230 Similarity result



Age:Young
Gender:Male
Face:Normal
Glasses:No

10:25:04

Age:Young
Gender:Female
Face:Normal
Glasses:No

10:24:58

Age:Young
Gender:Female
Face:Normal
Glasses:No

10:24:08

99%

10:21:59

Type:Tripwire
Alarm Object:...

5.11.3.4.3 Smart Search for Face Recognition

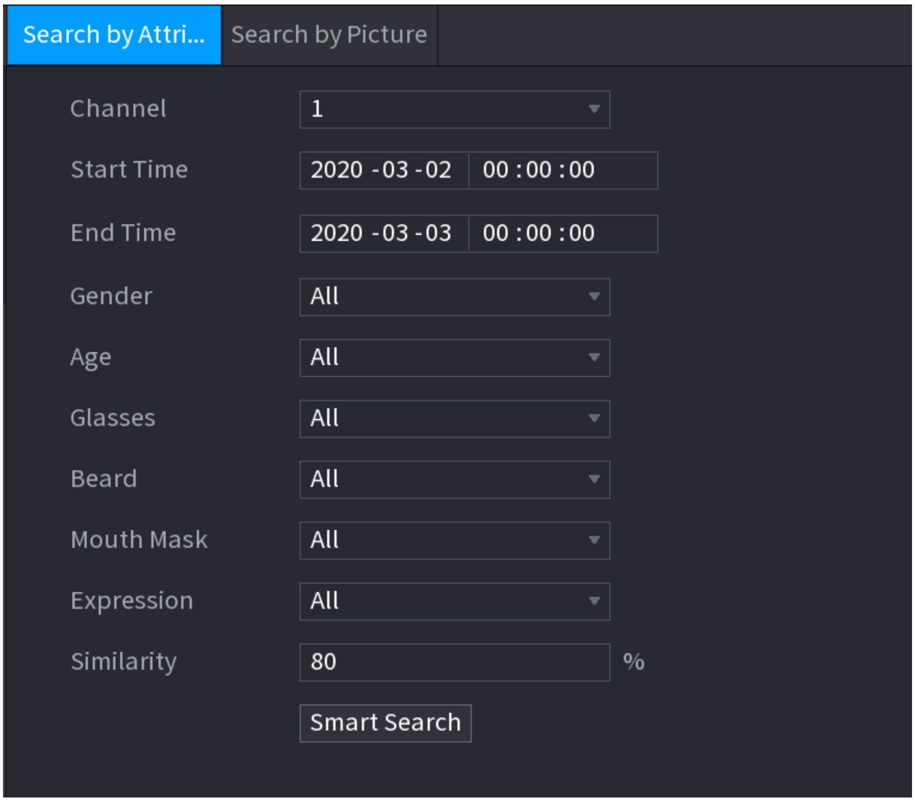
You can compare the detected faces with the face database and play back.

- Search by attributes: Search the face database by the face attributes.
- Search by picture: Search the face database by uploading face pictures.

Searching by Attributes

Step 1 Select **Main Menu > AI > AI Search > Face Recognition > Search by Attributes**.

Figure 5-231 Search by attributes



Search by Attri... | Search by Picture

Channel: 1

Start Time: 2020 -03 -02 00 :00 :00

End Time: 2020 -03 -03 00 :00 :00

Gender: All

Age: All

Glasses: All

Beard: All

Mouth Mask: All

Expression: All

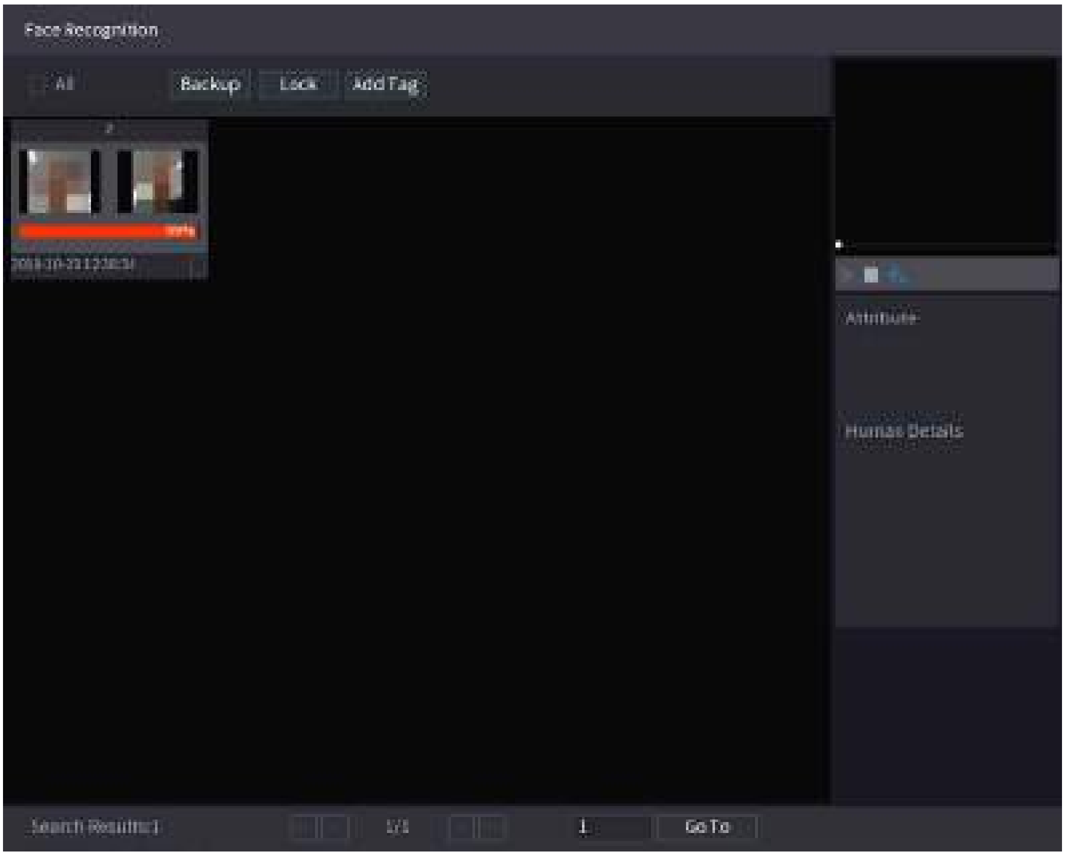
Similarity: 80 %

Smart Search

Step 2 Select the channel and set the parameters such as start time, end time, gender, age, glasses, beard, mask, and similarity according to your requirement.

Step 3 Click **Smart Search**.

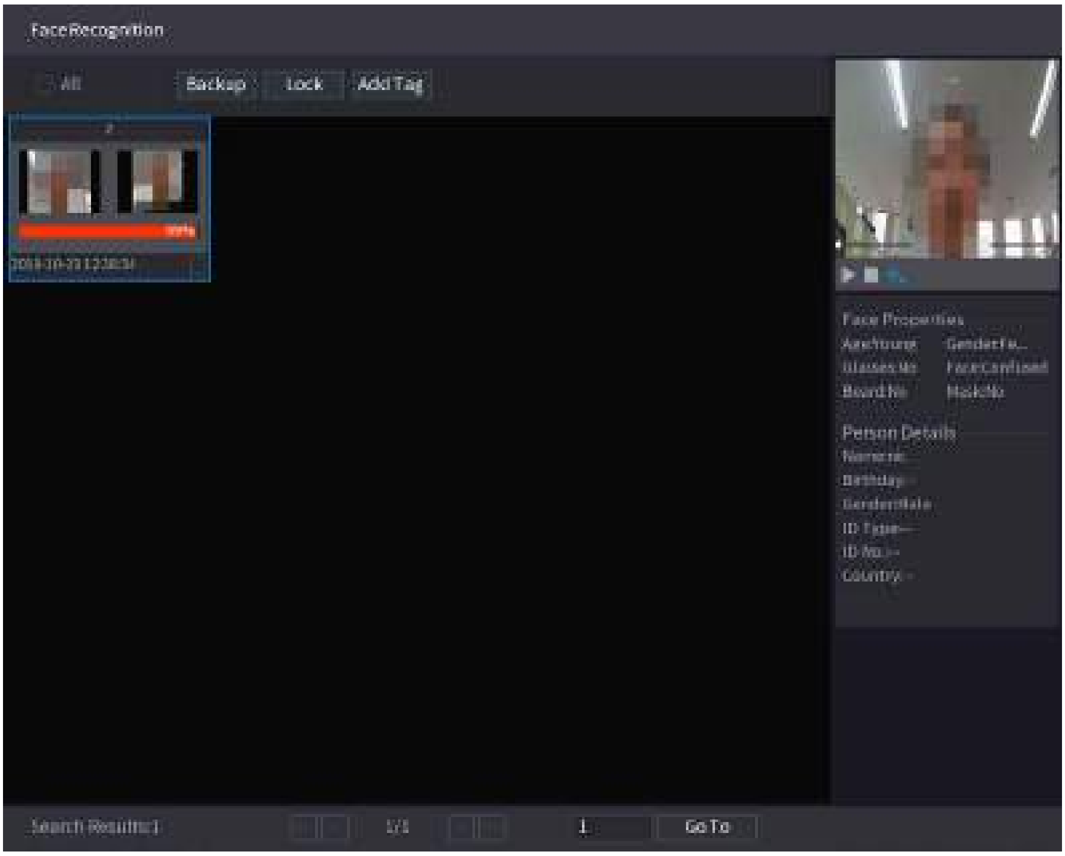
Figure 5-232 Search results



Step 4 Click the picture that you want to play back.

The picture with registered information is displayed.

Figure 5-233 Registered information



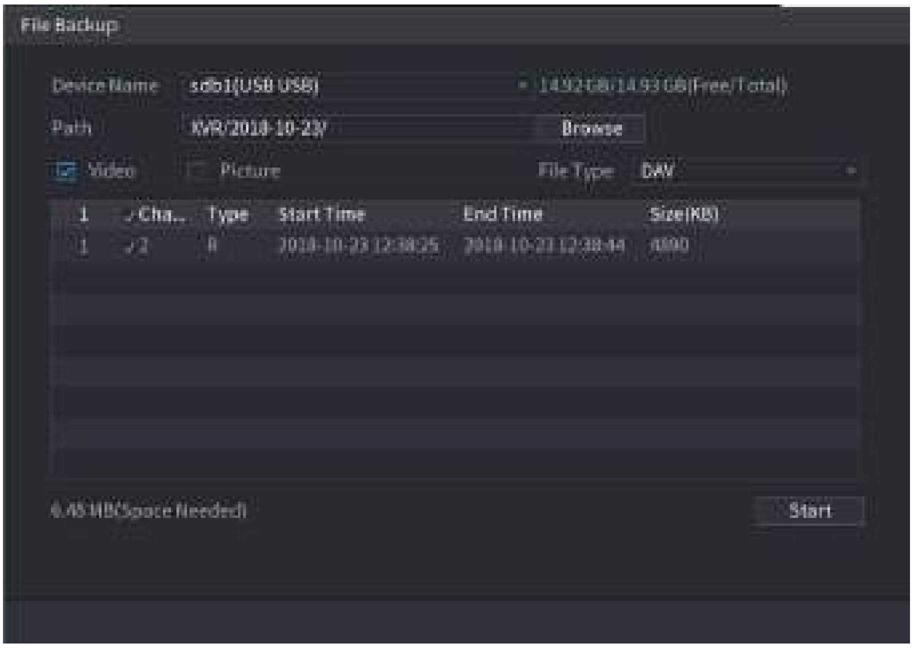
Step 5 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To export the database file (.csv) to the external storage device, select files, click **Export**, and then select the save path.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-234 Backup



File Backup

Device Name: sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path: KVR/2018-10-23/

☑ Video ☐ Picture File Type: DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	6890

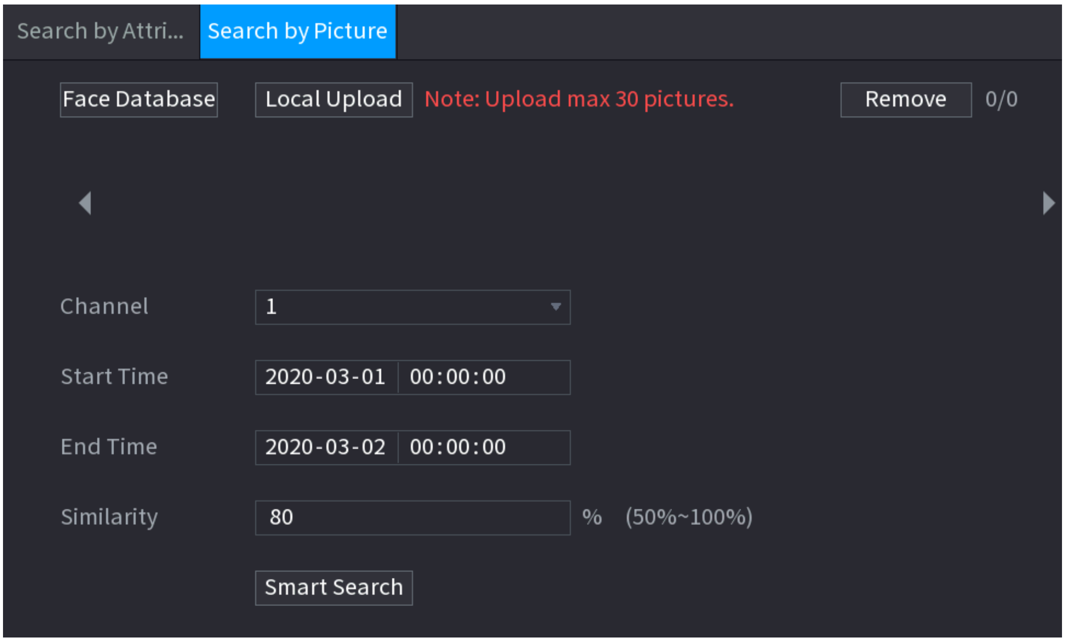
6.48 MB(Space Needed)

- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a mark to the file, select the files and then click **Add Mark**.

Search by Picture

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Face Recognition** > **Search by Picture**.

Figure 5-235 Search by picture



Note: Upload max 30 pictures.

0/0

Channel: 1

Start Time: 2020-03-01 00:00:00

End Time: 2020-03-02 00:00:00

Similarity: 80 % (50%~100%)

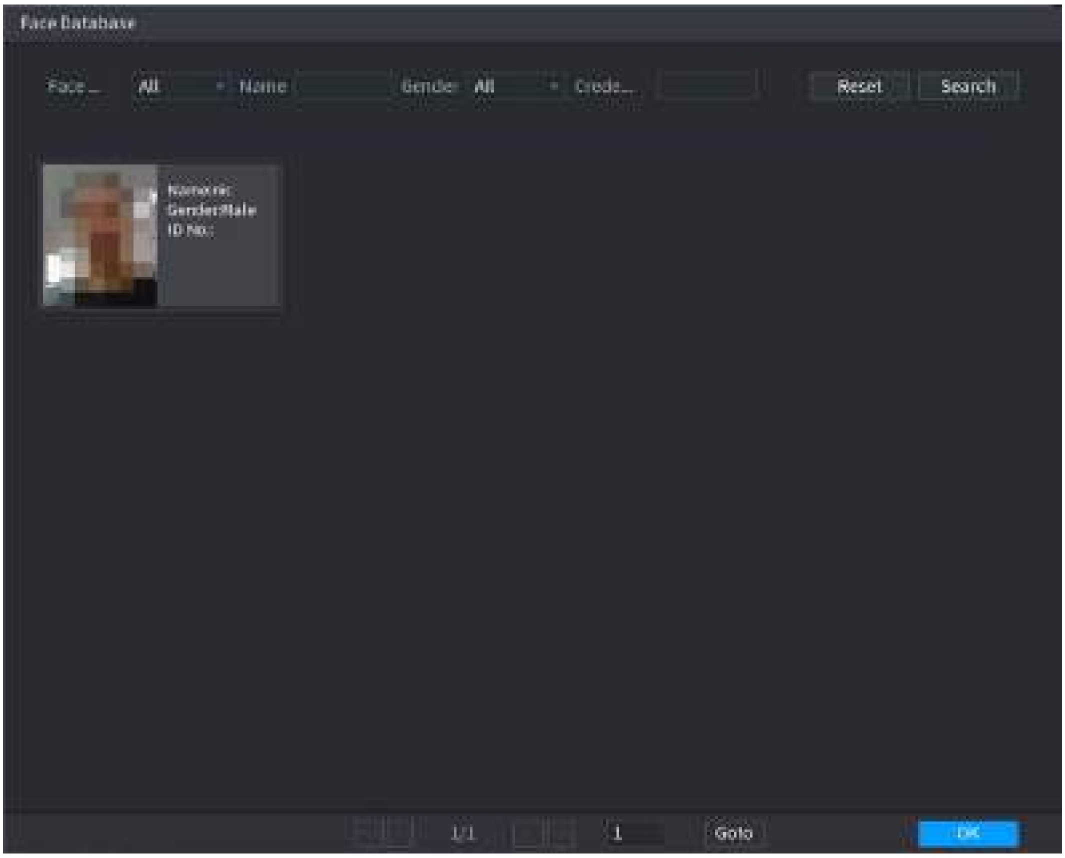
Step 2 Upload face pictures from **Face Database** or **Local Upload**.

Maximum 30 pictures can be uploaded at one time, and the system support searching 8 pictures at one time.

- Face Database

1) Click **Face Database**.

Figure 5-236 Face database



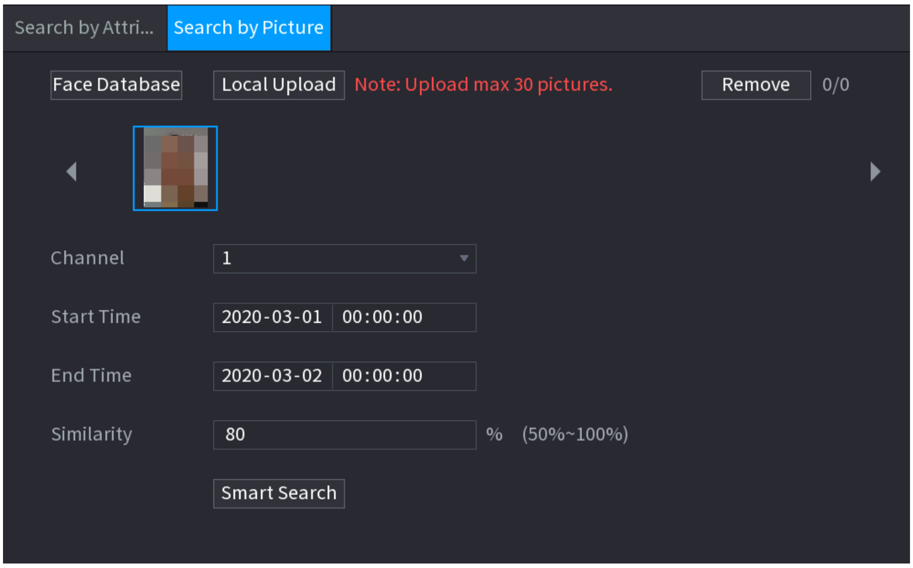
2) Set the searching parameters by selecting the face database and gender, and entering name and ID No. according to your actual requirement.

3) Click **Search** to display the results that satisfy the requirement.

Click **Reset** to clear the searching parameters.

4) Select the picture and then click Save.

Figure 5-237 Search by picture



Note: Upload max 30 pictures.

Channel 1

Start Time 2020-03-01 00:00:00

End Time 2020-03-02 00:00:00

Similarity 80 % (50%~100%)

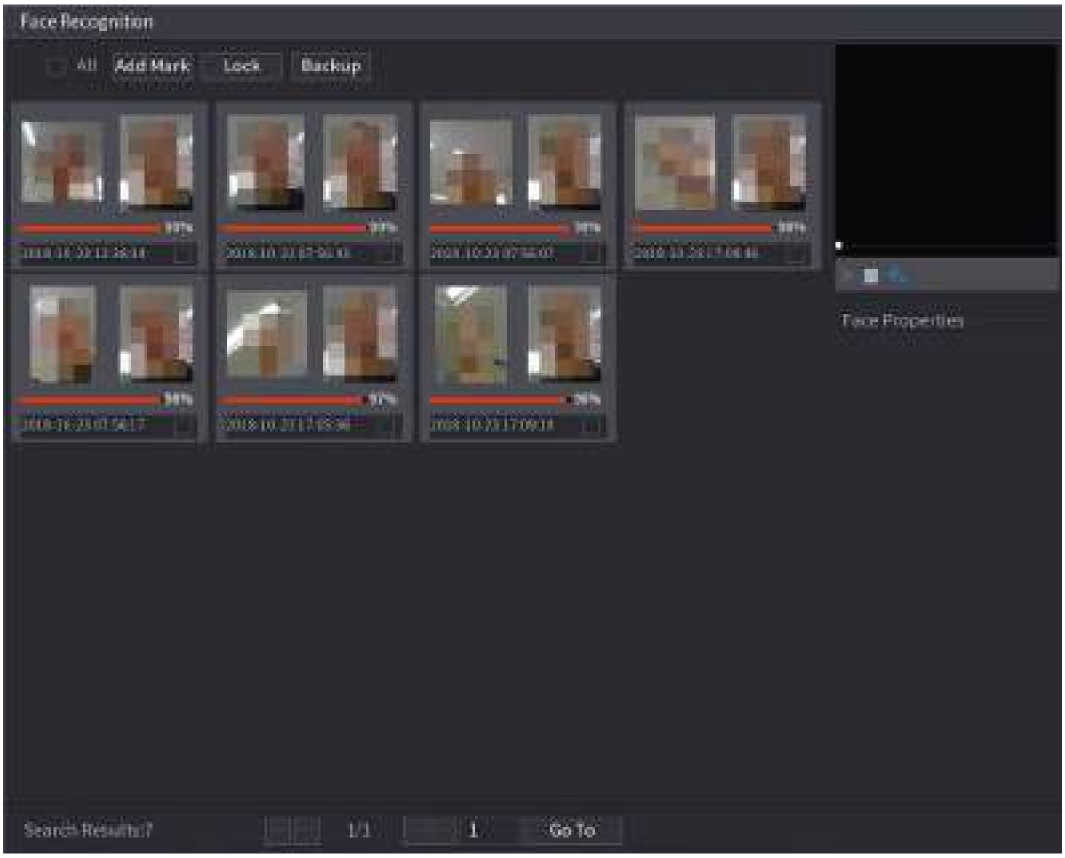
- Local Upload

Plug the USB storage device (with face pictures) to the Device, and then click **Local Upload**. Then select the picture from the USB storage device, and then click **OK**. The selected face pictures are uploaded.

Step 3 After the face pictures are uploaded, continue to configure other parameters (channel, start time, end time, and similarity).

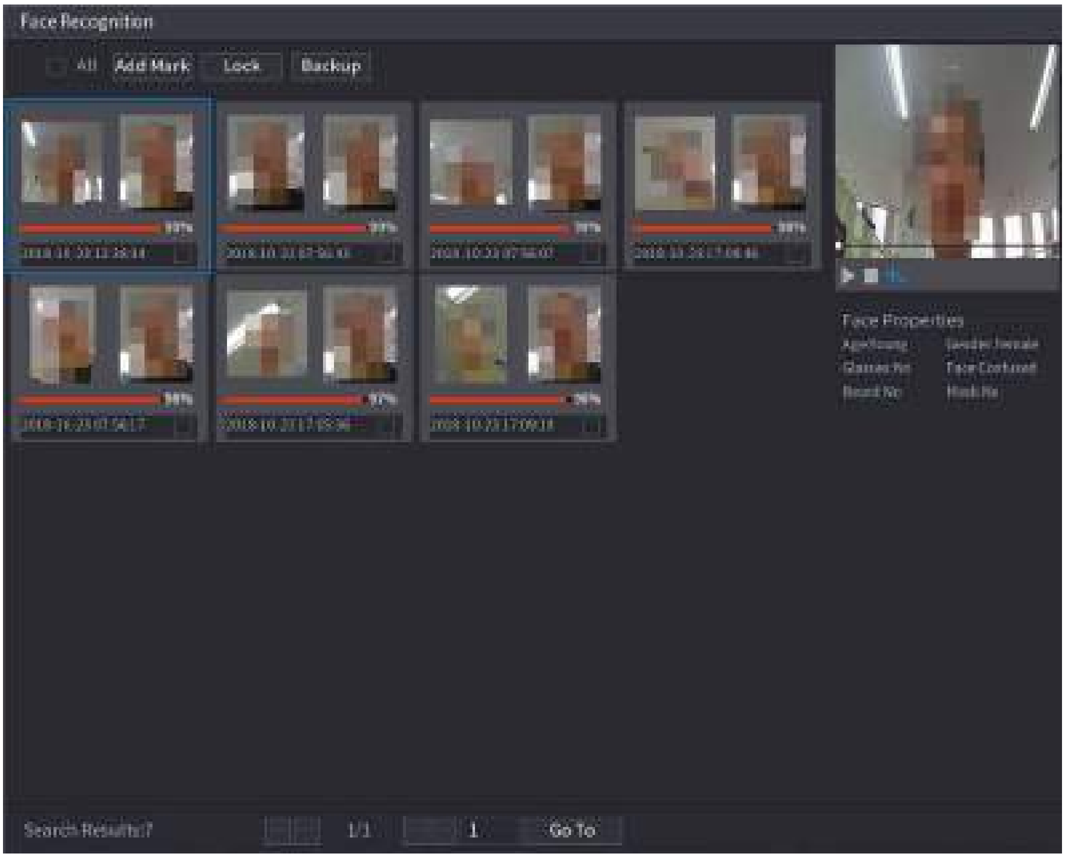
Step 4 Click **Smart Search**.

Figure 5-238 Search results



Step 5 Select the face picture that you want to play back.

Figure 5-239 Playback



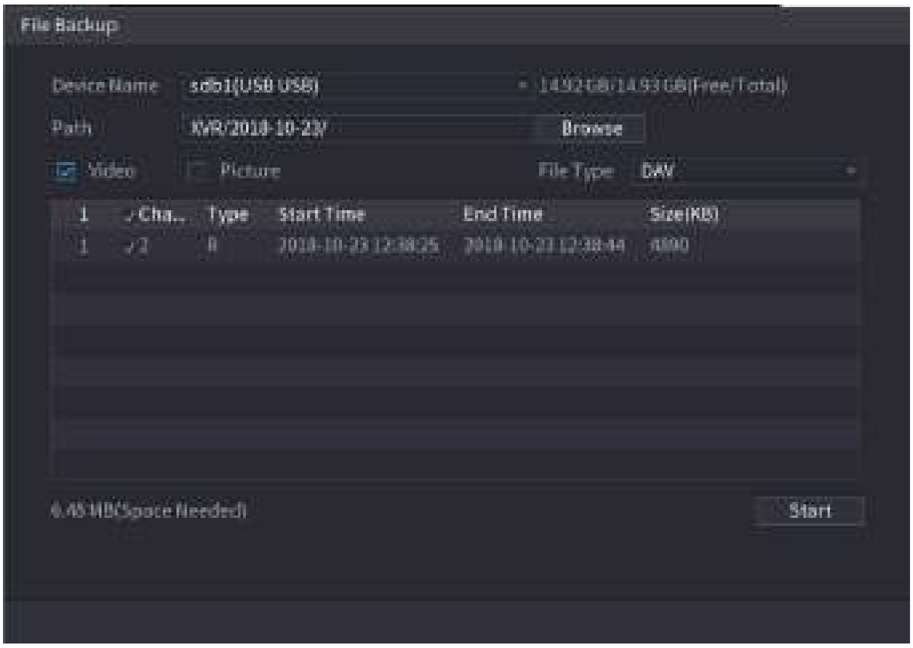
Step 6 Click ▶ to play back the recorded video.

Double-click on the playing page to switch between full screen playing and thumbnail playing.

You can also do the following operations to the recorded files.

- To add a mark to the file, select the files and then click **Add Mark**.
- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

Figure 5-240 Backup



File Backup

Device Name: sdb1(USB USB) 14.92 GB/14.93 GB(Free/Total)

Path: XVR/2018-10-23/ Browse

☑ Video □ Picture File Type: DAV

1	✓Cha...	Type	Start Time	End Time	Size(KB)
1	✓2	R	2018-10-23 12:38:25	2018-10-23 12:38:44	4890

6.48 MB(Space Needed)

Start

5.12 IoT Function

5.12.1 Configuring Sensor Settings

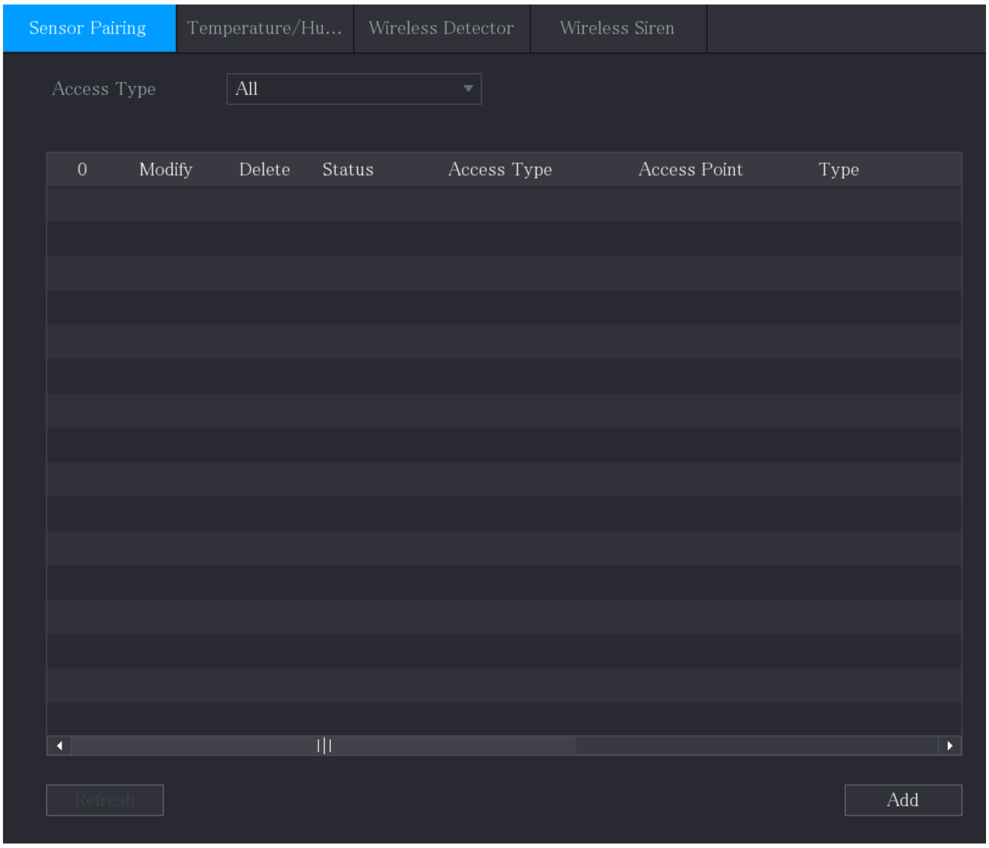
You can connect external sensors wirelessly through the Device with USB gateway or through connecting to a camera gateway. After connection, you can activate alarm events through external sensors.

5.12.1.1 Connecting Sensor through Device

Only the Device with USB gateway supports this function.

Step 1 Select **Main Menu** > **IoT** > **Management** > **Sensor Pairing**.

Figure 5-241 Sensor pairing

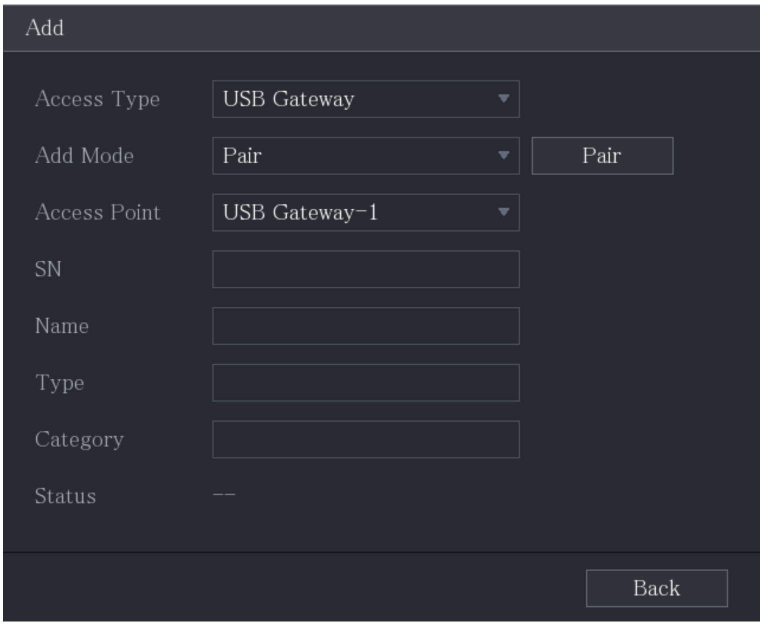


Access Type: All

Step 2 In the **Access Type** list, select **USB Gateway**.

Step 3 Click **Add**.

Figure 5-242 Add USB gateway



Access Type: USB Gateway

Add Mode: Pair

Access Point: USB Gateway-1

SN

Name

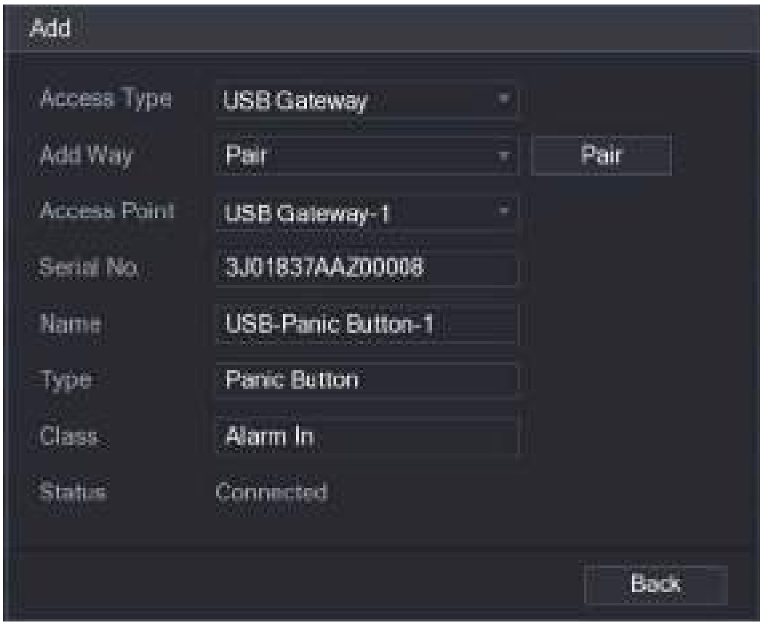
Type

Category

Status: --

Step 4 Click **Pair**.

Figure 5-243 Pair



Add

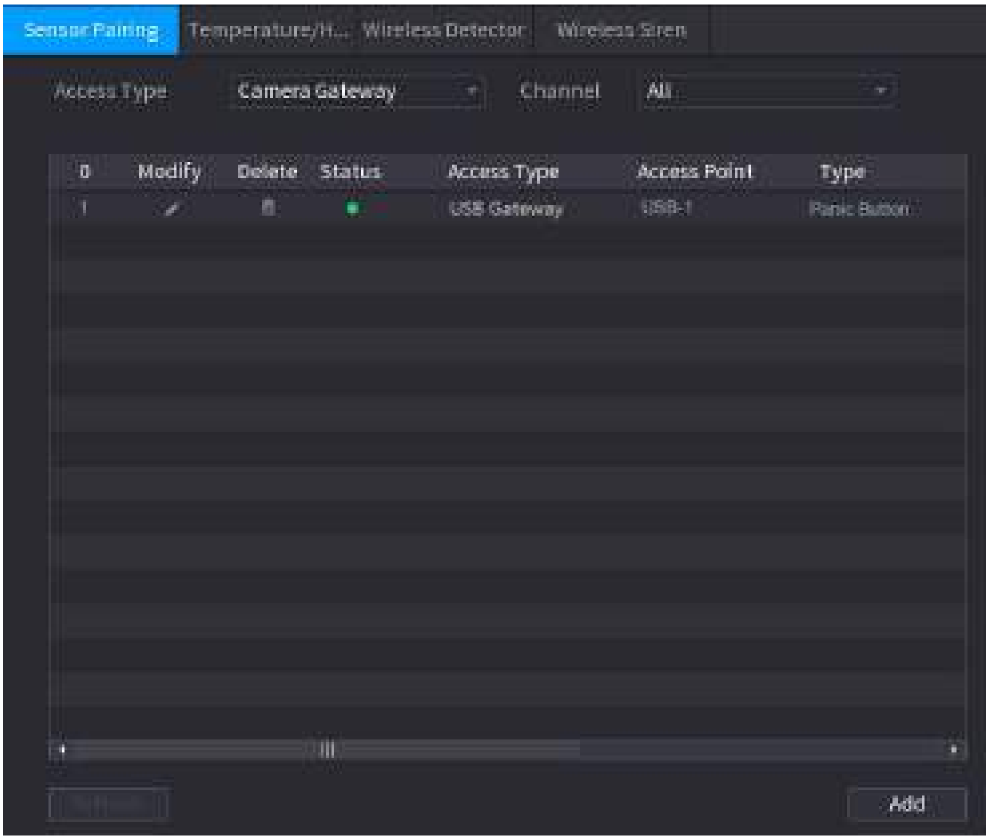
Access Type	USB Gateway
Add Way	Pair
Access Point	USB Gateway-1
Serial No.	3J01837AAZ00008
Name	USB-Panic Button-1
Type	Panic Button
Class	Alarm In
Status	Connected

Step 5 Click **Back** to exit the pairing page.

The added sensor information is displayed.

Click ✎ to modify the sensor name; click 🗑 to delete sensor information.

Figure 5-244 Sensor pairing



Access Type: Camera Gateway

Channel: All

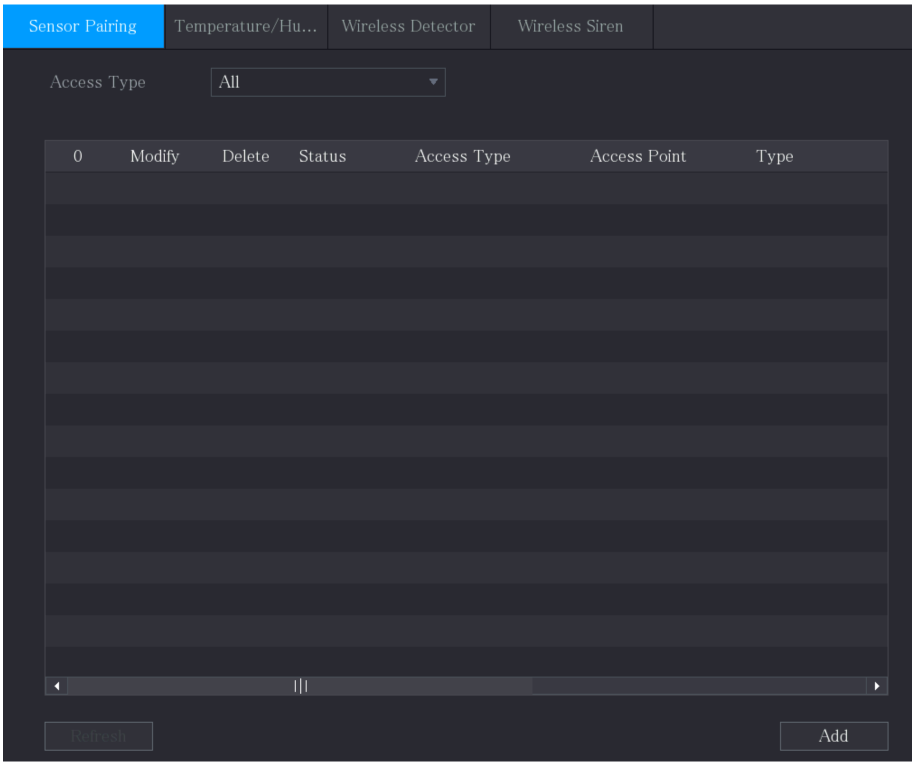
0	Modify	Delete	Status	Access Type	Access Point	Type
1	✎	🗑	●	USB Gateway	USB-1	Panic Button

5.12.1.2 Connecting Sensor through Camera with Gateway

Only the camera with gateway supports this function.

Step 1 Select **Main Menu** > **IoT** > **Management** > **Sensor Pairing**.

Figure 5-245 Sensor pairing



Access Type: All

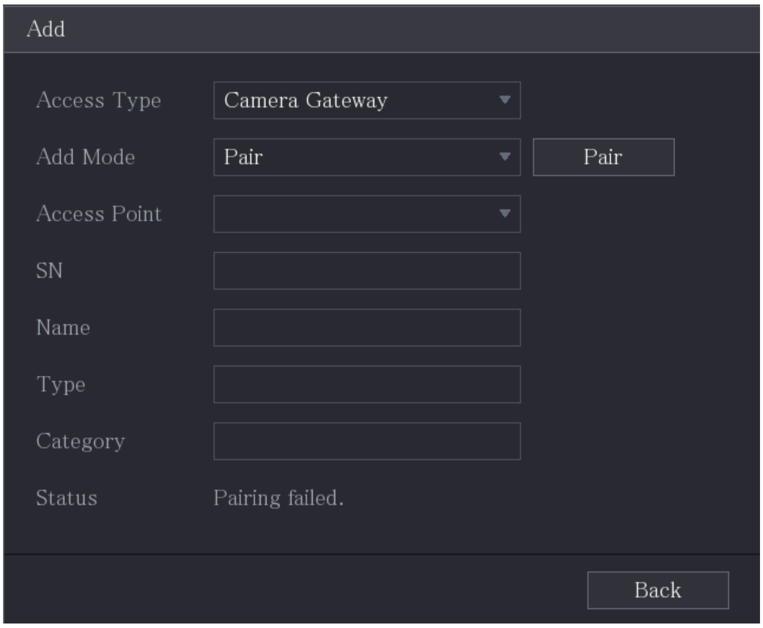
0	Modify	Delete	Status	Access Type	Access Point	Type

Step 2 In the **Access Type** list, select **Camera Gateway**.

Step 3 In the **Channel** list, select the channel that is connected to the camera.

Step 4 Click **Add**.

Figure 5-246 Add camera gateway



Access Type: Camera Gateway

Add Mode: Pair

Access Point:

SN:

Name:

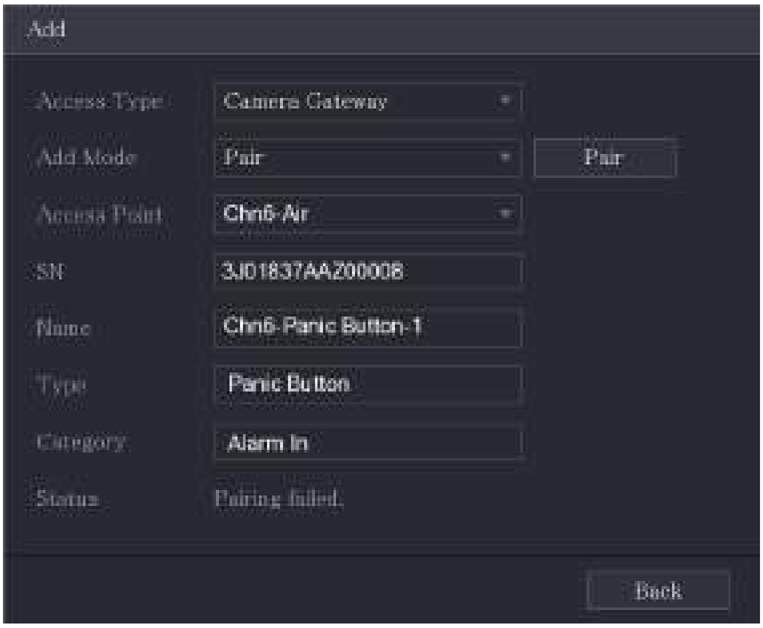
Type:

Category:

Status: Pairing failed.

Step 5 Click **Pair**.

Figure 5-247 Pair



Add

Access Type: Camera Gateway

Add Mode: Pair

Access Point: Chn6-Air

SN: 3JD1837AAZ00008

Name: Chn6-Panic Button-1

Type: Panic Button

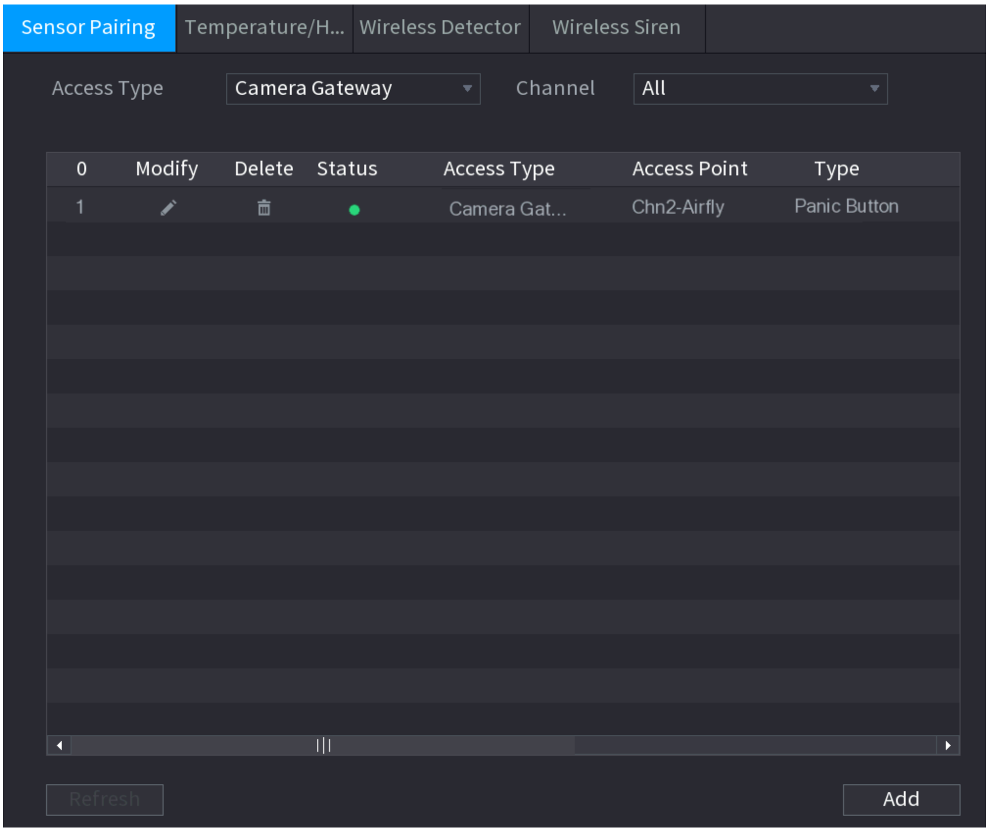
Category: Alarm In

Status: Pairing failed.

Step 6 Click **Back** to exit the pairing page.

Click ✎ to modify the sensor name; click 🗑 to delete sensor information.

Figure 5-248 Sensor pairing



Access Type: Camera Gateway

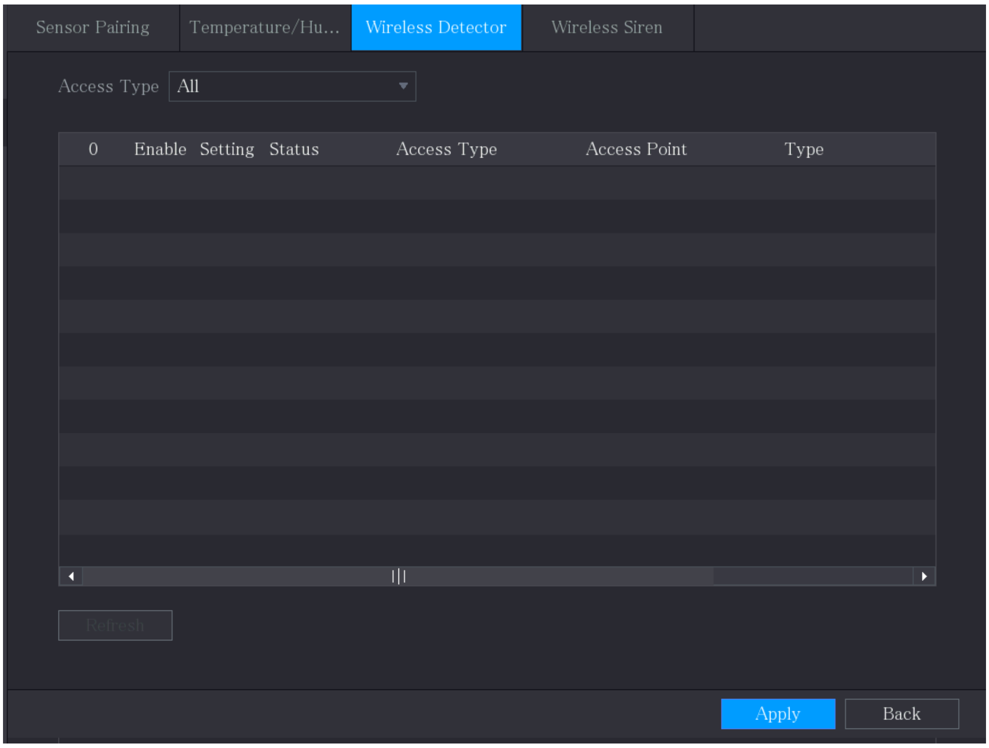
Channel: All

0	Modify	Delete	Status	Access Type	Access Point	Type
1	✎	🗑	●	Camera Gat...	Chn2-Airfly	Panic Button

5.12.1.3 Configuring Alarm Linkage

Step 1 Select **Main Menu** > **IoT** > **Management** > **Wireless Detector**.

Figure 5-249 Wireless detector



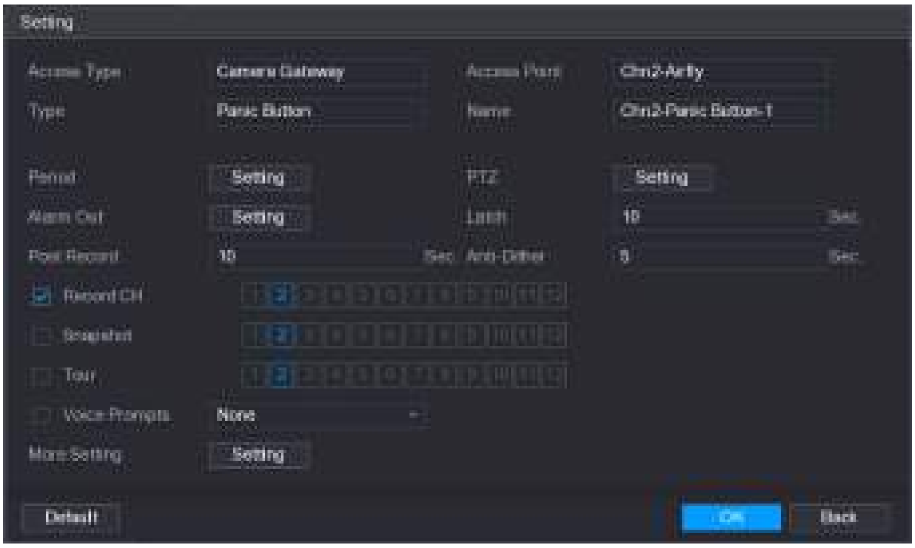
Access Type: All

Step 2 In the **Access Type** list, select **USB Gateway**, **Camera Gateway,** or **All**.

When **Access Type** is **Camera Gateway**, you can select **Channel** to filter the status of present wireless detector.

Step 3 Click ⚙.

Figure 5-250 Setting



Access Type: Camera Gateway
Access Point: Chn2-Arfly
Type: Panic Button
Name: Chn2-Panic Button-1
Latch: 10 Sec.
Post Record: 10 Sec.
Anti-Dither: 5 Sec.
☑ Record CH
□ Snapshot
□ Tour
□ Voice Prompts: None

Step 4 Configure the settings for alarm linkage.

Table 5-41 Alarm linkage settings

Parameter	Description
Name	Enter the customized alarm name.

Parameter	Description
Schedule	Click **Setting** to display setting page. Define a period during which the motion detection is active. For details, see "Setting Motion Detection Period" section in "5.10.4.1 Configuring Motion Detection Settings."
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Alarm-out Port	Click **Setting** to display setting page. ● Local Alarm: Enable alarm activation through the alarm devices connected to the selected output port. ● Extension Alarm: Enable alarm activation through the connected alarm box. ● Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm event occurs. 📖 The recording for alarm and auto recording must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Snapshot	Select the **Snapshot** checkbox to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > CAMERA > Encode > Snapshot**, in the **Type** list, select **Event**.
Tour	Select the **Tour** checkbox to enable a tour of the selected channels.
Alarm Tone	Select to enable audio broadcast/voice prompts in response to a local alarm event.

Parameter	Description
More Setting	● Show Message: Select the **Show Message** checkbox to enable a pop-up message in your local host PC. ● Buzzer: Select the checkbox to activate a buzzer noise at the Device. ● Video Matrix: Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "**Main Menu > DISPLAY > Tour**." Not all models support this function. ● Send Email: Enable the system to send an email notification when an alarm event occurs. To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**. ● Log: Select the checkbox to enable the Device to record a local alarm log. ● Extra screen: Select the checkbox to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in **Main Menu > DISPLAY > Tour > Sub Screen.** ● Not all models support this function. ● To use this function, extra screen shall be enabled.

Step 5 Click **OK** to save the settings.

Step 6 On the **Wireless Detector** page, click **Apply** to complete the settings.

5.12.2 Configuring Temperature and Humidity Camera

You can view, search and export the temperature and humidity data of camera with such sensors and configure the alarm event settings.

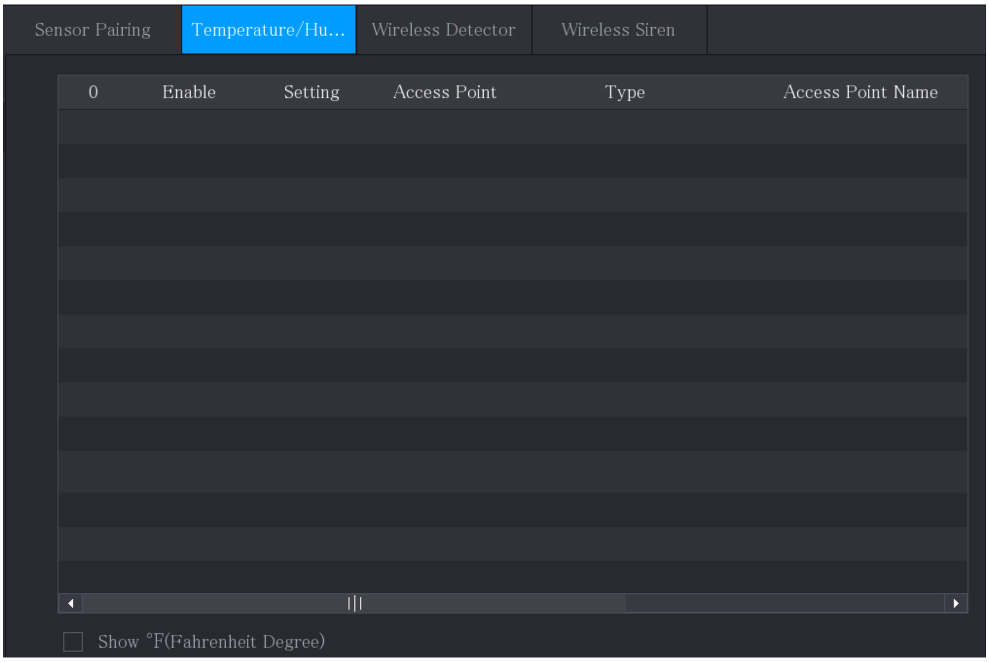
To use this function, make sure there is at least one camera with temperature and humidity sensor has been connected to the Device.

5.12.2.1 Enabling Detecting Function

You should enable the IoT function the first time when you enter this page.

Step 1 On the main menu, select **IoT > Management > Temperature/Humidity**.

Figure 5-251 Temperature/Humidity

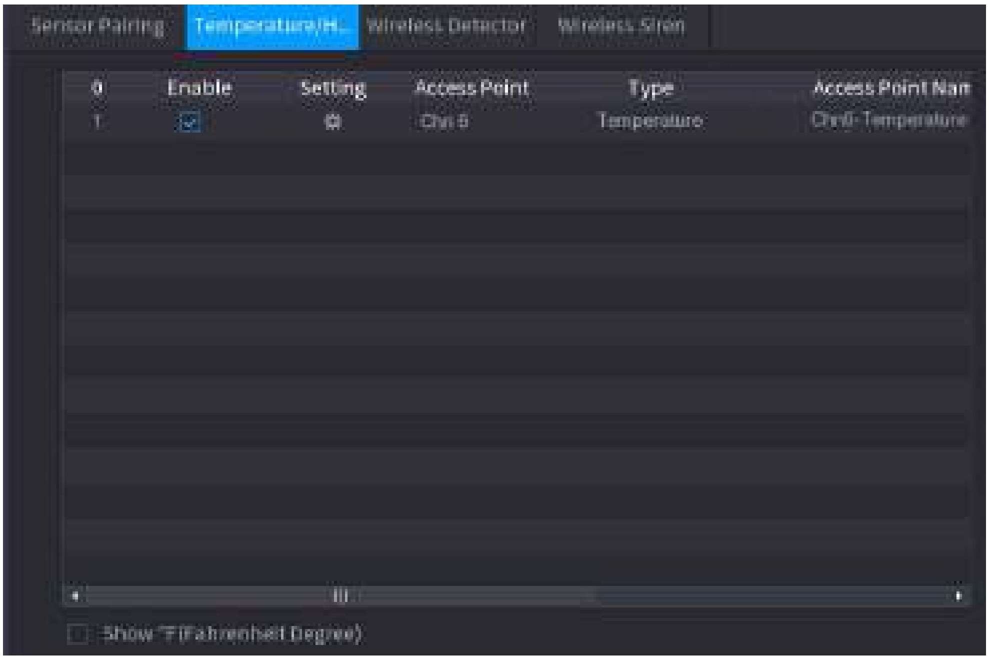


0	Enable	Setting	Access Point	Type	Access Point Name

□ Show °F(Fahrenheit Degree)

Step 2 Select the **Enable** checkboxes to enable IoT function.

Figure 5-252 Enable



0	Enable	Setting	Access Point	Type	Access Point Nam
1	☑	⚙	Chn 5	Temperature	Chn5-Temperature

□ Show °F(Fahrenheit Degree)

The Device starts detecting the temperature and humidity data from the camera and display on the **Realtime Display** page.

Step 3 (Optional) Set temperature displaying mode.

When **Show°F (Fahrenheit Degree)** is selected, the temperature will be displayed by Fahrenheit degree in **Realtime Display** tab.

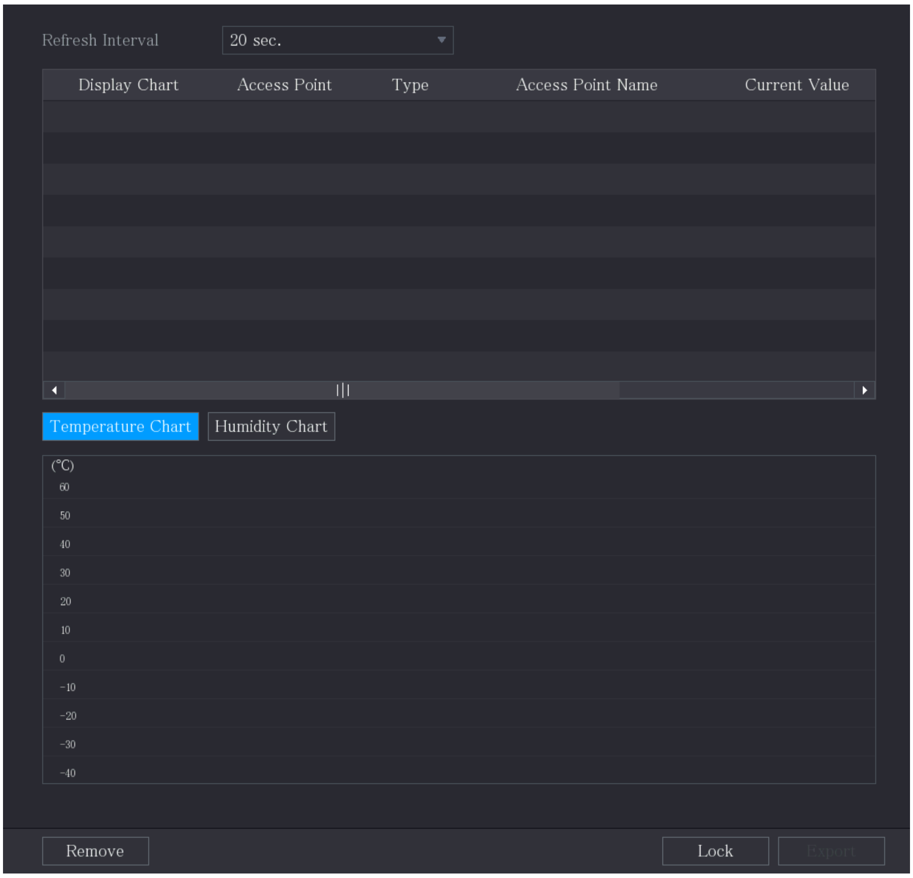
5.12.2.2 Viewing Temperature and Humidity Data

You can view the temperature and humidity data on the **Realtime Display** page after the IoT function is enabled.

In the **Refresh Interval** box, select data refresh interval. For example, you can select **5 Sec**.

You can also display the temperature and humidity data in graphical way by selecting the **Display Chart** checkbox.

Figure 5-253 Chart



Refresh Interval: 20 sec.

Display Chart	Access Point	Type	Access Point Name	Current Value

Click **Remove** to delete the data.

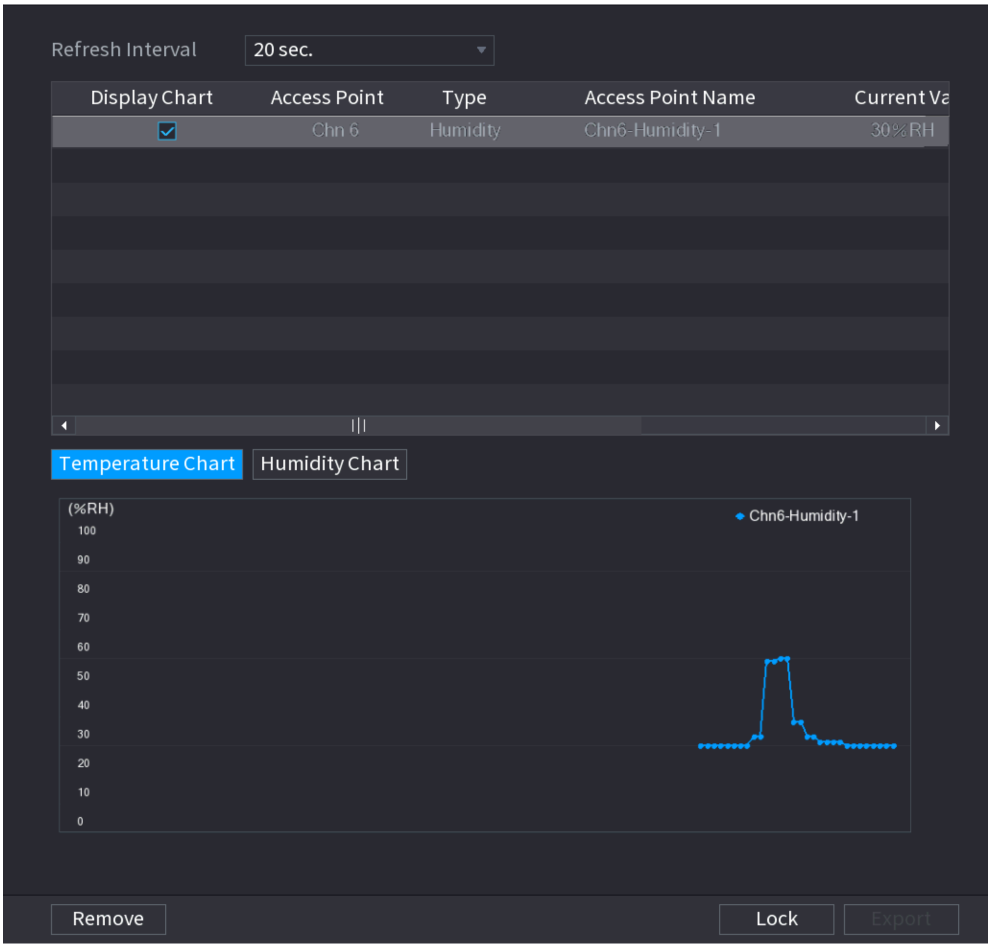
5.12.2.3 Exporting Temperature and Humidity Data

You can export the temperature and humidity data in .BMP format. This section uses exporting humidity data as an example.

Step 1 Prepare a USB device and plug it into the Device.

Step 2 On the **Realtime Display** page, click the **Humidity** tab.

Figure 5-254 Humidity



Refresh Interval: 20 sec.

Display Chart	Access Point	Type	Access Point Name	Current Va
☑	Chn 6	Humidity	Chn6-Humidity-1	30%RH

Step 3 Click **Lock** to lock the data.

The export button is enabled.

Step 4 Click **Export**. The system starts exporting the data.

Step 5 Click **OK**.

You can find the exported data on your USB device.

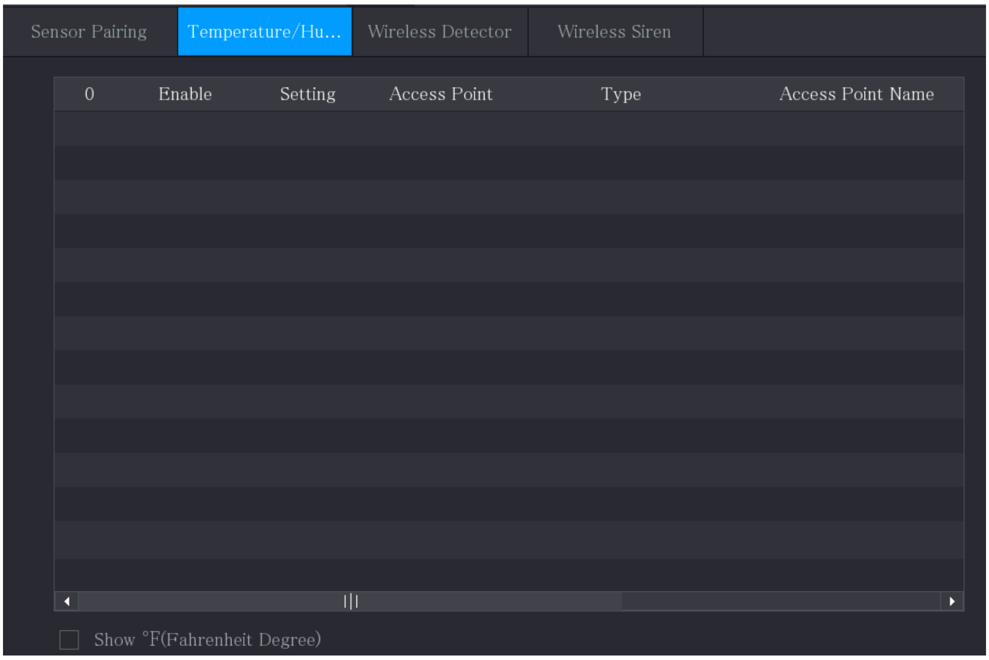
5.12.2.4 Configuring Alarm Linkage

You can configure alarm linkage settings for temperature and humidity data.

5.12.2.4.1 Configuring Alarm Linkage for Temperature Data

Step 1 On the home page, select **IoT** > **Management** > **Temperature/Humidity**.

Figure 5-255 Temperature/Humidity



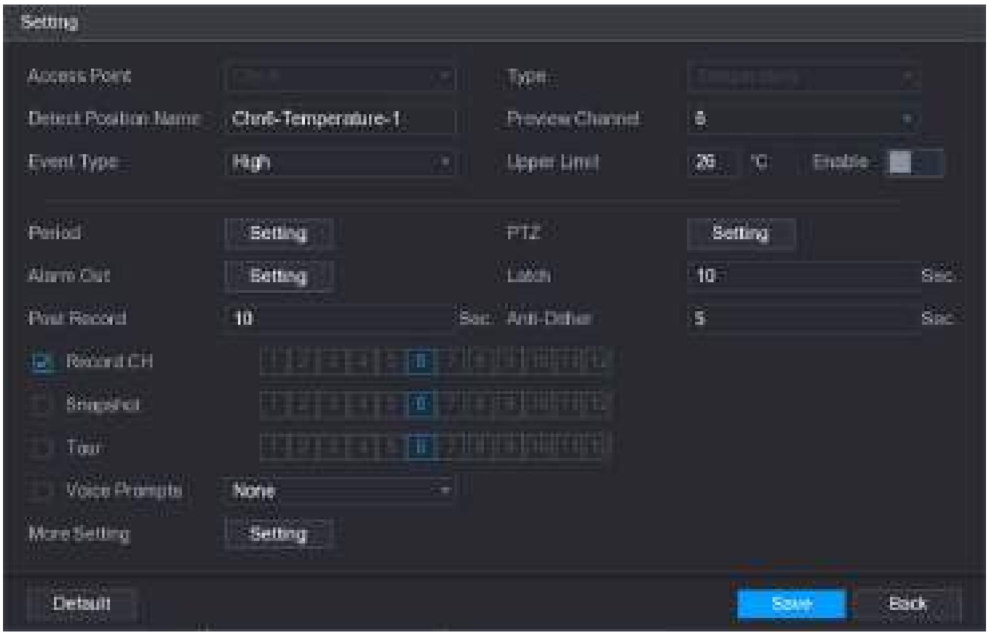
Sensor Pairing | Temperature/Hu... | Wireless Detector | Wireless Siren

0	Enable	Setting	Access Point	Type	Access Point Name

□ Show °F(Fahrenheit Degree)

Step 2 On the temperature information line, click ⚙.

Figure 5-256 Setting



Setting

Access Point | Type

Detect Position Name: Chn6-Temperature-1 | Preview Channel: 6

Event Type: High | Upper Limit: 26 °C | Enable

Period: Setting | PTZ: Setting

Alarm Out: Setting | Latch: 10 Sec.

Post Record: 10 Sec. | Anti-Dither: 5 Sec.

☑ Record CH: 1 2 3 4 5 6 7 8 9 10 11 12

□ Snapshot: 1 2 3 4 5 6 7 8 9 10 11 12

□ Tour: 1 2 3 4 5 6 7 8 9 10 11 12

□ Voice Prompts: None

More Setting: Setting

Default | Save | Back

Step 3 Configure the settings for alarm linkage.

Table 5-42 Alarm linkage settings

Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Type	**Temperature** by default.
Detect Position Name	Set the detect position name.
Preview Channel	Select the channel that you want to preview to help monitor the channel of access point. This channel could be the channel of access point or any other channels according to your actual situation.

Parameter	Description
Event Type	Select event type as **High** or **Low**, and set the upper and low temperature limit respectively. For example, select event type as **High** and set upper limit as **28**, the alarm occurs when the temperature reaches 28 °C.
Upper Limit	
Enable	Enable the alarm function.
Schedule	Define a period during which the alarm setting is active. For more information about setting the period, see "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. ● External Alarm: Enable alarm activation through the connected alarm box. ● Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Snapshot	Select the checkbox to take a snapshot of the selected channel. 📖 To use this function, make sure the snapshot is enabled motion detect alarms in **Main Menu > STORAGE > Schedule > Snapshot**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs. 📖 The recording for IoT alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Tour	Select the checkbox to enable a tour of the selected channels. 📖 To use this function, make sure the tour is enabled and configured in **Main Menu > DISPLAY > Tour**.
Alarm Tone	Select to enable audio broadcast/alarm tones in response to a temperature alarm event.

Parameter	Description
More Setting	● Show Message: Select the **Show Message** checkbox to enable a pop-up message in your local host PC. ● Buzzer: Select the checkbox to activate a buzzer noise at the Device. ● Video Matrix: Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "**Main Menu > DISPLAY > Tour**." 📖 Not all models support this function. ● Send Email: Enable the system to send an email notification when an alarm event occurs. 📖 To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**. ● Log: Select the checkbox to enable the Device to record a local alarm log. ● Extra screen: Select the checkbox to enable the function. When an alarm event occurs, the extra screen outputs the settings configured in **Main Menu > DISPLAY > Tour > Sub Screen.** 📖 ● Not all models support this function. ● To use this function, extra screen shall be enabled.

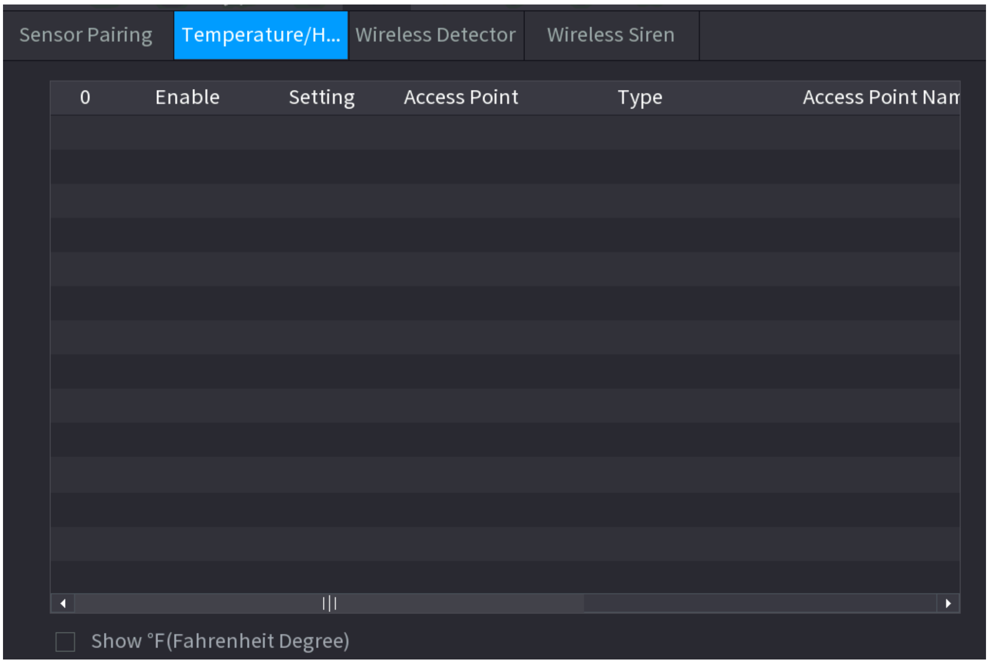
Step 4 Click **Save** to save the settings.

5.12.2.4.2 Configuring Alarm Settings for Humidity Data

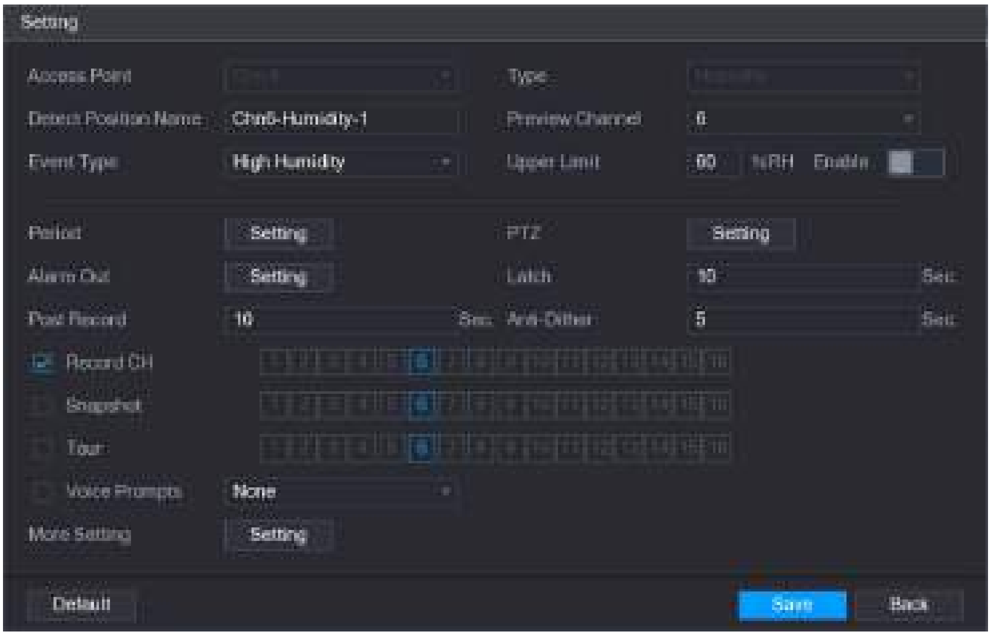
You can configure the alarm event by setting the humidity data.

Step 1 On the home page, select **IoT > Management > Temperature/Humidity**.

Figure 5-257 Temperature/Humidity



Step 2 On the humidity information line, click ⚙.



Setting

Detect Position Name: Chn6-Humidity-1

Preview Channel: 6

Event Type: High Humidity

Upper Limit: 60 %RH

Post Record: 10 Sec.

Latch: 10 Sec.

Anti-Dither: 5 Sec.

☑ Record CH

Voice Prompts: None

Figure 5-258 Setting

Step 3 Configure the settings for the following parameters.

Table 5-43 Alarm settings

Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Type	**Humidity** by default.
Detect Position Name	Set the detect position name.
Preview Channel	Select the channel that you want to preview to help monitor the channel of access point. This channel could be the channel of access point or any other channels according to your actual situation.
Event Type	Select event type as **High Humidity** or **Low Humidity**, and set the upper and low humidity limit respectively. For example, select event type as **High Humidity** and set upper limit as **60**, the alarm occurs when the humidity reaches 60%RH.
Upper Limit	
Enable	Enable the alarm function.
Schedule	Define a period during which the alarm setting is active. For more information about setting the period, see "5.10.4.1 Configuring Motion Detection Settings."
Alarm-out Port	Click **Setting** to display setting page. ● General Alarm: Enable alarm activation through the alarm devices connected to the selected output port. ● External Alarm: Enable alarm activation through the connected alarm box. ● Wireless Siren: Enable alarm activation through devices connected by USB gateway or camera gateway.

Parameter	Description
PTZ Linkage	Click **Setting** to display the PTZ page. Enable PTZ linkage actions, such as selecting the preset that you want to be called when an alarm event occurs.
Post-Alarm	Set a length of time for the Device to delay turning off alarm after the external alarm is cancelled. The value ranges from 0 seconds to 300 seconds, and the default value is 10 seconds. If you enter 0, there will be no delay.
Post Record	Set a length of time for the Device to delay turning off recording after the alarm is cancelled. The value ranges from 10 seconds to 300 seconds, and the default value is 10 seconds.
Anti-Dither	Configure the time period from end of event detection to the stop of alarm.
Snapshot	Select the checkbox to take a snapshot of the selected channel. To use this function, make sure the snapshot is enabled motion detect alarms in **Main Menu > STORAGE > Schedule > Snapshot**.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs. The recording for IoT alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Tour	Select the checkbox to enable a tour of the selected channels. To use this function, make sure the tour is enabled and configured in **Main Menu > DISPLAY > Tour**.
Alarm Tone	Select to enable audio broadcast/voice prompts in response to a temperature alarm event.
More Setting	● Show Message: Select the **Show Message** checkbox to enable a pop-up message in your local host PC. ● Buzzer: Select the checkbox to activate a buzzer noise at the Device. ● Video Matrix: Select the checkbox to enable the function. When an alarm event occurs, the video output port outputs the settings configured in "**Main Menu > DISPLAY > Tour**." Not all models support this function. ● Send Email: Enable the system to send an email notification when an alarm event occurs. To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**. ● Log: Select the checkbox to enable the Device to record a local alarm log.

Step 4 Click **Save** to save the settings.

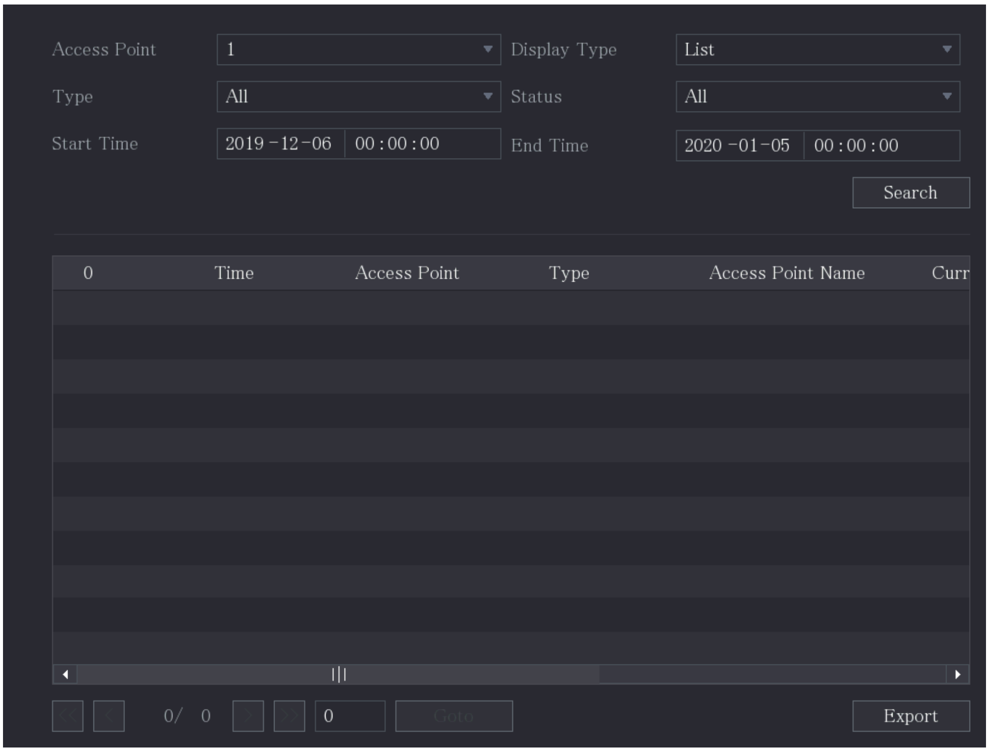
5.12.2.5 Searching IoT Information

You can search and backup all your IoT data.

To back up the data, you should prepare a USB device and plug it into the Device.

Step 1 On the home page, select **IoT** > **IOT Search**.

Figure 5-259 IOT search



Access Point: 1
Display Type: List
Type: All
Status: All
Start Time: 2019 -12-06 00 : 00 : 00
End Time: 2020 -01-05 00 : 00 : 00

0	Time	Access Point	Type	Access Point Name	Curr

Step 2 Configure the parameters settings.

Table 5-44 IOT search parameters

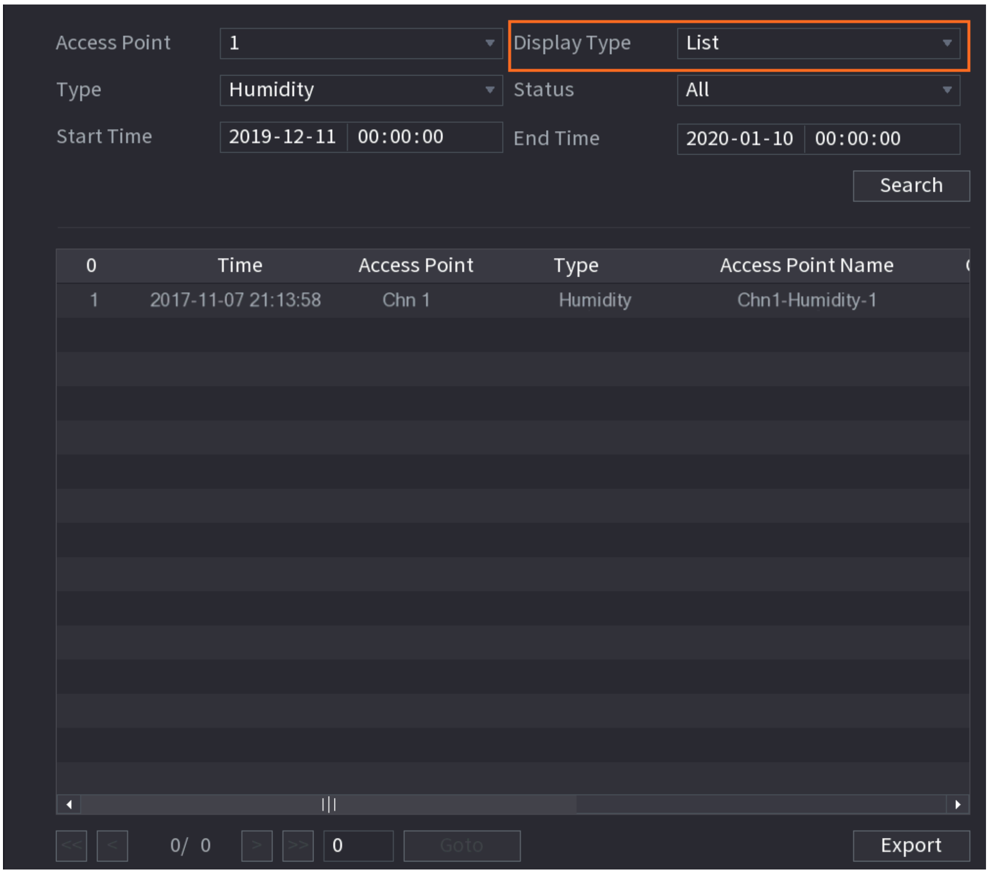
Parameter	Description
Access Point	Indicates the channel that the camera is connected to.
Display Type	In the **Display Type** list, select **List** or **Diagram**.
Type	Select the information type that you want to search. You can select **Humidity** or **Temperature**.
Status	Select the information state that you want to search. This option is available when you select **List** in the **Display Type** list.
Start Time	Enter the start time and end time for the information that you want to search.
End Time	

Step 3 Click **Search**.

The system starts search according to your parameters settings. After searching is finished, the result displays.

Click **Goto** to switch result pages.

Figure 5-260 List



Access Point: 1

Display Type: List

Type: Humidity

Status: All

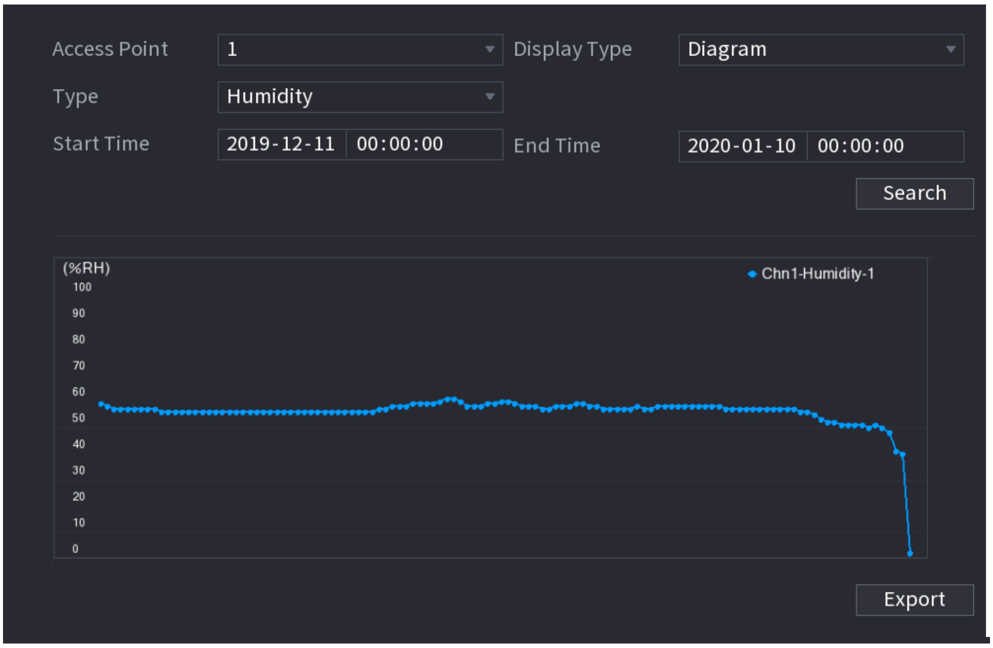
Start Time: 2019-12-11 00:00:00

End Time: 2020-01-10 00:00:00

0	Time	Access Point	Type	Access Point Name
1	2017-11-07 21:13:58	Chn 1	Humidity	Chn1-Humidity-1

0/ 0 0

Figure 5-261 Diagram



Access Point: 1

Display Type: Diagram

Type: Humidity

Start Time: 2019-12-11 00:00:00

End Time: 2020-01-10 00:00:00

Step 4 Click **Export.** The system starts exporting the data.

Step 5 Click **OK**.

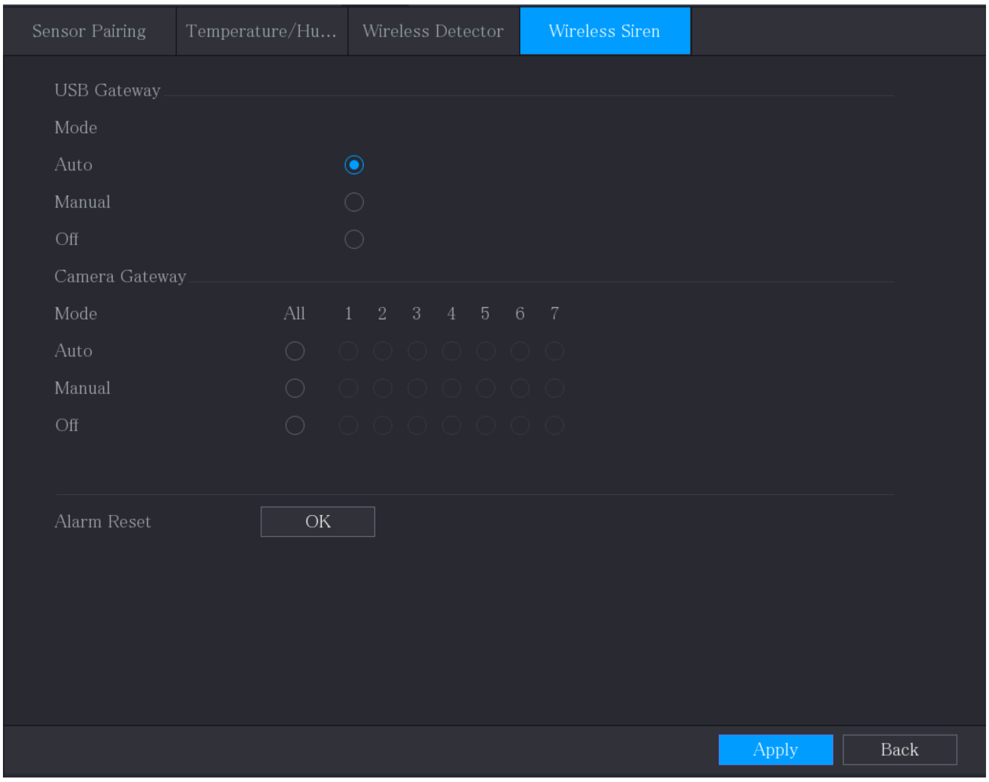
You can find the exported data on your USB device.

5.12.3 Configuring Wireless Siren

You can connect the wireless siren to the Device, when there is an alarm event activated on the Device, the wireless siren generates alarms.

Step 1 Select **Main Menu** > **IoT** > **Management** > **Wireless Siren**.

Figure 5-262 Wireless siren



Step 2 Configure the settings for the wireless alarm output.

Table 5-45 Wireless alarm output parameters

Parameter	Description
USB Gateway, Camera Gateway	● **Auto**: Automatically activate alarm if the alarm output function for wireless siren is enabled for specific events. For example, if you want to enable the alarm output through wireless siren for motion detection, see "Alarm Output" parameter in 0. ● **Manual**: Activate alarm immediately. ● **Off**: Do not activate alarm.
Alarm Release	Click **OK** to clear all alarm output status of wireless siren.

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

5.13 Configuring POS Settings

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.

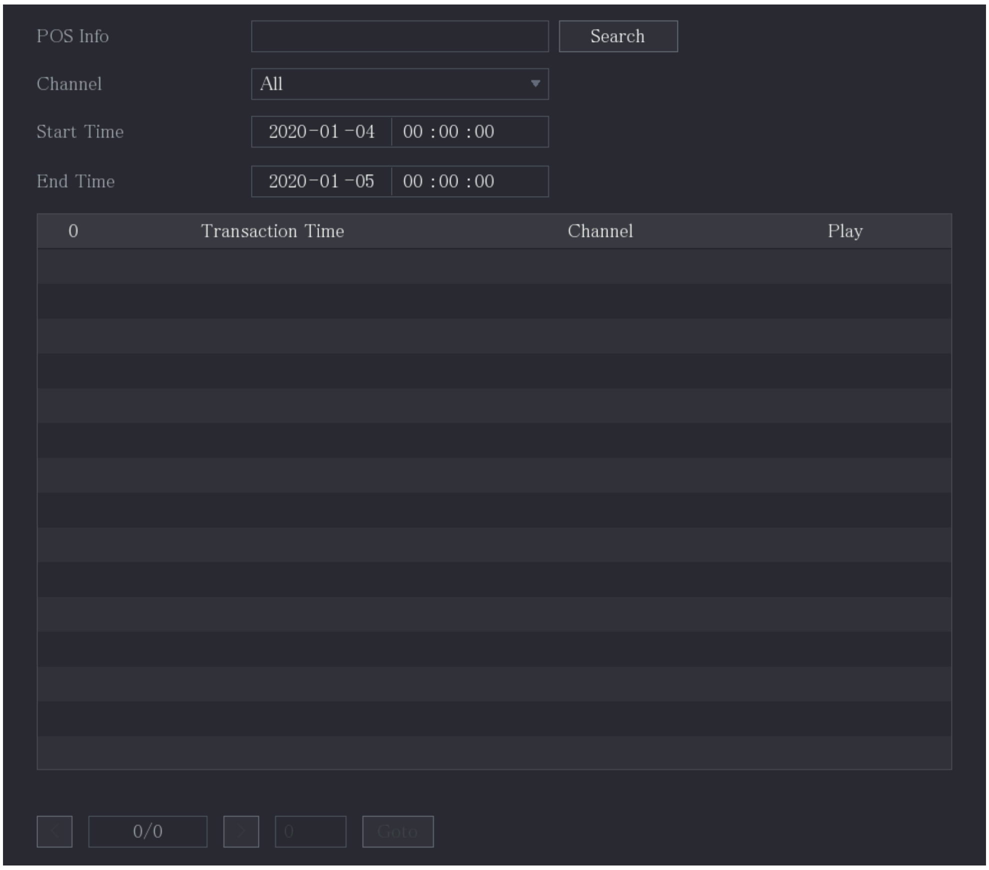
Playing POS information in the local playback and viewing the POS information in the live view screen only support single-channel mode and four-channel mode. Displaying monitoring screen and playing back in the web support multi-channel mode.

5.13.1 Searching the Transaction Records

The system supports fuzzy search.

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

Figure 5-263 POS search



POS Info

Channel: All

Start Time: 2020-01-04 00 :00 :00

End Time: 2020-01-05 00 :00 :00

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.

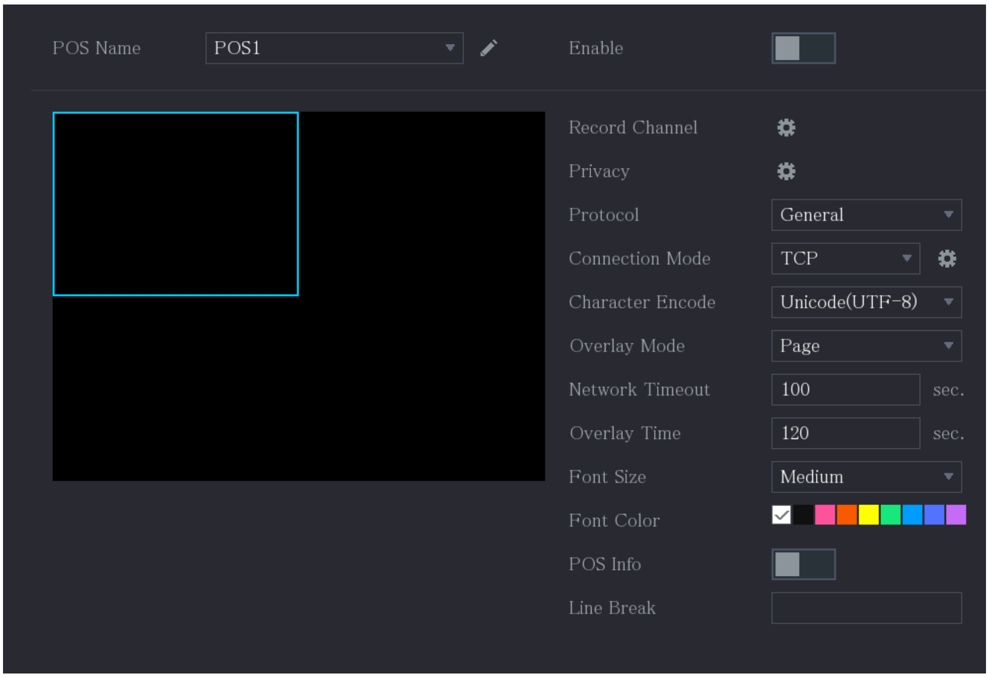
Step 4 Click **Search**.

The searched transaction results display in the table.

5.13.2 Configuring POS Settings

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

Figure 5-264 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 settings for the POS parameters.

Table 5-46 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 supports 21 Chinese characters or 63 English characters.
Enable	Enable the POS function.
Record Channel	Select the channel(s) that you want to record. The selected channel(s) starts recording after an alarm occurs. 🕮 The recording for POS alarms and auto recording function must be enabled. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.9.1 Enabling Record Control."
Privacy	Enter the privacy content.
Protocol	Select **POS** by default. Different machine corresponds to different protocol.
Connection Mode	In the **Connect Type** list, select the connection protocol type. Click ⚙, the IP Address page 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 **Page** or **ROLL**. ● **Page** means to turn a page when there are 16 lines of overlay information. ● **ROLL** means to roll up the page when there are 16 lines of overlay information. The first line disappears each time. 📖 When local preview mode is 4-split, overlay information is substituted when there are 8 lines.
Network Timeout	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.
Overlay Time	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	In the Font Size list, select **Small**, **Medium**, or **Large** 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 screen.
Line Break	It does not need to configure. The system goes to a new line 1s after no data is received. If you enter a line delimiter, the system goes to a new line when overlay information identifies the line delimiter (hexadecimal). For example, if line delimiter is F and overlay information is 123F6789, the local preview and web overlay information is displayed as: 123 6789

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

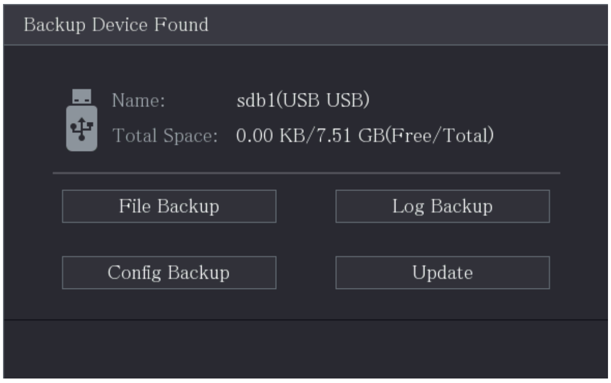
5.14 Configuring Backup Settings

5.14.1 Finding USB Device

When you inset a USB storage device into the USB port of the Device, the Device detects the USB storage device and pops up **Find USB device** page, which provides you a shortcut to perform backup and upgrading operations.

For details, see "5.14.2 Backing up Files", "5.21.2 Viewing Log Information", "5.20.4 Exporting and Importing System Settings", and "5.20.6 Updating the Device."

Figure 5-265 Backup device



Backup Device Found

Name: sdb1(USB USB)

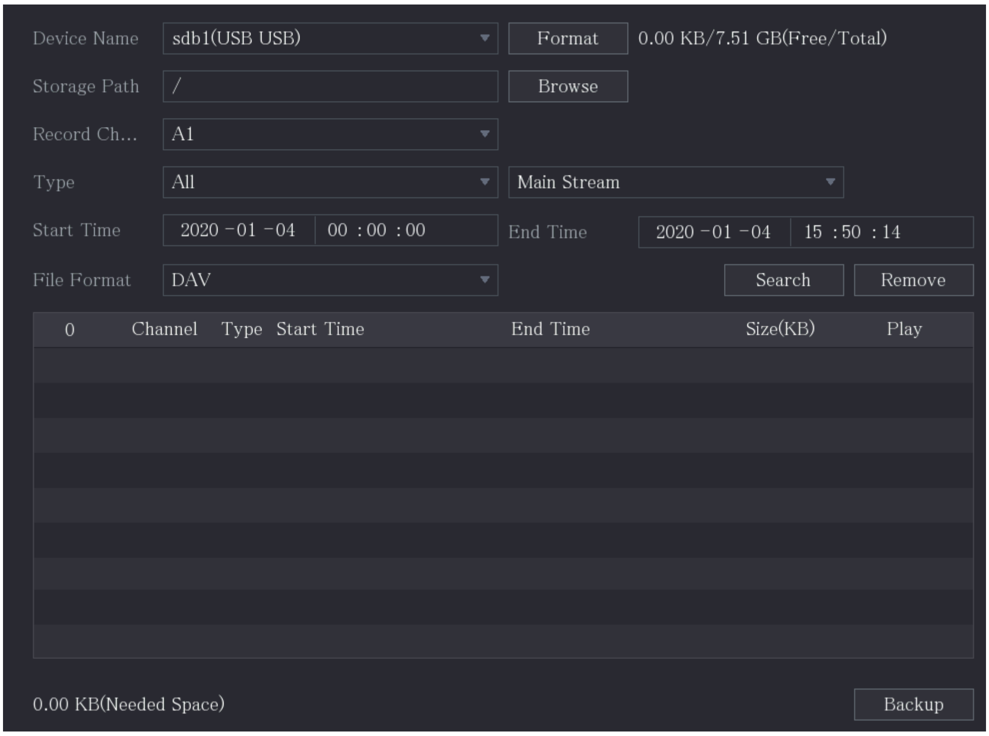
Total Space: 0.00 KB/7.51 GB(Free/Total)

5.14.2 Backing up Files

You can back up the recorded videos and snapshots.

Step 1 Select **Main Menu** > **Backup**.

Figure 5-266 Backup



Device Name: sdb1(USB USB) 0.00 KB/7.51 GB(Free/Total)

Storage Path: /

Record Ch...: A1

Type: All, Main Stream

Start Time: 2020 -01 -04 00 :00 :00 End Time: 2020 -01 -04 15 :50 :14

File Format: DAV

0	Channel	Type	Start Time	End Time	Size(KB)	Play

0.00 KB(Needed Space)

Step 2 Configure the settings for the backup parameters.

Table 5-47 Backup parameters

Parameter	Description
Device Name	In the **Device Name** list, select the device that you want to back up the files to.
Format	Click **Format**, the **Format** page is displayed. ● If the capacity of external storage device is less than 2 TB, you can select **FAT32** or **NTFS** to format it. ● If the capacity of external storage device is equal to or more than 2 TB, you can only select **NTFS** to format it.

Parameter	Description
Path	Click **Browse**, the **Browse** page is displayed. Select the route where you want to search for the files.
Record Channel	In the **Record Channel** list, select the channel where you want to search for the files.
Type	In the **Type** list, select the file type that you want to search.
Start Time	Enter the start time and end time for the files that you want to search.
End Time	
File Format	In the **File Format** list, select the file format as **DAV** or **MP4** that you want to search.

Step 3 Click **Search** to search the files that meet the configured settings.

The searched results will display in the table.

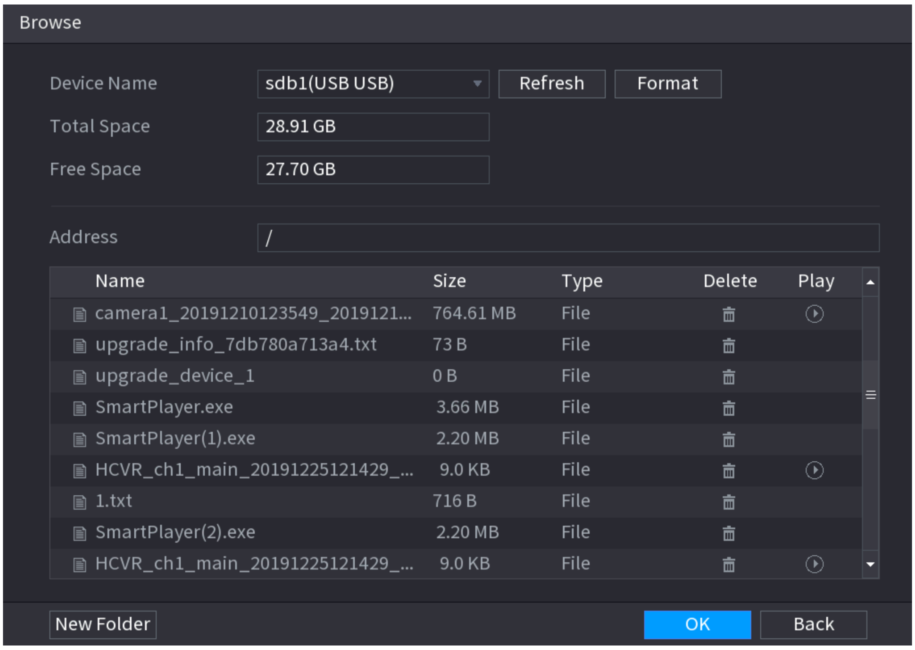
Step 4 Select the files that you want to back up.

Step 5 Click **Backup** to back up the selected files to the configured path.

Click **Remove** to remove all the searched results.

The system will display a backup progress bar. A dialog box will be prompted When backup is completed.

Figure 5-267 Browse



Browse

Device Name: sdb1(USB USB)

Total Space: 28.91 GB

Free Space: 27.70 GB

Address: /

Name	Size	Type	Delete	Play
camera1_20191210123549_2019121...	764.61 MB	File	🗑	▶
upgrade_info_7db780a713a4.txt	73 B	File	🗑	
upgrade_device_1	0 B	File	🗑	
SmartPlayer.exe	3.66 MB	File	🗑	
SmartPlayer(1).exe	2.20 MB	File	🗑	
HCVR_ch1_main_20191225121429_...	9.0 KB	File	🗑	▶
1.txt	716 B	File	🗑	
SmartPlayer(2).exe	2.20 MB	File	🗑	
HCVR_ch1_main_20191225121429_...	9.0 KB	File	🗑	▶

Step 6 Click **OK**.

5.15 Network Management

5.15.1 Configuring Network Settings

You can ensure the network interworking between the Device and other devices through configuring the network settings.

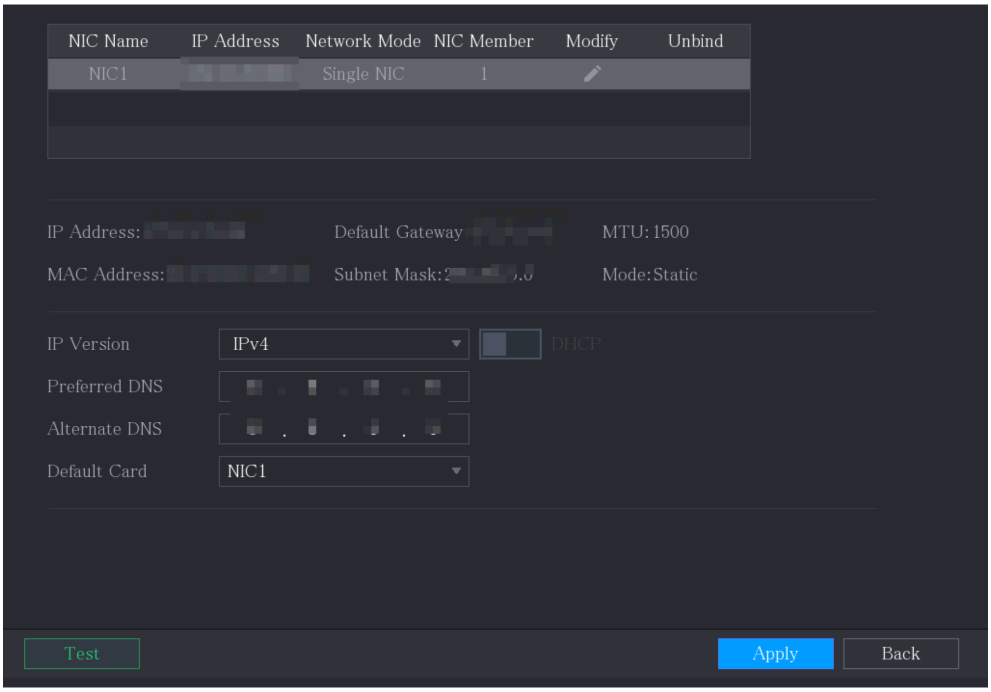
5.15.1.1 Configuring TCP/IP Settings

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

Select **Main Menu** > **NETWORK** > **TCP/IP**, the **TCP/IP** page is displayed.

For details about parameter settings, see "5.1.4.4 Configuring Network Settings."

Figure 5-268 TCP/IP



NIC Name	IP Address	Network Mode	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]

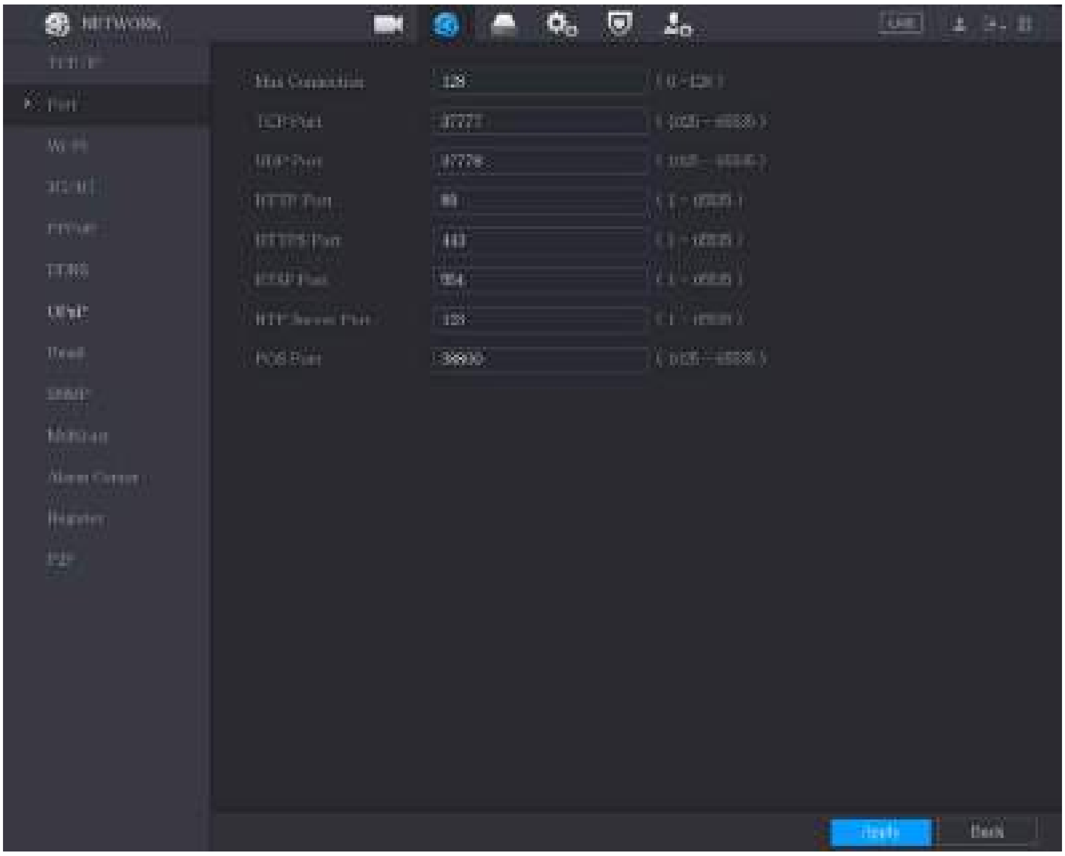
Default Card: NIC1

5.15.1.2 Configuring Port Settings

You can configure the maximum connection accessing the Device from Client such as WEB, Platform, and Mobile Phone and configure each port settings.

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

Figure 5-269 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)

Step 2 Configure the settings for the connection parameters.

The parameter setting can take effect without need to reboot the device.

Table 5-48 Connection parameters

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as WEB, Platform, and Mobile Phone. Select a value between 1 and 128. The default value setting is 128.
TCP Port	The default value setting is 37777. You can enter the value according to your actual situation.
UDP Port	The default value setting is 37778. You can 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 enter other value, for example, 70, and then you should enter 70 after the IP address when logging in the Device by browser.
RTSP Port	The default value setting is 554. You can enter the value according to your actual situation.
POS Port	Data transmission. The value range is from 1 through 65535. The default value is 38800.
NTP Server Port	The default value setting is 123. You can enter the value according to your actual situation.

Parameter	Description
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.

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

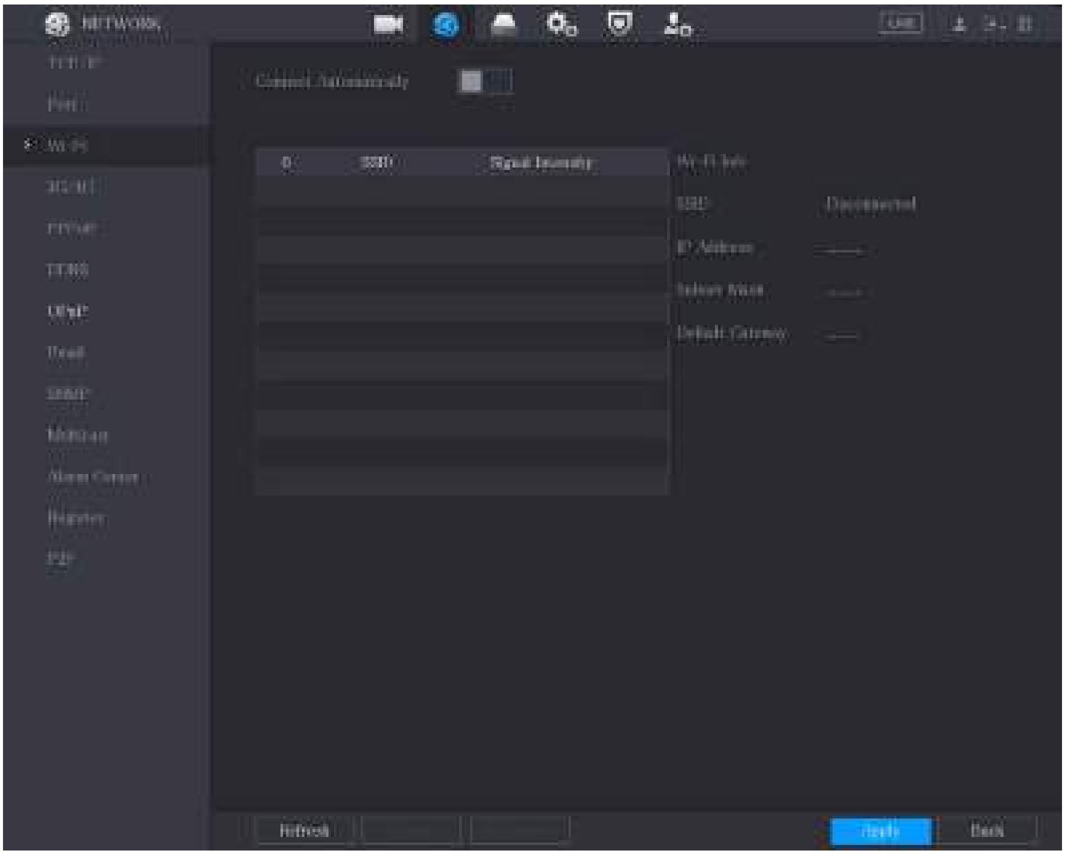
5.15.1.3 Configuring Wi-Fi Connection Settings

You can make wireless connection between the Device and the other devices in the same network through Wi-Fi settings, facilitating the devices connection and mobility.

Only the Device with Wi-Fi module supports this function.

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

Figure 5-270 Wi-Fi



Step 2 Configure the settings for the Wi-Fi connection parameters.

Table 5-49 Wi-Fi connection parameters

Parameter	Description
Connect Automatically	Enable **Connect Automatically**. After the Device is restarted, it will automatically connect to the nearest hotspot that had been connected successfully.
Refresh	Refresh the hotspot list. The self-adaption function such as adding password is supported if such setting was once configured.
Connect	In the hotpots list, select a hotspot, and then click **Connect**. ● To reconnect the same hotspot, disconnect first and then reconnect. ● To connect to other hotspot, disconnect from the current connected hotspot first, and then connect to the other hotspot.
Disconnect	To disconnect from a hotspot, click **Disconnect**.

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

After the Device is connected to a Wi-Fi hotspot, in the **Wi-Fi Info** area, the current hotspot, IP address, subnet mask, and default gateway are displayed.

5.15.1.4 Configuring 3G/4G Settings

You can connect a wireless 3G/4G module to the USB port of the Device and then access the Device with the IP address provided by the module.

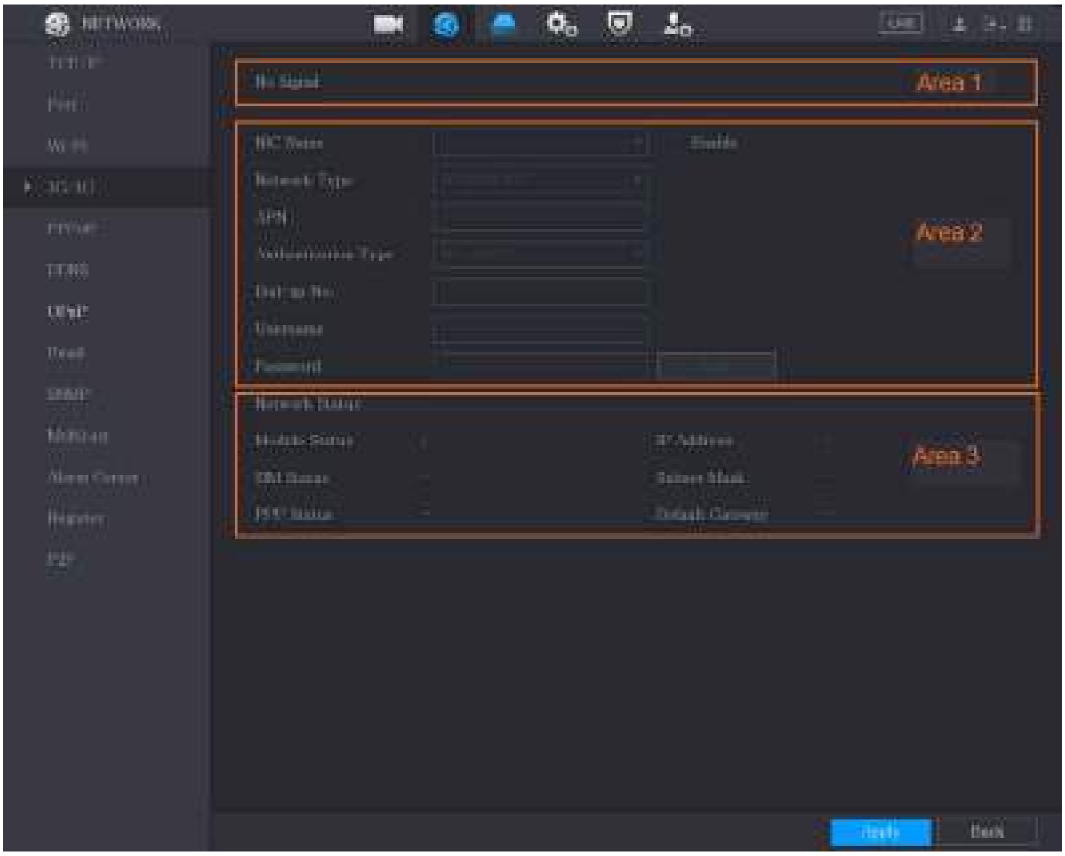
📖

Not all models support this function.

Step 1 Connect the wireless 3G/4G module to the USB port of the Device.

Step 2 Select **Main Menu** > **NETWORK** > **3G/4G**.

Figure 5-271 3G/4G



The 3G/4G page consists of three areas:

- Area 1: Displays the signal strength.
- Area 2: Displays the module configurations.
- Area 3: Displays the connection state.

The information of Area 2 will display after the 3G/4G module is connected; while the information of Area 1 and Area 3 will display only after the 3G/4G function is enabled.

Step 3 The Device starts identifying the wireless module and displays the recognized information for the parameters in Area 2.

Table 5-50 Recognized information

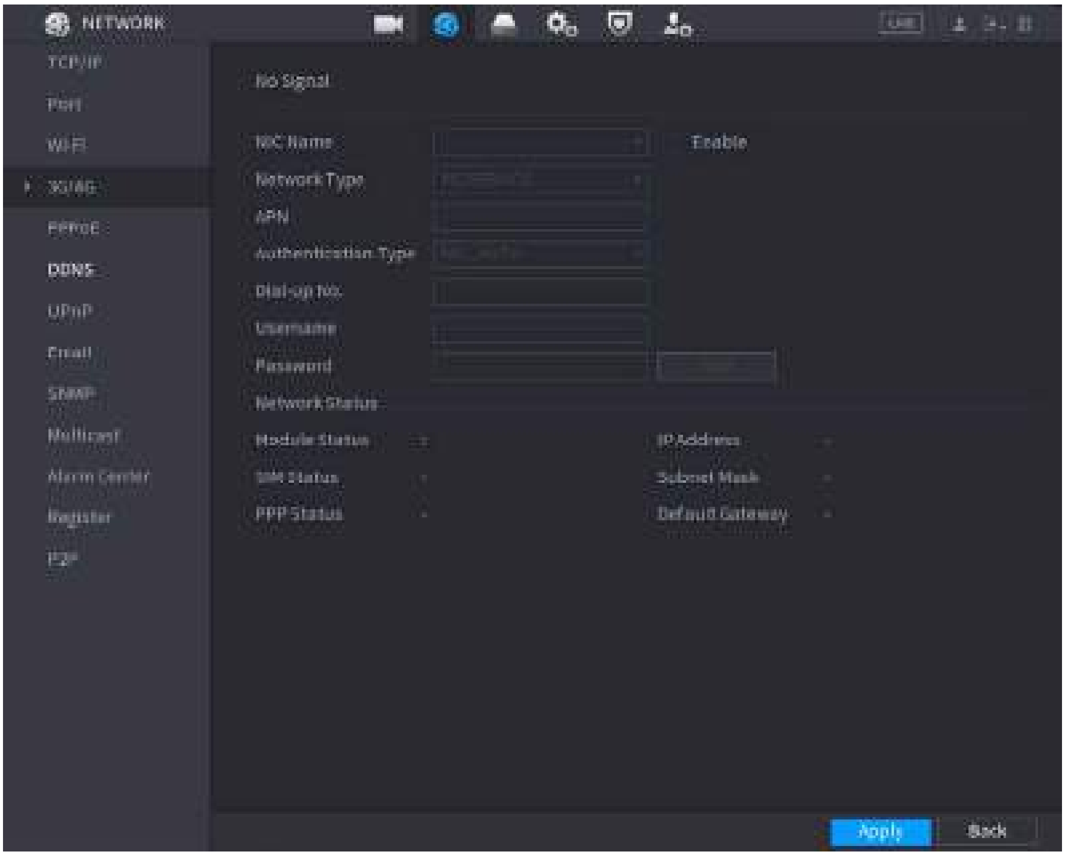
Parameter	Description
NIC Name	Displays the name of Ethernet card.
Network Type	Displays the network type. Different type represents different supplier.
APN	Displays the default APN number.
Dial-up No.	Displays the default dial No.
Authentication Type	Authentication mode. You can select **PAP**, **CHAP**, or **NO_AUTH**.
Username, Password	Enter the username and password for authentication.

Step 4 Select the **Enable** checkbox.

Step 5 Click **Dial** to start connecting.

After the connection is established, the result is displayed in the **Wireless Network** area.

Figure 5-272 Wireless network



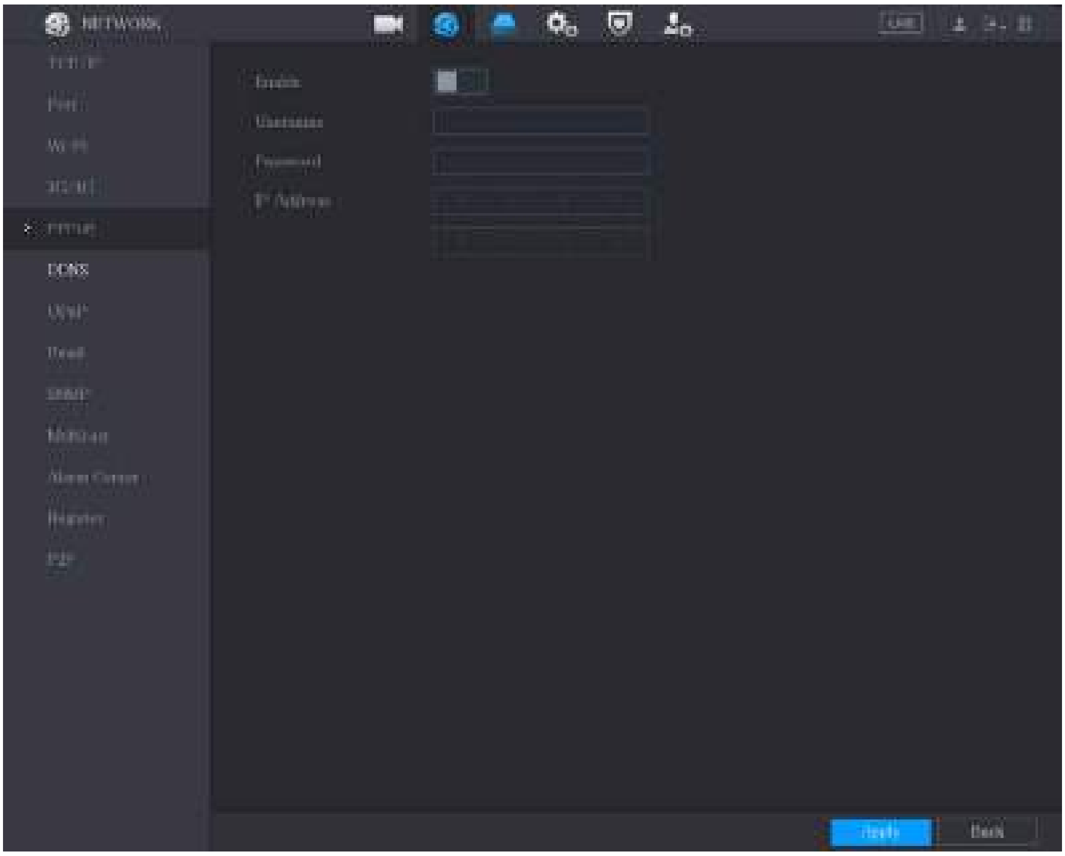
Step 6 Click **Apply** to complete the settings.

5.15.1.5 Configuring PPPoE Settings

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 in the WAN. To use this function, firstly you need to obtain the user name and password from the Internet Service Provider.

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

Figure 5-273 PPPoE



Step 2 Enable the PPPoE function.

Step 3 In the **Username** box and **Password** box, enter the user name and password accordingly provided by the Internet Service Provider.

Step 4 Click **Apply** to complete the settings.

The system pops up a message to indicate the successfully saved. 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.

5.15.1.6 Configuring DDNS Settings

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, ensuring you access the Device by using the domain.

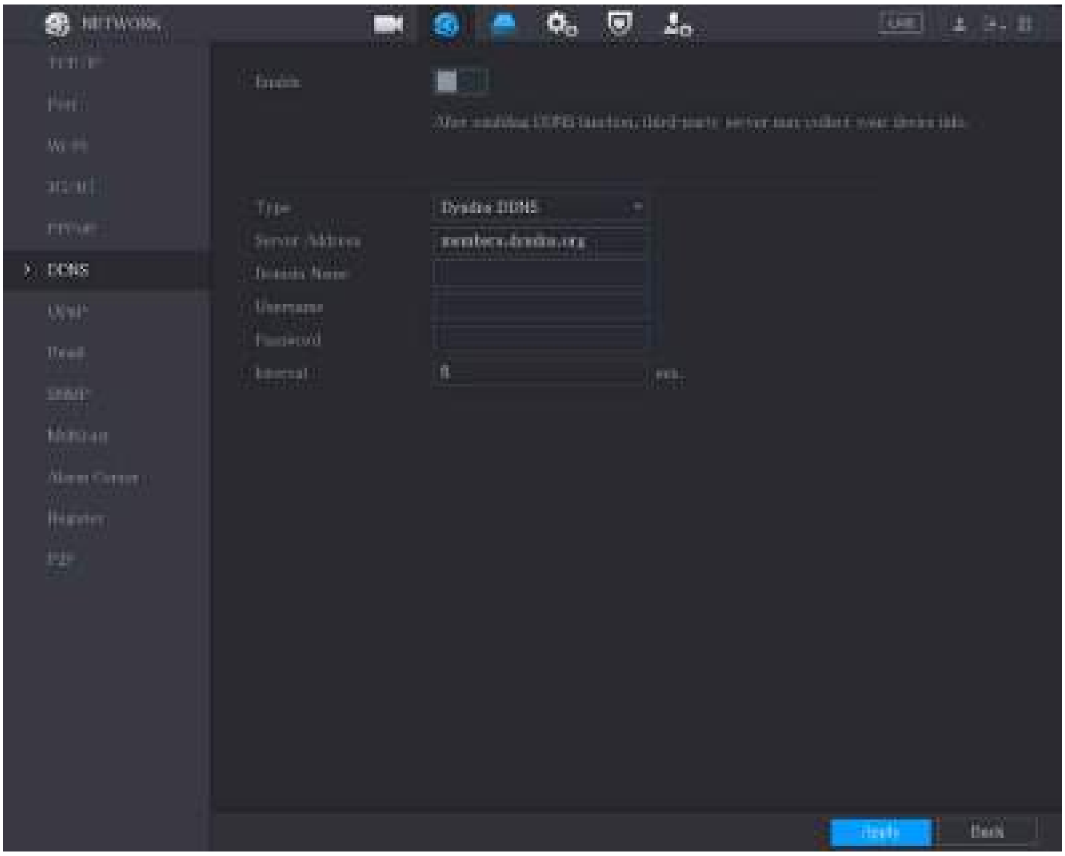
Preparation

Confirm if the Device supports the DDNS Type and log in the website provided by the DDNS service provider to register the information such as domain from PC located in the WAN.

After you have registered and logged in the DDNS website successfully, you can view the information of all the connected devices under this user name.

Procedure

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



Enable

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

Type: Dyndns DDNS

Server Address: members.dyndns.org

Domain Name

Username

Password

Interval

Figure 5-274 DDNS

Step 2 Configure the settings for the DDNS parameters.

Table 5-51 DDNS parameters

Parameter	Description
Enable	Enable the DDNS function. After enabling DDNS function, the third-party might collect your Device information.
Type	Type and address of DDNS service provider. ● Type: Dyndns DDNS; address: members.dyndns.org ● Type: NO-IP DDNS; address: dynupdate.no-ip.com ● Type: CN99 DDNS; address: members.3322.org
Server Address	
Domain Name	The domain name for registering on the website of DDNS service provider.
User Name	Enter the user name and password obtained from DDNS service provider. You need to register (including user name and password) on the website of DDNS service provider.
Password	
Interval	Enter the amount of time that you want to update the DDNS.

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

Enter the domain name in the browser on your PC, and then press **Enter**.

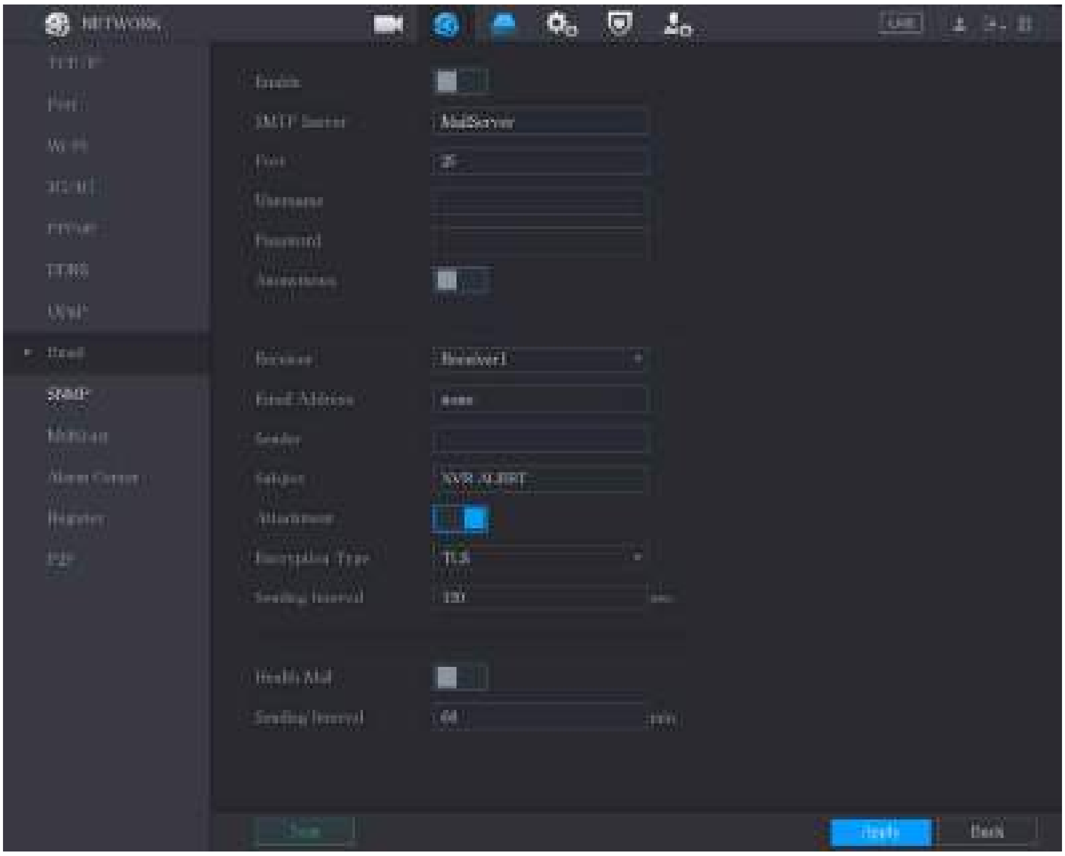
If the web page of the Device is displayed, the configuration is successful. If not, the configuration is failed.

5.15.1.7 Configuring EMAIL Settings

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

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

Figure 5-275 Email



Enable
SMTP Server MailServer
Port 25
Username
Password
Anonymous
Receiver Receiver1
Email Address
Sender
Subject NVR ALERT
Attachment
Encryption Type TLS
Sending Interval 120 sec.
Health Mail
Sending Interval 60 min.

Step 2 Configure the settings for the email parameters.

Table 5-52 Email parameters

Parameter	Description
Enable	Enable the email function. 📖 There might be risk of sending data to specified email address after it is enabled.
SMTP Server	Enter the address of SMTP server of sender's email account.
Port	Enter the port value of SMTP server. The default value setting is 25. You can enter the value according to your actual situation.
Username	Enter the user name and password of sender's email account.
Password	
Anonymous	If enable the anonymity function, you can login as anonymity.

Parameter	Description
Receiver	In the **Receiver** list, select the number of receiver that you want to receive the notification. The Device supports up to three mail receivers.
Email Address	Enter the email address of mail receiver(s).
Sender	Enter the sender's email address. It supports maximum three senders separated by comma.
Subject	Enter the email subject. Supports Chinese, English and numerals. It supports maximum 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: **NONE**, **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.
Sending Interval (sec.)	This is the interval that the system sends an email for the same type of alarm event, which means, the system does not send an email upon any alarm event. This setting helps to avoid the large amount 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 (Min.)	This is the interval that 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 3 Click **Apply** to complete the settings.

5.15.1.8 Configuring UPnP Settings

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.

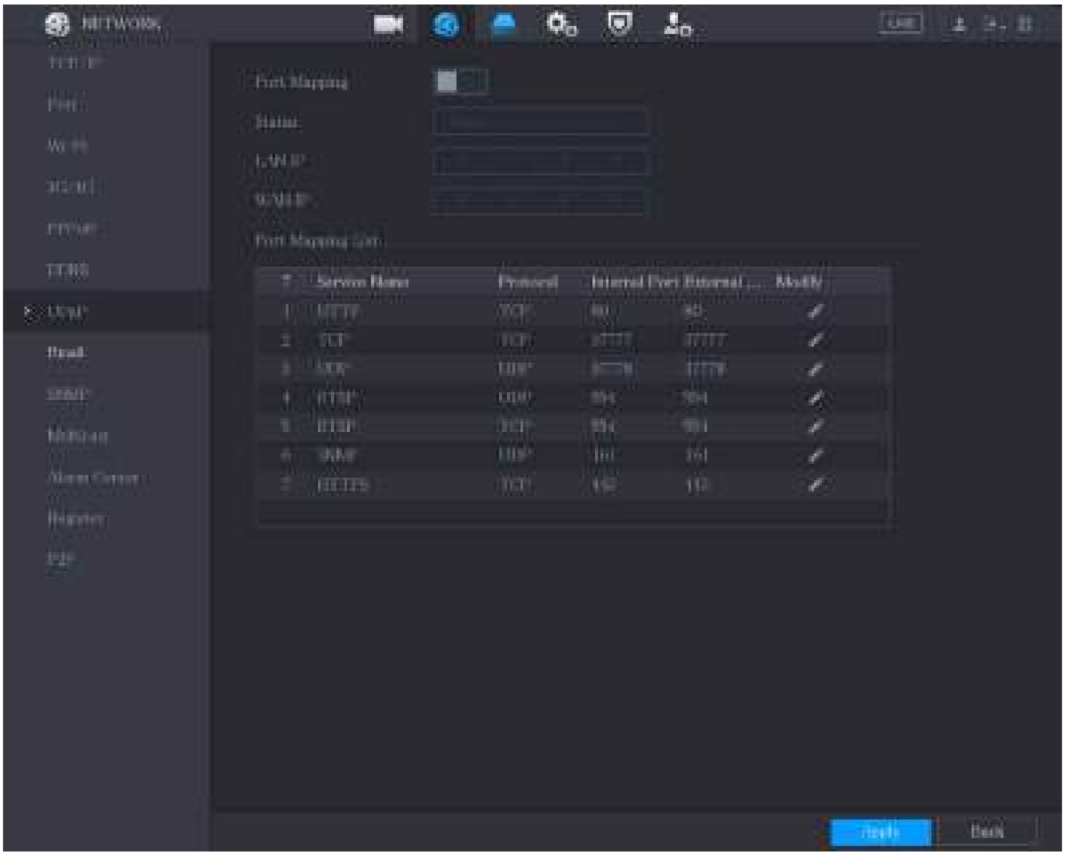
Preparation

- Log in to the router to set the WAN port to enable the IP address to connect into the WAN.
- Enable the UPnP function at the router.
- Connect the Device with the LAN port on the router to connect into the LAN.
- 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.

Procedure

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

Figure 5-276 UPnP



Port Mapping ■

Status

LAN IP

WAN IP

Port Mapping List

†	Service Name	Protocol	Internal Port	External ...	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	SNMP	UDP	161	161	✎
7	HTTPS	TCP	443	443	✎

Step 2 Configure the settings for the UPnP parameters.

Table 5-53 UPnP parameters

Parameter	Description
Port Mapping	Enable the UPnP function. After it is enabled, the intranet services and ports shall be mapped to extranet, proceed with caution.
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 without performing any configurations.
WAN IP	Enter IP address of router on the WAN. After mapping succeeded, the system obtains IP address automatically without performing any configurations.

Parameter	Description
Port Mapping List	The settings in PAT table correspond to the UPnP PAT table on the router. ● Service Name: Name of network server. ● Protocol: Type of protocol. ● Int. Port: Internal port that is mapped on the Device. ● Ext. 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 in the LAN, reasonably arrange the ports mapping 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 LAN Device.

5.15.1.9 Configuring SNMP Settings

Not all models support this function.

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.

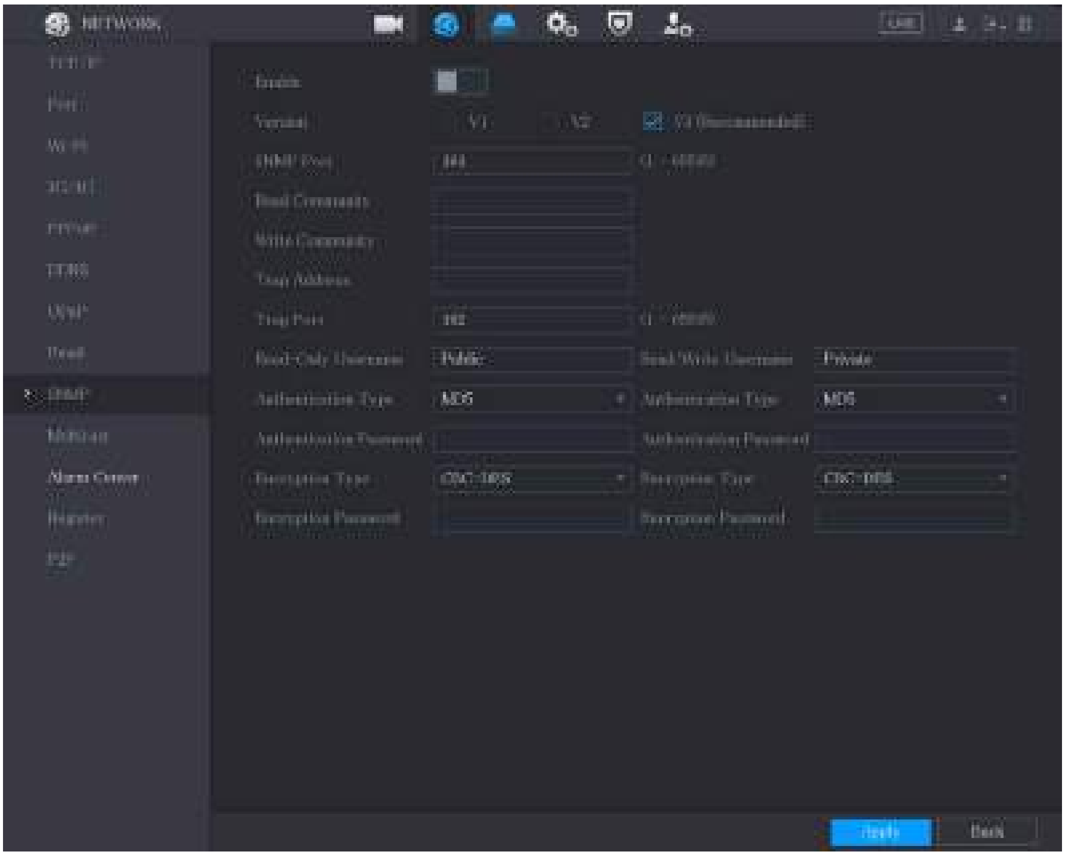
Preparation

- 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.

Procedure

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

Figure 5-277 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 Username: Private
Authentication Type: MD5 — Authentication Type: MD5
Authentication Password: — Authentication Password:
Encryption Type: CBC-DES — Encryption Type: CBC-DES
Encryption Password: — Encryption Password:

Step 2 Configure the settings for the SNMP parameters.

Table 5-54 SNMP parameters

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

Parameter	Description
Encryption Type	In the **Encryption Type** list, select an encryption type. The default setting is CBC-DES.

Step 3 Compile the two MIB files by MIB Builder.

Step 4 Run MG-SOFT MIB Browser to load in the module from compilation.

Step 5 On the MG-SOFT MIB Browser, enter the Device IP that you want to manage, and then select the version number to query.

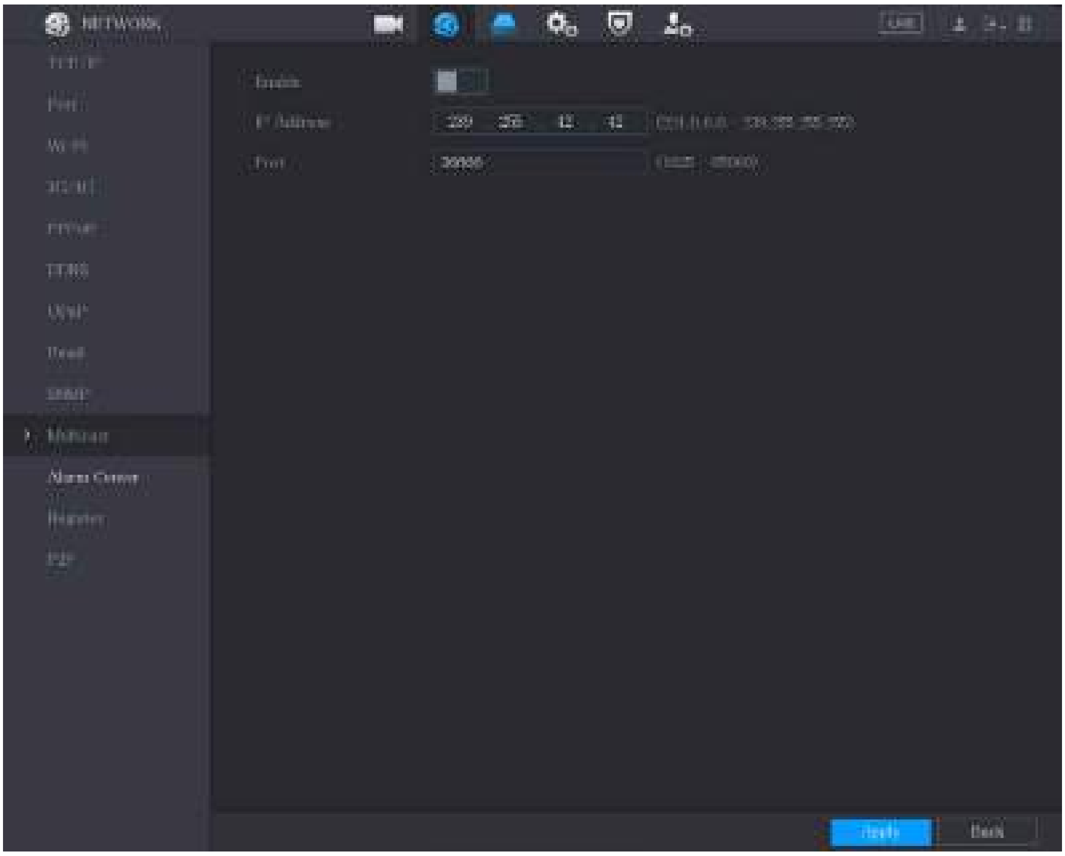
Step 6 On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

5.15.1.10 Configuring Multicast Settings

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.

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

Figure 5-278 Multicast



Enable

IP Address 239 . 255 . 42 . 42 (224.0.0.0 - 239.255.255.255)

Port 36666 (1025 - 65000)

Step 2 Configure the settings for the multicast parameters.

Table 5-55 Multicast parameters

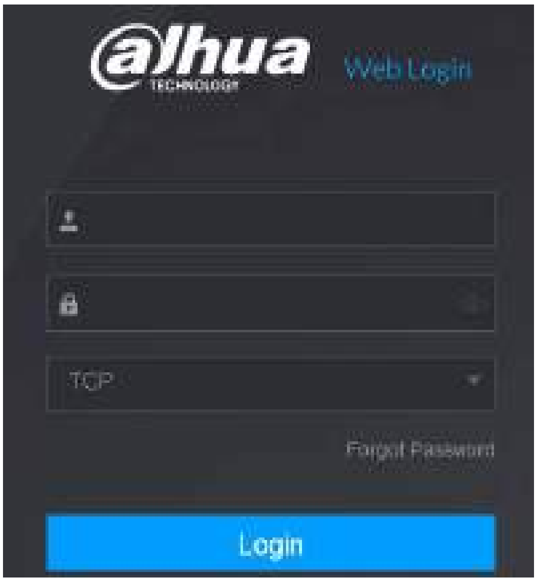
Parameter	Description
Enable	Enable the multicast function.
IP Address	Enter the IP address that you want to use as the multicast IP. The IP address ranges from 224.0.0.0 through 239.255.255.255.
Port	Enter the port for the multicast. The port ranges from 1025 through 65000.

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

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

On the web login dialog box, in the **Type** list, select **MULTICAST**. The web will automatically obtain the multicast IP address and join. Then you can view the video through multicast function.

Figure 5-279 Login

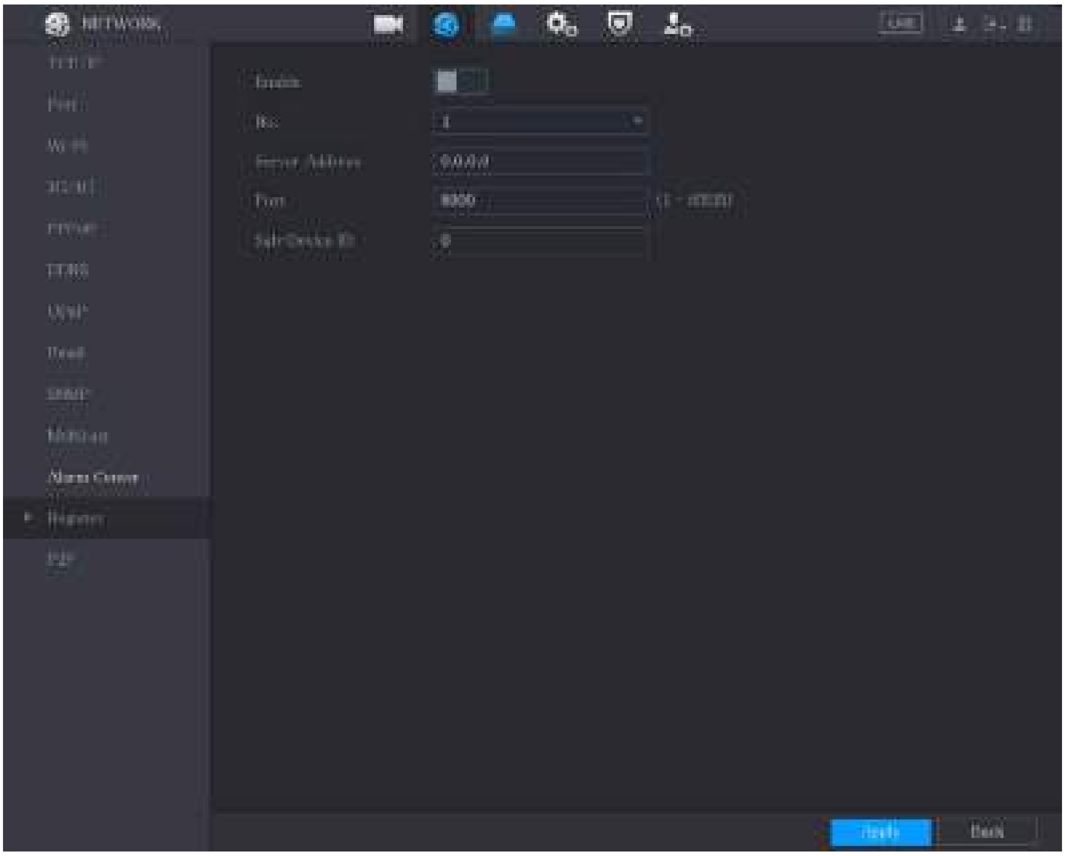


5.15.1.11 Configuring Register Settings

You can register the Device into the specified proxy server which acts as the transit to make it easier for the client software to access the Device.

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

Figure 5-280 Register



Enable □
No. 1
Server Address 0.0.0.0
Port 8000 (1 - 65535)
Sub Device ID 0

Step 2 Configure the settings for the register parameters.

Table 5-56 Register parameters

Parameter	Description
Enable	Enable the register function.
No.	The default value is 1.
Server IP Address	Enter the server IP address or the server domain that you want to register to.
Port	Enter the port of the server.
Sub Service ID	This ID is allocated by the server and used for the Device.

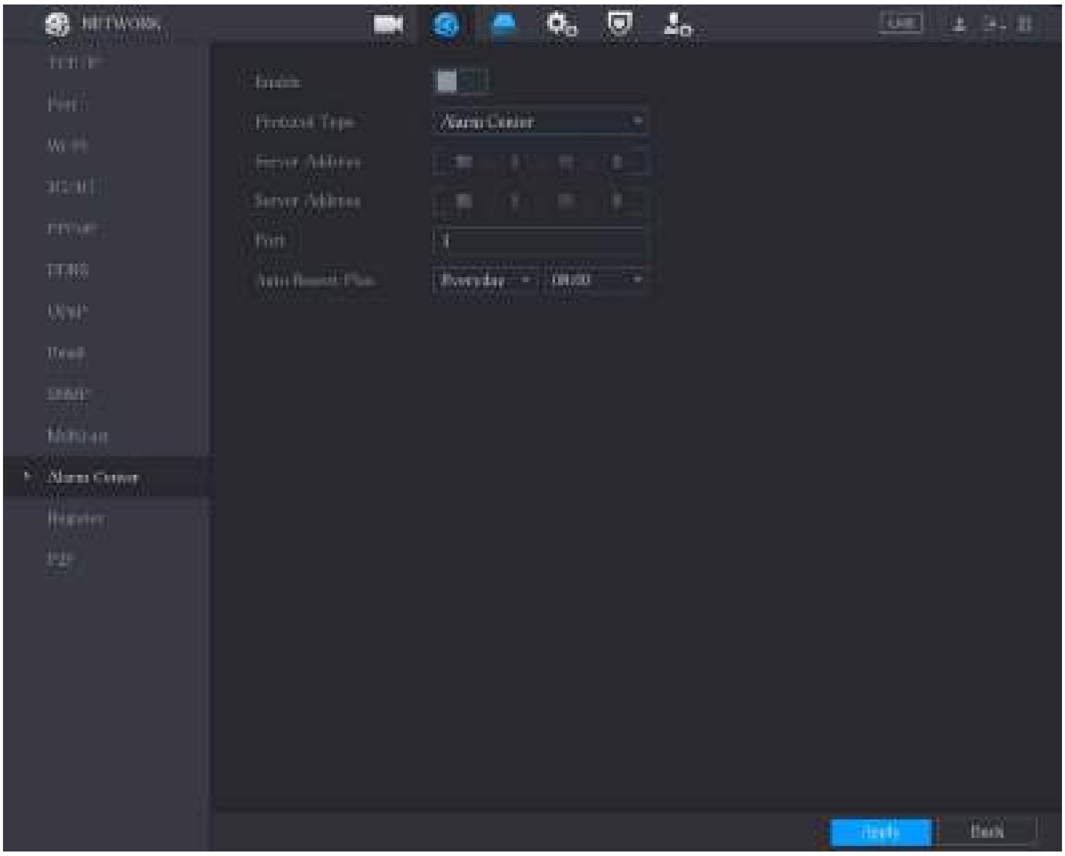
Step 3 Click **Apply** to complete the settings.

5.15.1.12 Configuring Alarm Center Settings

You can configure the alarm center server to receive the uploaded alarm information. To use this function, the **Report Alarm** checkbox must be selected. For details about alarm event settings, see "5.10 Alarm Events Settings."

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

Figure 5-281 Alarm center



Enable

Protocol Type: Alarm Center

Server Address

Server Address

Port

Auto Report Plan: Everyday 08:00

Step 2 Configure the settings for the alarm center parameters.

Table 5-57 Alarm center parameters

Parameter	Description
Enable	Enable the alarm center function.
Protocol Type	In the **Protocol Type** list, select protocol type. The default is **ALARM CENTER**.
Server Address	The IP address and communication port of the PC installed with alarm client.
Port	
Auto Report Plan	In the Auto Report Plan list, select time cycle and specific time for uploading alarm.

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

5.15.1.13 Configuring P2P Settings

You can manage the devices by using P2P technology to download the application and register the devices. For details, see "5.1.4.5 Configuring P2P Settings."

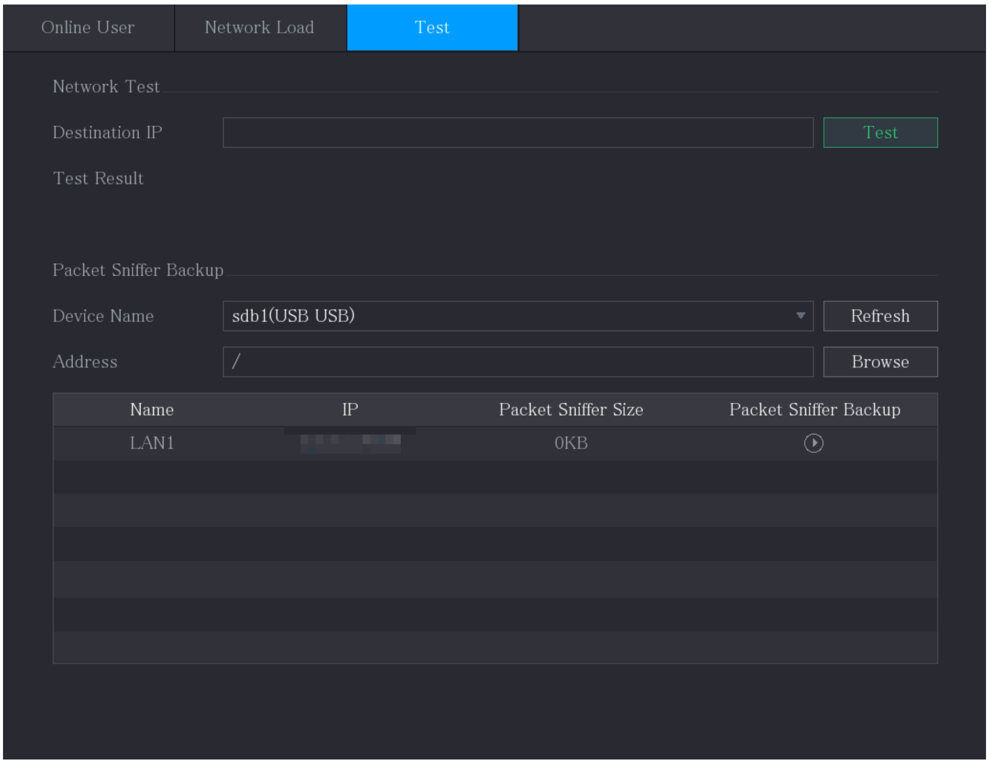
5.15.2 Configuring Network Testing Settings

5.15.2.1 Testing the Network

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

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

Figure 5-282 Network test



Network Test

Destination IP

Test Result

Packet Sniffer Backup

Device Name: sdb1(USB USB)

Address: /

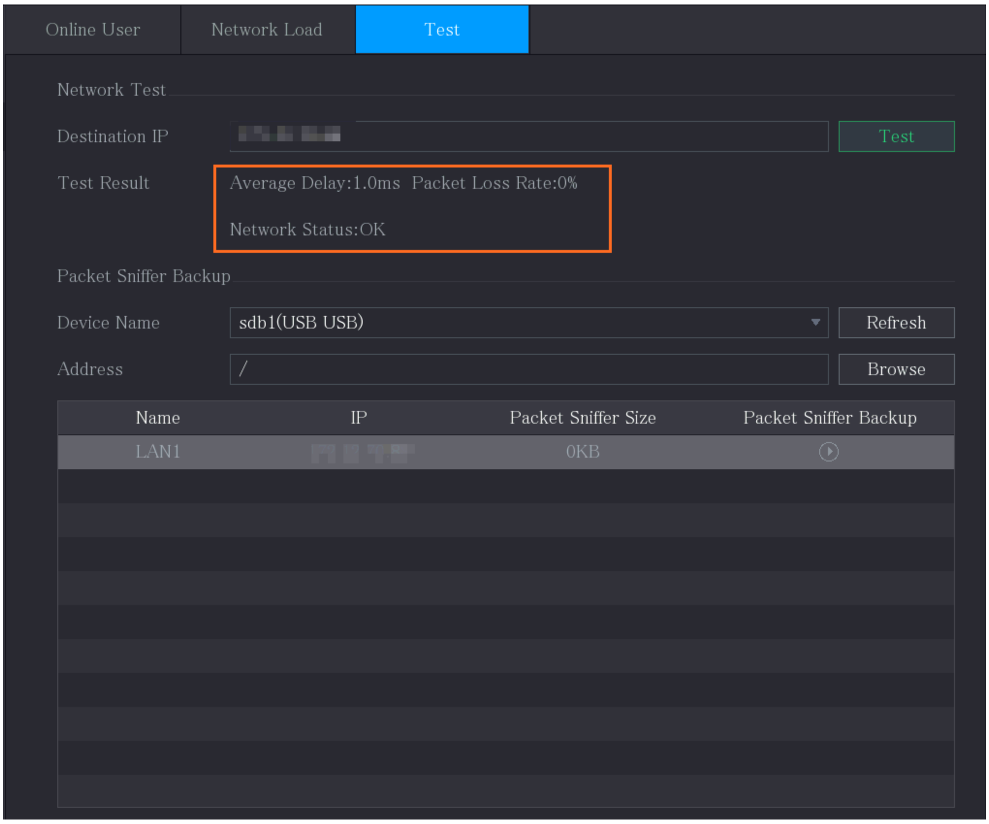
Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	[redacted]	0KB	▶

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.

Figure 5-283 Test result



Network Test

Destination IP [redacted] Test

Test Result: Average Delay:1.0ms Packet Loss Rate:0%

Network Status:OK

Packet Sniffer Backup

Device Name: sdb1(USB USB) Refresh

Address: / Browse

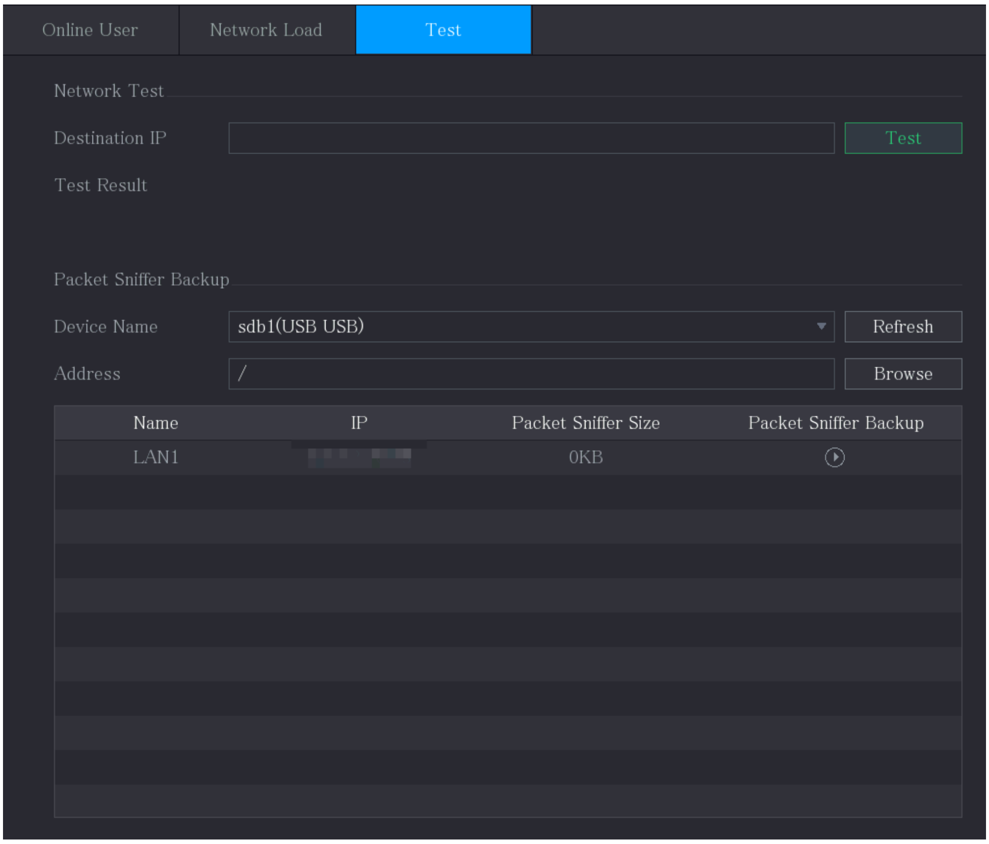
Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	[redacted]	0KB	▷

5.15.2.2 Capturing Packet and Backing up

Packet capture means the operations such as capturing, resending, and editing data that are sent and received during network transmission. When there is network abnormality, you can perform packet capturing and back up into the USB storage device. This date can be provided to the technical support for analyzing the network condition.

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

Figure 5-284 Test



Online User | Network Load | Test

Network Test

Destination IP:

Test Result

Packet Sniffer Backup

Device Name: sdb1(USB USB) — Refresh

Address: / — Browse

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

Step 2 Connect a USB storage device to the Device.

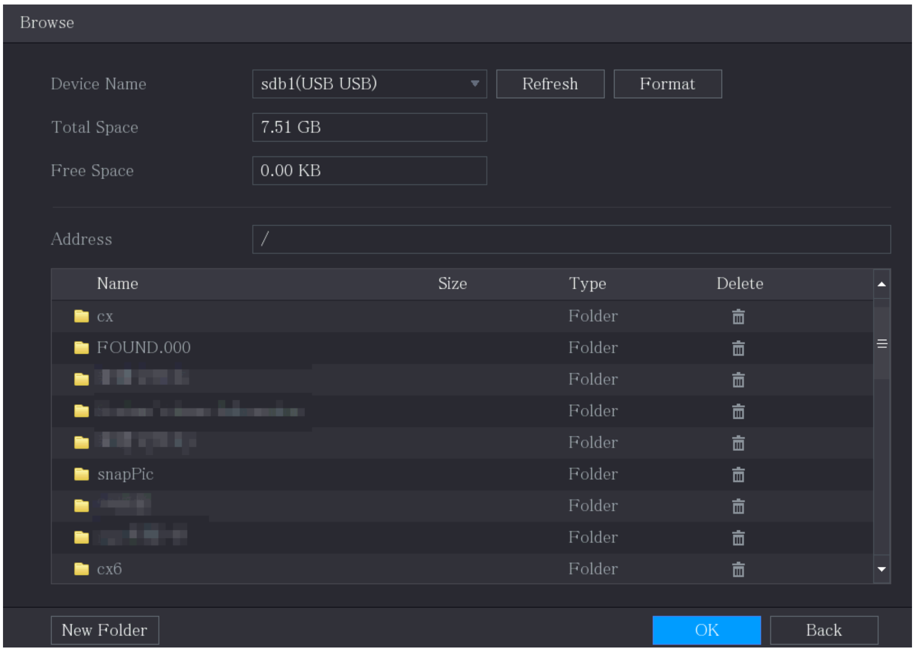
Step 3 Click **Refresh**.

The Device starts detecting the USB storage device and displays its name in the **Device Name** box.

Step 4 Select the route of the data that you want to capture and back up.

1) In the **Packet Sniffer Backup** area, click **Browse**.

Figure 5-285 Browse



Browse

Device Name: sdb1(USB USB) — Refresh — Format

Total Space: 7.51 GB

Free Space: 0.00 KB

Address: /

Name	Size	Type	Delete
cx		Folder	🗑
FOUND.000		Folder	🗑
[redacted]		Folder	🗑
[redacted]		Folder	🗑
[redacted]		Folder	🗑
snapPic		Folder	🗑
[redacted]		Folder	🗑
[redacted]		Folder	🗑
cx6		Folder	🗑

New Folder — OK — Back

2) Select the route.

- If several USB storage devices are connected to the Device, you can select from the **Device Name** list.
- Click Refresh to total space, free space and the file list in the selected USB storage device.
- In the case of insufficient capacity, click 🗑 to delete the needless files.
- Click **New Folder** to create a new folder in the USB storage device.

3) Click **OK** to save the route selection settings.

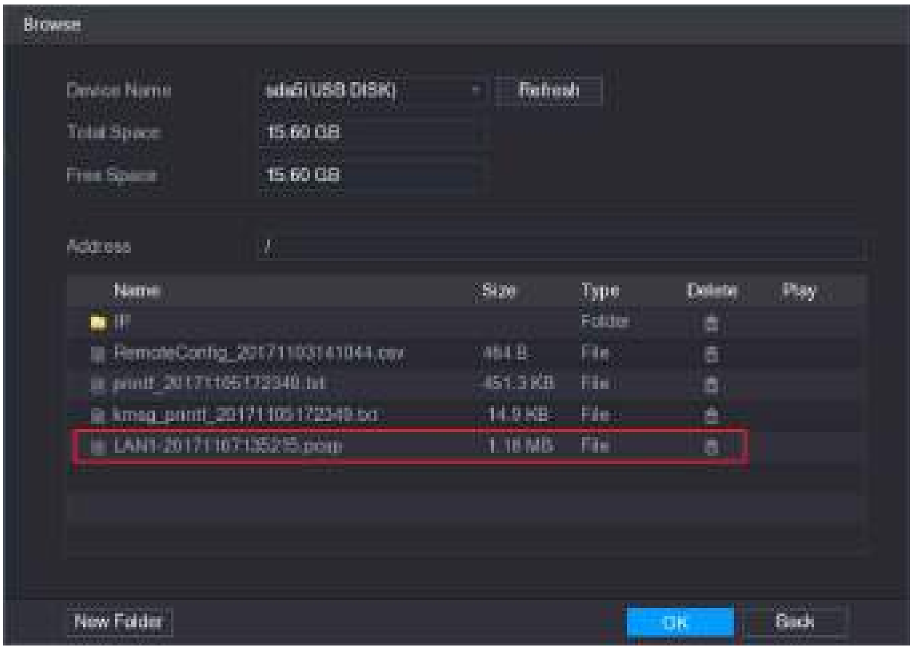
Step 5 Click ▶ to start packet capturing and backing up.

- Only the data packet of one LAN can be captured at one time.
- After capturing starts, you can exit the **Test** page to perform other operations such as web login and monitoring.

Step 6 Click ⏸ to stop capturing.

The backup data is saved in the selected route under the naming style "LAN name-time.pcap." You can open it by using Wireshark software.

Figure 5-286 Backup data



Browse

Device Name: sda5(USB DISK)

Total Space: 15.60 GB

Free Space: 15.60 GB

Address: /

Name	Size	Type	Delete	Play
IP		Folder	🗑	
RemoteConfig_20171103141044.csv	464 B	File	🗑	
printf_20171105172340.txt	451.3 KB	File	🗑	
kmsg_printf_20171105172349.txt	14.9 KB	File	🗑	
LAN1-20171107135215.pcap	1.18 MB	File	🗑	

5.16 Configuring Account Settings

You can add, modify and delete user accounts, groups, and ONVIF users, and set security questions for admin account.

- The user name supports 31 characters and group name supports 15 characters. The user name can be consisted of letter, number, "_", "@", ".".

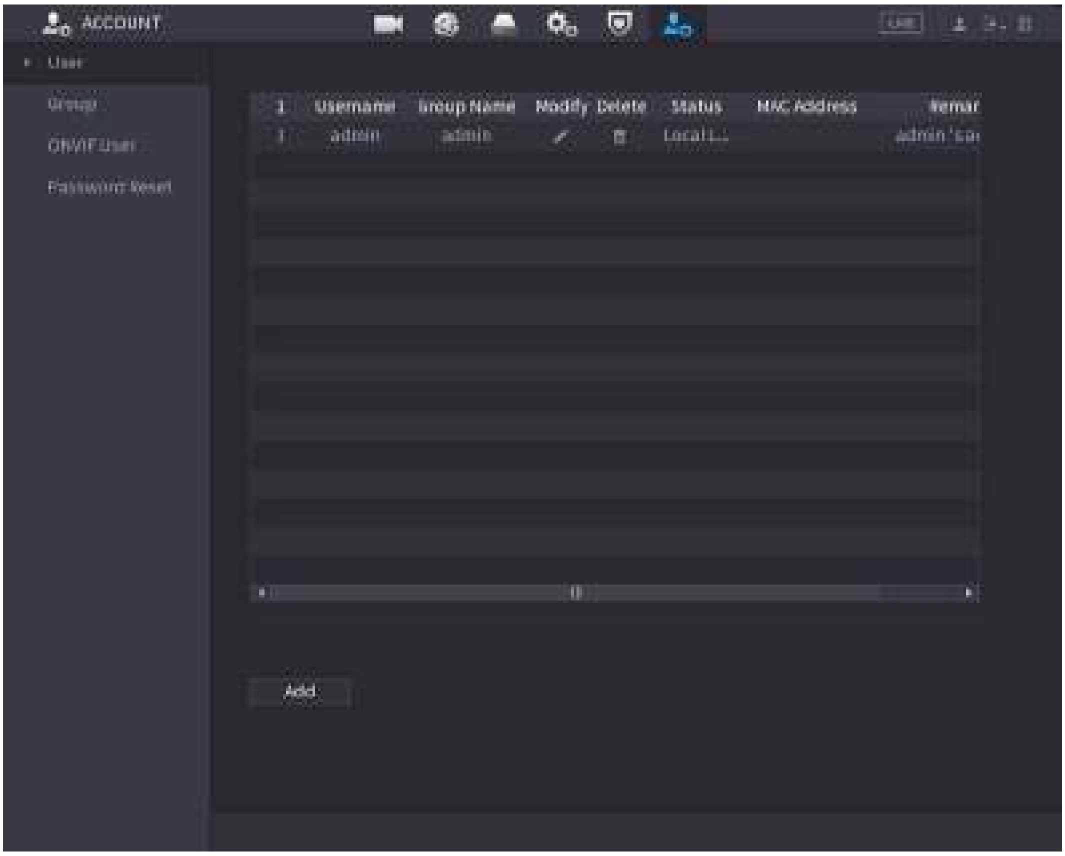
- You can set maximum 64 users and 20 groups. The group name by "User" and "Admin" cannot be deleted. You can set other groups and define the relevant permissions. However, the admin account cannot be set randomly.
- You can manage the account by user and group and the name cannot be repeated. Every user must belong to a group, and one user only belongs to one group.

5.16.1 Configuring User Account

5.16.1.1 Adding a User Account

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

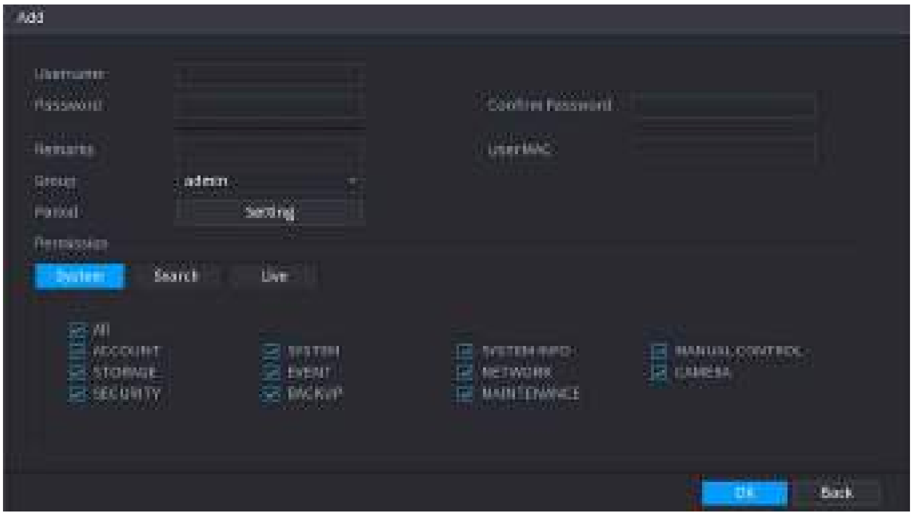
Figure 5-287 User



1	Username	Group Name	Modify	Delete	Status	MAC Address	Remar
1	admin	admin	✎	🗑	Local L...		admin 'sa

Step 2 Click **Add**.

Figure 5-288 Add user



Step 3 Configure the settings for the parameters of adding a user account.

Table 5-58 Parameters of adding user

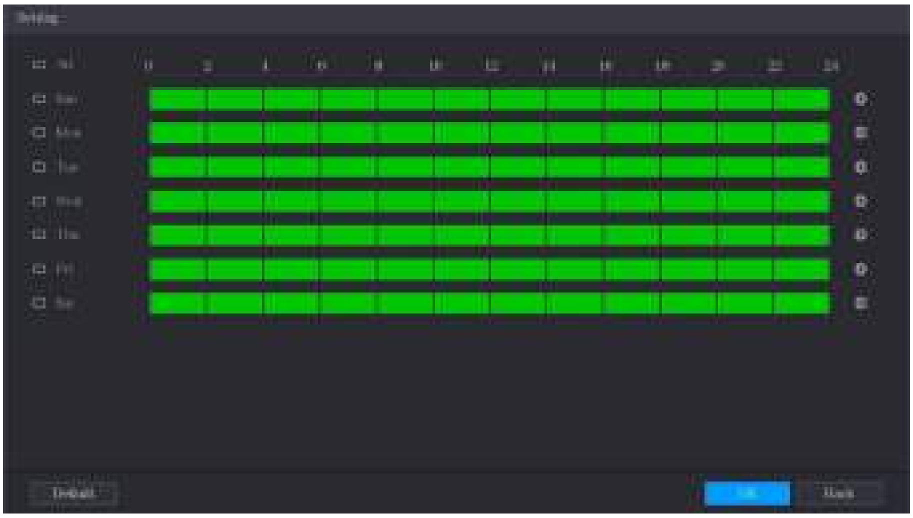
Parameter	Description
Username	Enter a user name and password for the account.
Password	
Confirm Password	Re-enter the password.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address
Group	Select a group for the account. 📖 The user rights must be within the group permission.
Period	Click **Setting** to display **Setting** page. Define a period during which the new account can log in to the device. The new account cannot log in to the device during the time beyond the set period.
Permission	In the **Permission** area, select the checkboxes in the **System** tab, **Playback** tab, and **Monitor** tab. 📖 To manage the user account easily, when defining the user account authority, it is recommended not to give the authority to the common user account higher that the advanced user account.

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

Setting Permitted Period

Step 1 Next to **Period**, click **Setting**.

Figure 5-289 Setting

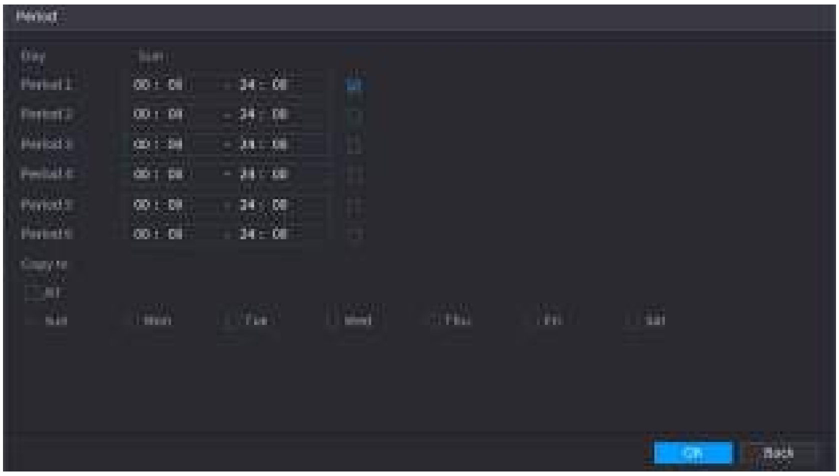


Step 2 Define the permitted period. By default, it is active all the time.

- Define the period by drawing.
  - ◇ Define for a specified day of a week: On the timeline, click the half-hour blocks to select the active period.
  - ◇ Define for several days of a week: Click □ before each day, the icon switches to 🔗. On the timeline of any selected day, click the half-hour blocks to select the active periods, all the days with 🔗 will take the same settings.
  - ◇ Define for all days of a week: Click **All**, all the □ switches to 🔗. On the timeline of any day, click the half-hour blocks to select the active periods, all the days will take the same settings.
- Define the period by editing. Take Sunday as an example.

1) Click ⚙.

Figure 5-290 Period



2) Enter the time frame for the period and select the checkbox to enable the settings.

◇ There are six periods for you to set for each day.

◇ Under **Copy**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.

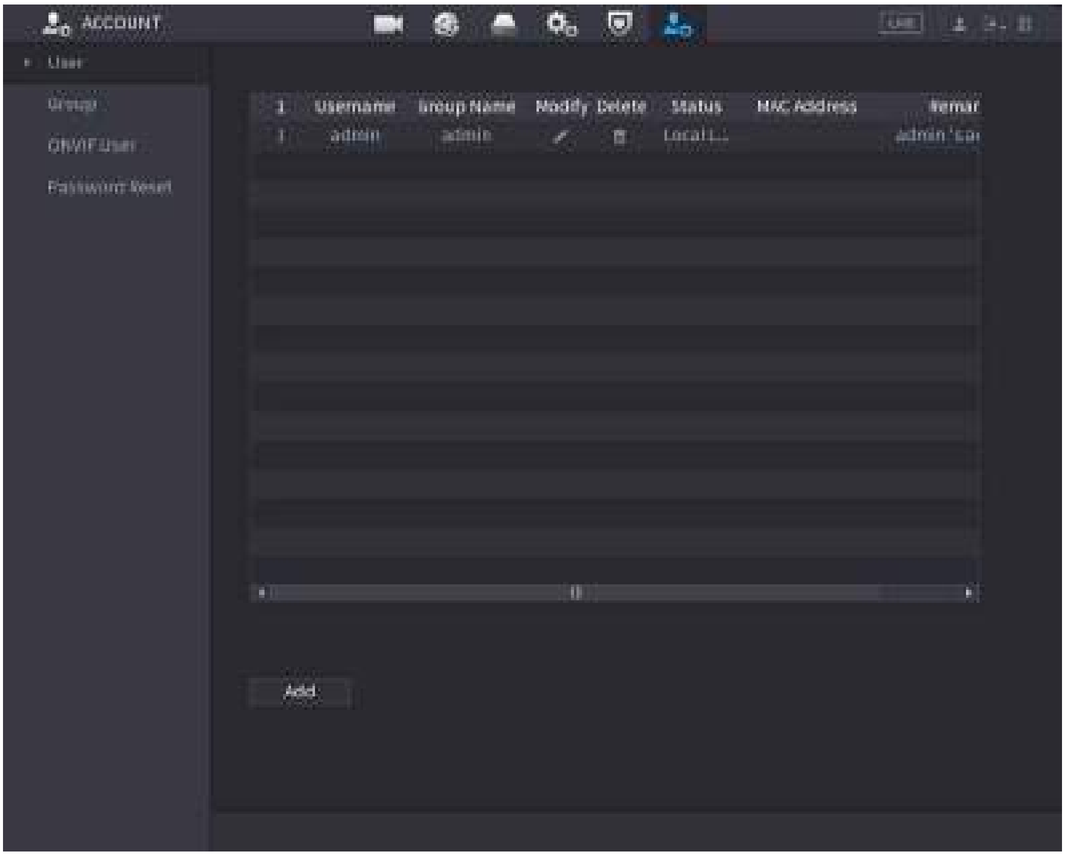
3) Click **OK** to save the settings.

Step 3 Click **OK**.

5.16.1.2 Modify a User Account

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

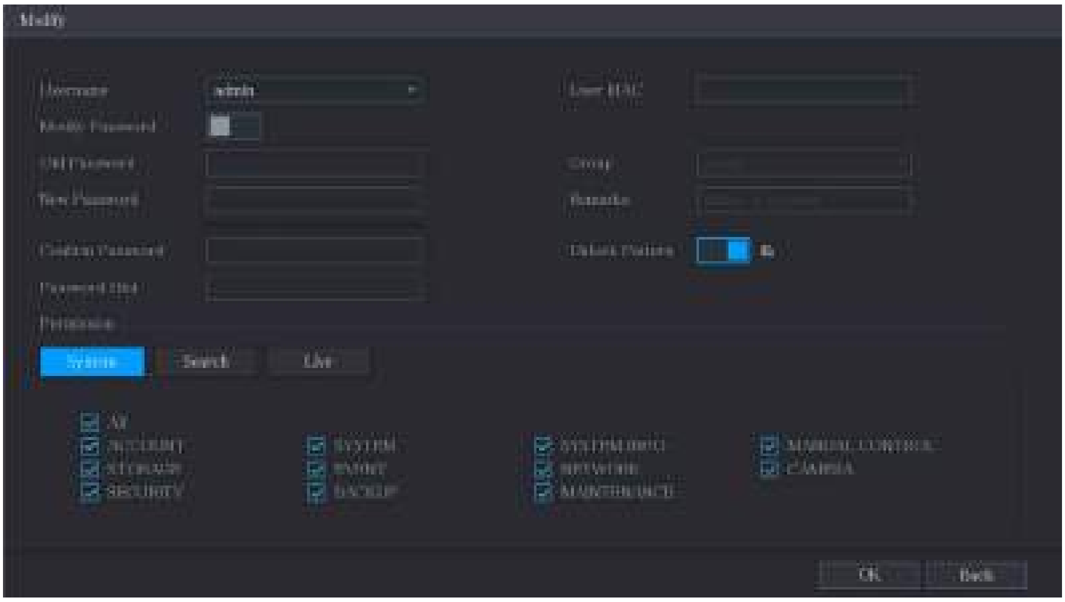
Figure 5-291 User



1	Username	Group Name	Modify	Delete	Status	MAC Address	Remar
1	admin	admin	✎	🗑	Local L...		admin 'sa

Step 2 Click ✎ for the user account that you want to modify.

Figure 5-292 Modify



Modify

Username: admin

Modify Password: □

Old Password

New Password

Confirm Password

Password Hint

User MAC

Group

Remarks

Unlock Pattern

Permission

☑ ALL

☑ ACCOUNT ☑ SYSTEM ☑ SYSTEM INFO ☑ MANUAL CONTROL

☑ STORAGE ☑ EVENT ☑ NETWORK ☑ CAMERA

☑ SECURITY ☑ BACKUP ☑ MAINTENANCE

Step 3 Change the settings for password, user name, user group, user MAC, memo, period, and authority.

The new password can be set from 8 digits through 32 digits and contains at least two types from number, letter and special characters (excluding"'", """, ";", ":" and "&").

For the admin account, you enable/disable the unlock pattern and modify password hint.

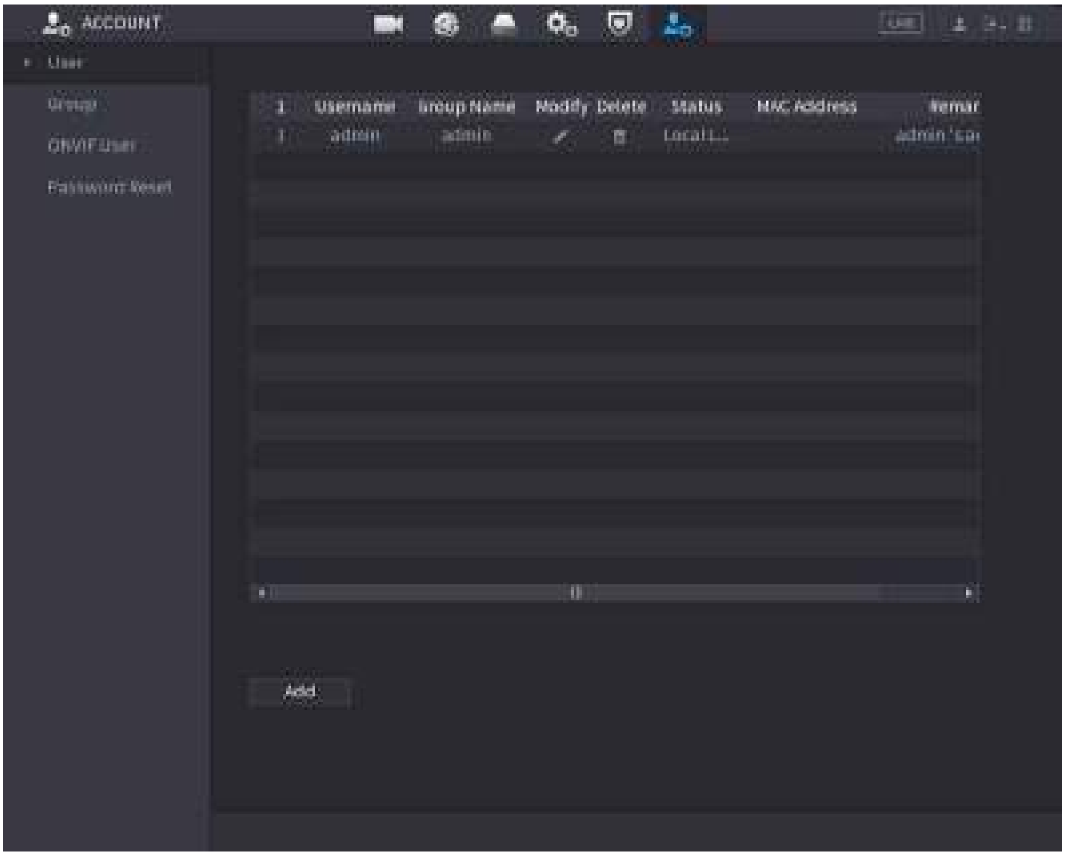
- To use the unlock pattern, enable **Unlock Pattern**, click ▣, draw a pattern in the **Unlock Pattern** page, and then click **Save** to save the setting.
- Enter password hint text in **Password Hint** box.

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

5.16.1.3 Deleting a User Account

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

Figure 5-293 User



1	Username	Group Name	Modify	Delete	Status	MAC Address	Remar
1	admin	admin	✎	🗑	Local L...		admin 'ca

Step 2 Click 🗑 for the user account that you want to delete.

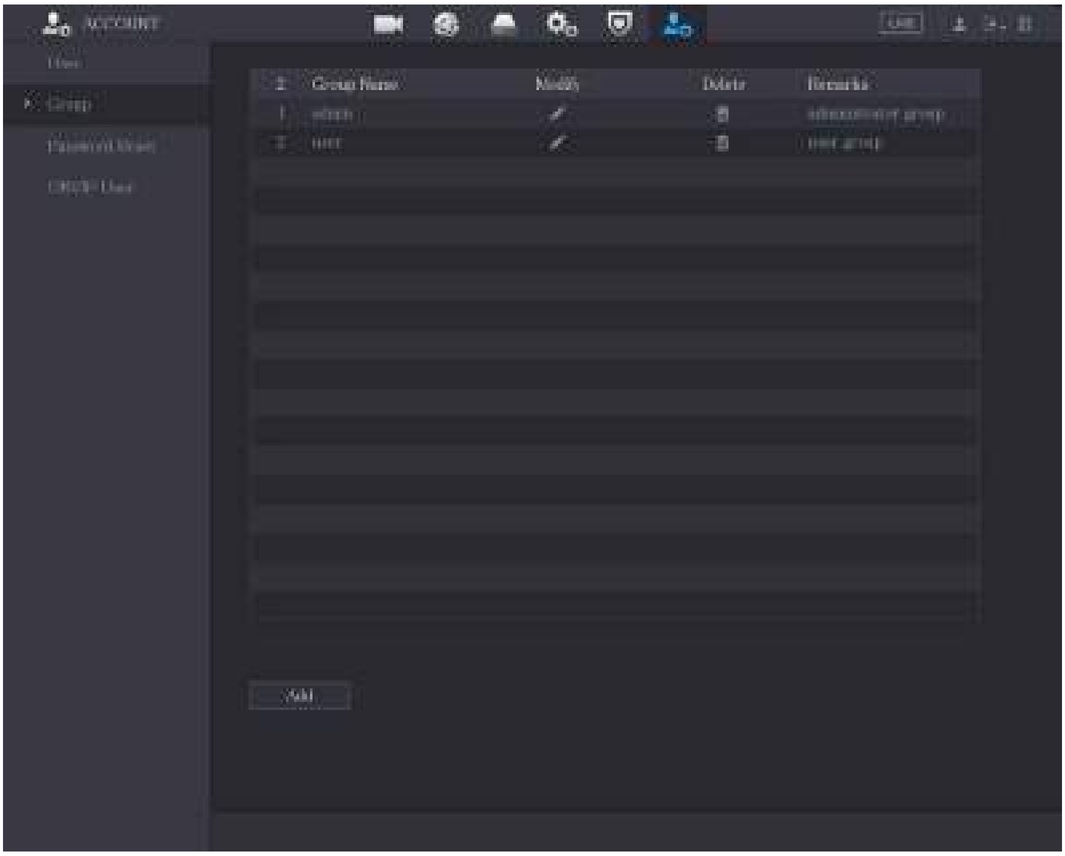
Step 3 Click **OK** to delete a user account.

5.16.2 Configuring Group Account

5.16.2.1 Adding a Group

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

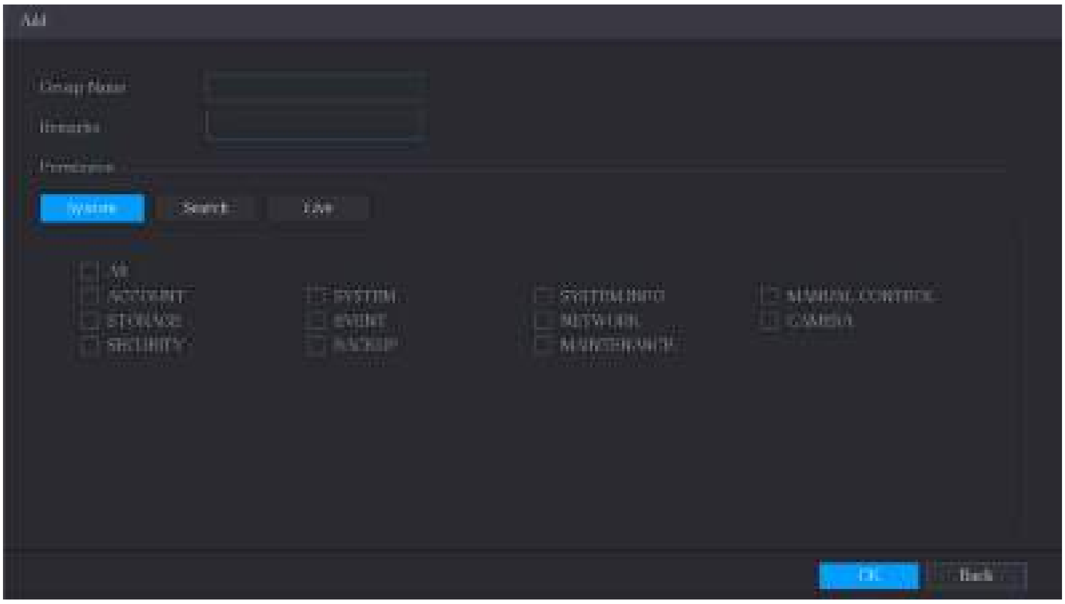
Figure 5-294 Group



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

Step 2 Click **Add**.

Figure 5-295 Add group



Step 3 Configure the settings for the parameters of adding a group.

Table 5-59 Parameters of adding a group

Parameter	Description
Group Name	Enter a name for the group.
Remarks	Optional. Enter a description of the account.

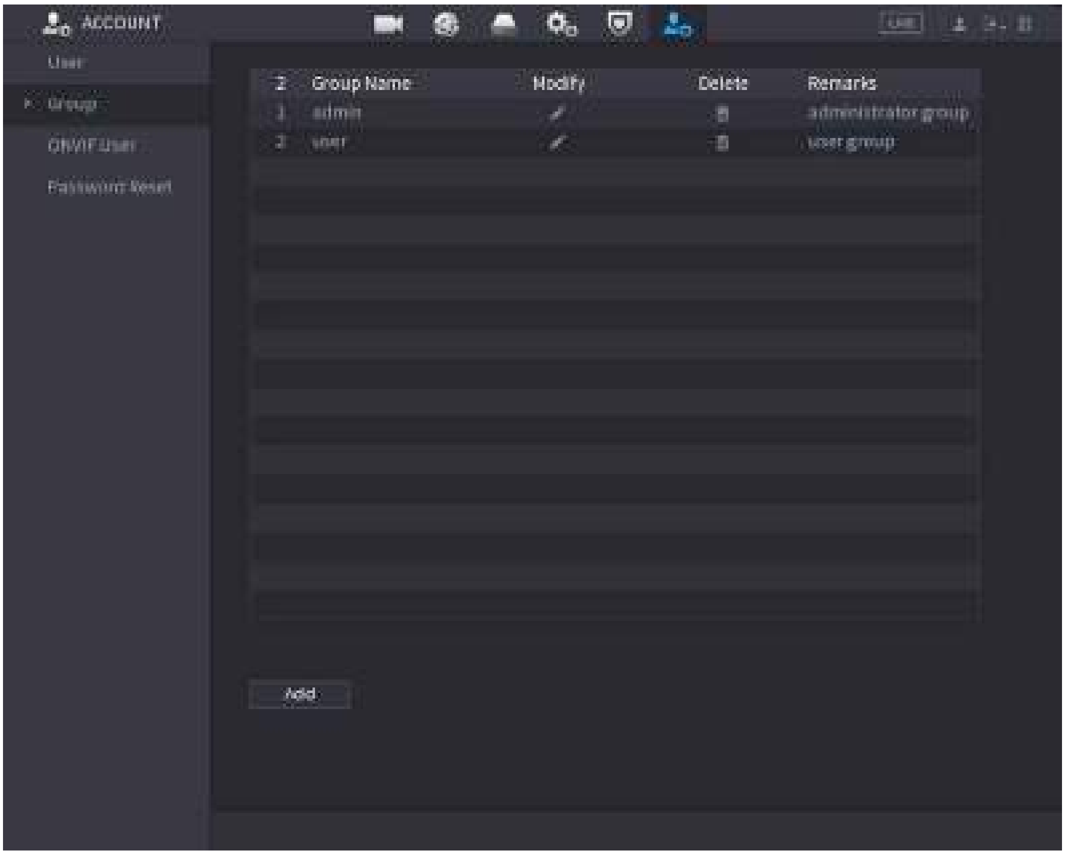
Parameter	Description
Permission	In the **Permission** area, select the checkboxes in the **System** tab, **Playback** tab, and **Monitor** tab.

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

5.16.2.2 Modifying a Group

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

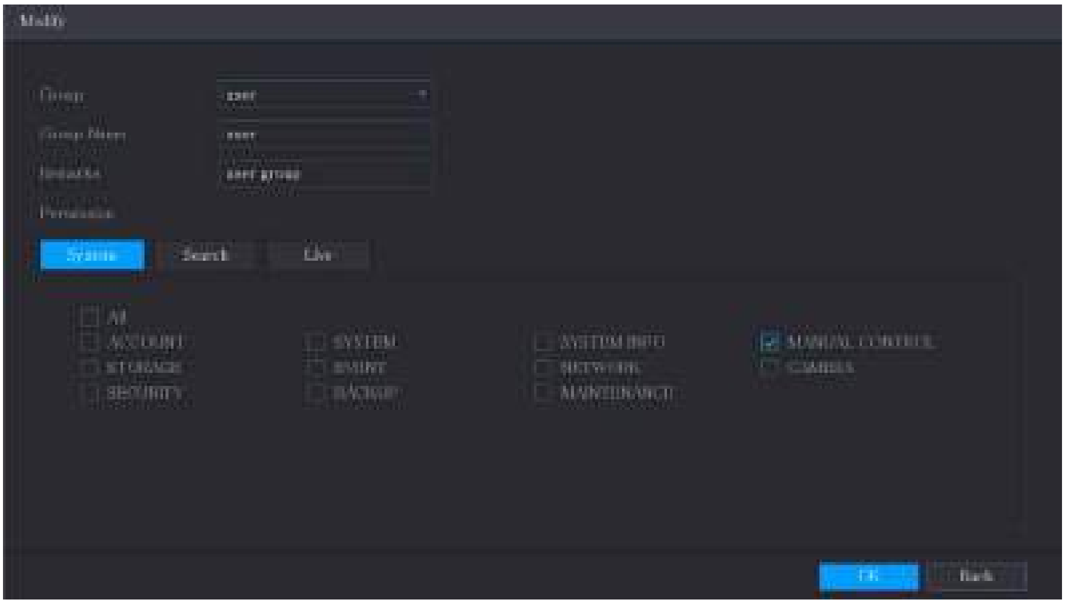
Figure 5-296 Group



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

Step 2 Click ✎ for the group account that you want to modify.

Figure 5-297 Modify



Group: user

Group Name: user

Remarks: user group

Permission

□ All

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

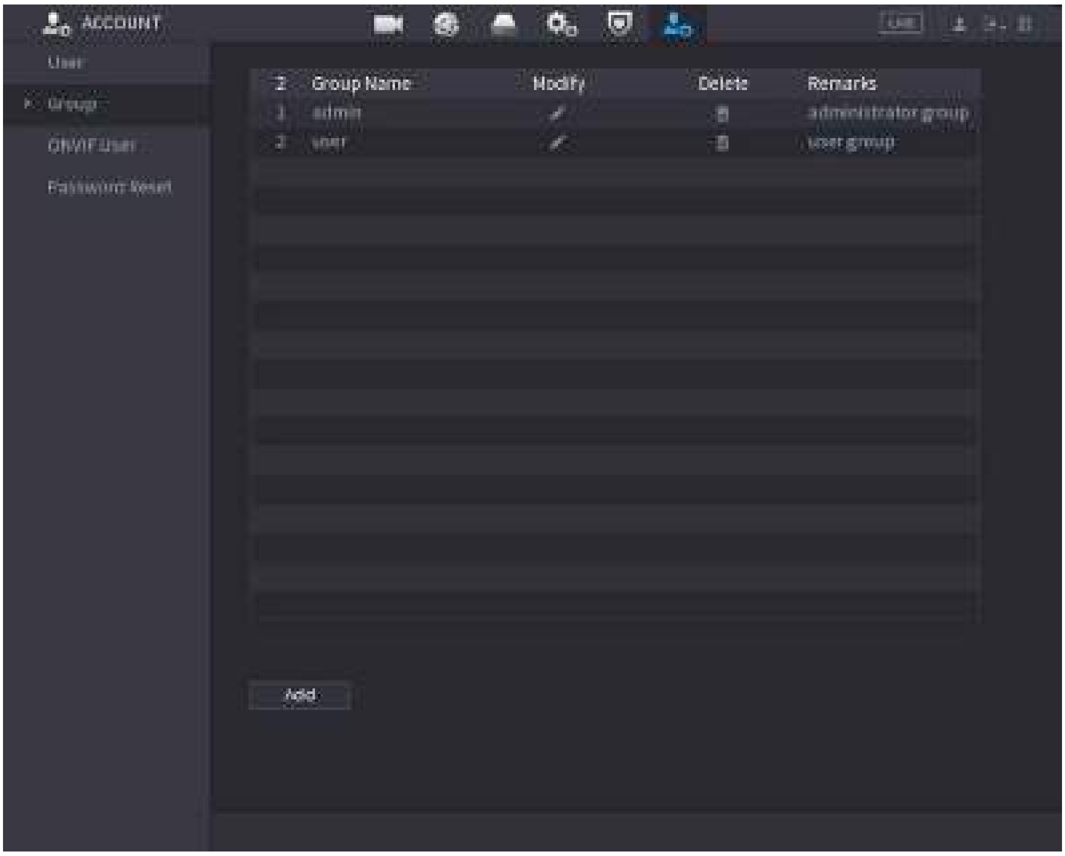
Step 3 Change the settings for group name, memo, and authority.

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

5.16.2.3 Deleting a Group

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

Figure 5-298 Group



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

Step 2 Click 🗑 for the user account that you want to delete.

Step 3 Click **OK** to delete a group.

5.16.3 Configuring ONVIF Users

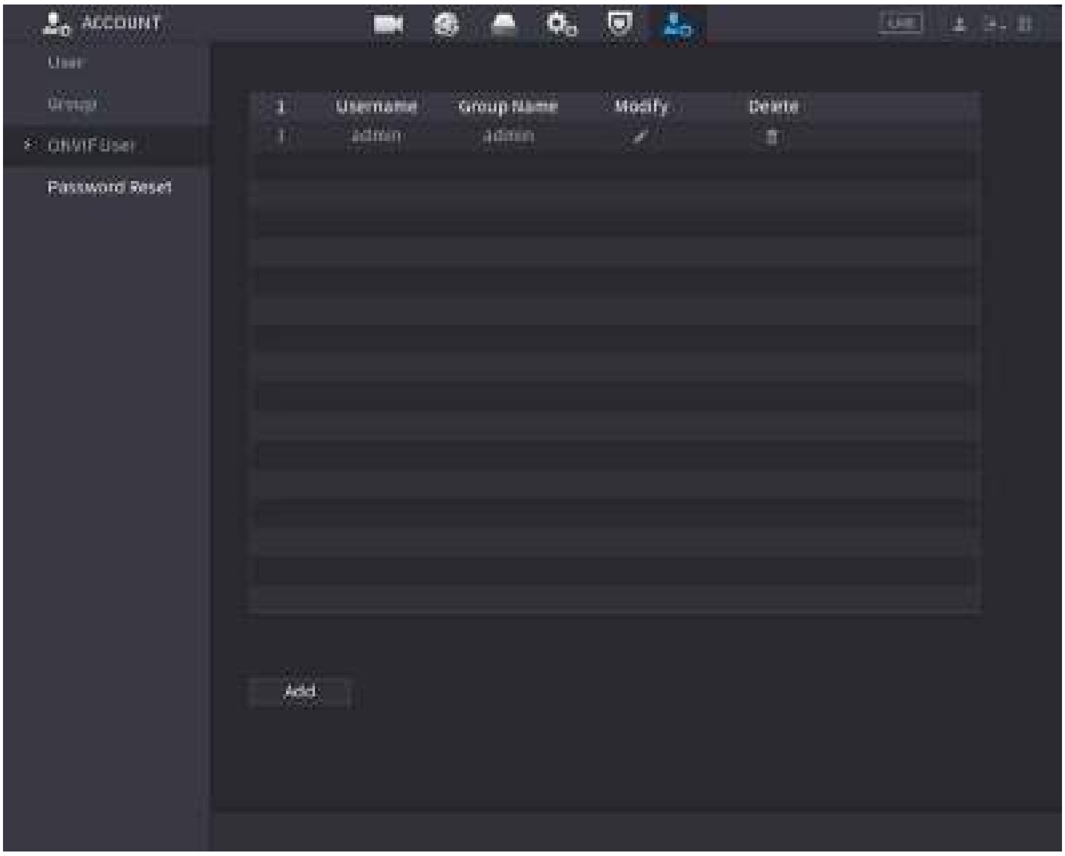
The device manufactured by other company can connect to the Device through ONVIF protocol by an authorized ONVIF account.

📖

The admin account is created for ONVIF users right after the Device has been initialized

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

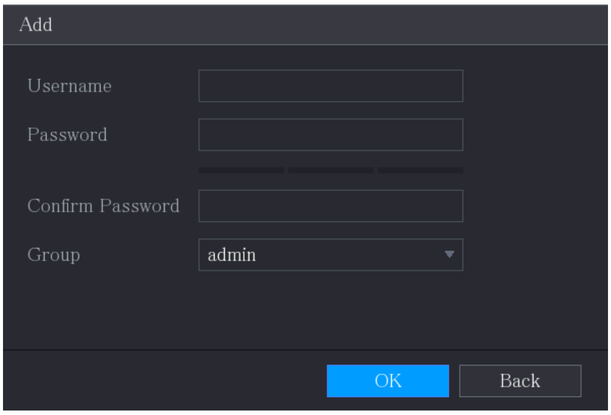
Figure 5-299 ONVIF user



1	Username	Group Name	Modify	Delete
1	admin	admin	✎	🗑

Step 2 Click **Add**.

Figure 5-300 Add ONVIF user



Username	
Password	
Confirm Password	
Group	admin

Step 3 Enter user name, password, and select the group that you want this account to belong to.

Step 4 Click **OK** to save the settings.

Click ✎ to modify the account; Click 🗑 to delete the account.

5.17 Audio Management

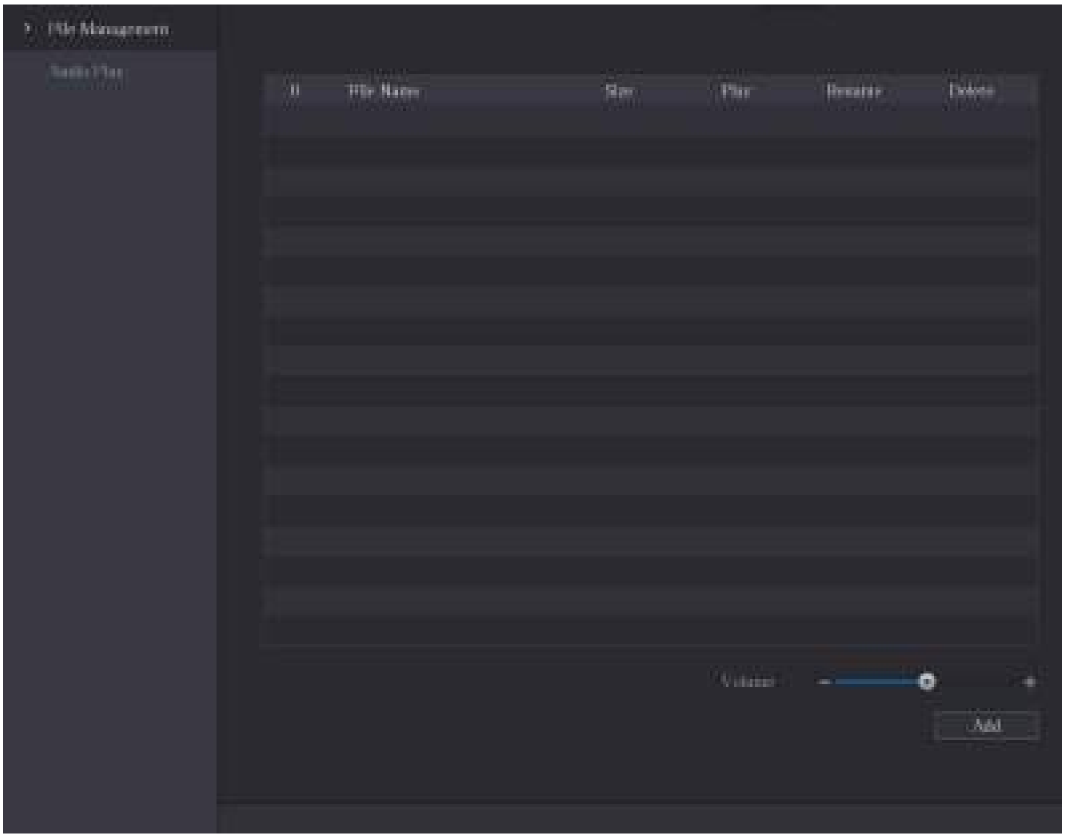
Audio management function manages audio files and configures the playing schedule. When there is an alarm event, the audio file can be activated.

5.17.1 Configuring Audio Files

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

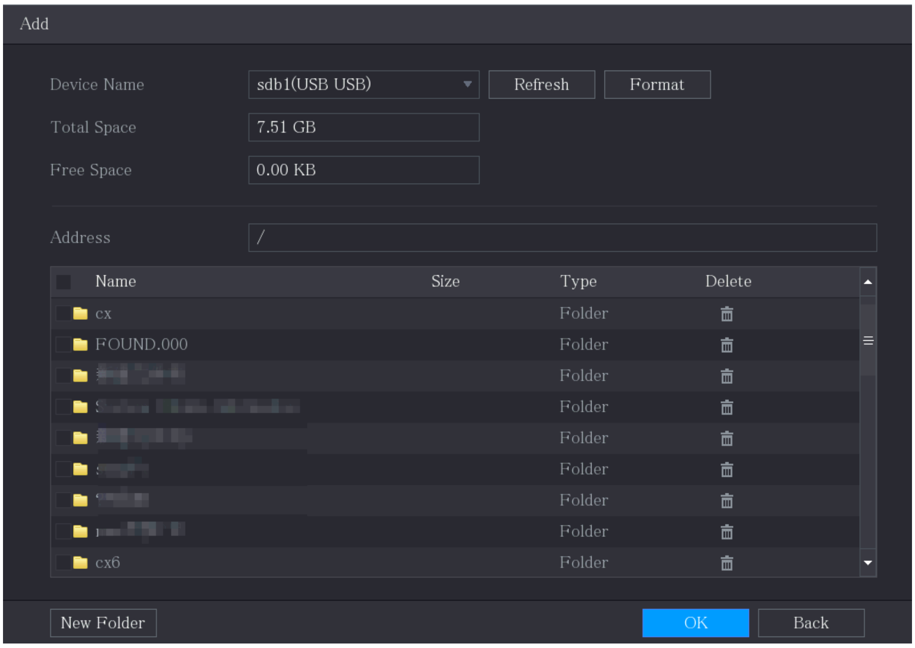
Step 1 Select **Main Menu** > **AUDIO** > **File Management**.

Figure 5-301 File management



Step 2 Click **Add**.

Figure 5-302 Add file



Add

Device Name: sdb1(USB USB) | Refresh | Format

Total Space: 7.51 GB

Free Space: 0.00 KB

Address: /

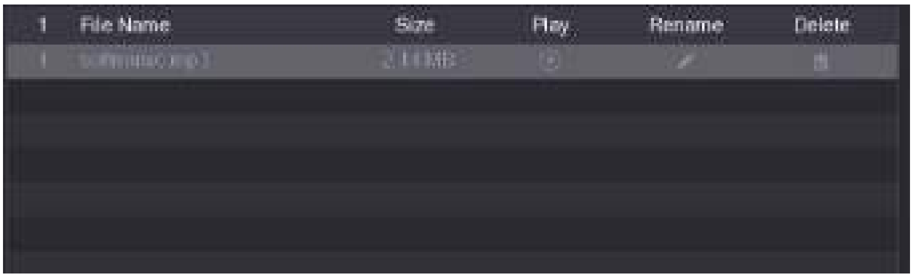
□	Name	Size	Type	Delete
□	cx		Folder	🗑
□	FOUND.000		Folder	🗑
□	[redacted]		Folder	🗑
□	[redacted]		Folder	🗑
□	[redacted]		Folder	🗑
□	[redacted]		Folder	🗑
□	[redacted]		Folder	🗑
□	[redacted]		Folder	🗑
□	cx6		Folder	🗑

Step 3 Select the audio files that you want to import.

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.

Figure 5-303 Imported file



1	File Name	Size	Play	Rename	Delete
1	[illegible]	[illegible]	○	✎	🗑

The imported audio files are automatically saved into the HDD, so you do not need to connect to the USB storage device to get the file next time.

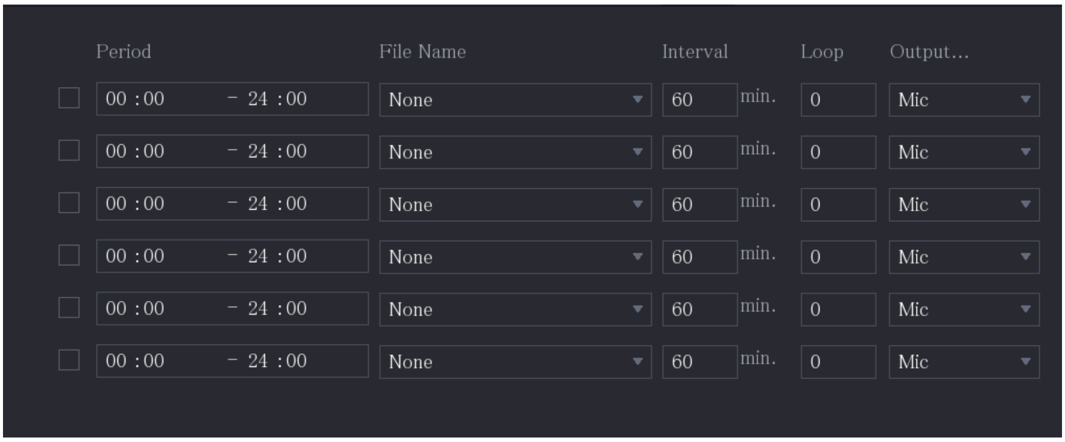
- Click ▶ to play the audio file.
- Click ✎ to rename the audio file.
- Click 🗑 to delete the audio file.
- To decrease or increase the playing volume, move the slider to the left or to the right.

5.17.2 Configuring Playing Schedule for Audio Files

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

Step 1 Select **Main Menu** > **AUDIO** > **Audio Play**.

Figure 5-304 Audio play



	Period	File Name	Interval		Loop	Output...
□	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 settings for the schedule parameters.

Figure 5-305 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.
Repeat	Configure how many times you want to repeat the playing in the defined period.
Output Port	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.

- The finish time for audio playing is decided by audio file size and the configured interval.
- Playing priority: Alarm event > Talkback > Trial listening > Audio file.

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

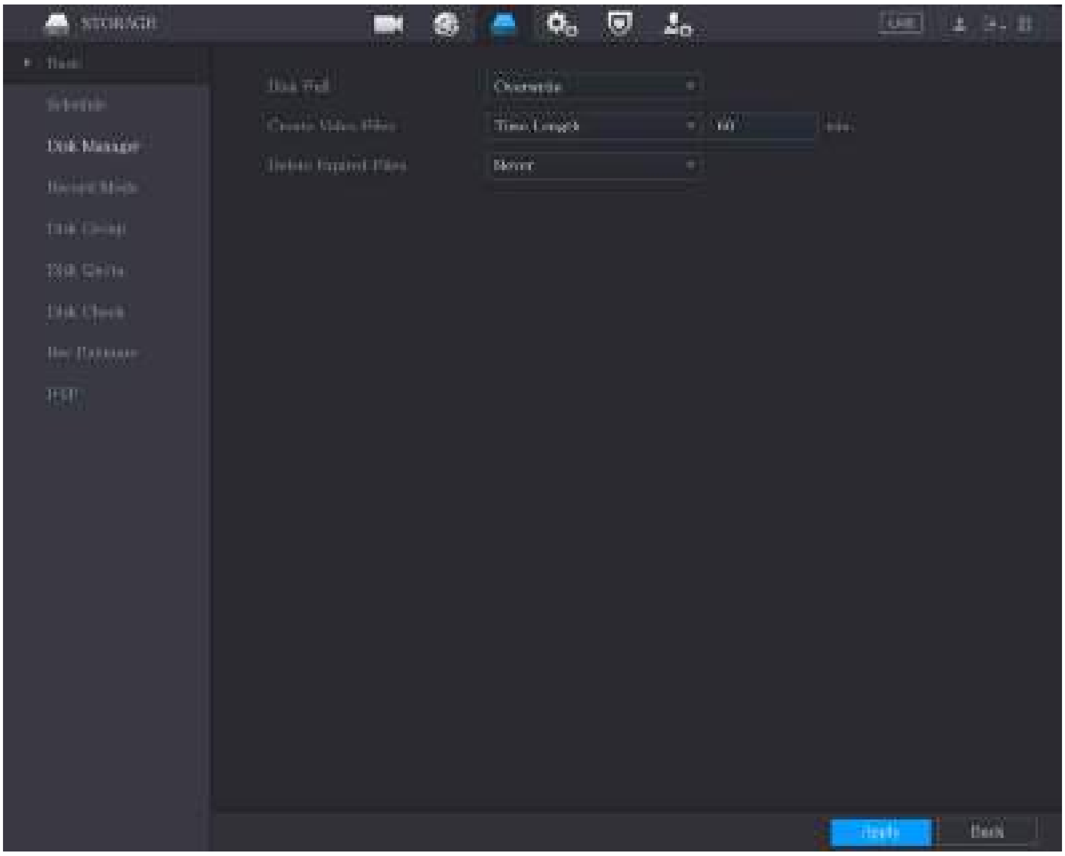
5.18 Storage Management

Storage management function manages the stored resources such as recorded video files and storage space. The function aims at providing easier operation and improving the storage efficiency.

5.18.1 Configuring Basic Settings

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

Figure 5-306 Basic



Disk Full: Overwrite

Create Video Files: Time Length 60 min.

Delete Expired Files: Never

Step 2 Configure the settings for the basic settings parameters.

Table 5-60 Basic settings parameters

Parameter	Description
Disk Full	Configure the settings for the situation all the read/write discs are full. ● Select **Stop** to stop recording ● Select **Overwrite** to overwrite the recorded video files always from the earliest time.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired Files	Configure whether to delete the old files and if yes, configure the days.

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

5.18.2 Configuring the Recording and Snapshot Schedule

The system starts recording and taking snapshot according to the configured schedule. For details, see "5.1.4.9 Configuring Recorded Video Storage Schedule" and "5.1.4.10 Configuring Snapshot Storage Schedule."

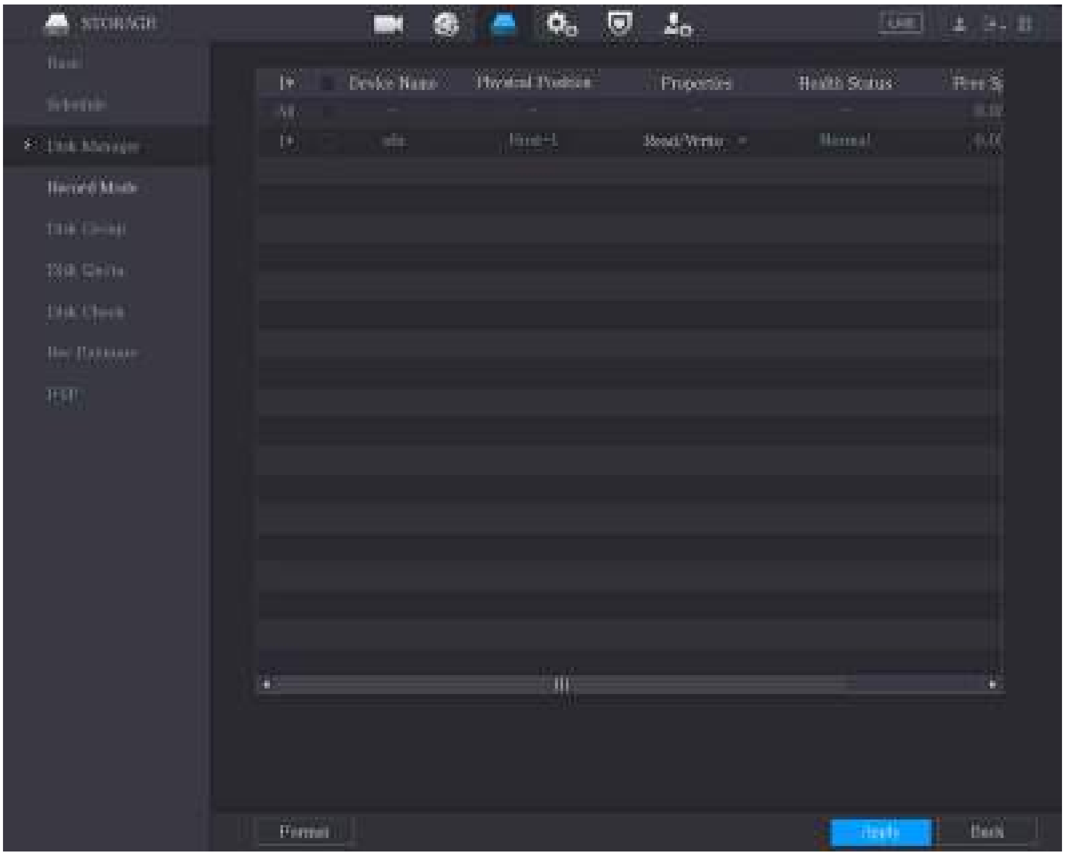
5.18.3 Configuring Disk Manager

You can view the HDD information, format HDD, and configure the HDD type through HDD manager.

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

In the table, you can view the information of current HDD, such as device name, HDD type, status, total space and free space, and serial number of the HDD port.

Figure 5-307 Disk manager

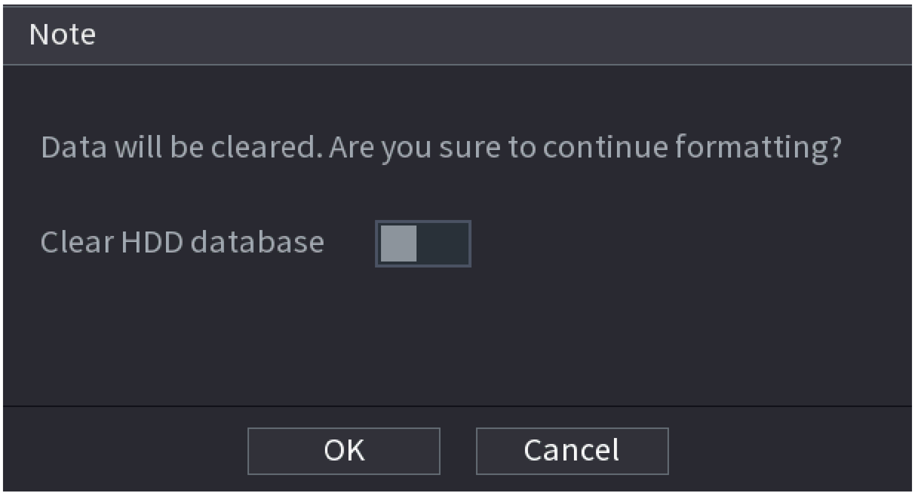


▾	□	Device Name	Physical Position	Properties	Health Status	Free S
All	□	--	--	--	--	[illegible]
1	--	sda	Host-1	Read/Write ▾	Normal	[illegible]

Step 2 Configuring the settings for the HDD manager.

- HDD type setting: In the **Properties** list, select **Read/Write**, **Read Only**, and then click **Apply** to save the settings.
- HDD format: Select the HDD that you want to format, click **Format**, and enable **Clear HDD database** in the pop-up message, click **OK** and enter the password of admin user in the prompted dialog box, click **OK** and then following the on-screen instructions to complete formatting.
- Formatting HDD will erase all data on the disk, proceed with caution.

Figure 5-308 Note



Note

Data will be cleared. Are you sure to continue formatting?

Clear HDD database

5.18.4 Configuring Record

Record type includes auto and manual record. You can configure record type of main stream and sub stream. See "5.7 Configuring Record Settings".

5.18.5 Configuring Advance Settings

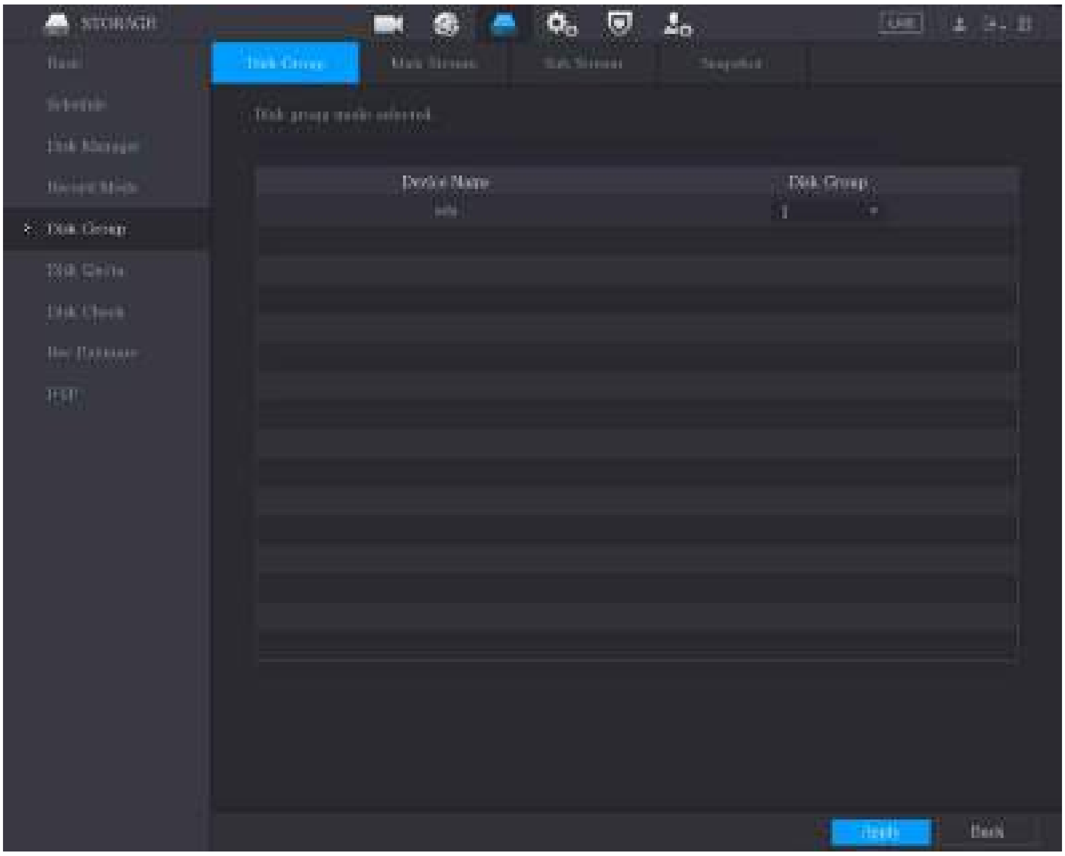
Create HDD group, and save main stream, sub stream and snapshot of designated channels to the HDD group.

⚠

- If the page displays that "Current HDD Mode is Quota Group", click "Change to HDD Group Mode", and then configure HDD group.
- You can enable either HDD Group Mode or Quota Group. The system prompts to reboot the device each time when you switch the mode.

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

Figure 5-309 Disk group



Disk group mode selected.

Device Name	Disk Group
[illegible]	1

Step 2 Select group for each HDD, and then click **Apply** to complete the settings.

Step 3 After configuring HDD group, click **Main Stream**, **Sub Stream** and **Snapshot** tabs respectively, to configure the saving of main stream, sub stream and snapshot information of different channels to different HDD groups.

Figure 5-310 Main stream

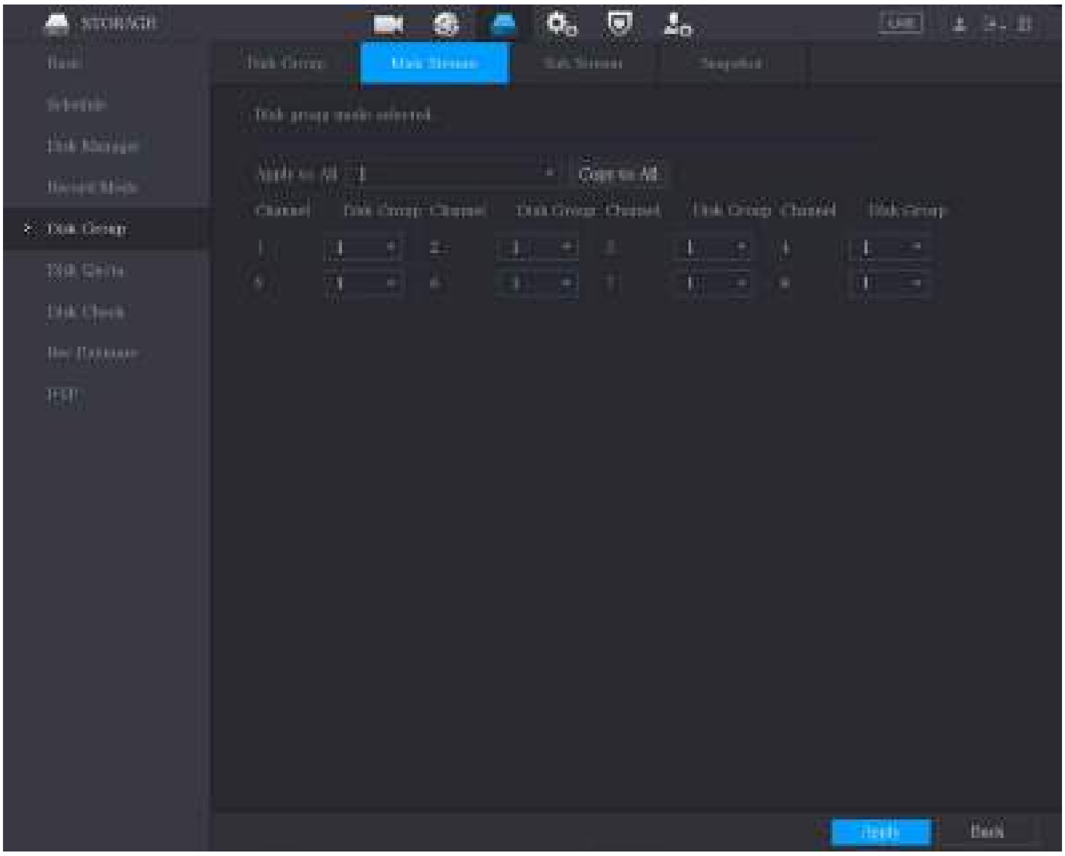


Figure 5-311 Sub stream

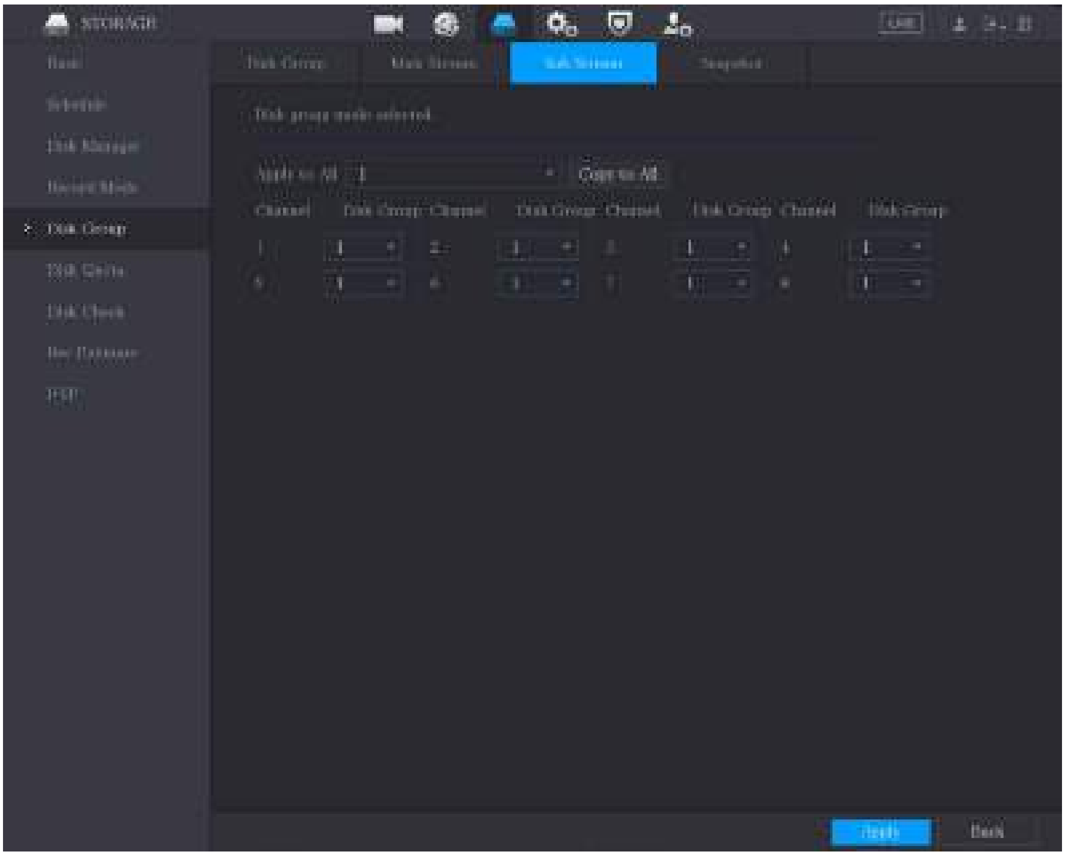
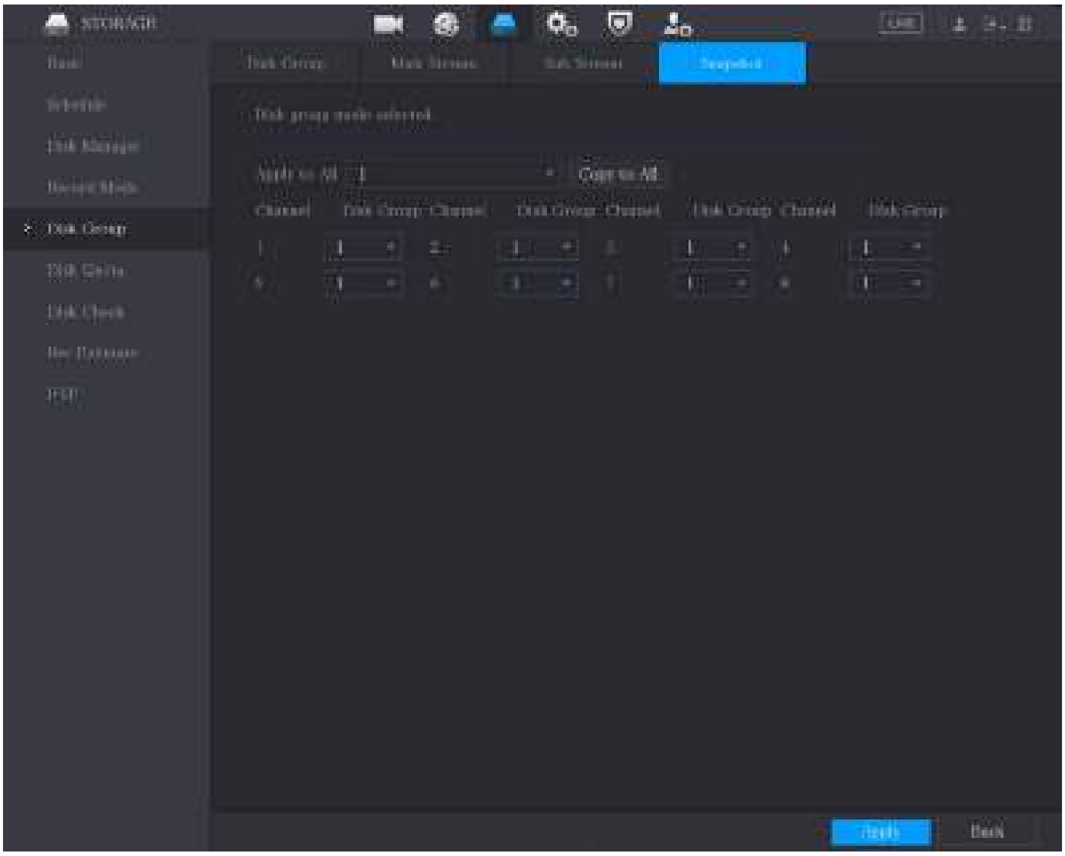


Figure 5-312 Snapshot



Disk group mode selected

Apply to All 1

Channel	Disk Group	Channel	Disk Group	Channel	Disk Group	Channel	Disk Group
1	1	2	1	3	1	4	1
5	1	6	1	7	1	8	1

Step 4 Click **Apply** to complete the settings.

5.18.6 Configuring Disk Quota

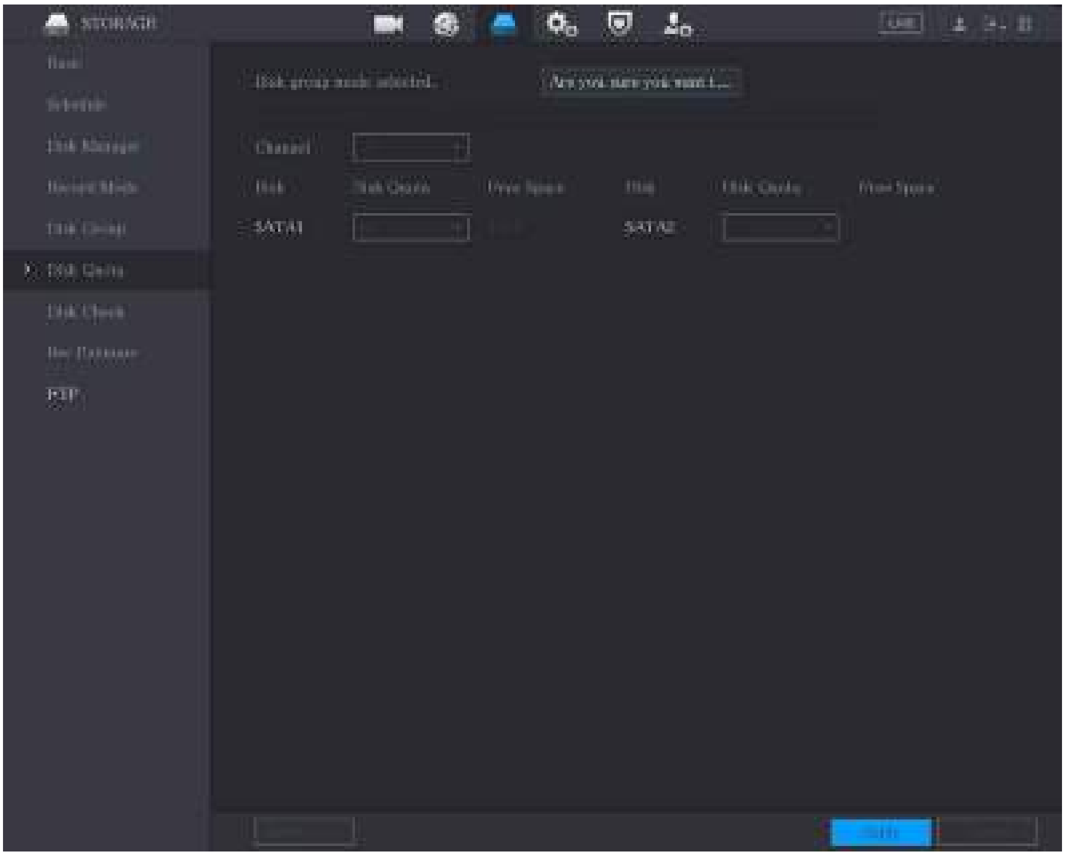
By configuring quota, allocate fixed storage capacity to each channel, and distribute the storage space of each channel reasonably.

⚠

- If the page displays that "Current HDD Mode is HDD Group", click "Change to Quota Mode", and then configure quota.
- You can enable either HDD Group Mode or Quota Group. The system prompts to reboot the device each time when you switch the mode.

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

Figure 5-313 Disk quota

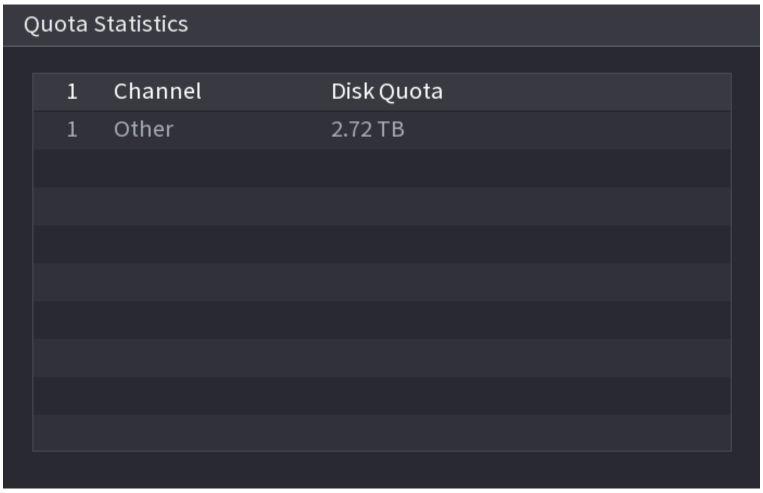


Step 2 Select the channels you want to configure, and select quota from the drop-down list of corresponding HDD.

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

Click **Quota Statistics** to view the quota of each channel in HDD.

Figure 5-314 Quota statistics



Quota Statistics

1	Channel	Disk Quota
1	Other	2.72 TB

5.18.7 Configuring HDD Detecting Settings

Not all models support this function.

HDD detecting function detects the current status of HDD to let you know the HDD performance and replace the defective HDD.

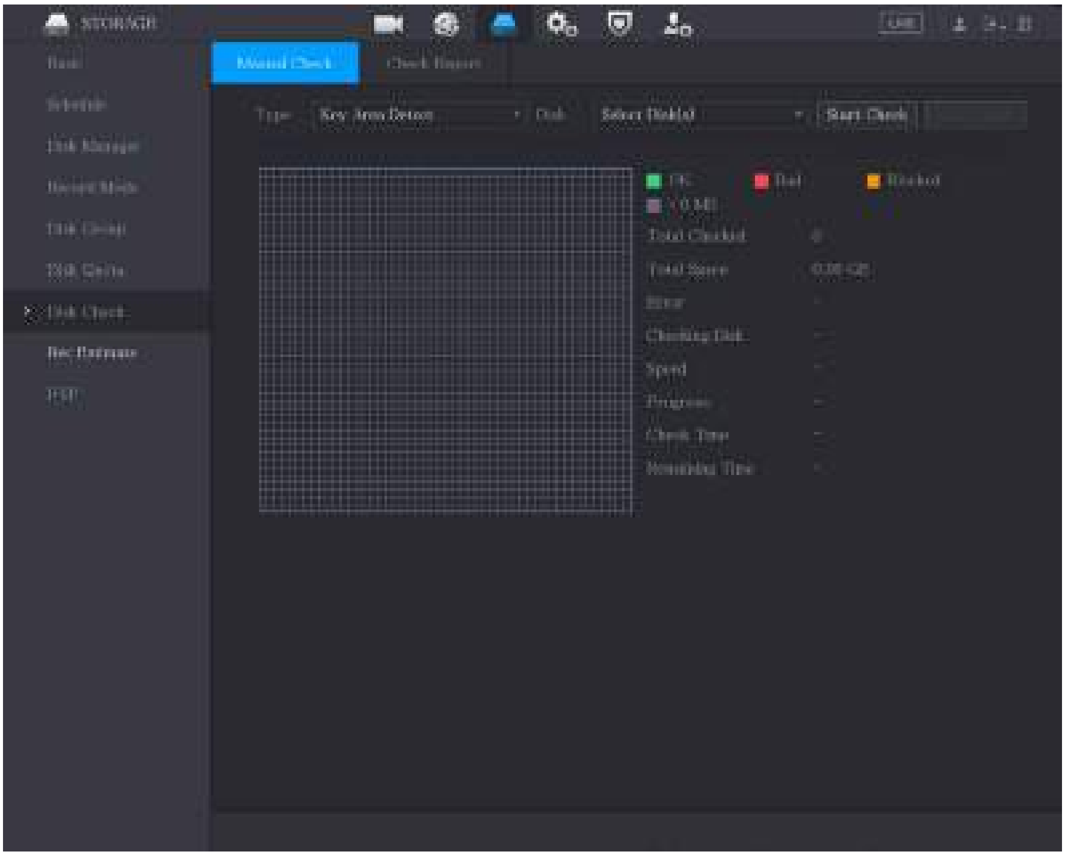
5.18.7.1 Checking HDD

You can detect HDD by key area detect and global detect.

- Key area detect: Detect the files saved in HDD. The detected bad track can be repaired by formatting. If there are no files in HDD, the system cannot detect the bad track.
- Global detect: Detect the whole HDD through Windows, which takes time and might affect the HDD that is recording the video.

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

Figure 5-315 Manual check



Type: Key Area Detect
Disk: Select Disk(s)

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

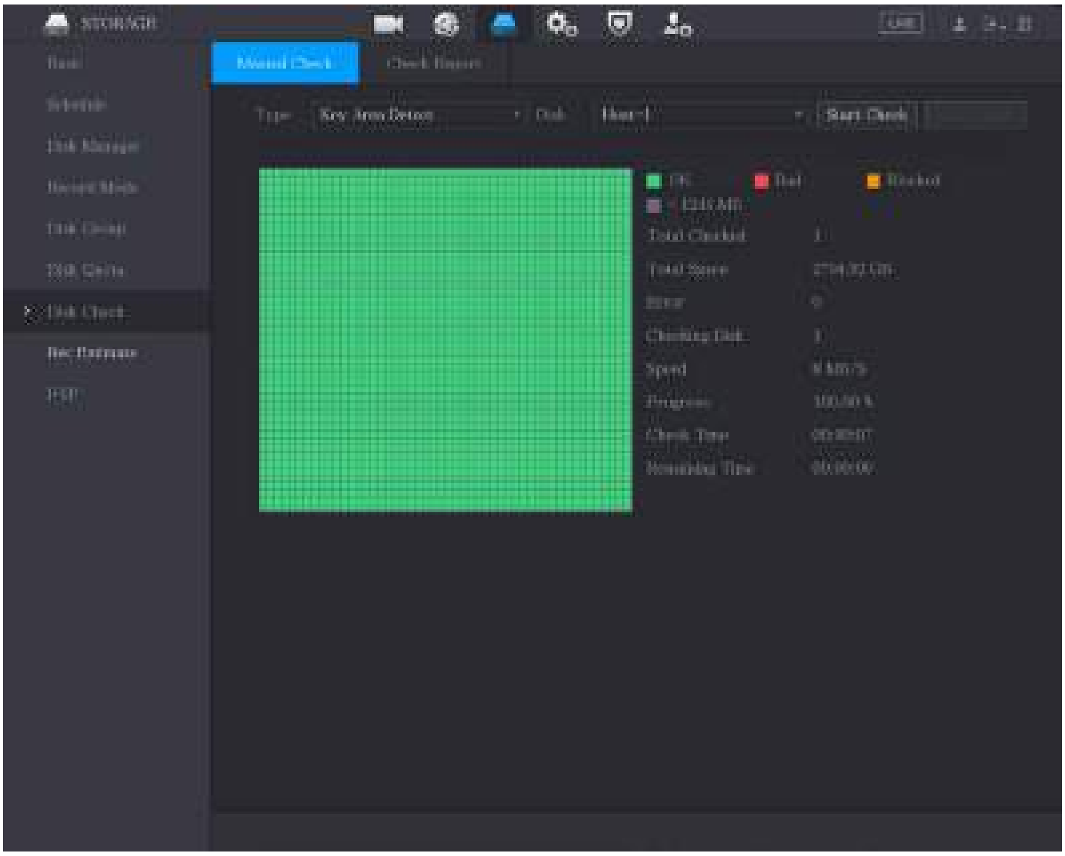
Step 2 In the **Type** list, select **Key Area Detect** or **Global Check**; and in the **Disk** list, select the HDD that you want to detect.

Step 3 Click **Start Check**.

The system starts detecting the HDD.

During detecting, click **Pause** to pause detecting, click **Continue** to restart detecting, and click **Stop Detect** to stop detecting.

Figure 5-316 Start check



STORAGE

Basic
Schedule
Disk Manager
Record Mode
Disk Group
Disk Quota
Disk Check
Rec Estimate
FTP

Manual Check | Check Report

Type Key Area Detect Disk Host-1 Start Check

🟩 OK 🟥 Bad 🟧 Blocked
▨ = 1246 MB

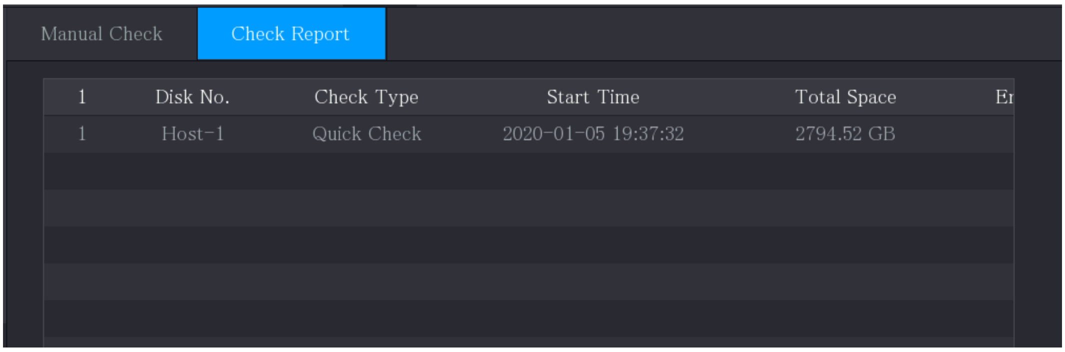
Total Checked	1
Total Space	2794.52 GB
Error	0
Checking Disk	1
Speed	8 MB/S
Progress	100.00 %
Check Time	00:30:07
Remaining Time	00:00:00

5.18.7.2 View Detecting Results

After the detecting is completed, you can view the detecting reports to find out the problem and replace the defective HDD to avoid data loss.

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

Figure 5-317 Check report



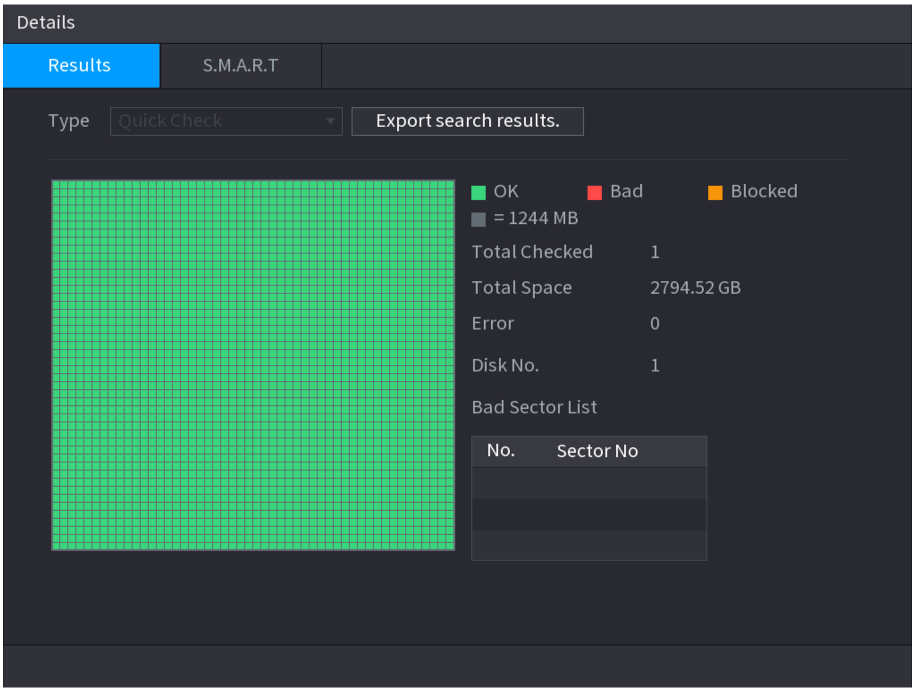
Manual Check | Check Report

1	Disk No.	Check Type	Start Time	Total Space	Er
1	Host-1	Quick Check	2020-01-05 19:37:32	2794.52 GB	

Step 2 Click 🗎.

You can view detecting results and S.M.A.R.T reports.

Figure 5-318 Results



Details

Type Quick Check

🟩 OK 🟥 Bad 🟧 Blocked

■ = 1244 MB

Total Checked 1

Total Space 2794.52 GB

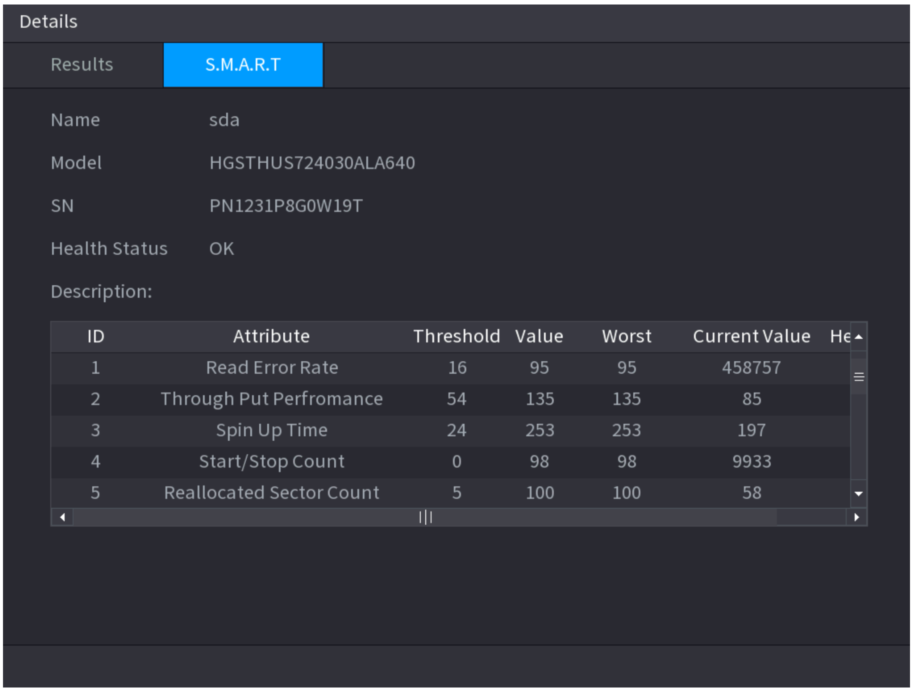
Error 0

Disk No. 1

Bad Sector List

No.	Sector No

Figure 5-319 S.M.A.R.T



Details

Name sda

Model HGSTHUS724030ALA640

SN PN1231P8G0W19T

Health Status OK

Description:

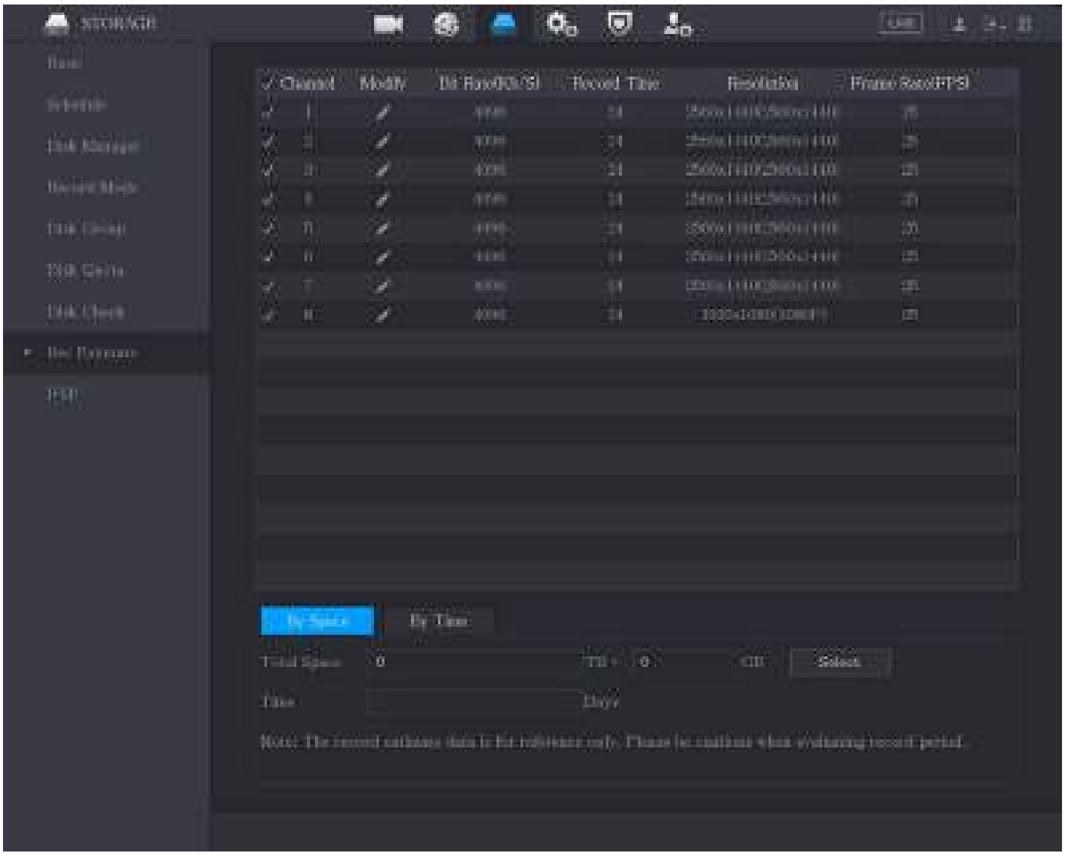
ID	Attribute	Threshold	Value	Worst	Current Value	He
1	Read Error Rate	16	95	95	458757	
2	Through Put Perfromance	54	135	135	85	
3	Spin Up Time	24	253	253	197	
4	Start/Stop Count	0	98	98	9933	
5	Reallocated Sector Count	5	100	100	58	

5.18.8 Configuring 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 5-320 Rec estimate



✓	Channel	Modify	Bit Rate(Kb/S)	Record Time	Resolution	Frame Rate(FPS)
✓	1	✎	4096	24	2560x1440(2560x1440)	25
✓	2	✎	4096	24	2560x1440(2560x1440)	25
✓	3	✎	4096	24	2560x1440(2560x1440)	25
✓	4	✎	4096	24	2560x1440(2560x1440)	25
✓	5	✎	4096	24	2560x1440(2560x1440)	25
✓	6	✎	4096	24	2560x1440(2560x1440)	25
✓	7	✎	4096	24	2560x1440(2560x1440)	25
✓	8	✎	4096	24	1920x1080(1080P)	25

By Space | By Time

Total Space: 0 TB = 0 GB [Select]

Time: 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.

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

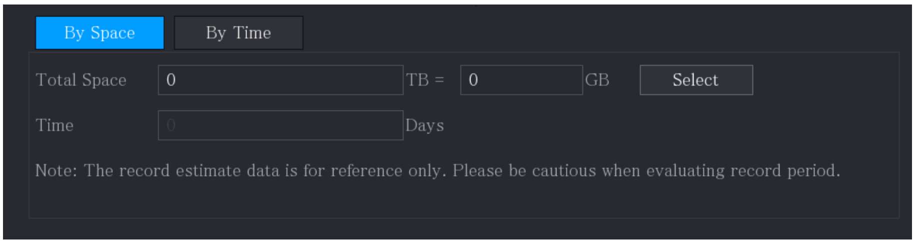
Then the system will calculate the time period that can be used for storage according to the channels settings and HDD capacity.

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

Calculating Recording Time

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

Figure 5-321 By space



By Space | By Time

Total Space: 0 TB = 0 GB [Select]

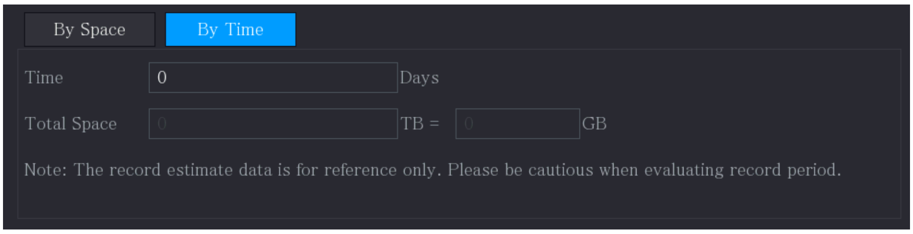
Time: 0 Days

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

Step 2 Click **Select**.

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

Figure 5-322 By time



Time 0 Days

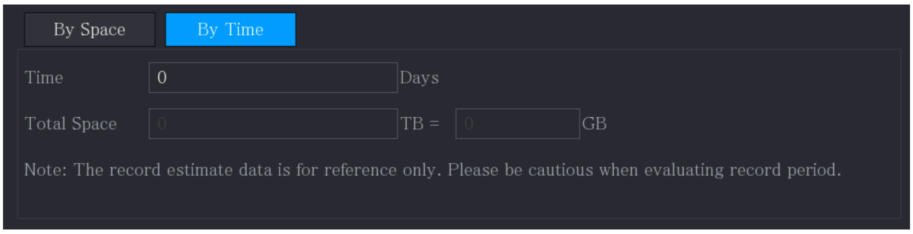
Total Space 0 TB = 0 GB

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

Calculating HDD Capacity for Storage

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

Figure 5-323 By time



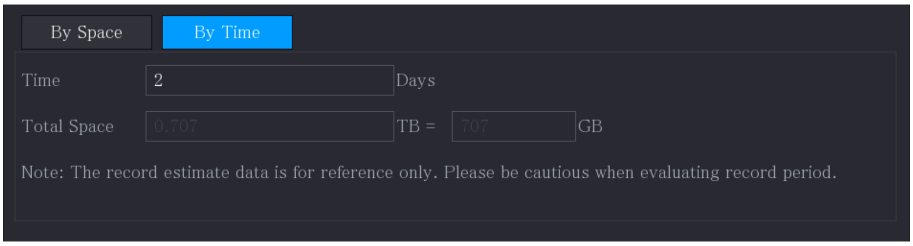
Time 0 Days

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.

Figure 5-324 Total space



Time 2 Days

Total Space 0.707 TB = 707 GB

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

5.18.9 Configuring FTP Storage Settings

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

Preparation

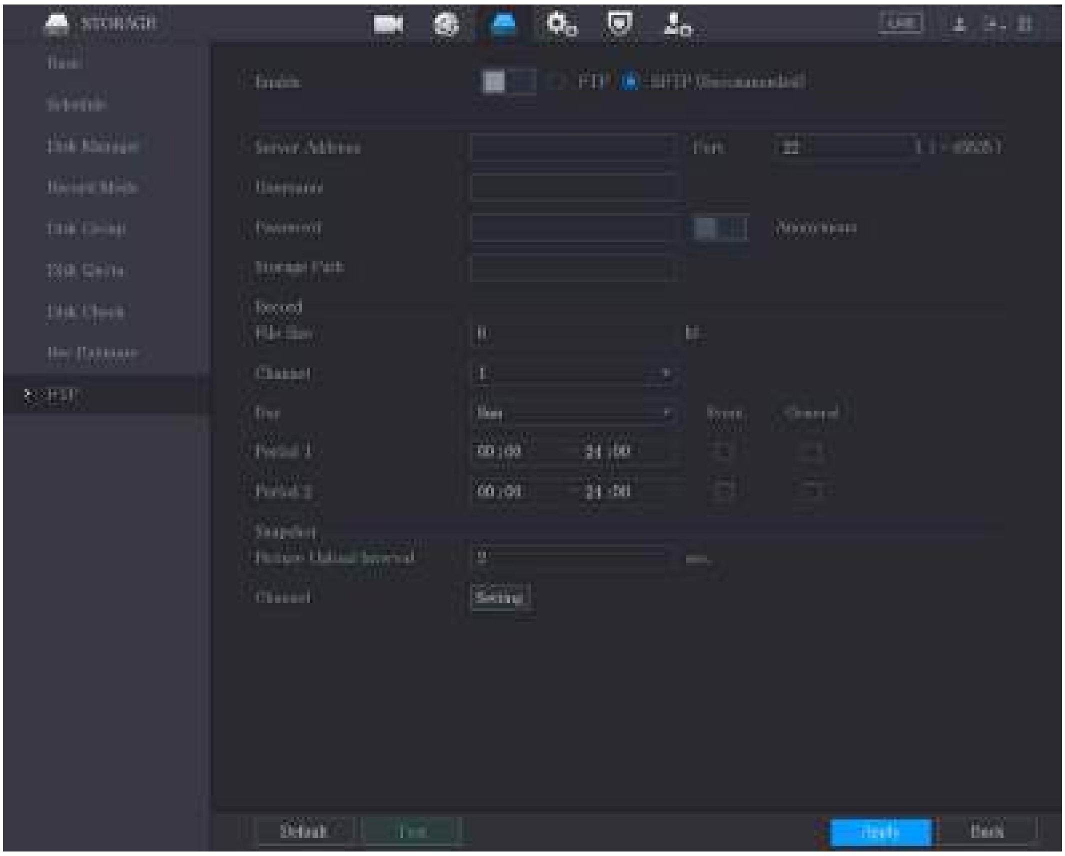
Purchase or download a FTP server and install it on your PC.

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

Procedure

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

Figure 5-325 FTP



Step 2 Configure the settings for the FTP settings parameters.

Table 5-61 FTP settings parameters

Parameter	Description
Enable	Enable the FTP upload function.
FTP type	● FTP: Plaintext transmission. ● SFTP: Encrypted transmission (recommended)
Server Address	IP address of FTP server.
Port	● FTP: The default is 21. ● SFTP: The default is 22.
Anonymous	Enter the user name and password to log in to the FTP server. Enable the anonymity function, and then you can login anonymously without entering the user name and password.
Username	
Password	
Storage Path	Create folder on FTP server. ● If you do not enter the name of remote directory, 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.

Parameter	Description
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 (Sec.)	● 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, select **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**.

The system pops up a message to indicate success or failure. If failed, check the network connection or configurations.

Step 4 Click **Apply** to complete the settings.

5.19 Security Center

You can set security options to strengthen device security and use the device in a much safer way.

5.19.1 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 about the security status of the device.

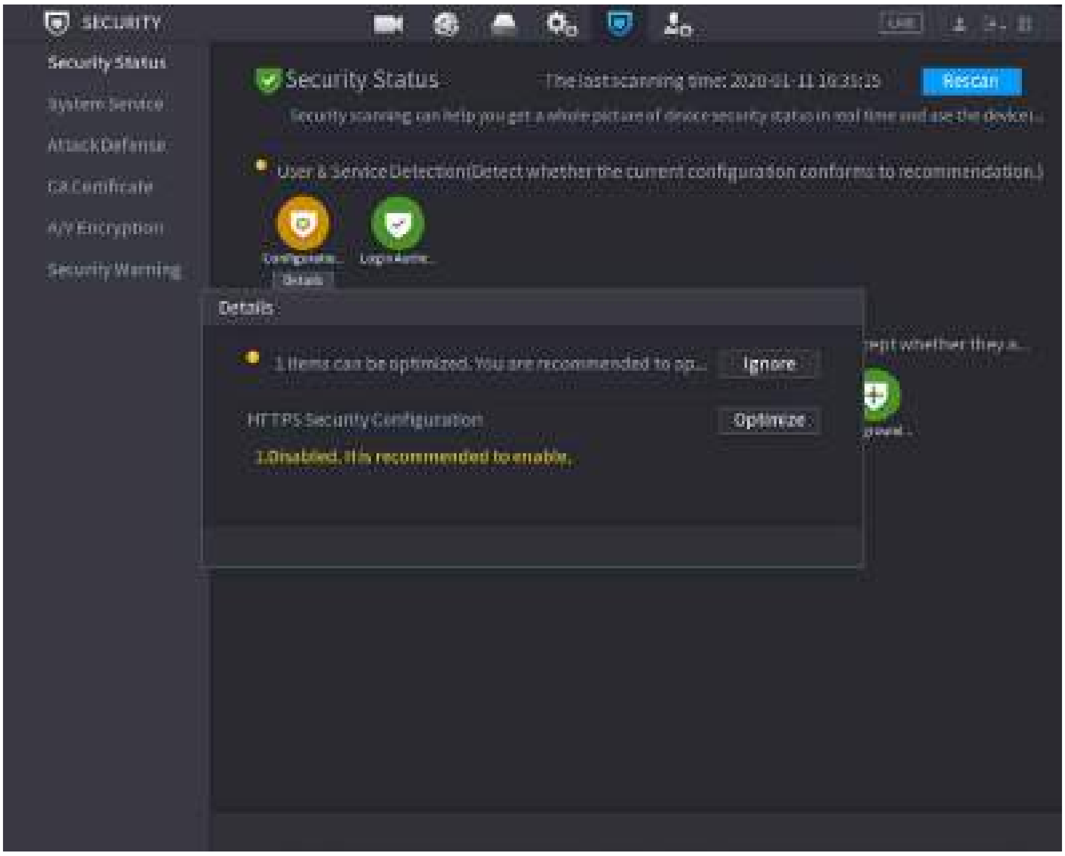
Detecting User and Service

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 login authentication, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

- 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 5-326 Security status



Security Status The last scanning time: 2020-01-11 10:31:15

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

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

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, move mouse pointer on the icon to see the on-screen instructions.

Scanning Security Status

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

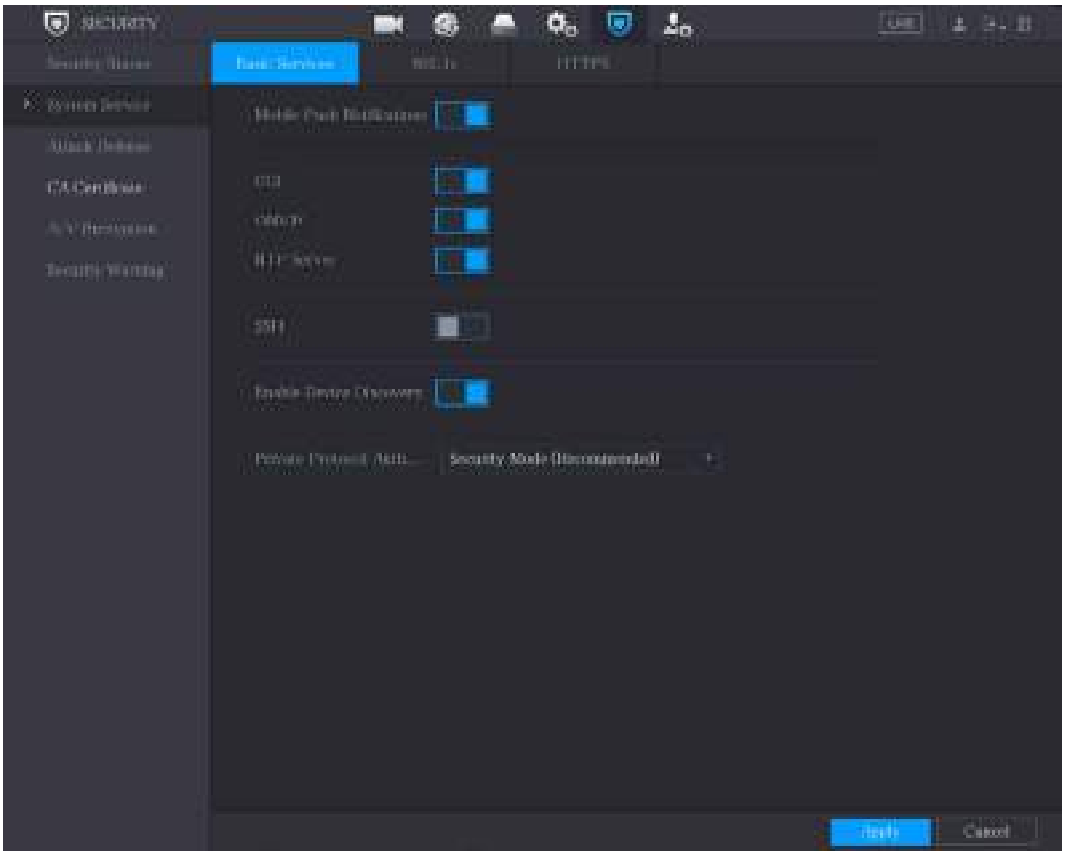
5.19.2 System Service

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

5.19.2.1 Basic Services

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

Figure 5-327 Basic services



Step 2 Select **Basic Services** and configure parameters.

There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled.

Table 5-62 Basic services 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. There might be safety risk if this service is enabled. Disable this function when it is not in use.
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default. There might be safety risk if this service is enabled. Disable this function when it is not in use.

Parameter	Description
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default. 📖 There might be safety risk if this service is enabled. Disable this function when it is not in use.
NTP Server	After enabling this function, a NTP server can be used to synchronize the device. This function is enabled by default.
SSH	After enabling this function, you can use SSH service. This function is disabled by default. 📖 There might be safety risk if this service is enabled. Disable this function when it is not in use.
Enable Device Discovery	After enabling this function, the device can be searched by other devices.
Private Protocol Authentication Mode	● Security Mode (Recommended): Uses Digest access authentication when connecting to DVR. ● Compatible Mode: Select this mode when the client does not support Digest access authentication.

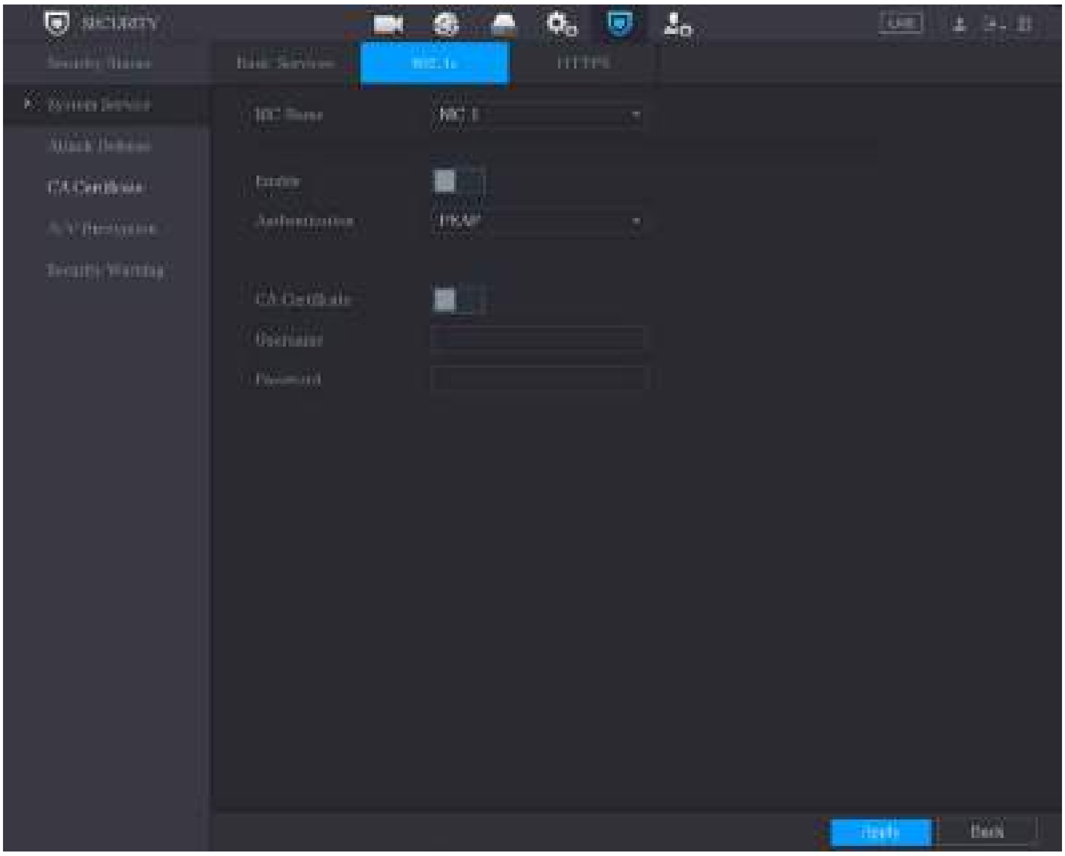
Step 3 Click **Apply** to complete the settings.

5.19.2.2 802.1x

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

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

Figure 5-328 802.1x



NIC Name: NIC 1

Enable □

Authentication: PEAP

CA Certificate □

Username

Password

Step 2 Select the Ethernet card you want to certify.

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

Table 5-63 802.1x parameters

Parameter	Description
NIC Name	Select a NIC.
Authentication	● PEAP: protected EAP protocol. ● TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details about importing and creating a certificate, see 5.19.4.
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

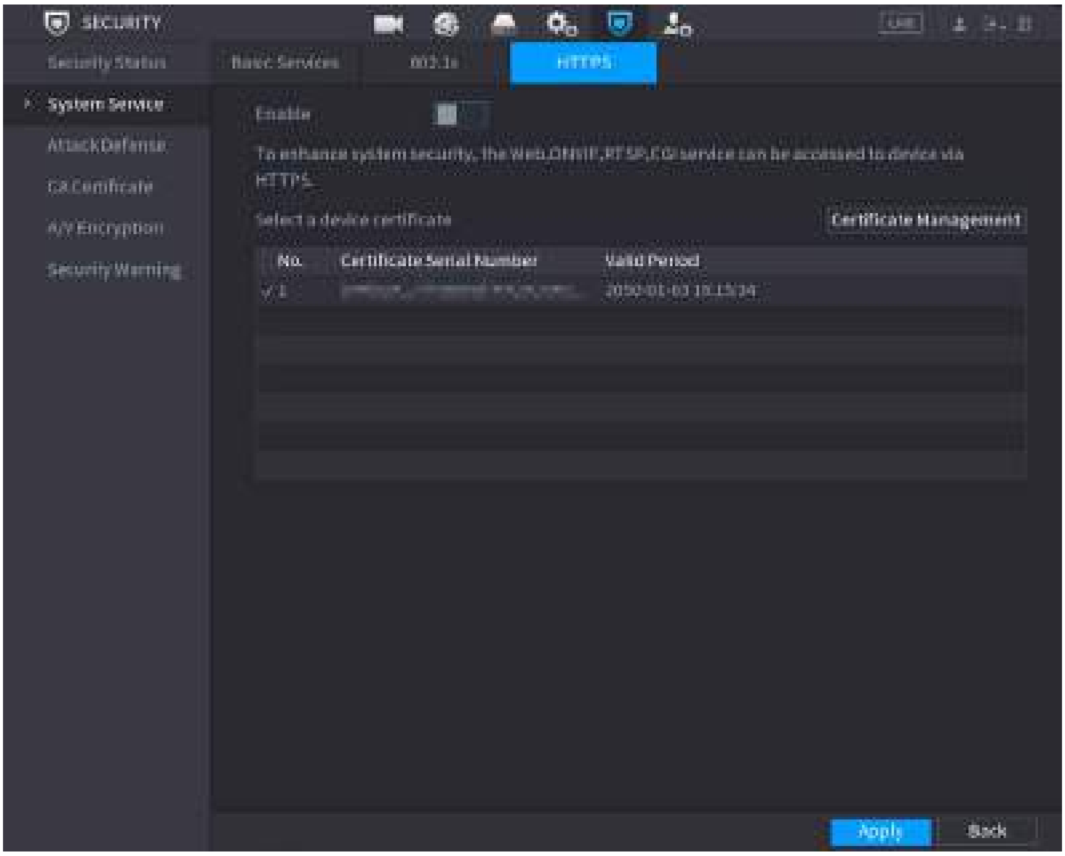
Step 4 Click **Apply** to complete the settings.

5.19.2.3 HTTPS

We recommend that you enable HTTPS function to enhance system security.

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

Figure 5-329 HTTPS



Enable

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

Select a device certificate

No.	Certificate Serial Number	Valid Period
✓ 1	[illegible]	2050-01-03 10:15:34

Step 2 Select **Enable** to enable HTTPS function.

Step 3 Click **Certificate Management** to create or import a HTTPS certificate from USB drive. For details about importing or creating a CA certificate, see 5.19.4.

Step 4 Select a HTTPS certificate.

Step 5 Click **Apply** to complete the settings.

5.19.3 Attack Defense

5.19.3.1 Firewall

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

Step 2 Select **Enable** to enable firewall.

Step 3 Configure the parameters.

Table 5-64 Firewall parameters

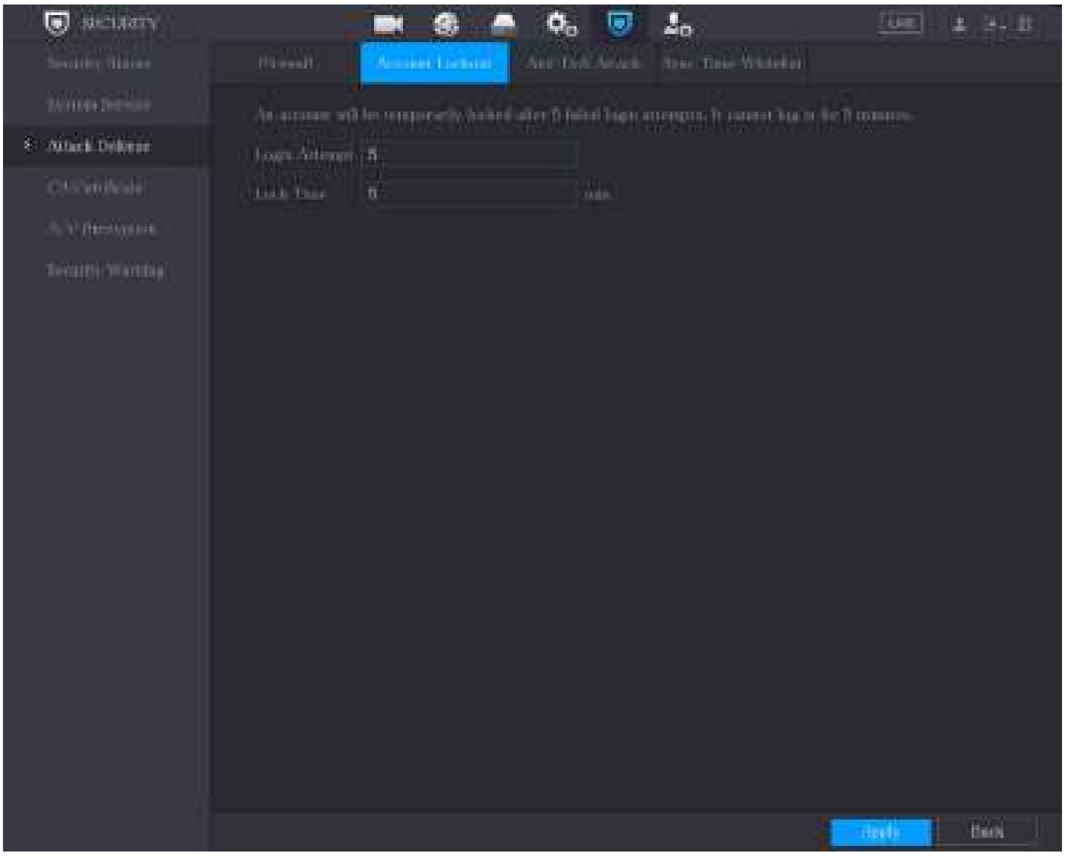
Parameter	Description
Mode	Mode can be configured when Type is Network Access. ● If Allowlist is enabled, you can visit device port successfully with IP/MAC hosts in the allowlist. ● If Blocklist is enabled, you cannot visit device port with IP/MAC hosts in blocklist.
Add	When Type is Network Access, you can configure IP Address, IP Segment and MAC Address.
Type	You can select IP address, IP segment and MAC address.
IP Address	Enter IP Address, Start Port and End Port that is allowed or forbidden. 📖 When Type is IP Address, they can be configured. Start Port and End Port can be configured only in Network Access Type.
Start Port	
End Port	
Start Address/End Address	Enter Start Address and End Address of IP Segment. 📖 When Type is IP Segment, they can be configured.
MAC Address	Enter MAC Address that is allowed or forbidden 📖 When Type is MAC Address, it can be configured.

Step 4 Click **Apply** to complete the settings.

5.19.3.2 Account Lockout

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

Figure 5-330 Account lockout



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

Login Attempt 5

Lock Time 5 min.

Step 2 Set parameters.

Table 5-65 Lockout parameters

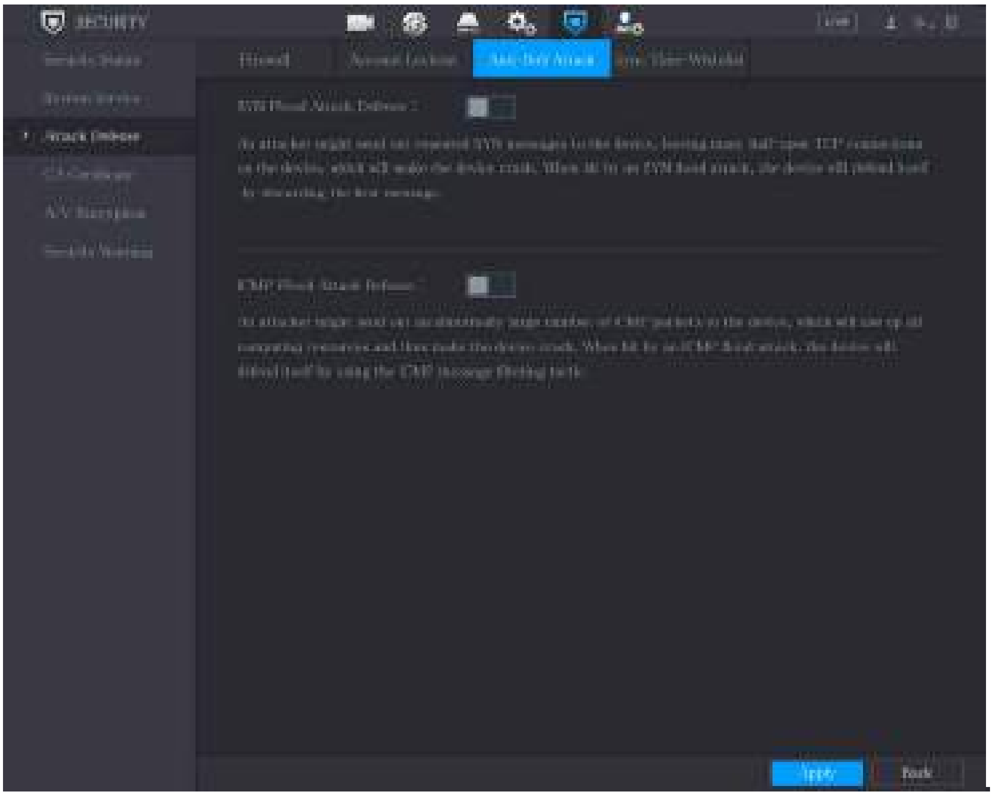
Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number. Value range: 5–30. Default value: 5.
Lock Time	Set how long the account is locked for. Value range: 5–120 minutes. Default value: 5 minutes.

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

5.19.3.3 Anti-Dos Attack

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

Figure 5-331 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 then make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

5.19.3.4 Sync Time-Allowlist

The synchronization is only allowed with hosts in the trusted list.

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

Step 2 Select **Enable** to enable **Sync Time-Allowlist** function.

Step 3 Configure the parameters.

Table 5-66 Time-allowlist parameters

Parameter	Description
Add	You can add trusted hosts for time synchronization.
Type	Select IP address or IP segment for hosts to be added.
IP Address	Input the IP address of a trusted host. When Type is IP Address, it can be configured
Start Address	Input the start IP address of trusted hosts. When Type is IP Segment, it can be configured

Parameter	Description
End Address	Input the end IP address of trusted hosts. When Type is IP Segment, it can be configured

Step 4 Click **Apply** to complete the settings.

5.19.4 CA Certificate

You can create or import device certificate and install trusted CA Certificate.

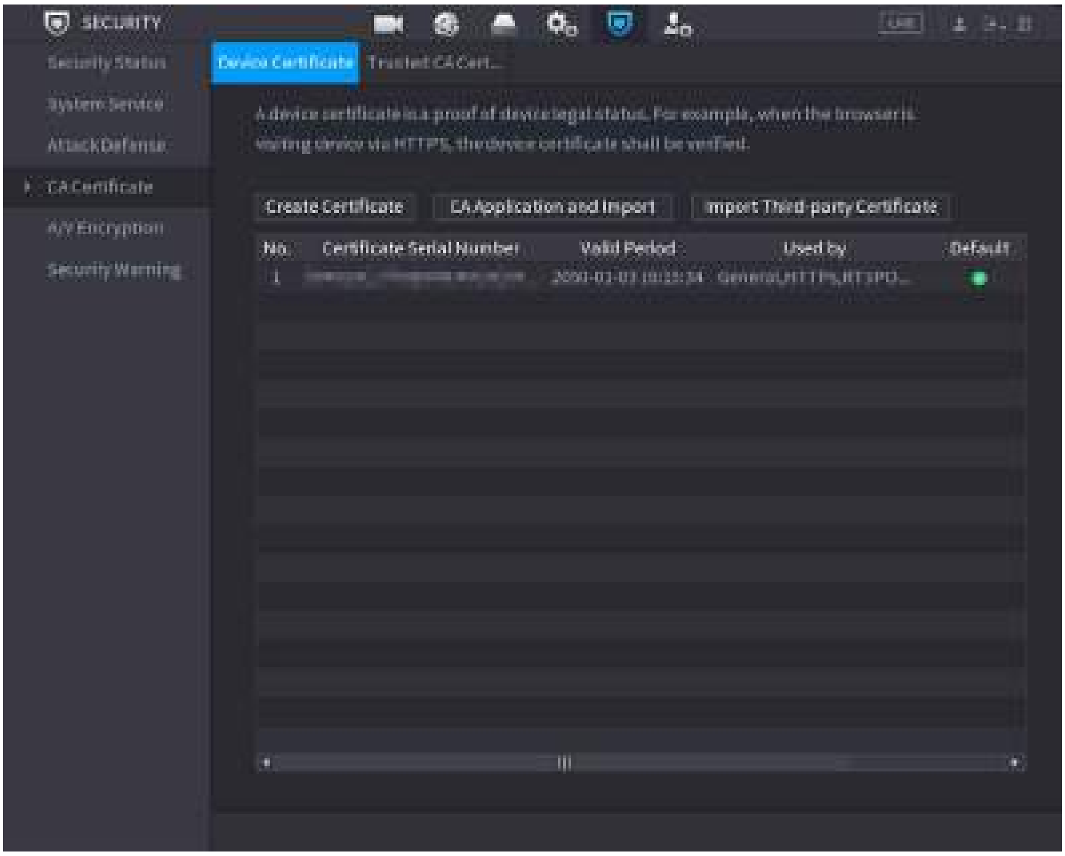
5.19.4.1 Device Certificate

Create Certificate

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

- Click ⬇ to download the certificate to local storage.
- Click 🗑 to delete the certificate. The deleted certificate cannot be restored, proceed with caution.

Figure 5-332 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	Valid Period	Used by	Default
1	[redacted]	2050-01-03 10:15:34	General,HTTPS,RTSPO...	●

Step 2 Configure parameters.

Table 5-67 Device certificate parameters

Parameter	Description
County	This parameter is user defined.
State	This parameter is user defined.
City Name	This parameter is user defined.
Valid Period	Input a valid period for the certificate.
Organization	This parameter is user defined.
Organization Unit	This parameter is user defined.
Domain Name	Input the IP address of the certificate.

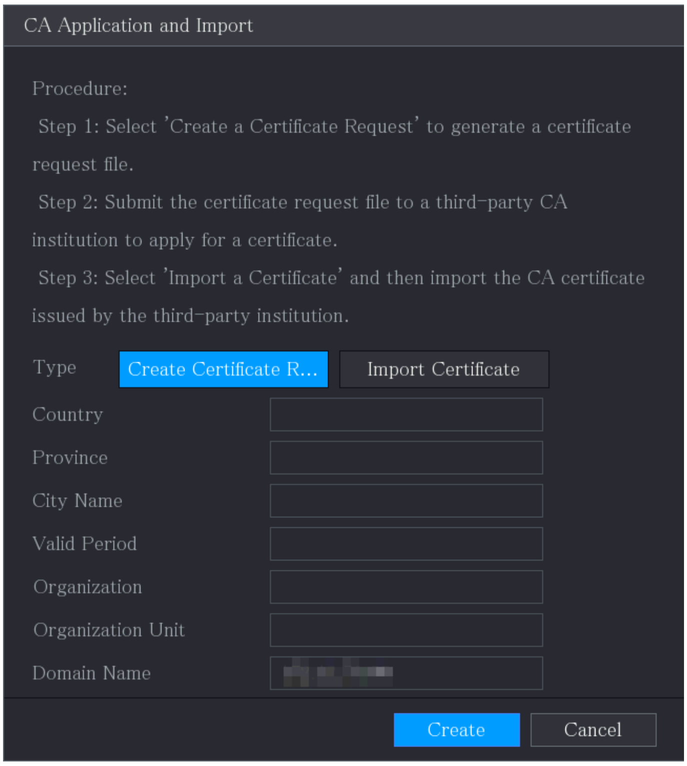
Step 3 Click **Create**.

CA Application and Import

Follow the on-screen instructions to finish CA application and import.

Insert a USB flash drive before operating.

Figure 5-333 CA application and import



CA Application and Import

Procedure:

Step 1: Select 'Create a 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 a Certificate' and then import the CA certificate issued by the third-party institution.

Type: Create Certificate R... | Import Certificate

Country

Province

City Name

Valid Period

Organization

Organization Unit

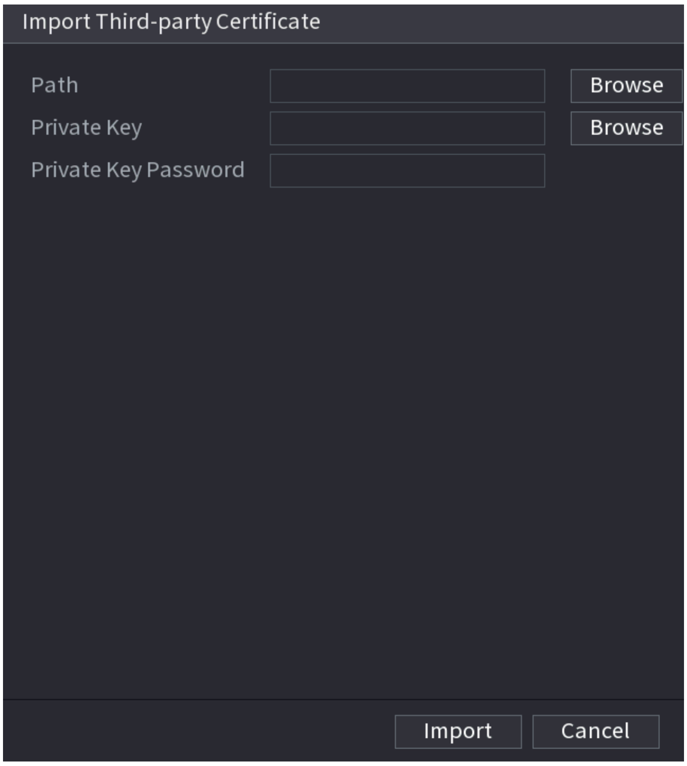
Domain Name [redacted]

Import Third-Party Certificate

Insert the USB flash drive with third-party certificate before importing.

Step 1 Select **Import Third-party Certificate**.

Figure 5-334 Import third-party certificate



Import Third-party Certificate

Step 2 Configure Parameters.

Table 5-68 Import 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 password of encrypted private key. When the private key is not encrypted, you don't need to this parameter.

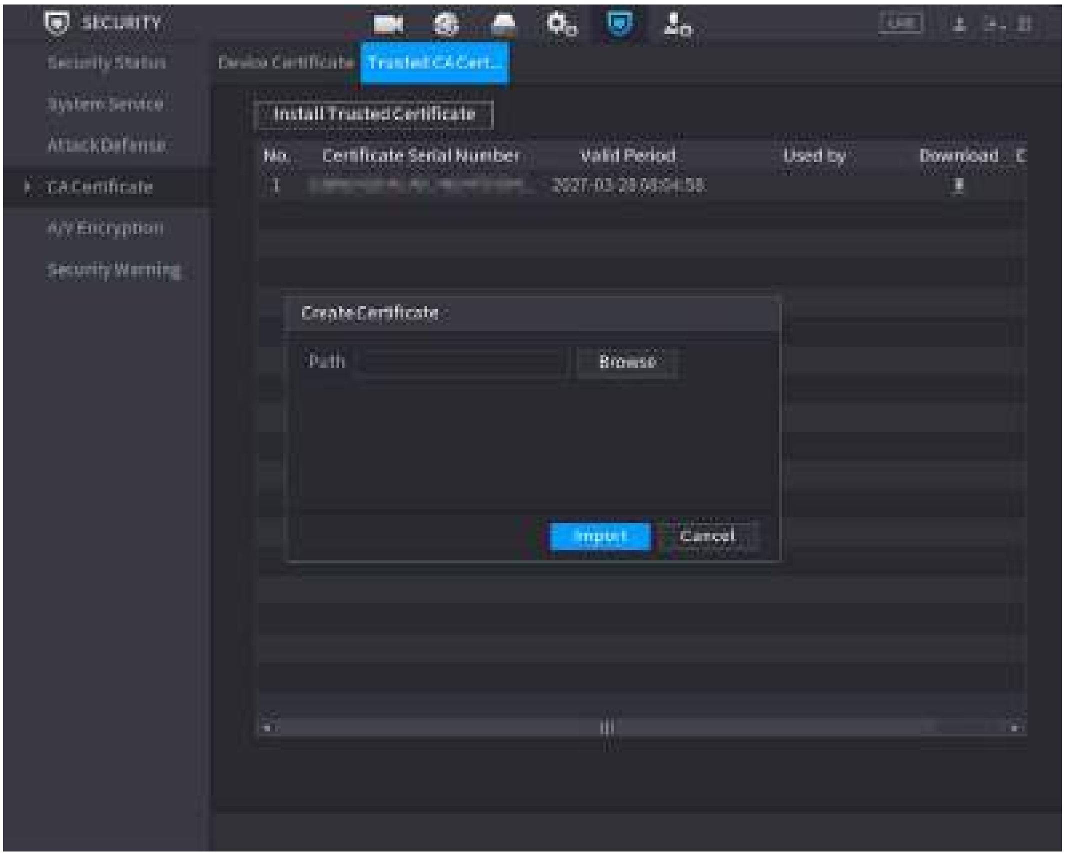
Step 3 Click **Create**.

5.19.4.2 Trusted CA Certificate

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

Step 2 Click **Install Trusted Certificate**.

Figure 5-335 Install certificate



No.	Certificate Serial Number	Valid Period	Used by	Download	E
1	[redacted]	2027-03-28 08:04:58			

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

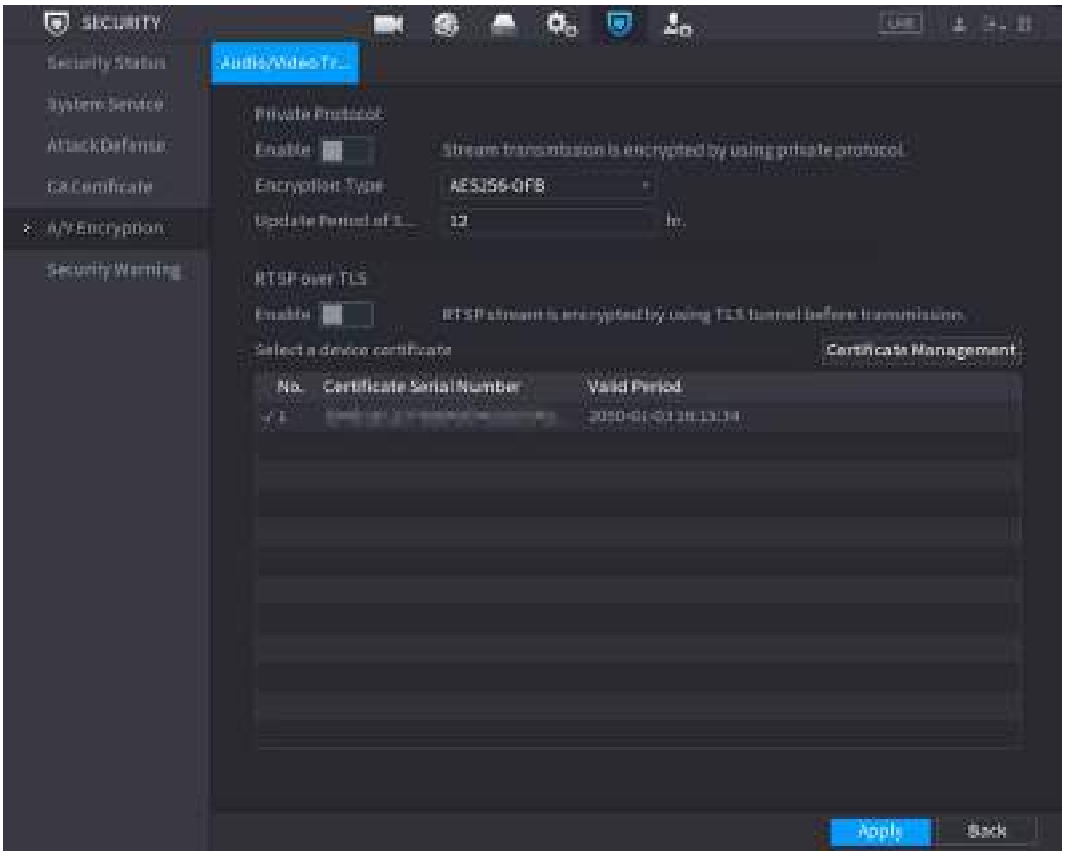
Step 4 Click **Import.**

5.19.5 Audio/Video Encryption

The device supports audio and video encryption during data transmission.

Step 1 Select **Main Menu** > **SECURITY** > **A/V Encryption** > **Audio/Video Transmission**.

Figure 5-336 Audio/video transmission



Private Protocol

Enable □ Stream transmission is encrypted by using private protocol.

Encryption Type: AES256-OFB

Update Period of S...: 12 hr.

RTSP over TLS

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

Select a device certificate

Certificate Management

No.	Certificate Serial Number	Valid Period
✓ 1	[redacted]	2050-01-01 18:13:34

Apply Back

Step 2 Configure parameters.

Table 5-69 Transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety vulnerability 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 data breach if this service is disabled. We recommend that you enable this function.
	Select a device certificate	Select a device certificate for RTSP over TLS.

Area	Parameter	Description
	Certificate Management	For details about certificate management, see "5.19.4.1 Device Certificate".

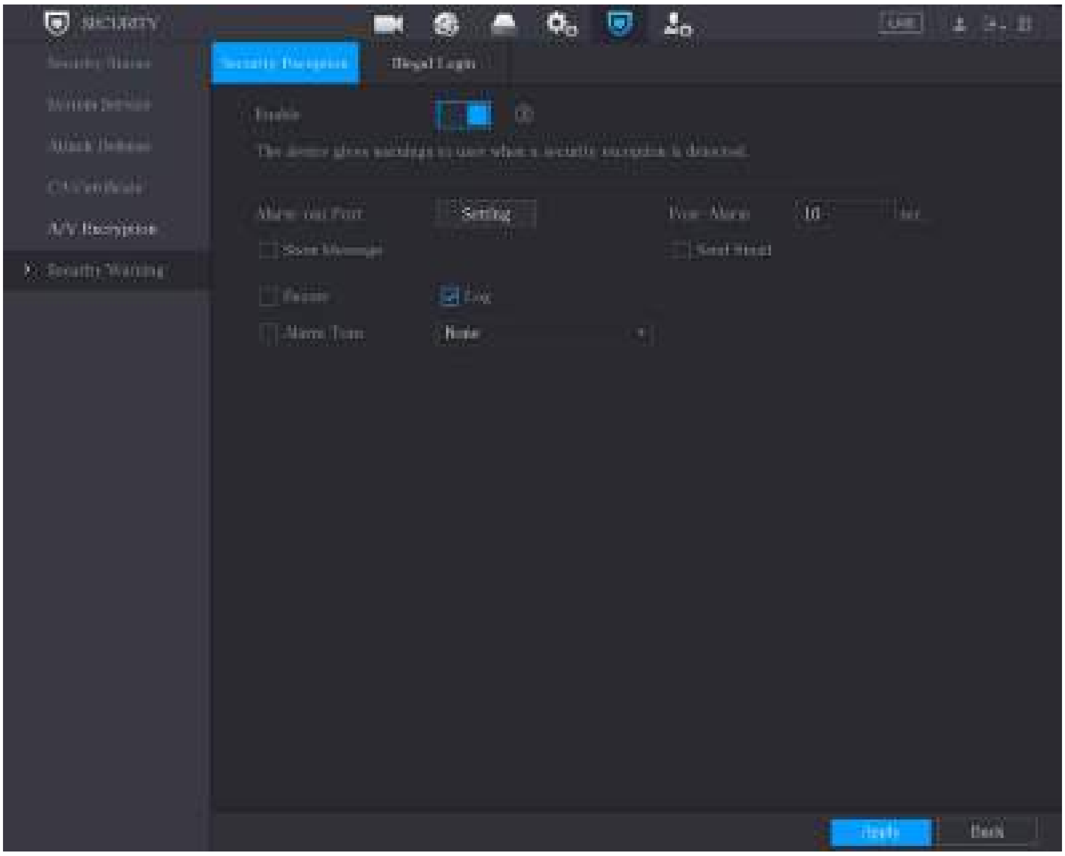
Step 3 Click **Apply** to complete the settings.

5.19.6 Security Warning

5.19.6.1 Security Exception

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

Figure 5-337 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 Select **Enable** and configure parameters.

Table 5-70 Security exception parameters

Parameter	Description
Alarm-out Port	The alarm device (such as lights, sirens, etc.) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.

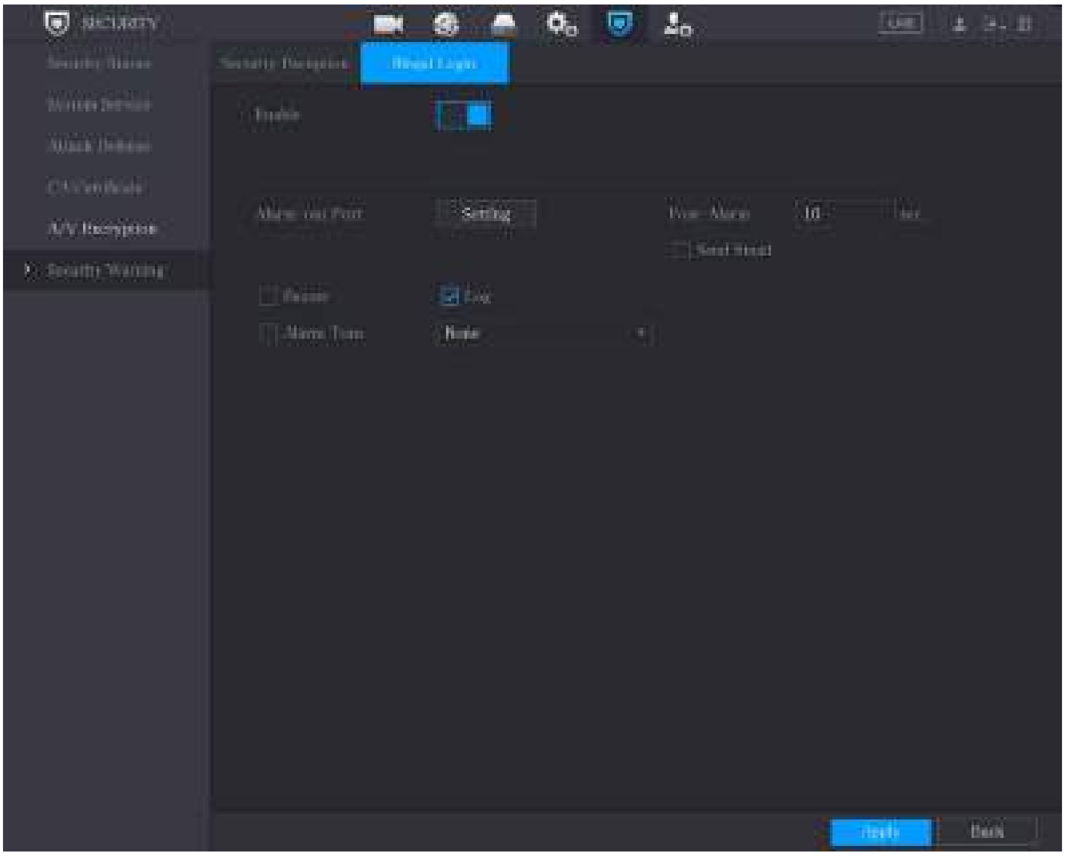
Parameter	Description
Post-Alarm	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds to 300 seconds.
Show Message	Checkbox to enable a pop-up message in your local host PC.
Buzzer	Select the checkbox to activate the buzzer when an alarm occurs.
Alarm Tone	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs. See "5.17 Audio Management" to add audio file first.
Log	Select the checkbox, the NVR device records the alarm information in the log when an alarm occurs.
Send Email	Select the checkbox. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**.
?	Security Event monitoring explanation. It indicates the type of attacks that can trigger security exception. ● Unauthorized executable program trying to run ● Web URL brute-force attack ● Session connection overload ● Session ID brute-force attack

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

5.19.6.2 Illegal Login

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

Figure 5-338 Illegal login



Enable ☑

Alarm-out Port: Setting

Post-Alarm: 10 sec.

□ Send Email

□ Buzzer ☑ Log

□ Alarm Tone: None

Step 2 Select **Enable** and configure parameters.

Table 5-71 Illegal login parameters

Parameter	Description
Alarm-out Port	The alarm device (such as lights, sirens) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.
Post-Alarm	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds through 300 seconds.
Buzzer	Select the checkbox to activate the buzzer when an alarm occurs.
Alarm Tone	Check the box and then select the corresponding audio file from the dropdown list. System plays the audio file when the alarm occurs. See "5.17 Audio Management" to add audio file first
Log	Select the checkbox, the NVR device records the alarm information in the log when an alarm occurs.

Parameter	Description
Send Email	Select the checkbox. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. 📖 To use this function, make sure the email function is enabled in **Main Menu > NETWORK > Email**.

5.20 Configuring System Settings

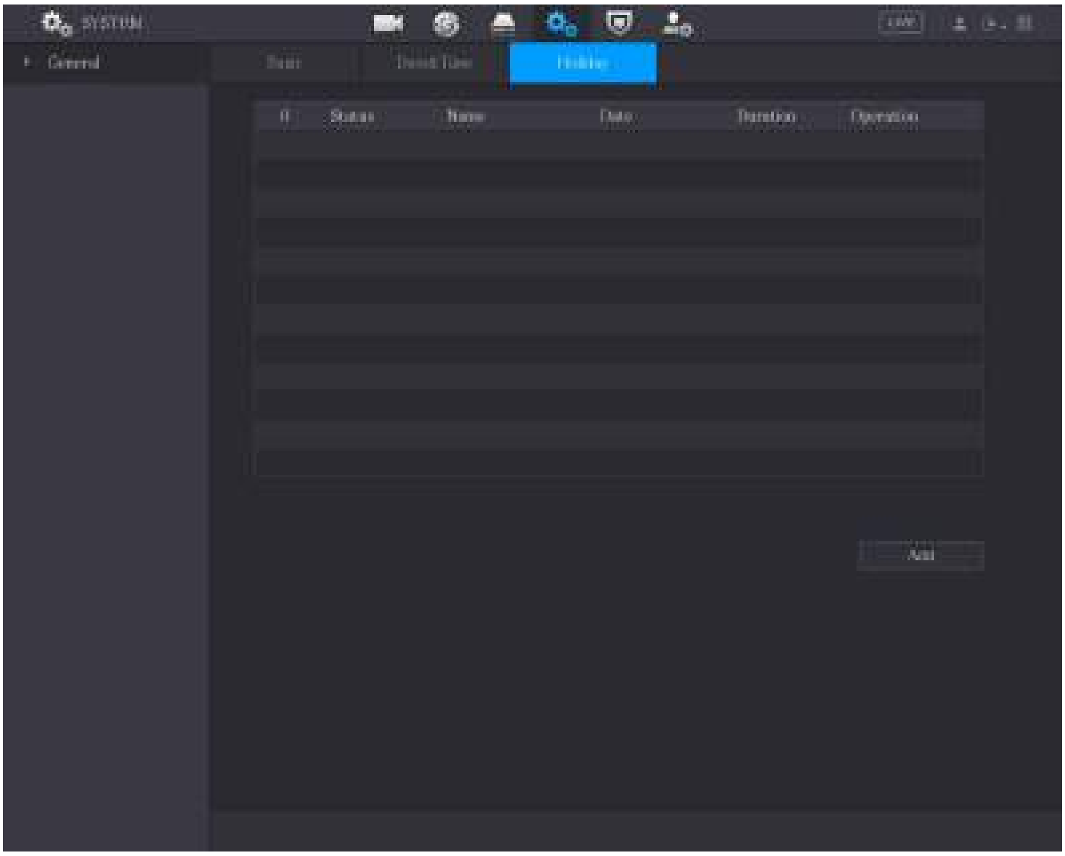
5.20.1 Configuring General System Settings

You can configure the device basic settings, time settings, and holiday settings.

To configure the holiday settings, do the following:

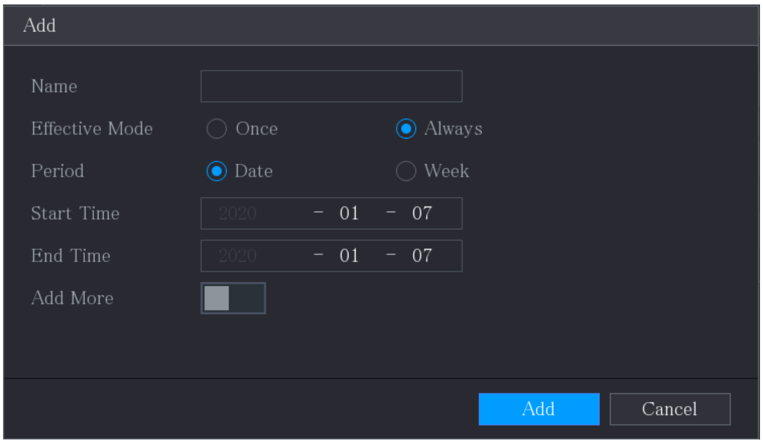
Step 1 Select **Main Menu > SYSTEM > General > Holiday**.

Figure 5-339 Holiday



Step 2 Click **Add**.

Figure 5-340 Add holiday



Add

Name

Effective Mode ○ Once ● Always

Period ● Date ○ Week

Start Time 2020 - 01 - 07

End Time 2020 - 01 - 07

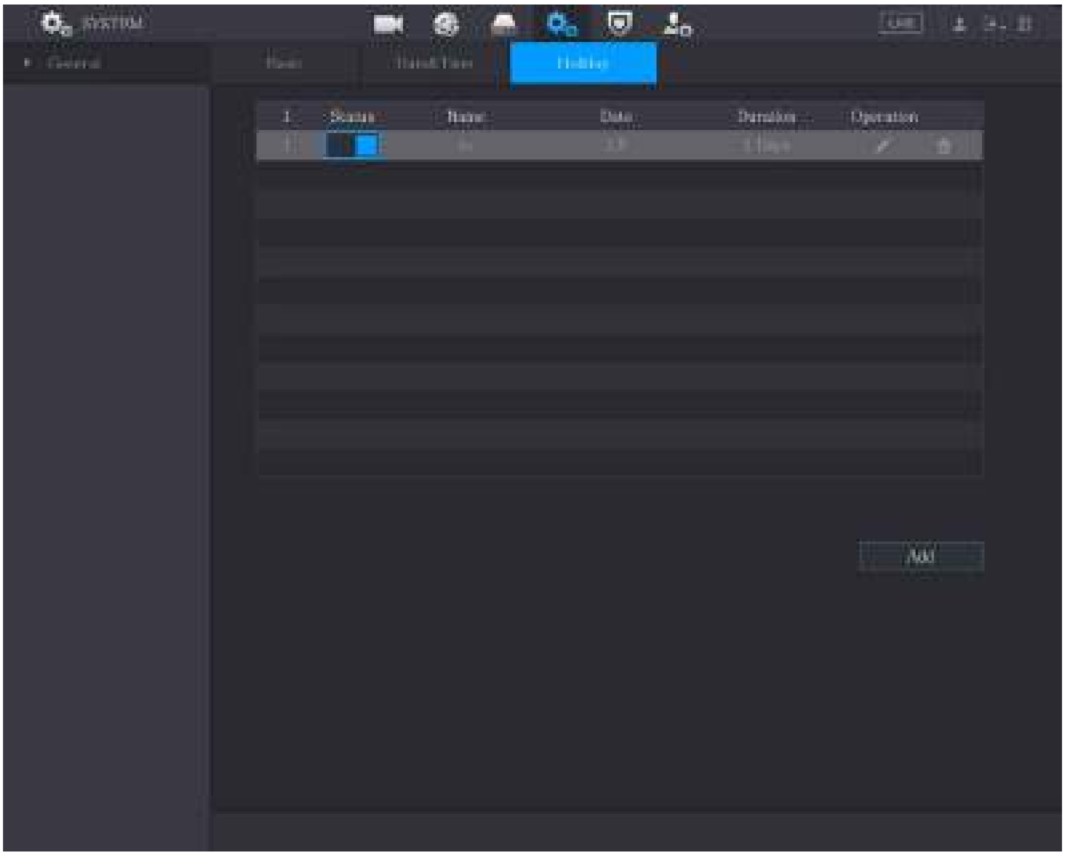
Add More

Step 3 Configure the holiday name, repeat mode, time range according to your actual situation.

Step 4 Click **Add**.

Enable the **Add More** function, so you can continue adding holiday information.

Figure 5-341 Added holiday



1	Status	Name	Date	Duration	Operation
[illegible]	●	[illegible]	[illegible]	[illegible]	

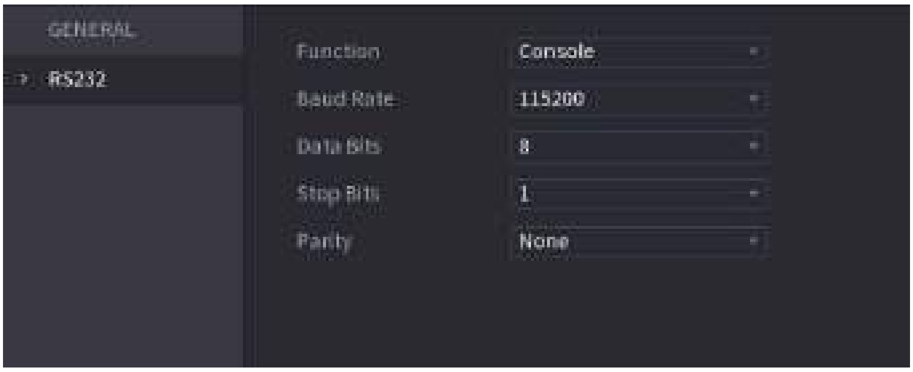
5.20.2 Configuring RS-232 Settings

You can configure serial port function, Baud rate and other parameters.

Only some series products support this RS-232.

Select **Main Menu** > **SYSTEM** > **RS232**.

Figure 5-342 RS-232



Function: Console
Baud Rate: 115200
Data Bits: 8
Stop Bits: 1
Parity: None

Table 5-72 RS-232 parameters

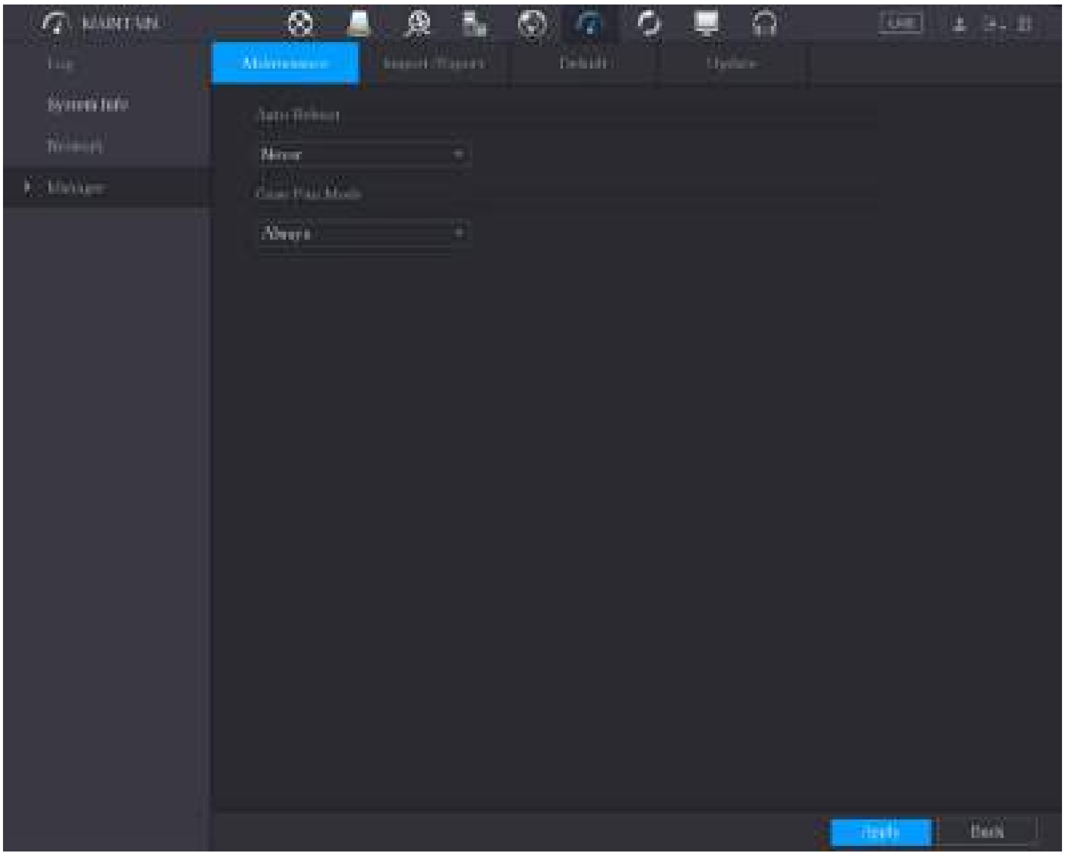
Parameter	Description
Function	Select serial port control protocol. ● Console: Upgrade the program and debug with the console and mini terminal software. ● Keyboard: Control this Device with special keyboard. ● Adapter: Connect with PC directly for transparent transmission of data. ● Protocol COM: Configure the function to protocol COM, in order to overlay card number. ● PTZ Matrix: Connect matrix control. It is **Console** by default.
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. It is none by default.

5.20.3 Configuring System Maintenance Settings

When the Device has been running for a long time, you can configure the auto reboot when the Device is not working. You can also configure the case fan mode to reduce noise and extend the service life.

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

Figure 5-343 Maintenance



Auto Reboot: Never

Case Fan Mode: Always

Step 2 Configure the settings for the system maintenance parameters.

Table 5-73 Maintenance parameters

Parameter	Description
Auto Reboot	In the **Auto Reboot** list, select the reboot time.
Case Fan Mode	In the **Case Fan Mode** list, you can select **Always** or **Auto**. If you select **Auto**, the case fan will stop or start according to the external conditions such as the Device temperature. 📖 Not all models support this function, and it is only supported on the local configuration page.

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

5.20.4 Exporting and Importing System Settings

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

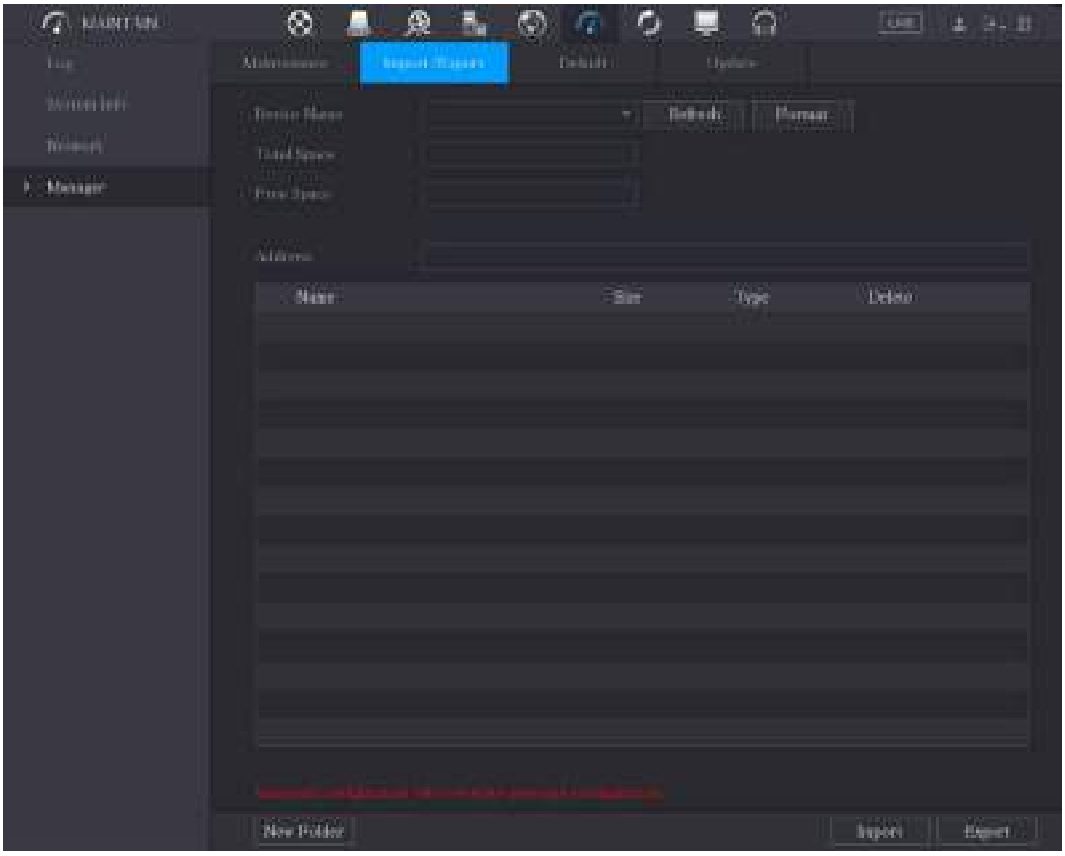
📖

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

Exporting System Settings

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

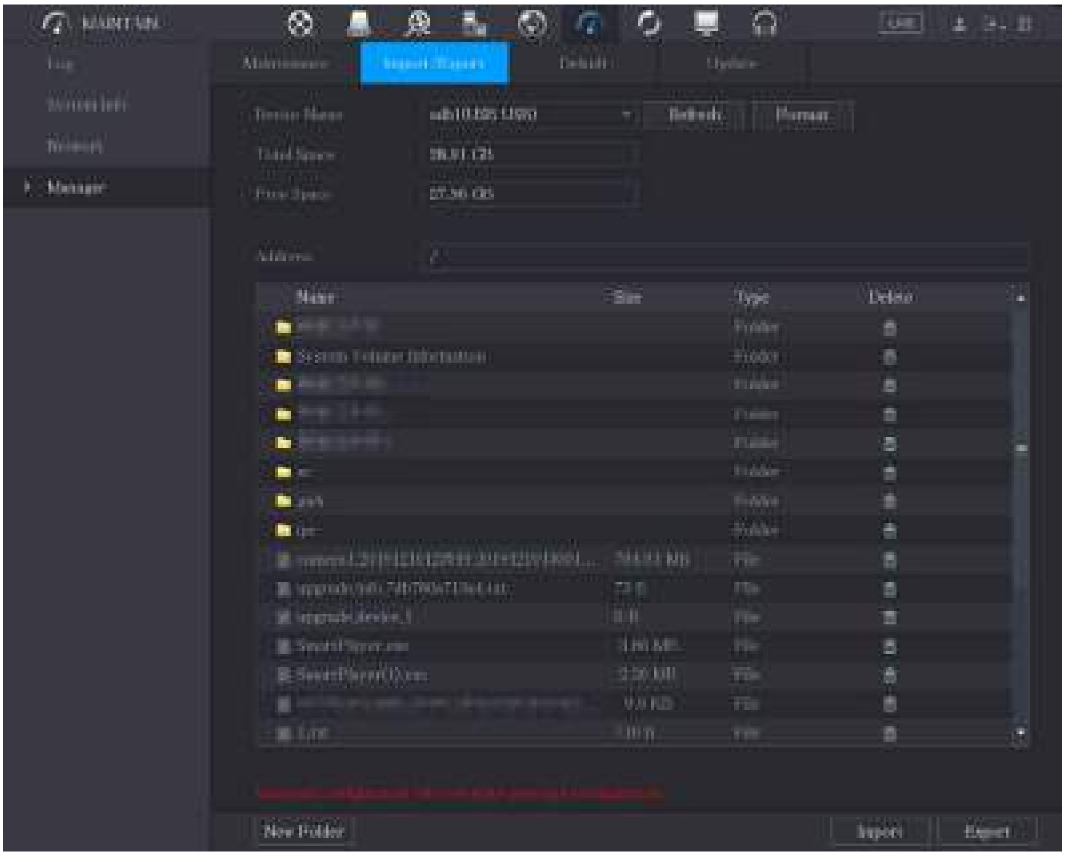
Figure 5-344 Import/Export



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

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

Figure 5-345 Connected device



Step 4 Click **Export**.

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

Importing System Settings

Step 1 Insert a USB storage device containing the exported configuration files from another Device) into one of the USB ports on the Device.

Step 2 Select **Main Menu > SYSTEM > Import/Export**.

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

Step 4 Click on the configuration folder (under the name style of "Config_[YYYYMMDDhhmmss]") that you want to import.

Step 5 Click **Import**.

The Device will reboot after the imported is succeeded.

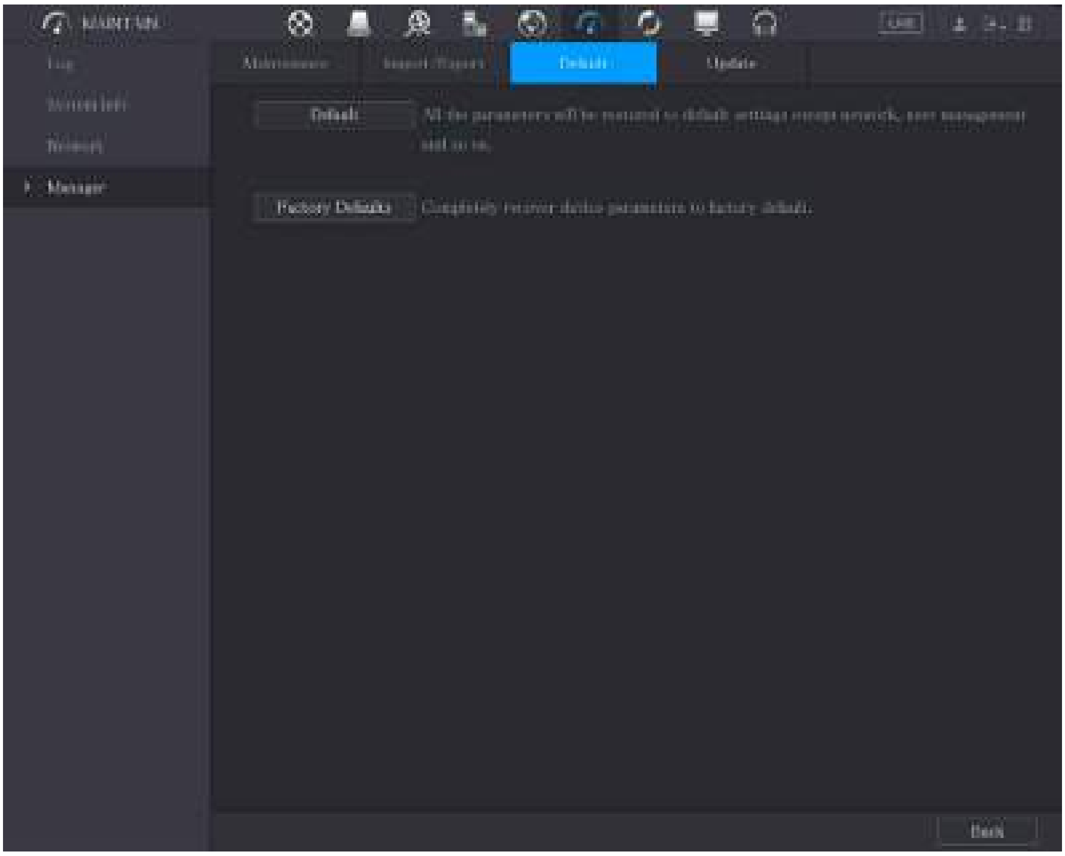
5.20.5 Restoring Default Settings

Only Admin account supports this function.

You can select the settings that you want to restore to the factory default.

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

Figure 5-346 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.

- Click **Default** to restore all parameters to default settings except parameters such as network, user management.
- Click **Factory Default**, select **OK** and then enter the password of admin user in the prompted dialog box to completely recover device parameters to factory default.

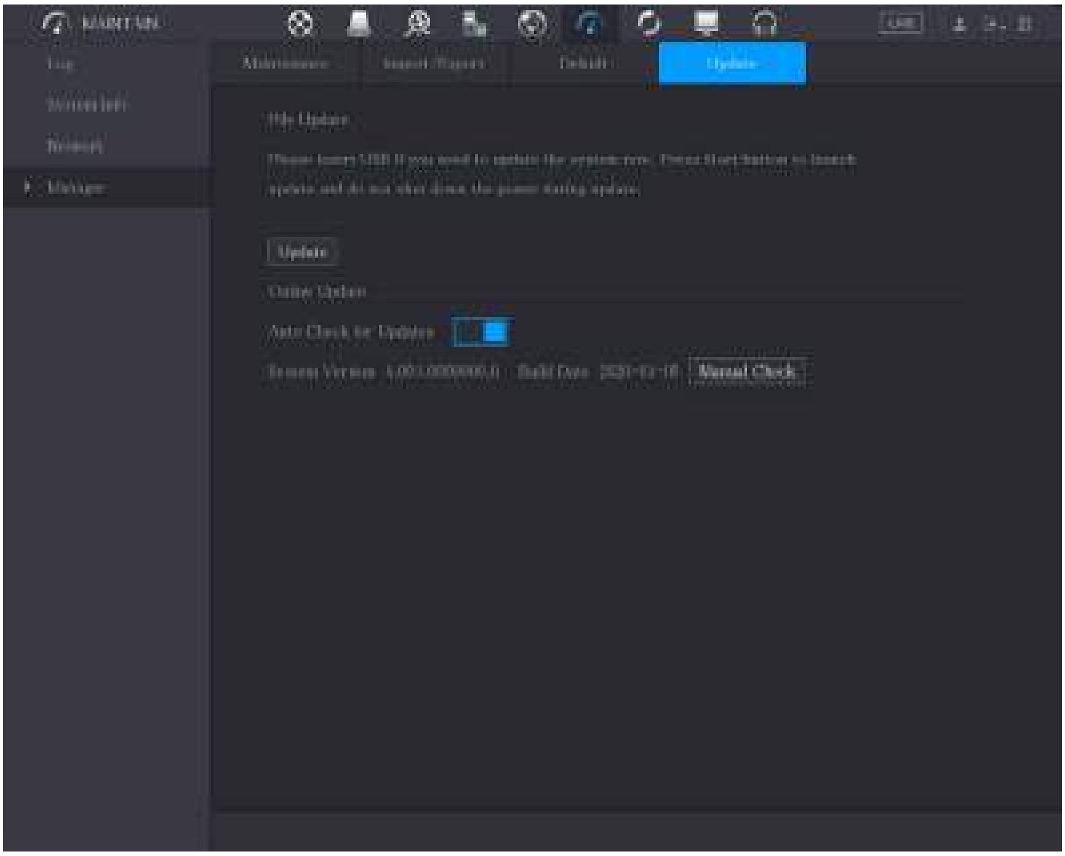
5.20.6 Updating the Device

5.20.6.1 Updating File

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 5-347 Update



File Update

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

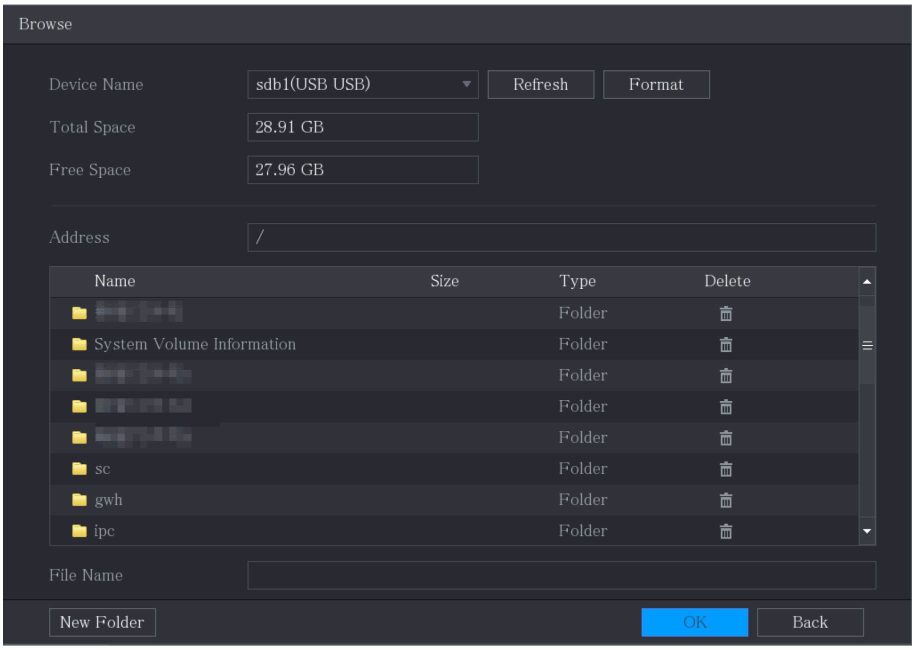
Online Update

Auto Check for Updates

System Version 4.001.0000000.0 Build Date 2021-01-18

Step 3 Click **Update**.

Figure 5-348 Browse



Device Name sdb1(USB USB)

Total Space 28.91 GB

Free Space 27.96 GB

Address /

Name	Size	Type	Delete
[redacted]		Folder	🗑
System Volume Information		Folder	🗑
[redacted]		Folder	🗑
[redacted]		Folder	🗑
[redacted]		Folder	🗑
sc		Folder	🗑
gwh		Folder	🗑
ipc		Folder	🗑

File Name

Step 4 Click the file that you want to upgrade.

Step 5 Click **OK**.

5.20.6.2 Performing Online Upgrade

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.

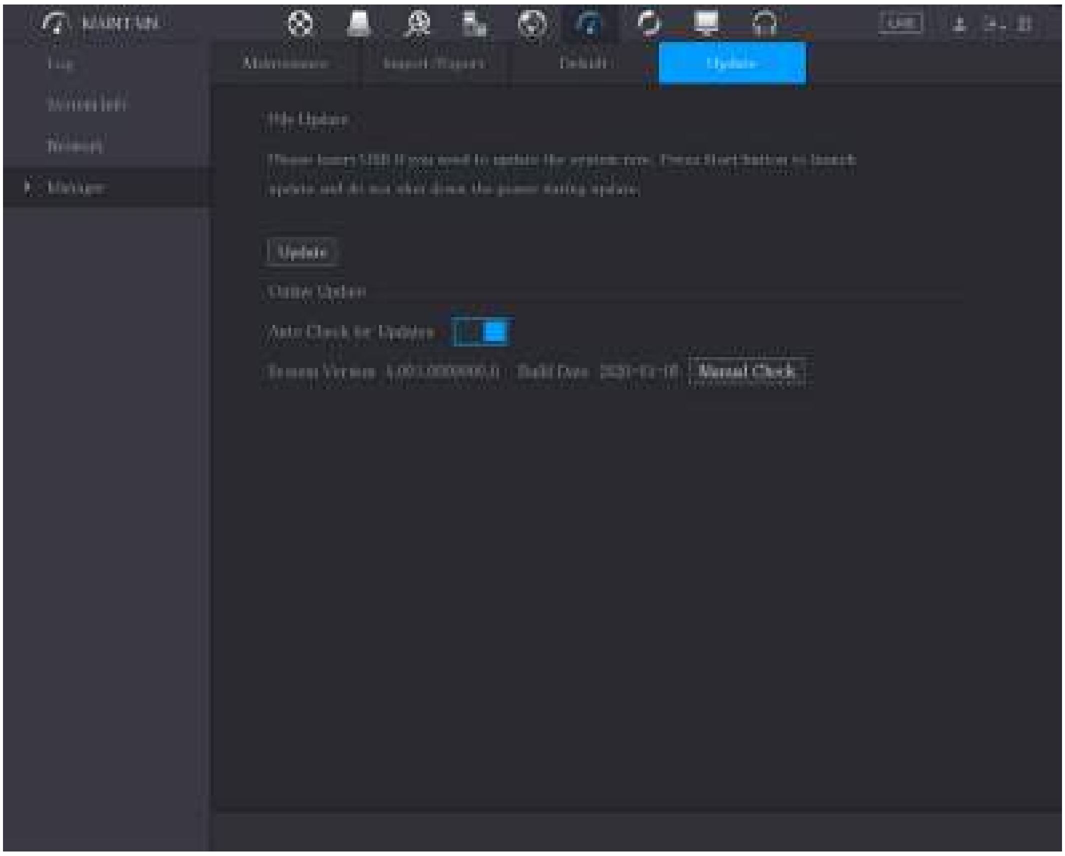
- Auto check: The Device checks if there is any new version available at intervals.
- Manual check: Perform real-time check whether there is any new version available.

⚠

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

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

Figure 5-349 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 Version [illegible] Build Date [illegible]

Step 2 Check whether there is any new version available.

- Auto check: 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 the step 3.

Step 3 Click **Upgrade now**.

5.20.6.3 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 checks whether there is a USB storage device connected and if there is 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.

5.20.7 Exporting Intelligent Diagnosis Data

When an error occurs, go to **Main Menu** > **MAINTAIN** > **Intelligent Diagnosis** to export intelligent diagnosis data for troubleshooting. The maintenance tasks, such as the import and export of configuration, can be performed in COS Pro Portal. For details, see the corresponding user's manual.

5.21 Viewing Information

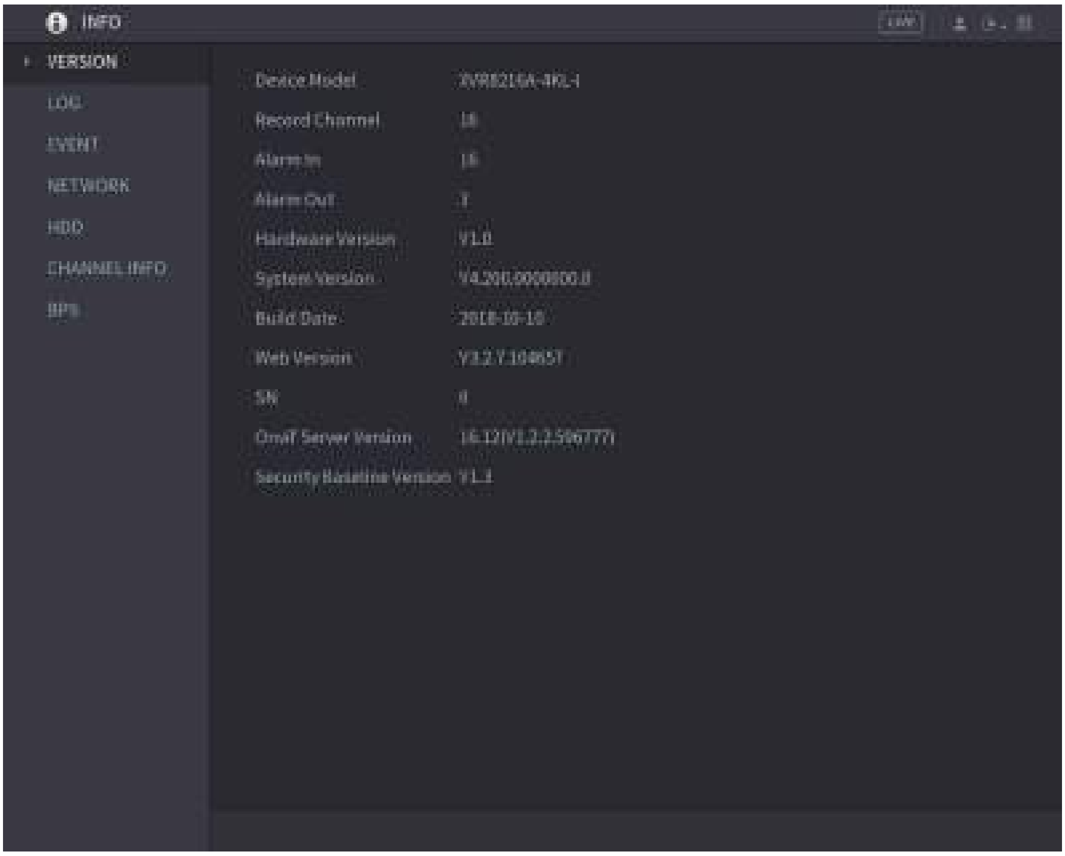
You can view the information such as log information, HDD information, and version details

5.21.1 Viewing Version Details

You can view the version details such as device model, system version, and build date.

Select **Main Menu** > **INFO** > **VERSION**.

Figure 5-350 Version



Device Model	XVR5216A-4KL-I
Record Channel	16
Alarm In	16
Alarm Out	3
Hardware Version	V1.0
System Version	V4.200.0000000.0
Build Date	2018-10-10
Web Version	V3.2.7.104657
SN	0
Onvif Server Version	16.12(V1.2.2.596777)
Security Baseline Version	V1.1

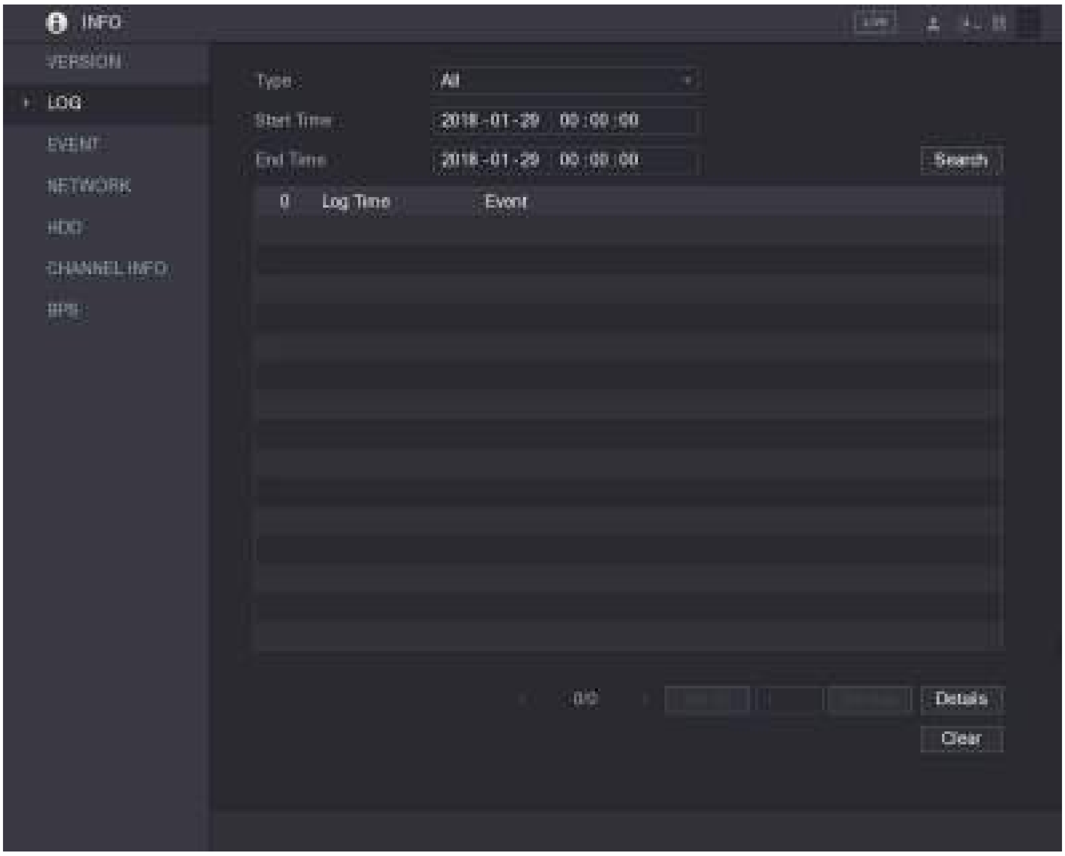
5.21.2 Viewing Log Information

You can view and search the log information.

- If there is HDD installed, the logs about system operations are saved in the memory of the Device and other types of logs are saved into the HDD. If there is no HDD installed, the other types of logs are also saved in the memory of the Device.
- When formatting the HDD, the logs will not be lost. However, if you take out the HDD from the Device, the logs might be lost.

Step 1 Select **Main Menu > INFO > LOG**.

Figure 5-351 Log



Type: All

Start Time 2018-01-29 00:00:00

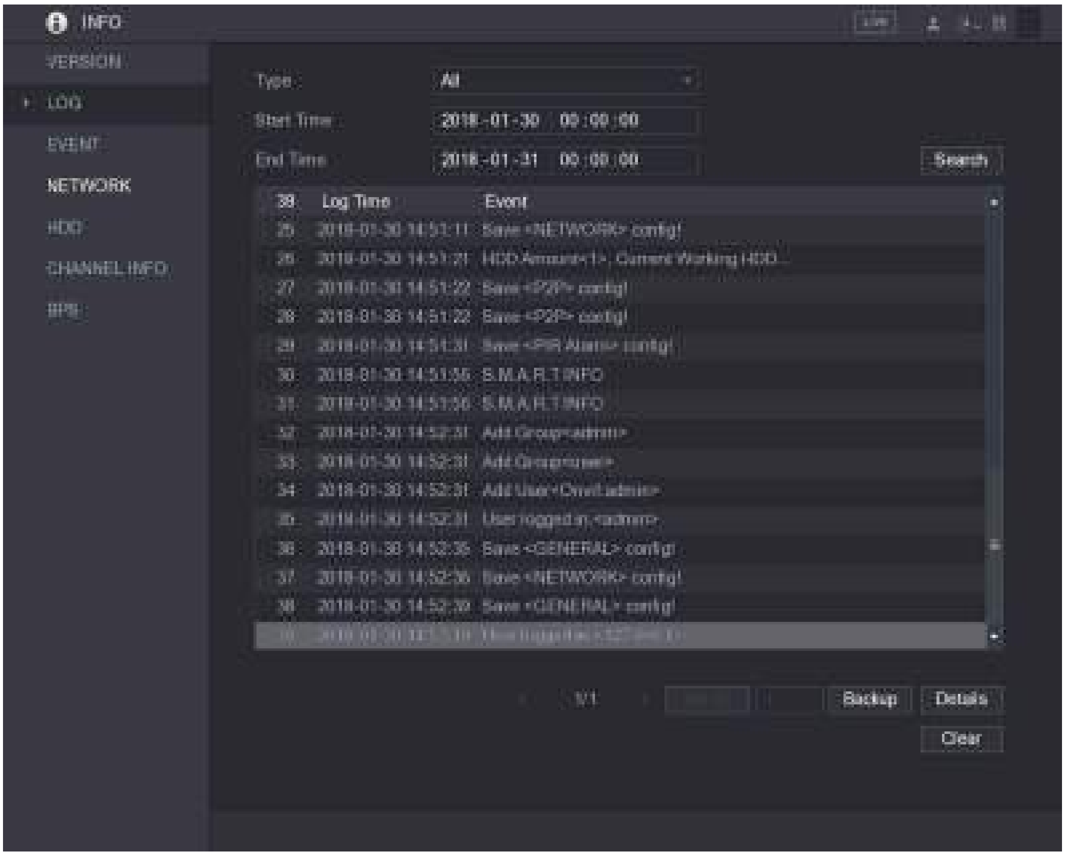
End Time 2018-01-29 00:00:00

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

Step 3 In the **Start Time** box and **End Time** box, enter the time period to search, and then click **Search**.

The search results are displayed.

Figure 5-352 Search results



Type: All

Start Time: 2018 -01 -30 00 :00 :00

End Time: 2018 -01 -31 00 :00 :00

38	Log Time	Event
25	2018-01-30 14:51:11	Save <NETWORK> config!
26	2018-01-30 14:51:21	HDD Amount<1>, Current Working HDD...
27	2018-01-30 14:51:22	Save <P2P> config!
28	2018-01-30 14:51:22	Save <P2P> config!
29	2018-01-30 14:51:31	Save <PIR Alarm> config!
30	2018-01-30 14:51:56	S.M.A.R.T INFO
31	2018-01-30 14:51:56	S.M.A.R.T INFO
32	2018-01-30 14:52:31	Add Group<admin>
33	2018-01-30 14:52:31	Add Group<user>
34	2018-01-30 14:52:31	Add User<Own\admin>
35	2018-01-30 14:52:31	User logged in.<admin>
36	2018-01-30 14:52:35	Save <GENERAL> config!
37	2018-01-30 14:52:36	Save <NETWORK> config!
38	2018-01-30 14:52:39	Save <GENERAL> config!
[illegible]	[illegible]	[illegible]

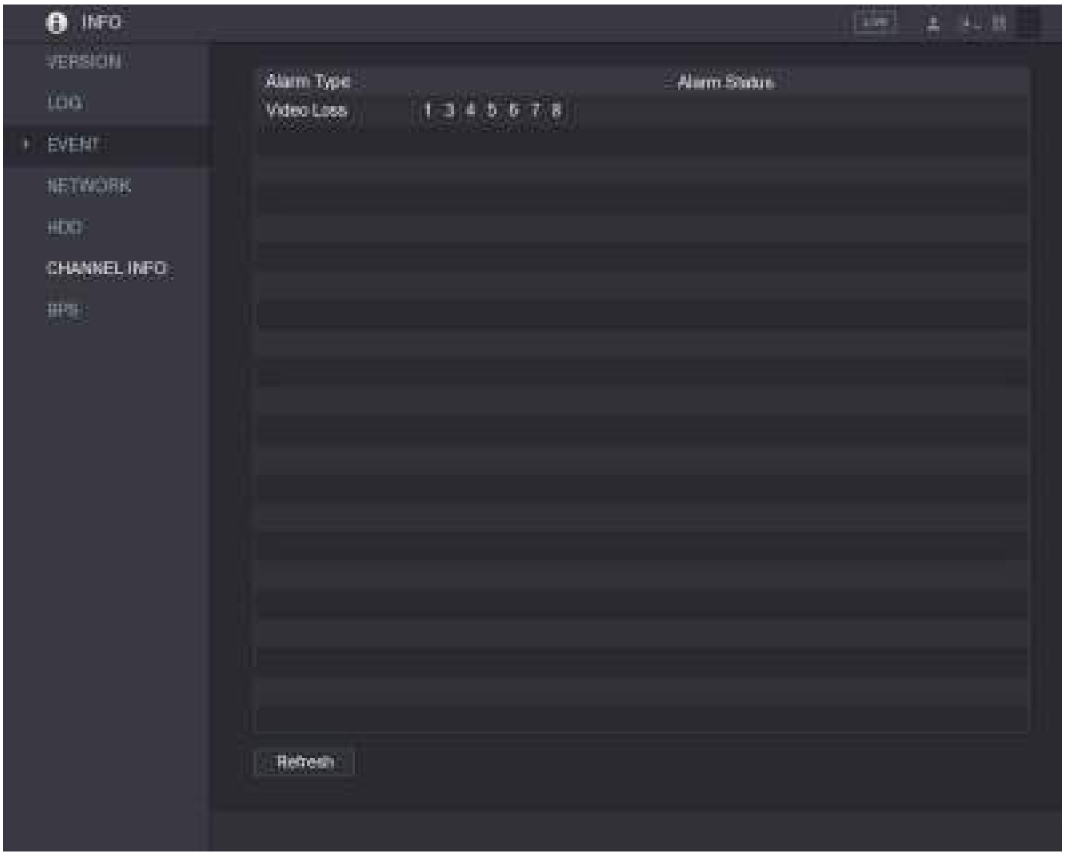
- Click **Details** or double-click the log that you want to view, the **Detailed Information** page is displayed. Click **Next** or **Previous** to view more log information.
- Click **Backup** to back up the logs into the USB storage device.
- Click **Clear** to remove all logs.

5.21.3 Viewing Event Information

You can view the event information of the Device and channel.

Select **Main Menu > INFO > EVENT**, the **EVENT** page is displayed.

Figure 5-353 Event



Alarm Type	Alarm Status
Video Loss	1 3 4 5 6 7 8

5.21.4 Viewing Network Information

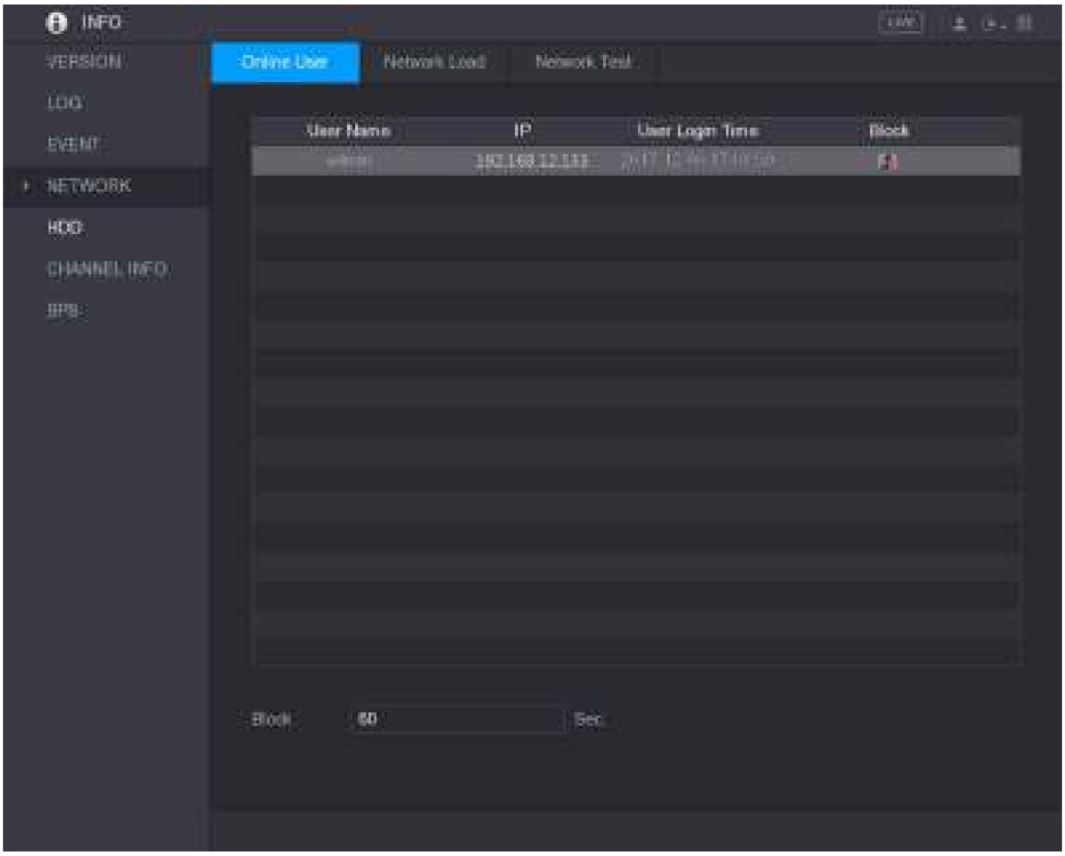
You can view the online users, network data transmission details, and test network. For details about testing network, see "5.15.2.1 Testing the Network."

5.21.4.1 Viewing Online Users

You can view the online user information and block any user for a period of time.

Select **Main Menu > INFO > NETWORK > Online users**, the **Online users** page is displayed.

Figure 5-354 Online user



User Name	IP	User Login Time	Block
admin	192.168.12.111	[illegible]	

Block 60 Sec.

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.

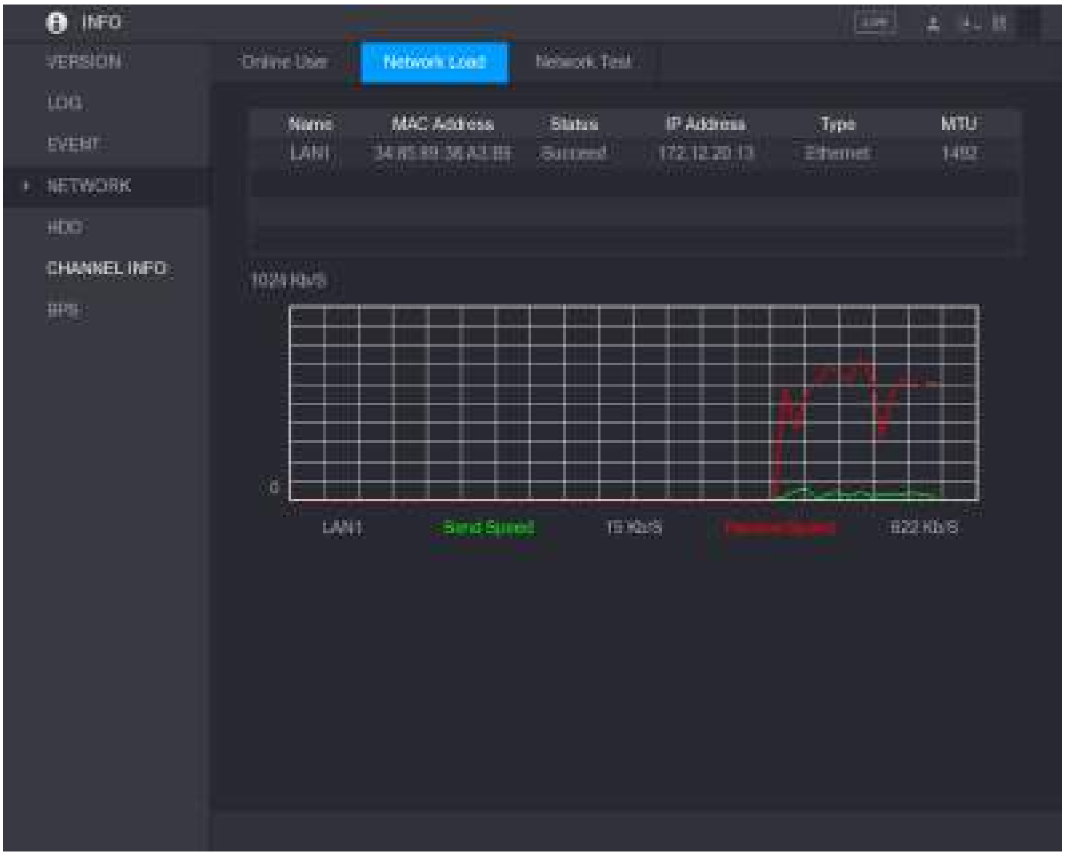
The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

5.21.4.2 Viewing the Network Load

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

Step 1 Select **Main Menu > INFO > NETWORK > Network Load**.

Figure 5-355 Network load



Name	MAC Address	Status	IP Address	Type	MTU
LAN1	34:85:89:36:A3:B8	Succeed	172.12.20.13	Ethernet	1492

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.

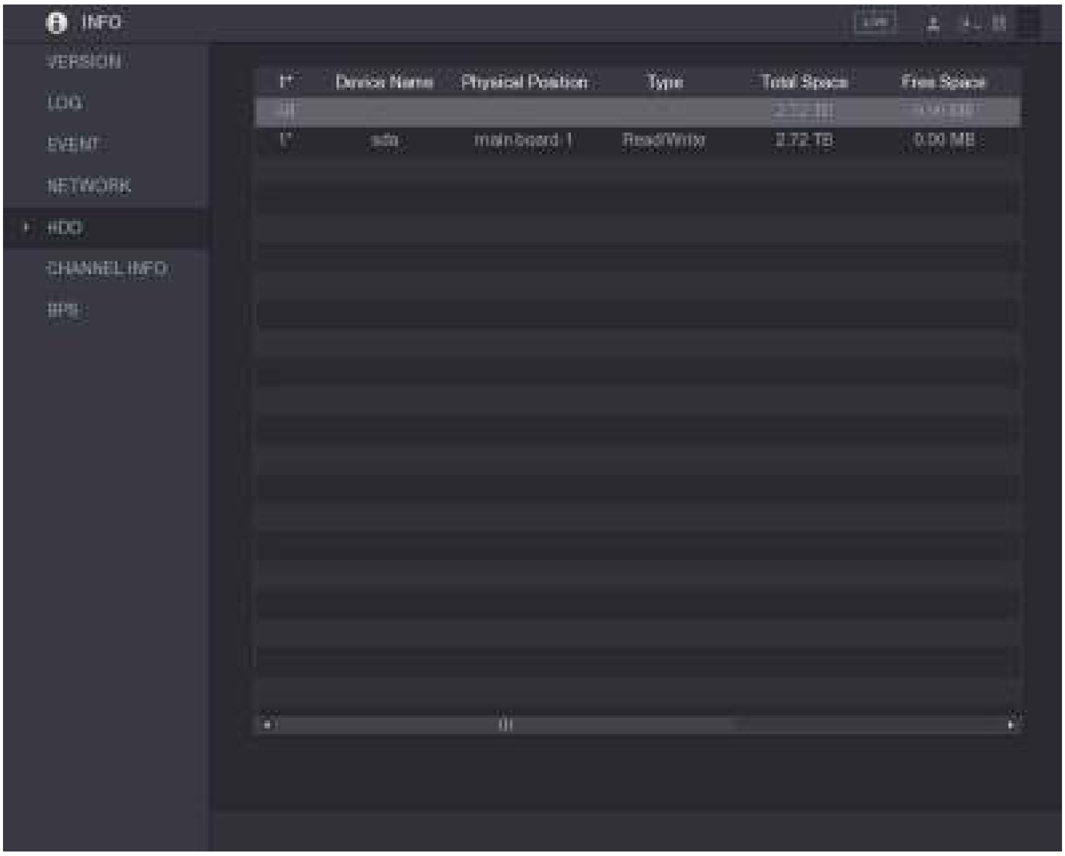
- The default display is LAN1 load.
- Only one LAN load can be displayed at one time.

5.21.5 Viewing HDD Information

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

Select **Main Menu > INFO > HDD**, the **HDD** page is displayed.

Figure 5-356 HDD



1*	Device Name	Physical Position	Type	Total Space	Free Space
All				2.72 TB	0.00 MB
1*	sda	main board 1	Read/Write	2.72 TB	0.00 MB

Table 5-74 HDD parameters

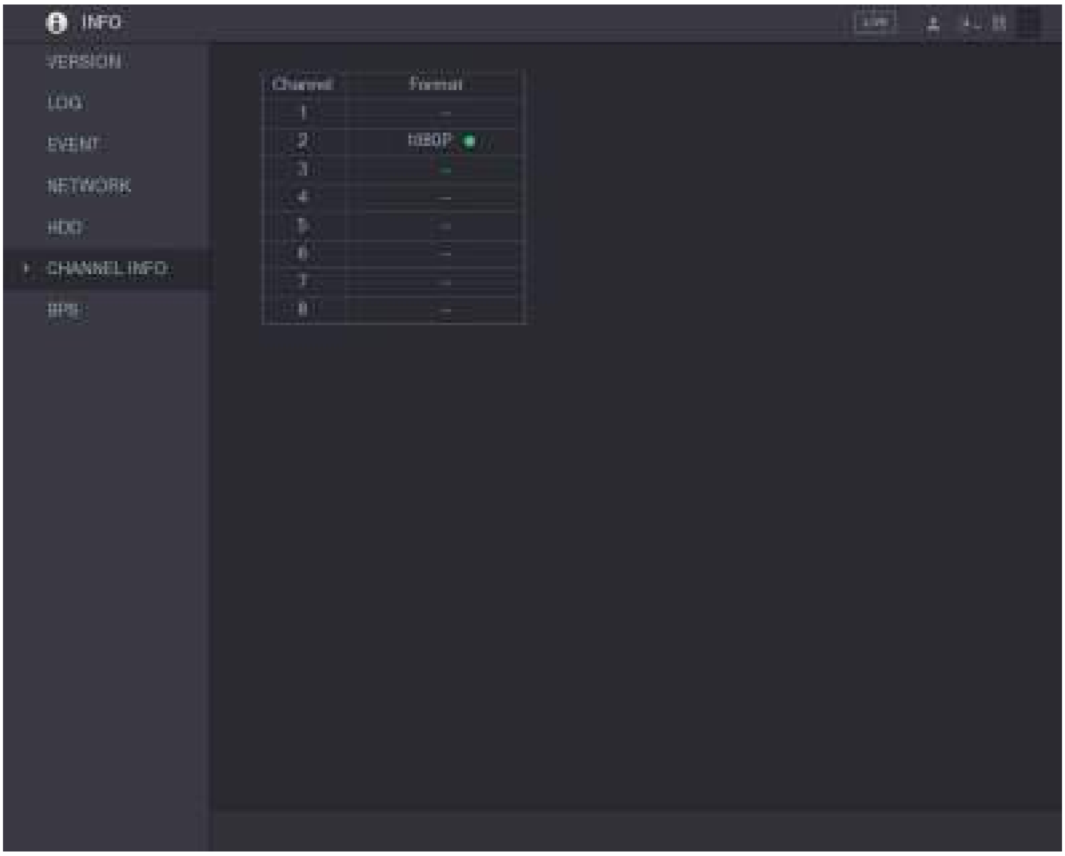
Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Type	Indicates HDD type.
Total Space	Indicates the total capacity of HDD.
Free Space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

5.21.6 Viewing Channel Information

You can view the camera information connected to each channel.

Select **Main Menu** > **INFO** > **CHANNEL INFO**, the **CHANNEL INFO** page is displayed.

Figure 5-357 Channel information



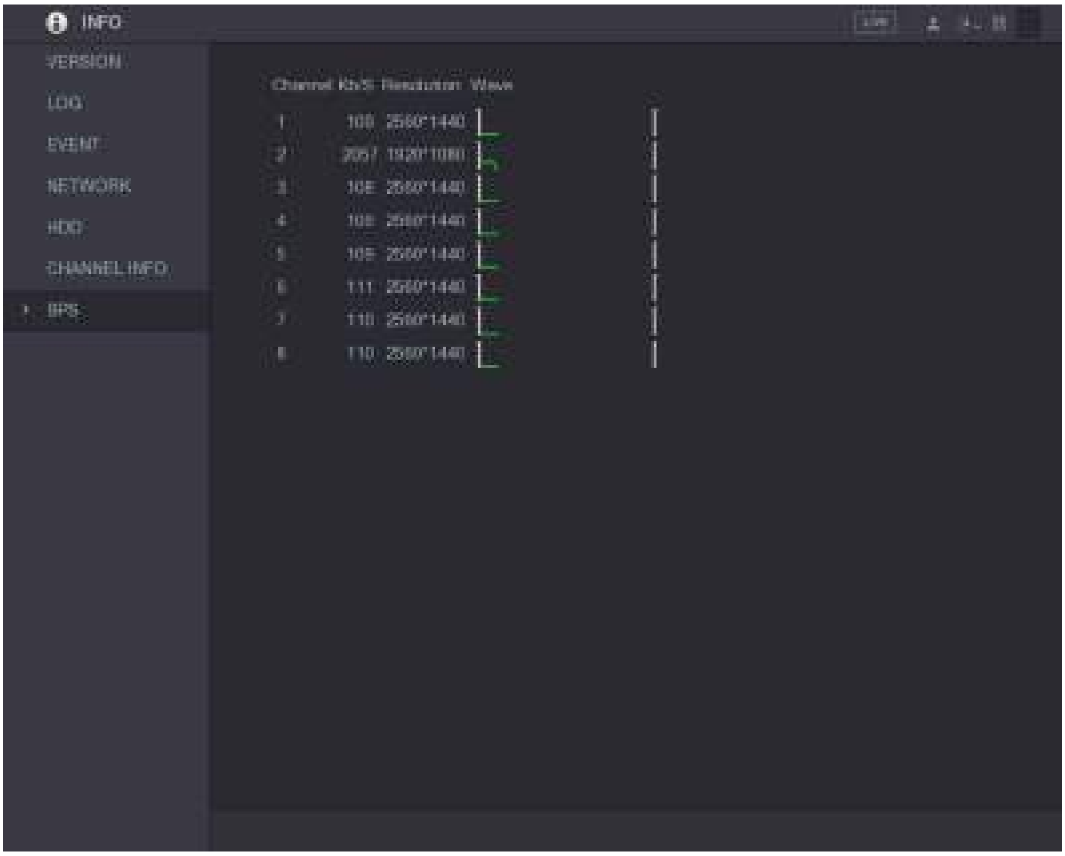
Channel	Format
1	--
2	1080P ●
3	--
4	--
5	--
6	--
7	--
8	--

5.21.7 Viewing Data Stream Information

You can view the real-time data stream rate and resolution of each channel.

Select **Main Menu** > **INFO** > **BPS**, the **BPS** page is displayed.

Figure 5-358 BPS



Channel	Kb/S	Resolution	Wave
1	100	2560*1440	
2	2057	1920*1080	
3	108	2560*1440	
4	108	2560*1440	
5	108	2560*1440	
6	111	2560*1440	
7	110	2560*1440	
8	110	2560*1440	

5.22 Logging out of the Device

On the top right of the Main Menu page or on any page after you have entered the Main Menu, click ⇨ ▾.

- Select **Logout**, you will log out the device.
- Select **Reboot**, the Device will be rebooted.
- Select **Shutdown**, the Device will be turned off.

6 Web Operations

- The pages in the Manual are used for introducing the operations and only for reference. The actual page might be different dependent on the model you purchased. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- 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 log in to the device. For detailed information, refer to Smart PSS user's manual.

6.1 Connecting to Network

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

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 "5.1.4.4 Configuring Network Settings."

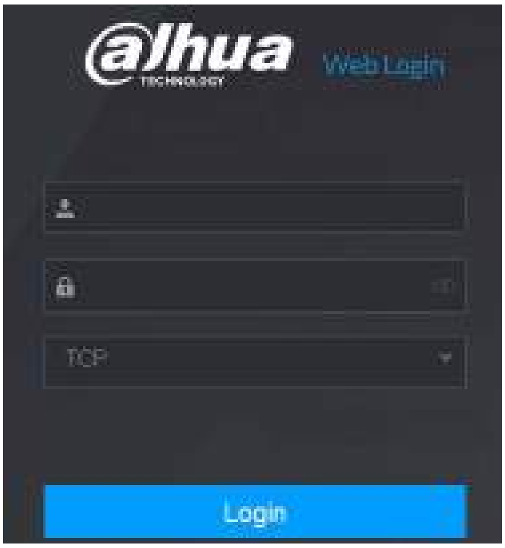
Step 3 On your PC, check the network connection of the Device by using "ping ***.***.***.***". Usually the return value of TTL is 255.

6.2 Logging in to the Web

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

The Login in dialog box is displayed.

Figure 6-1 Login



Step 2 Enter the user name and password.

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

Step 3 Click **Login**.

6.3 Introducing Web Main Menu

After you have logged in the web, the main menu is displayed.

Figure 6-2 Main menu

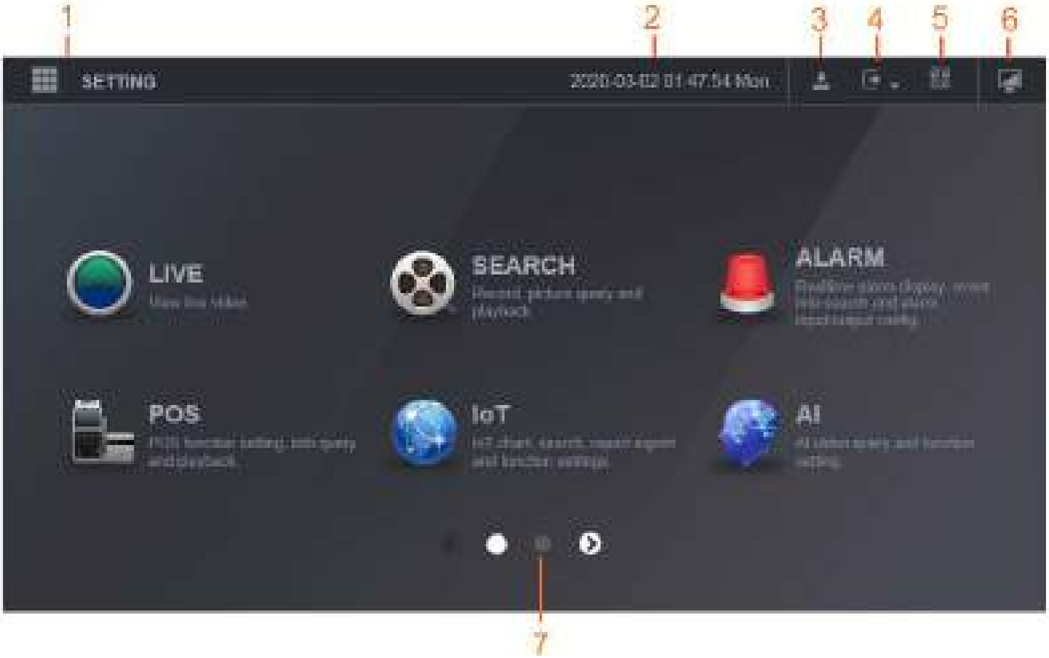

1
2
3
4
5
6
SETTING
2020-03-02 01:47:54 Mon
LIVE
View live Video
SEARCH
Record, picture query and playback
ALARM
POS
POS function setting, both query and playback
IoT
IoT chart, search, report export and function settings
AI
AI video query and function setting
7

Table 6-1 Main menu description

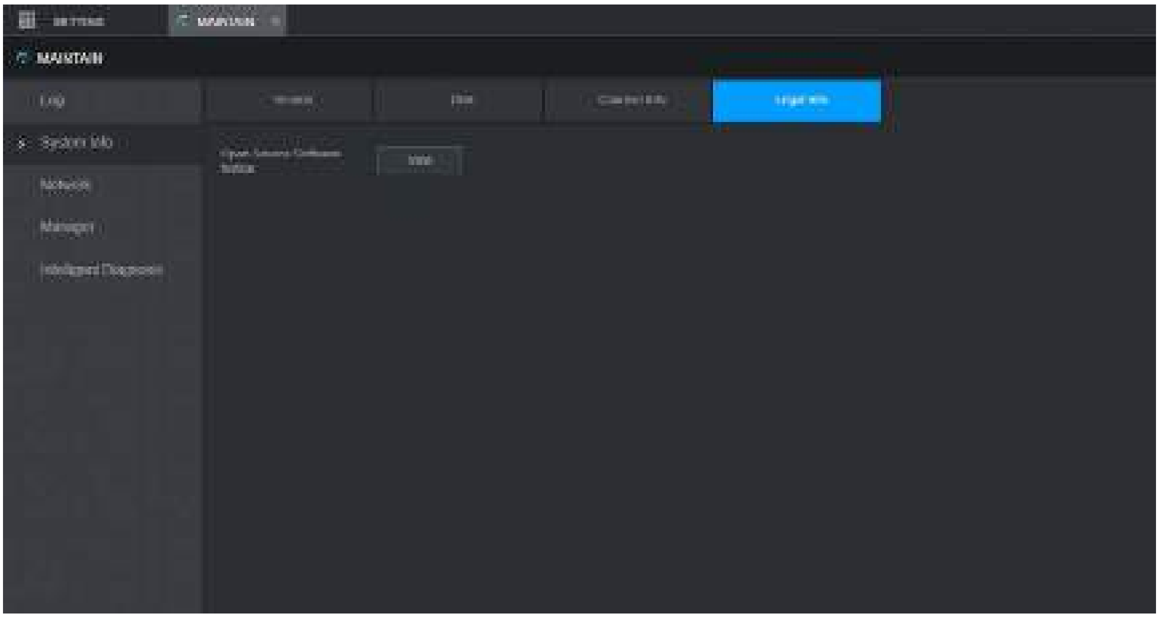
No.	Icon	Description
1	▦	Includes configuration menu through which you can configure camera settings, network settings, storage settings, system settings, account settings, and view information.
2	None	Displays system date and time.
3	👤	When you point to 👤, the current user account is displayed.
4	⇥ ▾	Click ⇥ ▾, select **Logout**, **Reboot**, or **Shutdown** according to your actual situation.

No.	Icon	Description
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, please refer to the P2P operation manual. You can also configure P2P function in the local configurations. See "5.1.4.5 Configuring P2P Settings."
6	🖥	Displays the web main menu.
7	None	Includes eight function tiles: **LIVE**, **VIDEO**, **ALARM**, **IoT**, **AI**, **BACKUP**, **DISPLAY**, and **AUDIO**. Click each tile to open the configuration page 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. ● **VIDEO**: Search for and play back the recorded video saved on the Device. ● **ALARM**: Search for alarm information and configure alarm event actions. ● **AI**: Configure face detection, face recognition, and IVS functions. ● **IoT**: You can view, search and export the temperature and humidity data of camera and configure the alarm event settings. ● **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.

6.4 Viewing Open-source Software Notice

Log in to the web, select **MAINTAIN** > **System Info** > **Legal Info**, and then click **View** to view open-source software notice.

Figure 6-3 Legal information



7 FAQ

1. **DVR cannot boot up properly.**

   There are following possibilities:

   - Input power is not correct.
   - Power connection is not correct.
   - Power switch button is damaged.
   - Program upgrade is wrong.
   - HDD malfunction or something wrong with HDD jumper configuration.
   - Seagate DB35.1, DB35.2, SV35 or Maxtor 17-g has compatibility problem. Upgrade to the latest version to solve this problem.
   - Front panel error.
   - Main board is damaged.

2. **DVR frequently shuts down or stops running.**

   There are following possibilities:

   - Input voltage is not stable or it is too low.
   - HDD malfunction or something wrong with jumper configuration.
   - Button power is not enough.
   - Front video signal is not stable.
   - Working environment is too harsh, too much dust.
   - Hardware malfunction.

3. **Hard disk cannot be detected.**

   There are following possibilities:

   - HDD is broken.
   - HDD jumper is damaged.
   - HDD cable connection is loose.
   - Main board SATA port is broken.

4. There is no video output whether it is one-channel, multiple-channel or all-channel output.

There are following possibilities:

- Program is not compatible. Upgrade to the latest version.
- Brightness is 0. Restore factory default setup.
- There is no video input signal or it is too weak.
- Check privacy mask setup or your screen saver.
- DVR hardware malfunctions.

5. Real-time video color is distorted.

There are following possibilities:

- When using BNC output, NTSC and PAL setup is not correct. The real-time video becomes black and white.
- DVR and monitor resistance is not compatible.
- Video transmission is too long or degrading is too huge.
- DVR color or brightness setup is not correct.

6. Cannot search local records.

There are following possibilities:

- HDD jumper is damaged.
- HDD is broken.
- Upgraded program is not compatible.
- The recorded file has been overwritten.
- Record function has been disabled.

7. Video is distorted when searching local records.

There are following possibilities:

- Video quality setup is too low.
- Program read error, bit data is too small. There is mosaic in the full screen. Restart the DVR to solve this problem.
- HDD data jumper error.
- HDD malfunction.
- DVR hardware malfunctions.

8. No audio under monitor state.

There are following possibilities:

- It is not a power picker.
- It is not a power acoustics.
- Audio cable is damaged.
- DVR hardware malfunctions.

9. There is audio under monitor state but no audio under playback state.

There are following possibilities:

- Setup is not correct. Enable audio function.
- Corresponding channel has no video input. Playback is not continuous when the screen is blue.

10. System time is not correct.

There are following possibilities:

- Setup is not correct.
- Battery contact is not correct or voltage is too low.
- Crystal oscillator is broken.

11. Cannot control PTZ on DVR.

There are following possibilities:

- 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 DVR protocol is not compatible.
- PTZ decoder and DVR 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.

12. Motion detection function does not work.

There are following possibilities:

- Period setup is not correct.
- Motion detection zone setup is not correct.
- Sensitivity is too low.

- For some versions, there is hardware limit.

13. Cannot log in client-end or web.

There are following possibilities:

- For Windows 98 or Windows ME user, update your system to Windows 2000 sp4. Or you can install client-end software of lower version. Note right now, our DVR 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 user name is invalid.
- Client-end is not compatible with DVR program.

14. There is only mosaic no video when preview or playback video file remotely.

There are following possibilities:

- Network fluency is not good.
- Client-end resources are limit.
- There is multiple-cast group setup in DVR. This mode can result in mosaic. Usually we do not recommend this mode.
- There is privacy mask or channel protection setup.
- Current user has no right to monitor.
- DVR local video output quality is not good.

15. Network connection is not stable.

There are following possibilities:

- Network is not stable.
- IP address conflict.
- MAC address conflict.
- PC or DVR network card is not good.

16. Burn error /USB back error.

There are following possibilities:

- Burner and DVR 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.

17. Keyboard cannot control DVR

There are following possibilities:

- DVR 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.

18. Alarm signal cannot be disarmed.

There are following possibilities:

- 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.

19. Alarm function is null.

There are following possibilities:

- 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.

20. Remote control does not work.

There are following possibilities:

- Remote control address is not correct.
- Distance is too far or control angle is too small.
- Remote control battery power is low.
- Remote control is damaged or DVR front panel is damaged.

21. Record storage period is not enough.

There are following possibilities:

- 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.

22. Cannot playback the downloaded file.

There are following possibilities:

- 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.

23. 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.

24. When I login via HTTPS, a dialogue says the certificate for this website is for other address.

Create server certificate again.

25. When I login via HTTPS, a dialogue says the certificate is not trusted.

Download root certificate again.

26. When I login via HTTPS, a dialogue says the certificate has expired or is not valid yet.

Make sure your PC time is the same as the device time.

27. I connect the general analog camera to the device, there is no video output.

There are following possibilities:

- Check camera power supplying, data cable connection and other items.
- This series device does not support the analog camera of all brands. Make sure the device supports general standard definition analog camera.

28. I connect the standard definition analog camera or the coaxial camera to the device, there is no video output.

There are following possibilities:

- Check camera power supplying, or camera data cable connection.

- For the product supports analog standard definition camera/HD camera, you need to go to the **Main Menu > CAMERA > CHANNEL TYPE** to select corresponding channel type and then restart the DVR.

29. I cannot connect to the IP channel.

There are following possibilities:

- Check the camera is online or not.
- Check IP channel setup is right or not (such as IP address, user name, password, connection protocol, and port number).
- The camera has set the allowlist (Only the specified devices can connect to the camera).

30. After I connected to the IP channel, the one-window output is OK, but there is no multiple-window output.

There are following possibilities:

- Check the sub stream of the camera has been enabled or not.
- Check the sub stream type of the camera is H.264 or not.
- Check the device supports camera sub stream resolution or not (such as 960H, D1, and HD1).

31. After I connected to the IP channel, the multiple-window output is OK, but there is no one-window output.

There are following possibilities:

- Check there is video from the IP channel or not. Go to the **Main Menu > INFO > BPS** to view bit stream real-time information.
- Check the main stream of the camera has been enabled or not.
- Check the main stream type of the camera is H.264 or not.
- Check the device supports camera main stream resolution or not (such as 960H, D1, and HD1).
- Check camera network transmission has reached the threshold or not. Check the online user of the camera.

32. After I connected to the IP channel, there is no video output in the one-window or the multiple-window mode. But I can see there is bit stream.

There are following possibilities:

- Check the main stream/sub stream type of the camera is H.264 or not.
- Check the device supports camera main stream/sub stream resolution or not (such as 1080P, 720P, 960H, D1, and HD1).
- Check the camera setup. Make sure It supports the products of other manufacturers.

33. DDNS registration failed or cannot access the device domain name.

There are following possibilities:

- Check the device is connected to the WAN. Check the device has got the IP address if the PPPoE can dial. If there is a router, check the router to make sure the device IP is online.
- Check the corresponding protocol of the DDNS is enabled. Check the DDNS function is OK or not.
- Check DNS setup is right or not. Default Google DNS server is 8.8.8.8, 8.8.5.5. You can use different DNS provided by your ISP.

34. I cannot use the P2P function on my cell phone or the web.

There are following possibilities:

- Check the device P2P function is enabled or not. (Main menu->Setting->Network->P2P)
- Check the device is in the WAN or not.
- Check cell phone P2P login mode is right or not.

- It is the specified device P2P login port or not when you are using P2P client.
- Check user name or password is right or not.
- Check P2P SN is right or not. You can use the cell phone to scan the QR code on the device P2P page (**Main Menu > Network > P2P**), or you can use the version information of the WEB to confirm. (For some previous series products, the device SN is the main board SN, it might result in error.)

35. I connect the standard definition camera to the device, there is no video output.

There are following possibilities:

- Check the DVR supports standard definition signal or not. Only some series product supports analog standard definition signal, coaxial signal input.
- Check channel type is right or not. For the product supports analog standard definition camera/HD camera, you need to go to the **Main Menu > CAMERA > CHANNEL TYPE** to select corresponding channel type (such as analog) and then restart the DVR. In this way, the DVR can recognize the analog standard definition.
- Check camera power supplying, or camera data cable connection.

36. I cannot connect to the IP camera.

There are following possibilities:

- Check DVR supports IP channel or not. Only some series products support A/D switch function, it can switch analog channel to the IP channel to connect to the IP camera. From **Main Menu > CAMERA > CHANNEL TYPE**, select the last channel to switch to the IP channel. Some series product products support IP channel extension, it supports N+N mode.
- Check the IPC and the DVR is connected or not. Go to the **Main Menu > CAMERA > REGISTRATION** to search to view the IP camera is online or not. Or you can go to the **Main Menu > INFO > NETWORK > Network Test**, you can input IP camera IP address and then click the Test button to check you can connect to the IP camera or not.
- Check IP channel setup is right or not (such as IP address, manufacturer, port, user name, password, and remote channel number).

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 front panel 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 Glossary

The abbreviations in this glossary are related to the Manual.

Appendix Table 1-1 Glossary

Abbreviations	Full term
BNC	Bayonet Nut Connector
CBR	Constant Bit Rate
CIF	Common Intermediate Format
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DST	Daylight Saving Time
DVR	Digital Video Recorder
FTP	File Transfer Protocol
HDD	Hard Disk Drive
HDMI	High Definition Multimedia Interface
HTTP	Hyper Text Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
IVS	Intelligent Video System
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
NTSC	National Television Standards Committee
ONVIF	Open Network Video Interface Forum
PAL	Phase Alteration Line
PAT	Port Address Translation
POS	Point of Sale
PPPoE	Point-to-Point Protocol over Ethernet
PSS	Professional Surveillance Software
PTZ	Pan Tilt Zoom
RCA	Radio Corporation of American
RTSP	Real Time Streaming Protocol
S.M.A.R.T	Self-Monitoring-Analysis and Reporting Technology
SATA	Serial Advanced Technology Attachment
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPnP	Universal Plug and Play

Abbreviations	Full term
VBR	Variable Bit Rate
VGA	Video Graphics Array
WAN	Wide Area Network

Appendix 2 HDD Capacity Calculation

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

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

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

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

Step 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 MB.

Formula (2): $m_i = q_i \times h_i \times D_i$

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

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

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

In the formula: c means total number of channels in one DVR

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

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

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

You can refer to the following table for the file size in one hour per channel. (All the data listed below are for reference only.)

Appendix Table 2-1 HDD capacity calculation

Bit Stream Size (max)	File Size	Bit Stream Size (max)	File Size
96 Kbps	42 MB	128 Kbps	56 MB
160 Kbps	70 MB	192 Kbps	84 MB
224 Kbps	98 MB	256 Kbps	112 MB

Bit Stream Size (max)	File Size	Bit Stream Size (max)	File Size
320 Kbps	140 MB	384 Kbps	168 MB
448 Kbps	196 MB	512 Kbps	225 MB
640 Kbps	281 MB	768 Kbps	337 MB
896 Kbps	393 MB	1024 Kbps	450 MB
1280 Kbps	562 MB	1536 Kbps	675 MB
1792 Kbps	787 MB	2048 Kbps	900 MB

Appendix 3 Compatible Backup Devices

Appendix 3.1 Compatible USB List

Appendix Table 3-1 Compatible USB

Manufacturer	Model	Capacity
Sandisk	Cruzer Micro	512 MB
Sandisk	Cruzer Micro	1 GB
Sandisk	Cruzer Micro	2 GB
Sandisk	Cruzer Freedom	256 MB
Sandisk	Cruzer Freedom	512 MB
Sandisk	Cruzer Freedom	1 GB
Sandisk	Cruzer Freedom	2 GB
Kingston	DataTravelerⅡ	1 GB
Kingston	DataTravelerⅡ	2 GB
Kingston	DataTraveler	1 GB
Kingston	DataTraveler	2 GB
Maxell	USB Flash Stick	128 MB
Maxell	USB Flash Stick	256 MB
Maxell	USB Flash Stick	512 MB
Maxell	USB Flash Stick	1 GB
Maxell	USB Flash Stick	2 GB
Kingax	Super Stick	128 MB
Kingax	Super Stick	256 MB
Kingax	Super Stick	512 MB
Kingax	Super Stick	1 GB
Kingax	Super Stick	2 GB
Netac	U210	128 MB
Netac	U210	256 MB
Netac	U210	512 MB
Netac	U210	1 GB
Netac	U210	2 GB
Netac	U208	4 GB
Teclast	Ti Cool	128 MB
Teclast	Ti Cool	256 MB
Teclast	Ti Cool	512 MB
Teclast	Ti Cool	1 GB
Sandisk	Cruzer Micro	2 GB
Sandisk	Cruzer Micro	8 GB
Sandisk	Ti Cool	2 GB

Manufacturer	Model	Capacity
Sandisk	Hongjiao	4 GB
Lexar	Lexar	256 MB
Kingston	Data Traveler	1 GB
Kingston	Data Traveler	16 GB
Kingston	Data Traveler	32 GB
Aigo	L8315	16 GB
Sandisk	250	16 GB
Kingston	Data Traveler Locker+	32 GB
Netac	U228	8 GB

Appendix 3.2 Compatible SD Card List

Appendix Table 3-2 Compatible SD card

Manufacturer	Standard	Capacity	Card type
Transcend	SDHC6	16 GB	Big
Kingston	SDHC4	4 GB	Big
Kingston	SD	2 GB	Big
Kingston	SD	1 GB	Big
Sandisk	SDHC2	8 GB	Small
Sandisk	SD	1 GB	Small

Appendix 3.3 Compatible Portable HDD List

Appendix Table 3-3 Compatible portable HDD

Manufacturer	Model	Capacity
YDStar	YDstar HDD box	40 GB
Netac	Netac	80 GB
Iomega	Iomega RPHD-CG" RNAJ50U287	250 GB
WD Elements	WCAVY1205901	1.5 TB
Newsmy	Liangjian	320 GB
WD Elements	WDBAAR5000ABK-00	500 GB
WD Elements	WDBAAU0015HBK-00	1.5 TB
Seagate	FreeAgent Go(ST905003F)	500 GB
Aigo	H8169	500 GB

Appendix 3.4 Compatible USB DVD List

Appendix Table 3-4 Compatible USB DVD

Manufacturer	Model
Samsung	SE-S084
BenQ	LD2000-2K4

Appendix 3.5 Compatible SATA DVD List

Manufacturer	Model
LG	GH22NS30
Samsung	TS-H653 Ver.A
Samsung	TS-H653 Ver.F
Samsung	SH-224BB/CHXH
SONY	DRU-V200S
SONY	DRU-845S
SONY	AW-G170S
Pioneer	DVR-217CH

Appendix 3.6 Compatible SATA HDD List

Upgrade the DVR firmware to latest version to ensure the accuracy of the table below. Here we recommend HDD of 500 GB to 4 TB capacity.

Appendix Table 3-5 Compatible SATA HDD

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	Video 3.5	ST1000VM002	1 TB	SATA
Seagate	Video 3.5	ST2000VM003	2 TB	SATA
Seagate	Video 3.5	ST3000VM002	3 TB	SATA
Seagate	Video 3.5	ST4000VM000	4 TB	SATA
Seagate	SV35	ST1000VX000	1 TB	SATA
Seagate	SV35	ST2000VX000	2 TB	SATA
Seagate	SV35	ST3000VX000	3 TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST1000VX002	1 TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST2000VX004	2 TB	SATA
Seagate	SV35 (Support HDD data recovery offered by Seagate)	ST3000VX004	3 TB	SATA
Seagate	SkyHawk HDD	ST1000VX001	1 TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	SkyHawk HDD	ST1000VX005	1 TB	SATA
Seagate	SkyHawk HDD	ST2000VX003	2 TB	SATA
Seagate	SkyHawk HDD	ST2000VX008	2 TB	SATA
Seagate	SkyHawk HDD	ST3000VX006	3 TB	SATA
Seagate	SkyHawk HDD	ST3000VX010	3 TB	SATA
Seagate	SkyHawk HDD	ST4000VX000	4 TB	SATA
Seagate	SkyHawk HDD	ST4000VX007	4 TB	SATA
Seagate	SkyHawk HDD	ST5000VX0001	5 TB	SATA
Seagate	SkyHawk HDD	ST6000VX0001	6 TB	SATA
Seagate	SkyHawk HDD	ST6000VX0023	6 TB	SATA
Seagate	SkyHawk HDD	ST6000VX0003	6 TB	SATA
Seagate	SkyHawk HDD	ST8000VX0002	8 TB	SATA
Seagate	SkyHawk HDD	ST8000VX0022	8 TB	SATA
Seagate	SkyHawk HDD	ST100000VX0004	10 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST1000VX003	1 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST2000VX005	2 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST3000VX005	3 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST4000VX002	4 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST5000VX0011	5 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST6000VX0011	6 TB	SATA
Seagate	SkyHawk HDD (Support HDD data recovery offered by Seagate)	ST8000VX0012	8 TB	SATA
WD	WD Green	WD10EURX (EOL)	1 TB	SATA
WD	WD Green	WD20EURX (EOL)	2 TB	SATA
WD	WD Green	WD30EURX (EOL)	3 TB	SATA
WD	WD Green	WD40EURX (EOL)	4 TB	SATA
WD	WD Purple	WD10PURX	1 TB	SATA
WD	WD Purple	WD20PURX	2 TB	SATA
WD	WD Purple	WD30PURX	3 TB	SATA
WD	WD Purple	WD40PURX	4 TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
WD	WD Purple	WD50PURX	5 TB	SATA
WD	WD Purple	WD60PURX	6 TB	SATA
WD	WD Purple	WD80PUZX	8 TB	SATA
WD	WD Purple	WD10PURZ	1 TB	SATA
WD	WD Purple	WD20PURZ	2 TB	SATA
WD	WD Purple	WD30PURZ	3 TB	SATA
WD	WD Purple	WD40PURZ	4 TB	SATA
WD	WD Purple	WD50PURZ	5 TB	SATA
WD	WD Purple	WD60PURZ	6 TB	SATA
WD	WD Purple	WD80PURZ	8 TB	SATA
WD	WD Purple	WD4NPURX	4 TB	SATA
WD	WD Purple	WD6NPURX	6 TB	SATA
TOSHIBA	Mars	DT01ABA100V	1 TB	SATA
TOSHIBA	Mars	DT01ABA200V	2 TB	SATA
TOSHIBA	Mars	DT01ABA300V	3 TB	SATA
TOSHIBA	Sonance	MD03ACA200V	2 TB	SATA
TOSHIBA	Sonance	MD03ACA300V	3 TB	SATA
TOSHIBA	Sonance	MD03ACA400V	4 TB	SATA
TOSHIBA	Sonance	MD04ABA400V	4 TB	SATA
TOSHIBA	Sonance	MD04ABA500V	5 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST1000NM0033	1 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST2000NM0033	2 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST3000NM0033	3 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST4000NM0033	4 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST1000NM0055	1 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST2000NM0055	2 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST3000NM0005	3 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST4000NM0035	4 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST6000NM0115	6 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST8000NM0055	8 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST10000NM0016	10 TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
Seagate	Constellation ES series (SATA interface)	ST4000NM0024	4 TB	SATA
Seagate	Constellation ES series (SATA interface)	ST6000NM0024	6 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST1000NM0023	1 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST2000NM0023	2 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST3000NM0023	3 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST4000NM0023	4 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0014	6 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST1000NM0045	1 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST2000NM0045	2 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST3000NM0025	3 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST4000NM0025	4 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0095	6 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST6000NM0034	6 TB	SATA
Seagate	Constellation ES series (SAS interface)	ST8000NM0075	8 TB	SATA
WD	WD RE series (SATA interface)	WD1003FBYZ	1 TB	SATA
WD	WD RE series (SATA interface)	WD1004FBYZ (replace WD1003FBYZ)	1 TB	SATA
WD	WD RE series (SATA interface)	WD2000FYYZ	2 TB	SATA
WD	WD RE series (SATA interface)	WD2004FBYZ (replace WD2000FYYZ)	2 TB	SATA
WD	WD RE series (SATA interface)	WD3000FYYZ	3 TB	SATA
WD	WD RE series (SATA interface)	WD4000FYYZ	4 TB	SATA
WD	WD (SATA interface)	WD2000F9YZ	2 TB	SATA
WD	WD (SATA interface)	WD3000F9YZ	3 TB	SATA
WD	WD (SATA interface)	WD4000F9YZ	4 TB	SATA
WD	WD (SATA interface)	WD4002FYYZ	4 TB	SATA

Manufacturer	Series	Model	Capacity	Port Mode
WD	WD (SATA interface)	WD6001FSYZ	6 TB	SATA
WD	WD (SATA interface)	WD6002FRYZ	6 TB	SATA
WD	WD (SATA interface)	WD8002FRYZ	8 TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUS724030ALA640	3 TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUS726060ALE610	6 TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUH728060ALE600	6 TB	SATA
HITACHI	Ultrastar series (SATA interface)	HUH728080ALE600	8 TB	SATA
HITACHI	Ultrastar series (SAS interface)	HUS726020AL5210	2 TB	SATA
HITACHI	Ultrastar series (SAS interface)	HUS726040AL5210	4 TB	SATA
HITACHI	Ultrastar series (SAS interface)	HUS726060AL5210	6 TB	SATA
Seagate	Pipeline HD Mini	ST320VT000	320 GB	SATA
Seagate	Pipeline HD Mini	ST500VT000	500 GB	SATA
Seagate	Pipeline HD Mini	ST2000LM003 (EOL)	2 TB	SATA
TOSHIBA	2.5-inch PC series	MQ01ABD050V	500 GB	SATA
TOSHIBA	2.5-inch PC series	MQ01ABD100V	1 TB	SATA
SAMSUNG	HN-M101MBB	HN-M101MBB (EOL)	1 TB	SATA
Seagate	2.5-inch enterprise series	ST1000NX0313	1 TB	SATA
Seagate	2.5-inch enterprise series	ST2000NX0253	2 TB	SATA

Appendix 4 Compatible CD/DVD Burner List

Upgrade the DVR firmware to latest version to ensure the accuracy of the table below. And you can use the USB cable with the model recommended to set USB burner.

Appendix Table 4-1 Compatible CD/DVD burner

Manufacturer	Model	Port Type	Type
Sony	DRX-S50U	USB	DVD-RW
Sony	DRX-S70U	USB	DVD-RW
Sony	AW-G170S	SATA	DVD-RW
Samsung	TS-H653A	SATA	DVD-RW
Panasonic	SW-9588-C	SATA	DVD-RW
Sony	DRX-S50U	USB	DVD-RW
BenQ	5232WI	USB	DVD-RW

Appendix 5 Compatible Displayer List

Refer to the following table form compatible displayer list.

Appendix Table 5-1 Compatible displayer

Brand	Model	Dimension (Unit: inch)
BENQ (LCD)	ET-0007-TA	19-inch (wide screen)
DELL (LCD)	E178FPc	17-inch
BENQ (LCD)	Q7T4	17-inch
BENQ (LCD)	Q7T3	17-inch
HFNOVO (LCD)	LXB-L17C	17-inch
SANGSUNG (LCD)	225BW	22-inch (wide screen)
HFNOVO (CRT)	LXB-FD17069HB	17-inch
HFNOVO (CRT)	LXB-HF769A	17-inch
HFNOVO(CRT)	LX-GJ556D	17-inch
Samsung (LCD)	2494HS	24-inch
Samsung (LCD)	P2350	23-inch
Samsung (LCD)	P2250	22-inch
Samsung (LCD)	P2370G	23-inch
Samsung (LCD)	2043	20-inch
Samsung (LCD)	2243EW	22-inch
Samsung (LCD)	SMT-1922P	19-inch
Samsung (LCD)	T190	19-inch
Samsung (LCD)	T240	24-inch
LG (LCD)	W1942SP	19-inch
LG (LCD)	W2243S	22-inch
LG (LCD)	W2343T	23-inch
BENQ (LCD)	G900HD	18.5-inch
BENQ (LCD)	G2220HD	22-inch
PHILIPS (LCD)	230E	23-inch
PHILIPS (LCD)	220CW9	23-inch
PHILIPS (LCD)	220BW9	24-inch
PHILIPS (LCD)	220EW9	25-inch

Appendix 6 Compatible Switcher

Appendix Table 6-1 Compatible switcher

Brand	Model	network working mode
D-LinK	DES-1016D	10/100M self-adaptive
D-LinK	DES-1008D	10/100M self-adaptive
Ruijie	RG-S1926S	Five network modes: ● AUTO ● HALF-10M ● FULL-10M ● HALF-100M ● FULL-100M
H3C	H3C-S1024	10/100M self-adaptive
TP-LINK	TL-SF1016	10/100M self-adaptive
TP-LINK	TL-SF1008+	10/100M self-adaptive

Appendix 7 Earthing

Appendix 7.1 What is the Surge

Surge is a short current or voltage change during a very short time. In the circuit, it lasts for microsecond. In a 220 V circuit, the 5KV or 10KV voltage change during a very short time (about microseconds) can be called a surge. The surge comes from two ways: external surge and internal surge.

- The external surge: The external surge mainly comes from the thunder lightning. Or it comes from the voltage change during the on/off operation in the electric power cable.
- The internal surge: The research finds 88% of the surge from the low voltage comes from the internal of the building such as the air conditioning, elevator, electric welding, air compressor, water pump, power button, duplicating machine and other device of inductive load.

The lightning surge is far above the load level the PC or the micro devices can support. In most cases, the surge can result in electric device chip damage, PC error code, accelerating the part aging, data loss and etc. Even when a small 20 horsepower inductive engine boots up or stops, the surge can reach 3000 V to 5000 V, which can adversely affect the electronic devices that use the same distribution box.

To protect the device, you need to evaluate its environment, the lightning affection degree objectively. Because surge has close relationship with the voltage amplitude, frequency, network structure, device voltage-resistance, protection level, ground and etc. The thunder proof work shall be a systematic project, emphasizing the all-round protection (including building, transmission cable, device, ground and etc.). There shall be comprehensive management and the measures shall be scientific, reliable, practical and economic. Considering the high voltage during the inductive thundering, the International Electrotechnical Commission (IEC) standard on the energy absorbing step by step theory and magnitude classification in the protection zone, you need to prepare multiple precaution levels.

You can use the lightning rod, lightning strap or the lightning net to reduce the damage to the building, personal injury or the property.

The lightning protection device can be divided into three types:

- Power lightning arrester: There are 220 V single-phrase lightning arrester and 380 V three-phrase lightning arrester (mainly in parallel connection, sometimes use series connection) You can parallel connect the power lightning arrester in the electric cable to reduce the short-time voltage change and release the surge current. From the BUS to the device, there are usually three levels so that system can reduce the voltage and release the current step by step to remove the thunderstorm energy and guarantee the device safety. You can select the replaceable module type, the terminal connection type and portable socket according to your requirement.
- Signal lightning arrester: This device is mainly used in the PC network, communication system. The connection type is serial connection. Once you connected the signal lightning arrestor with the signal port, it can cut the channel of the thunderstorm to the device, and on the other hand, it can discharge the current to the ground to guarantee the device proper work. The signal lightning arrester has many specifications, and widely used in many devices such as telephone, network, analog communication, digital communication, cable TV and satellite antenna. For all the input port, especially those from the outdoor, you need to install the signal lightning arrester.

- Antenna feed cable lightning arrester: It is suitable for antenna system of the transmitter or the device system to receive the wireless signal. It uses the serial connection too.

Note, when you select the lightning arrester, pay attention to the port type and the earthing reliability. In some important environment, you need to use special shielded cable. Do not parallel connect the thunder proof ground cable with the ground cable of the lightning rod. Make sure they are far enough and grounded respectively.

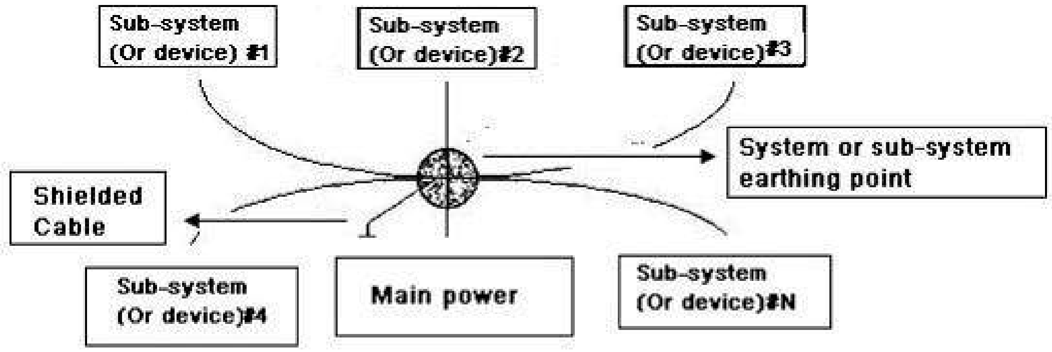
Appendix 7.2 The Earthing Modes

We all know the earthing is the most complicated technology in the electromagnetism compatibility design since there is no systematic theory or module. The earthing has many modes, but the selection depends on the system structure and performance.

The following are some successfully experience from our past work.

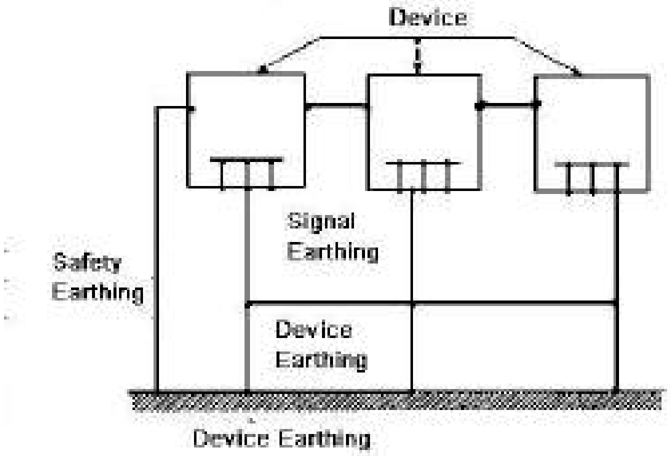
- **One-point ground:** In the following figure you can see there is a one-point ground. This connection provides common point to allow signal to be transmitted in many circuits. If there is no common point, the error signal transmission occurred. In the one-point ground mode, each circuit is just grounded only and they are connected at the same point. Since there is only one common point, there is no circuit and so, there is no interference.

Appendix Figure 7-1 One-point ground



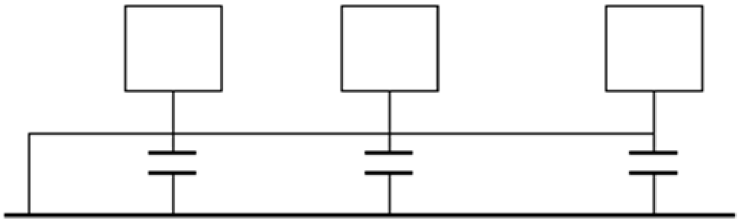
- **Multiple-point ground:** In the following figure, you can see the internal circuit uses the chassis as the common point. While at the same time, all devices chassis use the earthing as the common point. In this connection, the ground structure can provide the lower ground resistance because when there are multiple-point grounds; each ground cable is as short as possible. And the parallel cable connection can reduce the total conductance of the ground conductor. In the high-frequency circuit, you need to use the multiple-point ground mode and each cable needs to connect to the ground. The length shall be less than the 1/20 of the signal wavelength.

Appendix Figure 7-2 Multiple-point ground



- **Mixed ground:** The mix ground consists of the feature of the one-point ground and multiple-point ground. For example, the power in the system needs to use the one-point ground mode while the radio frequency signal requires the multiple-point ground. So, you can use the following figure to earth. For the direct current (DC), the capacitance is open circuit and the circuit is one-point ground. For the radio frequency signal, the capacitance is conducive and the circuit adopts multiple-point ground.

Appendix Figure 7-3 Mixed ground



When connecting devices of huge size (the device physical dimension and connection cable is big comparing with the wave path of existed interference), then there is possibility of interference when the current goes through the chassis and cable. In this situation, the interference circuit path usually lies in the system ground circuit.

When considering the earthing, you need to think about two aspects: One is the system compatibility, and the other is the external interference coupling into the earth circuit, which results in system error. For the external interference is not regular, it is not easy to resolve.

Appendix 7.3 Thunder Proof Ground Method in the Monitor System

- The monitor system shall have sound thunder proof earthing to guarantee personnel safety and device safety.
- The monitor system working ground resistance shall be less than 1 Ω.
- The thunder proof ground shall adopt the special ground cable from the monitor control room to the ground object. The ground cable adopts copper insulation cable or wire and its ground

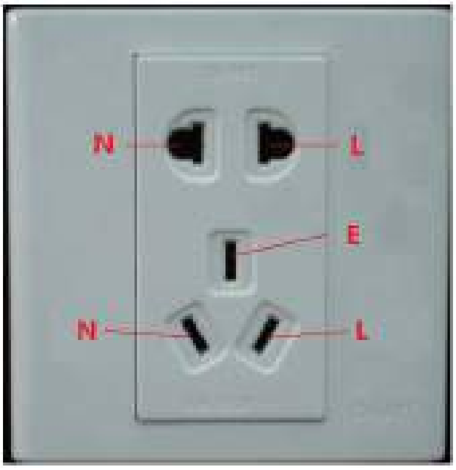
section shall be more than 20mm^2.

- The ground cable of the monitor system cannot short circuit or mixed connected with the strong alternative current cable.
- For all the ground cables from the control room to the monitor system or ground cable of other monitor devices, use the copper resistance soft cable and its section shall be more than 4 mm^2.
- The monitor system usually can adopt the one-point ground.
- Connect the ground end of 3-pin socket in the monitor system to the ground port of the system (protection ground cable)

Appendix 7.4 The Shortcut Way to Check the Electric System by Digital Multimeter

For 220 VAC socket, from the top to the bottom, E (ground cable), N (neutral cable), L (live cable). Refer to the following figure.

Appendix Figure 7-4 Socket



There is a shortcut way to check whether these three cables connection are standard or not (not the accurate check).

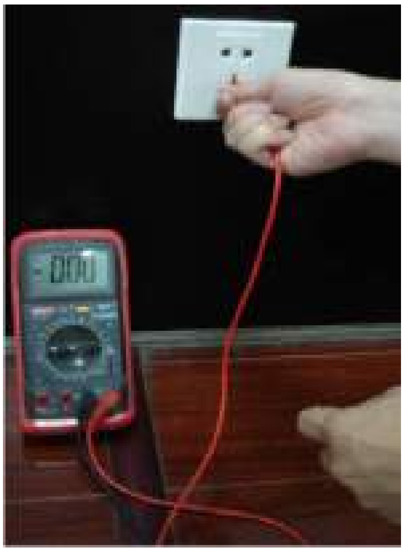
⚠

In the following operations, the multimeter range shall be at 750 V.

For E (earth cable)

Turn the digital multimeter to 750 VAC, use your one hand to hold the metal end, and then the other hand inserts the pen to the E port of the socket. See the following figure. If the multimeter shows 0, then you can see current earth cable connection is standard. If the value is more than 10, then you can know there is inductive current and the earth cable connection is not proper.

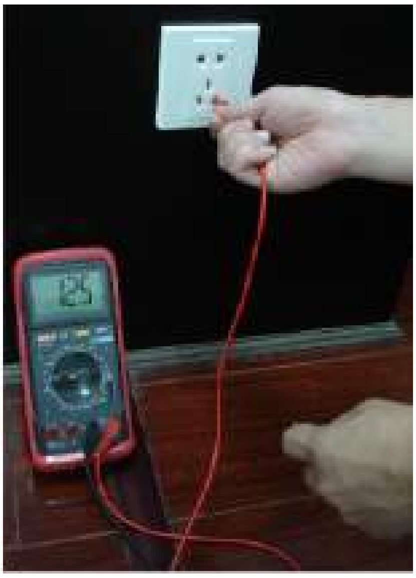
Appendix Figure 7-5 Check earth cable connection



For L (live cable)

Turn the digital multimeter to 750 VAC, use your one hand to hold the metal end, and then the other hand inserts the pen to the L port of the socket. See the following figure. If the multimeter shows 125, then you can see current live cable connection is standard. If the value is less than 60, then you can know current live cable connection is not proper or it is not the live cable at all.

Appendix Figure 7-6 Check live cable connection



For N (Neutral cable)

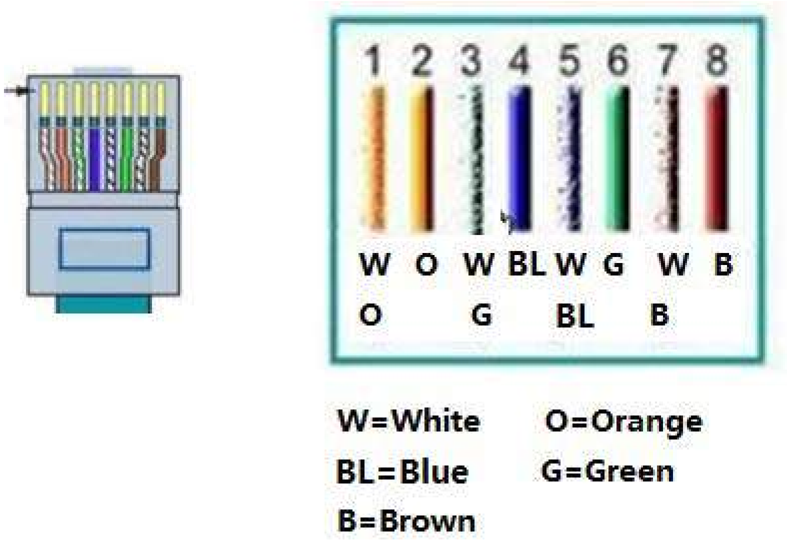
Turn the digital multimeter to 750 VAC, use your one hand to hold the metal end, and then the other hand inserts the pen to the N port of the socket. See the following figure. If the multimeter shows 0, then you can see current N cable connection is standard. If the value is more than 10, then you can see there is inductive current and the neutral cable connection is not proper. If the value is 120, then you can know that you have misconnected the neutral cable to the live cable.

Appendix Figure 7-7 Check neutral cable connection

Appendix 8 RJ45-RS232 Connection Cable Definition

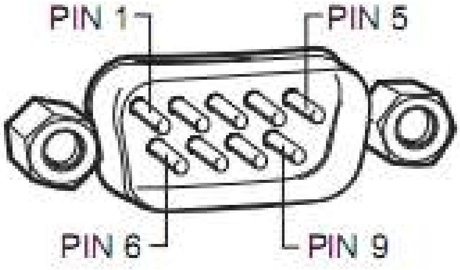
Refer to the following figure for RJ-45 cable definition.

Appendix Figure 8-1 RJ-45



Refer to the following figure for RS-232 pin definition.

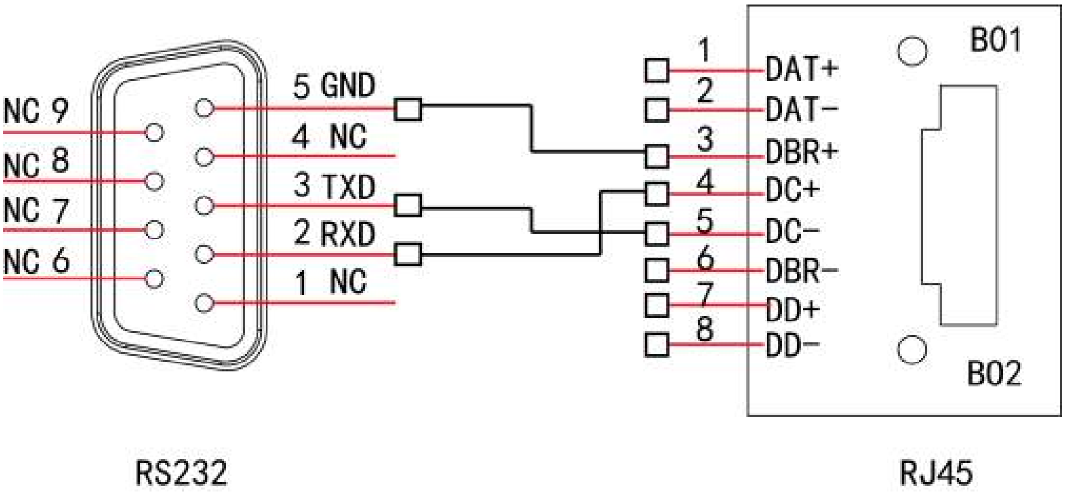
Appendix Figure 8-2 RS-232



Cross Connection

Refer to the following figure for connection information.

Appendix Figure 8-3 Cross connection



Refer to the following table for detailed crossover cable connection information.

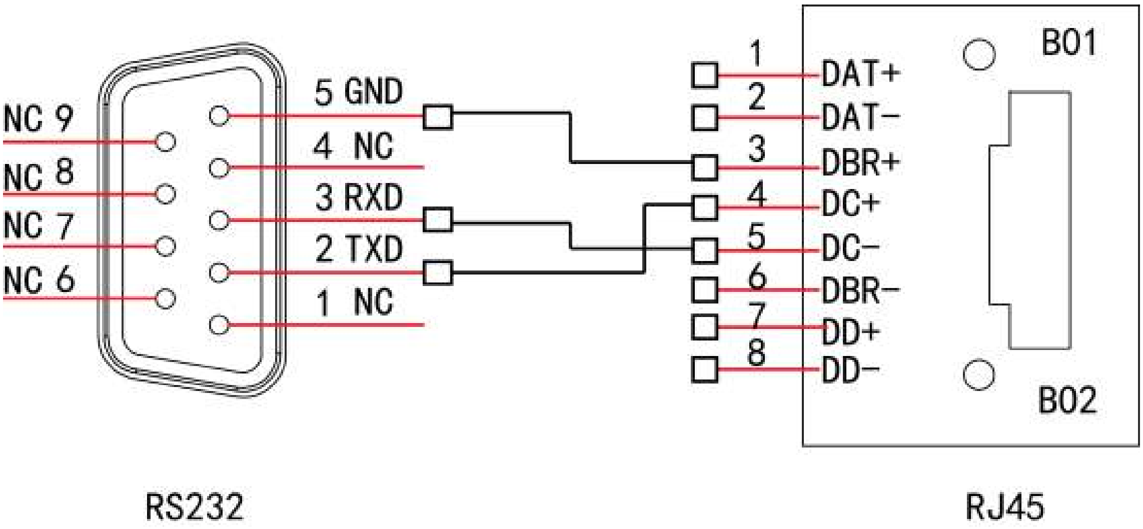
Appendix Table 8-1 Crossover cable connection

RJ45 (T568B)	RJ45 (Network cable)	RS-232	Signal Description
4	Blue	2	RXD
5	White and blue	3	TXD
3	White and green	5	GND

Straight Connection

Refer to the following figure for straight cable connection information.

Appendix Figure 8-4 Straight cable connection



Refer to the following table for straight connection information.

Appendix Table 8-2 Straight connection

RJ45 (T568B)	RJ45 (Network cable)	RS-232	Signal Description
4	Blue	3	RXD
5	White and blue	2	TXD
3	White and green	5	GND

Appendix 9 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic 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, we recommend you 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, we recommend you 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.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

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