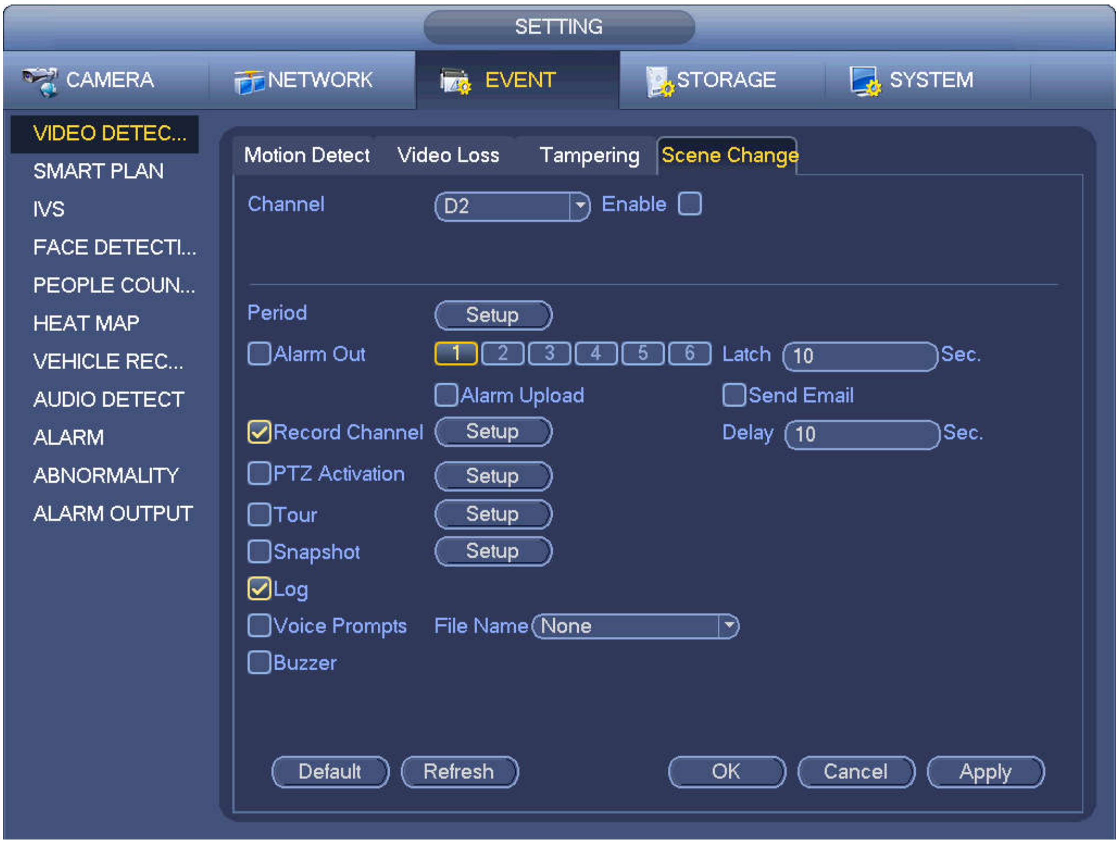


Channel D2 Enable □

Period Setup

□ Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□ Alarm Upload □ Send Email

☑ Record Channel Setup Delay 10 Sec.

□ PTZ Activation Setup

□ Tour Setup

□ Snapshot Setup

☑ Log

□ Voice Prompts File Name None

□ Buzzer

Figure 4-116

4.7.2 Smart Plan

The smart plan is for the smart network camera. If you do not set a rule here, you cannot use the intelligent functions in IVS (Chapter 4.7.3), Face detection (Chapter 4.7.4) and People counting (Chapter 4.7.5) when you are connecting to a smart network camera.

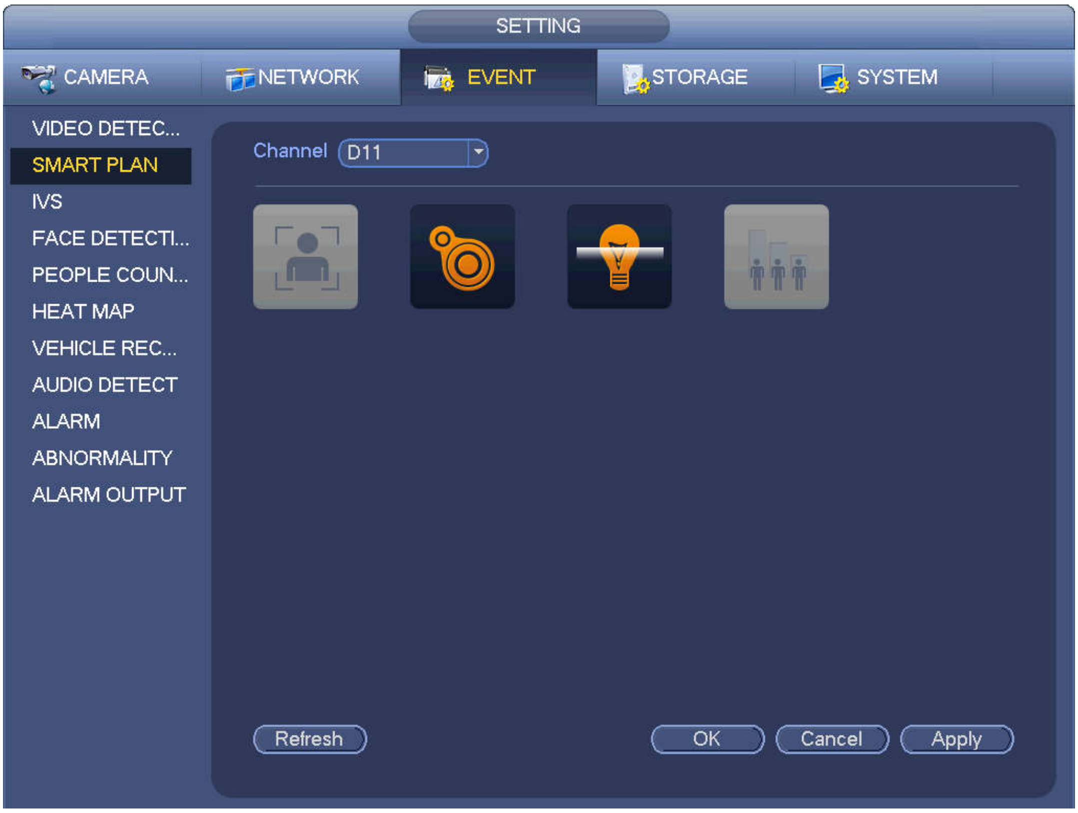
There are two types to realize intelligent analytics function.

Note

- Smart network camera supports intelligent functions: Some smart camera supports the intelligent functions. For NVR, it just displays the intelligent alarm information from the smart network camera and set or playback the record file.
- NVR supports intelligent functions: The connected network camera does not support intelligent video analytics function. The NVR supports the analytics function.

In this interface, you can quickly add an intelligent rule for one preset. The intelligent rule includes human face detection, behavior analytics and people counting.

From main menu->Setting->Event->Smart plan, the interface is shown as below. See Figure 4-117.



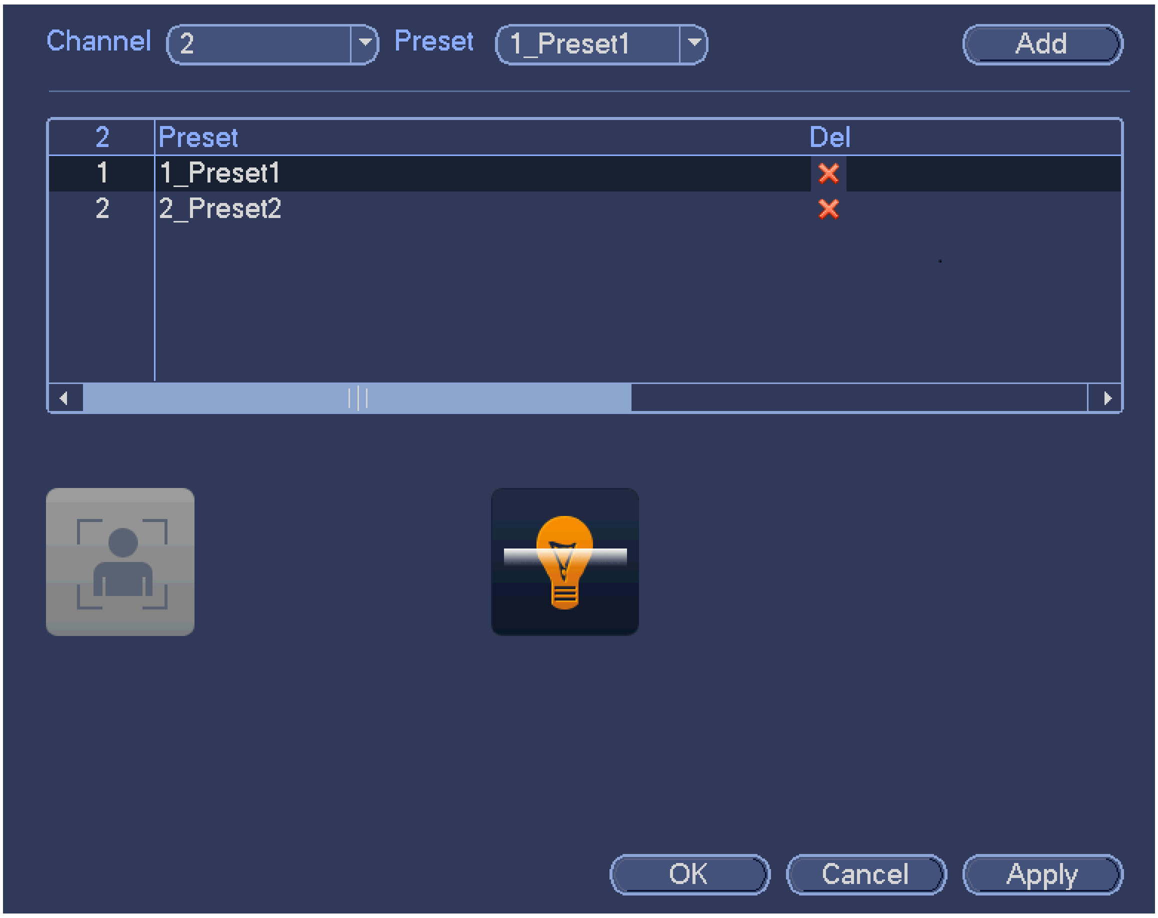
Channel D11

Figure 4-117

Please select a channel number and a preset. Click Add.
The preset is now on the list. See Figure 4-118.

Note

Some smart camera does not need to add the preset. Please refer to the actual product for detailed information.



Channel 2 Preset 1_Preset1

2	Preset	Del
1	1_Preset1	✕
2	2_Preset2	✕

Figure 4-118

Select a smart plant from the dropdown list and then click the corresponding intelligent plan icon. See Figure 4-118.

Note

- The NVR supports general behavior analytics (IVS), human face detection, heat map, and people counting. Different network camera supports different smart plans. Please refer to the actual product for detailed information.
- The general behavior analytics (IVS) and human face detection function cannot be valid at the same time. For example, when add the IVS plan to the preset 1, the human face detection icon becomes grey.

Click OK to complete the setup.

4.7.3 IVS (General Behavior Analytics) (Optional)

The general behavior analysis refers to the system to analyze and process the video and extract the key information from the video. Once the video can match the previously set detection rule, system can trigger the corresponding alarm operations.

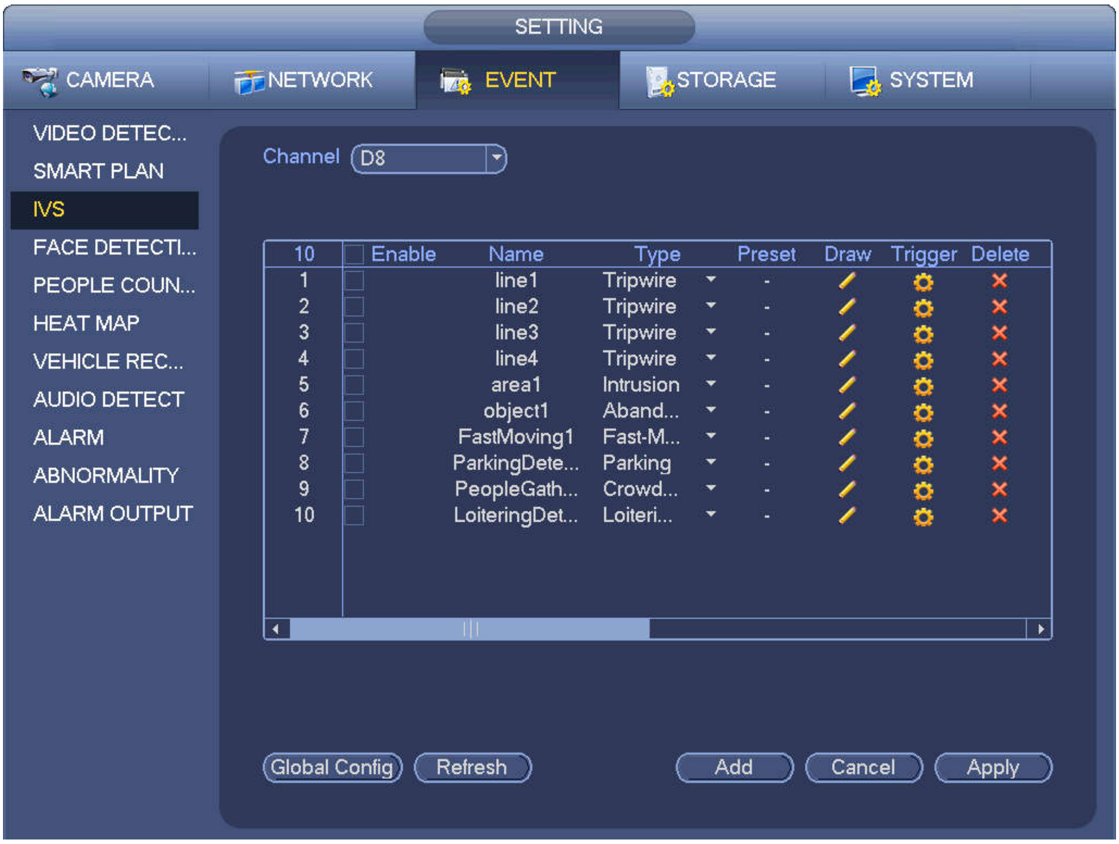
Note

- This function is for some series product only. Please refer to the actual product for detailed information.
- The IVS function and the human face detection function cannot be valid at the same time.

The IVS function environment shall meet the following requirements:

- The object total size shall not be more than 10% of the whole video.
- The object size on the video shall not be more than 10pixels*10 pixels. The abandoned object size shall be more than 15pixels*15 pixels (CIF resolution). The object width shall not be more than 1/3 of the video height and width. The recommended height is 10% of the video.
- The object and the background brightness different shall be more than 10 grey levels.
- The object shall remain on the video for more than 2 seconds. The moving distance is larger than its own width and shall not be smaller than 15pixels (CIF resolution).
- The surveillance environment shall not be too complicated. The IVS function is not suitable for the environment of too many objects or the changing light.
- The surveillance environment shall not contain glasses, reflection light from the ground, and water. Free of tree branches, shadow, mosquito and bugs. Do not use the IVS function in the backlight environment, avoid direct sunlight.

From main menu->Setting->Event->Behavior Analytics, you can go to the behavior analytics interface. Here you can set general behavior analytics rule. System can generate an alarm as the mode you previously set once there is any object violates the rule. See Figure 4-119.



Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✎	⚙	✕
2	□	line2	Tripwire ▾	-	✎	⚙	✕
3	□	line3	Tripwire ▾	-	✎	⚙	✕
4	□	line4	Tripwire ▾	-	✎	⚙	✕
5	□	area1	Intrusion ▾	-	✎	⚙	✕
6	□	object1	Aband... ▾	-	✎	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✎	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✎	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✎	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✎	⚙	✕

Figure 4-119

Select a channel from the dropdown list.

Click Add button to add a rule and then select a rule type from the dropdown list.

Set corresponding parameters.

Click Apply button to complete the setup.

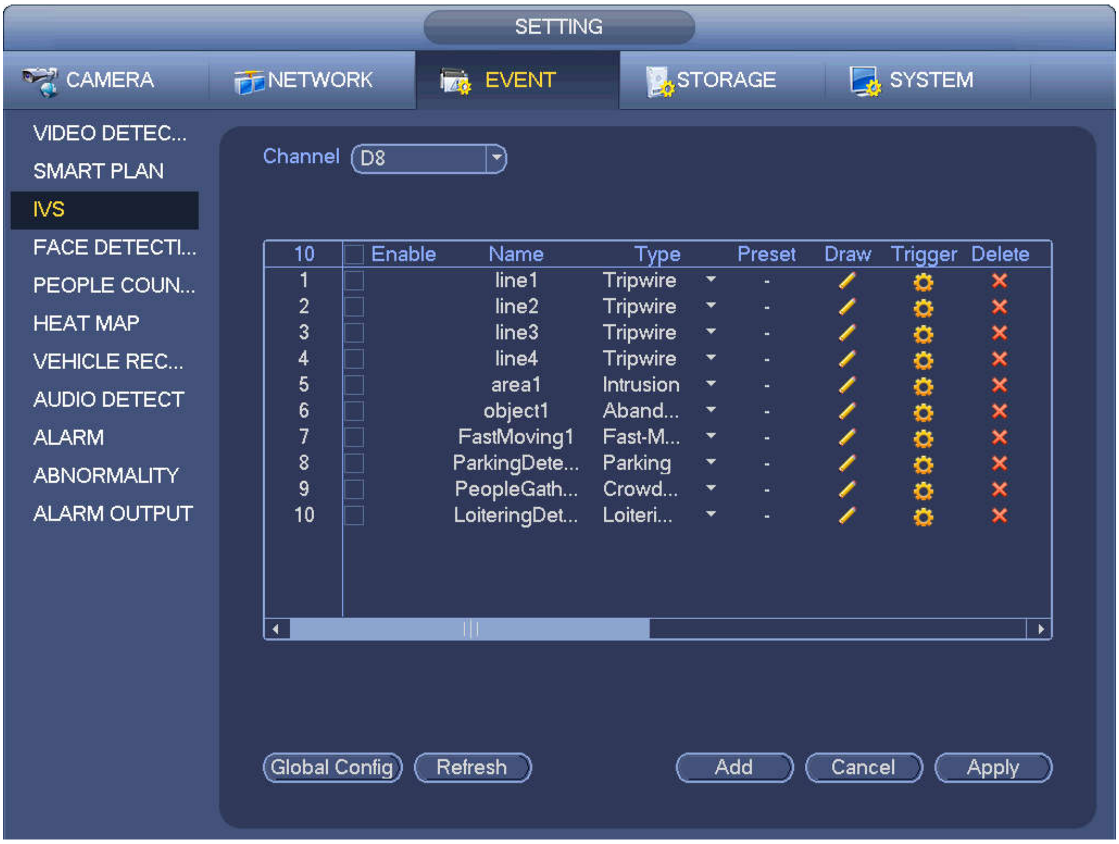
4.7.3.1 Tripwire (Optional)

System generates an alarm once there is any object crossing the tripwire in the specified direction.

- The tripwire supports customized setup. It can be a straight line or a curve.
- Support one-direction or dual-direction detection.

- Support several tripwires at the same scene suitable for complicated environment.
- Support object size filter.

From main menu->Setting->Event->Behavior analytics, the interface is shown as below. See Figure 4-120.

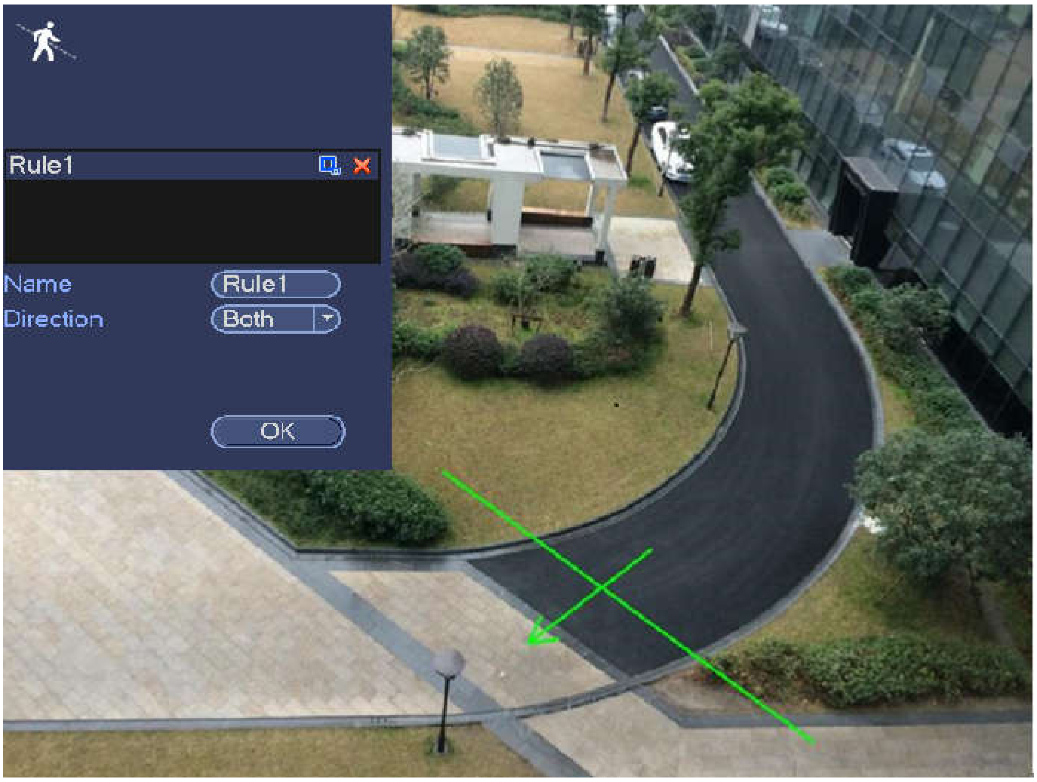


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✎	⚙	✕
2	□	line2	Tripwire ▾	-	✎	⚙	✕
3	□	line3	Tripwire ▾	-	✎	⚙	✕
4	□	line4	Tripwire ▾	-	✎	⚙	✕
5	□	area1	Intrusion ▾	-	✎	⚙	✕
6	□	object1	Aband... ▾	-	✎	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✎	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✎	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✎	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✎	⚙	✕

Figure 4-120

Click Draw button ✎ to draw the tripwire. See Figure 4-121.



Rule1

Name: Rule1

Direction: Both

Figure 4-121

Select direction, and then input customized rule name.

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Direction (A→B/B→A/A↔B): System can generate an alarm once there is any object crossing in the specified direction.
- Target filter: Click, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a tripwire. The tripwire can be a direct line, curve or polygon. Right click mouse to complete.

Tips

Click ☒ to delete the corresponding rule.

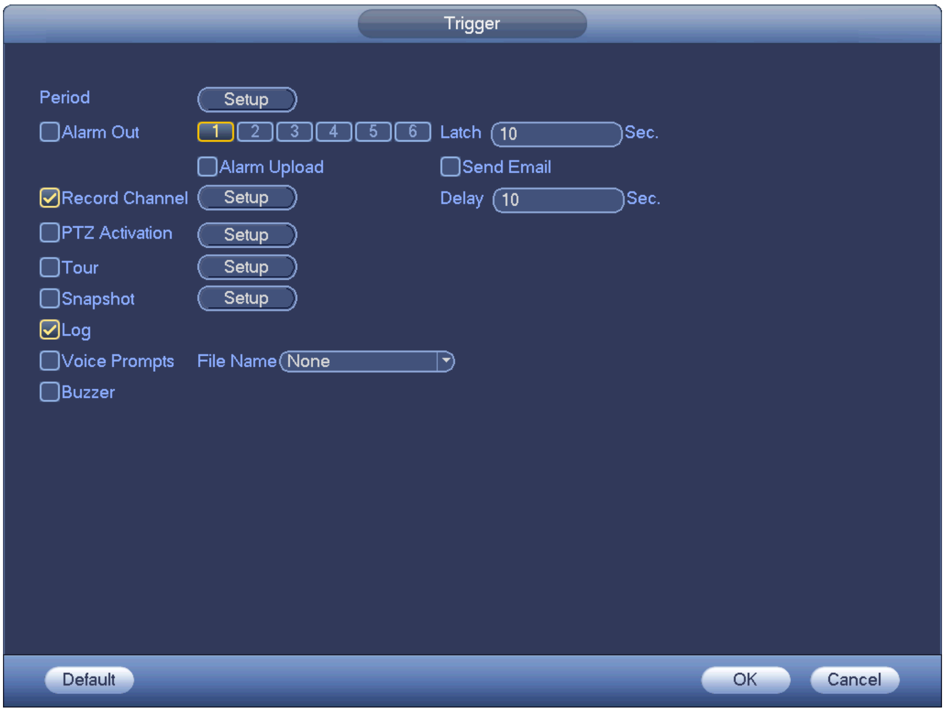
Click, you can see the following interface. See Figure 4-122.

You can refer to the following information to set other parameters.

- Channel: Select a channel from the dropdown list to set tripwire function.
- Enable: Check the box here to enable tripwire function.
- Rule: input customized rule name here.
- Period: Click set button, you can see an interface is shown as in Figure 4-112. Here you can set tripwire period. System only enables tripwire operation in the specified periods. There are two ways for you to set periods. Please note system only supports 6 periods in one day.

- ✧ In Figure 4-112, Select icon ▭ of several dates, all checked items can be edited together. Now the icon is shown as 🔗. Click ⌫ to delete a record type from one period.
- ✧ In Figure 4-112. Click button ⚙ after one date or a holiday, you can see an interface shown as in Figure 4-113.

- Alarm output: when an alarm occurs, system enables peripheral alarm devices.
- Latch: when tripwire complete, system auto delays detecting for a specified time. The value ranges from 1-300(Unit: second)
- Show message: System can pop up a message to alarm you in the local host screen if you enabled this function.
- Alarm upload: System can upload the alarm signal to the network (including alarm center) if you enabled current function.
- Send email: System can send out email to alert you when an alarm occurs.
- Record channel: System auto activates tripwire channel(s) to record once an alarm occurs. Please make sure you have set intelligent record in Schedule interface(Main Menu->Setting->Schedule) and schedule record in manual record interface(Main Menu->Advanced->Manual Record)
- PTZ activation: Here you can set PTZ movement when an alarm occurs. Such as go to preset, tour &pattern when there is an alarm. Click "select" button, you can see an interface is shown as in Figure 4-111.
- Record Delay: System can delay the record for specified time after alarm ended. The value ranges from 10s to 300s.
- Tour: Here you can enable tour function when an alarm occurs. System one-window tour.
- Snapshot: You can enable this function to snapshot image when a motion detect alarm occurs.
- Buzzer: Highlight the icon to enable this function. The buzzer beeps when an alarm occurs.



Period

□Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□Alarm Upload □Send Email

☑Record Channel Delay 10 Sec.

□PTZ Activation

□Tour

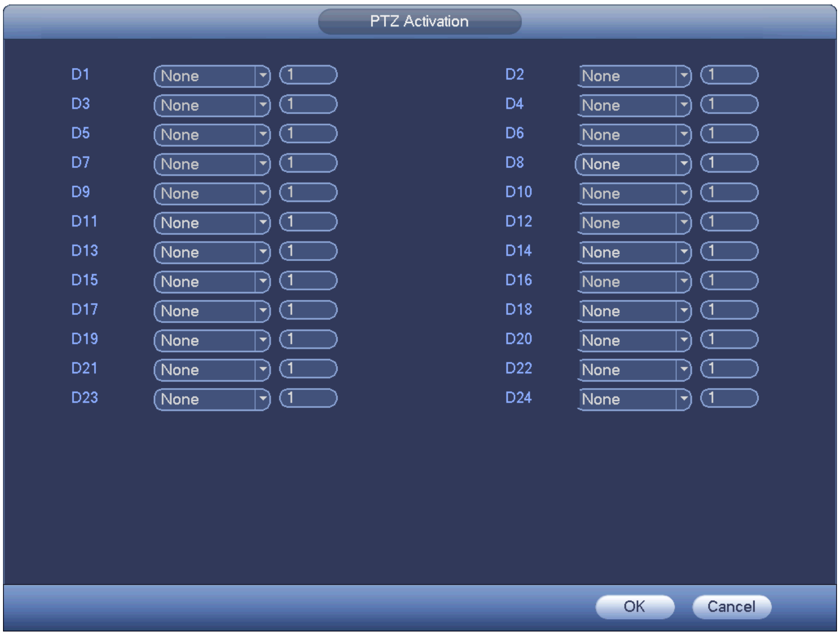
□Snapshot

☑Log

□Voice Prompts File Name None

□Buzzer

Figure 4-122



PTZ Activation

D1	None	1	D2	None	1
D3	None	1	D4	None	1
D5	None	1	D6	None	1
D7	None	1	D8	None	1
D9	None	1	D10	None	1
D11	None	1	D12	None	1
D13	None	1	D14	None	1
D15	None	1	D16	None	1
D17	None	1	D18	None	1
D19	None	1	D20	None	1
D21	None	1	D22	None	1
D23	None	1	D24	None	1

Figure 4-123

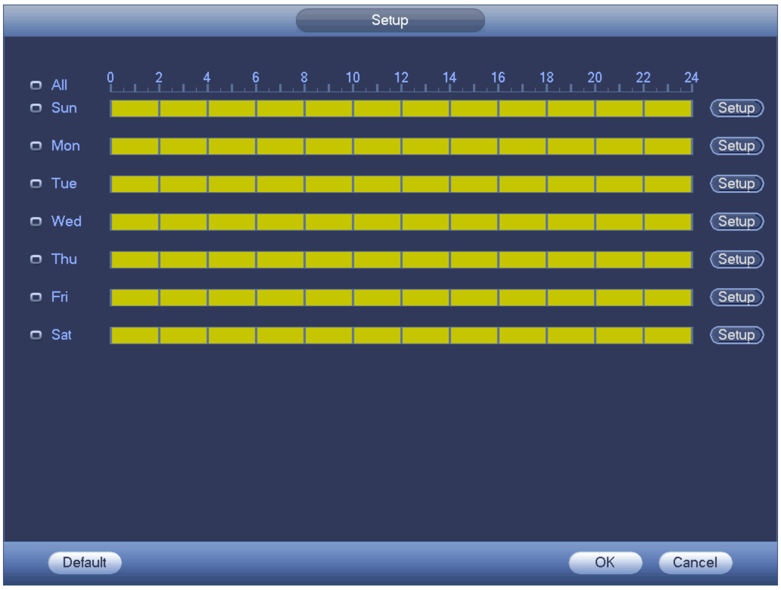
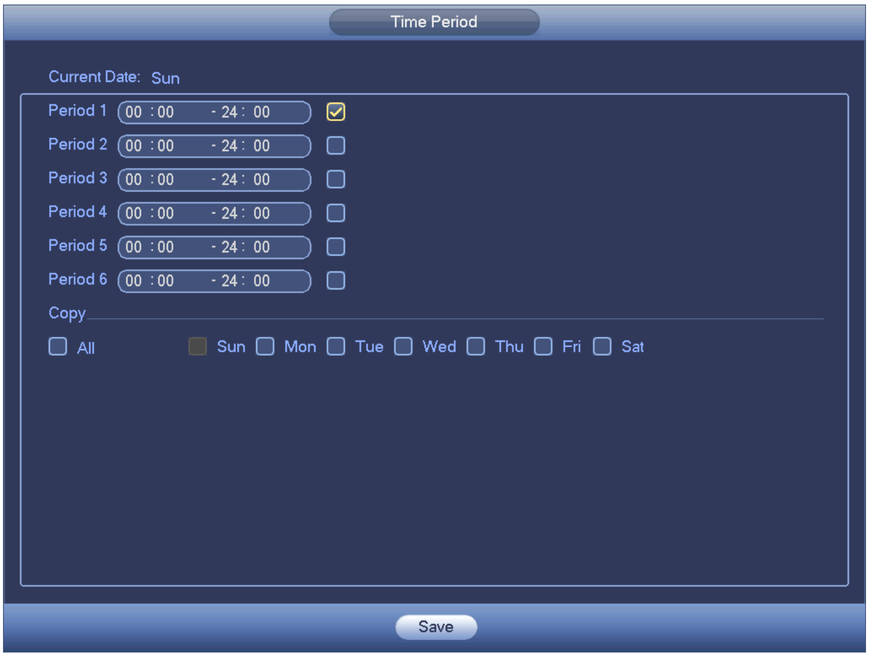


Figure 4-124



Time Period

Current Date: Sun

Period 1 00 : 00 - 24 : 00 ☑

Period 2 00 : 00 - 24 : 00 □

Period 3 00 : 00 - 24 : 00 □

Period 4 00 : 00 - 24 : 00 □

Period 5 00 : 00 - 24 : 00 □

Period 6 00 : 00 - 24 : 00 □

Copy

□ All □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

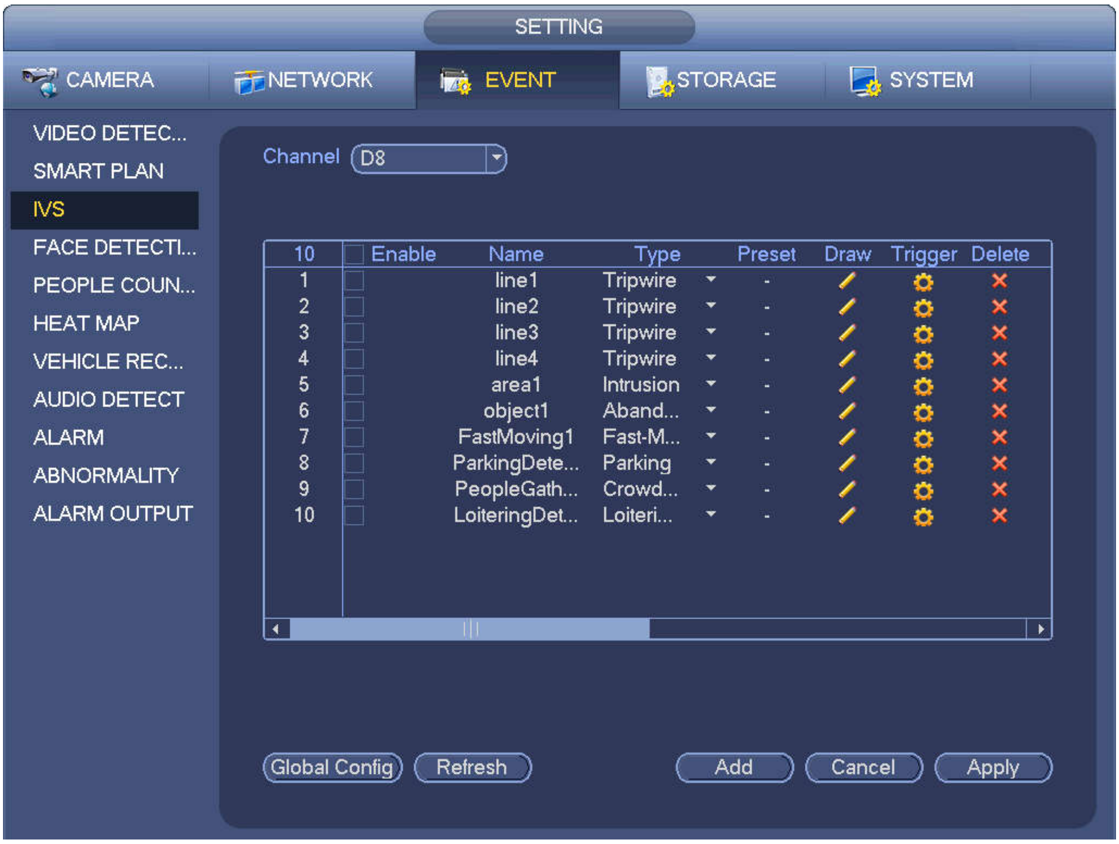
Figure 4-125

After you set the corresponding parameters, click OK button in Figure 4-122., and then click the Apply button in Figure 4-120 to complete the setup.

4.7.3.2 Intrusion (Cross warning zone) (Optional)

System generates an alarm once there is any object entering or exiting the zone in the specified direction. From main menu->Setting->Event->Behavior analytics, click Add button and then select type as intrusion, the interface is shown as below. See Figure 4-126.

- System supports customized area shape and amount.
- Support enter/leave/both detection.
- Can detect the moving object operation in the specified zone, customized trigger amount and staying time.
- Support objects filter function.

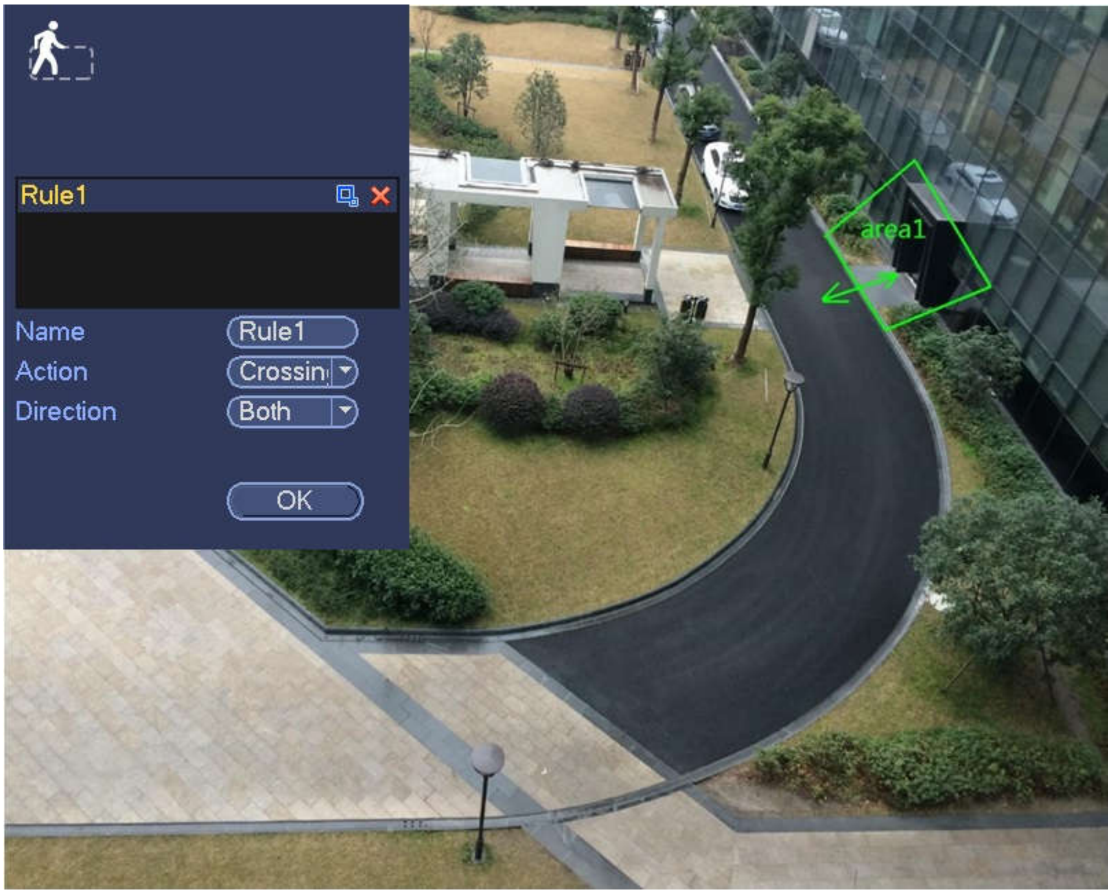


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✏	⚙	✕
2	□	line2	Tripwire ▾	-	✏	⚙	✕
3	□	line3	Tripwire ▾	-	✏	⚙	✕
4	□	line4	Tripwire ▾	-	✏	⚙	✕
5	□	area1	Intrusion ▾	-	✏	⚙	✕
6	□	object1	Aband... ▾	-	✏	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✏	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✏	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✏	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✏	⚙	✕

Figure 4-126

Click draw button ✏ to draw the zone. See Figure 4-127.



Rule1

Name: Rule1

Action: Crossin

Direction: Both

OK

Figure 4-127

Select direction, and then input customized rule name.

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Direction (A→B/B→A/A↔B): System can generate an alarm once there is any object crossing in the specified direction.
- Target filter: Click ⧉, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a warning zone. Right click mouse to complete the setup.

Tips

Click ✕ to delete the corresponding rule.

Click ⚙, you can refer to chapter 4.7.3.1 to set other parameters.

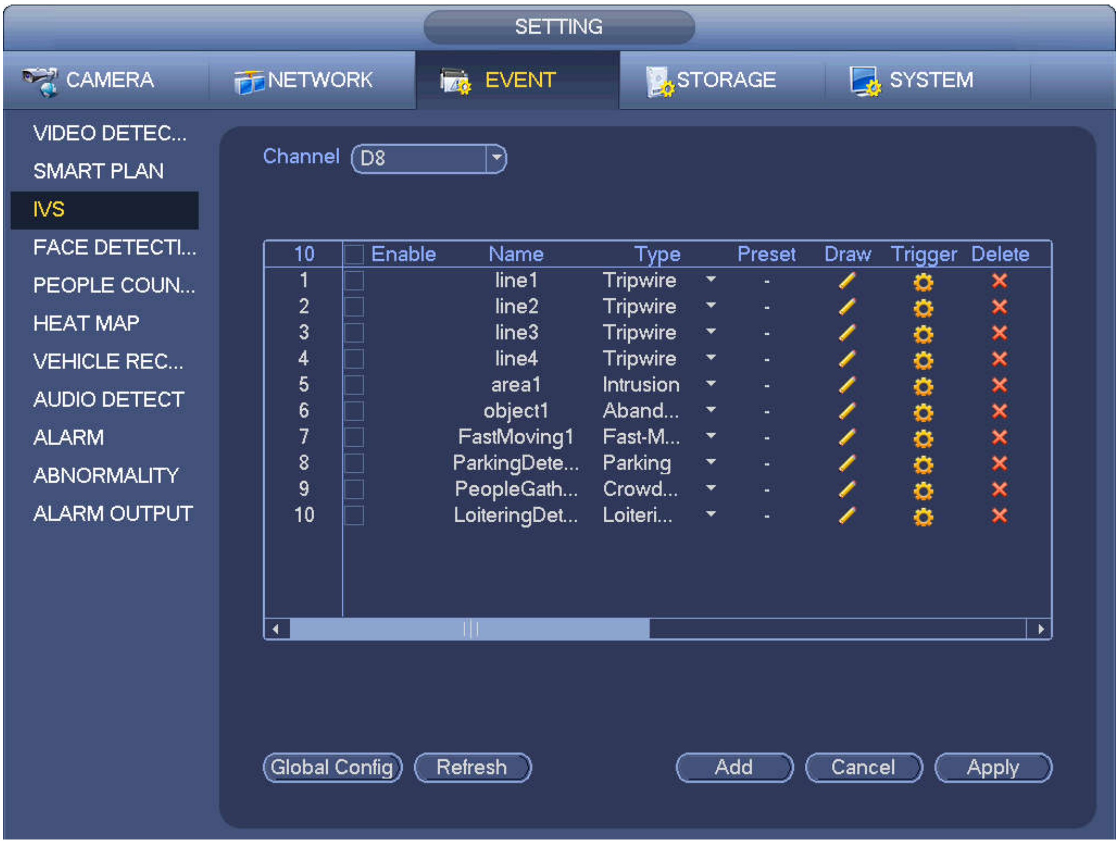
Click Apply to complete the setup.

4.7.3.3 Abandoned Object Detect (Optional)

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

From main menu->Setting->Event->Behavior analytics, select the type as abandoned object, the object interface is shown as below. See Figure 4-128.

- System supports customized area shape and amount.
- Support duration setup.
- Support objects filter function.

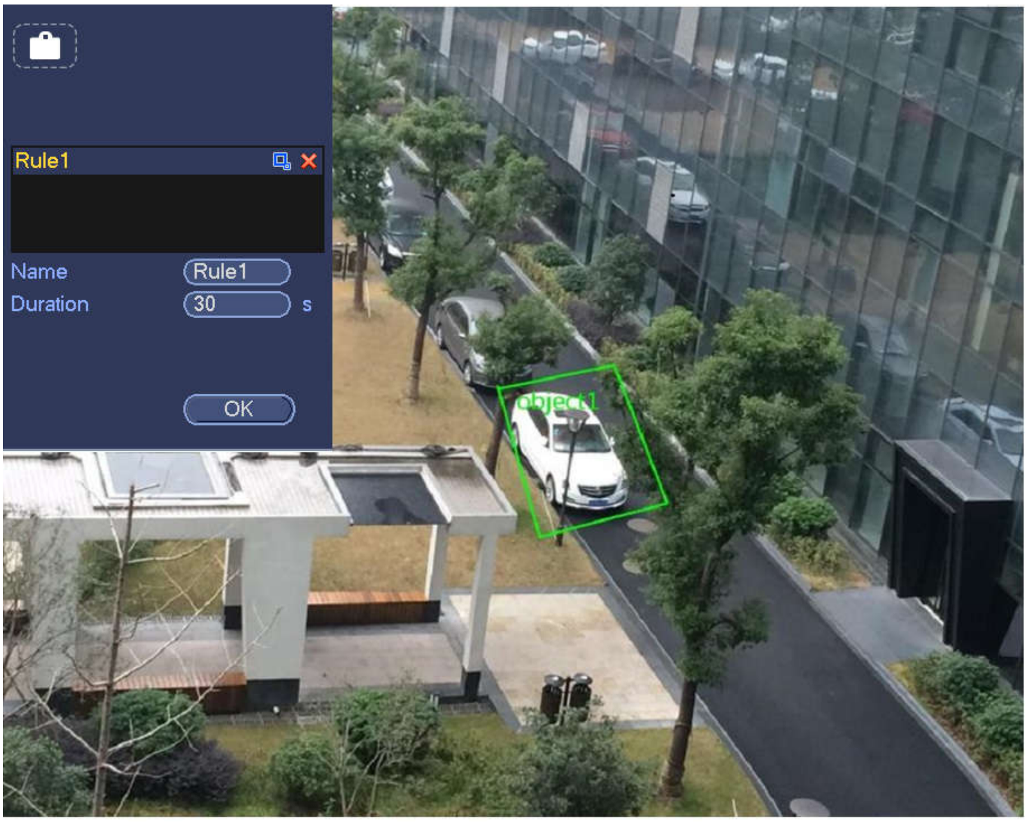


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✏	⚙	✕
2	□	line2	Tripwire ▾	-	✏	⚙	✕
3	□	line3	Tripwire ▾	-	✏	⚙	✕
4	□	line4	Tripwire ▾	-	✏	⚙	✕
5	□	area1	Intrusion ▾	-	✏	⚙	✕
6	□	object1	Aband... ▾	-	✏	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✏	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✏	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✏	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✏	⚙	✕

Figure 4-128

Click draw button ✏ to draw the zone. See Figure 4-129.



Name: Rule1

Duration: 30 s

Figure 4-129

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Duration: System can generate an alarm once the object is in the zone for the specified period.
- Target filter: Click, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a zone, until you draw a rectangle, you can right click mouse.

Tips

Click ☒ to delete the corresponding rule.

Click ⚙, you can refer to the chapter 4.7.3.1 to set other parameters.

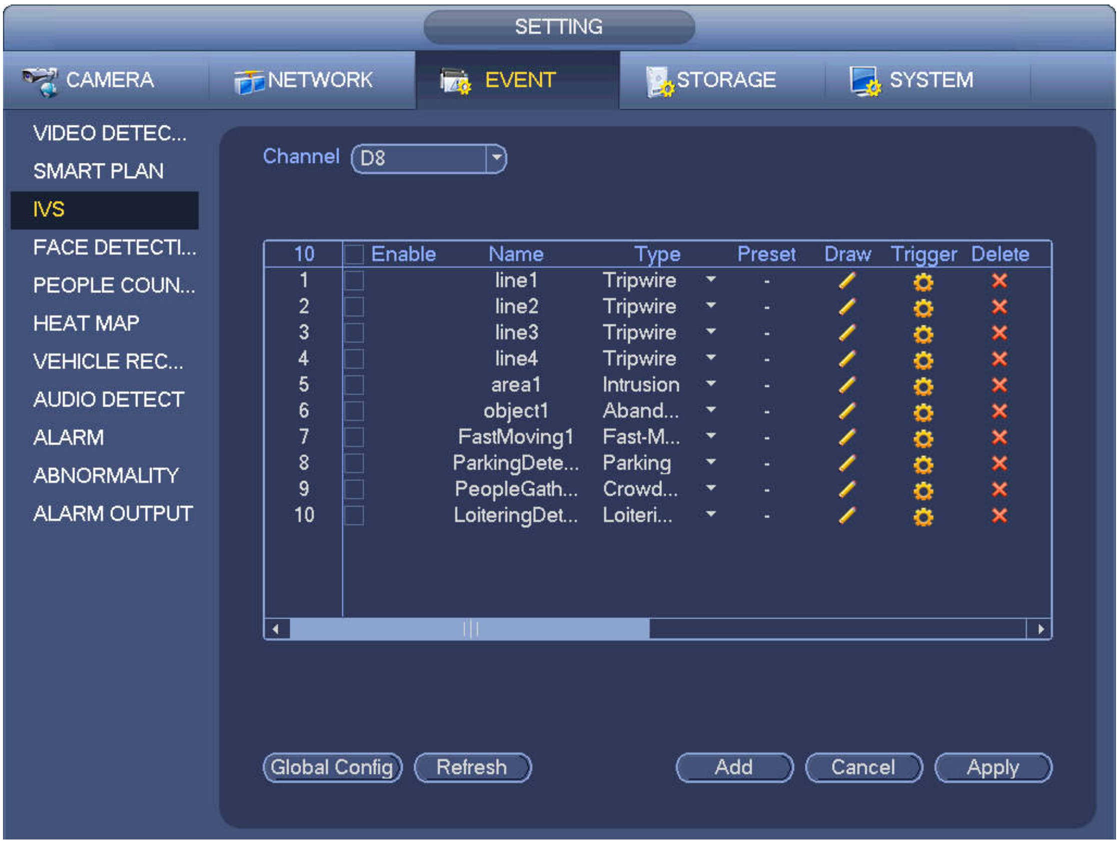
Click Apply to complete the setup.

4.7.3.4 Missing Object Detection (Optional)

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

From main menu->Setting->Event->Behavior analytics, select the type as abandoned object, the object interface is shown as below. See Figure 4-130.

- System supports customized area shape and amount.
- Support duration setup.
- Support objects filter function.

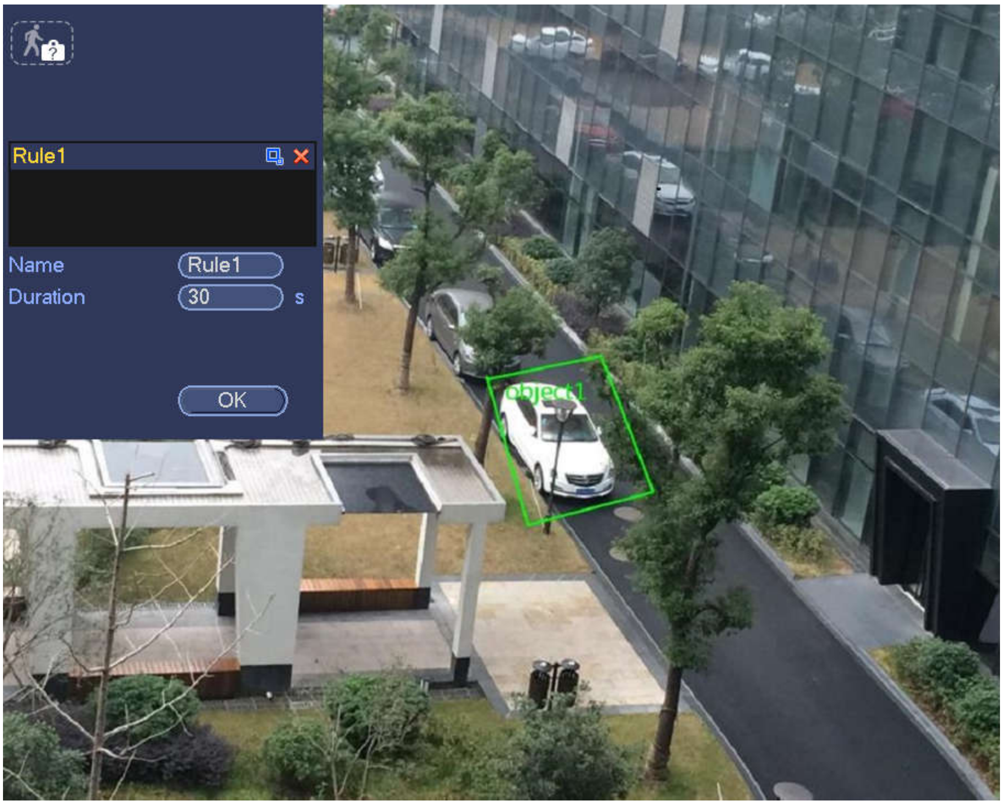


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✎	⚙	✕
2	□	line2	Tripwire ▾	-	✎	⚙	✕
3	□	line3	Tripwire ▾	-	✎	⚙	✕
4	□	line4	Tripwire ▾	-	✎	⚙	✕
5	□	area1	Intrusion ▾	-	✎	⚙	✕
6	□	object1	Aband... ▾	-	✎	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✎	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✎	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✎	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✎	⚙	✕

Figure 4-130

Click Draw button ✎ to draw a zone. See Figure 4-131.



Name Rule1

Duration 30 s

Figure 4-131

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Duration: System can generate an alarm once the object in the zone is missing for the specified period.
- Target filter: Click ⧉, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a zone, until you draw a rectangle, you can right click mouse.

Tips

Click ✕ to delete the corresponding rule.

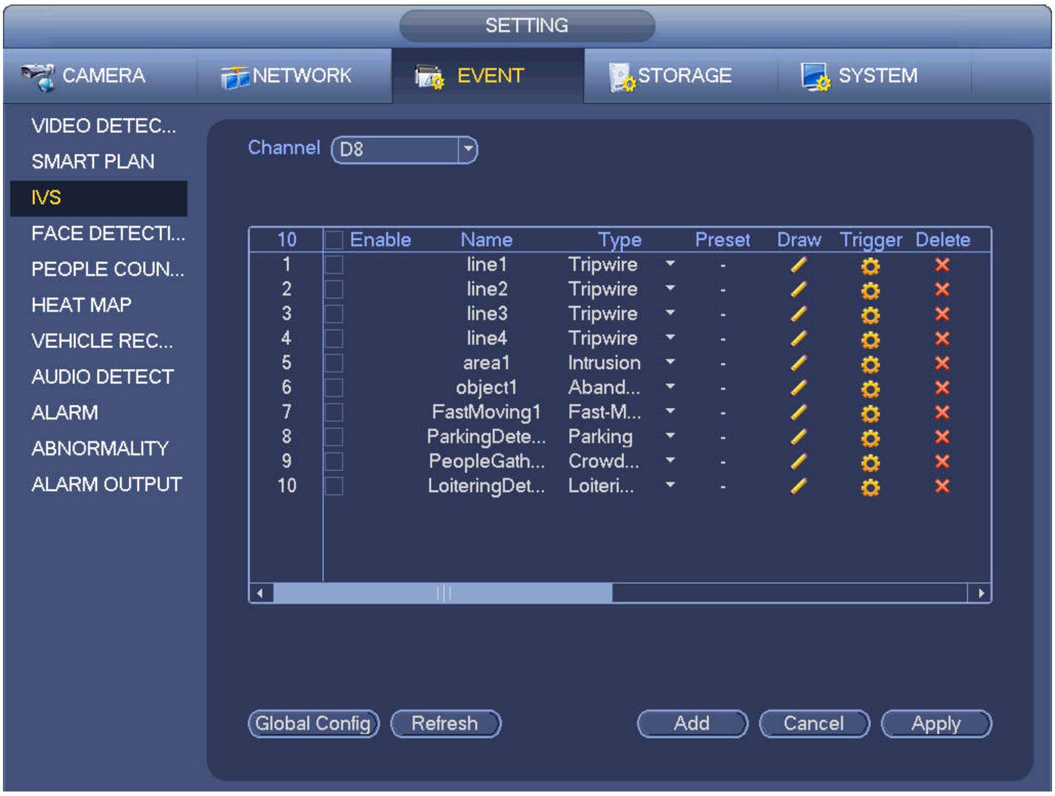
Click ⚙, you can refer to the chapter 4.7.3.1 to set other parameters.

Click Apply to complete the setup.

4.7.3.5 Loitering Detection (Optional)

System can generate an alarm once the object is staying in the specified zone longer than the threshold. From main menu->Setting->Event->Behavior analytics, select the type as loitering, the object interface is shown as below. See Figure 4-132.

- System supports customized area shape and amount.
- Support duration setup.
- Support objects filter function.

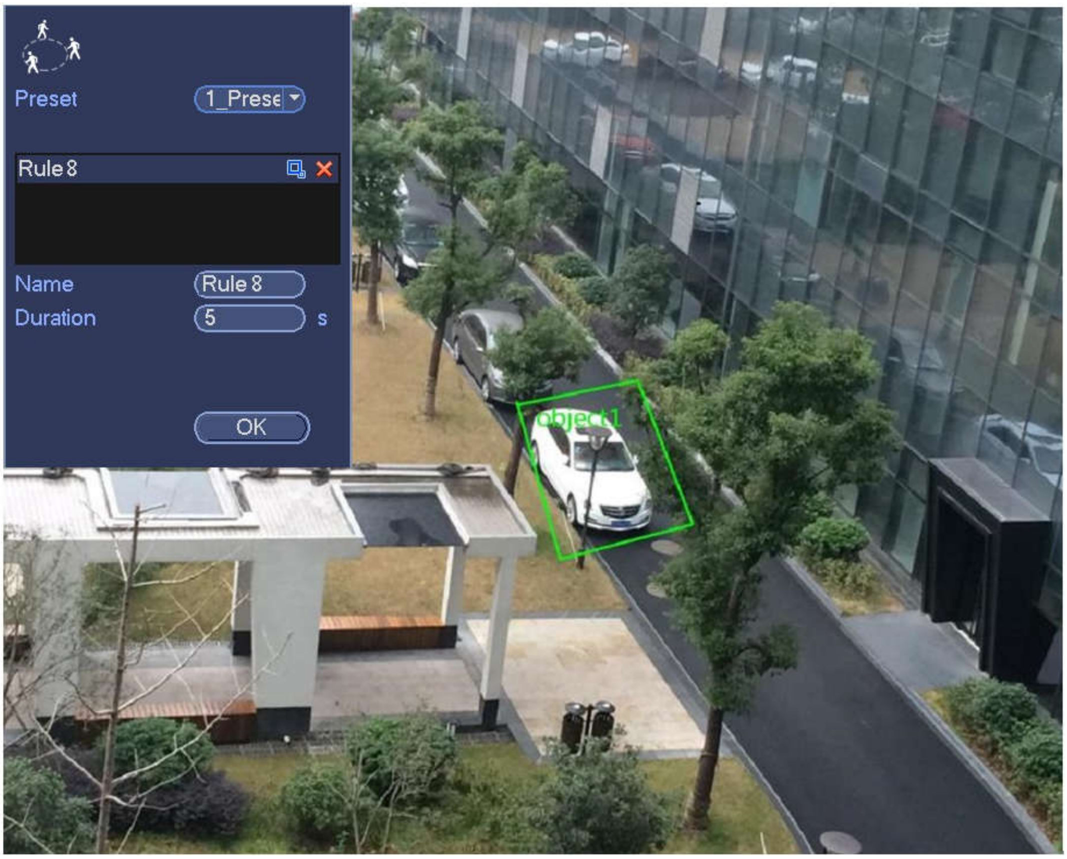


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✎	⚙	✕
2	□	line2	Tripwire ▾	-	✎	⚙	✕
3	□	line3	Tripwire ▾	-	✎	⚙	✕
4	□	line4	Tripwire ▾	-	✎	⚙	✕
5	□	area1	Intrusion ▾	-	✎	⚙	✕
6	□	object1	Aband... ▾	-	✎	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✎	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✎	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✎	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✎	⚙	✕

Figure 4-132

Click draw button ✎ to draw the zone. See Figure 4-133.



Preset 1_Prese

Rule 8

Name Rule 8

Duration 5 s

Figure 4-133

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Duration: System can generate an alarm once the object is in the zone for the specified period.
- Target filter: Click ⧉, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a zone, until you draw a rectangle, you can right click mouse.

Tips

Click ✕ to delete the corresponding rule.

Click ⚙, you can refer to the chapter 4.7.3.1 to set other parameters.

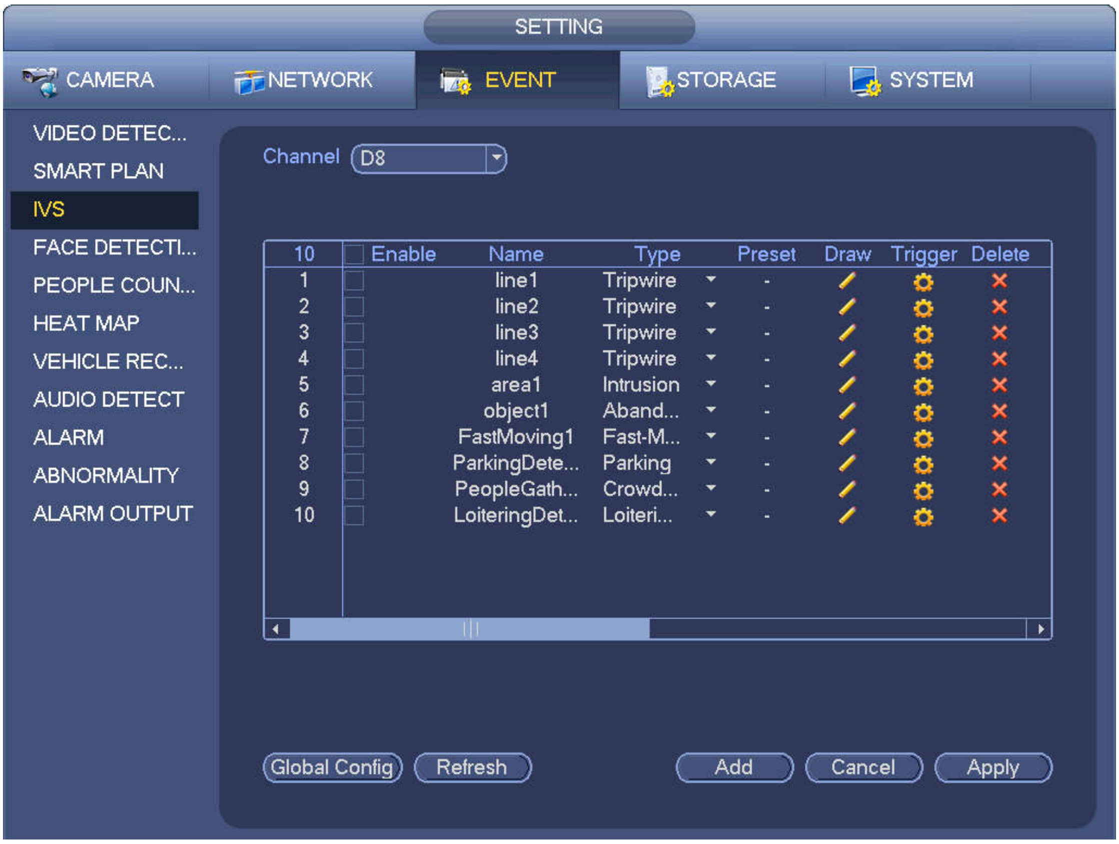
Click Apply to complete the setup.

4.7.3.6 Crowd Gathering Detection (Optional)

System can generate an alarm once the people amount gathering in the specified zone is larger than the threshold.

From main menu->Setting->Event->Behavior analytics, select the type as crowd gathering detect, the interface is shown as below. See Figure 4-134.

- Customized zone and amount setup.
- Duration setup.
- Sensitivity setup.
- Min gathering zone setup.

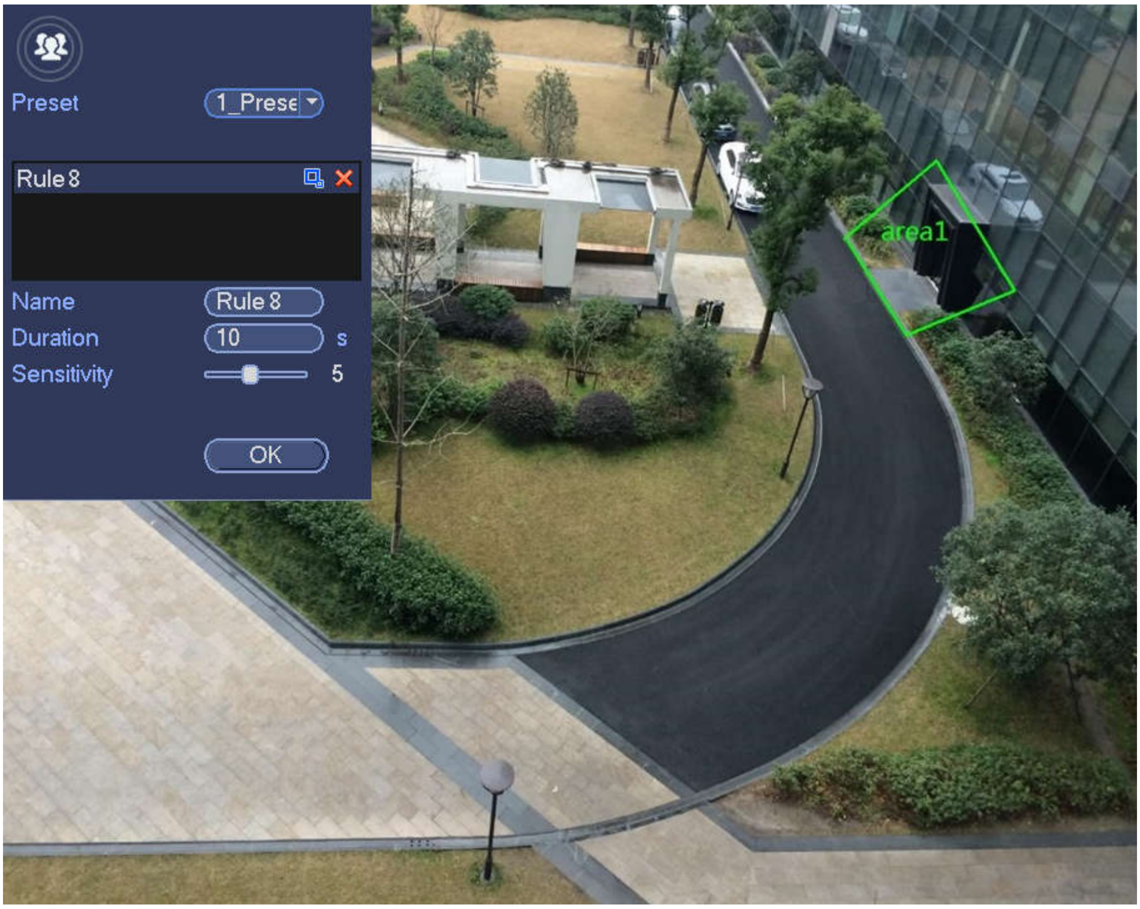


Channel D8

10	□ Enable	Name	Type		Preset	Draw	Trigger	Delete
1	□	line1	Tripwire	▾	-	✏	⚙	✕
2	□	line2	Tripwire	▾	-	✏	⚙	✕
3	□	line3	Tripwire	▾	-	✏	⚙	✕
4	□	line4	Tripwire	▾	-	✏	⚙	✕
5	□	area1	Intrusion	▾	-	✏	⚙	✕
6	□	object1	Aband...	▾	-	✏	⚙	✕
7	□	FastMoving1	Fast-M...	▾	-	✏	⚙	✕
8	□	ParkingDete...	Parking	▾	-	✏	⚙	✕
9	□	PeopleGath...	Crowd...	▾	-	✏	⚙	✕
10	□	LoiteringDet...	Loiteri...	▾	-	✏	⚙	✕

Figure 4-134

Click draw button ✏ to draw the zone. See Figure 4-135.



Preset 1_Prese

Rule8

Name Rule8

Duration 10 s

Sensitivity 5

OK

Figure 4-135

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Duration: System can generate an alarm once the object is in the zone for the specified period.
- Sensitivity: It is to set alarm sensitivity. The value ranges from 1 to 10.The default setup is 5.
- Target filter: Click⧉, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a zone, until you draw a rectangle, you can right click mouse.

Tips

Click ☒ to delete the corresponding rule.

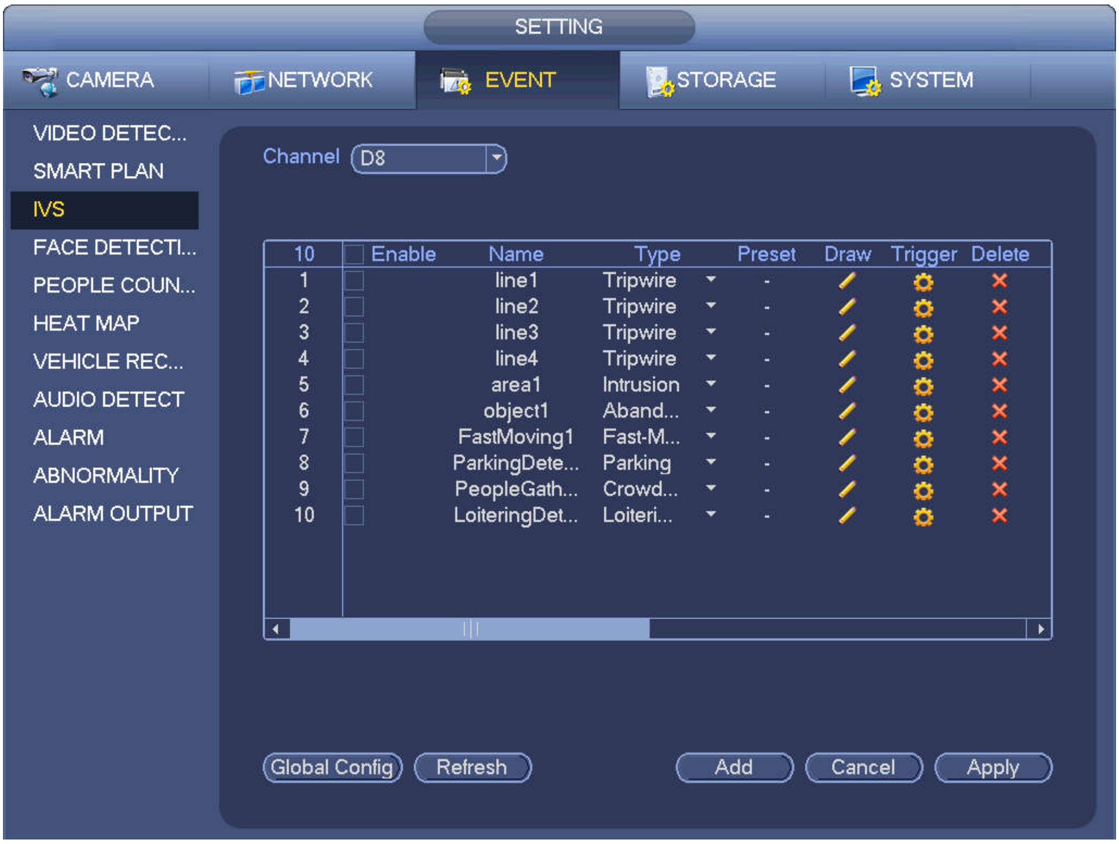
Click ⚙, you can refer to the chapter 4.7.3.1 to set other parameters.

Click Apply to complete the setup.

4.7.3.7 Fast moving (Optional)

It is to detect the fast moving object in the specified zone.

From main menu->Setting->Event->Behavior analytics, select the type as fast moving, the interface is shown as below. See Figure 4-136.

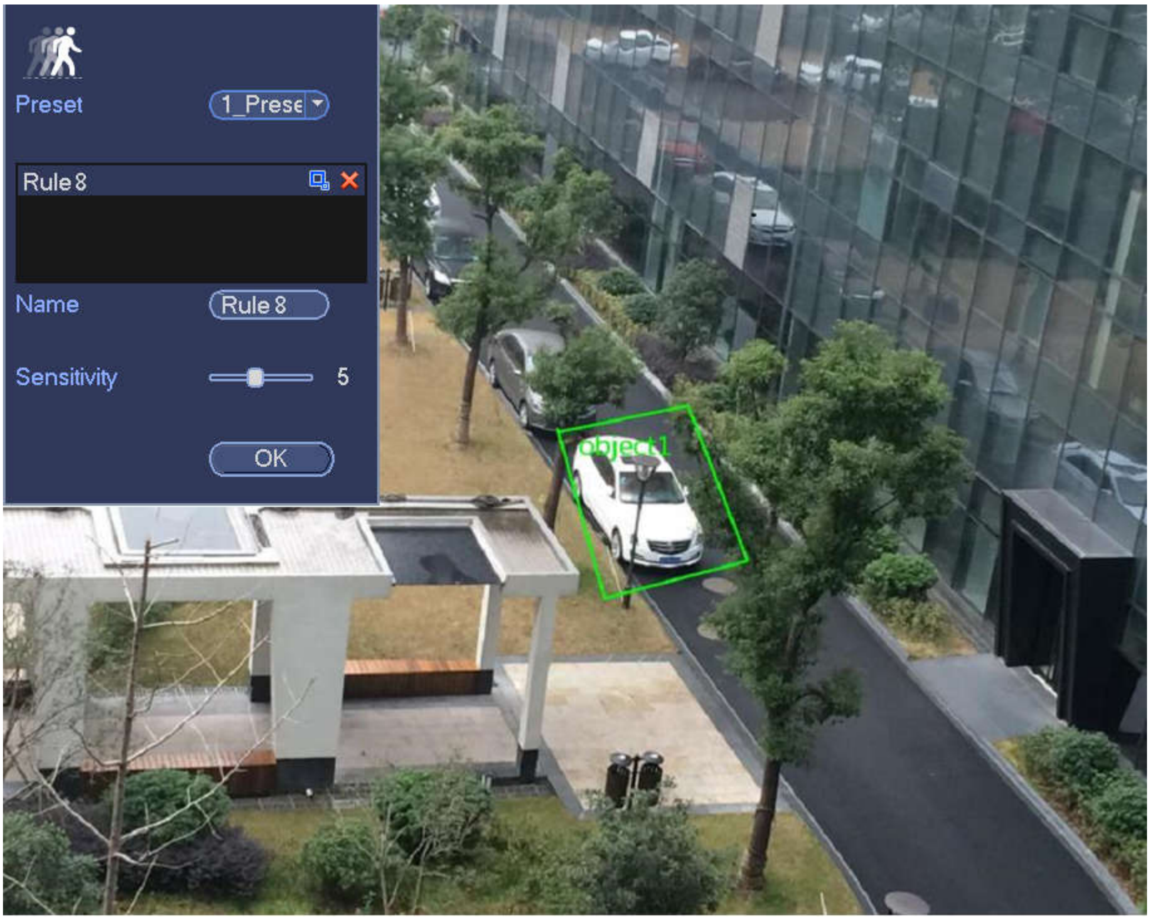


Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✏	⚙	✕
2	□	line2	Tripwire ▾	-	✏	⚙	✕
3	□	line3	Tripwire ▾	-	✏	⚙	✕
4	□	line4	Tripwire ▾	-	✏	⚙	✕
5	□	area1	Intrusion ▾	-	✏	⚙	✕
6	□	object1	Aband... ▾	-	✏	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✏	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✏	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✏	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✏	⚙	✕

Figure 4-136

Click draw button ✏ to draw the zone. See Figure 4-137.



Preset 1_Prese

Rule 8

Name Rule 8

Sensitivity 5

Figure 4-137

- Preset: Select a preset you want to use behavior analytics.
- Name: Input customized rule name.
- Sensitivity: It is to set alarm sensitivity. The value ranges from 1 to 10.The default setup is 5.
- Target filter: Click, you can set filter object size. Each rule can set two sizes (min size/max size). Once the object is smaller than the min size or larger than the max size, there is no alarm. Please make sure the max size is larger than the min size.

Now you can draw a rule. Left click mouse to draw a zone, until you draw a rectangle, you can right click mouse.

Tips

Click ☒ to delete the corresponding rule.

Click ⚙, you can refer to the chapter 4.7.3.1 to set other parameters.

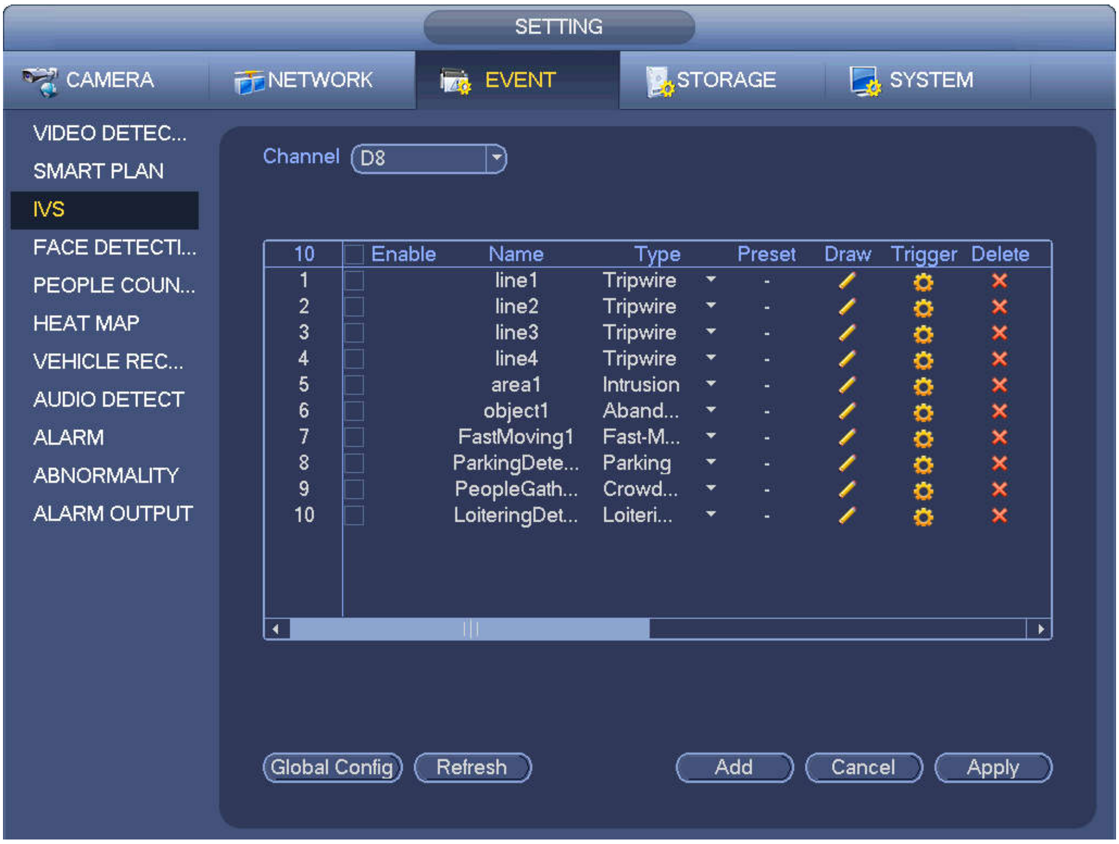
Click Apply to complete the setup.

4.7.3.8 Global Setup (Optional)

After set one horizontal gauge and three vertical gauge and the actual distances between each gauge, the system can estimate the network camera internal parameters(internal geometrical features and optical properties) and external parameters (the network camera position and direction on the actual environment),it can confirm the actual distance on the current surveillance environment.

From main menu->Setting->Event->IVS (Behavior analytics), enter the following interface. See Figure

4-138.



Channel D8

10	□ Enable	Name	Type	Preset	Draw	Trigger	Delete
1	□	line1	Tripwire ▾	-	✎	⚙	✕
2	□	line2	Tripwire ▾	-	✎	⚙	✕
3	□	line3	Tripwire ▾	-	✎	⚙	✕
4	□	line4	Tripwire ▾	-	✎	⚙	✕
5	□	area1	Intrusion ▾	-	✎	⚙	✕
6	□	object1	Aband... ▾	-	✎	⚙	✕
7	□	FastMoving1	Fast-M... ▾	-	✎	⚙	✕
8	□	ParkingDete...	Parking ▾	-	✎	⚙	✕
9	□	PeopleGath...	Crowd... ▾	-	✎	⚙	✕
10	□	LoiteringDet...	Loiteri... ▾	-	✎	⚙	✕

Figure 4-138

Click Global config button, the interface is shown as below. See Figure 4-139.

- Channel: Please select a channel from the dropdown list.
- Preset: Select a preset you want to set the rule. Please note, you need to add a preset first, otherwise, you cannot see the preset dropdown list. If there is no preset, you can draw a rule in current channel.
- Calibration zone:

✧ Click Add zone ⊞, you can draw a calibration zone at the left pane of the interface. Select a zone and then click Delete zone button; you can remove the selected zone.

✧ Select gauge type (horizontal/tilt), you can set the corresponding length. You can draw three tilt gauges and one horizontal gauge at the left pane of the interface.

- Select Width/Height and then click Verify, you can draw a line in the calibration zone, and then you can see its actual length.
- Refresh preset: Click it to get the latest preset setup.

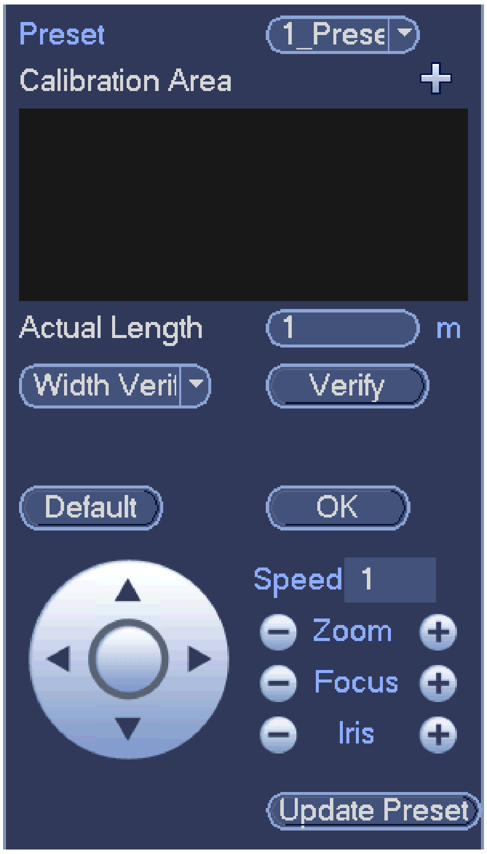


Figure 4-139

4.7.4 Face Detect (Optional)

System processes and analyzes the video from the camera. System can generate an alarm when it detects there is any human face information.

From main menu->Setting->Event->Face detect, the interface is shown as in Figure 4-140.

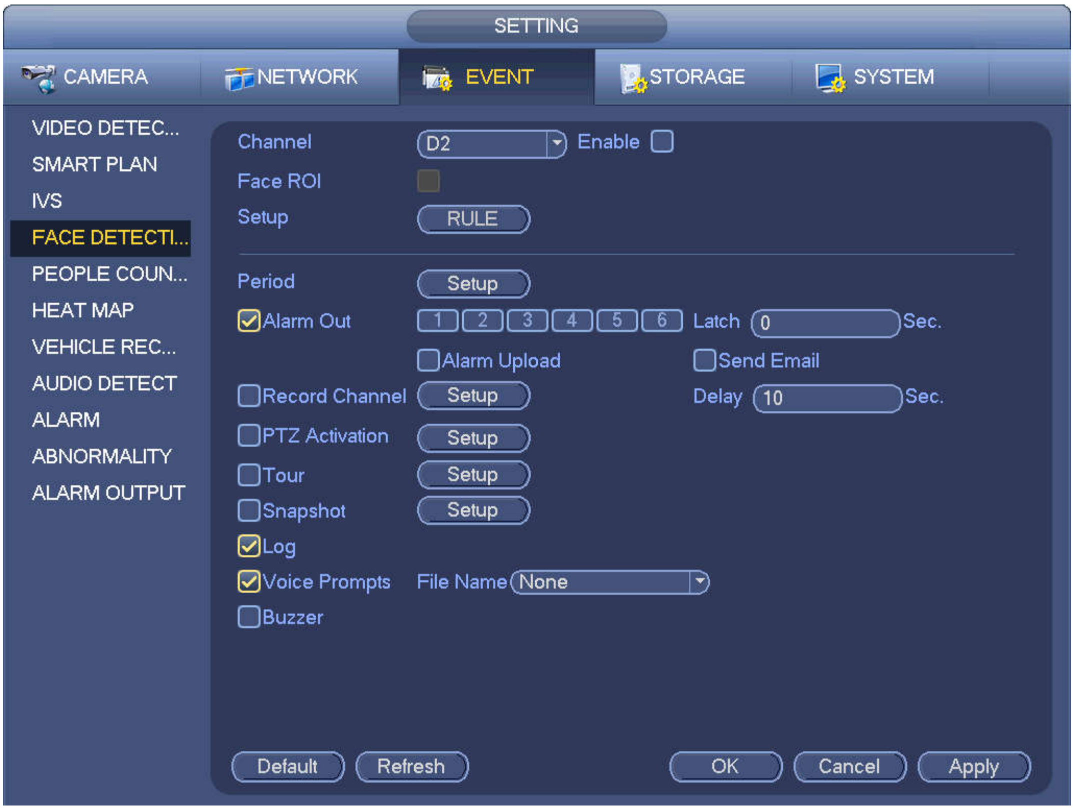
- Face ROI: Check the box here, system can enhance the human face display pane.

Note

Make sure the connected camera supports human face detect function if you want to use face ROI function.

- Log: Check the box here, system can record face detect log.

You can refer to the chapter 4.7.1.1 Motion detect to set other parameters.



Channel D2 Enable □

Face ROI □

Setup RULE

Period Setup

☑Alarm Out 1 2 3 4 5 6 Latch 0 Sec.

□Alarm Upload □Send Email

□Record Channel Setup Delay 10 Sec.

□PTZ Activation Setup

□Tour Setup

□Snapshot Setup

☑Log

☑Voice Prompts File Name None

□Buzzer

Figure 4-140

4.7.5 People Counting (Optional)

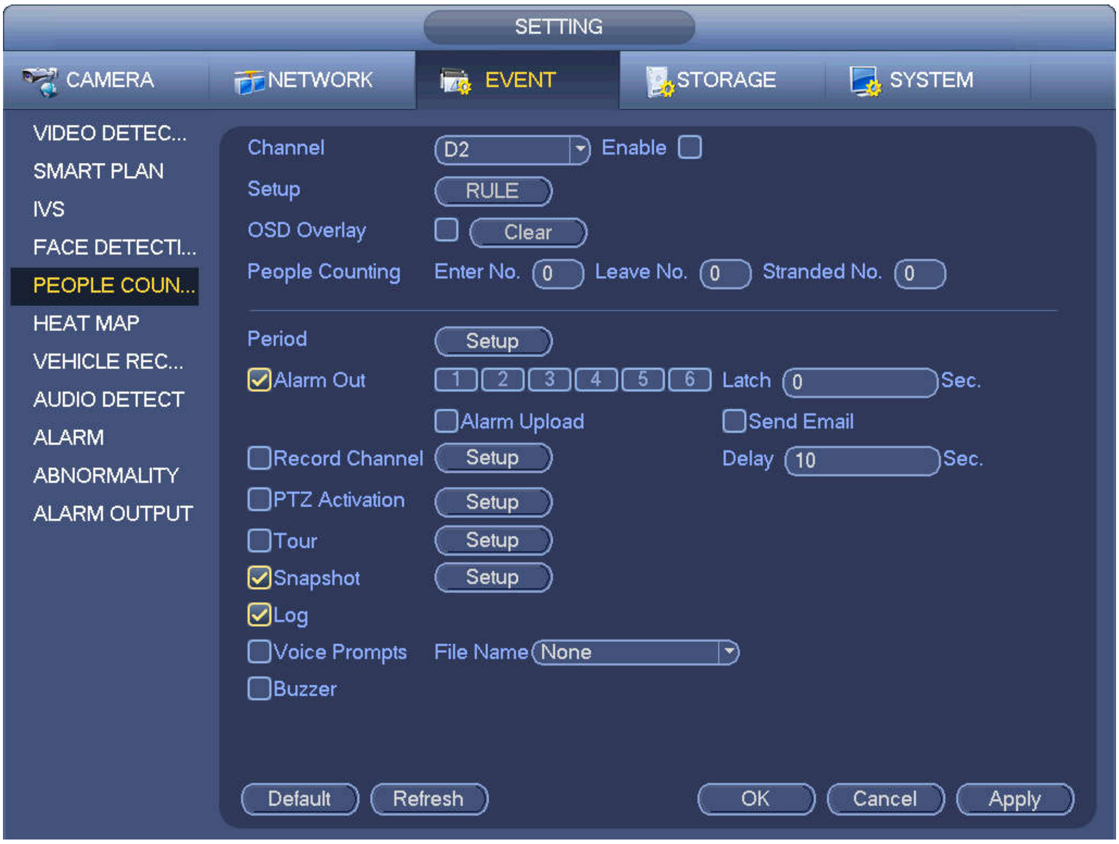
System adopts video image and graphics analysis technology. System can calculate the entry/exit people amount in the specified zone on the video. It can generate an alarm when the amount has exceeded the threshold.

From main menu->Setting->Event->People counting, you can see an interface shown as in Figure 4-141.

- Enable: Check the box to enable people counting function.
- OSD overlay: Check the box here; you can view the people amount on the surveillance video.
- Rule setup: Click Set button, you can set people counting zone, name, and direction (entry/exit).
- Entry No.: It is to set people entry amount. System can generate an alarm once the amount has exceeded the threshold.
- Exit No.: It is to set people exit amount. System can generate an alarm once the amount has exceeded the threshold.
- Remaining No.: It is to set people staying amount in the zone. System can generate an alarm once the amount has exceeded the threshold.

You can refer to the chapter 4.7.1.1 motion detect to set other parameters.

Click OK to complete the setup.



Channel D2 Enable □

Setup RULE

OSD Overlay □ Clear

People Counting Enter No. 0 Leave No. 0 Stranded No. 0

Period Setup

☑ Alarm Out 1 2 3 4 5 6 Latch 0 Sec.

□ Alarm Upload □ Send Email

□ Record Channel Setup Delay 10 Sec.

□ PTZ Activation Setup

□ Tour Setup

☑ Snapshot Setup

☑ Log

□ Voice Prompts File Name None

□ Buzzer

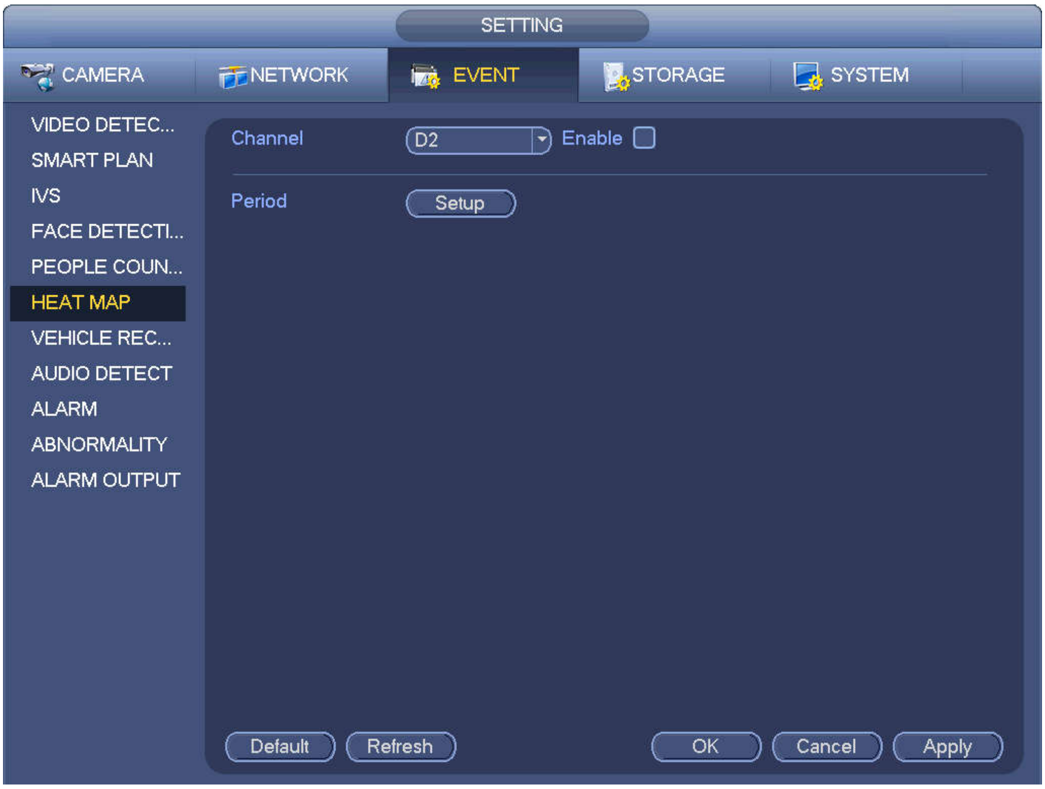
Figure 4-141

After you set the people counting function, from main menu->Info->Event->People counting, you can view people counting statistics report. Please refer to chapter 4.7.1.1 Motion detect for detailed information.

4.7.6 Heat Map

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

Step 1 From main menu->Setting->Event->Heat map.
Enter heat map interface. See Figure 4-142.



Channel D2 Enable □

Period Setup

Figure 4-142

Step 2 Select a channel number and then check the box to enable the function.

Step 3 Click Setup button.

Enter setup interface. See Figure 4-143.

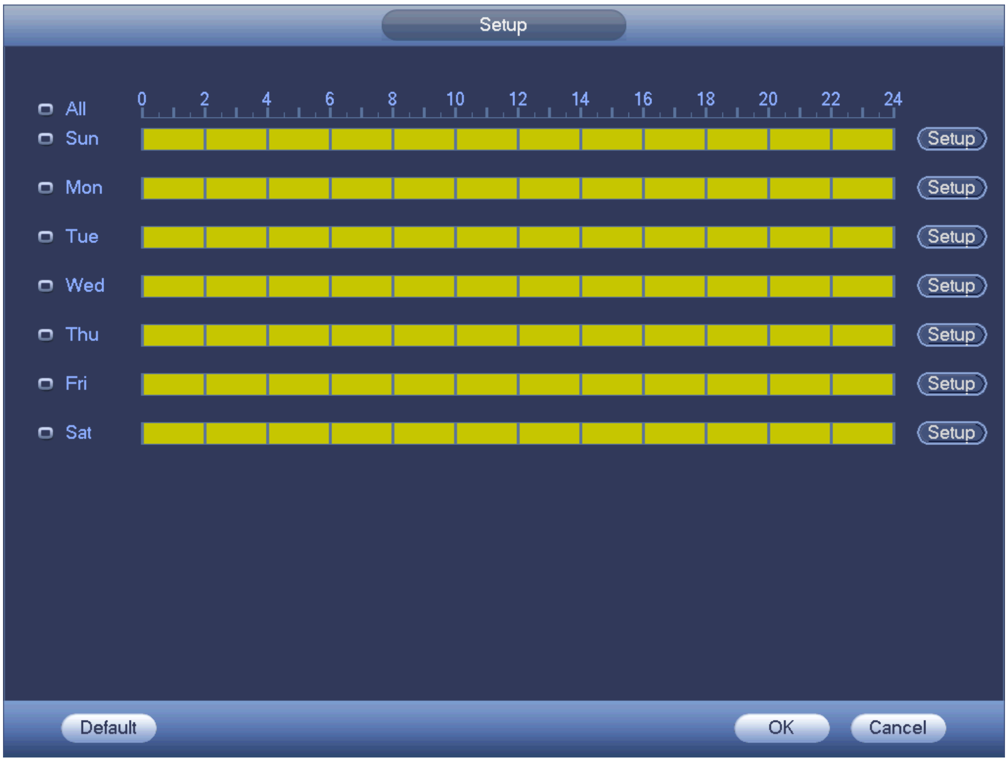


Figure 4-143

Step 4 Set arm/disarm period. Refer to chapter 4.7.1.1 Motion detect for detailed setup information.

Step 5 Click Apply button to complete setup.

Note

After set the heat map parameters, go to main menu->Info->Event->Heat map to view heat map report. Refer to chapter 4.10.2.3.3 for detailed setup information.

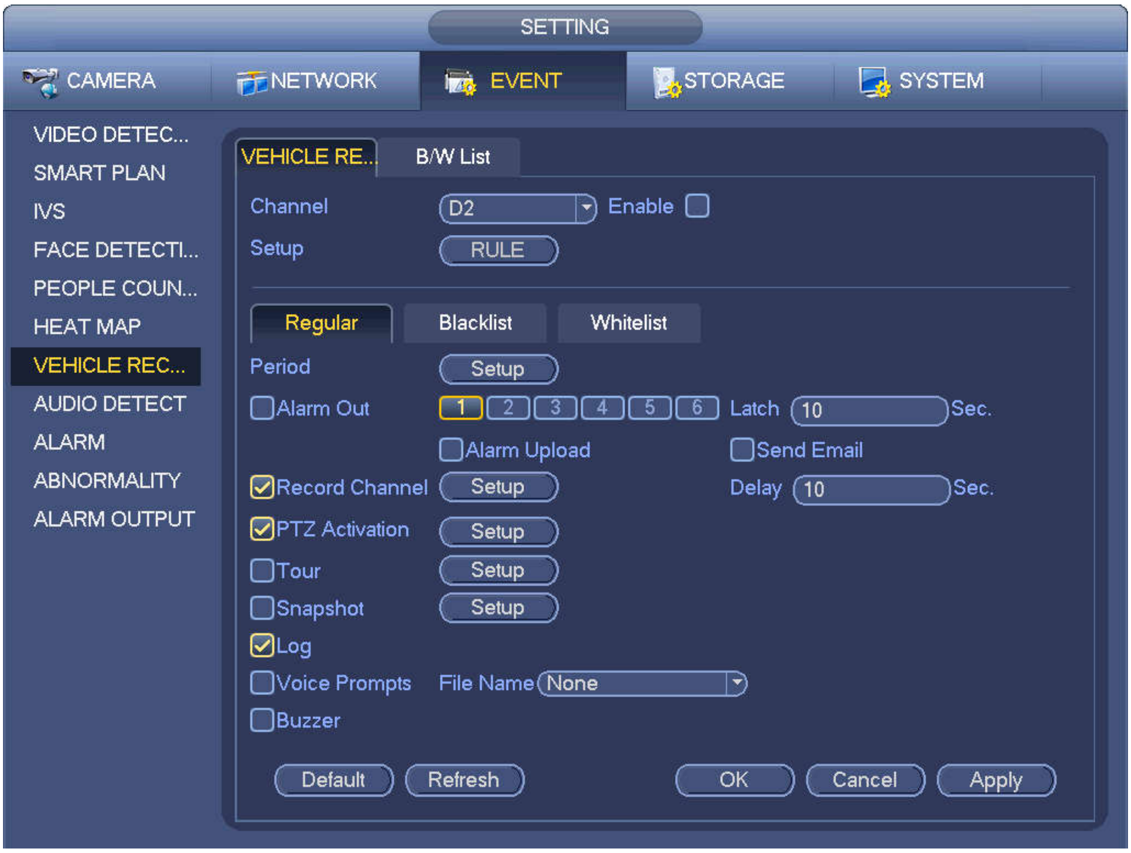
4.7.7 Plate Recognition

4.7.7.1 Plate recognition settings

Device can generate an alarm when it detects the corresponding plate information.

Please follow the steps listed below.

Step 1 From main menu->Setup->Event->Vehicle Recognition-> Vehicle Recognition. Enter Vehicle Recognition interface. See Figure 4-144.



Channel D2 Enable □

Setup RULE

Period Setup

□ Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□ Alarm Upload □ Send Email

☑ Record Channel Setup Delay 10 Sec.

☑ PTZ Activation Setup

□ Tour Setup

□ Snapshot Setup

☑ Log

□ Voice Prompts File Name None

□ Buzzer

Figure 4-144

Step 2 Check Enable to enable plate recognition function.

Step 3 Select a channel number and then click the Rule to set the plate recognition name and detection zone.

Step 4 Click Regular, blacklist, whitelist to set.

Note

Before use blacklist alarm or whitelist alarm function, please add the corresponding plate information. Refer to chapter 4.7.7.2 B/W list for detailed information.

- Regular: In this interface, device triggers an alarm when it detects all plate numbers.
- Blacklist: In this interface, device triggers an alarm when it detects plate number in the blacklist.

- Whitelist: In this interface, device triggers an alarm when it detects plate number in the whitelist.

4.7.7.2 B/W List

It is to set the blacklist and the whitelist. It includes add, delete, import, export blacklist/whitelist.

After setting the blacklist/whitelist, in the plate snapshot list on the preview interface, the blacklist plate number is red, the whitelist plate number is green, the regular plate number is white.

Add blacklist/whitelist

Step 1 From main menu->Setting->Event->Vehicle Recognition->B/W list.

Enter B/W list interface. See Figure 4-145.

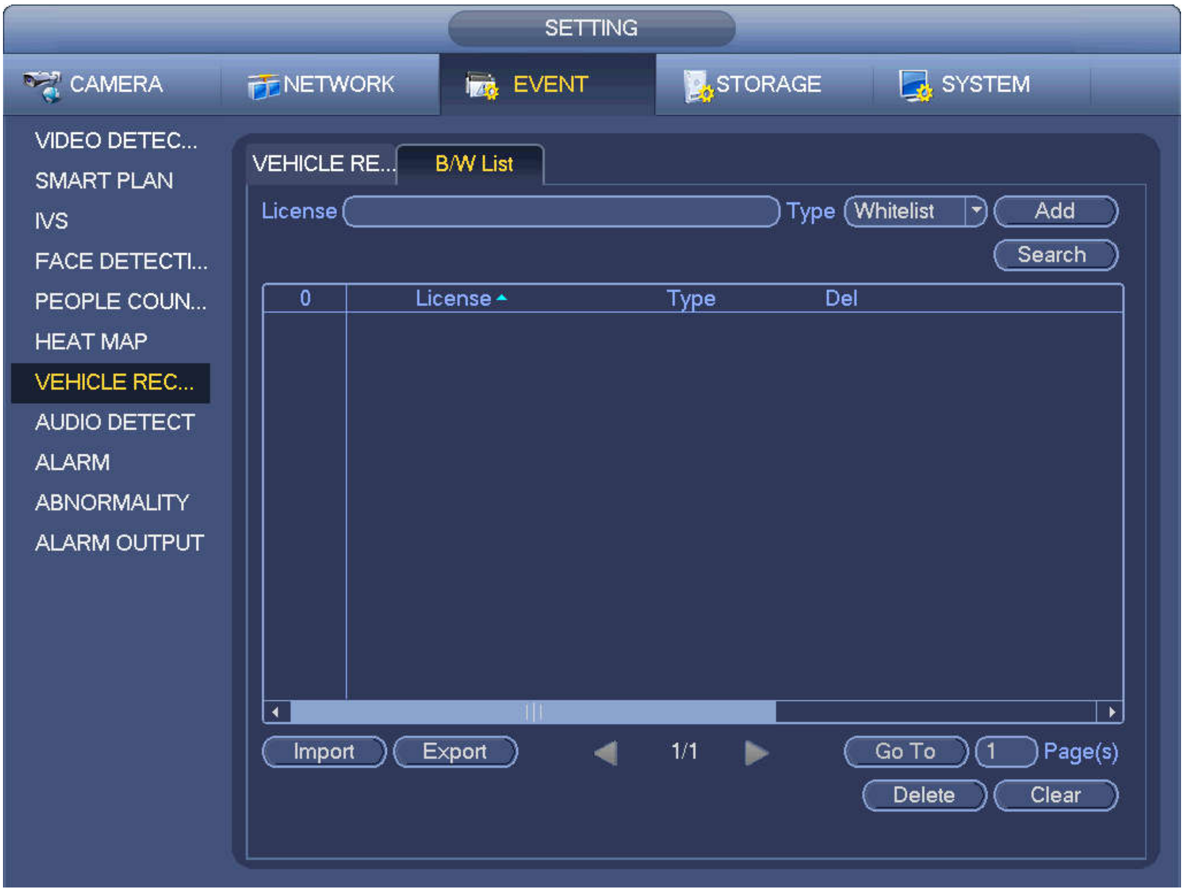


Figure 4-145

Step 2 Set plate number and then select type as blacklist or whitelist.

Step 3 Click Add button.

Delete blacklist/whitelist

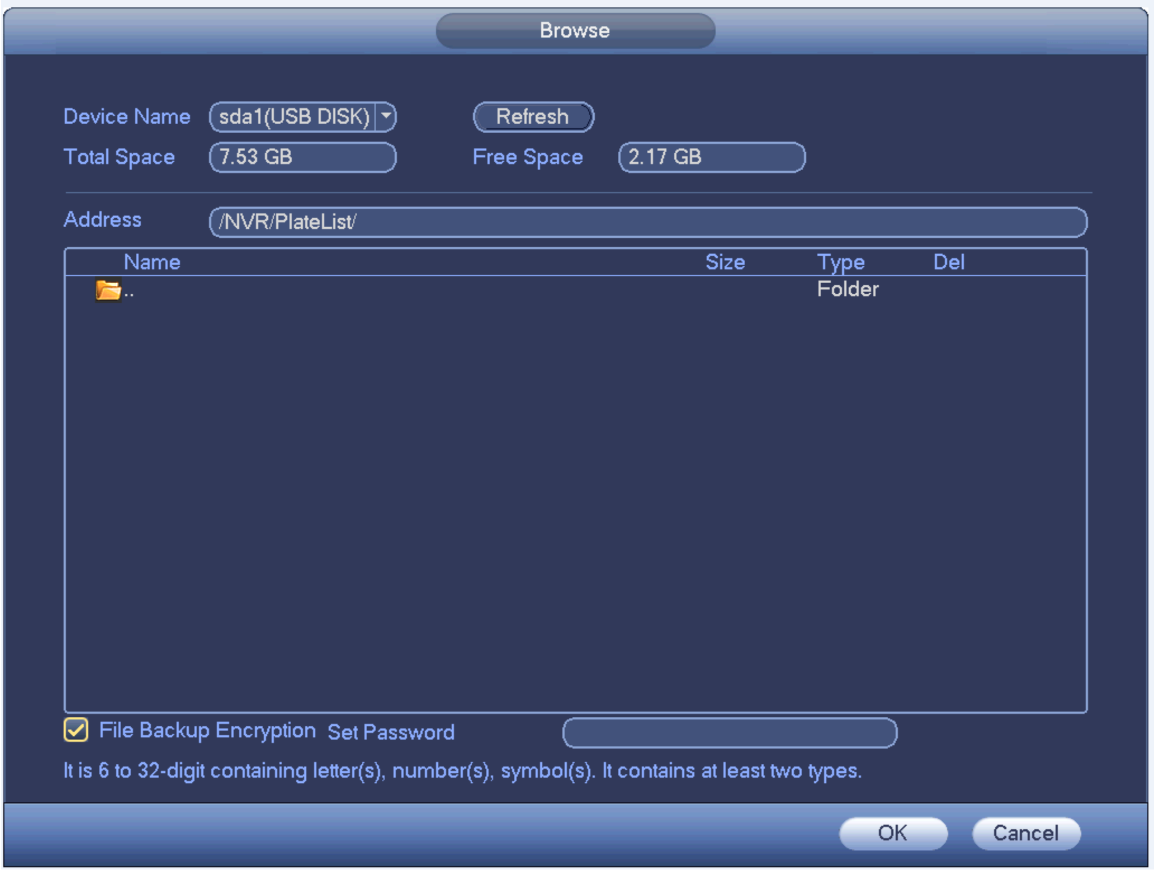
Set type as blacklist, whitelist or all, click Search button, device displays the corresponding information.

- Check the box before the plate number and then click Delete or ✖ to delete a plate number.
- Click Clear to delete all plate information in the blacklist/whitelist.

Import/export blacklist/whitelist

Device supports blacklist/whitelist import/export function via the USB device. The import file supports .csv and xlsx. The export file is .csv.

- Import blacklist/whitelist: Set the type as blacklist or whitelist and then click Import button. Select the corresponding file and then click Open button to import.
- Export blacklist/whitelist: Set the type as blacklist or whitelist and then click Export button. The Browse interface is displayed. See Figure 4-146. Select the file save path, enter the encryption password, and then click Save.



It is 6 to 32-digit containing letter(s), number(s), symbol(s). It contains at least two types.

Figure 4-146

NOTE

Backup encryption is enabled by default when exporting the black/white list.

- If file backup encryption is enabled, the extension name of the exported file is .backup.
- If the backup encryption is disabled, the extension name of the exported file is .csv. It might lead to data leakage.

4.7.8 Audio Detect (Optional)

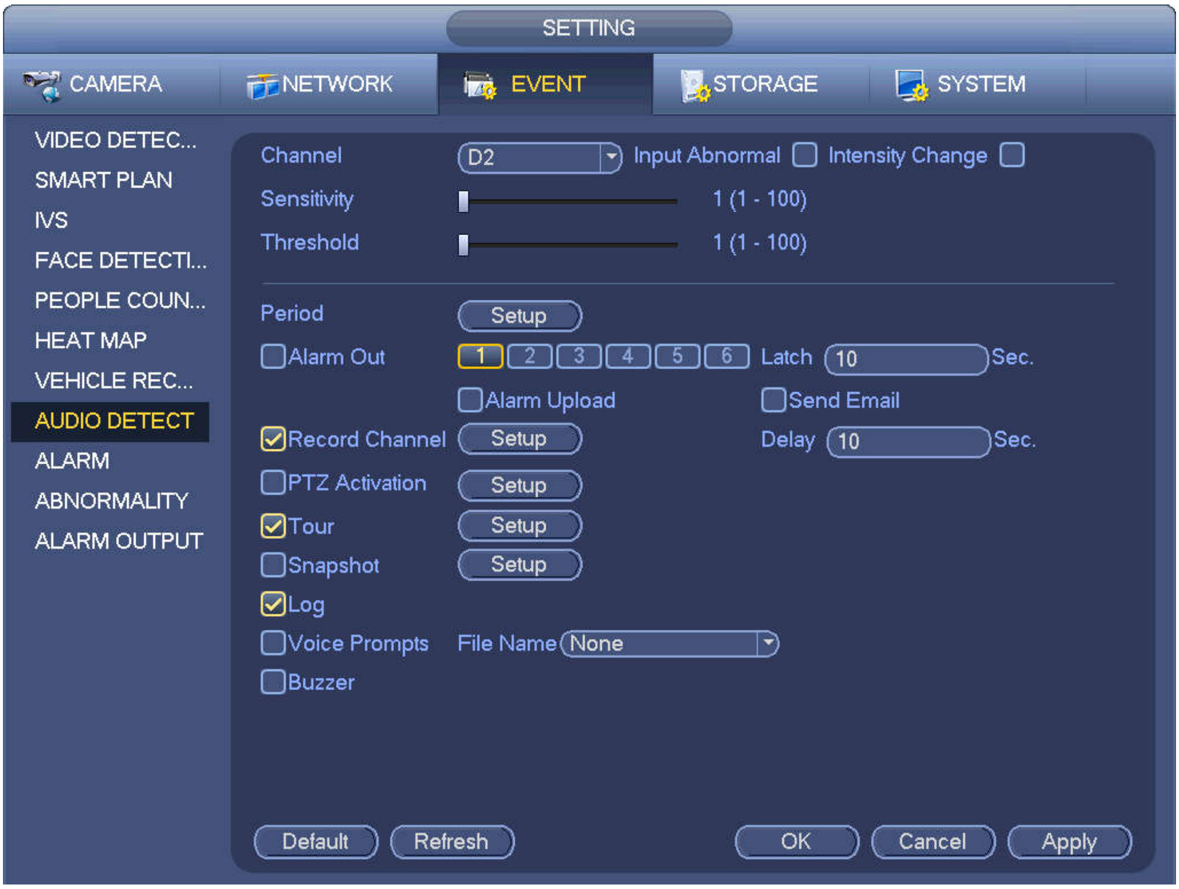
System can generate an alarm once it detect the audio is not clear, the tone color has changed or the is abnormal or audio volume changes.

From main menu->Setting->Event->Audio detect, you can see an interface shown as in Figure 4-147.

- Input abnormal: Check the box here, system can generate an alarm once the audio input is abnormal.
- Intensity change: Check the box here, system can generate an alarm once the audio volume becomes strong.
- Sensitivity: It refers to the audio recognition sensitivity. The higher the value is, the higher the sensitivity is.

- Threshold: It is to set intensity change threshold. The smaller the value is, the higher the sensitivity is.
- Log: Check the box here, system can record audio detect alarm log.

Refer to the chapter 4.7.1.1 Motion Detect to set other parameters.



Channel D2 Input Abnormal □ Intensity Change □

Sensitivity 1 (1 - 100)

Threshold 1 (1 - 100)

Period Setup

□Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□Alarm Upload □Send Email

☑Record Channel Setup Delay 10 Sec.

□PTZ Activation Setup

☑Tour Setup

□Snapshot Setup

☑Log

□Voice Prompts File Name None

□Buzzer

Figure 4-147

4.7.9 Alarm Settings

In the main menu, from Setting->Event->Alarm, you can see alarm setup interface.

- Alarm in: Here is for you to select channel number.

In the main menu, from Setting->Event->Alarm, you can see alarm setup interface. See Figure 4-148.

There are four alarm types. See Figure 4-148 to Figure 4-151.

✧ Local alarm: After connect the alarm device to the NVR alarm input port, system can trigger the corresponding alarm operations when there is alarm signal from the alarm input port to the NVR.

✧ Network alarm: NVR trigger corresponding alarm operations when it receives the alarm signal via the network transmission.

✧ IPC external alarm: When the network camera connected peripheral device has triggered an alarm, it can upload the alarm signal to the NVR via the network transmission. The system can trigger the corresponding alarm operations.

✧ IPC offline alarm: When the network connection between the NVR and the network camera is off, the system can trigger the corresponding alarm operations.

- Enable: Please you need to highlight this button to enable current function.
- Type: normal open or normal close.
- Period: Click set button, you can see an interface is shown as in Figure 4-153. There are two ways for you to set periods. There are max 6 periods in one day. There are four record types: regular,

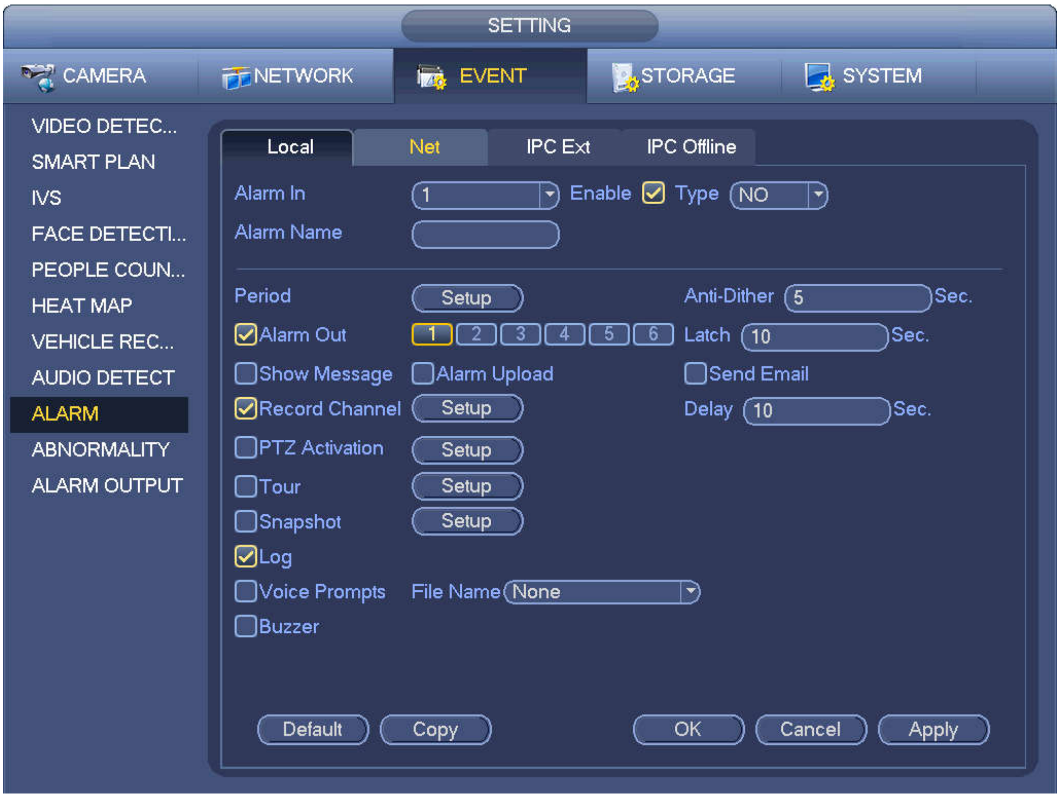
motion detection (MD), Alarm, MD & alarm.

- ✧ In Figure 4-153, Select icon ▢ of several dates, all checked items can be edited together. Now the icon is shown as 🔗. Click ✎ to delete a record type from one period.
- ✧ In Figure 4-153. Click button ⚙ after one date or a holiday, you can see an interface shown as in Figure 4-154. There are four record types: regular, motion detection (MD), Alarm, MD & alarm.

- PTZ activation: When an alarm occurred, system can activate the PTZ operation. The PTZ activation lasts an anti-dither period. See Figure 4-152.
- Anti-dither: Here you can set anti-dither time. The value ranges from 5 to 600s. The anti-dither time refers to the alarm signal lasts time. It can be seem as the alarm signal activation stays such as the buzzer, tour, PTZ activation, snapshot, channel record. The stay time here does not include the latch time. During the alarm process, the alarm signal can begin an anti-dither time if system detects the local alarm again. The screen prompt, alarm upload, email and etc will not be activated. For example, if you set the anti-dither time as 10 second, you can see the each activation may last 10s if the local alarm is activated. During the process, if system detects another local alarm signal at the fifth second, the buzzer, tour, PTZ activation, snapshot, record channel will begin another 10s while the screen prompt, alarm upload, email will not be activated again. After 10s, if system detects another alarm signal, it can generate an alarm since the anti-dither time is out.
- Alarm output: The number here is the device alarm output port. You can select the corresponding ports(s) so that system can activate the corresponding alarm device(s) when an alarm occurred.
- Latch: When the anti-dither time ended, the channel alarm you select in the alarm output may last the specified period. The value ranges from 1 to 300 seconds. This function is not for other alarm activation operations. The latch is still valid even you disable the alarm event function directly.
- Show message: System can pop up a message to alarm you in the local host screen if you enabled this function.
- Alarm upload: System can upload the alarm signal to the network (including alarm center and the WEB) if you enabled current function. System only uploads the alarm channel status. You can go to the WEB and then go to the Alarm interface to set alarm event and alarm operation. Please go to the Network interface to set alarm center information.
- Send email: System can send out the alarm signal via the email to alert you when alarm occurs. Once you enable the snap function, system can also send out an image as the attachment. Please go to the Main Menu->Setting ->Network->Email interface to set.
- Record channel: you can select proper channel to record alarm video (Multiple choices).
  - ✧ You need to set alarm record mode as Schedule in Record interface (Main Menu->Advanced->Record). Please note the manual record has the highest priority. System record all the time no matter there is an alarm or not if you select Manual mode.
  - ✧ Now you can go to the Schedule interface (Main Menu->Setting->Schedule) to set the record type, corresponding channel number, week and date. You can select the record type:Regular/MD/Alarm/MD&Alarm. Please note, you cannot select the MD&Alarm and MD(or Alarm) at the same time.
  - ✧ Now you can go to the Encode interface to select the alarm record and set the encode parameter (Main Menu->Setting->Encode).

✧ Finally, you can set the alarm input as the local alarm and then select the record channel. The select channel begins alarm record when an alarm occurred. Please note system begins the alarm record instead of the MD record if the local alarm and MD event occurred at the same time.

- Tour: Here you can enable tour function when an alarm occurs. System supports 1/8-window tour. Please go to chapter4.3.6.2 Display for tour interval setup. Please note the tour setup here has higher priority than the tour setup you set in the Display interface. Once there two tours are both enabled, system can enable the alarm tour as you set here when an alarm occurred. If there is no alarm, system implements the tour setup in the Display interface.
- Snapshot: You can enable this function to snapshot image when an alarm occurs.
- Buzzer: Highlight the icon to enable this function. The buzzer beeps when an alarm occurs.



Alarm In 1 Enable ☑ Type NO

Alarm Name

Period Setup Anti-Dither 5 Sec.

☑Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□Show Message □Alarm Upload □Send Email

☑Record Channel Setup Delay 10 Sec.

□PTZ Activation Setup

□Tour Setup

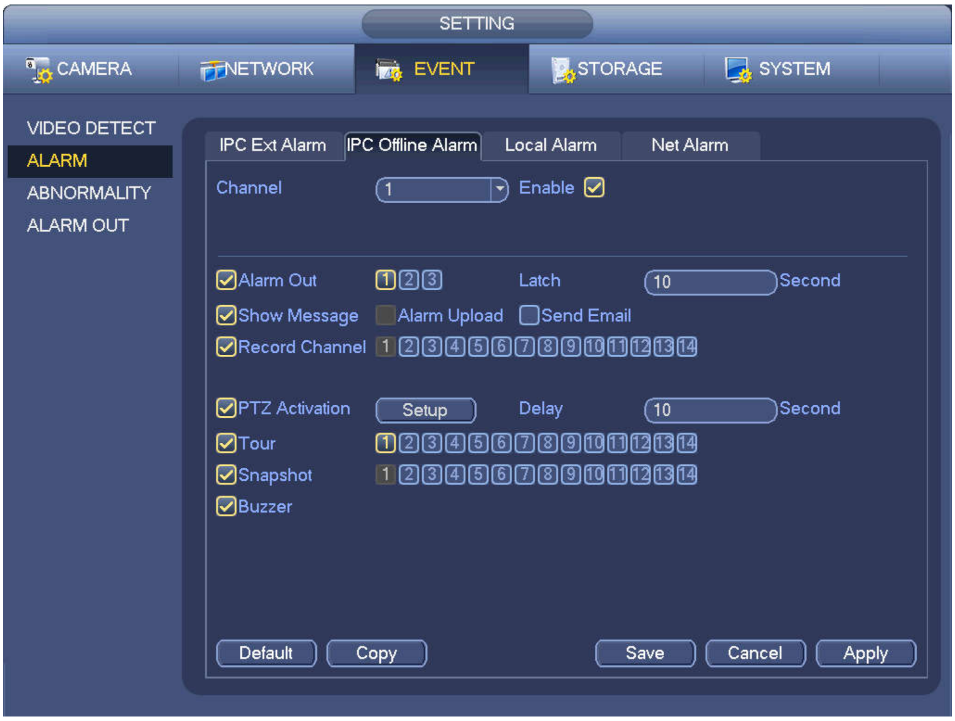
□Snapshot Setup

☑Log

□Voice Prompts File Name None

□Buzzer

Figure 4-148



Channel 1 Enable ☑

☑Alarm Out 1 2 3 Latch 10 Second

☑Show Message □Alarm Upload □Send Email

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

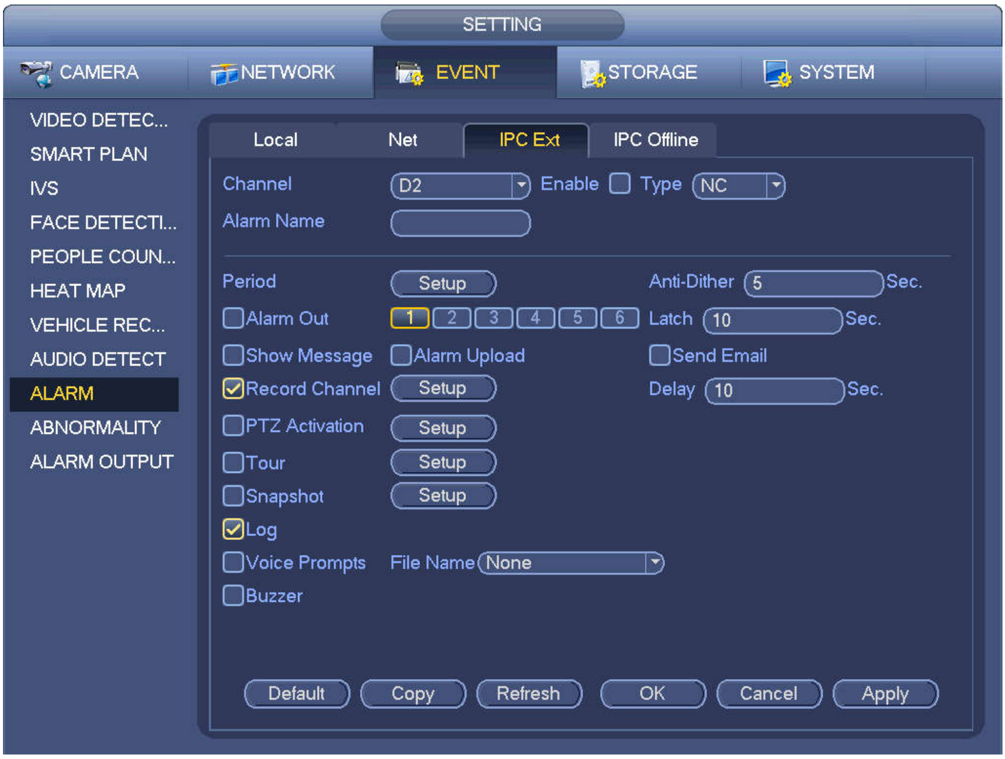
☑PTZ Activation Setup Delay 10 Second

☑Tour 1 2 3 4 5 6 7 8 9 10 11 12 13 14

☑Snapshot 1 2 3 4 5 6 7 8 9 10 11 12 13 14

☑Buzzer

Figure 4-149



Channel D2 Enable □ Type NC

Alarm Name

Period Setup Anti-Dither 5 Sec.

□Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

□Show Message □Alarm Upload □Send Email

☑Record Channel Setup Delay 10 Sec.

□PTZ Activation Setup

□Tour Setup

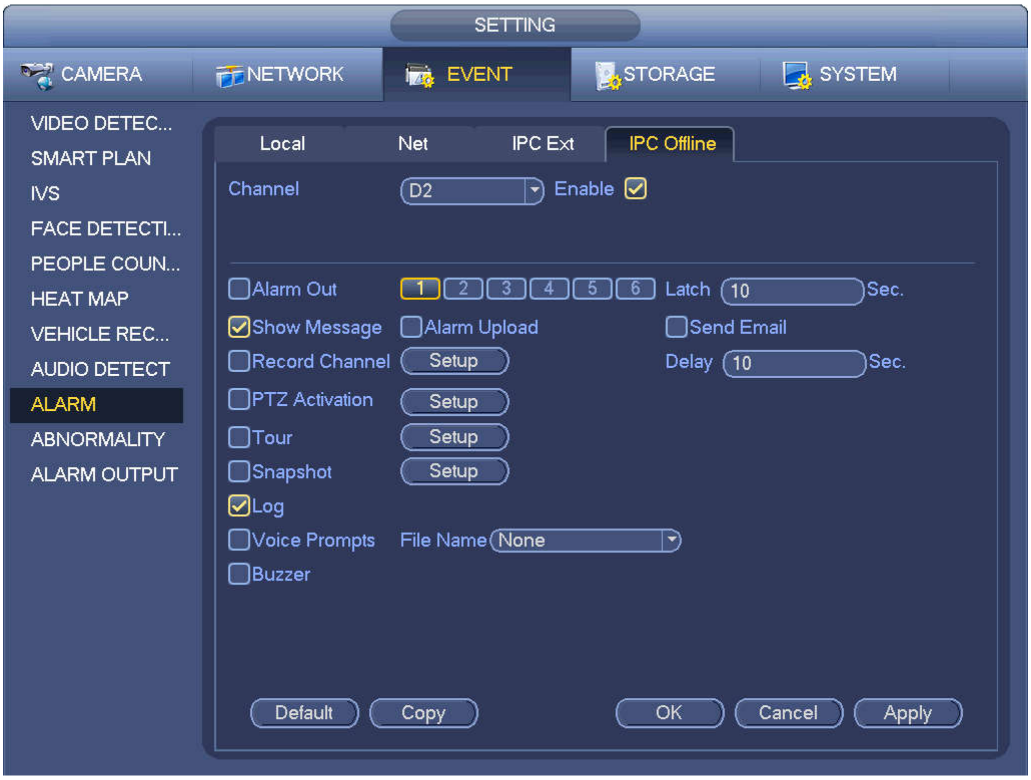
□Snapshot Setup

☑Log

□Voice Prompts File Name None

□Buzzer

Figure 4-150



Channel D2 Enable ☑

□Alarm Out 1 2 3 4 5 6 Latch 10 Sec.

☑Show Message □Alarm Upload □Send Email

□Record Channel Setup Delay 10 Sec.

□PTZ Activation Setup

□Tour Setup

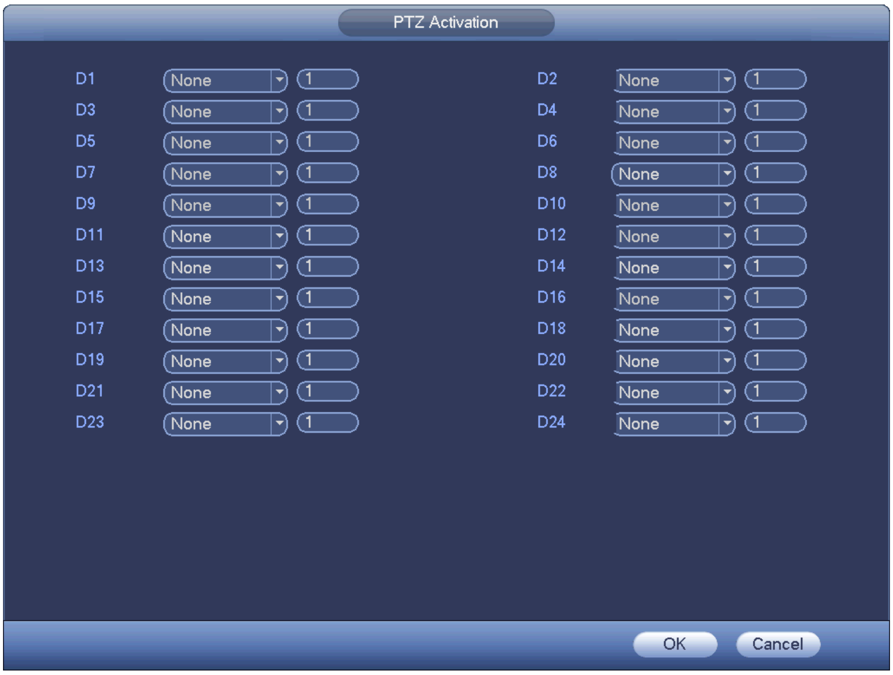
□Snapshot Setup

☑Log

□Voice Prompts File Name None

□Buzzer

Figure 4-151



D1	None	1	D2	None	1
D3	None	1	D4	None	1
D5	None	1	D6	None	1
D7	None	1	D8	None	1
D9	None	1	D10	None	1
D11	None	1	D12	None	1
D13	None	1	D14	None	1
D15	None	1	D16	None	1
D17	None	1	D18	None	1
D19	None	1	D20	None	1
D21	None	1	D22	None	1
D23	None	1	D24	None	1

Figure 4-152

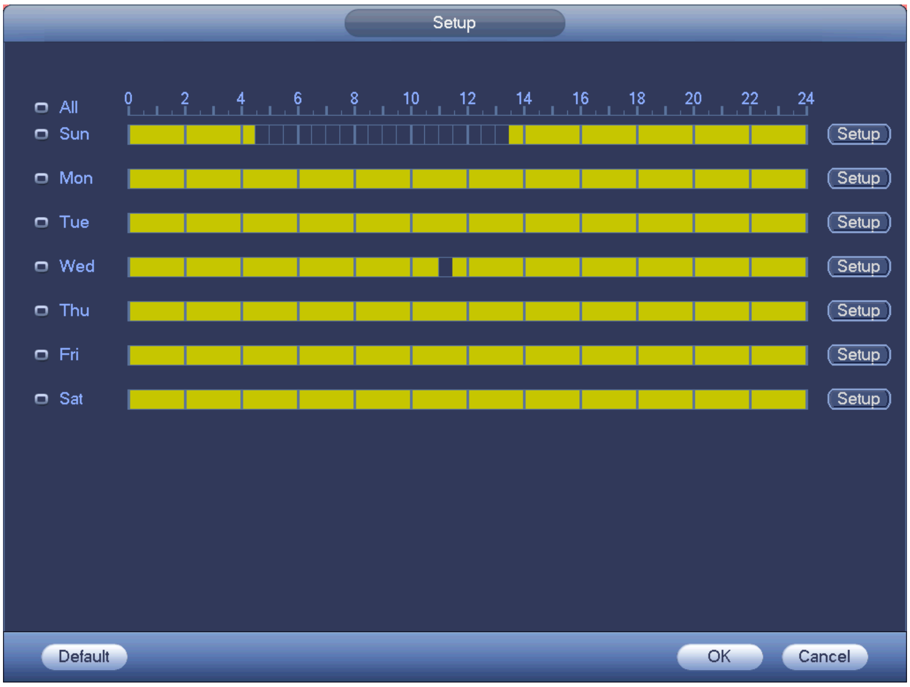
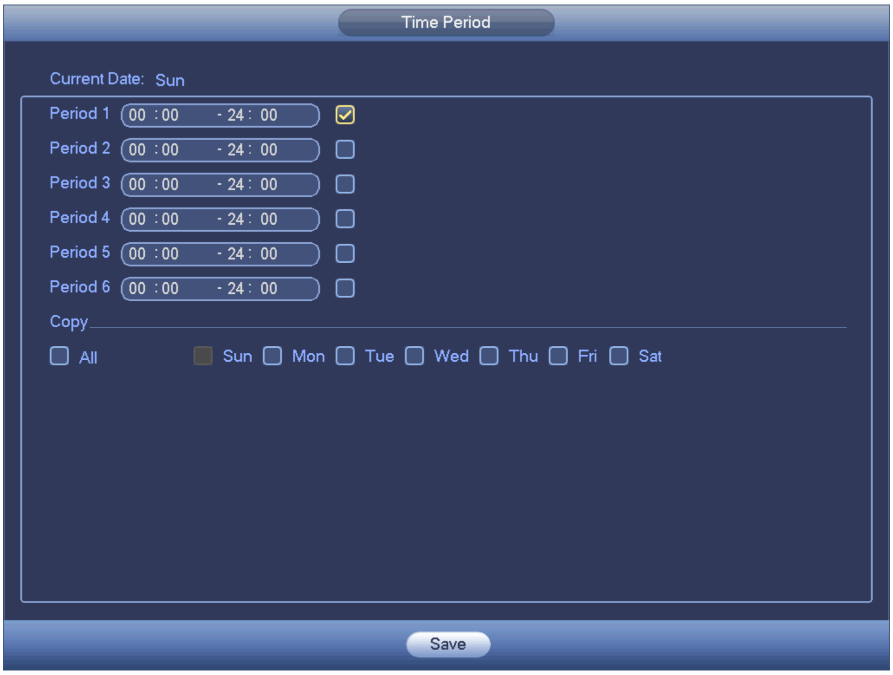


Figure 4-153



Current Date: Sun

Period 1 00 : 00 - 24 : 00 ☑
Period 2 00 : 00 - 24 : 00 □
Period 3 00 : 00 - 24 : 00 □
Period 4 00 : 00 - 24 : 00 □
Period 5 00 : 00 - 24 : 00 □
Period 6 00 : 00 - 24 : 00 □

Copy

□ All ■ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Figure 4-154

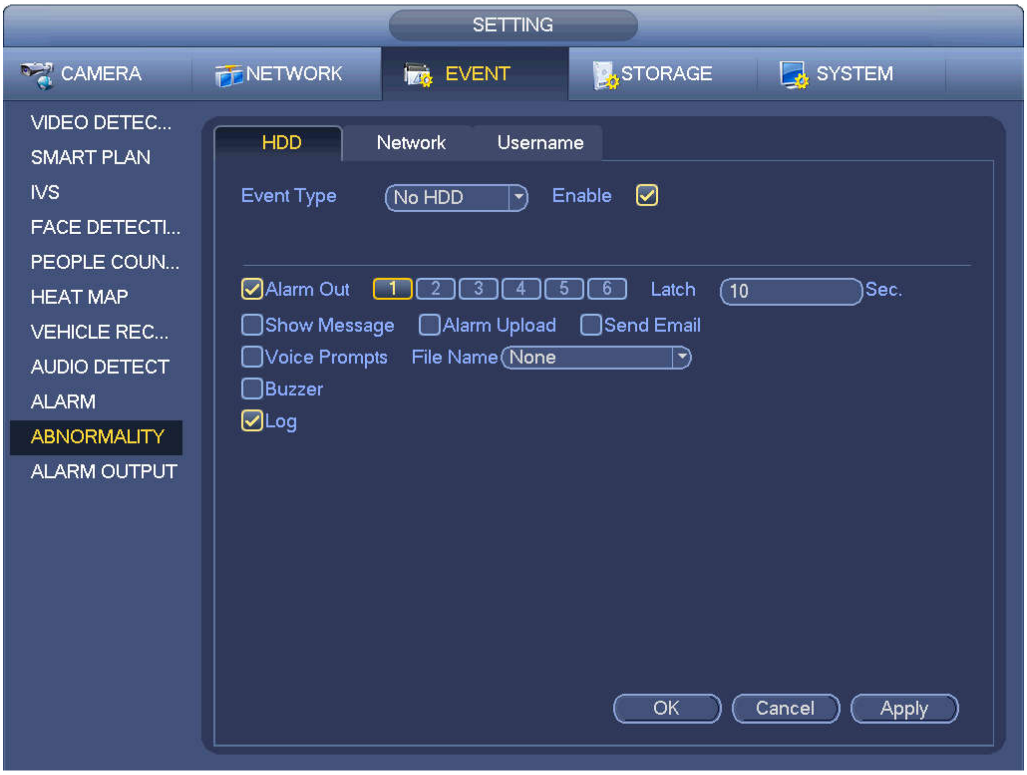
Please highlight icon □ to select the corresponding function. After setting all the setups please click save button.

4.7.10 Abnormality

There are three types: Disk/Network/User.

- ✧ Disk: Disk error, no disk, no space. See Figure 4-155.
- ✧ Network: Disconnection, IP conflict, MAC conflict. See Figure 4-156.
- ✧ User: Illegal login. Figure 4-157.

- Alarm output: Please select alarm activation output port (multiple choices).
- Less than: System can alarm you when the HDD space is less than the threshold you set here (For HDD no space type only).
- Attempts: In user interface, select illegal login from the dropdown list. Here you can set login attempts. The value ranges from 1 to 10.
- Lock time: In user interface, select illegal login from the dropdown list. Here you can set account lock time. The value ranges from 1 to 30 minutes.
- Latch: Here you can set corresponding delaying time. The value ranges from 1s-300s. System automatically delays specified seconds in turning off alarm and activated output after external alarm cancelled.
- Show message: system can pop up the message in the local screen to alert you when alarm occurs.
- Alarm upload: System can upload the alarm signal to the network (including alarm center) if you enabled current function. For disconnection event, IP conflict event and MAC conflict event, this function is null.
- Send email: System can send out email to alert you when alarm occurs.
- Buzzer: Highlight the icon to enable this function. The buzzer beeps when an alarm occurs.



Event Type: No HDD Enable ☑

☑ Alarm Out [1] 2 3 4 5 6 Latch 10 Sec.

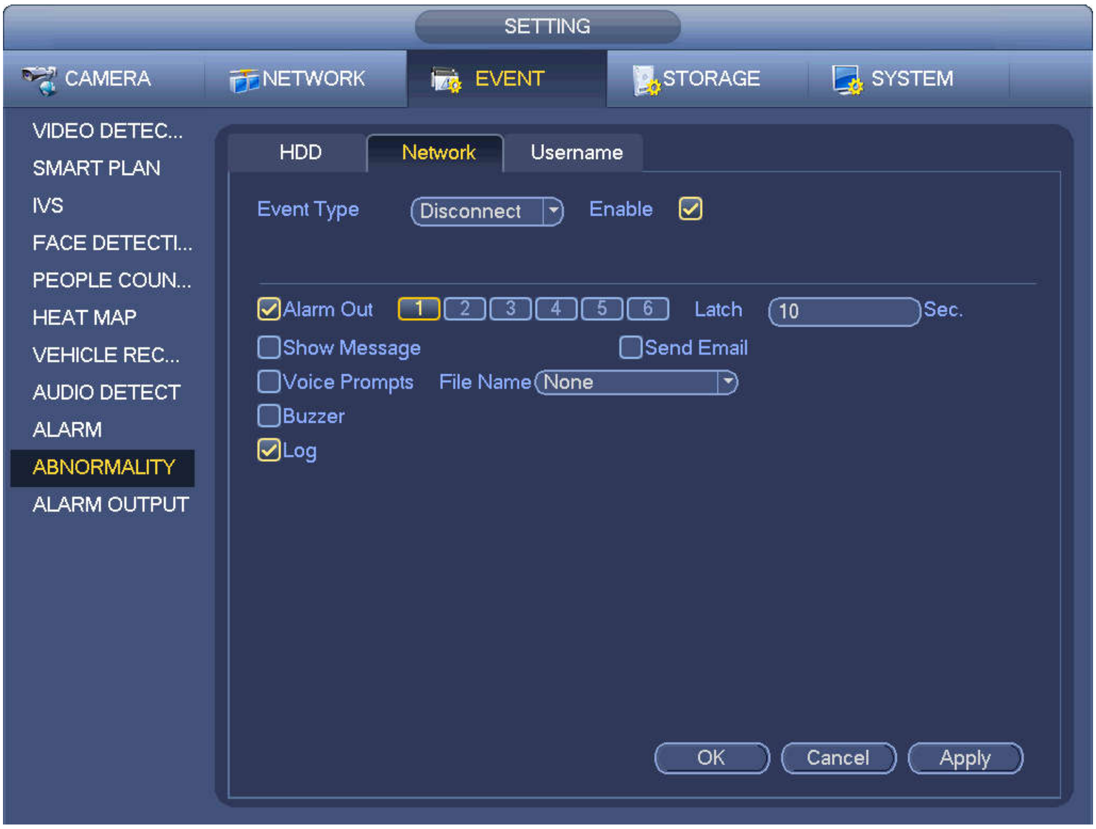
□ Show Message □ Alarm Upload □ Send Email

□ Voice Prompts File Name None

□ Buzzer

☑ Log

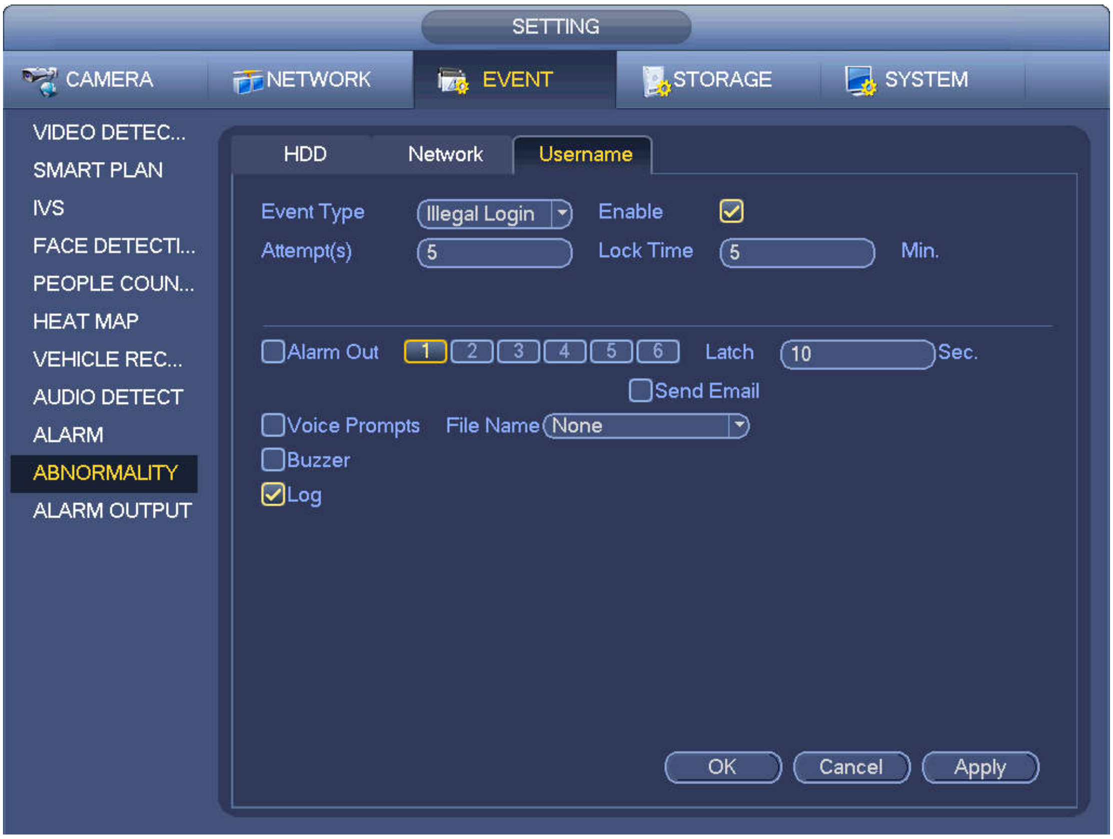
Figure 4-155



Event Type: Disconnect
Enable ☑

☑ Alarm Out 1 2 3 4 5 6 Latch 10 Sec.
□ Show Message □ Send Email
□ Voice Prompts File Name None
□ Buzzer
☑ Log

Figure 4-156



Event Type: Illegal Login
Enable ☑
Attempt(s) 5
Lock Time 5 Min.

□ Alarm Out 1 2 3 4 5 6 Latch 10 Sec.
□ Send Email
□ Voice Prompts File Name None
□ Buzzer
☑ Log

Figure 4-157

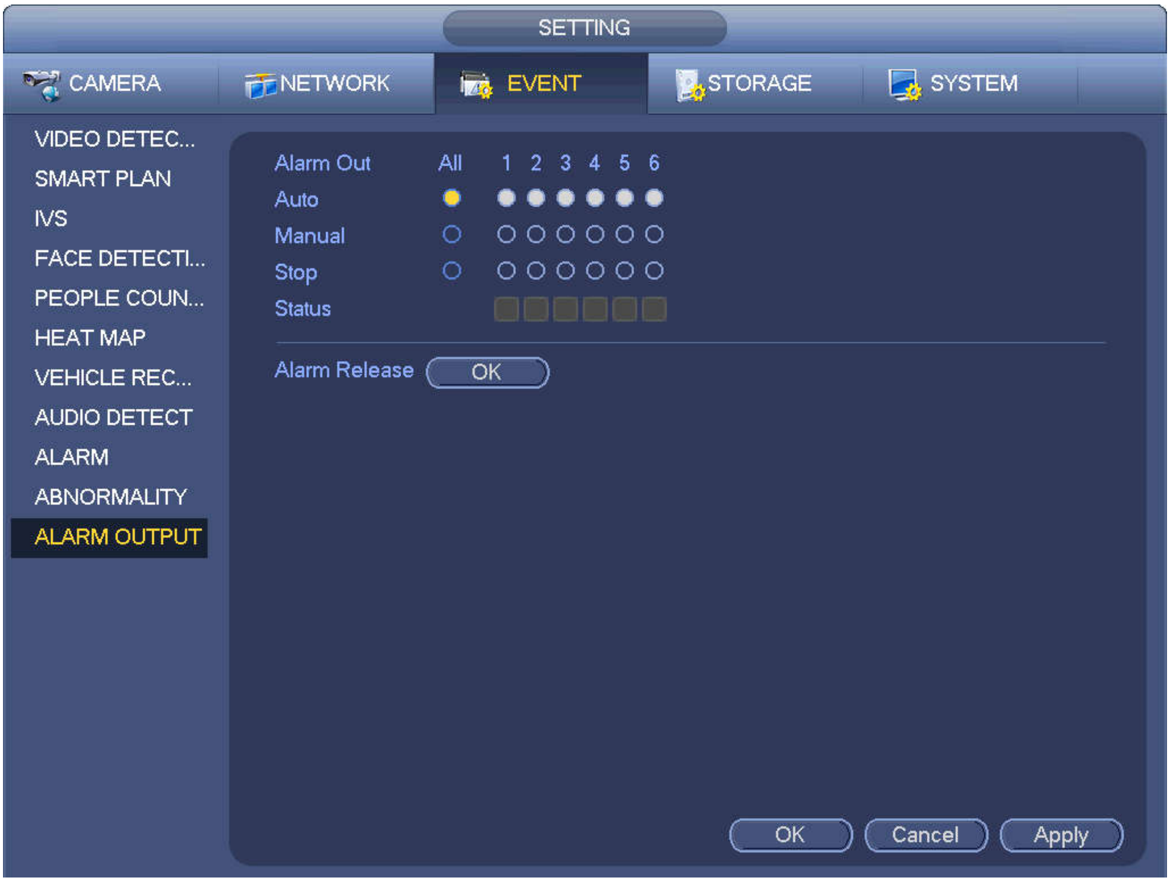
4.7.11 Alarm output

From Main menu->Setting->Event->Alarm output, you can see an interface shown as in Figure 4-158.

Here is for you to set proper alarm output (Auto/manual/stop). Connect the alarm device to the system alarm output port, and set the mode as auto, system can trigger the corresponding operations when an alarm occurs.

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

Click OK button of the alarm reset, you can clear all alarm output status.



Alarm Out	All	1	2	3	4	5	6
Auto	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○
Status		■	■	■	■	■	■

Alarm Release OK

Figure 4-158

Please highlight icon ■ to select the corresponding alarm output.

After all the setups please click OK button.

4.7.12 POS

Connect the device with the POS, the device can receive the POS information and overlay corresponding info on the video.

Note

- For the local-end, this function supports 1/4-window display and 1-window playback.
- This function is for the cashier of the supermarket and etc. The device can get the information from the POS and then overlay the txt information on the video.

Step 1 From main menu->Setting->System->POS, the interface is shown as below. See Figure 4-159.

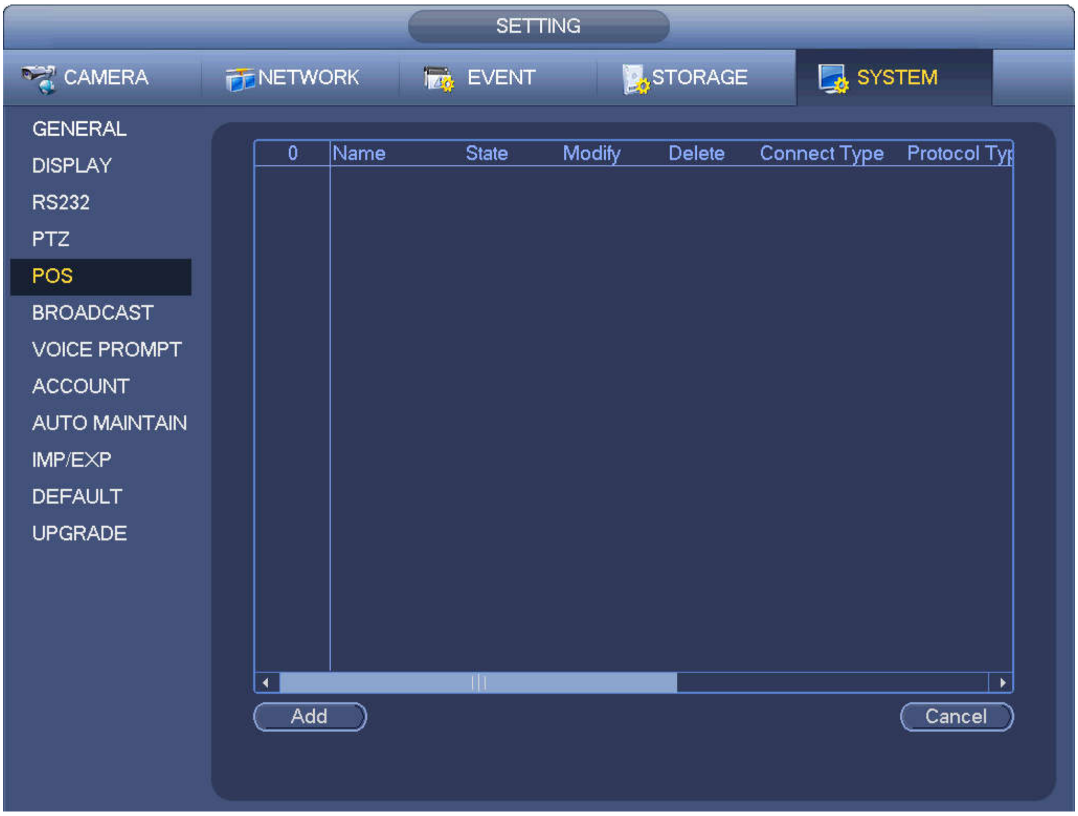


Figure 4-159

Step 2 Click Add button, the interface is shown as below. See Figure 4-160.

Set parameters.

- Enable: Check the box to enable POS function.
- Name: Set POS name.

1. Click ✎
2. Input POS name on the pop-up dialogue box.
3. Click OK button.

Note

The POS name shall be unique.

System max supports 64 English letters.

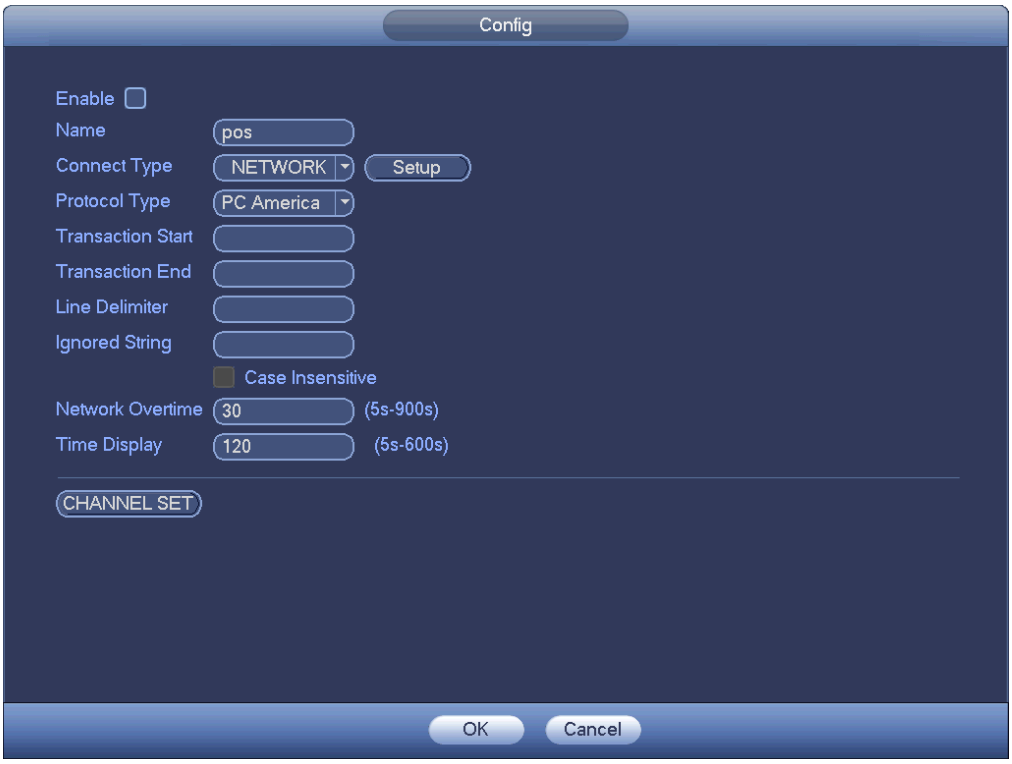
- Event: Set POS arm/disarm period, record channel and etc. Click Setup to go to the interface. For detailed information, please refer to chapter 4.7.1.1 motion detect.
- Privacy：After enable this function, once the overlay information contain the privacy character, it displays as *. For example, the privacy character is 12,56,89, the local preview and WEB surveillance information is shown as **34**7** if the overlay information is 123456789. For detailed information, please refer to chapter 4.7.12.1 privacy setup.
- Protocol type: The default setup is POS.
- Connection type: It is to set and NVR connection mode. It includes UDP,TCP,RS232,RS485. After set the connection type, please click the Setup button to set the corresponding parameters. For detailed information, please refer to chapter 4.7.12.2 connection type.
- Convert: It is to set font type.
- Overlay: It is to set overlay mode. It includes turn and roll.

  - Turn: Once the overlay information has reached 8 lines, NVR turn to the next page.
  - Roll: Once the overlay information has reached 8 lines, NVR displays the next new line and delete the oldest line.
- Network overtime: Once there is no POS data for the specified period, NVR automatically deletes POS information after specified period.
- Font size: The overlay font size.
- Color: The overlay font color.
- POS Info: Check the box to overlay information on the local preview window.
- Advanced: Click ︾ to enter advanced settings interface.
- Transaction start/transaction end: It is to set transaction start and end character. The overlay information only displays the character after the start string and before the end string. For example, the start character is 12 and the end character is 90, NVR displays 34567 on local preview and Web preview interface if the sending out information is 123456789.
- Line delimiter: After set the line delimiter, the overlay information after the delimiter is displayed in the new line. For example, the line delimiter is 45 and the overlay information is 123456789, NVR displays 123 in the first line and displays 6789 in the second line.
- Hex: Check the Hex to switch ASCII code.
- Case insensitive: Check the box to enable case insensitive function.
  - When this function is enabled, set the start character as “aa”, NVR cannot distinguish the upper and lower case when sending out information “11aA23456”. The NVR overlays information is “23456” on local surveillance and Web preview.
  - When this function is disabled, set the start character as “aa”, NVR can distinguish the upper and lower case when sending out information “11aA23456”. The NVR does not overlay information local surveillance and Web preview.

4.7.12.1 Privacy Setup

Step 1 Click Setup

Enter Setup interface. See Figure 4-160,



Config

Enable ☐

Name: pos

Connect Type: NETWORK

Protocol Type: PC America

Transaction Start:

Transaction End:

Line Delimiter:

Ignored String:

☐ Case Insensitive

Network Overtime: 30 (5s-900s)

Time Display: 120 (5s-600s)

Figure 4-160

Step 2 Set privacy information.

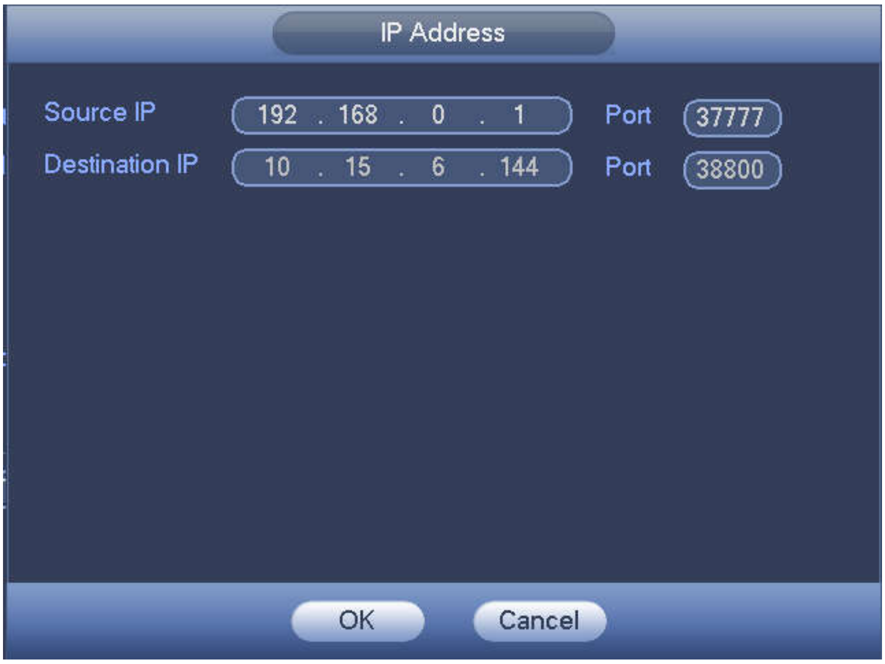
Step 3 Click OK button.

4.7.12.2 Connection type

- **Connection type is UDP or TCP.**

Step 1 Click Setup.

Enter Setup interface. See Figure 4-161.



IP Address

Source IP: 192 . 168 . 0 . 1 Port: 37777

Destination IP: 10 . 15 . 6 . 144 Port: 38800

Figure 4-161

Step 2 Source IP and port refers to POS IP address and port.

Note

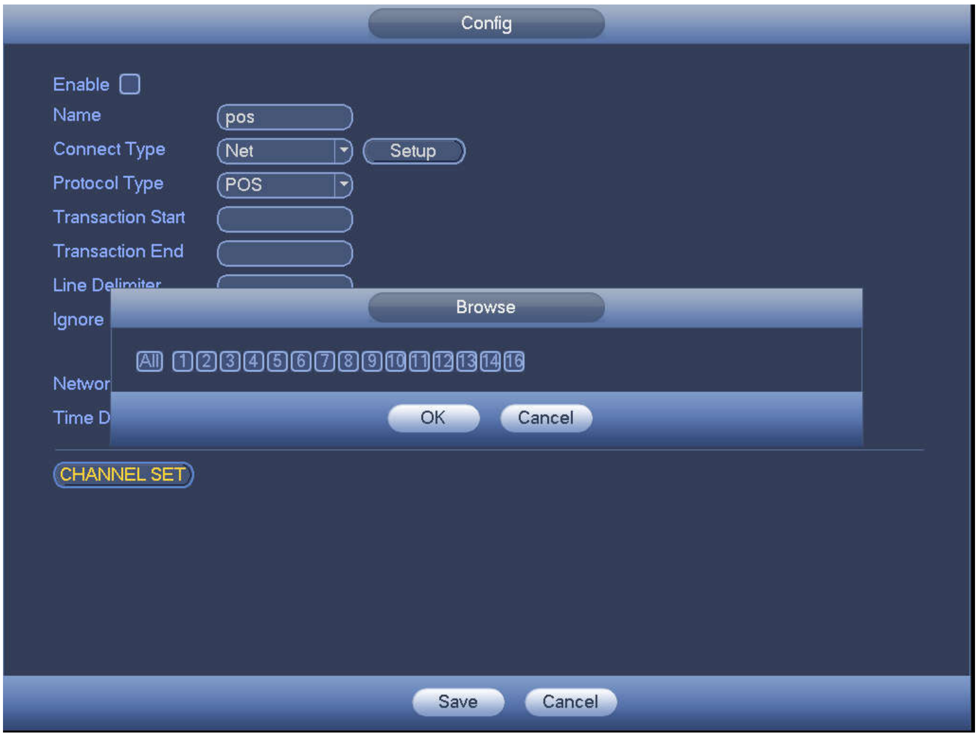
Destination IP and port refers to NVR IP address and port. System can auto get and display.

Step 3 Click OK to complete setup.

- **Connection mode is RS232 or RS485.**

Step 1 Click Setup.

Enter Setup interface. See Figure 4-162.



Config

Enable □

Name: pos

Connect Type: Net

Protocol Type: POS

Transaction Start

Transaction End

Line Delimiter

Ignore

Networ

Time D

Browse

All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 16

Figure 4-162

Step 2 Set address, baud rate, data bit, stop bit and parity.

Note

Make sure the parameters here are the same with the POS setup.

Step 3 Click OK to complete setup.

4.8 Network

4.8.1 Network Settings

4.8.1.1 TCP/IP

The single network adapter interface is shown as in Figure 4-163 and the dual network adapters interface is shown as in Figure 4-164.

- Network Mode : Includes multiple access, fault tolerance, and load balancing
  - ✧ Multiple-address mode: eth0 and eth1 operate separately. You can use the services such as HTTP, RTP service via etho0 or the eth1. Usually you need to set one default card (default setup is etho) to request the auto network service form the device-end such as DHCP, email, FTP and etc. In multiple-address mode, system network status is shown as offline once one card is offline.

- ✧ Network fault-tolerance: In this mode, device uses bond0 to communicate with the external devices. You can focus on one host IP address. At the same time, you need to set one master card. Usually there is only one running card (master card).System can enable alternate card when the master card is malfunction. The system is shown as offline once these two cards are both offline. Please note these two cards shall be in the same LAN.
- ✧ Load balance: In this mode, device uses bond0 to communicate with the external device. The eth0 and eth1 are both working now and bearing the network load. Their network load are general the same. The system is shown as offline once these two cards are both offline. Please note these two cards shall be in the same LAN.

- Default Network Card: Please select eth0/eth1/bond0(optional) after enable multiple-access function
- Main Network Card: Please select eth0/eth1 (optional).after enable multiple access function.

Note: The dual-Ethernet port series support the above three configurations and supports functions as multiple-access, fault-tolerance and load balancing.

- IP Version: There are two options: IPv4 and IPv6. Right now, system supports these two IP address format and you can access via them.
- MAC address: The host in the LAN can get a unique MAC address. It is for you to access in the LAN. It is read-only.
- IP address: Here you can use up/down button (▲▼) or input the corresponding number to input IP address. Then you can set the corresponding subnet mask the default gateway.
- Default gateway: Here you can input the default gateway. Please note system needs to check the validity of all IPv6 addresses. The IP address and the default gateway shall be in the same IP section. That is to say, the specified length of the subnet prefix shall have the same string.
- DHCP: It is to auto search IP. When enable DHCP function, you cannot modify IP/Subnet mask /Gateway. These values are from DHCP function. If you have not enabled DHCP function, IP/Subnet mask/Gateway display as zero. You need to disable DHCP function to view current IP information. Besides, when PPPoE is operating, you cannot modify IP/Subnet mask /Gateway.
- MTU: It is to set MTU value of the network adapter. The value ranges from 1280-7200 bytes. The default setup is 1500 bytes. Please note MTU modification may result in network adapter reboot and network becomes off. That is to say, MTU modification can affect current network service. System may pop up dialog box for you to confirm setup when you want to change MTU setup. Click OK button to confirm current reboot, or you can click Cancel button to terminate current modification. Before the modification, you can check the MTU of the gateway; the MTU of the NVR shall be the same as or is lower than the MTU of the gateway. In this way, you can reduce packets and enhance network transmission efficiency.

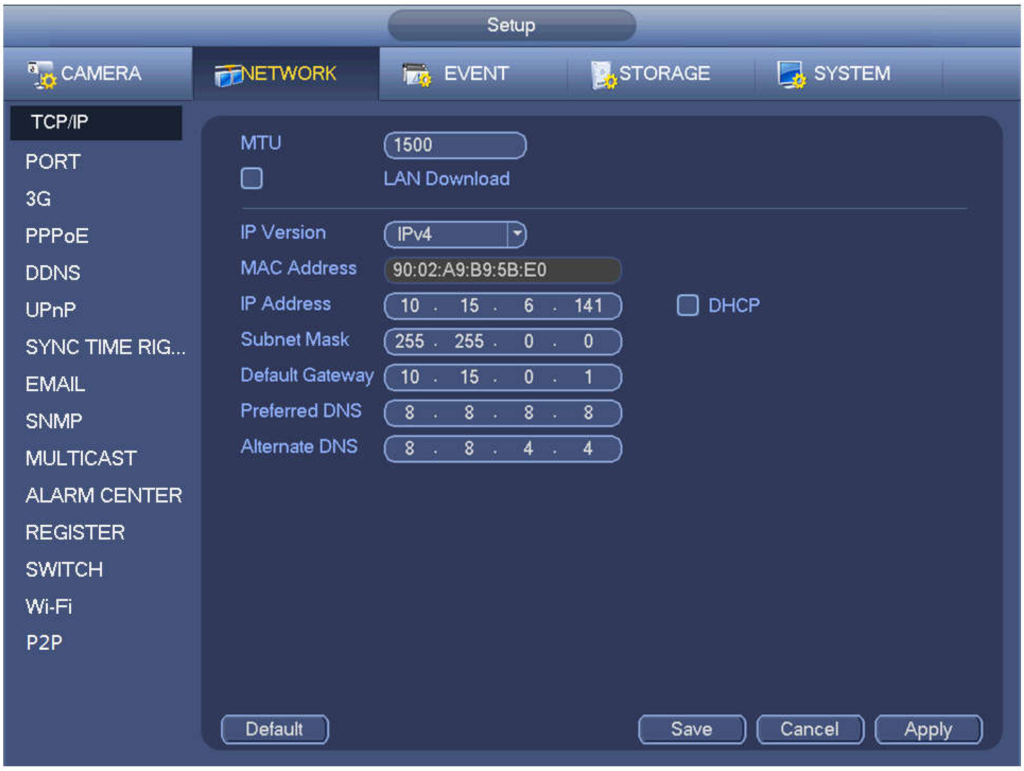
The following MTU value is for reference only.

- ✧ 1500: Ethernet information packet max value and it is also the default value. It is the typical setup when there is no PPPoE or VPN. It is the default setup of some router, switch or the network adapter.
- ✧ 1492: Recommend value for PPPoE.
- ✧ 1468: Recommend value for DHCP.

- Preferred DNS server: DNS server IP address.
- Alternate DNS server: DNS server alternate address.
- Transfer mode: Here you can select the priority between fluency/video qualities.
- LAN download: System can process the downloaded data first if you enable this function. The download speed is 1.5X or 2.0X of the normal speed.

- LAN download: System can process the downloaded data first if you enable this function. The download speed is 1.5X or 2.0X of the normal speed.

After completing all the setups please click save button, system goes back to the previous menu.



MTU 1500

□ LAN Download

IP Version IPv4

MAC Address 90:02:A9:B9:5B:E0

IP Address 10 . 15 . 6 . 141 □ DHCP

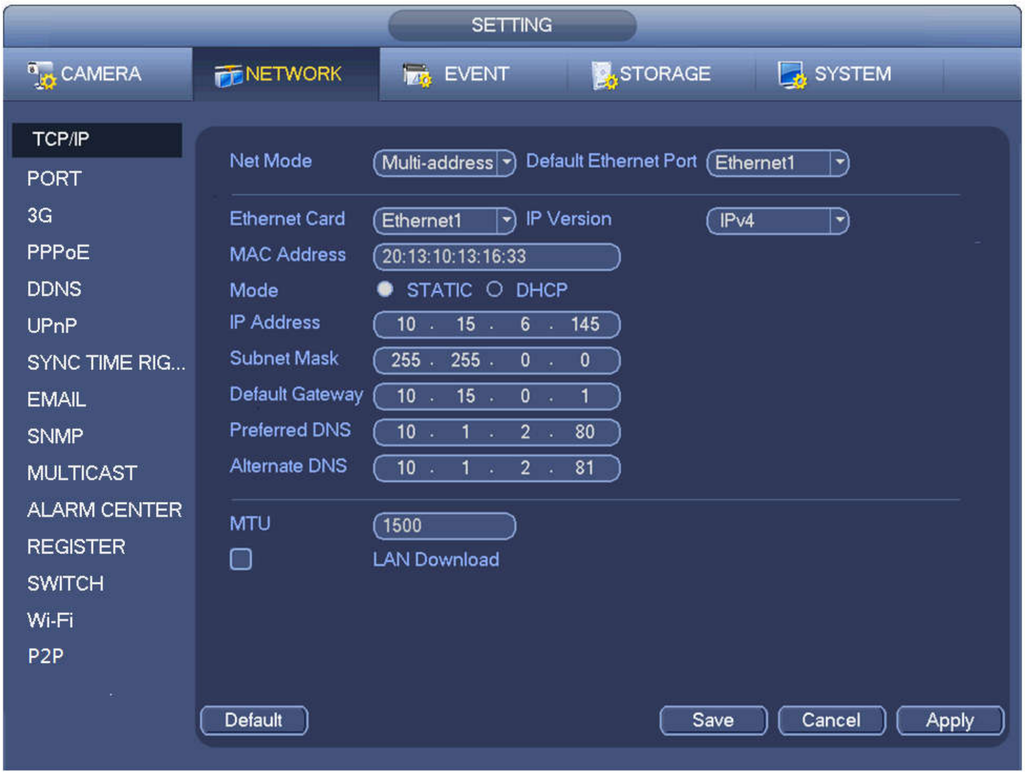
Subnet Mask 255 . 255 . 0 . 0

Default Gateway 10 . 15 . 0 . 1

Preferred DNS 8 . 8 . 8 . 8

Alternate DNS 8 . 8 . 4 . 4

Figure 4-163



Net Mode Multi-address Default Ethernet Port Ethernet1

Ethernet Card Ethernet1 IP Version IPv4

MAC Address 20:13:10:13:16:33

Mode ● STATIC ○ DHCP

IP Address 10 . 15 . 6 . 145

Subnet Mask 255 . 255 . 0 . 0

Default Gateway 10 . 15 . 0 . 1

Preferred DNS 10 . 1 . 2 . 80

Alternate DNS 10 . 1 . 2 . 81

MTU 1500

□ LAN Download

Figure 4-164

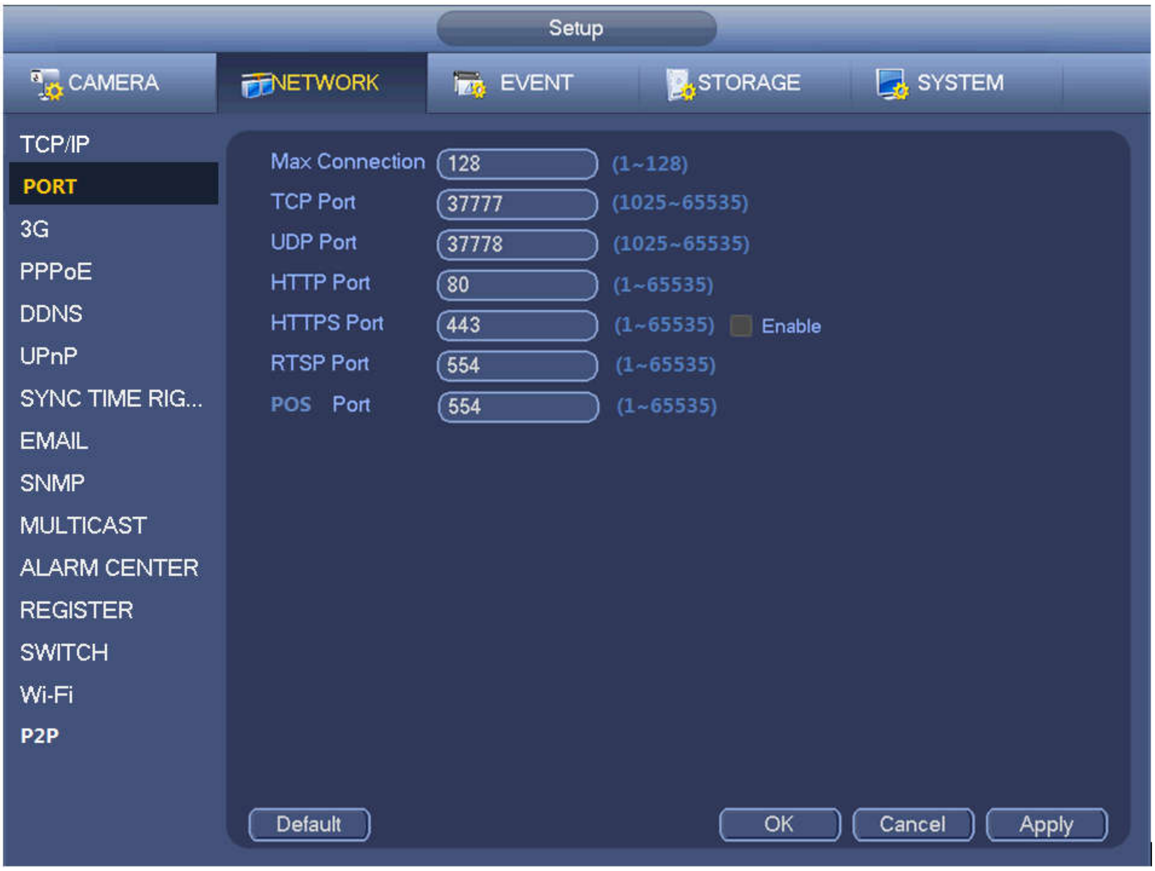
4.8.1.2 Port

The connection setup interface is shown as in Figure 4-165.

- Max connection: The max client login amount (such as WEB, platform, cellphone and etc). The value ranges from 1 to 128(default).
- TCP port: Default value is 37777.
- UDP port: Default value is 37778.
- HTTP port: Default value is 80.
- HTTPS port: Select the Enable check box and configure the port according to your actual needs. The default value is 443. After HTTPS is enabled, HTTP will be switched to HTTPS by force to transmit data in a safer way.
- RTSP port: Default value is 554.

CAUTION

System needs to reboot after you changed and saved any setup of the above ports. Make sure the port values here do not conflict.



Max Connection 128 (1~128)

TCP Port 37777 (1025~65535)

UDP Port 37778 (1025~65535)

HTTP Port 80 (1~65535)

HTTPS Port 443 (1~65535) □ Enable

RTSP Port 554 (1~65535)

POS Port 554 (1~65535)

Figure 4-165

4.8.1.3 Wi-Fi AP

Note

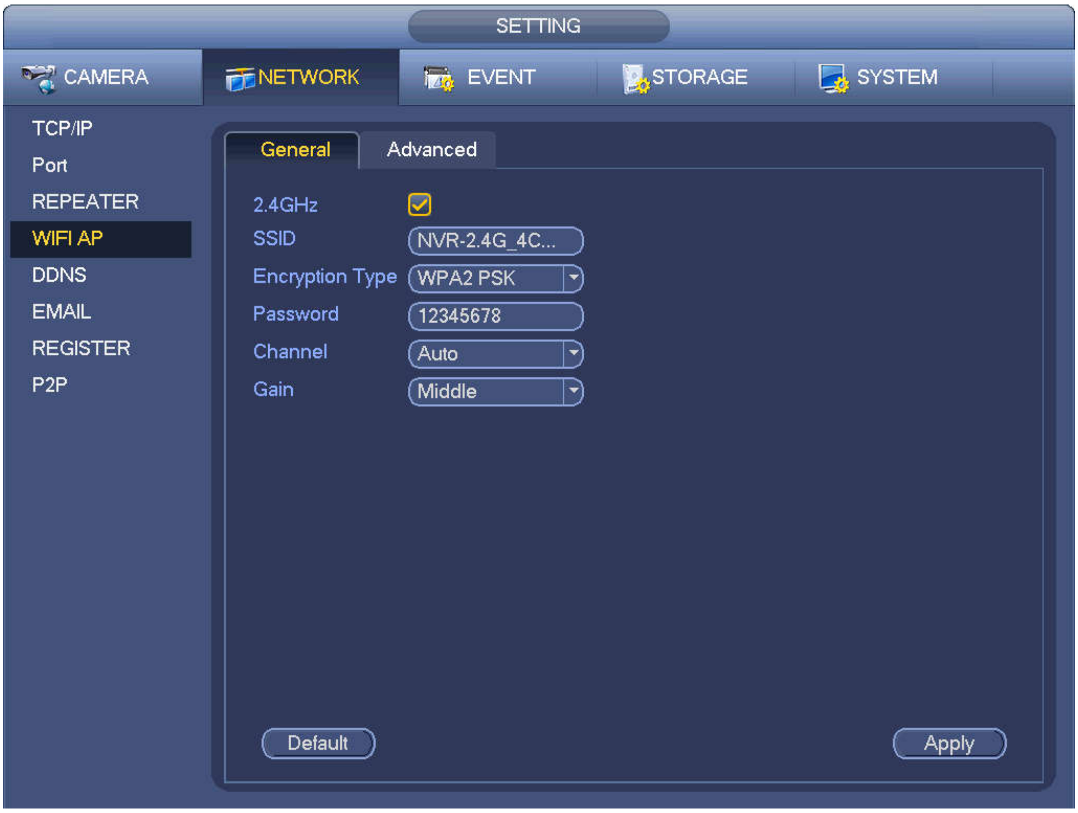
This function is available only for NVR devices with built-in Wi-Fi module. See the actual situation.

4.8.1.3.1 General Settings

The Wi-Fi AP interface is shown as below. See Figure 4-166. Here you can set Wi-Fi hotspot, so that the network camera can use the hotspot to connect to the network.

- 2.4GHz: Please check the box to enable the function.
- SSID: It is to set SSID name. You can use this name to search the device.
- Password: It is to set SSID password. You can use this password to connect to the network.

- Encryption Type: Select encryption type from the dropdown list.
- Channel: Please select a channel from the dropdown list. The default setup is auto.
- Gain: There are three options: High/middle/low. Please select from the dropdown list.



2.4GHz ☑

SSID: NVR-2.4G_4C...

Encryption Type: WPA2 PSK

Password: 12345678

Channel: Auto

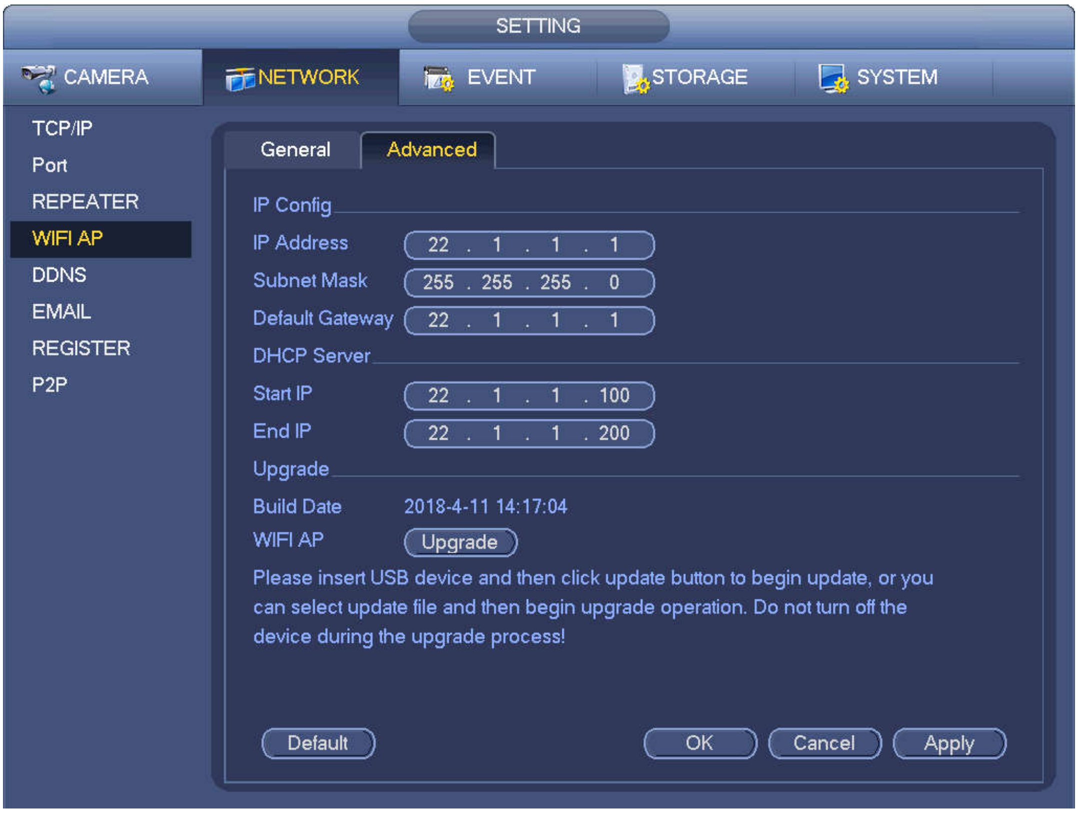
Gain: Middle

Figure 4-166

4.8.1.3.2 Advanced

Click Advanced and you can see an interface shown as below. See
Figure 4-167.

- IP Address: Input Wi-Fi AP IP address.
- Subnet Mask: Input Wi-Fi AP subnet mask.
- Default Gateway: Input Wi-Fi AP gateway.
- Start IP/End IP: Input start IP and end IP of the network cameras. The NVR can allocate the IP addresses in the range you specified here.
- Upgrade: Click it to upgrade Wi-Fi AP module.



IP Config

IP Address: 22 . 1 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 22 . 1 . 1 . 1

DHCP Server

Start IP: 22 . 1 . 1 . 100

End IP: 22 . 1 . 1 . 200

Upgrade

Build Date: 2018-4-11 14:17:04

WIFI AP

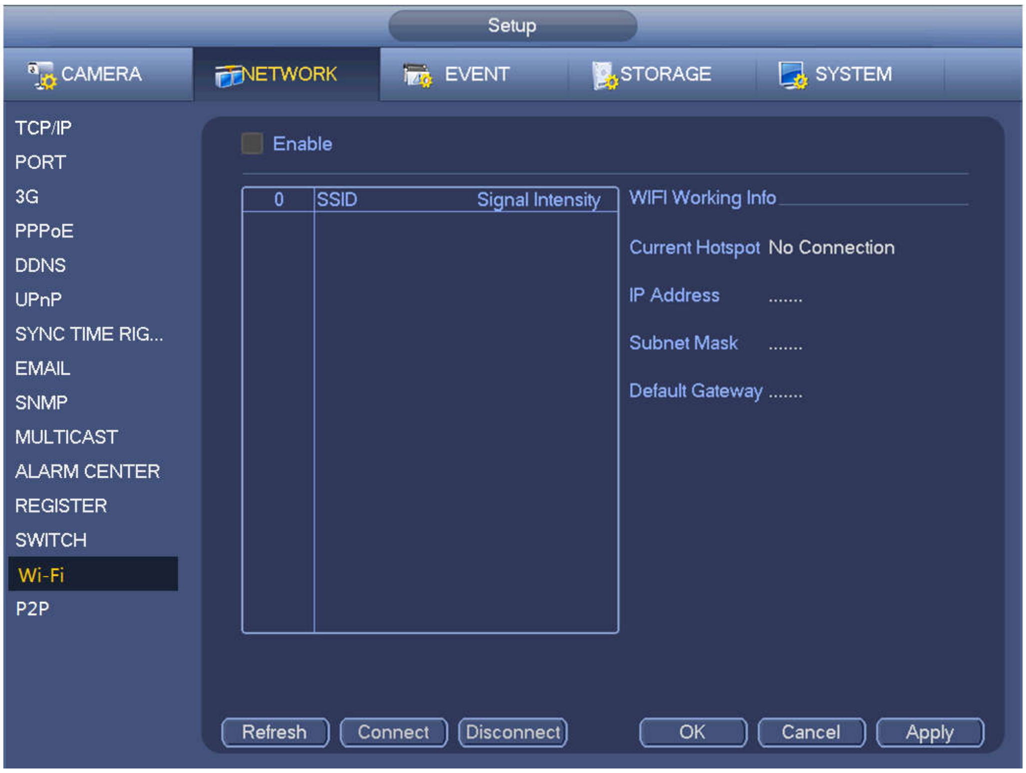
Please insert USB device and then click update button to begin update, or you can select update file and then begin upgrade operation. Do not turn off the device during the upgrade process!

Figure 4-167

4.8.1.4 Wi-Fi

The Wi-Fi interface is shown as below. See Figure 4-168.

- Enable: Check the box here to enable Wi-Fi function.
- Refresh: You can click it to search the hotspot list again. It can automatically add the information such as the password if you have set it before.
- Disconnect: Here you can click it to turn off the connection.
- Connect: Here you can click it to connect to the hotspot. System needs to turn off current connection and then connect to a new hotspot if there is connection of you selected one.



□ Enable

0	SSID	Signal Intensity

WIFI Working Info

Current Hotspot No Connection

IP Address ....

Subnet Mask ....

Default Gateway ....

Figure 4-168

- Wi-Fi working status: Here you can view current connection status.

Please note:

- After successful connection, you can see Wi-Fi connection icon at the top right corner of the preview interface.
- When the hotspot verification type is WEP, system displays as AUTO since the device cannot detect its encryption type.
- System does not support verification type WPA and WPA2. The display may become abnormal for the verification type and encryption type.

After device successfully connected to the Wi-Fi, you can view the hotspot name, IP address, subnet mask, default gateway and etc. Right now system support TOTOLINK_N2200UP module.

4.8.1.5 Repeater

The device supports repeater function for front-end IPCs to effectively extend video transmission distance and range.

NOTE

Only some devices support this function.

Repeater is available for devices with built-in Wi-Fi module and the front-end IPC shall support repeater.

Binding Repeater

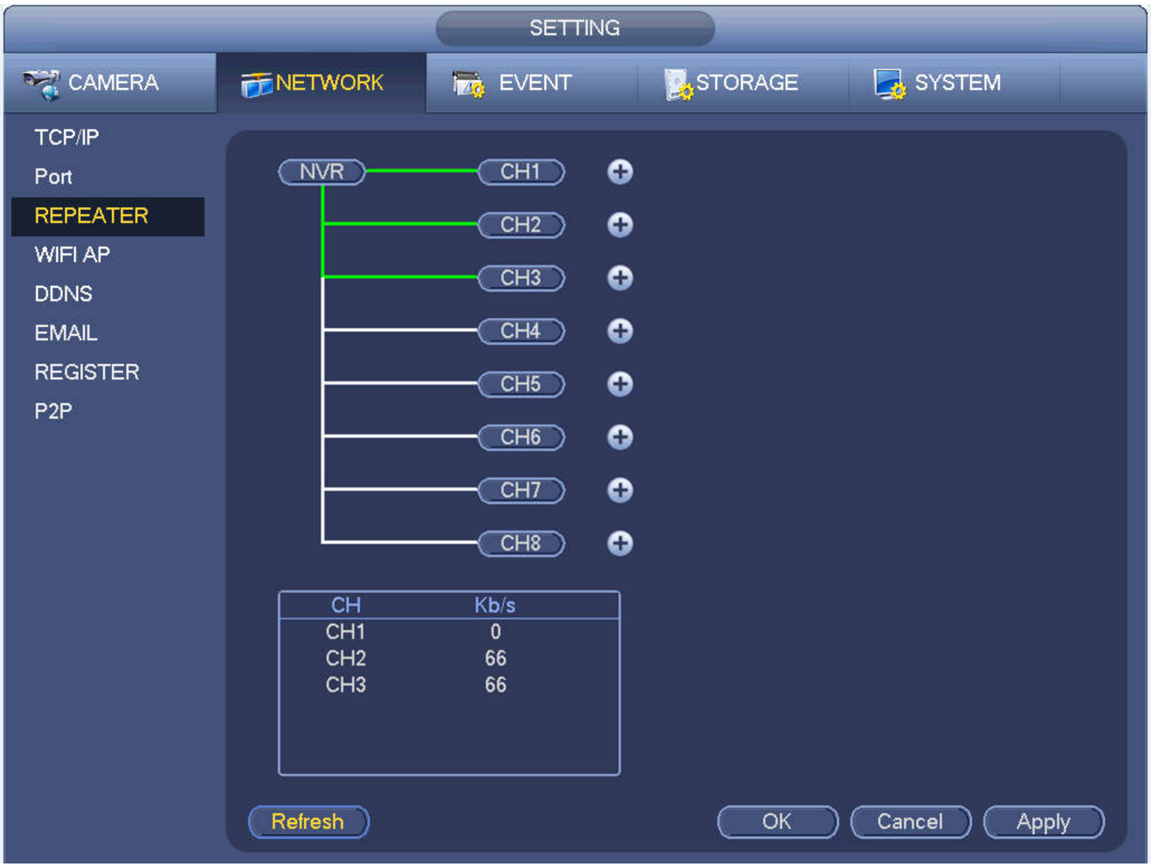
Step 1 Turn on the NVR device and IPCs, and then directly connect all the IPCs to the NVR device via Wi-Fi.

Step 2 Enter from main menu > Setting > Network > Repeater.

Step1 The Repeater interface is displayed. See Figure 4-169.

NOTE

When the connection line is green, the channel has conneted to Wi-Fi IPC successfully.

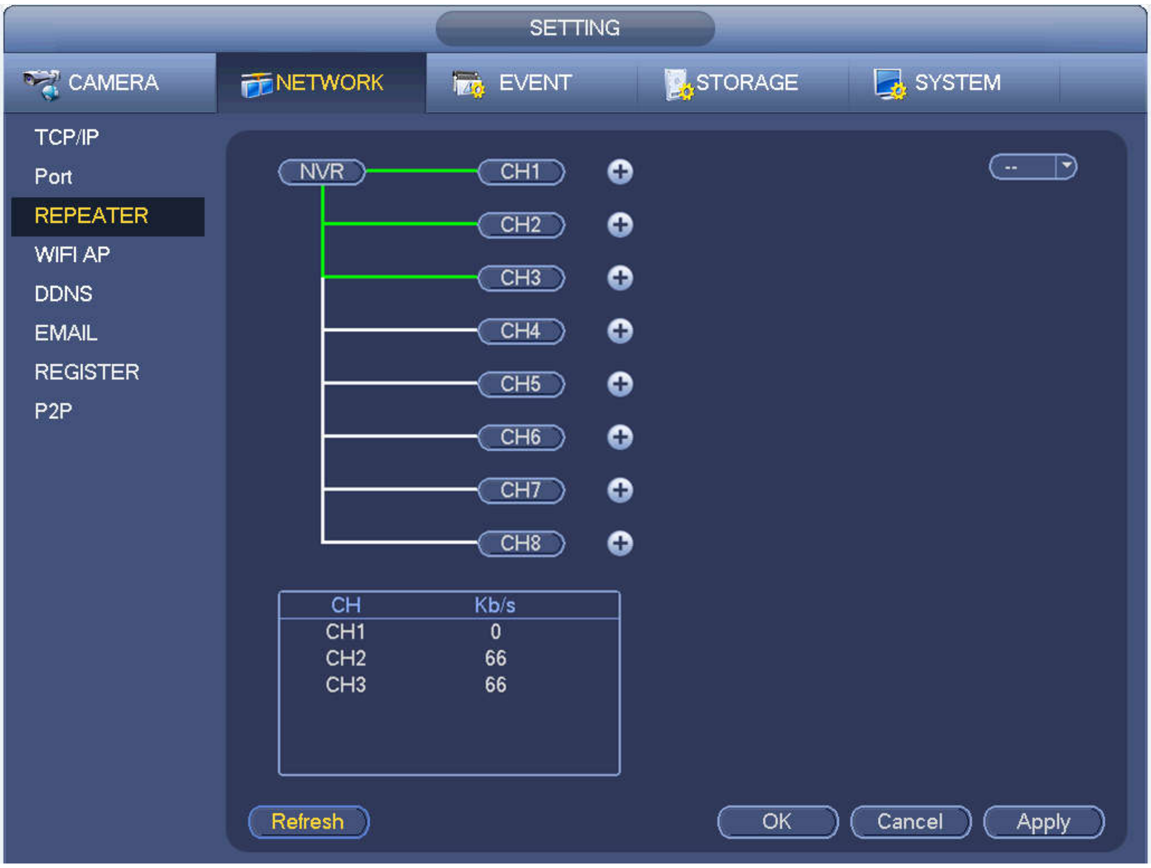


CH	Kb/s
CH1	0
CH2	66
CH3	66

Figure 4-169

Step 3 Click ⊕ after the channel you want to set the repeater function.

System displays the icon to add channel. See Figure 4-170.

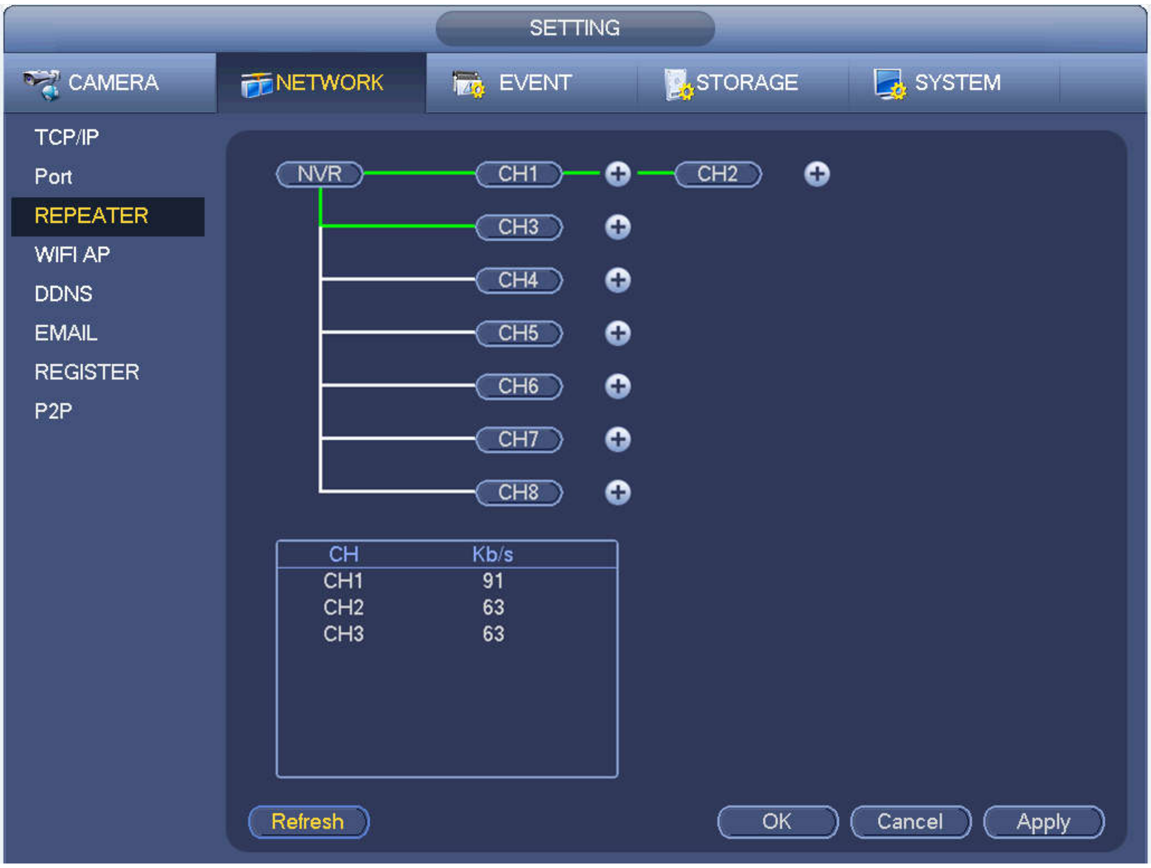


CH	Kb/s
CH1	0
CH2	66
CH3	66

Figure 4-170

Step 4 Click and select the channel you want to add.

After the adding is successful, system displays the following interface. See Figure 4-171.



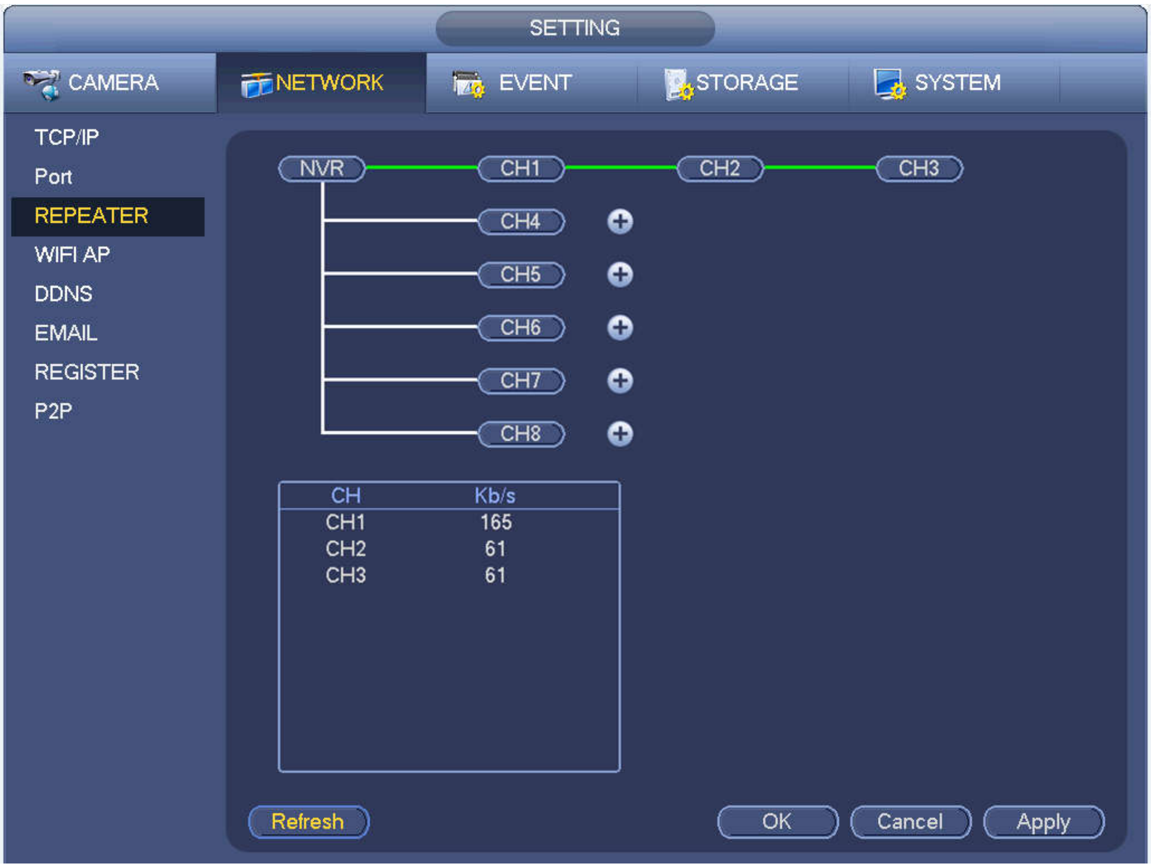
CH	Kb/s
CH1	91
CH2	63
CH3	63

Figure 4-171

NOTE

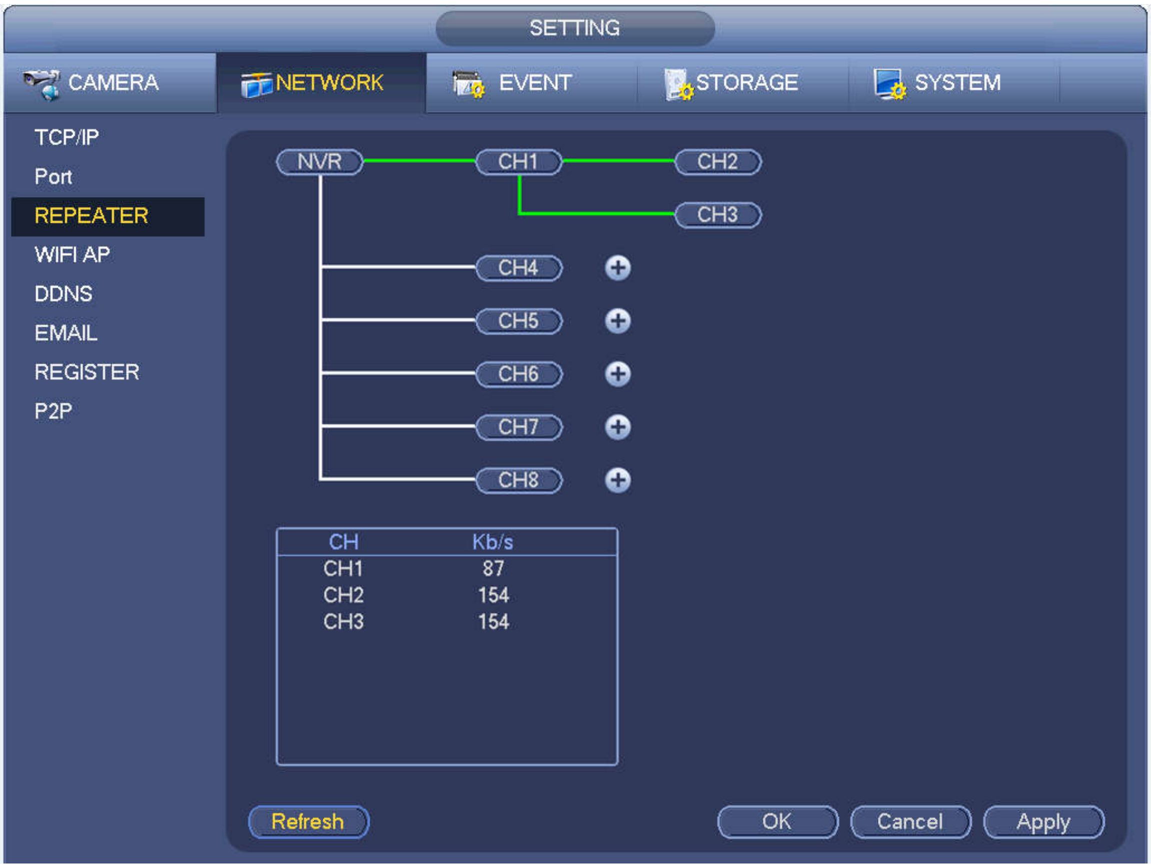
To take Figure 4-171 as an example, the IPC connected to CH1 is the primary repeater and the IPC connected to CH2 is the secondary repeater. Each primary repeater can connect 2 Wi-Fi IPCs at most in series or in parallel.

- When connecting IPCs in series, the IPC in CH2 works as a secondary repeater to connect the IPC in CH3. See Figure 4-172.
- When connecting IPCs in parallel, the IPC in CH1 works as a primary repeater to connect the IPCs in CH2 and CH3. See Figure 4-173.



CH	Kb/s
CH1	165
CH2	61
CH3	61

Figure 4-172



CH	Kb/s
CH1	87
CH2	154
CH3	154

Figure 4-173

Step 5 Click Apply or OK to save the configuration.

Unbinding Repeater

If you want to unbind the repeater, click the corresponding channel and the IPC in this channel will connect to the NVR device directly.

NOTE

You can delete repeater IPC only from the last level

4.8.1.6 3G

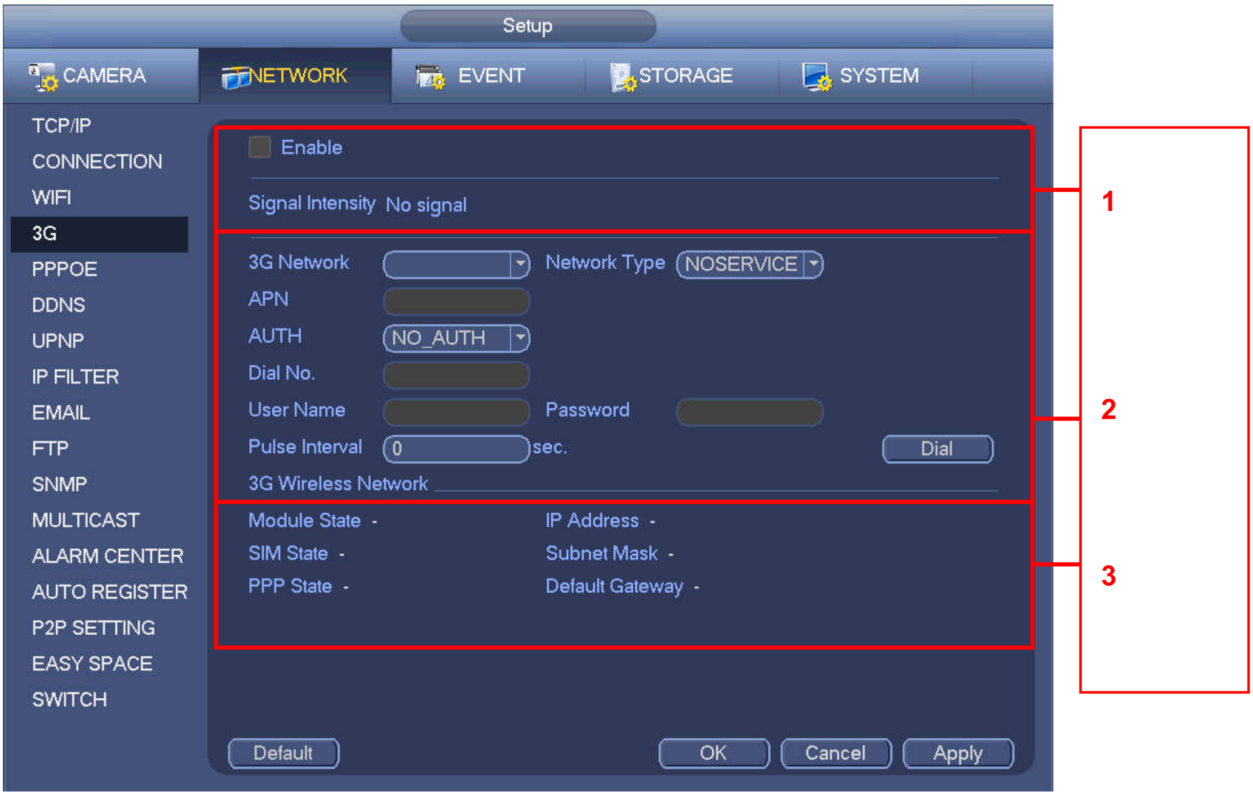
3G setup interface is shown as below. See Figure 4-174.

Please refer to the following contents for the parameter information.

- Pane 1: Display 3G signal intensity after you enabled 3G function.
- Pane 2: Display 3G module configuration information after you enabled 3G function.
- Pane 3: Display 3G module status information after you enabled 3G function.

It is to display current wireless network signal intensity such as EVDO, CDMA1x, WCDMA, WCDMA, EDGE and etc.

- 3G module: It is to display current wireless network adapter name.
- 3G Enable/Disable: Check the box here to enable 3G module.
- Network type: There are various network types for different 3G network modules. You can select according to your requirements.
- APN: It is the wireless connection server. It is to set you access the wireless network via which method.
- AUTH: It is the authentication mode. It supports PAP/CHAP.
- Dial number: Please input 3G network dialup number you got from your ISP.
- User name: It is the user name for you to login the 3G network.
- Password: It is the password for you to login the 3G network.
- Pulse interval: You can set dialup duration. Once you disable the extra stream, the connection time begins. For example, if you input 5 seconds here, then 3G network connection period is 5 seconds. The device automatically disconnect when time is up. If there is no extra stream, 3G network connection is valid all the time. **If the alive time is 0, then the 3G network connection is valid all the time.**
- Dial: Here you can enable or disable 3G network connection/disconnection manually.
- 3G wireless network: Here is to display wireless network status, SIM card status, dial status. If the 3G connection is OK, then you can see the device IP address the wireless network automatically allocates.



□ Enable

Signal Intensity No signal

3G Network

Network Type NOSERVICE

APN

AUTH NO_AUTH

Dial No.

User Name

Password

Pulse Interval 0 sec.

3G Wireless Network

Module State -

IP Address -

SIM State -

Subnet Mask -

PPP State -

Default Gateway -

Figure 4-174

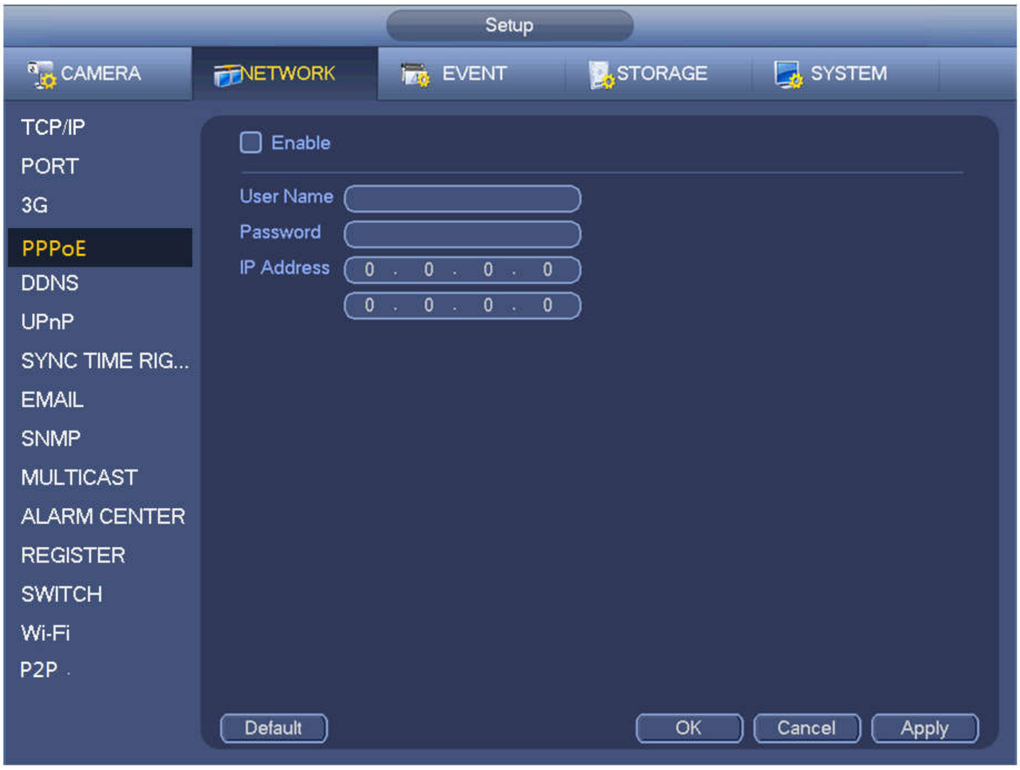
4.8.1.7 PPPoE

PPPoE interface is shown as in Figure 4-175.

Input “PPPoE name” and “PPPoE password” you get from your ISP (Internet service provider).

Click save button, you need to restart to activate your configuration.

After rebooting, NVR will connect to internet automatically. The IP in the PPPoE is the NVR dynamic value. You can access this IP to visit the unit.



☐ Enable

User Name

Password

IP Address 0 . 0 . 0 . 0

0 . 0 . 0 . 0

Figure 4-175

4.8.1.8 DDNS

DDNS (Dynamic Domain Name Server) is to dynamically refresh the DNS domain name and IP address if the device IP address has changed frequently. The user can use the domain to access the device.

Preparation

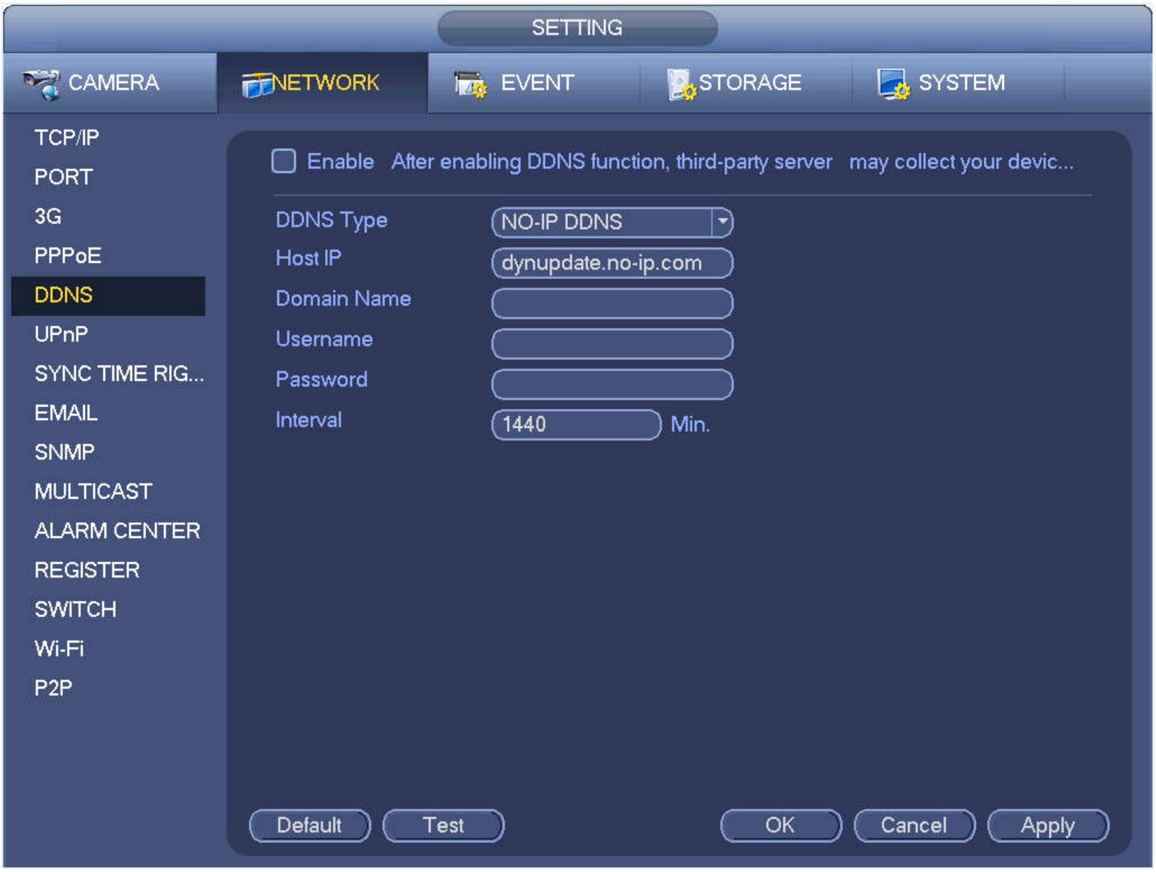
Before the operation, make sure the device supports DNS type and go to the DDNS service provider website to register the domain name via the PC.

NOTE

After you register the device and log in the DDNS website, you can view all connected device information of the current user.

Step 1 Enter from main memu > Setup > Network > DDNS.

DDNS setup interface is shown as in Figure 4-176.



☐ Enable After enabling DDNS function, third-party server may collect your devic...

DDNS Type	NO-IP DDNS
Host IP	dynupdate.no-ip.com
Domain Name	
Username	
Password	
Interval	1440 Min.

Figure 4-176

Step 2 Select the Enable check box to enable DDNS function.

NOTE

When DDNS is enabled, the third-party server might collect your device information.

Step 3 Configure the DDNS parameters according to practical situation.

- Type/address:

✧ Dyndns DDNS is members.dyndns.org.

✧ NO-IP DDNS is dynupdate.no-ip.com.

✧ CN99 DDNS is members.3322.org.

- Domain: The domain name registered on the DDNS service provider website.
- User name/password: Input the user name and password got from the DDNS service provider. Make sure you have logged in the DDNS service provider website to register an account (user name and password).
- Interval: After DDNS boots up, it sends out refresh query regularly. The unit is minute.

Step 4 Click Apply or Save to complete setup.

Step 5 Open a browser and input domain name, click Enter key.

The setting is right if you can view device WEB interface. Otherwise, please check the parameters.

4.8.1.9 UPnP

The UPNP protocol is to establish a mapping relationship between the LAN and the WAN. Please input the router IP address in the LAN in Figure 4-163. See Figure 4-177.

- UPNP on/off :Turn on or off the UPNP function of the device.

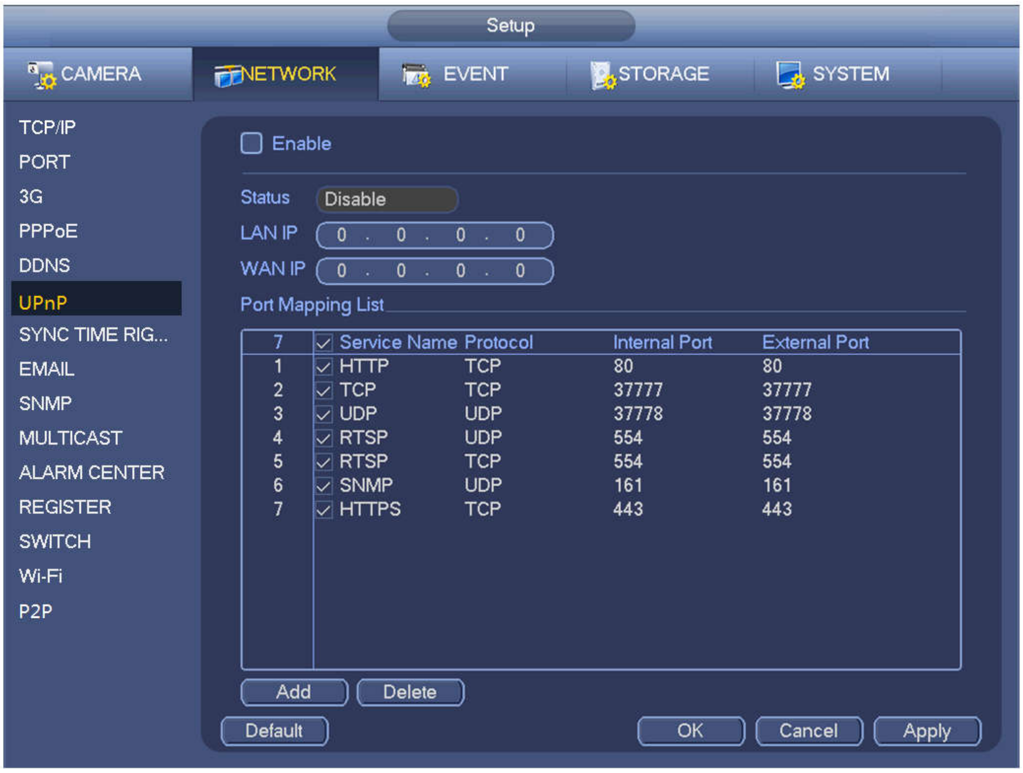
- Status: When the UPNP is offline, it shows as “Unknown”. When the UPNP works it shows “Success”
- Router LAN IP: It is the router IP in the LAN.
- WAN IP: It is the router IP in the WAN.
- Port Mapping list: The port mapping list here is the one to one relationship with the router’s port mapping setting.
- List:
  - ✧ Service name: Defined by user.
  - ✧ Protocol: Protocol type
  - ✧ Internal port: Port that has been mapped in the router.
  - ✧ External port: Port that has been mapped locally.
- Default: UPNP default port setting is the HTTP, TCP and UDP of the NVR.
- Add to the list: Click it to add the mapping relationship.
- Delete: Click it to remove one mapping item.

Double click one item; you can change the corresponding mapping information. See Figure 4-178.

Important:

When you are setting the router external port, please use 1024~5000 port. Do not use well-known port 1~255 and the system port 256~1023 to avoid conflict.

For the TCP and UDP, please make sure the internal port and external port are the same to guarantee the proper data transmission.



□ Enable

Status: Disable

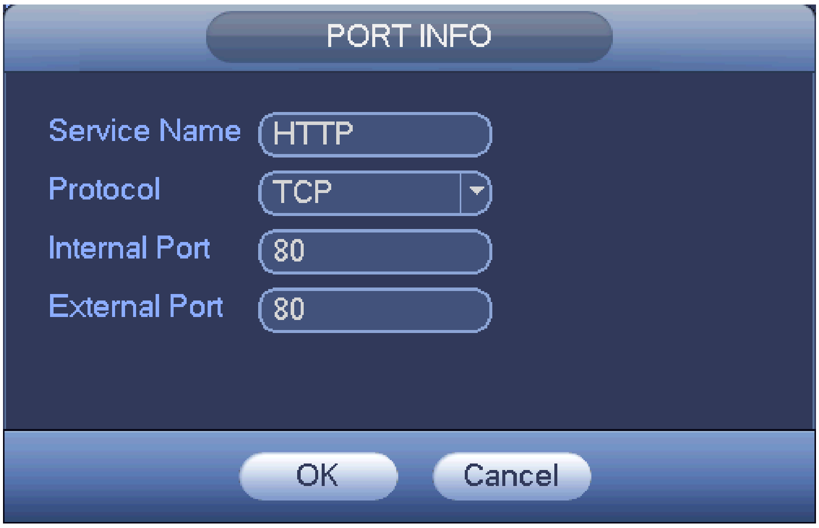
LAN IP: 0 . 0 . 0 . 0

WAN IP: 0 . 0 . 0 . 0

Port Mapping List

7	☑ Service Name	Protocol	Internal Port	External Port
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

Figure 4-177



PORT INFO

Service Name: HTTP

Protocol: TCP

Internal Port: 80

External Port: 80

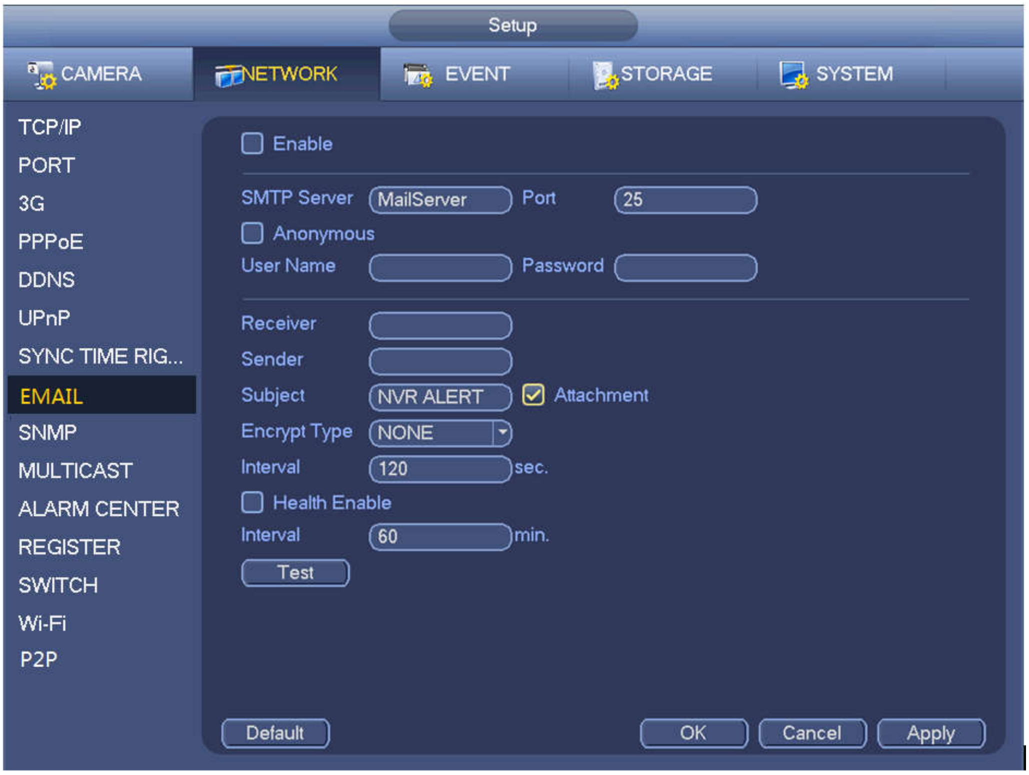
Figure 4-178

4.8.1.10 Email

The email interface is shown as below. See Figure 4-179.

- SMTP server: Please input your email SMTP server IP here.
- Port: Please input corresponding port value here.
- User name: Please input the user name to login the sender email box.
- Password: Please input the corresponding password here.
- Sender: Please input sender email box here.
- Title: Please input email subject here. System support English character and Arabic number. Max 32-digit.
- Receiver: Please input receiver email address here. System max supports 3 email boxes. System automatically filters same addresses if you input one receiver repeatedly.
- SSL enable: System supports SSL encryption box.
- Interval: The send interval ranges from 0 to 3600 seconds. 0 means there is no interval.
- Health email enable: Please check the box here to enable this function. This function allows the system to send out the test email to check the connection is OK or not.
- Interval: Please check the above box to enable this function and then set the corresponding interval. System can send out the email regularly as you set here. Click the Test button, you can see the corresponding dialogue box to see the email connection is OK or not.

Please note system will not send out the email immediately when the alarm occurs. When the alarm, motion detection or the abnormity event activates the email, system sends out the email according to the interval you specified here. This function is very useful when there are too many emails activated by the abnormity events, which may result in heavy load for the email server.



☐ Enable

SMTP Server MailServer Port 25

☐ Anonymous

User Name Password

Receiver

Sender

Subject NVR ALERT ☑ Attachment

Encrypt Type NONE

Interval 120 sec.

☐ Health Enable

Interval 60 min.

Figure 4-179

4.8.1.11 SNMP

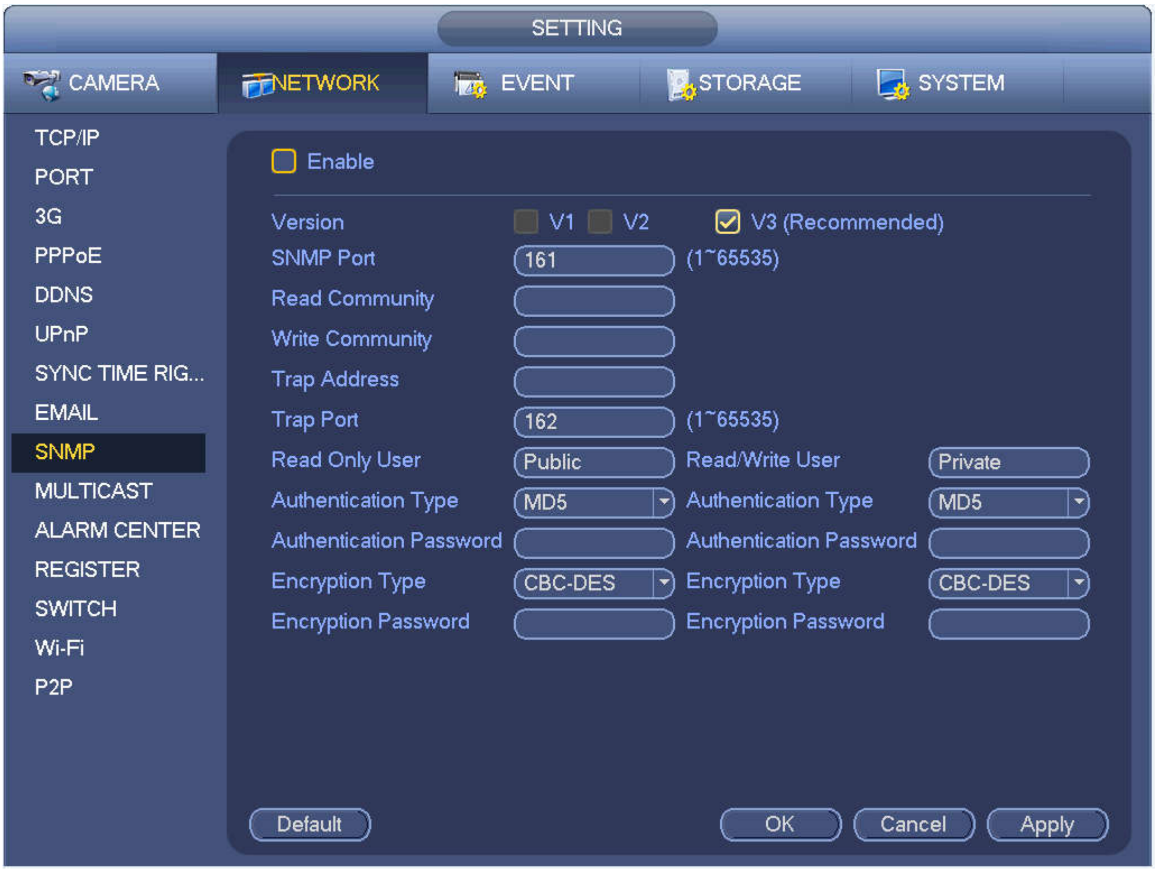
SNMP is an abbreviation of Simple Network Management Protocol. It provides the basic network management frame of the network management system. SNMP is widely used in various scenarios, network devices, software and systems.

Preparation:

- Install SNMP monitor and management tool, such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the corresponding MIB file from the technical support.

Step 1 Enter from main menu > Setup > Network > SNMP.

The SNMP interface is displayed. See Figure 4-180.



□ Enable

Version □ V1 □ V2 ☑ V3 (Recommended)

SNMP Port 161 (1~65535)

Read Community

Write Community

Trap Address

Trap Port 162 (1~65535)

Read Only User Public Read/Write User Private

Authentication Type MD5 Authentication Type MD5

Authentication Password Authentication Password

Encryption Type CBC-DES Encryption Type CBC-DES

Encryption Password Encryption Password

Figure 4-180

Step 2 Select the SNMP check box.

Step 3 Configure the parameyers. For details, see the following table.

Parameter	Description
Version	Select the check box of the corresponding version. NOTE System selects V3 by default. There might be risks for V1 and V2.
SNMP Port	Enter the SNMP port number.
Read Community/Write Community	The read community/write community string supported by the program.
Trap Address	Enter the IP address of the PC installed with MG-SOFT MIB Browser. It is the destination address to receive trap information from the device.
Trap Port	The destination port to receive trap information from the device.
Read Only User	Enter the read only username to access the NVR device.
Read/Write User	Enter the read/write username to access the NVR device.
Authentication	It includes MD5 and SHA. System automatically recognizes it after it is enabled.
Password	Enter the password for encryption and authentication. The password shall be no less than 8 characters.
Encryption Type	Select the encryption type. The default type is CBC-DES.

Step 4 Click OK to complete the configuration.

Step 5 View device info.

1) Run MIB Builder and MG-SOFT MIB Browser.

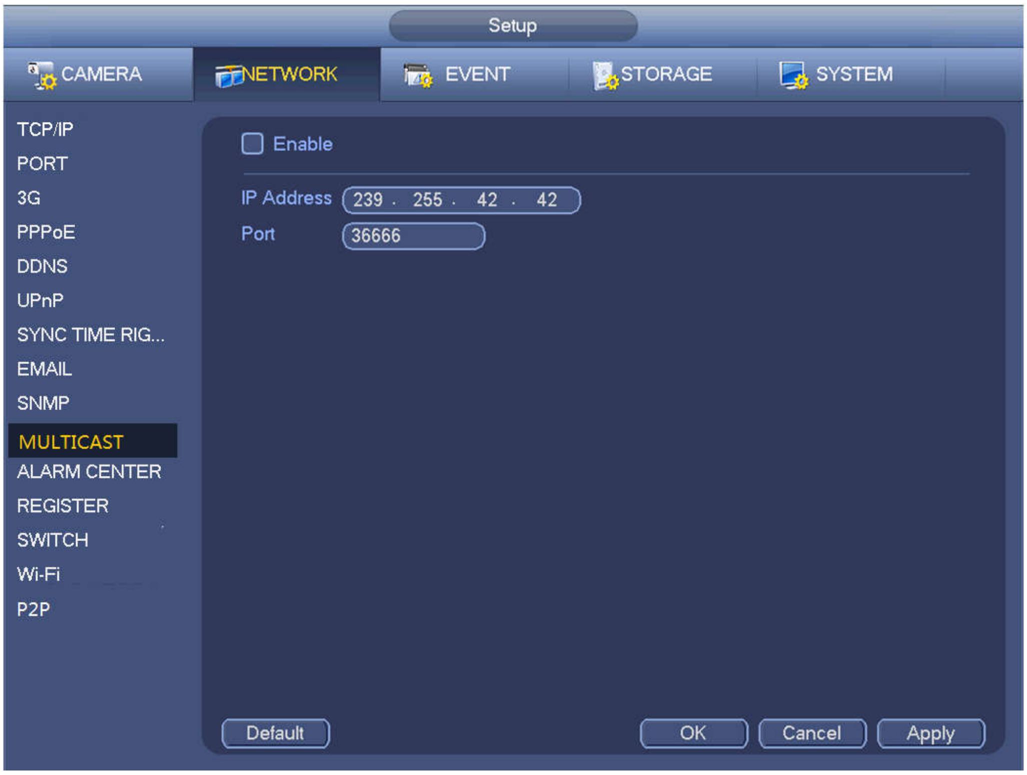
2) Compile the two MIB files with MIB Builder.
3) Load the compiled module to the software with MG-SOFT MIB Browser.
4) Enter the PC IP address into MG-SOFT MIB Browser and select the version to search.
5) Expand the tree list in MG-SOFT MIB Browser to view the device configuration information, such as channel number and program version.

4.8.1.12 Multicast

When multiple users preview the video of a channel through the network at the same time, due to network bandwidth limitation, they might be unable to preview. You can set a multicast IP for NVR device (224.0.0.0 - 238.255.255.255) and adopt the way of multicast protocol access to solve the problem.

Step 6 Enter from main menu > Setup > Network > Multicast.

The Multicast interface is shown as in Figure 4-181.



□ Enable

IP Address 239 . 255 . 42 . 42

Port 36666

Figure 4-181

Step 7 Select the Enable check box to enable this function.

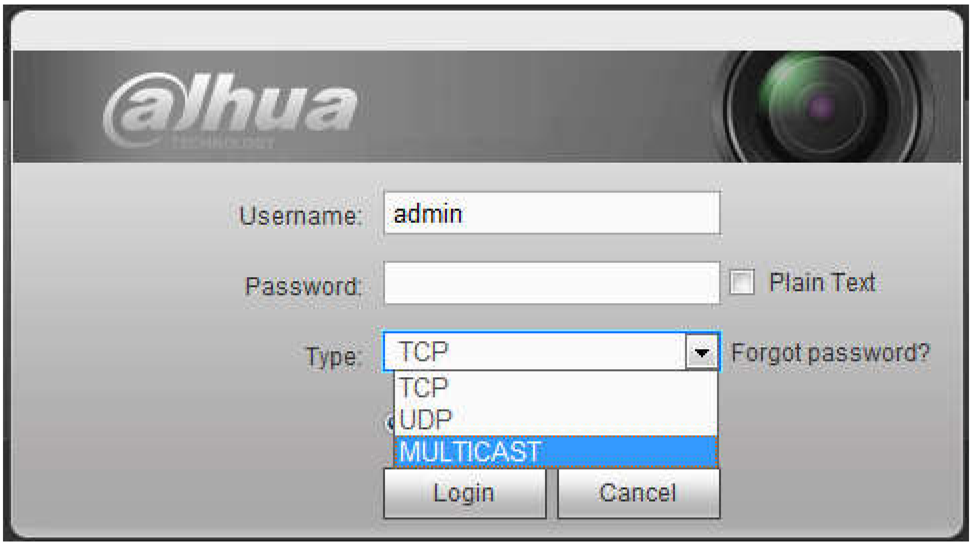
Step 8 Configure the parameters. For details, see the following table.

Parameter	Description
IP Address	Enter the multicast IP address to access the device (224.0.1.0-238.255.255.255).
Port	Enter the multicast port number to access the device (1025-65000).

Step 9 Click Apply or OK to complete the setting.

After configuring the multicast, you can log in Web with multicast.

Log in Web. In the Type drop-down list, select Milticast. See Figure 4-182. System will automatically obtain the multicast address and join the muiticast goup. Open the monitor and you can view the video in multicast way.



Username: admin

Password:

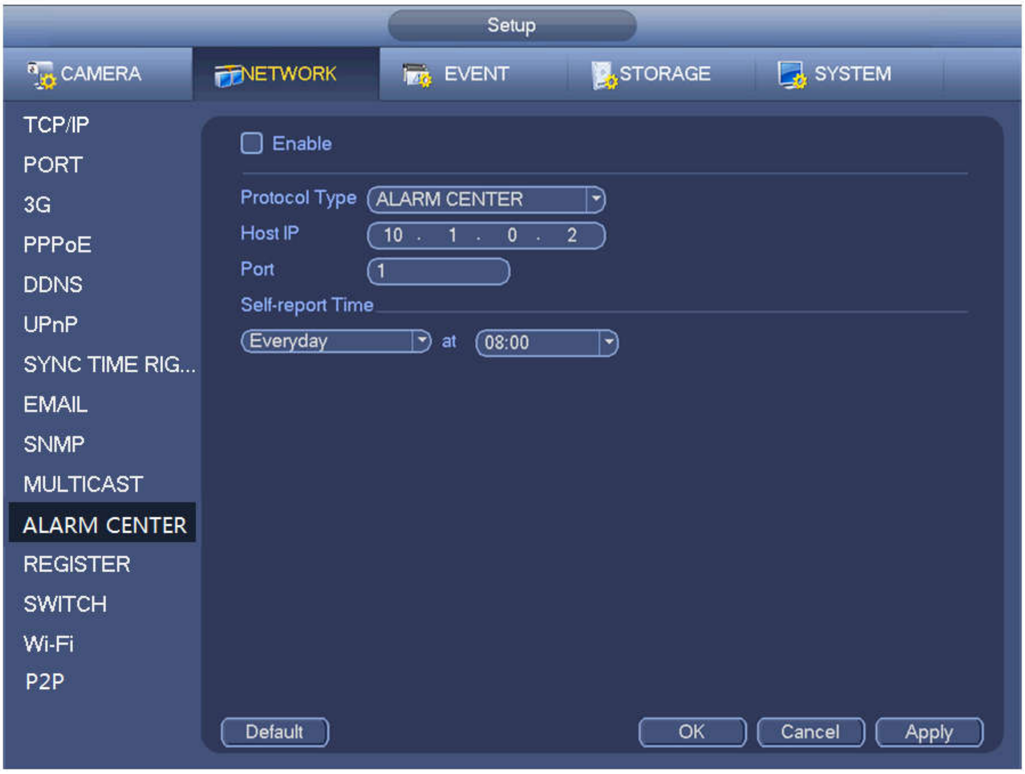
☐ Plain Text

Type: TCP

Figure 4-182

4.8.1.13 Alarm Centre

This interface is reserved for you to develop. See Figure 4-183.



☐ Enable

Protocol Type: ALARM CENTER

Host IP: 10 . 1 . 0 . 2

Port: 1

Self-report Time: Everyday at 08:00

Figure 4-183

4.8.1.14 Auto register

This function allows the device to auto register to the proxy you specified. In this way, you can use the client-end to access the NVR and etc via the proxy. Here the proxy has a switch function. In the network service, device supports the server address of IPv4 or domain.

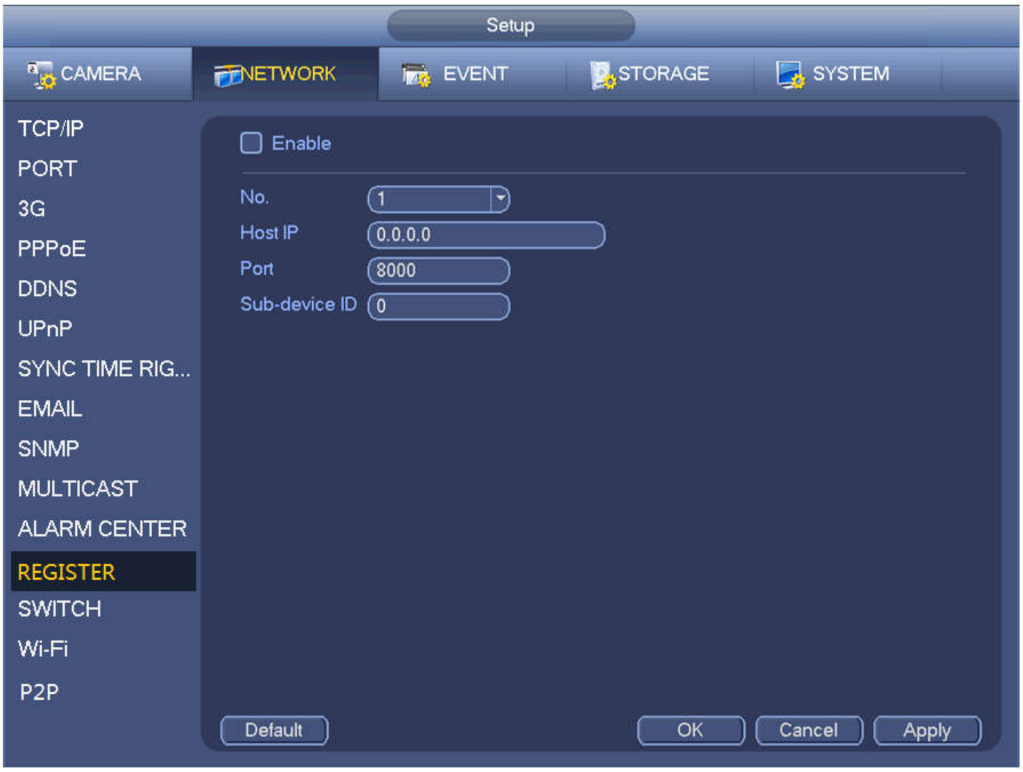
Please follow the steps listed below to use this function.

Please set proxy server address, port, and sub-device name at the device-end. Please enable the auto register function, the device can auto register to the proxy server.

1) The setup interface is shown as in Figure 4-184.

Important

Do not input network default port such as TCP port number.



□ Enable

No. 1

Host IP 0.0.0.0

Port 8000

Sub-device ID 0

Figure 4-184

2) The proxy server software developed from the SDK. Please open the software and input the global setup. Please make sure the auto connection port here is the same as the port you set in the previous step.

3) Now you can add device. Please do not input default port number such as the TCP port in the mapping port number. The device ID here shall be the same with the ID you input in Figure 4-184. Click Add button to complete the setup.

4) Now you can boot up the proxy server. When you see the network status is Y, it means your registration is OK. You can view the proxy server when the device is online.

Important

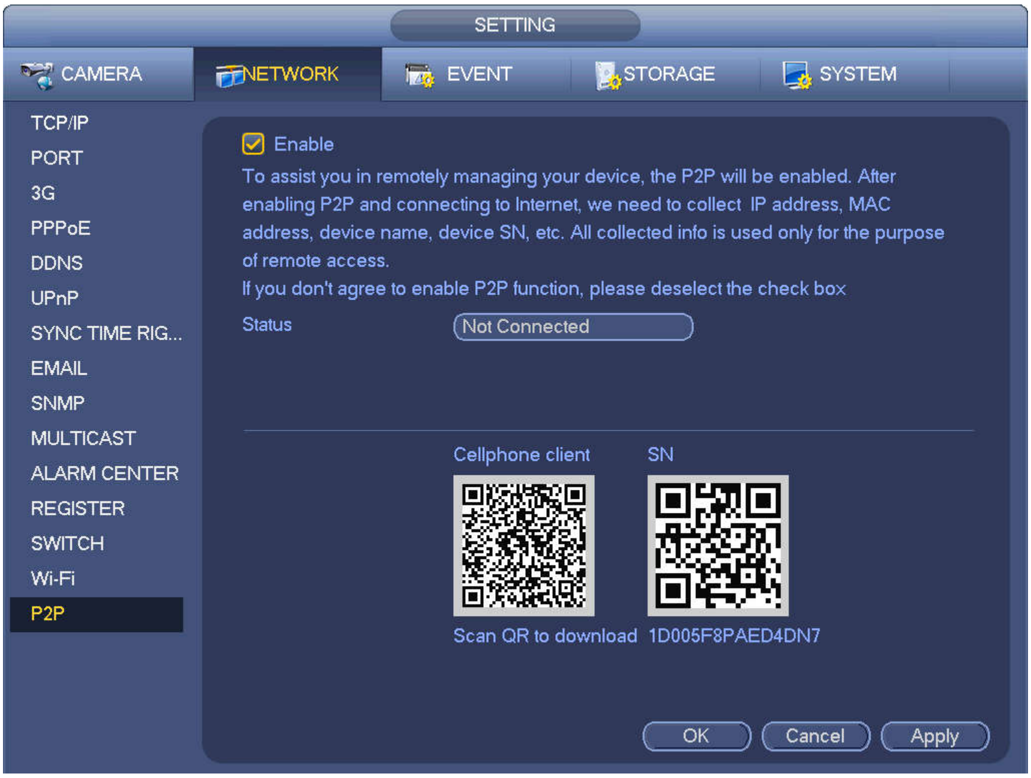
The server IP address can also be domain. But you need to register a domain name before you run proxy device server.

4.8.1.15 P2P

You can use your cell phone to scan the QR code and add it to the cell phone client.

Via the SN from scanning the QR code, you can access the device in the WAN. Please refer to the P2P operation manual included in the resources CD.

From main menu->Setting->Network->P2P, you can go to the following interface, the P2P interface is shown as in Figure 4-185.



☑ Enable

To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access.

If you don't agree to enable P2P function, please deselect the check box

Status: Not Connected

Scan QR to download

1D005F8PAED4DN7

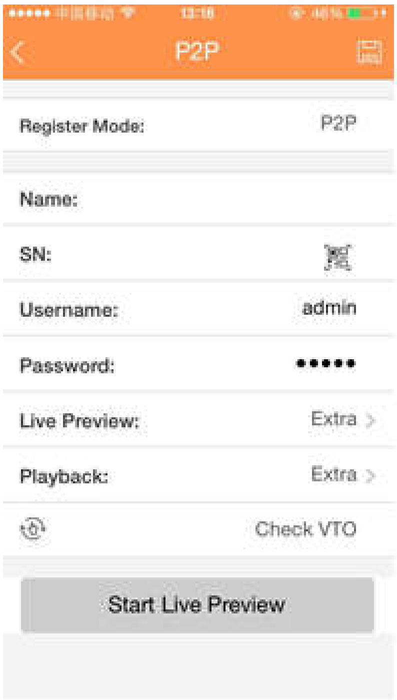
Figure 4-185

Here we use cell phone APP to continue.

Step 1 Use cell phone to scan the QR code and download the APP.

Step 2 After installation, run the APP and Live Preview, enter the main interface. Now you can add device to the APP.

1. Open App; tap 📹 to go to the Live preview.
2. Tap ☰ at the top left corner, you can see the main menu.
3. Tap Device manager button, you can use several modes (P2P/DDNS/IP and etc.) to add the device. Click 💾 to save current setup. Tap Start Live preview to view all-channel video from the connected device. See Figure 4-186.



Register Mode: P2P

Name:

SN:

Username: admin

Password: •••••

Live Preview: Extra

Playback: Extra

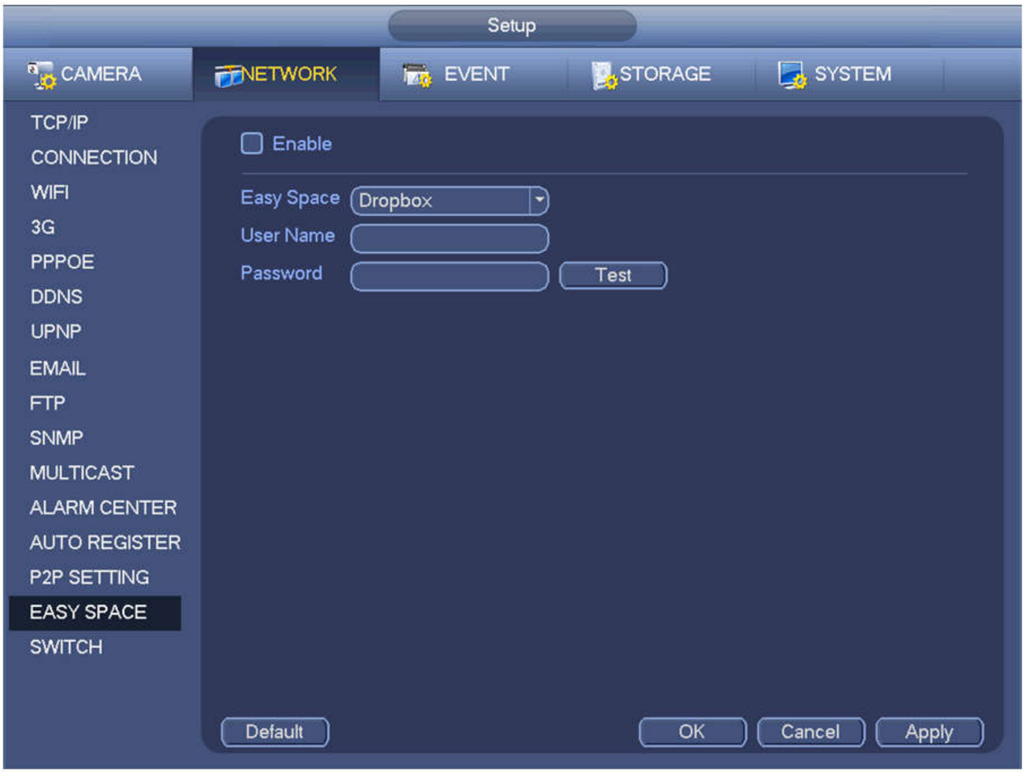
Figure 4-186

4.8.1.16 Easy Space

This function allows you to upload motion detect record or snapshot image to the dropbox and etc.

The easy space interface is shown as below. See Figure 4-187.

Please select the easy space address from the dropdown list and then input corresponding user name and password.



□ Enable

Easy Space: Dropbox

User Name:

Password:

Figure 4-187

Note:

- The uploaded file is for sub stream only. Please go to record control interface (main stream->setting->Storage->Record) and then select sub stream.
- The easy space function uses upload bandwidth. Usually the recommended upload bandwidth shall be more than 512kbps and please make sure the network is stable.
- The easy space upload data adopts safe SSL encryption connection. Please enable 1-channel to upload in case this function occupies too much CPU.

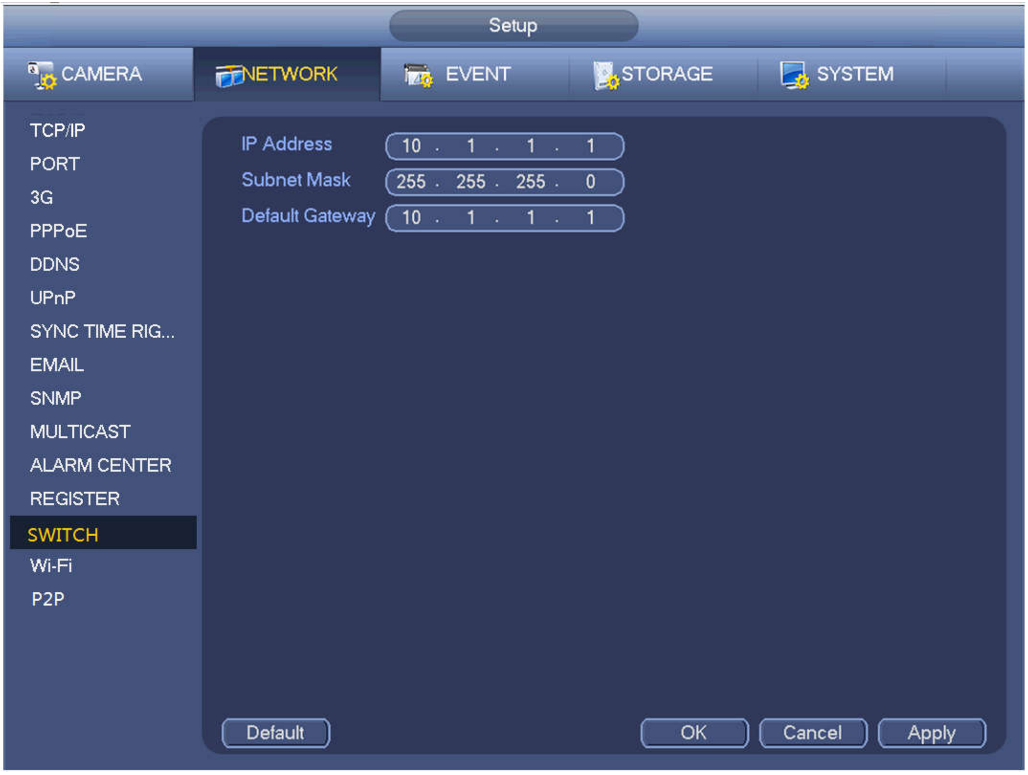
4.8.1.17 SWITCH

When connect a network camera to the PoE port of the NVR, NVR can automatically allocate the IP address according to the specified IP segment. The network camera can automatically register to the NVR.

It is for you to set IP address, subnet mask, gateway and etc of the Switch. See Figure 4-188.

Caution

- This function is for product of PoE port.
- Do not connect switch to the PoE port, otherwise the connection may fail.
- The SWITCH function of the NVR is enabled by default. The IP segment is 10.1.1.1. Usually we recommend the default setup.
- For the camera from the third party, make sure the camera supports ONVIF and DHCP function is enabled.



IP Address: 10 . 1 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 1 . 1 . 1

Figure 4-188

Refer to the following table for PoE notice.

Type	Note

Type	Note
Connect camera to the PoE	After connect the camera to the PoE, NVR allocate an IP address in the specified IP segment to the camera. NVR tries to use **arp ping to set.** If the NVR has enabled the DHCP function, it uses DHCP to set. ● After successfully set IP address, NVR can send out broadcast via the switch and get the corresponding response. Now The camera has registered to the NVR. Go to the preview interface, the corresponding channel has been used and there is a small PoE icon at the top left corner. ● Go to the Register interface to view the connected device list, you can see the PoE channel number, PoE port information and etc. Click IP search to display or refresh the information.
Remove camera from the PoE port	After remove the camera network cable from the PoE port, the channel displays “Cannot find the network host”. On the registration interface, the IP address is shown as offline.
The mapping policy when connect a camera to the PoE port.	The PoE port and the channel window is one to one correspondence. For example, connect a network camera to PoE port 1, it register to channel 1 by default.

4.8.2 Network Test

In this interface, you can see network test and network load information.

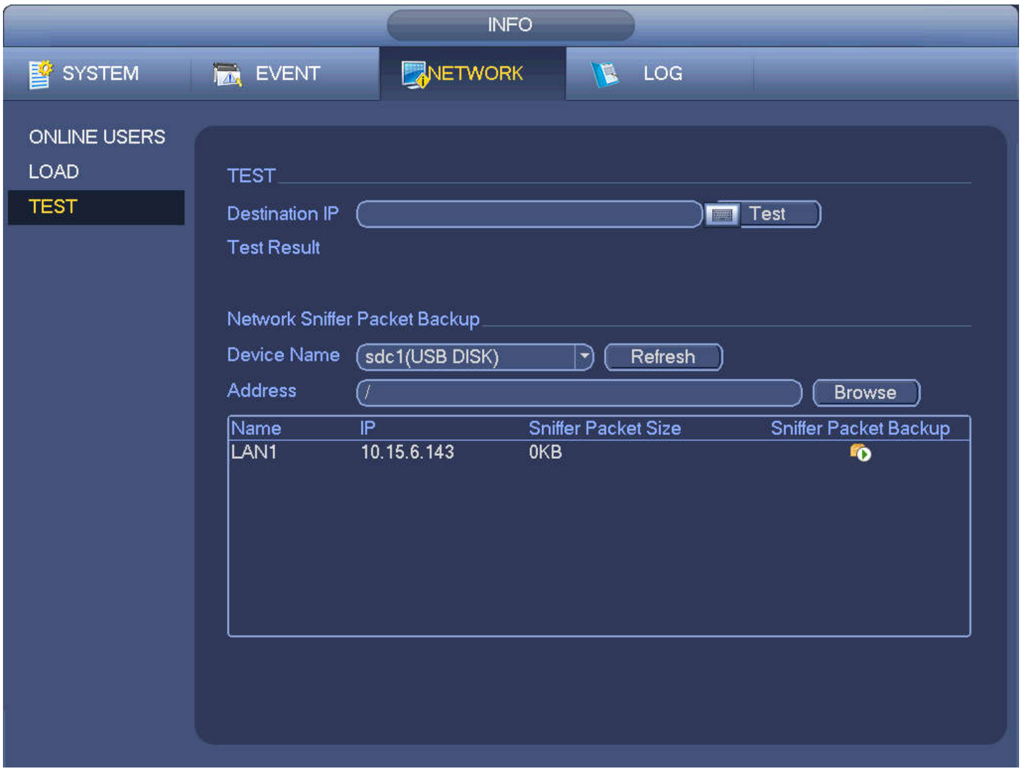
4.8.2.1 Network Test

From main menu->Info-Network->Test, the network test interface is shown as in Figure 4-189.

- Destination IP: Please input valid IPV4 address and domain name.
- Test: Click it to test the connection with the destination IP address. The test results can display average delay and packet loss rate and you can also view the network status as OK, bad, no connection and etc.
- Network Sniffer backup: Please insert USB2.0 device and click the Refresh button, you can view the device on the following column. You can use the dropdown list to select peripheral device. Click Browse button to select the snap path. The steps here are same as preview backup operation.

You can view all connected network adapter names (including Ethernet, PPPoE, Wi-Fi, and 3G), you can click the button ▶ on the right panel to begin Sniffer. Click the grey stop button to stop. Please note system cannot Sniffer several network adapters at the same time.

After Sniffer began, you can exit to implement corresponding network operation such as login WEB, monitor. Please go back to Sniffer interface to click 🟩 stop Sniffer. System can save the packets to the specified path. The file is named after “Network adapter name+time”. You can use software such as Wireshark to open the packets on the PC for the professional engineer to solve complicated problems.



TEST

Destination IP

Test Result

Network Sniffer Packet Backup

Device Name: sdc1(USB DISK)

Address: /

Name	IP	Sniffer Packet Size	Sniffer Packet Backup
LAN1	10.15.6.143	0KB	▶

Figure 4-189

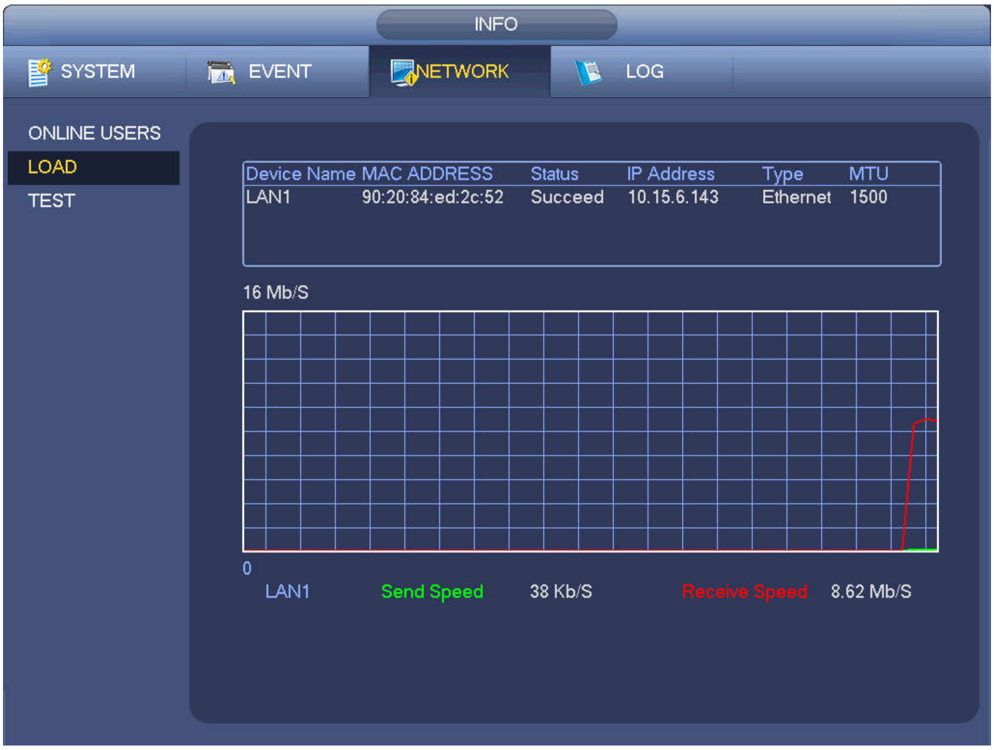
4.8.2.2 Network Load

From main menu->Info-Network->Load, network load is shown as in Figure 4-190. Here you can view the follow statistics of the device network adapter.

Here you can view information of all connected network adapters. The connection status is shown as offline if connection is disconnected. Click one network adapter, you can view the flow statistics such as send rate and receive rate at the top panel.

Note

- It is to display LAN1 network load by default.
- View one LAN network load by one time.



Device Name	MAC ADDRESS	Status	IP Address	Type	MTU
LAN1	90:20:84:ed:2c:52	Succeed	10.15.6.143	Ethernet	1500

LAN1 Send Speed 38 Kb/S Receive Speed 8.62 Mb/S

Figure 4-190

4.9 Storage

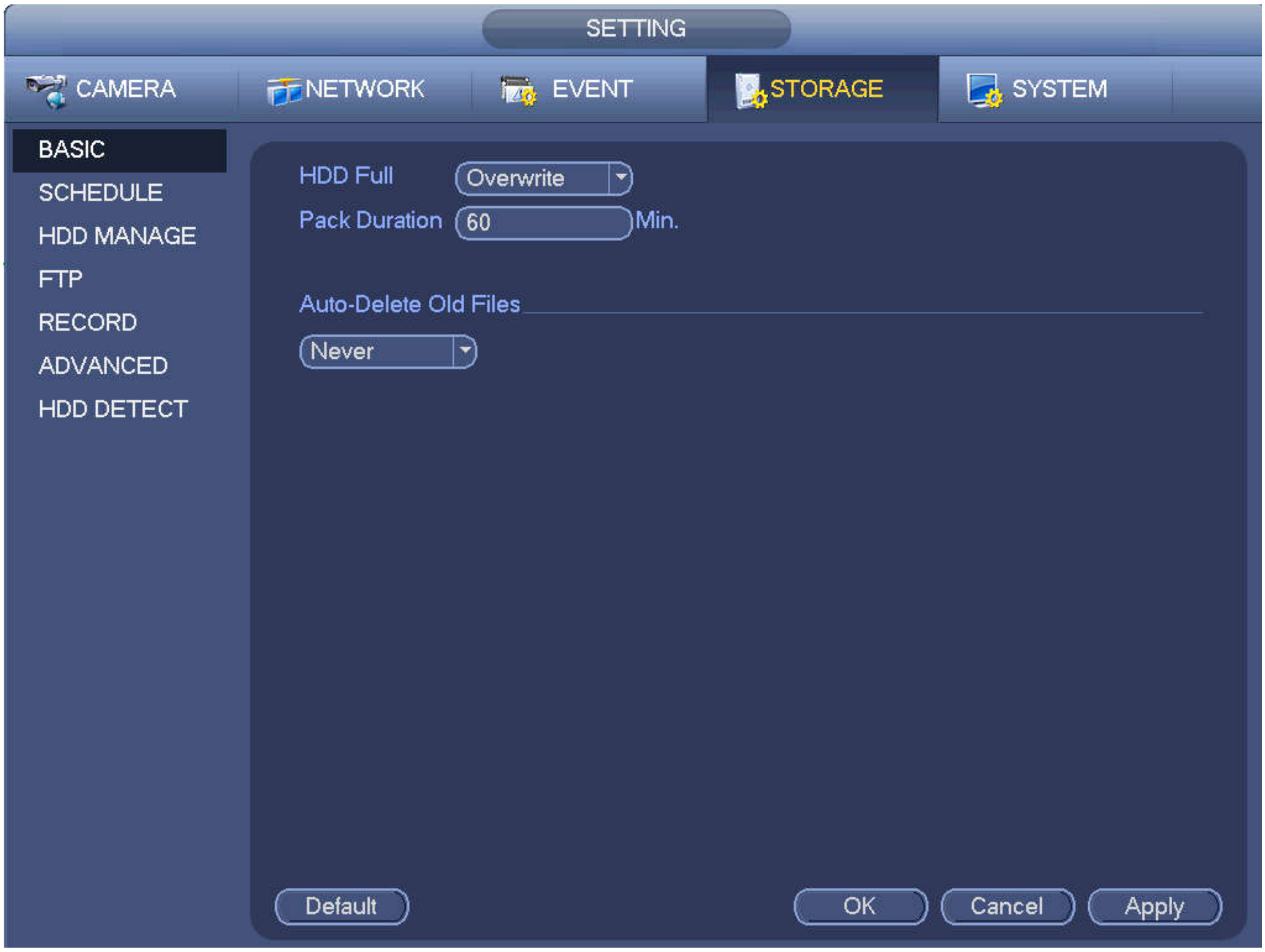
Here you can view HDD information such as type, status, total capacity, record time and etc. The operation includes format, resume from error, change HDD property (Read write, Read-only). Here you can also set alarm and HDD storage position.

4.9.1 Basic

It is to manage HDD storage space.

Step 1 From main menu->Setup->Storage->Basic.

Enter Basic interface. See Figure 4-191.



HDD Full: Overwrite

Pack Duration: 60 Min.

Auto-Delete Old Files: Never

Figure 4-191

Step 2 Set parameters.

- HDD full: It is to select working mode when hard disk is full. There are two options: stop recording or rewrite.
- Pack duration: It is to specify record duration. The max length is 120 minutes.
- Auto delete old files:
- ✧ Never: Do not auto delete old files.
- ✧ Customized: input customized period here and system can auto delete corresponding old files.
- ✧ The deleted file cannot be restored.

Step 3 Click Apply or Save to complete setup.

4.9.2 Schedule

It is to set schedule record and schedule snapshot. NVR can record or snapshot as you specified. For detailed information, please refer to chapter 4.1.4.6.1 schedule record and 4.1.4.6.2 schedule snapshot.

4.9.3 HDD

It is to view and sett HDD properties and format HDD.

It is to view current HDD type, status, capacity and etc. The operation includes format HDD, and change HDD property (read and write/read-only/redundancy).

- To prevent files be overwritten in the future, you can set HDD as read-only.
- To backup recorded video file, you can set HDD as redundant HDD.

Step 1 From Mani-menu->Setting->Storage->HDD Manager, you can go to HDD management interface.

See Figure 4-192.

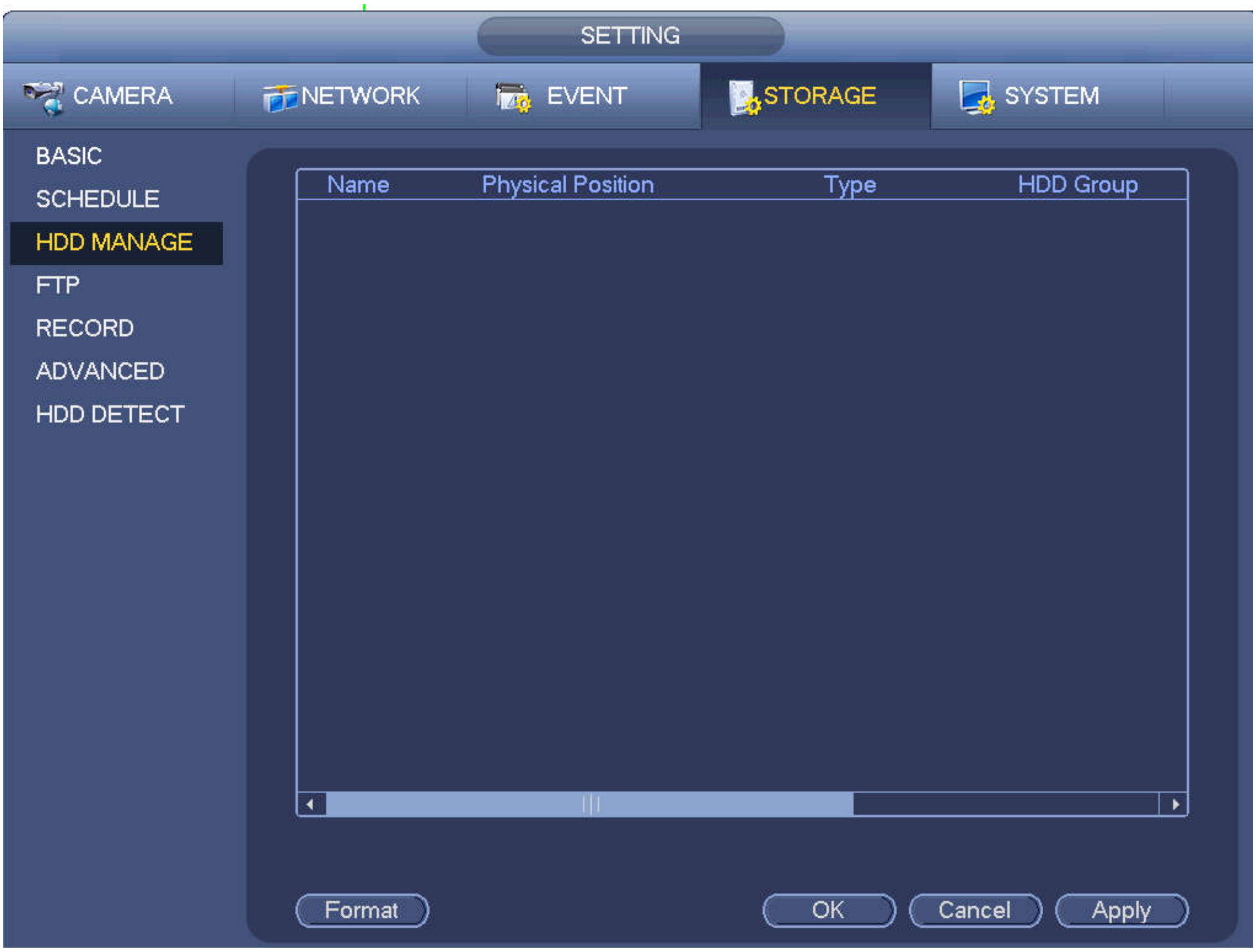


Figure 4-192

Step 2 Select a HDD and then select an time from the dropdown list. Click Execute button.

Step 3 Click OK button to complete the setup. You can see system needs to restart to activate current setup if you want to format the HDD.

4.9.4 FTP

It is to backup record file or image to the FTP to storage or view.

Before the operation, please download or purchase the FTP service tool and install on the PC.

Note

For the FTP user, please set FTP folder write right, otherwise system cannot upload the image.

Step 1 From main menu->Setting->Storage->FTP, enter FTP interface. See Figure 4-193.

Step 2 Select the Enable check box to enable FTP function. Select FTP type.

NOTE

FTP transmits data with clear text mode and SFTP transmits data with encrypted mode. SFTP is recommended.

Step 3 Set parameters.

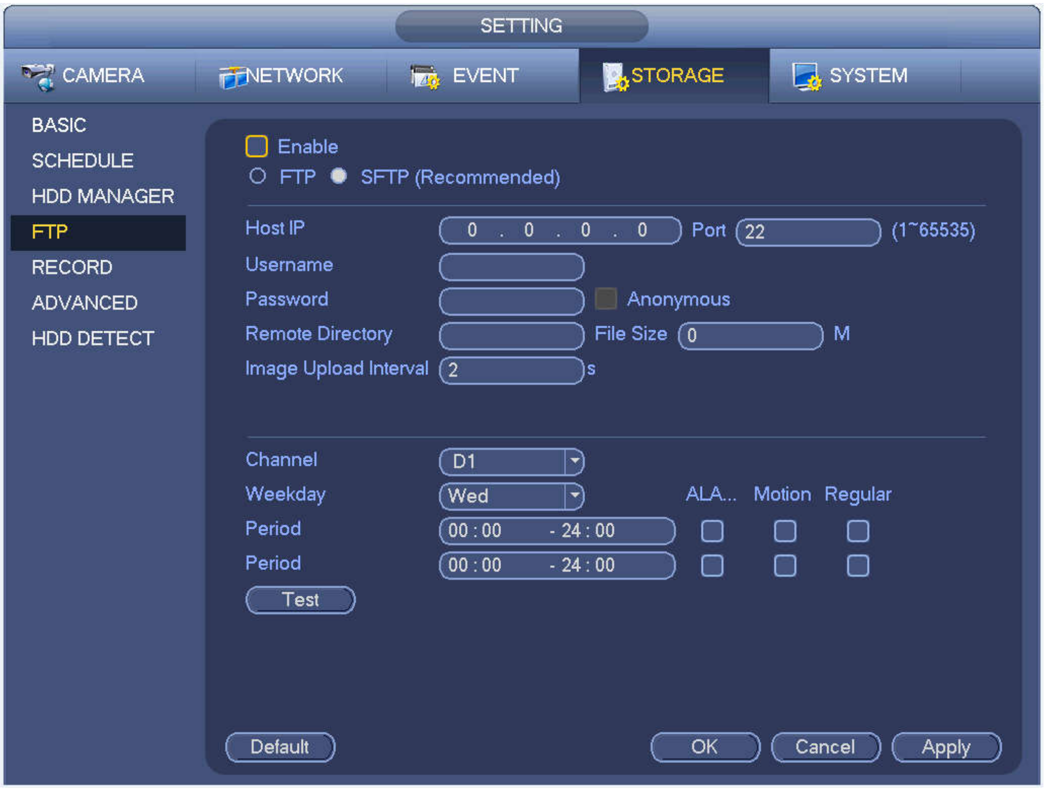
Here you can input FTP server address, port and remote directory. When remote directory is null, system automatically creates folders according to the IP, time and channel.

- IP address: The host IP you have installed the FTP server.
- Port: The default SFTP port number is 22 and the default FTP port number is 21.

- User name/Password: The account for you to access the FTP server.
- Remote directory: The folder you created under the root path of the FTP according to the corresponding rule.
  - ✧ If there is no remote directory, system can auto create different directories according to the IP, time and channel.
  - ✧ If there is remote directory, system can create corresponding folder under the FTP root path and then create different folders according to IP address, time and channel.
- File length: File length is upload file length. When setup is larger than the actual file length, system will upload the whole file. When setup here is smaller than the actual file length, system only uploads the set length and auto ignore the left section. When interval value is 0, system uploads all corresponding files.
- Image upload interval: It is the image upload interval. If the image upload interval is larger than the image snapshot frequency, system just uploads the lasted image.
  - ✧ If the image interval is 5 seconds and the snapshot frequency is 2 seconds, system will send out the latest image at the buffer at 5 seconds.
  - ✧ If the image upload interval is smaller than the snapshot frequency, system will upload at the snapshot frequency. For example, if the image interval is 5 seconds and the snapshot frequency is 10 seconds, system will send out the image at 10 seconds.
  - ✧ From main menu->Setting->Camera->Encode->Snapshot to set snapshot frequency.
- Channel: Select a channel from the dropdown list and then set week, period and record type.
- Week day/Period: Please select from the dropdown list and for each day, you can set two periods.
- Type: Please select uploaded record type (Alarm/intelligent/motion detect/regular). Please check the box to select upload type.

Step 4 Click the Test button, you can see the corresponding dialogue box to see the FTP connection is OK or not.

Step 5 Click Apply or Save to complete setup.



□ Enable

○ FTP ● SFTP (Recommended)

Host IP 0 . 0 . 0 . 0 Port 22 (1~65535)

Username

Password □ Anonymous

Remote Directory File Size 0 M

Image Upload Interval 2 s

Channel D1

Weekday Wed ALA... Motion Regular

Period 00 : 00 - 24 : 00 □ □ □

Period 00 : 00 - 24 : 00 □ □ □

Figure 4-193

4.9.5 Record Control

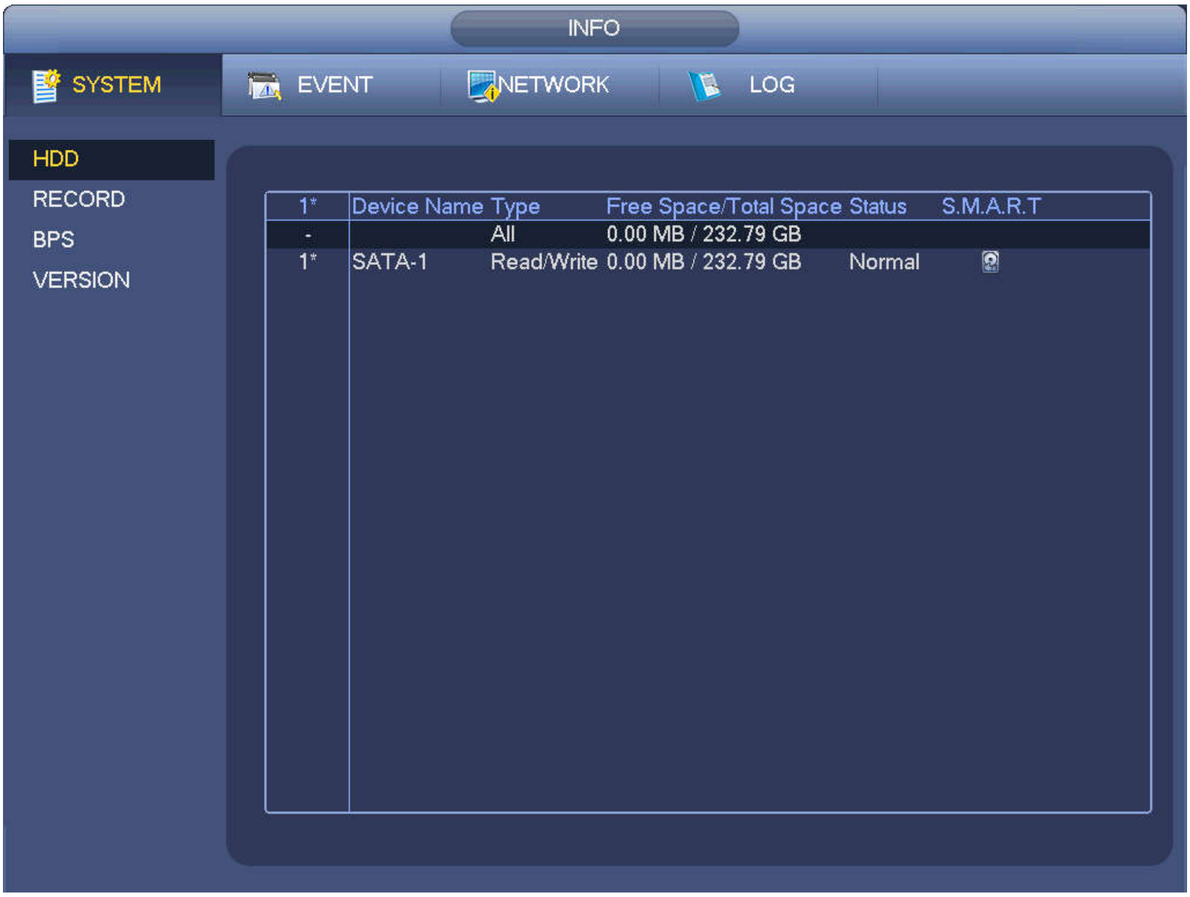
After you set schedule record or schedule snapshot function, please set auto record/snapshot function so that the NVR can automatically record or snapshot. For detailed information, please refer to chapter 4.1.4.6.3 record control.

4.9.6 HDD Information

Here is to list hard disk type, total space, free space, and status. See Figure 4-194.

○ means current HDD is normal.. - means there is no HDD.

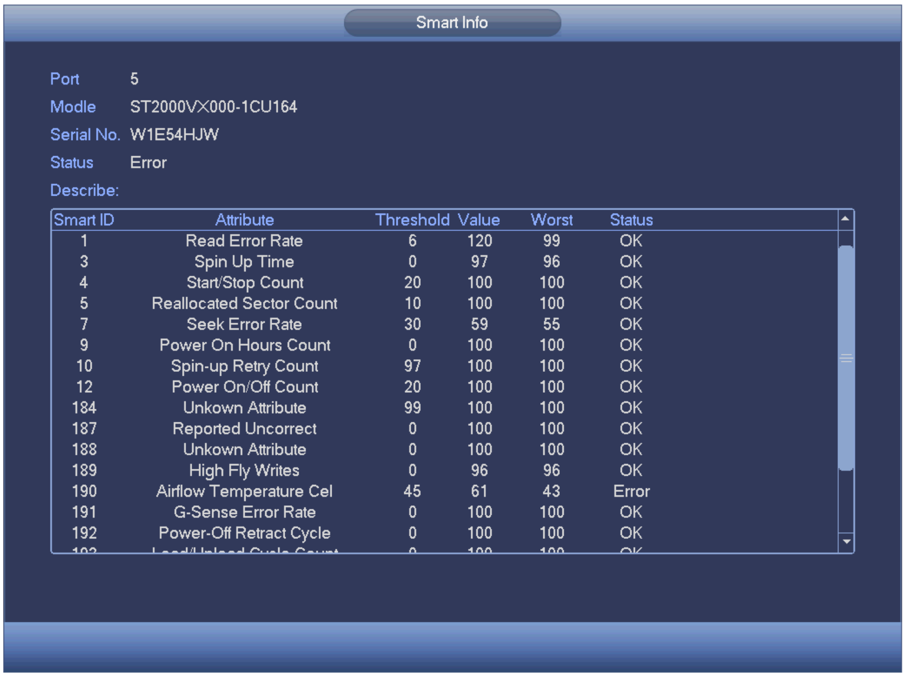
If disk is damaged, system shows as “?”. Please remove the broken hard disk before you add a new one.



1*	Device Name	Type	Free Space/Total Space	Status	S.M.A.R.T
-		All	0.00 MB / 232.79 GB		
1*	SATA-1	Read/Write	0.00 MB / 232.79 GB	Normal	

Figure 4-194

In Figure 4-194, click one HDD item, the S.M.A.R.T interface is shown as in Figure 4-195.



Port 5

Modle ST2000VX000-1CU164

Serial No. W1E54HJW

Status Error

Describe:

Smart ID	Attribute	Threshold	Value	Worst	Status
1	Read Error Rate	6	120	99	OK
3	Spin Up Time	0	97	96	OK
4	Start/Stop Count	20	100	100	OK
5	Reallocated Sector Count	10	100	100	OK
7	Seek Error Rate	30	59	55	OK
9	Power On Hours Count	0	100	100	OK
10	Spin-up Retry Count	97	100	100	OK
12	Power On/Off Count	20	100	100	OK
184	Unkown Attribute	99	100	100	OK
187	Reported Uncorrect	0	100	100	OK
188	Unkown Attribute	0	100	100	OK
189	High Fly Writes	0	96	96	OK
190	Airflow Temperature Cel	45	61	43	Error
191	G-Sense Error Rate	0	100	100	OK
192	Power-Off Retract Cycle	0	100	100	OK
193	Load/Unload Cycle Count	0	100	100	OK

Figure 4-195

Parameter	Function
SATA	1 here means there is 1 HDD. For different series product, the max HDD amount may vary, When HDD is working properly, system is shown as O. . “_” means there is no HDD.
SN	You can view the HDD amount the device connected to; ＊ means the second HDD is current working HDD.
Type	The corresponding HDD property.
Total space	The HDD total capacity.
Free space	The HDD free capacity.
Status	HDD can work properly or not.
Bad track	Display there is bad track or not.
Page up	Click it to view previous page.
Page down	Click it to view the next page.
View recording time	Click it to view HDD record information (file start time and end time).
View HDD type and capability	Click it to view HDD property, status and etc,

4.9.7 HDD Group

It is to set HDD group, and HDD group setup for main stream, sub stream and snapshot operation.

⚠ Caution

When you are setting HDD group, please set a HDD for each channel, otherwise NVR cannot save current setup.

The main stream is shown as in Figure 4-196.

- HDD: Here you can view the HDD amount the device can support.
- Group: It lists the HDD Group number of current hard disk.

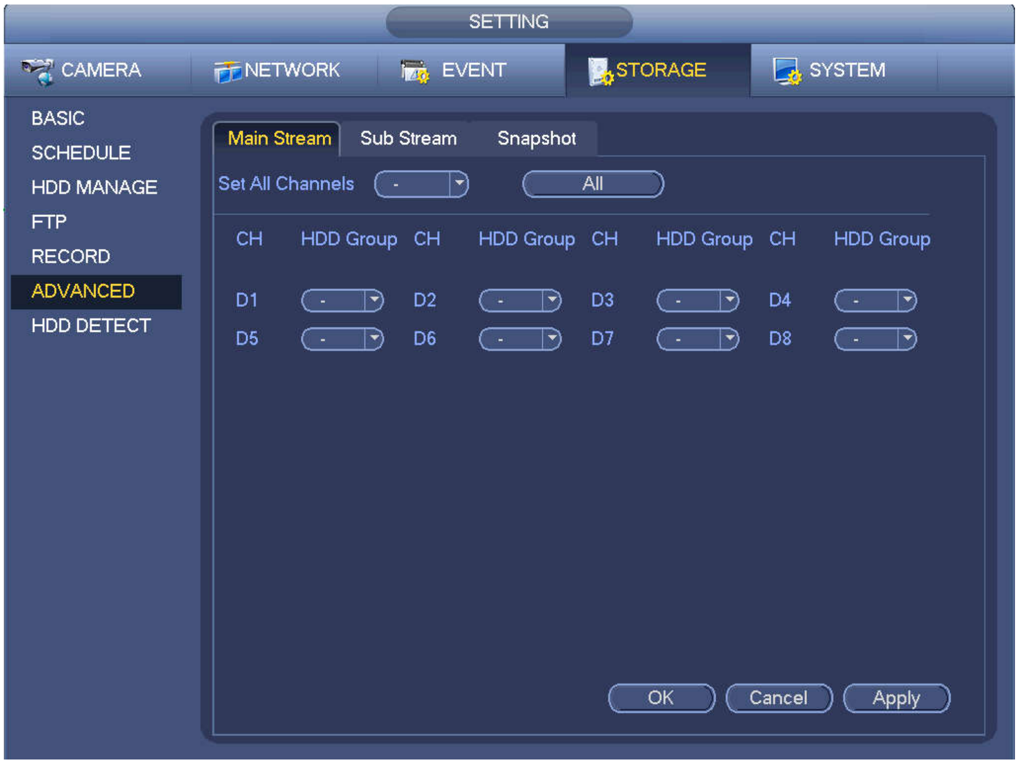


Figure 4-196

Please select the correspond group from the dropdown list and then click Apply button.

Click sub stream/snapshot button to set corresponding HDD group information.

4.9.8 HDD Detect

Note

This function is for some series product only.

The HDD detect function is to detect HDD current status so that you can clearly understand the HDD performance and replace the malfunction HDD.

There are two detect types:

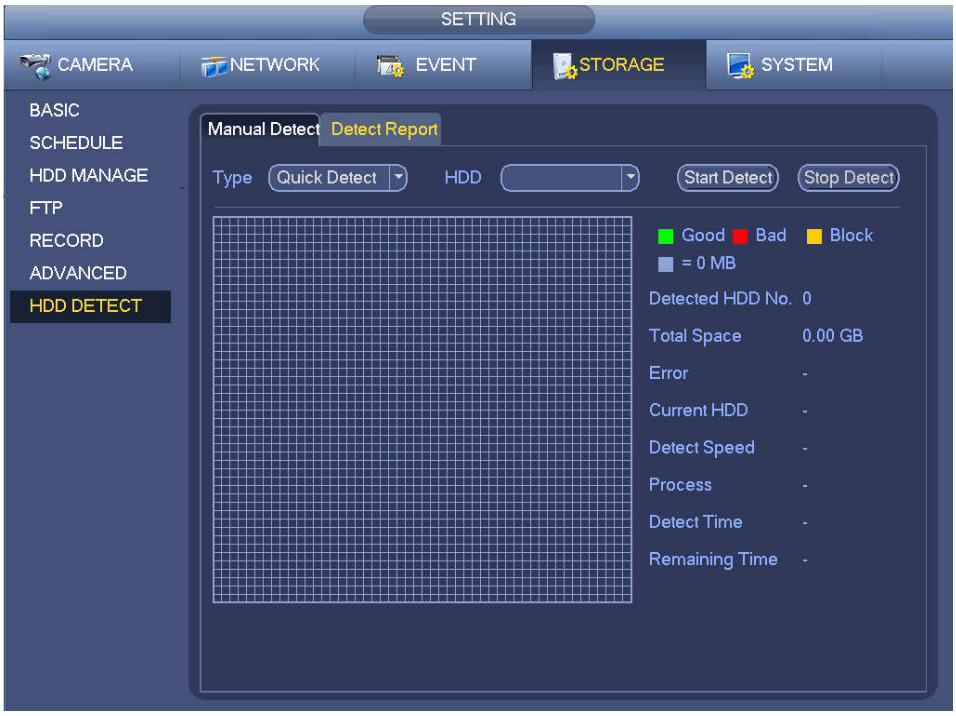
- Quick detect is to detect via the universal system files. System can quickly complete the HDD scan. If you want to use this function, please make sure the HDD is in use now. If the HDD is removed from other device, please make sure the write-data once was full after it installed on current device.
- Global detect adopts Windows mode to scan. It may take a long time and may affect the HDD

that is recording.

4.9.8.1 Manual Detect

From main menu->Setting->Storage->HDD Detect->Manual Detect, the interface is shown as below. See Figure 4-197.

Please select detect type and HDD. Click start detect to begin. You can view the corresponding detect information.



Type: Quick Detect

HDD:

🟩 Good 🟥 Bad 🟨 Block
▩ = 0 MB

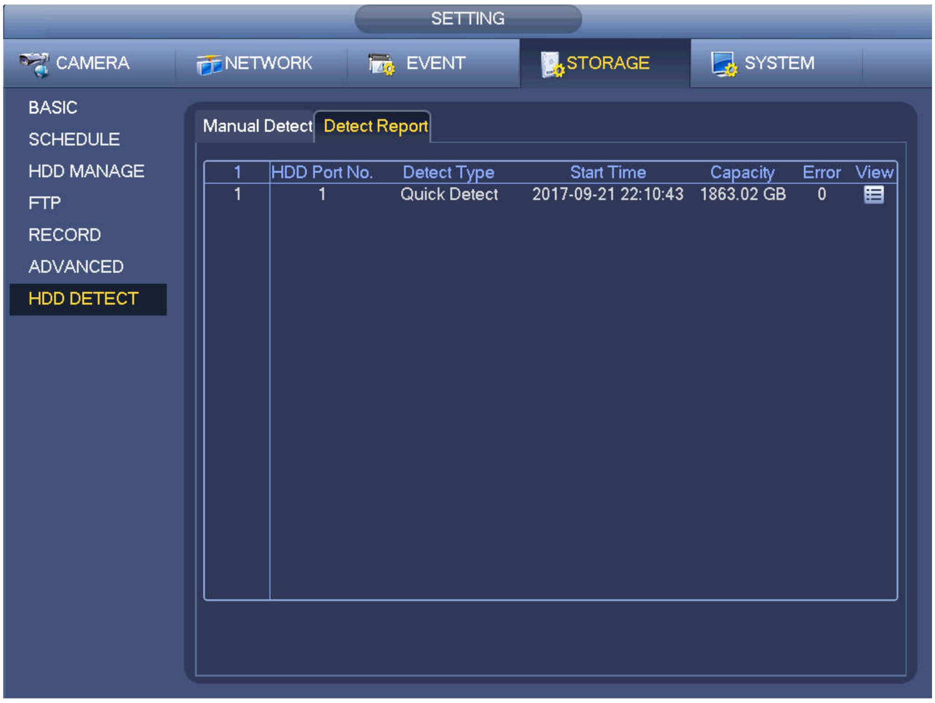
Detected HDD No.	0
Total Space	0.00 GB
Error	-
Current HDD	-
Detect Speed	-
Process	-
Detect Time	-
Remaining Time	-

Figure 4-197

4.9.8.2 Detect Report

After the detect operation, you can go to the detect report to view corresponding information.

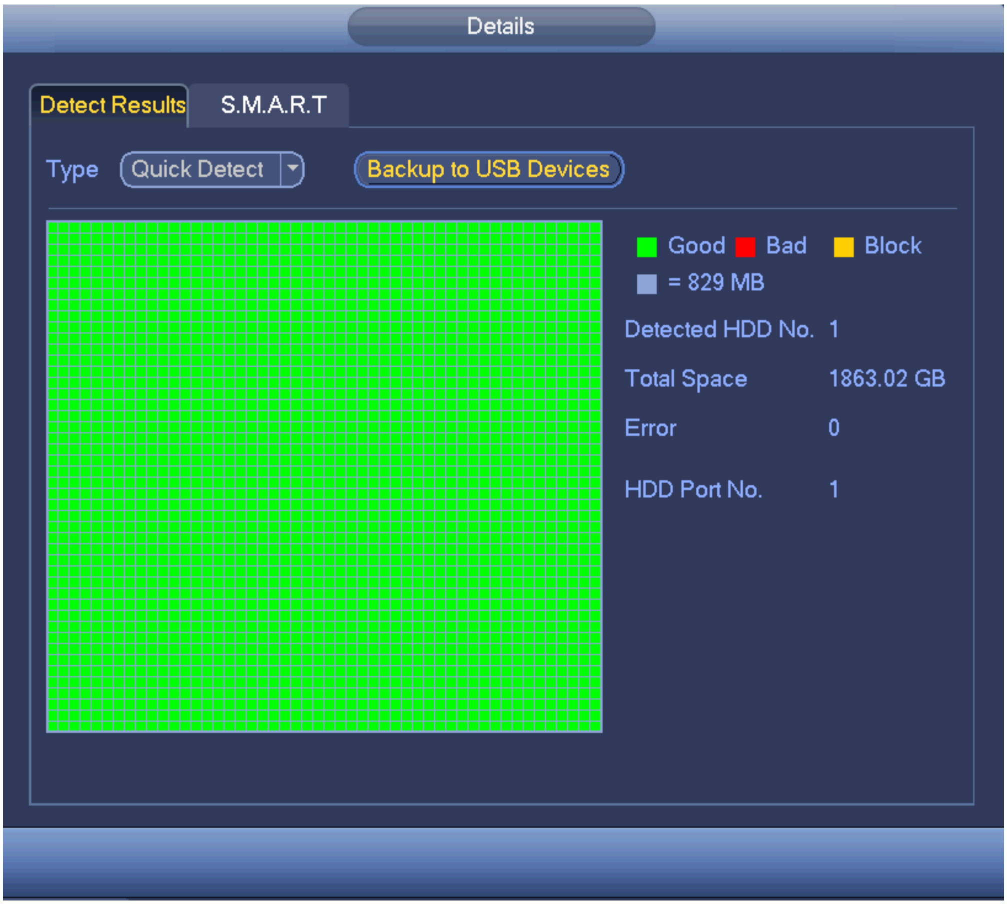
From main menu->Setting->Storage->HDD Detect->Manual Detect, the interface is shown as below. See Figure 4-198.



1	HDD Port No.	Detect Type	Start Time	Capacity	Error	View
1	1	Quick Detect	2017-09-21 22:10:43	1863.02 GB	0	▤

Figure 4-198

Click View, you can see the detailed information such as detect result, backup and S.M.A.R.T. See Figure 4-199 and Figure 4-200.



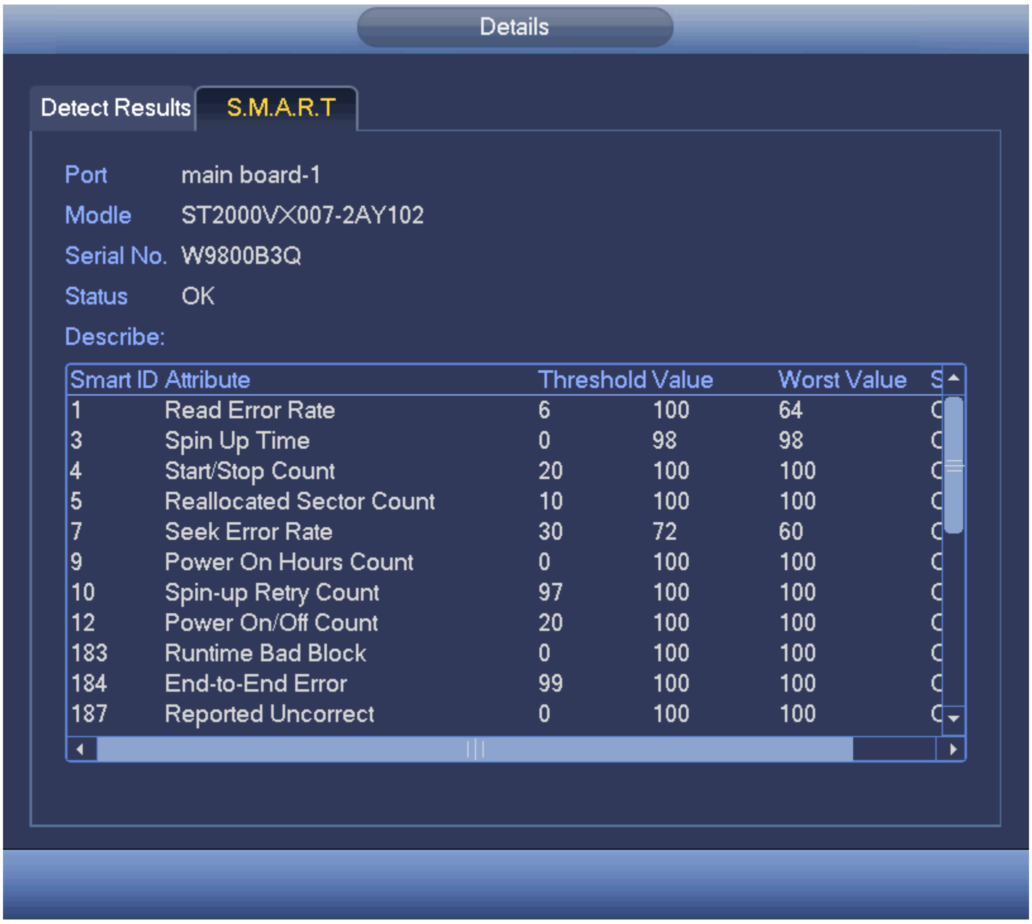
Type: Quick Detect

🟩 Good 🟥 Bad 🟨 Block

■ = 829 MB

Detected HDD No.	1
Total Space	1863.02 GB
Error	0
HDD Port No.	1

Figure 4-199



Port main board-1

Modle ST2000VX007-2AY102

Serial No. W9800B3Q

Status OK

Describe:

Smart ID	Attribute	Threshold	Value	Worst Value	S
1	Read Error Rate	6	100	64	C
3	Spin Up Time	0	98	98	C
4	Start/Stop Count	20	100	100	C
5	Reallocated Sector Count	10	100	100	C
7	Seek Error Rate	30	72	60	C
9	Power On Hours Count	0	100	100	C
10	Spin-up Retry Count	97	100	100	C
12	Power On/Off Count	20	100	100	C
183	Runtime Bad Block	0	100	100	C
184	End-to-End Error	99	100	100	C
187	Reported Uncorrect	0	100	100	C

Figure 4-200

4.9.9 RAID Manager

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

Note

- RAID function is for some series product only. Slight difference may be found on the user interface.
- Right now, NVR supports RAID0, RAID1, RAID5, RAID6, and RAID 10. Local hotspare supports RAID1, RAID5, RAID6, and RAID10.
- Refer to the following table for detailed information.

RAID Type	HDD Amount
RAID0	At least 2 HDDs.
RAID1	Only 2 HDDs.
RAID5	At least 3 HDDs. Usually recommend the RAID5 consists of 4 to 6 HDDs.
RAID6	At least 4 HDDs.
RAID10	At least 4 HDDs.

4.9.9.1 RAID Config

It is for you to manage RAID HDD. It can display RAID name, type, free space, total space, status and etc. Here you can add/delete RAID HDD.

Click Add button to select RAID type and then select HDDs, click OK button to add. See Figure 4-201.

One click to create RAID

- Click it to automatically create RAID5.
- For create RAID function, you can select the physical HDD that does not included in the RAID group or the created disk array to create a RAID5. You can refer to the following situations:
- There is no RAID, no hotspare disk: System directly creates the RAID5 and creates one hotspare disk at the same time.
- There is no RAID, but there is a hotspare disk: System creates the RAID5 only. It uses previous hotspare disk.
- There is RAID: System cancel the previous RAID setup and then create the new RAID5. System creates the hotspare disk if there is no one. System uses previous hotspare disk if there is hotspare disk available.
- The background will format the virtual disk.

Create manually

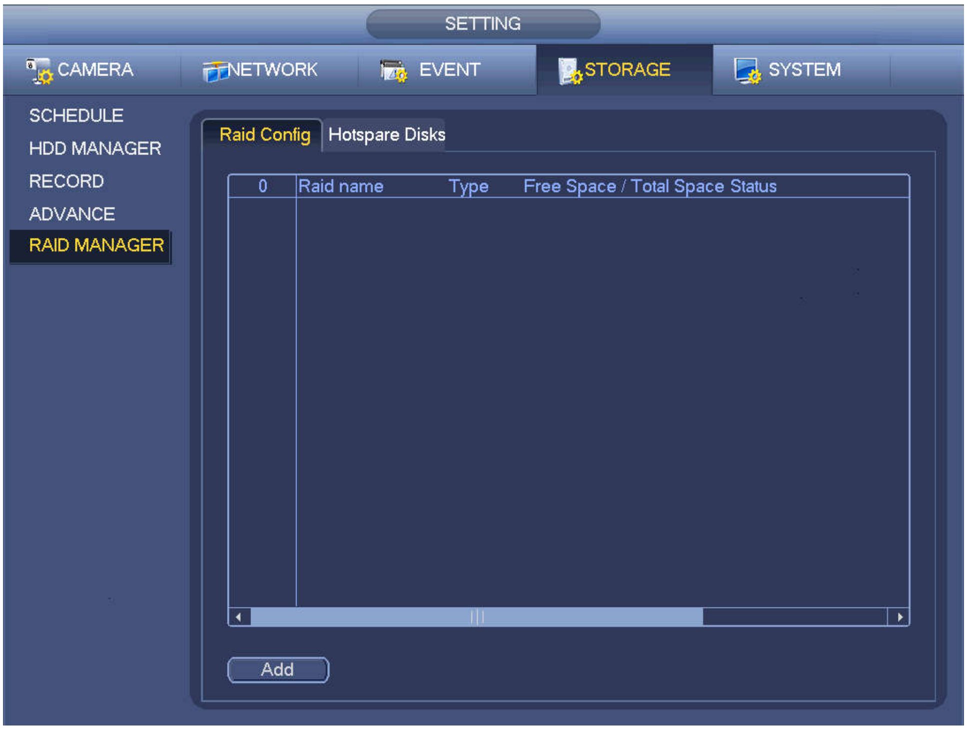
Step 1 Select RAID type first and then follow the prompts to set HDD amount.

Step 2 Click Create Manually button, system pops up dialogue box to warning you it is going to clear all data.

Step 3 Click OK button to complete the operation.

Note

Click ☒ to delete RAID.



0	Raid name	Type	Free Space / Total Space	Status

Figure 4-201

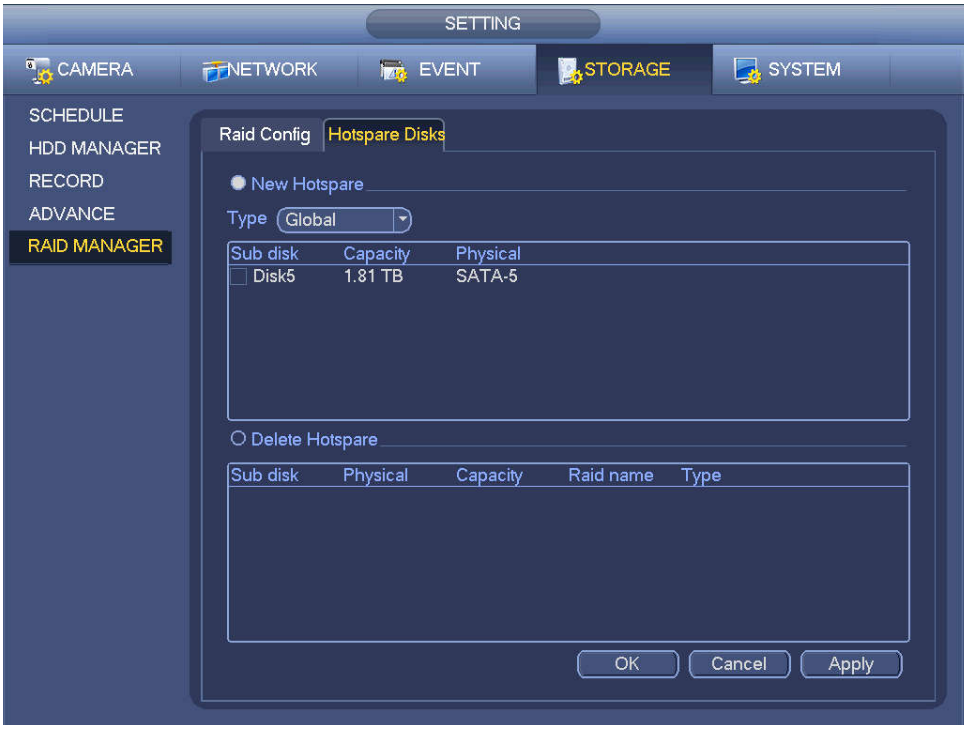
4.9.9.2 Hotspare disks

When a HDD of the RAID group is malfunction or abnormal, the hotspare HDD can replace the malfunction or abnormal HDD in case there is any data loss. It is to guarantee storage system reliability.

Click Hotspare disks tab name, you can add the hot spare HDD. See Figure 4-202. The type includes two options:

- Global: It is global hotspare disk. When any RAID becomes degrading, it can replace and build the RAID.
- Local: It is local hotspare disk. When the specified RAID becomes degrading, it can replace and build the RAID.

Select a hot spare device and then click Delete button. Click Apply button to delete.



● New Hotspare

Type Global

Sub disk	Capacity	Physical
□ Disk5	1.81 TB	SATA-5

○ Delete Hotspare

Sub disk	Physical	Capacity	Raid name	Type

Figure 4-202

4.10 Device Maintenance and Manager

4.10.1 Account

It is to manage users, user group and ONVIF user, set admin security questions.

Note

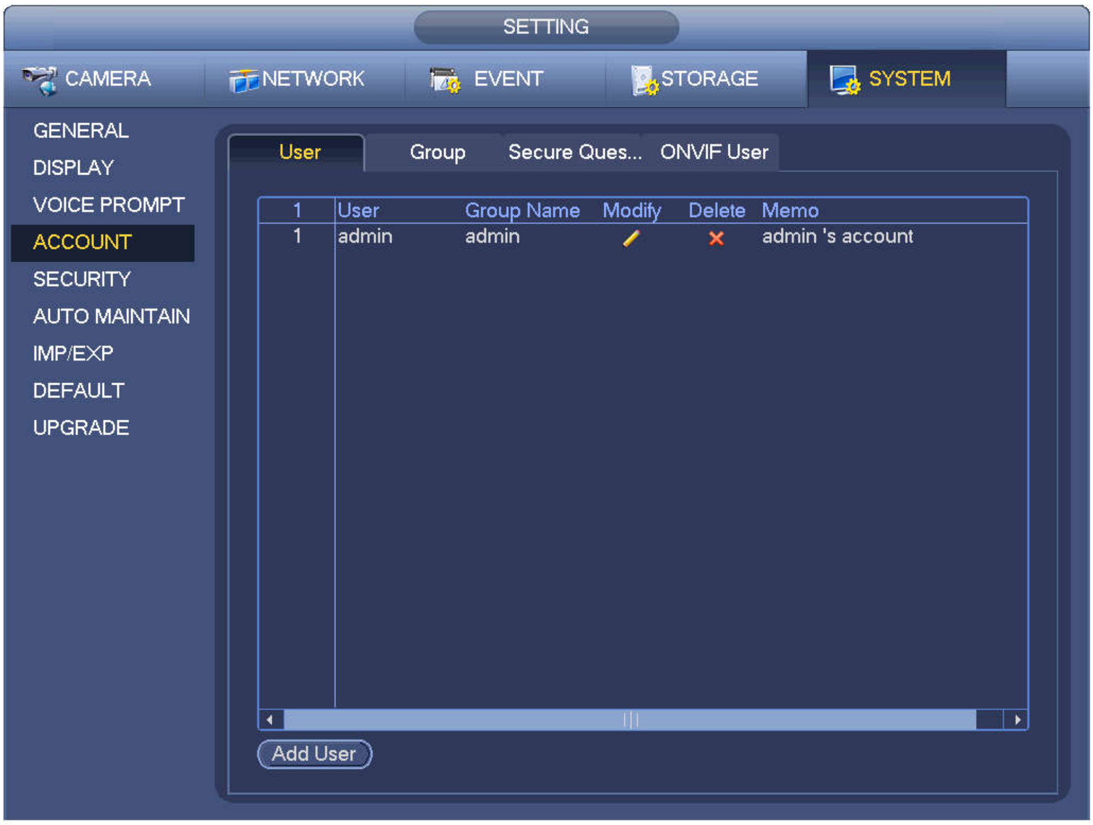
- For the user name, the string max length is 31-byte, and for the user group, the string max length is 15-byte. The user name can only contain English letters, numbers and "_"、"@"、".".
- The default user amount is 64 and the default group amount is 20. System account adopts two-level management: group and user. The user authorities shall be smaller than group authorities (The **admin** user authorities are set by default).
- For group or user management, there are two levels: admin and user. The user name shall be unique and one user shall only belong to one group.

4.10.1.1 User

4.10.1.1.1 Add User

Step 1 From main menu->Setting->System->Account->User.

Enter user interface. See Figure 4-203.

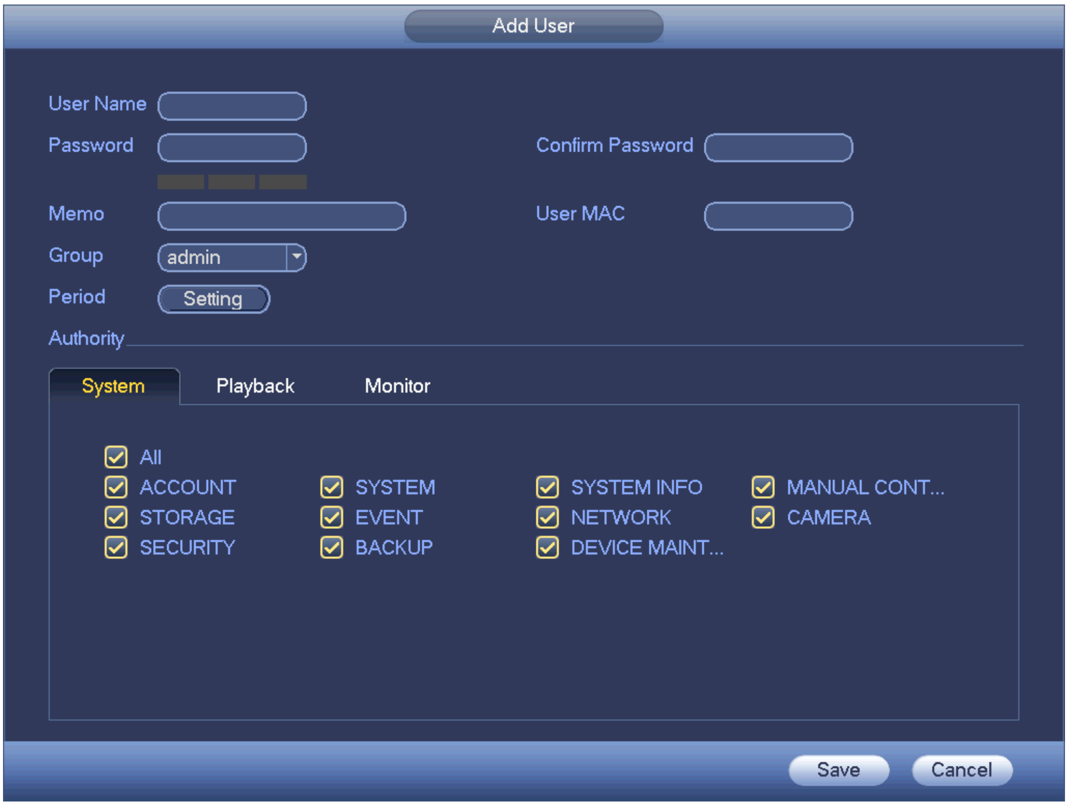


1	User	Group Name	Modify	Delete	Memo
1	admin	admin	✎	✕	admin 's account

Figure 4-203

Step 2 Click Add user button in Figure 4-203.

The interface is shown as in Figure 4-204.



Group: admin

☑ All
☑ ACCOUNT ☑ SYSTEM ☑ SYSTEM INFO ☑ MANUAL CONT...
☑ STORAGE ☑ EVENT ☑ NETWORK ☑ CAMERA
☑ SECURITY ☑ BACKUP ☑ DEVICE MAINT...

Figure 4-204

Step 3 Input the user name, password, select the group it belongs to from the dropdown list. Then you can check the corresponding rights for current user.

Note

For convenient user management, usually we recommend the general user right is lower than the admin account.

Step 4 Click the Set button after the period, you can set valid period to use current account. See Figure 4-205.

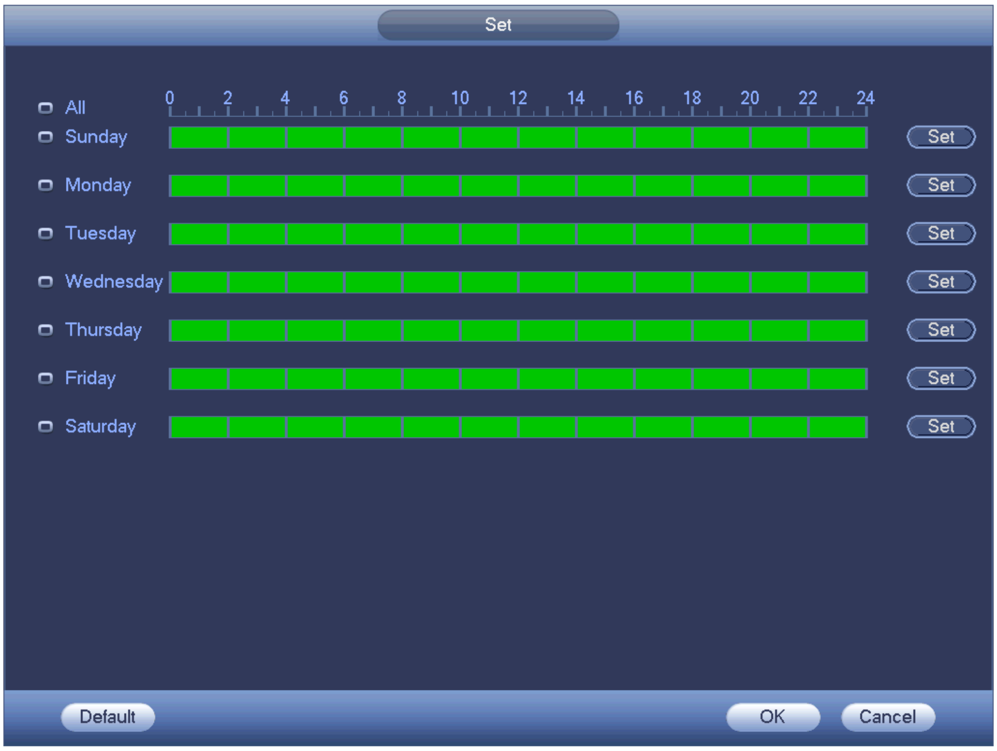


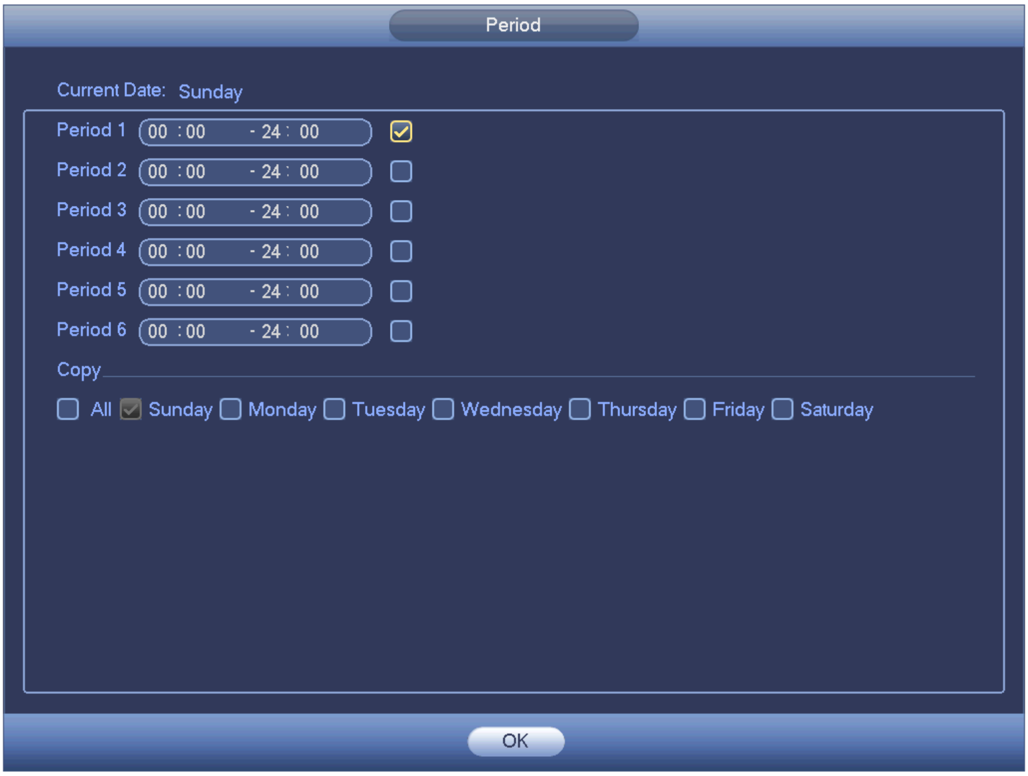
Figure 4-205

Step 5 Click Set button, you can set six periods in one day. See Figure 4-206.

Step 6 Check the box after the period, you can enable current setup.

Note

Check the box before the week; it is to save period settings to selected week day.



Period

Current Date: Sunday

Period 1 00 : 00 - 24 : 00 ☑

Period 2 00 : 00 - 24 : 00 □

Period 3 00 : 00 - 24 : 00 □

Period 4 00 : 00 - 24 : 00 □

Period 5 00 : 00 - 24 : 00 □

Period 6 00 : 00 - 24 : 00 □

Copy

□ All ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

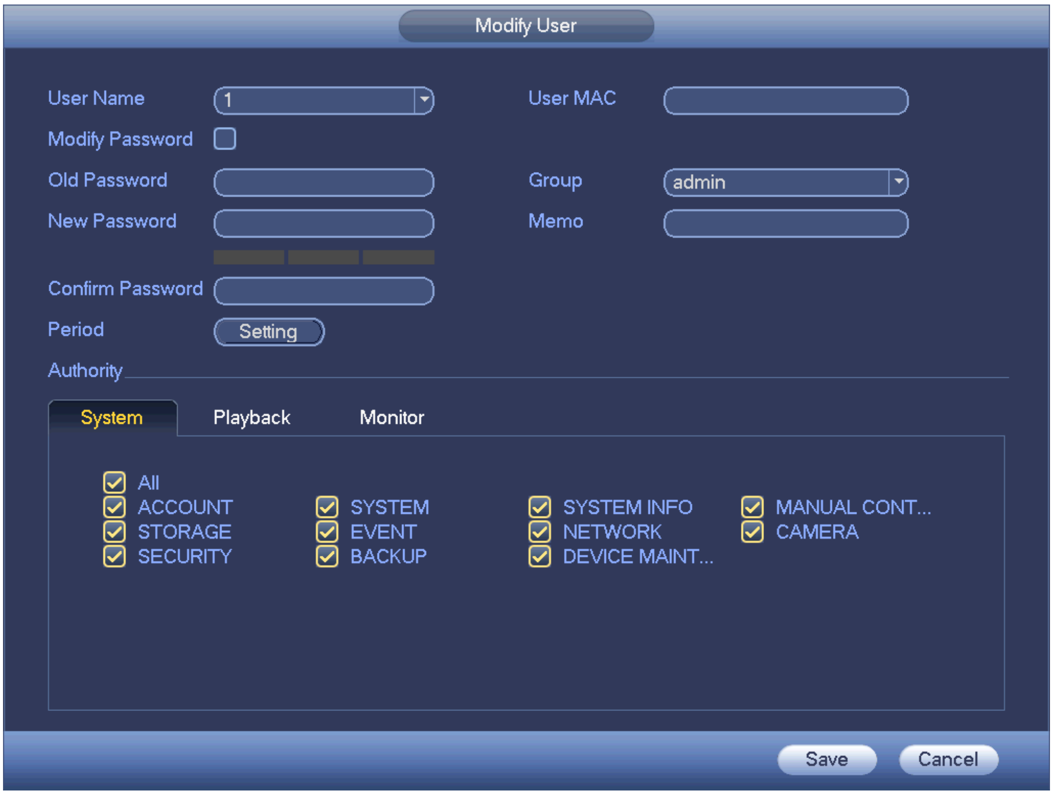
OK

Figure 4-206

Step 7 Click OK button.

4.10.1.1.2 Modify user

From main menu->Setting->System->Account->User, click ✎, you can go to the following interface to change user information. See Figure 4-207.



Modify User

User Name: 1

User MAC:

Modify Password □

Old Password:

Group: admin

New Password:

Memo:

Confirm Password:

Period: Setting

Authority

System | Playback | Monitor

☑ All

☑ ACCOUNT ☑ SYSTEM ☑ SYSTEM INFO ☑ MANUAL CONT...

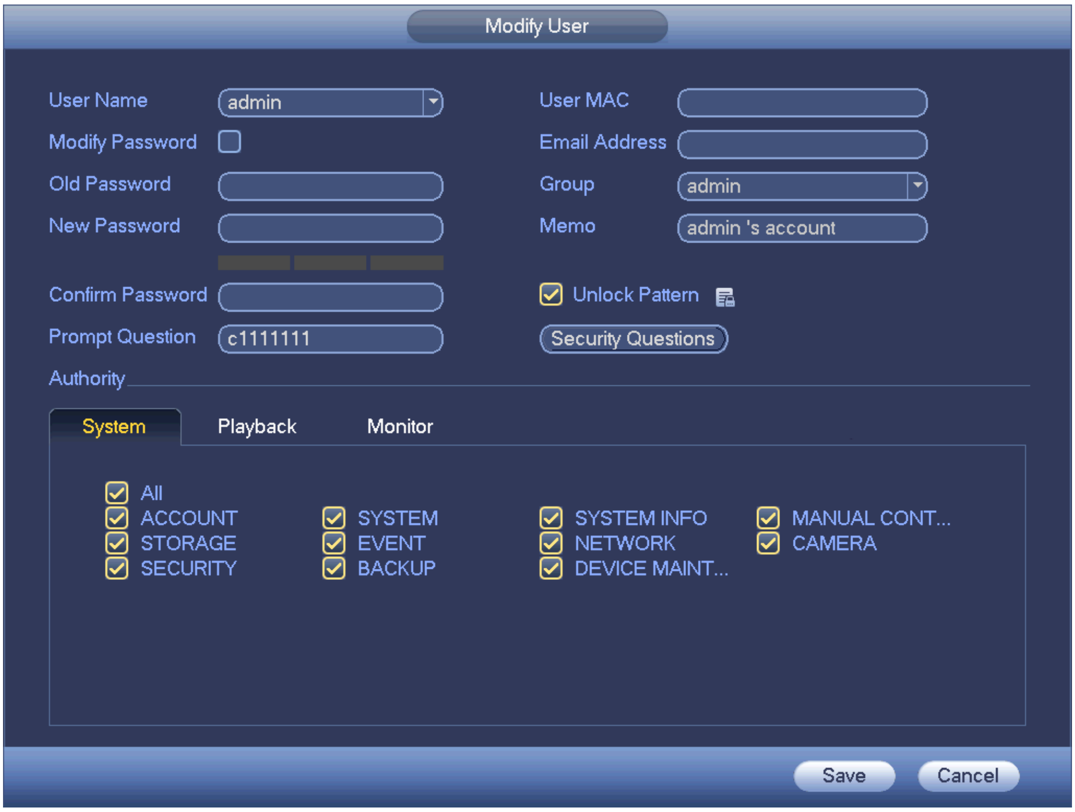
☑ STORAGE ☑ EVENT ☑ NETWORK ☑ CAMERA

☑ SECURITY ☑ BACKUP ☑ DEVICE MAINT...

Save Cancel

Figure 4-207

For **admin** user, you can change the email, enable/disable unlock pattern, change password prompt question, set security questions. See Figure 4-208.



User Name: admin

Modify Password: □

Old Password:

New Password:

Confirm Password:

Prompt Question: c1111111

User MAC:

Email Address:

Group: admin

Memo: admin 's account

☑ Unlock Pattern

Authority

System | Playback | Monitor

☑ All

☑ ACCOUNT ☑ SYSTEM ☑ SYSTEM INFO ☑ MANUAL CONT...

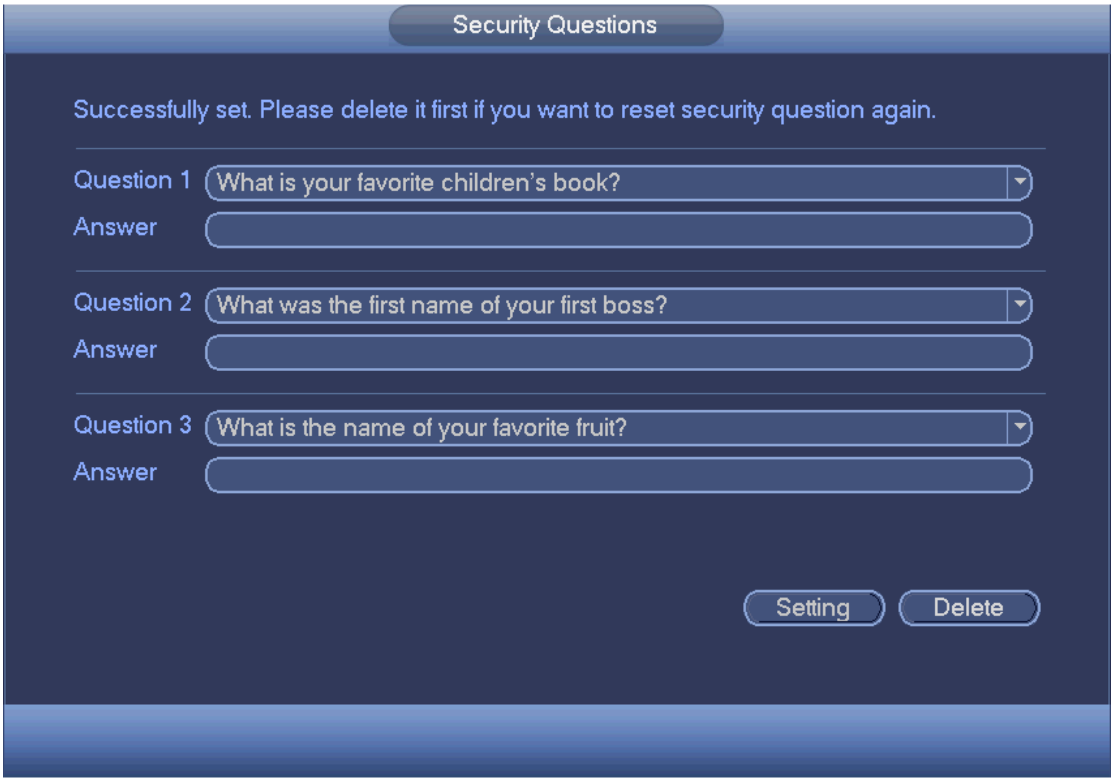
☑ STORAGE ☑ EVENT ☑ NETWORK ☑ CAMERA

☑ SECURITY ☑ BACKUP ☑ DEVICE MAINT...

Figure 4-208

- Input email information and then click Save, it is to set/change email address.
- Check the box to enable unlock pattern and then click, click Save to change unlock pattern.
- Set security question

Step 1 Click Security question, enter the following interface. See Figure 4-209.



Security Questions

Successfully set. Please delete it first if you want to reset security question again.

Question 1: What is your favorite children's book?

Answer:

Question 2: What was the first name of your first boss?

Answer:

Question 3: What is the name of your favorite fruit?

Answer:

Figure 4-209

Step 2 Input answers and then click Save button.

After successfully set security questions, you can answer the security questions to reset admin password.

Note

Select security questions from the dropdown list and then input the proper answers, click Delete button to reset security questions and answers again.

4.10.1.1.3 Change Password

In Figure 4-207, check the Modify password box, you can change password. Please input old password, and then input new password twice to confirm.

- Password/confirm password: The password ranges from 8 to 32 digitals. It can contain letters, numbers and special characters (excluding "'","''",";",":","&") . The password shall contain at least two categories. Usually we recommend the strong password.

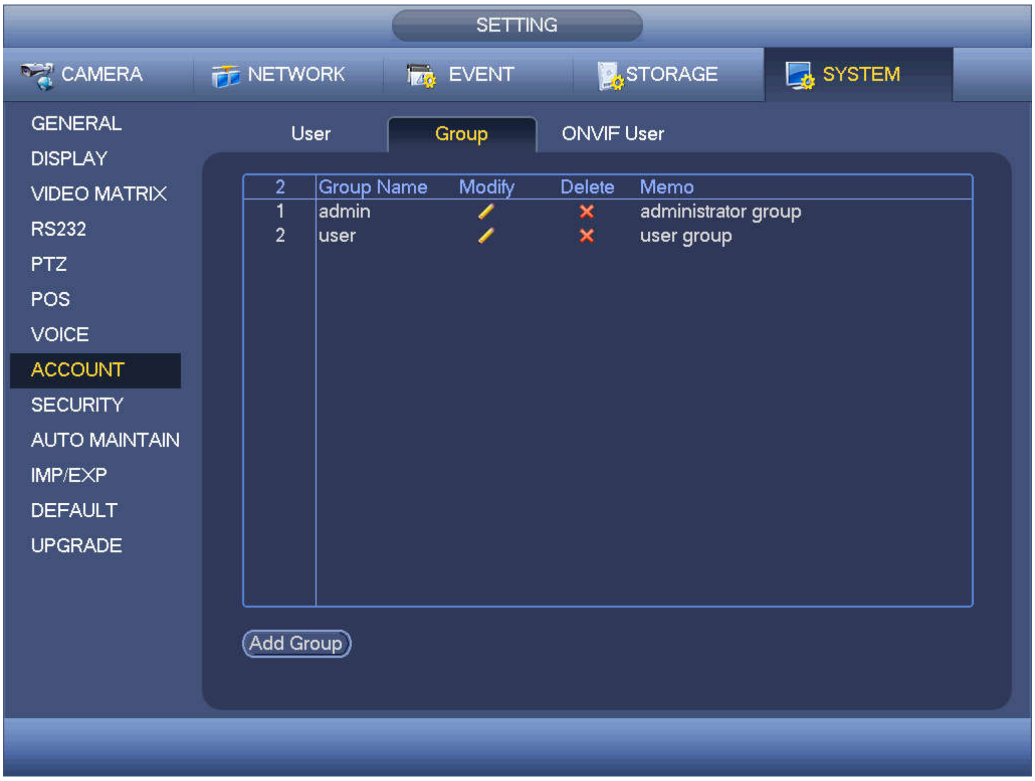
WARNING

STRONG PASSWORD RECOMMENDED-For your device own safety, please create a strong password of your own choosing. We also recommend you change your password periodically especially in the high security system.

4.10.1.2 Modify Group

Step 1 From main menu->Setting->System->Account->Group.

Enter add group interface. See Figure 4-210.



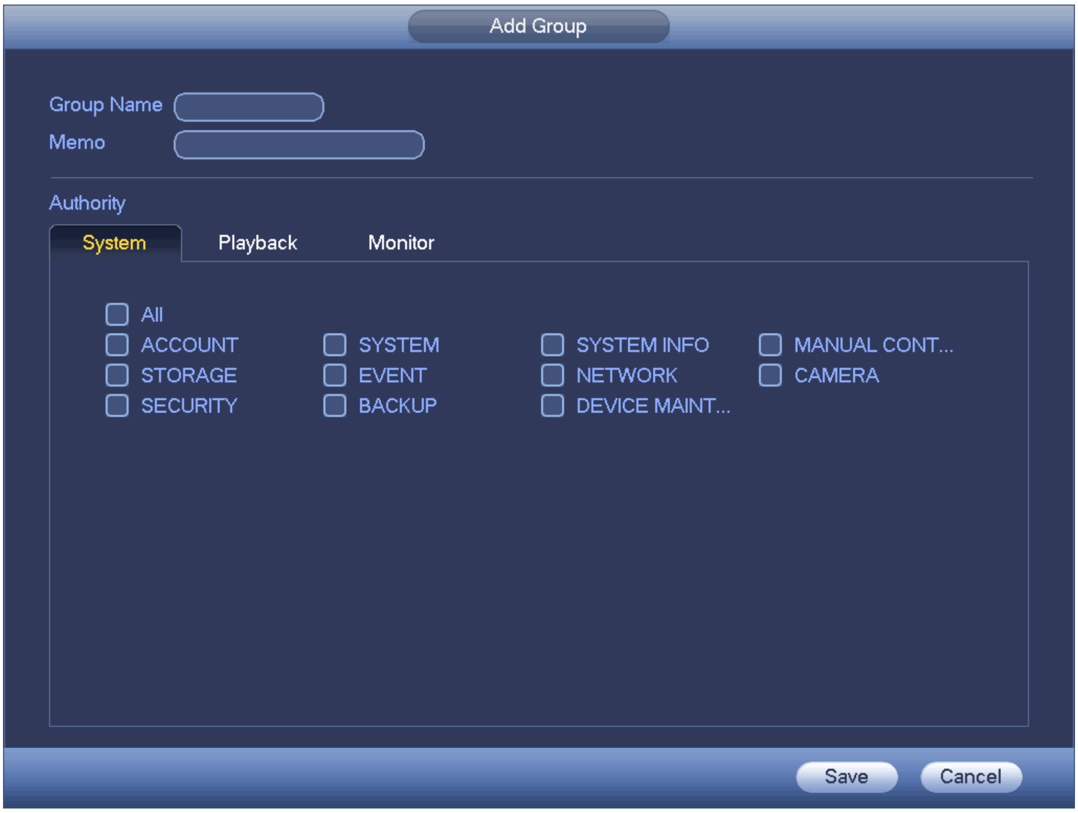
2	Group Name	Modify	Delete	Memo
1	admin	✎	✕	administrator group
2	user	✎	✕	user group

Figure 4-210

Step 2 Click add group button in Figure 4-210.

Enter Add group the interface. See Figure 4-211.

Step 3 Input group name and then input some memo information if necessary. Check the box to select authorities.



□ All
□ ACCOUNT □ SYSTEM □ SYSTEM INFO □ MANUAL CONT...
□ STORAGE □ EVENT □ NETWORK □ CAMERA
□ SECURITY □ BACKUP □ DEVICE MAINT...

Figure 4-211