Video Management Server
Web Client
User Manual

Manual Version: V1.04

Thank you for purchasing our product. If there are any questions, or requests, please do not hesitate to contact the dealer.

Notice

ⓘ **CAUTION!**

The default password is intended for your first login. For security, please change the password after your first login. You are recommended to set a strong password of no less than eight characters comprising at least three elements of the following four: digits, upper case letters, lower case letters and special characters. Please keep the password safe and change it regularly.

For security reasons, access from Internet with a weak password will be denied until it is changed to a strong one.

- The contents of this document are subject to change without prior notice. Updates will be added to the new version of this manual. We will readily improve or update the products or procedures described in the manual.
- Best effort has been made to verify the integrity and correctness of the contents in this document, but no statement, information, or recommendation in this manual shall constitute formal guarantee of any kind, expressed or implied. We shall not be held responsible for any technical or typographical errors in this manual.
- The illustrations in this manual are for reference only and may vary depending on the version or model.
- This manual is a guide for multiple product models and so it is not intended for any specific product.
- Due to uncertainties such as physical environment, discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.
- Use of this document and the subsequent results shall be entirely on the user's own responsibility.

Symbols

Symbol	Description
⚠ **WARNING!**	Contains important safety instructions and indicates situations that could cause bodily injury.
ⓘ **CAUTION!**	Means reader be careful and improper operations may cause damage or malfunction to product.
📝 **NOTE!**	Means useful or supplemental information about the use of product.

Contents

1 Overview

This manual describes how to manage and configure on the local Web client.

2 Basic Configuration

Organization Management

Create organizations and allocate resources (such as devices and channels) to different organizations for efficient management. Organizations are presented in a tree structure called organization tree. The root organization (root) is created by default, under which users may create other organizations.

Organization management includes:

- General organization: One device (such as an IPC or NVR) belongs to only one general organization; and all IPCs under the same NVR may only belong to the same organization.
- Custom organization: Provides a flexible way to manage devices. See Custom Organization.

General Organization

Basic > **Organization** > **General**

Click **Add** to create a general organization.

1. Enter a name and select a parent organization (by default is **root**).
2. Click **OK**.
3. The new organization appears on the organization tree on the left and the list on the right. It also appears in the organization name drop-down list that you can select when adding or editing a device.
4. In the organization list, click ✎ or 🗑 to edit or delete an organization.

NOTE!

- The root organization cannot be deleted.
- An organization cannot be deleted if it contains any organizations or resources (device or channel).

Custom Organization

Basic > **Organization** > **Custom**

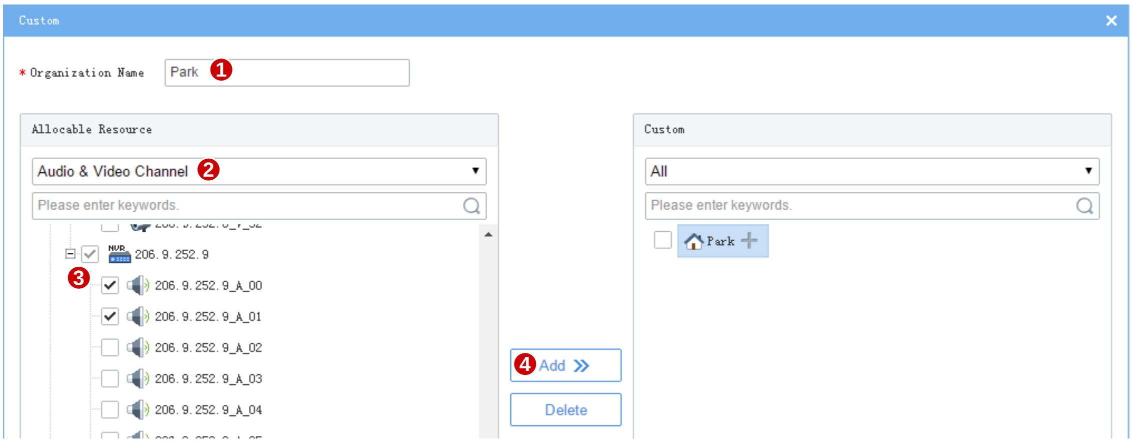
Custom organization provides a flexible way to manage devices and allows you to:

- Assign cameras under an NVR to different organizations.
- Assign cameras under different NVRs to one organization.
- Assign a camera to different organizations at the same time.

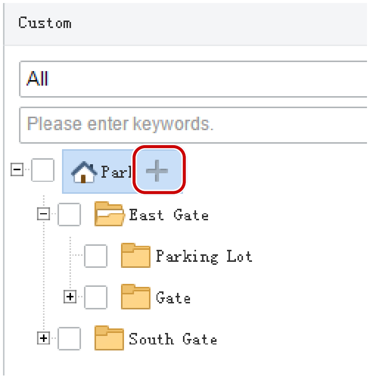
- Assign a custom organization to a role, so that users with this role can access certain resources on the software client.
- Assign resources of different types (e.g., audio & video channel) to different organizations.

Click **Add** to create a custom organization:

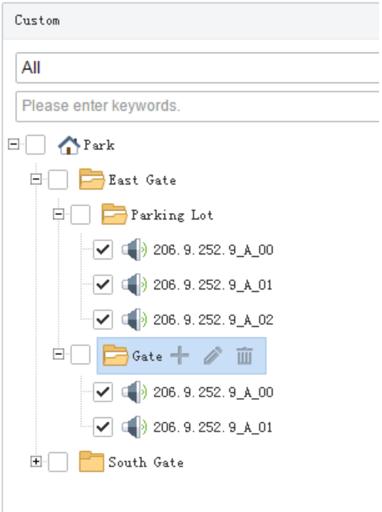
1. Enter a name. The organization name appears on the right.
2. (Optional) Select resource type (Audio & Video Channel). Enter keywords to filter if necessary.



3. To allocate resources to the root organization (e.g., park), select resources on the left, click the organization name on the right, and then click **Add**.
4. To add a new organization, click the add sign (+) and then enter a name in the field. The tree updates automatically. Add all the needed organizations in this way. Organizations can be edited or deleted.

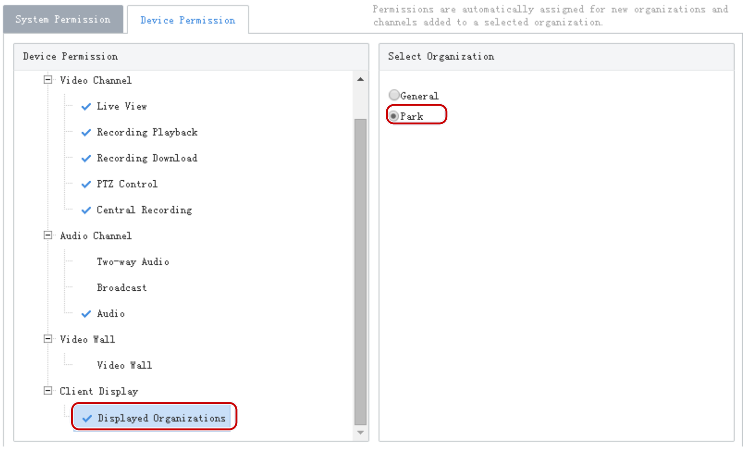


5. Click an organization on the right, select resources on the left, and then click **Add**. The selected resources are allocated to the organization. A resource can be allocated to multiple organizations (see figure below).



6. Click **OK**.

The new organization (e.g., Park) appears on the **Device Permission** tab (**Basic** > **User** > **Role**). If the organization is assigned to a role, users with this role can access resources in this organization.



Permissions are automatically assigned for new organizations and channels added to a selected organization.

NOTE!

- System permissions include operation permissions on the software client and management permissions on the Web client. The actual operation permissions depend on the selected operation permissions and the organization selected for **Displayed Organization**.
- For users with multiple roles, custom organizations assigned to these roles are displayed in resource lists of Live View, Playback, Sequence, View, Audio, Video Wall, and People Counting modules on the software client simultaneously.

User Management

Configure roles, assign permissions, and control user permissions by assigning roles. A role can be assigned to multiple users, and a user may have up to 16 roles.

Role

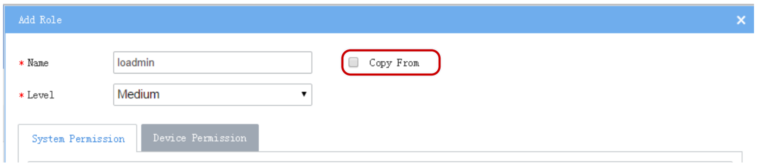
Basic > **User** > **Role**

Roles are used to limit user's permissions, including:

- **System Permission**: including operation permission (on software client) and management permissions (on Web client).
- **Device Permission**: Permission to access functions when using a device. You need to select permissions and specify allowed organizations or channels.
- **Level**: Used to differentiate priority when two users with the same system and device permissions are operating PTZ function at the same time.

Click **Add** to add a new role:

1. Enter the role name.
2. Select a level.
3. (Optional) Select **Copy From**. The existing roles in the system are listed. Select a role and then edit permissions for the new role based on the selected role. Permissions of the selected role will not change.



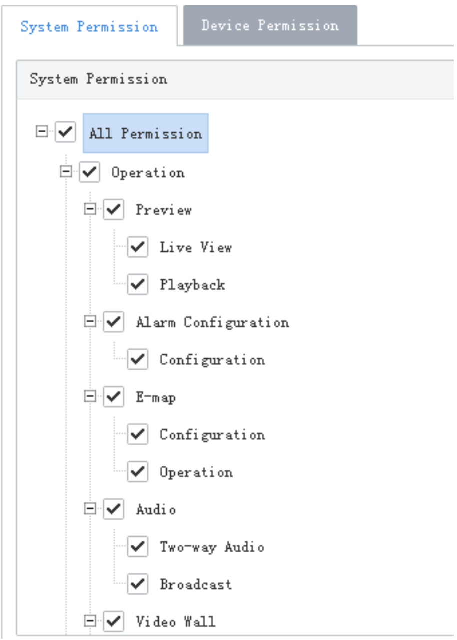
Add Role

* Name loadmin

* Level Medium

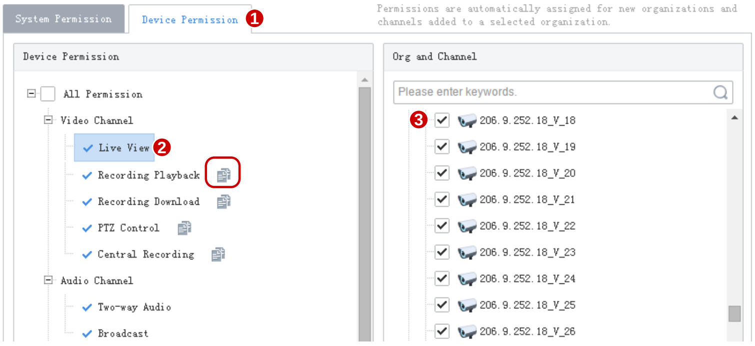
□ Copy From

4. On the **System Permission** tab, select permission to assign. For example, to assign live video and playback permissions, select **Preview** under **Operation**. **Live View** and **Playback** are selected automatically. To assign all permissions, select **All Permission**.



- ☑ All Permission
  - ☑ Operation
    - ☑ Preview
      - ☑ Live View
      - ☑ Playback
    - ☑ Alarm Configuration
      - ☑ Configuration
    - ☑ E-map
      - ☑ Configuration
      - ☑ Operation
    - ☑ Audio
      - ☑ Two-way Audio
      - ☑ Broadcast
    - ☑ Video Wall

5. Click **Device Permission** to assign device permissions: first click a permission on the left and then select channel(s) on the right.



Permissions are automatically assigned for new organizations and channels added to a selected organization.

TIP!

- After selecting a permission on the left (e.g., Live View), you also need to select camera(s) in the **Org and Channel** area on the right. By selecting a camera it means that the role will have **Live View** permission to this camera.
- Selecting **All Permission** will select all permissions and all channels. Selecting **root** will select all the listed channels.
- Clicking 🗐 copies permissions of the selected node (e.g., **Live View**) to the target node (e.g., **Recording Playback**). For example, to select the same channels for **Recording Playback** as **Live View**, click **Live View** first and then click 🗐 right to **Recording Playback**. Channels selected for **Live View** will be automatically selected for **Recording Playback**.
- The ✓ symbol that appears to the left of a permission (e.g., **Live View**) means channels have been selected for the permission.
- Click **Display Organizations** under the **Client Display** node to display all the organizations in the system on the right, including general and custom organizations. Select an organization as needed. For more information, see Custom Organization.

6. (Optional) Enter a description of the role.
7. Click **OK**.
8. The new role appears in the role list.

User

Basic > **User** > **User**

Add, edit or delete users. Control user permissions by specifying roles. Lock a user to deny login.

NOTE!

The admin user cannot be edited, deleted or locked.

Click **Add** to add a user. Some important parameters are described as follows:

- Username: Must be unique in the system and cannot change once set.
- Role: Up to 16 roles are allowed for a user. The user will have all the permissions included in the roles assigned.
- Password: Used to access the system.

- Valid Date: Specify the period during which the user have access to the system.
- Time Template: See User Time Template.
- Click to expand and enter more details.

Use buttons in the **Operation** column to manage existing users.

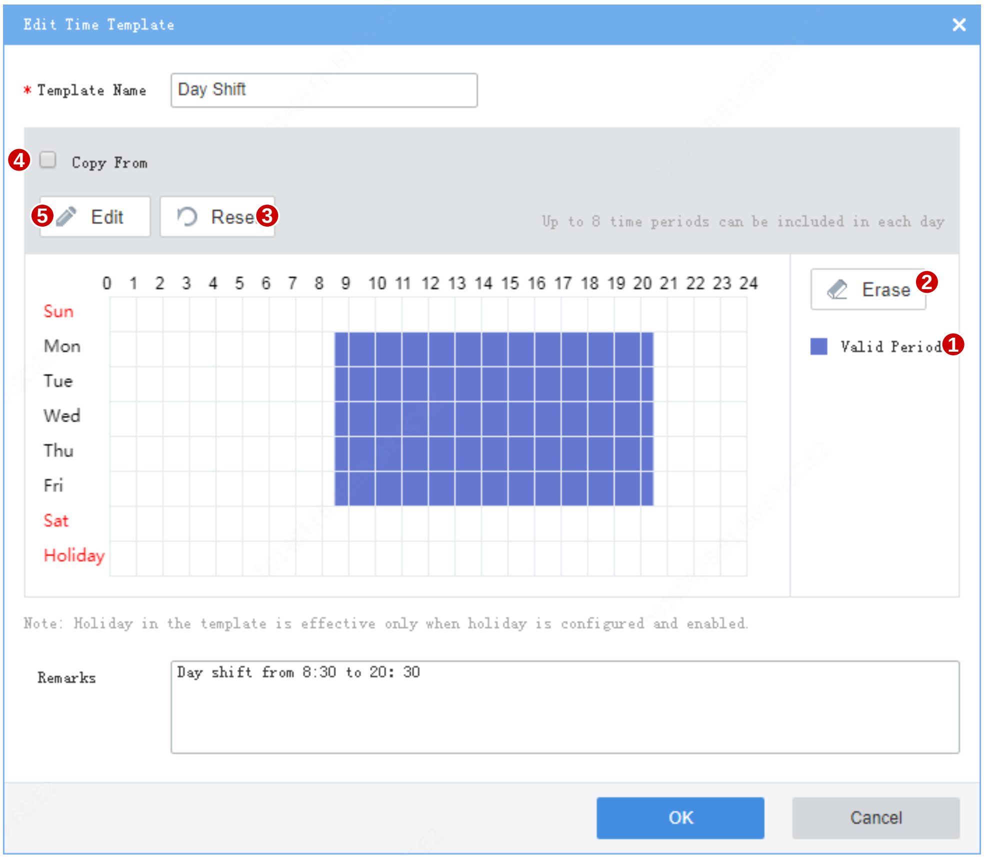
- Click to change roles, valid date and time template.
- Click to change the user's password. The new password takes effect at the user's next login. Only admin can change other users' passwords.
- Click to delete a user. A user who is logged in will be forced out of the system when deleted.

User Time Template

Basic > **User** > **User Time Template**

Use a user time template to restrict the time when a user can access the system. First you need to configure a time template, and then select it when you add or edit a user. Then the user can access the system only during the time set in the time template.

All-day is the default template in the system which can be edited but cannot be deleted. Using this template means there are no restrictions on login time.



Edit Time Template

* Template Name: Day Shift

□ Copy From

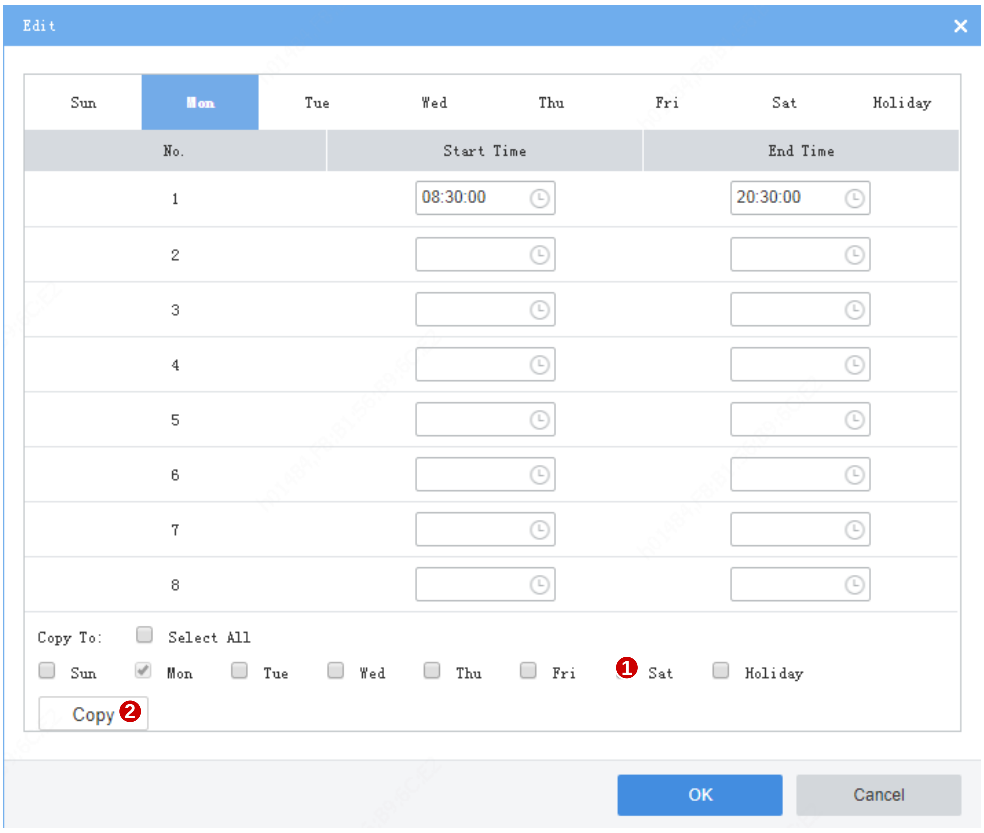
Up to 8 time periods can be included in each day

Note: Holiday in the template is effective only when holiday is configured and enabled.

Remarks: Day shift from 8:30 to 20: 30

Draw a user time template:

- Click **Valid Period** (1), and then click or drag on the calendar. Purple means time when login is allowed.
- To erase, click **Erase** (2), and then click or drag on the calendar. Purple changes to white, meaning login during this time is not allowed.
- To erase all, click **Reset** (3).
- To edit based on an existing template, select **Copy From** (4) and then select from the drop-down list.
- To set a complex time template, click **Edit** (5). Up to 8 periods are allowed each day.
- To apply the same settings to another day (e.g., Saturday), select the check box (1) and then click **Copy** (2).



No.	Start Time	End Time
1	08:30:00	20:30:00
2		
3		
4		
5		
6		
7		
8		

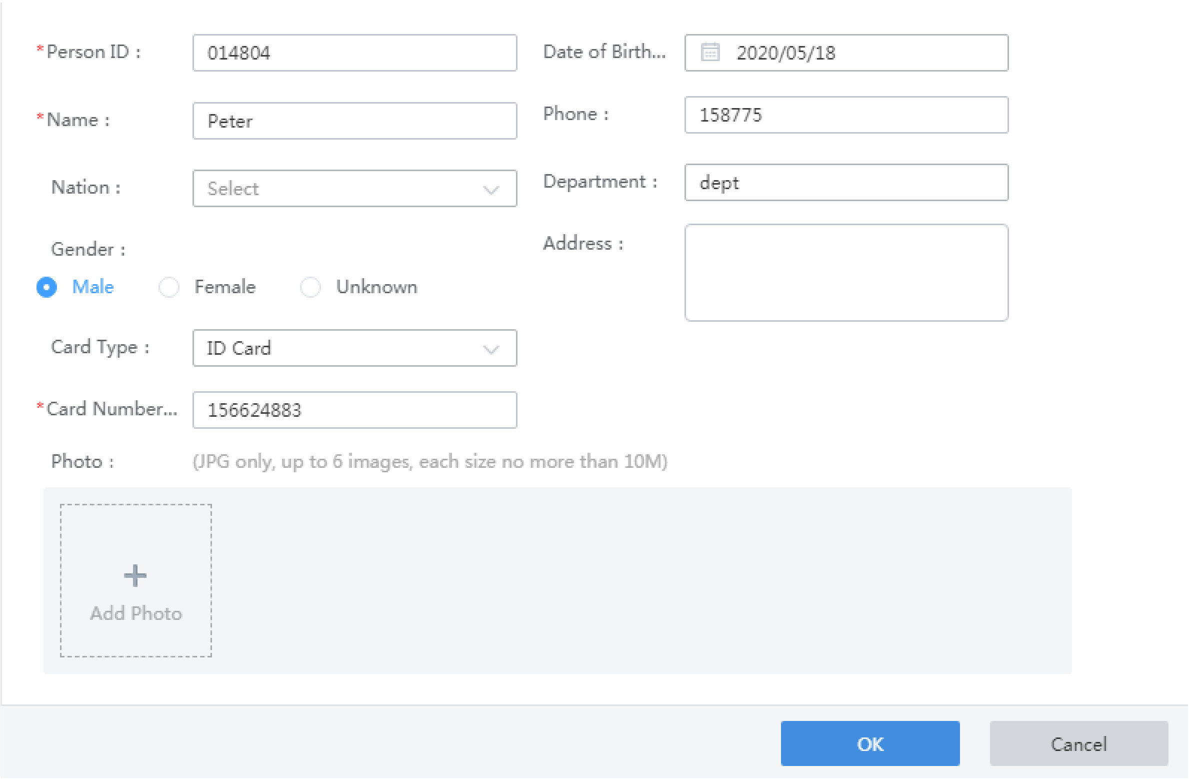
Copy To: □ Select All

□ Sun ☑ Mon □ Tue □ Wed □ Thu □ Fri 1 Sat □ Holiday

Person Management

Basic > **Person**

Click **Add** to add the basic information about a person.



*Person ID : 014804

Date of Birth... 2020/05/18

*Name : Peter

Phone : 158775

Nation : Select

Department : dept

Gender : ● Male ○ Female ○ Unknown

Address :

Card Type : ID Card

*Card Number... 156624883

Photo : (JPG only, up to 6 images, each size no more than 10M)

Device Management

Encoding Device

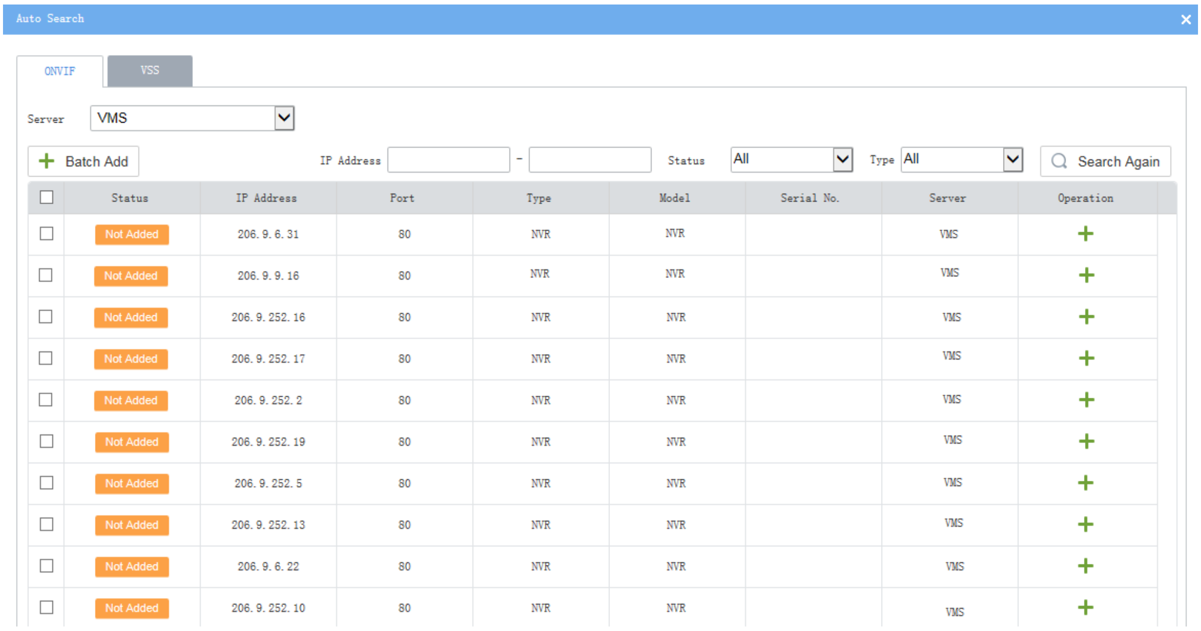
Basic > **Device** > **Device > Encoding Device**

Encoding devices include IPC, NVR and encoder.

NOTE!

- To add a device with a known IP or domain name, click the **Add** button. The steps below describe how to search and discover devices on the same subnet as the VMS.
- To add an IPC or NVR for live view using RTSP, click **Add**, and select **Custom** from the **Protocol** drop-down list. For detailed steps, see Appendix A Add a Device Using RTSP.

1. Click **Auto Search**. Encoding devices on the same subnet with the VMS are discovered.



Server: VMS

IP Address: -

Status: All

Type: All

□	Status	IP Address	Port	Type	Model	Serial No.	Server	Operation
□	Not Added	206.9.6.31	80	NVR	NVR		VMS	+
□	Not Added	206.9.9.16	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.16	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.17	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.2	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.19	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.5	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.13	80	NVR	NVR		VMS	+
□	Not Added	206.9.6.22	80	NVR	NVR		VMS	+
□	Not Added	206.9.252.10	80	NVR	NVR		VMS	+

2. To add a device, click + for the device in the **Operation** column. To add multiple devices with the same configurations including server, protocol, organization, and username/password, select checkboxes for these devices and click **Batch Add**.
3. You may search again using the following conditions:

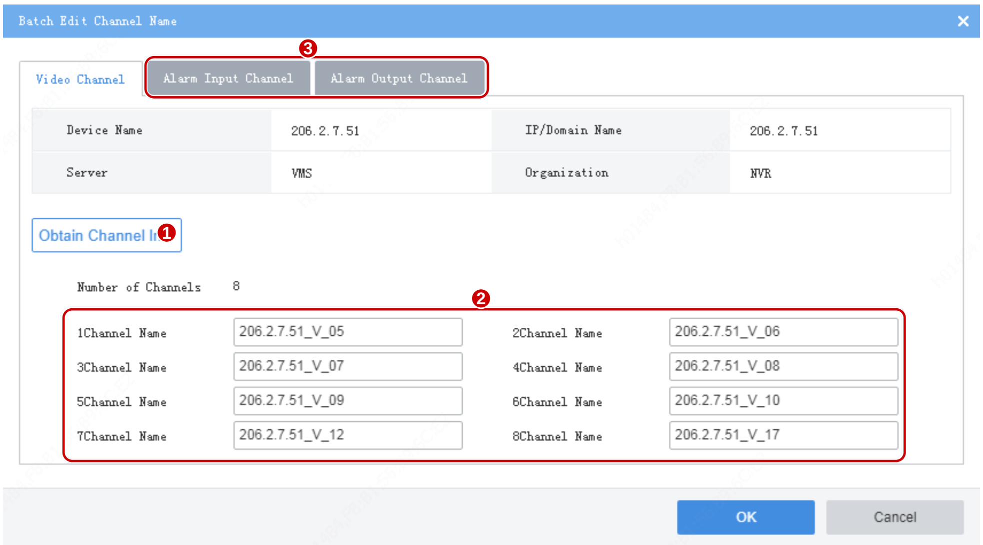
- **Server**: Search devices under the specified server.
- **IP**: Search devices within the specified IP range.
- Filter devices by status (added or not) and type (IPC, NVR).
- Click the **VSS** tab to search for VSS devices only. You need to complete VSS configuration first.

4. Check device status.

Tip!

If the device status is **Offline - Incorrect username/password**, click ✎ and enter the correct password. The device cannot get online unless the entered password is correct.

5. Click 🗎 for a device (e.g., an NVR) in the **Operation** column. A window as shown below appears. You can click **Obtain Channel Info** (1) to get channel information from the device, or rename the channels (2) on the VMS, or view alarm input or output channels of the device (3). Renaming channels does not change the channel names saved on the device (e.g., NVR).



Batch Edit Channel Name

Device Name	206.2.7.51	IP/Domain Name	206.2.7.51
Server	VMS	Organization	NVR

Number of Channels 8

1Channel Name	206.2.7.51_V_05	2Channel Name	206.2.7.51_V_06
3Channel Name	206.2.7.51_V_07	4Channel Name	206.2.7.51_V_08
5Channel Name	206.2.7.51_V_09	6Channel Name	206.2.7.51_V_10
7Channel Name	206.2.7.51_V_12	8Channel Name	206.2.7.51_V_17

6. To sync channel info (channel name) from devices to the VMS (for example, after channel names are changed on the NVR), select the device(s) and then click the **Sync Channel Info** button on the top of the device list. You can view the updated channel info at **Basic** > **Device** > **Channel**.

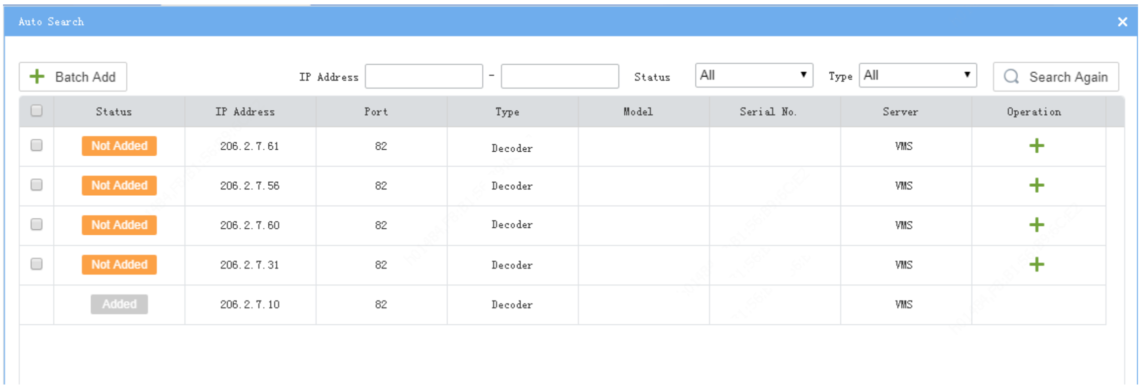
Decoding Device

Basic > **Device** > **Device > Decoder**

NOTE!

To add a device with a known IP or domain name, click the **Add** button. The following steps describe how to search and discover devices on the same subnet as the VMS.

1. Click **Auto Search**. Decoding devices on the same subnet with the VMS are discovered.



Auto Search

□	Status	IP Address	Port	Type	Model	Serial No.	Server	Operation
□	Not Added	206.2.7.61	82	Decoder			VMS	+
□	Not Added	206.2.7.56	82	Decoder			VMS	+
□	Not Added	206.2.7.60	82	Decoder			VMS	+
□	Not Added	206.2.7.31	82	Decoder			VMS	+
	Added	206.2.7.10	82	Decoder			VMS	

2. Click + for the device to add. To add devices with the same configurations (protocol, organization, username/password), select checkboxes for the devices and then click **Batch Add**.
3. You may set the following conditions and search again:

- **IP**: Search devices within the specified IP range.
- Filter devices by status (added or not) and type (decoder, DX).

4. Check device status.

Tip!

If the device status is **Offline - Incorrect username/password**, click ✎ and enter the correct password. The device cannot get online unless the entered password is correct.

Smart Device

Basic > **Device** > **Device > Smart Device**

Add smart devices to operate the Face Recognition, LPR and Mixed Traffic Detection modules on the software client.

1. Face recognition and LPR

Add smart IPC or NVR to operate the Face Recognition and LPR modules on the software client.

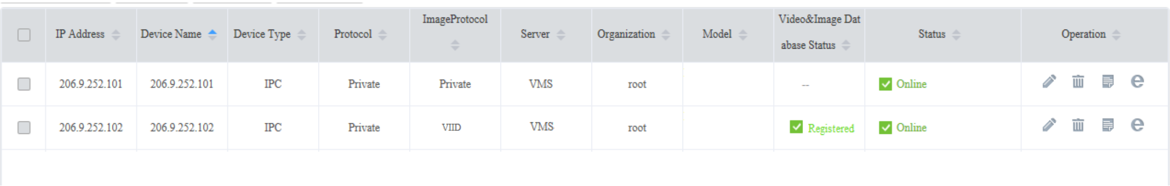
1. Click the **Auto Search** or **Add** button to add devices (see Encoding Device).

NOTE!

About setting the **Image Protocol** parameter:

- For an LPR camera or an NVR, select **VIID**. You need to complete VIID configuration on the device (see Video&Image Database), including the server IP (VMS' IP address), server port (5073), communication type (Video&Image Database) and username/password.
- For face recognition cameras, select **VIID** if it is a third-party camera; for Uniview cameras, choose **Private** or **VIID** as needed. **VIID** supports the capture and upload of face images, and **Private** supports more, such as face monitoring, face match/not match alarms, and structured data upload.

2. Check whether the device status is **Online**; if the image protocol is **VIID** and the device is registered successfully, **Registered** is displayed.



□	IP Address	Device Name	Device Type	Protocol	ImageProtocol	Server	Organization	Model	Video&Image Database Status	Status	Operation
□	206.9.252.101	206.9.252.101	IPC	Private	Private	VMS	root		--	✓ Online	✎ 🗑 ▤ e
□	206.9.252.102	206.9.252.102	IPC	Private	VIID	VMS	root		✓ Registered	✓ Online	✎ 🗑 ▤ e

2. Mixed traffic detection

Add smart devices to operate the Mixed Traffic Detection module on the software client.

1. First complete configurations on the camera's Web client, including enabling mixed traffic detection and specifying the type of objects to capture (motor vehicle, non-motor vehicle, or pedestrian).
2. Click the **Auto Search** or **Add** button to add devices (see Encoding Device).

NOTE!

Choose **Private** as the **Image Protocol** when you add the device.

Network Keyboard

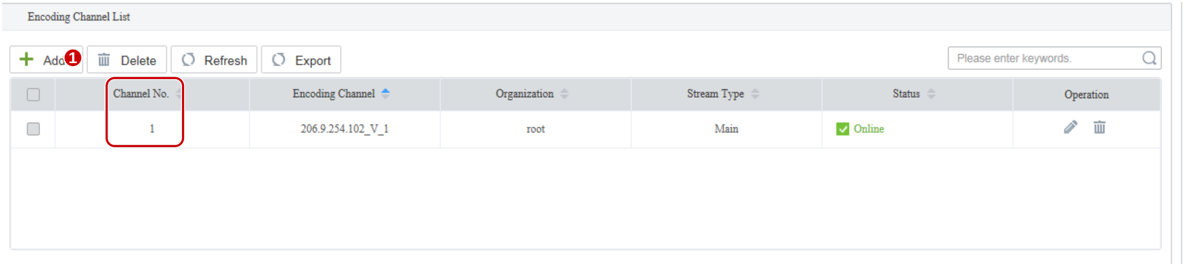
Basic > **Device** > **Device > Network Keyboard**

Add a network keyboard to use with a video wall to split windows, zoom in or out, adjust focus, and control the PTZ.

NOTE!

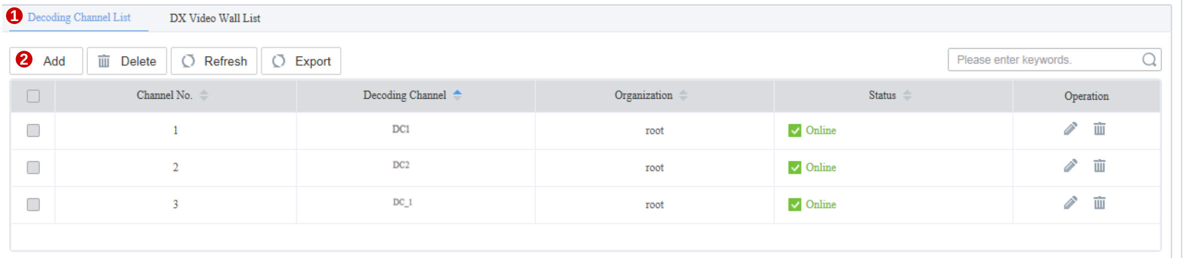
First refer to the Network Keyboard User Manual to set up the keyboard, including its registration with the VMS (by inputting the VMS' IP/port on the keyboard). And then follow the steps below to specify the video channel(s), decoding channel(s) or video wall(s) that you want to control using the keyboard.

1. Add video channels (cameras). Each video channel is assigned a channel number (e.g., 1).



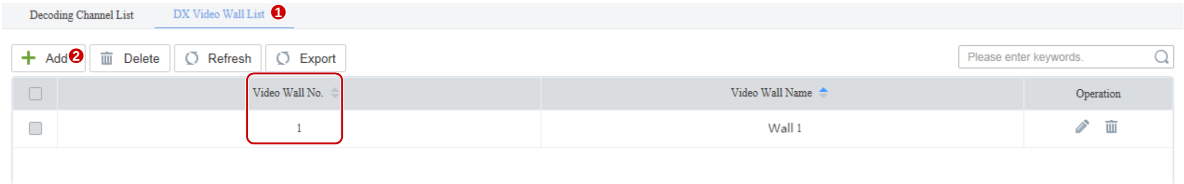
□	Channel No.	Encoding Channel	Organization	Stream Type	Status	Operation
□	1	206.9.254.102_V_1	root	Main	☑ Online	

2. To use the keyboard with a DC video wall, add decoding channels on the **Decoding Channel List** tab. Each decoding channel is assigned a channel number (e.g., 1, 2, 3).



□	Channel No.	Decoding Channel	Organization	Status	Operation
□	1	DC1	root	☑ Online	
□	2	DC2	root	☑ Online	
□	3	DC_1	root	☑ Online	

3. To use the keyboard with a DX video wall, add video wall(s) on the **DX Video Wall List** tab. Each video wall is assigned a video wall number (e.g., 1).



□	Video Wall No.	Video Wall Name	Operation
□	1	Wall 1	

4. After the above steps are completed, you can start video on the video wall by entering the assigned channel numbers and video wall number on the keyboard.

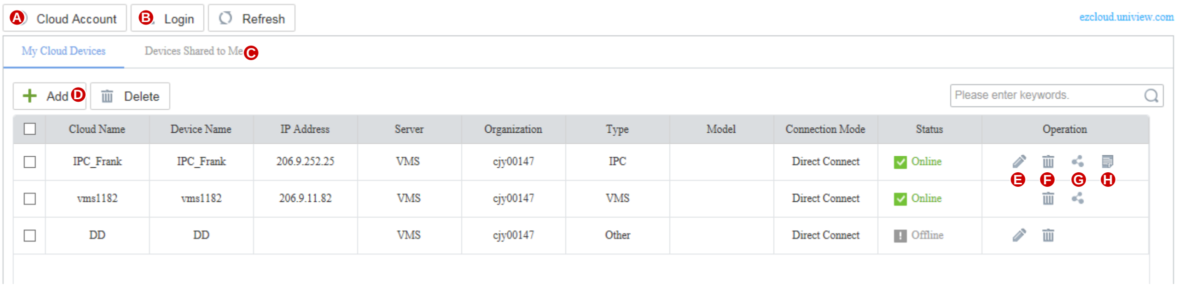
Cloud Device

Basic > **Device** > **Device** > **Cloud Device**

This function is mainly used to connect IPCs and NVRs to the VMS over the Internet. First register the IPCs and NVRs that support EZCloud to a cloud account, and then log in to the cloud account on the VMS to manage the registered IPCs and NVRs.

NOTE!

If an NVR has been added on the VMS via the Private, Onvif or VSS protocol, it is **NOT** recommended to add the NVR to the VMS again as a cloud device. This application may cause undesired service exceptions for certain NVR models.



☐	Cloud Name	Device Name	IP Address	Server	Organization	Type	Model	Connection Mode	Status	Operation
☐	IPC_Frank	IPC_Frank	206.9.252.25	VMS	cjy00147	IPC		Direct Connect	☑ Online	
☐	vms1182	vms1182	206.9.11.82	VMS	cjy00147	VMS		Direct Connect	☑ Online	
☐	DD	DD		VMS	cjy00147	Other		Direct Connect	! Offline	

Purpose	Description
Log in to a cloud account (B)	Enter your cloud account info to log in. When login succeeds, the cloud account appears on the tree on the left, and the existing devices under the cloud account are listed on the right. Login to multiple cloud accounts is allowed. You can click a cloud account on the tree to view devices under this account.
Manage cloud accounts (A)	Manage cloud accounts on the VMS. You can refresh the status, log out of a cloud account, view shared devices, and cancel sharings.
Add cloud device (D)	Add devices to specified online account(s). The device name and register code are required. The added devices are listed on the **My Cloud Devices** tab and are displayed as **Online** if they are successfully logged in. VMS cannot be added here.
Edit cloud device (E)	Rename a device. If the **Sync to Cloud** checkbox is selected, the new device name will be synced to cloud; otherwise, only the name saved on the VMS is changed.
Delete cloud device (F)	Delete a device from a cloud account.
Share cloud device (G)	Share device(s) with other cloud account(s). You need to specify a valid period for the sharing and assign permissions by selecting an existing user created on the device to share.
View cloud devices shared from other cloud accounts (C)	View device(s) shared with you from other cloud account(s). You can stop a sharing proactively.
Obtain channel info (H)	Obtain channel info of a cloud device, edit channel names.

Access Controller

Basic > **Device** > **Device** > **Access Controller**

Add and manage Uniview turnstiles or face recognition access controllers to operate the Access Control module on the software client.

NOTE!

For third-party access controllers, please add or manage at **Basic** > **Device** > **Device** > **Access Control**.

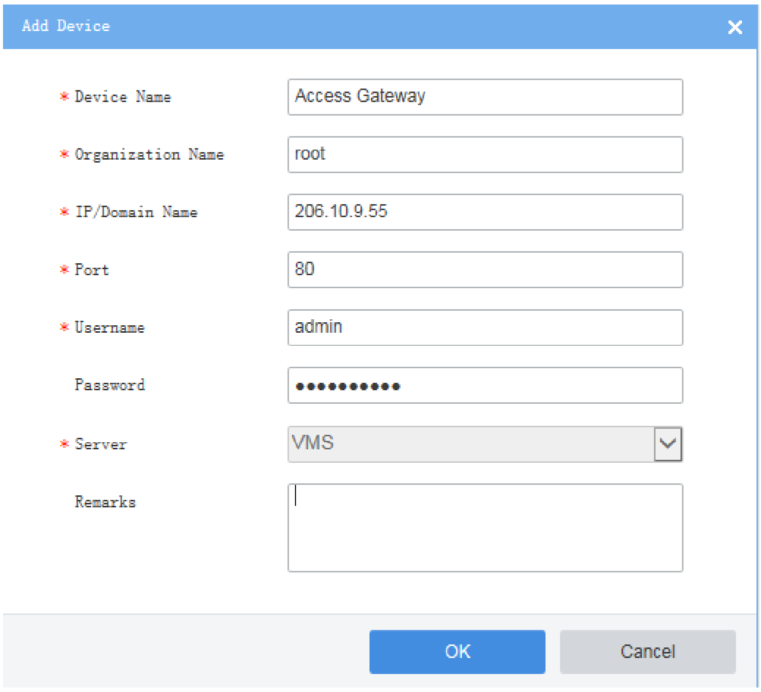
1. Click the **Auto Search** or **Add** button to add devices (see Encoding Device).
2. Make sure you select the correct access control type and set the correct IP/port.
3. Check whether the device status is **Online**. A door channel is added automatically if the added access controller is online.

Access Gateway

Basic > **Device** > **Device** > **Access Gateway**

Add an access gateway (EZAgent) so the VMS can receive alarms from alarm control panels and door access controllers, and users can arm/disarm zones, bypass/unbypass partitions, and open/close doors on the software client. See EZAgent User Manual for more information about the access gateway.

1. Click **Add**.



Add Device

* Device Name	Access Gateway
* Organization Name	root
* IP/Domain Name	206.10.9.55
* Port	80
* Username	admin
Password	●●●●●●●●●●
* Server	VMS
Remarks	

2. Complete settings in the dialog box.

NOTE!

- The **IP/Domain Name** is the IP address or domain name of the PC that hosts the EZAgent server.
- The **Password** is the password of the EZAgent server.

3. The added access gateway is displayed as **Online** if it is connected, and the alarm controllers, access controllers and their channels are displayed on the VMS.

NOTE!

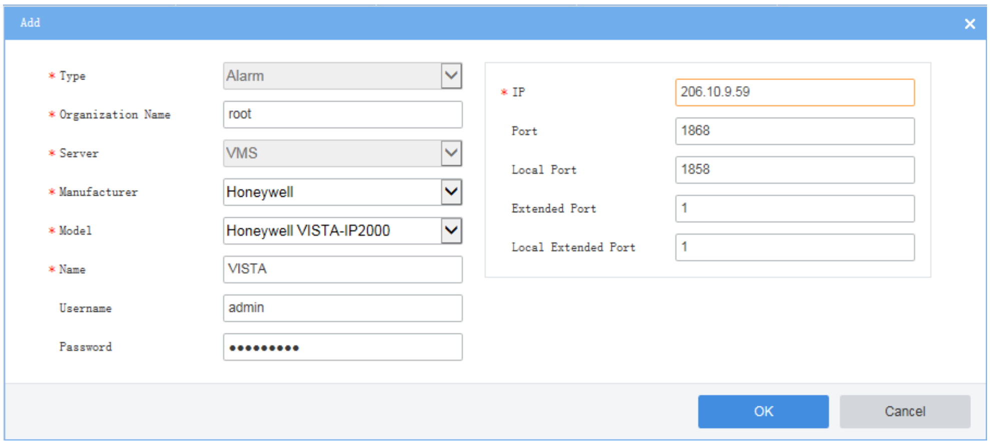
For alarm controllers and access controllers that are connected to the VMS via gateway, you cannot add their channels directly on the VMS' Web client; they can only be added on the EZAgent.

Alarm Control

Basic > **Device** > **Device** > **Alarm Control**

Add an alarm controller, so the VMS can receive alarms from it, and users can arm/disarm zones and bypass/unbypass partitions on the software client.

1. Click **Add**.
2. Choose the manufacturer and model and then complete the required settings.



* Type	Alarm
* Organization Name	root
* Server	VMS
* Manufacturer	Honeywell
* Model	Honeywell VISTA-IP2000
* Name	VISTA
Username	admin
Password	•••••••••

* IP	206.10.9.59
Port	1868
Local Port	1858
Extended Port	1
Local Extended Port	1

NOTE!

- Depending on the alarm controller, the **IP** may be that of the alarm controller or the PC where its management platform is installed.
- The username and password are required if users want to arm/disarm or bypass/unbypass on the software client.

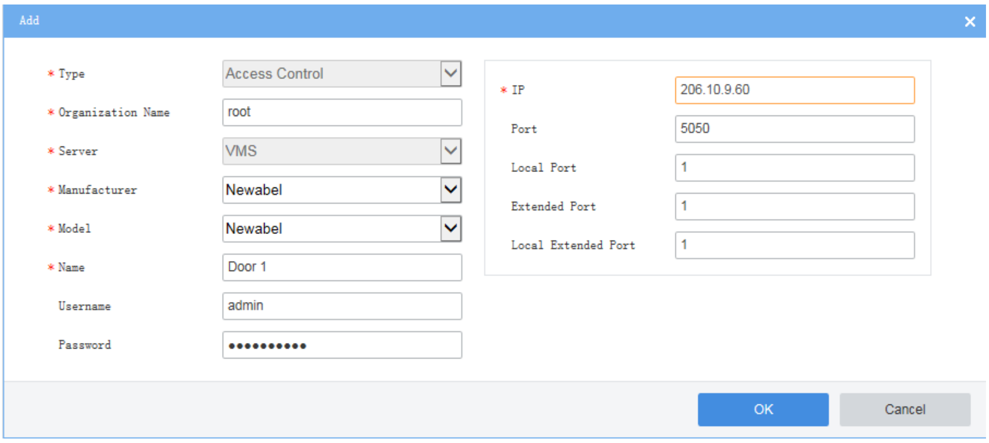
3. The added alarm controller is displayed as **Online** if it is connected.

Access Control

Basic > **Device** > **Device** > **Access Control**

Add an access controller, so the VMS can receive alarms from them, and users can open or close doors on the software client.

1. Click **Add**.
2. Choose the manufacturer and model and then complete the required settings.



* Type	Access Control
* Organization Name	root
* Server	VMS
* Manufacturer	Newabel
* Model	Newabel
* Name	Door 1
Username	admin
Password	••••••••••

* IP	206.10.9.60
Port	5050
Local Port	1
Extended Port	1
Local Extended Port	1

NOTE!

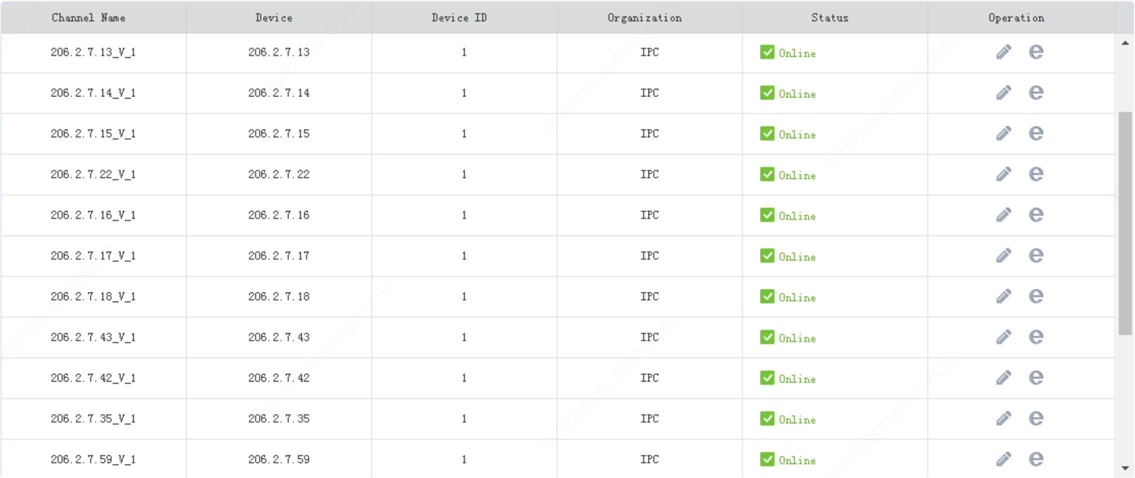
- Depending on the access controller, the **IP** may be that of the access controller or the PC where its management platform is installed.
- The username and password are required if users want to open or close doors on the software client.

3. The added access controller is displayed as **Online** if it is connected.

Encoding Channel

Basic > **Device** > **Channel > Encoding Channel**

View channel status, edit channel names, or open the Web page of the encoding device.

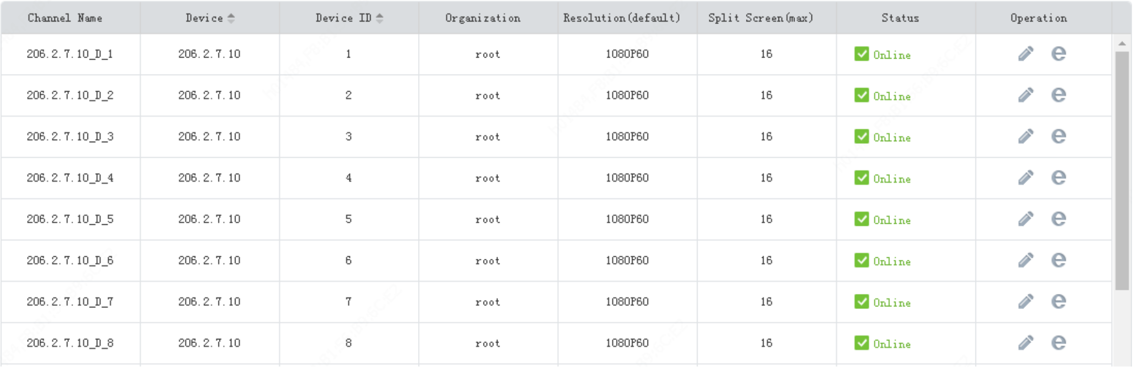


Channel Name	Device	Device ID	Organization	Status	Operation
206.2.7.13_V_1	206.2.7.13	1	IPC	✓ Online	✎ e
206.2.7.14_V_1	206.2.7.14	1	IPC	✓ Online	✎ e
206.2.7.15_V_1	206.2.7.15	1	IPC	✓ Online	✎ e
206.2.7.22_V_1	206.2.7.22	1	IPC	✓ Online	✎ e
206.2.7.16_V_1	206.2.7.16	1	IPC	✓ Online	✎ e
206.2.7.17_V_1	206.2.7.17	1	IPC	✓ Online	✎ e
206.2.7.18_V_1	206.2.7.18	1	IPC	✓ Online	✎ e
206.2.7.43_V_1	206.2.7.43	1	IPC	✓ Online	✎ e
206.2.7.42_V_1	206.2.7.42	1	IPC	✓ Online	✎ e
206.2.7.35_V_1	206.2.7.35	1	IPC	✓ Online	✎ e
206.2.7.59_V_1	206.2.7.59	1	IPC	✓ Online	✎ e

Decoding Channel

Basic > **Device** > **Channel > Decoding Channel**

View channel status and capability, edit channel names, or open the Web page of the decoding device.



Channel Name	Device	Device ID	Organization	Resolution(default)	Split Screen(max)	Status	Operation
206.2.7.10_D_1	206.2.7.10	1	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_2	206.2.7.10	2	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_3	206.2.7.10	3	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_4	206.2.7.10	4	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_5	206.2.7.10	5	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_6	206.2.7.10	6	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_7	206.2.7.10	7	root	1080P60	16	✓ Online	✎ e
206.2.7.10_D_8	206.2.7.10	8	root	1080P60	16	✓ Online	✎ e

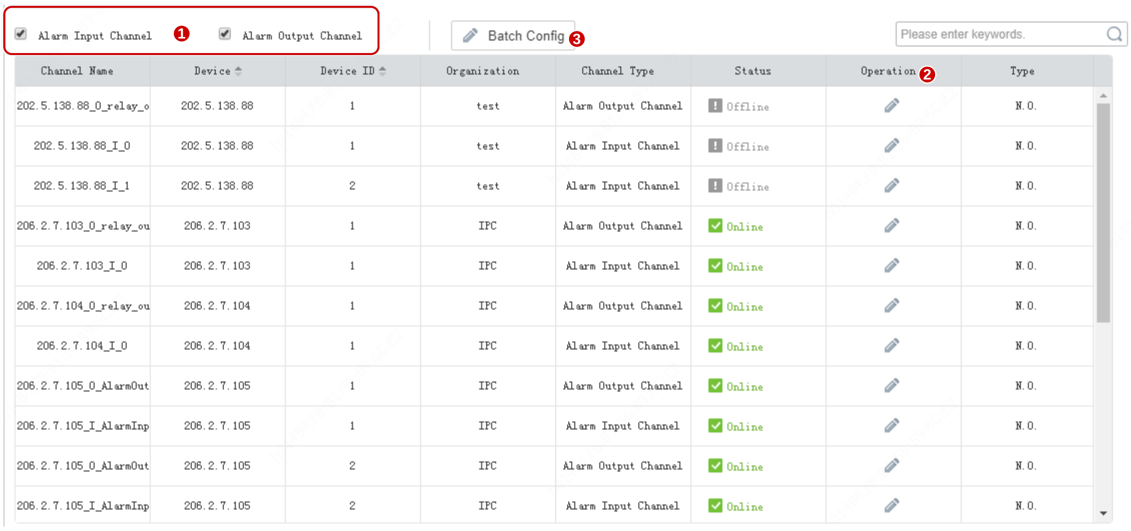
Alarm Channel

Basic > **Device** > **Channel > Alarm Channel**

View alarm input and output channels. You can select the checkbox(es) (1) to display the corresponding type(s) only.

Edit channel names or alarm types (N.O. or N.C.) in the **Operation** column (2). The alarm input channel can be enabled or disabled. For the alarm output channel, you can edit **Delay** to set the duration of the changed status before the default status is restored.

You can click the **Batch Config** button (3) to configure settings in batches.



Channel Name	Device	Device ID	Organization	Channel Type	Status	Operation	Type
202.5.138.88_O_relay_o	202.5.138.88	1	test	Alarm Output Channel	Offline	✎	N.O.
202.5.138.88_I_0	202.5.138.88	1	test	Alarm Input Channel	Offline	✎	N.O.
202.5.138.88_I_1	202.5.138.88	2	test	Alarm Input Channel	Offline	✎	N.O.
206.2.7.103_O_relay_ou	206.2.7.103	1	IPC	Alarm Output Channel	✓ Online	✎	N.O.
206.2.7.103_I_0	206.2.7.103	1	IPC	Alarm Input Channel	✓ Online	✎	N.O.
206.2.7.104_O_relay_ou	206.2.7.104	1	IPC	Alarm Output Channel	✓ Online	✎	N.O.
206.2.7.104_I_0	206.2.7.104	1	IPC	Alarm Input Channel	✓ Online	✎	N.O.
206.2.7.105_O_AlarmOut	206.2.7.105	1	IPC	Alarm Output Channel	✓ Online	✎	N.O.
206.2.7.105_I_AlarmInp	206.2.7.105	1	IPC	Alarm Input Channel	✓ Online	✎	N.O.
206.2.7.105_O_AlarmOut	206.2.7.105	2	IPC	Alarm Output Channel	✓ Online	✎	N.O.
206.2.7.105_I_AlarmInp	206.2.7.105	2	IPC	Alarm Input Channel	✓ Online	✎	N.O.

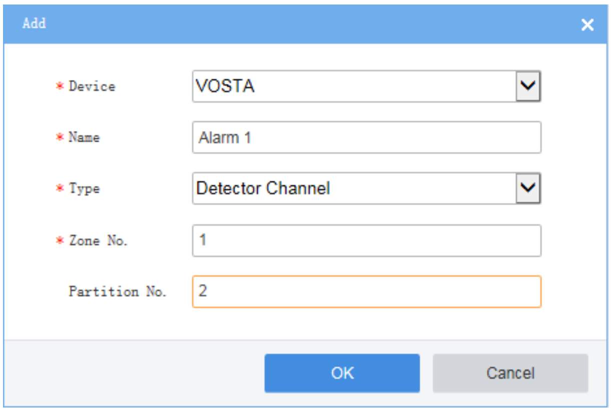
Tip!

N.O. means normally open, and N.C. means normally closed.

Detector Channel

Basic > **Device** > **Channel > Detector Channel**

Add detector channels, zones or partitions to an alarm control device on the VMS.

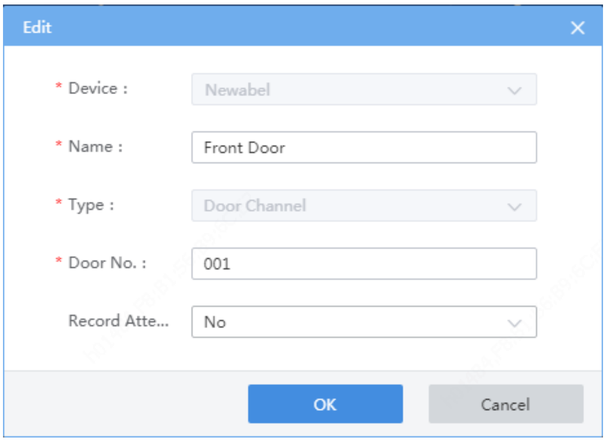


* Device	VOSTA
* Name	Alarm 1
* Type	Detector Channel
* Zone No.	1
Partition No.	2

Door Channel

Basic > **Device** > **Channel > Door Channel**

A door channel is automatically added when a Uniview access control device is added successfully. For third-party access controllers, door channels need to be added manually. You can edit a channel and use it to record attendance.



Edit

* Device : Newabel

* Name : Front Door

* Type : Door Channel

* Door No. : 001

Record Atte... No

External Alarm

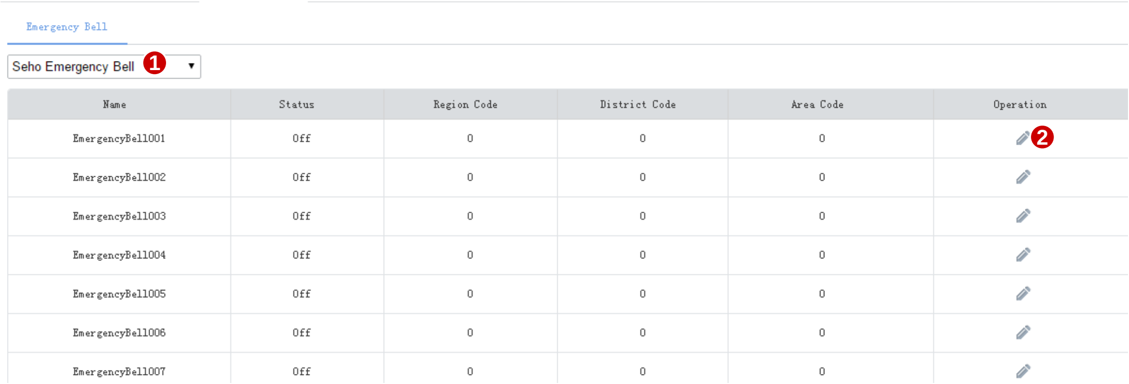
Basic > **Device** > **External Alarm**

Connect emergency bells to the VMS so that specified actions will be triggered on the VMS when an emergency bell alarm occurs. Actions include live view, preset (PTZ cameras), alarm output, alarm to video wall, buzzer or email.

NOTE!

First link the emergency bell to the VMS by setting the VMS' IP and port on the emergency bell. Two emergency bell types are supported (Seho and Hitec). For Seho, the port number is 25000, and for Hitec, the port number is 9010.

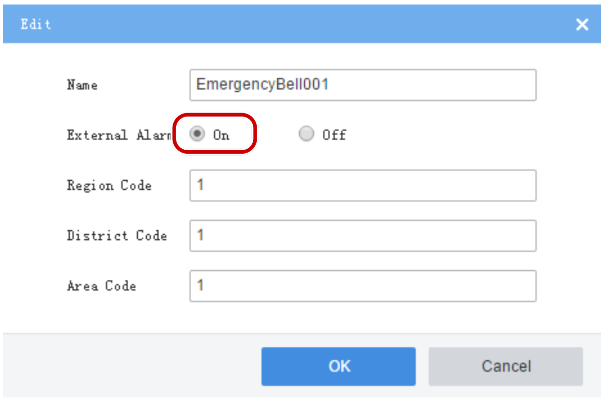
1. Select an emergency bell and then configure.



Seho Emergency Bell

Name	Status	Region Code	District Code	Area Code	Operation
EmergencyBell1001	Off	0	0	0	✎
EmergencyBell1002	Off	0	0	0	✎
EmergencyBell1003	Off	0	0	0	✎
EmergencyBell1004	Off	0	0	0	✎
EmergencyBell1005	Off	0	0	0	✎
EmergencyBell1006	Off	0	0	0	✎
EmergencyBell1007	Off	0	0	0	✎

2. Enable external alarm, and set the three codes properly. The VMS uses the combination to identify an emergency bell.


Edit

Name: EmergencyBell001

External Alarm: ● On ○ Off

Region Code: 1

District Code: 1

Area Code: 1

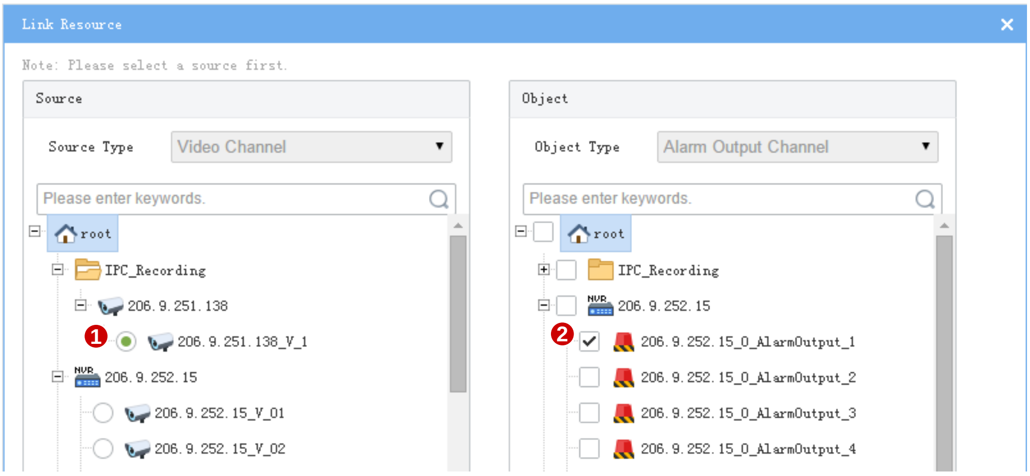
3. Configure actions to trigger at **Service** > **Alarm**.
4. Configure actions to trigger on the software client. See Alarm Configuration of the *Software Client User Manual*.

Link Resource

Basic > **Device** > **Link Resource**

Link a source (video channel) to an object (alarm output channel) so users can trigger alarm output manually on the software client.

1. Click **Allocate**. A dialog box appears.
2. Select the source on the left, and then select object(s) on the right. One source can link multiple objects. Click **OK**.


Link Resource

Note: Please select a source first.

Source

Source Type: Video Channel

Please enter keywords.

- root
  - IPC_Recording
    - 206.9.251.138
      - ● 206.9.251.138_V_1
  - 206.9.252.15
    - ○ 206.9.252.15_V_01
    - ○ 206.9.252.15_V_02

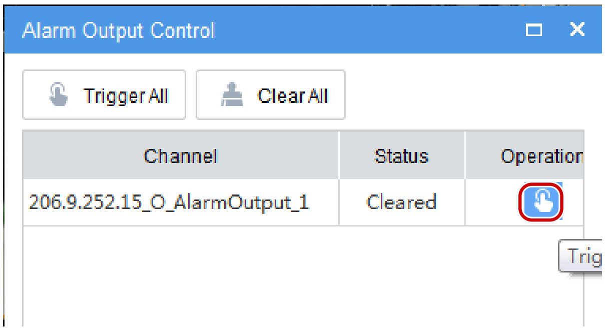
Object

Object Type: Alarm Output Channel

Please enter keywords.

- □ root
  - □ IPC_Recording
  - □ 206.9.252.15
    - ☑ 206.9.252.15_0_AlarmOutput_1
    - □ 206.9.252.15_0_AlarmOutput_2
    - □ 206.9.252.15_0_AlarmOutput_3
    - □ 206.9.252.15_0_AlarmOutput_4

3. When playing live video from the camera on the software client, you can click on the window toolbar to trigger the linked alarm device (e.g., alarm lamp) in the dialog box (see below).



Alarm Output Control

Trigger All | Clear All

Channel	Status	Operation
206.9.252.15_O_AlarmOutput_1	Cleared	

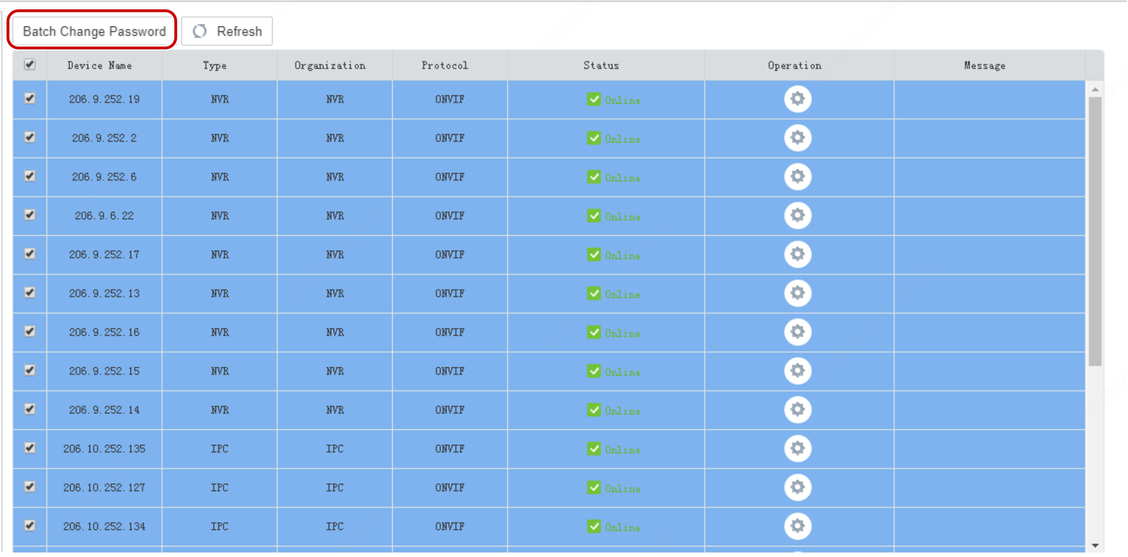
Batch Configuration

Batch Change Passwords

Basic > Batch Config > Batch Change Password

Batch change passwords of NVRs. This function is not available to VSS devices and cloud devices.

1. Select the organization on the left, and then select devices on the right. Click **Batch Change Password**.



Batch Change Password | Refresh

☑	Device Name	Type	Organization	Protocol	Status	Operation	Message
☑	206.9.252.19	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.2	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.6	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.6.22	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.17	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.13	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.16	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.15	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.9.252.14	NVR	NVR	ONVIF	✓ Online	⚙	
☑	206.10.252.135	IPC	IPC	ONVIF	✓ Online	⚙	
☑	206.10.252.127	IPC	IPC	ONVIF	✓ Online	⚙	
☑	206.10.252.134	IPC	IPC	ONVIF	✓ Online	⚙	

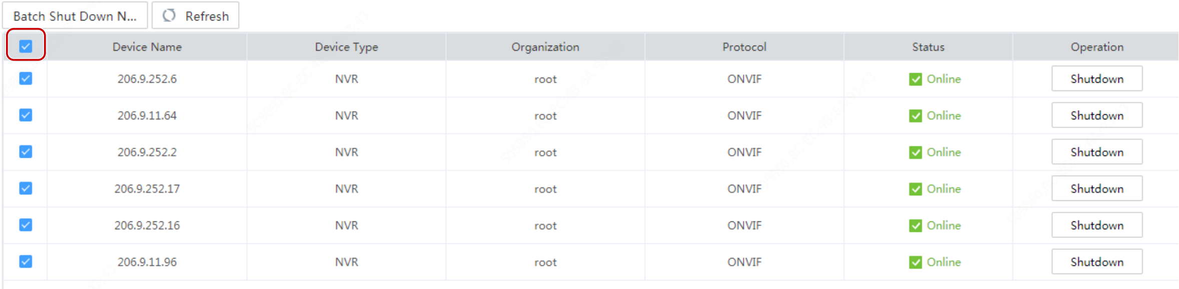
2. Enter the new passwords and then click **OK**.

Batch Shut Down NVRs

Basic > Batch Config > Batch Shut Down NVR

Shut down online NVRs in batches.

1. Select the NVR(s) to shut down. Selecting the checkbox on the top will select all the NVRs displayed on the current page.



☑	Device Name	Device Type	Organization	Protocol	Status	Operation
☑	206.9.252.6	NVR	root	ONVIF	☑ Online	Shutdown
☑	206.9.11.64	NVR	root	ONVIF	☑ Online	Shutdown
☑	206.9.252.2	NVR	root	ONVIF	☑ Online	Shutdown
☑	206.9.252.17	NVR	root	ONVIF	☑ Online	Shutdown
☑	206.9.252.16	NVR	root	ONVIF	☑ Online	Shutdown
☑	206.9.11.96	NVR	root	ONVIF	☑ Online	Shutdown

2. Click the **Batch Shut Down NVR** button.
3. Click the **Refresh** button. The selected NVR(s) disappear from the page.

NOTE!

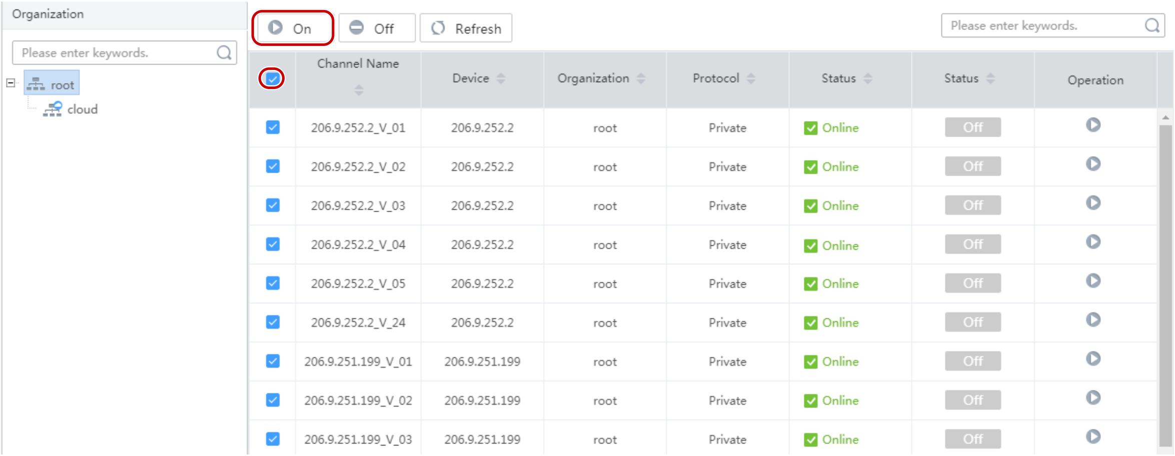
- This function is available to certain NVR versions. A message appears if the function is unavailable.
- This function is not available if the NVR is connected to the VMS via the VSS protocol.

Batch Scramble Streams

Basic > Batch Config > Batch Scramble Streams

Scramble video streams to enhance data security.

1. Select an organization on the left-side organization tree. Video channels in the organization are displayed.



☑	Channel Name	Device	Organization	Protocol	Status	Status	Operation
☑	206.9.252.2_V_01	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.252.2_V_02	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.252.2_V_03	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.252.2_V_04	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.252.2_V_05	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.252.2_V_24	206.9.252.2	root	Private	☑ Online	Off	▶
☑	206.9.251.199_V_01	206.9.251.199	root	Private	☑ Online	Off	▶
☑	206.9.251.199_V_02	206.9.251.199	root	Private	☑ Online	Off	▶
☑	206.9.251.199_V_03	206.9.251.199	root	Private	☑ Online	Off	▶

2. Select video channels for which you want to scramble streams and then click **On**. Selecting the checkbox on the top will select all the video channels on the current page.
3. To scramble the video stream of one video channel, click the corresponding ▶ for the video channel in the **Operation** column.

NOTE!

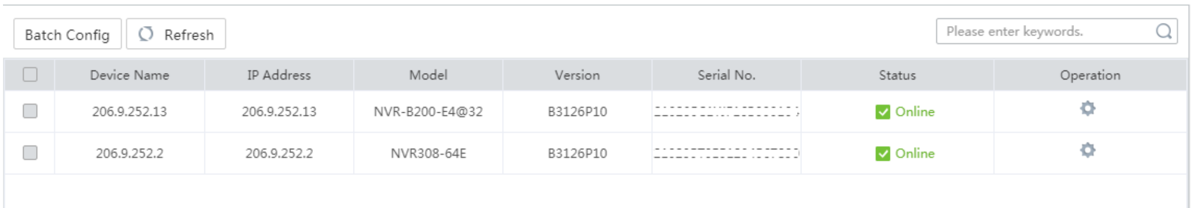
This function is available to devices connected via the private protocol.

Batch Configure Encoding Parameters

Basic > Batch Config > Batch Config Encoding Parameters

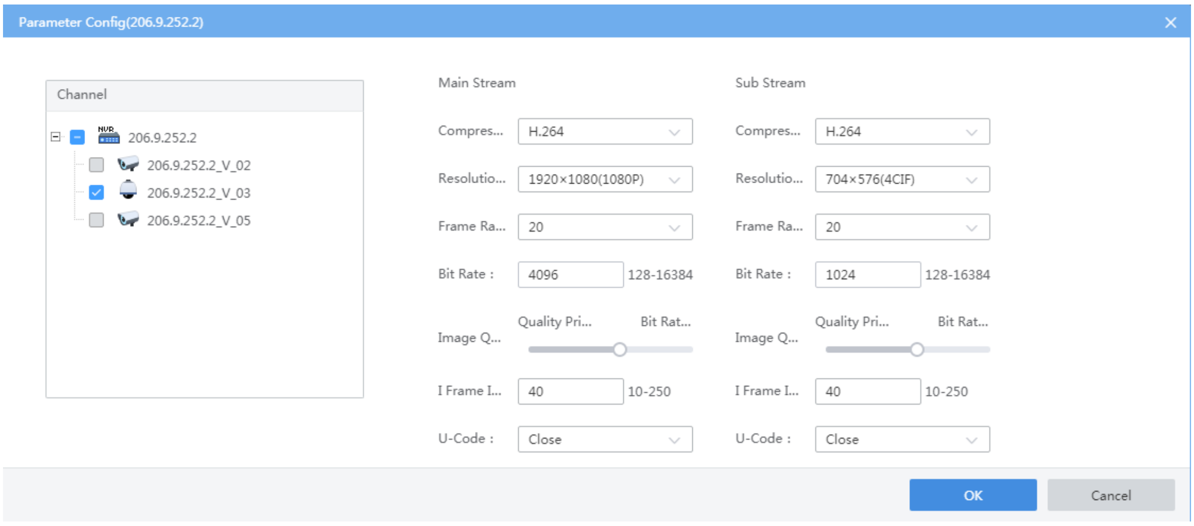
Configure encoding parameters in batches for IPC or NVR connected via the private protocol or ONVIF protocol. You can select and configure multiple IPCs of the same model or one NVR. Take an NVR as an example.

1. Select the NVR you want to configure and then click **Batch Config**.



□	Device Name	IP Address	Model	Version	Serial No.	Status	Operation
□	206.9.252.13	206.9.252.13	NVR-B200-E4@32	B3126P10	[redacted]	☑ Online	⚙
□	206.9.252.2	206.9.252.2	NVR308-64E	B3126P10	[redacted]	☑ Online	⚙

2. Select the channels and then configure the encoding parameters. Only the supported stream types are displayed. Stream types that are not supported are not displayed.



	Main Stream		Sub Stream	
Compres...	H.264		H.264	
Resolutio...	1920×1080(1080P)		704×576(4CIF)	
Frame Ra...	20		20	
Bit Rate :	4096	128-16384	1024	128-16384
Image Q...	Quality Pri...	Bit Rat...	Quality Pri...	Bit Rat...
I Frame I...	40	10-250	40	10-250
U-Code :	Close		Close	

3. Click **OK** to save the configurations.

3 Alarm Configuration

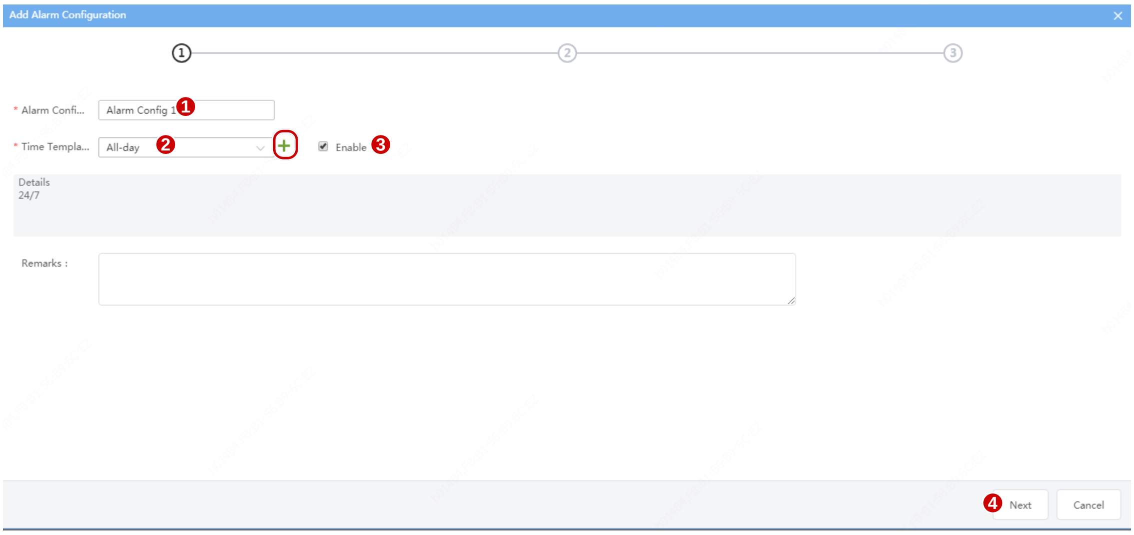
Alarm Configuration

Alarm Configuration > **Alarm Configuration**

Configure alarms so that certain alarms at specified sources will trigger actions such as buzzer and email.

Click **Add** and then follow the steps to add alarm configuration.

1. Complete settings including the alarm configuration name, time template, etc.



Add Alarm Configuration

* Alarm Confi... Alarm Config 1

* Time Templa... All-day

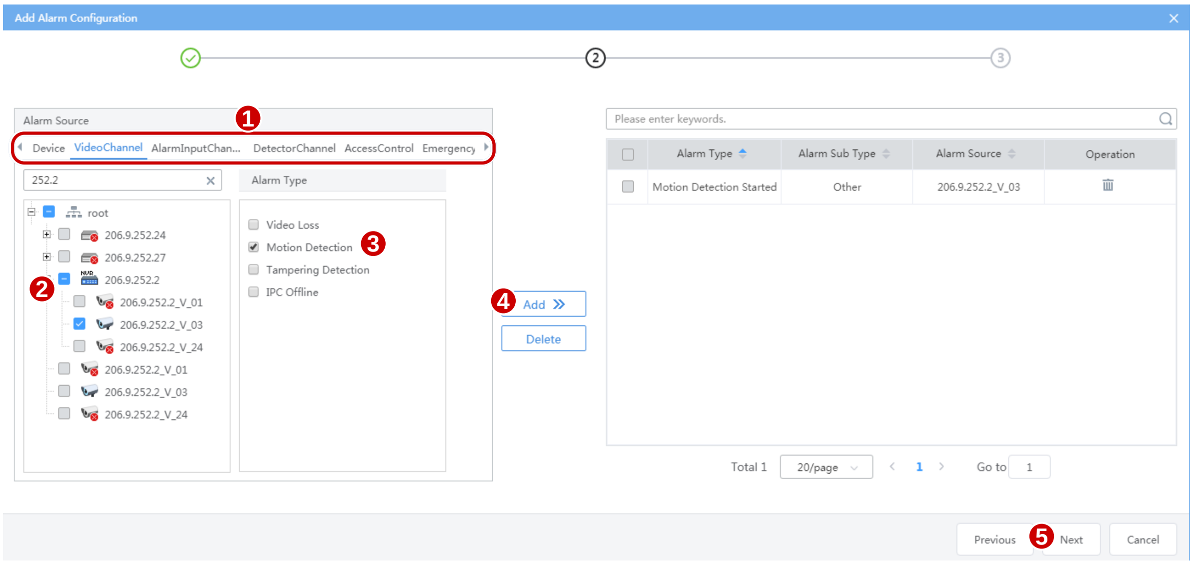
☑ Enable

Details
24/7

Remarks :

No.	Description
1	The alarm configuration name must be unique in the system.
2	Select a time template, or click + to create one. The alarm configuration is effective during the time set in the time template.
3	The alarm configuration is effective when the **Enable** checkbox is selected.

2. Set alarm source(s) and alarm type(s). When an alarm of the specified type occurs at the alarm source, it will trigger the object to perform the specified action(s). Up to 2000 combinations of alarm sources and alarm types are allowed.



Add Alarm Configuration

Alarm Source

Device | VideoChannel | AlarmInputChan... | DetectorChannel | AccessControl | Emergency

252.2

- root
  - 206.9.252.24
  - 206.9.252.27
  - 206.9.252.2
    - □ 206.9.252.2_V_01
    - ☑ 206.9.252.2_V_03
    - □ 206.9.252.2_V_24
  - □ 206.9.252.2_V_01
  - □ 206.9.252.2_V_03
  - □ 206.9.252.2_V_24

Alarm Type

□ Video Loss
☑ Motion Detection
□ Tampering Detection
□ IPC Offline

Please enter keywords.

□	Alarm Type	Alarm Sub Type	Alarm Source	Operation
□	Motion Detection Started	Other	206.9.252.2_V_03	🗑

Total 1 | 20/page | 1 | Go to 1

No.	Description
1	Select the alarm source type. **Note**: The types displayed may vary depending on the VMS model and version. The illustration is just an example.

No.	Description
2	Select alarm source(s).
3	Select alarm type(s).

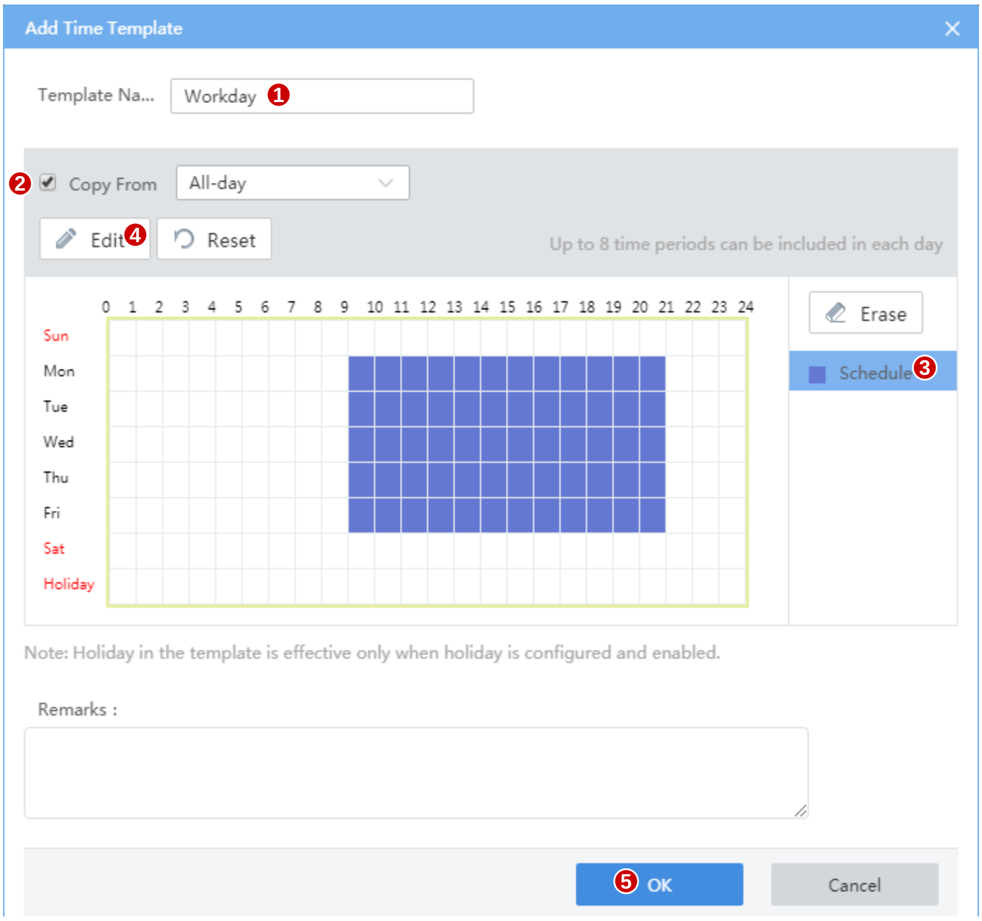
3. Set action(s) to trigger and object(s) to link. To trigger email, you also need to complete email settings (see Email0). To trigger buzzer, select **Enable Buzzer**. When an alarm of the specified type occurs at the alarm source, the linked object(s) will perform the specified action(s). One alarm source can link multiple objects and trigger multiple actions.
4. The alarm configuration appears in the list and can be deleted, enabled or disabled as needed. Alarm configuration is not effective when disabled.

Time Template

Alarm Configuration > **Time Template**

Configure time templates for alarm configuration. All-day is the default time template in the system. You may change its name, but cannot delete this template.

Click **Add** to create a time template:



Add Time Template

Template Na... Workday

☑ Copy From All-day

Up to 8 time periods can be included in each day

Note: Holiday in the template is effective only when holiday is configured and enabled.

Remarks :

1. Enter the template name, e.g., Workday. The template name must be unique in the system. A name that is easy to identify is recommended.
2. (Optional) Select **Copy From** and select a template from the drop-down list. Edit based on this template.

3. Click **Schedule** on the right and then drag the mouse to draw on the template. Use the **Erase** or **Reset** button to clear some or all settings.
4. To set precisely, click **Edit**. After completing the schedule for a day, you may copy the settings to other days by selecting the day(s) and clicking **Copy**.
5. Click **OK**.

NOTE!

A holiday in a time template is effective only when the holiday is configured and enabled (**System** > **Basic** > **Holiday**). See Holiday.

Contacts

Alarm Configuration > **Contacts**

Add a valid email address in **Contacts** as recipient before setting email as a triggered action.

Click **Test email** to test.

NOTE!

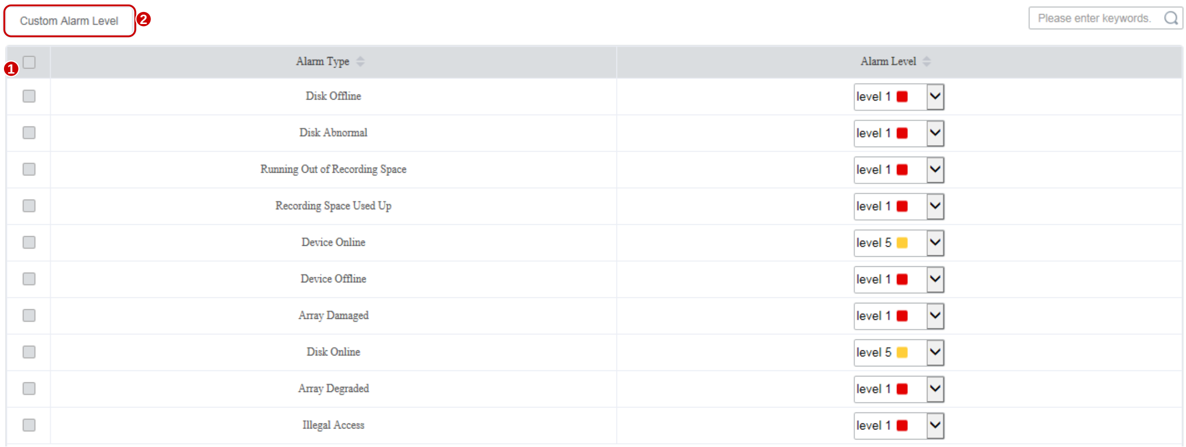
An email server must be configured before testing the email. For details, see Email.

Custom Alarm Level

Alarm Configuration > **Custom Alarm Level**

Assign alarm levels based on alarm type to distinguish alarm severity. There are five alarm levels (Level 1 to Level 5). Level 1 represents the severest and uses red.

Click an alarm source type (e.g., Device) on the left, and then, for the alarm type you want to configure, select the desired alarm level from the drop-down list. The settings are saved directly.



□	Alarm Type	Alarm Level
□	Disk Offline	level 1 🟥
□	Disk Abnormal	level 1 🟥
□	Running Out of Recording Space	level 1 🟥
□	Recording Space Used Up	level 1 🟥
□	Device Online	level 5 🟨
□	Device Offline	level 1 🟥
□	Array Damaged	level 1 🟥
□	Disk Online	level 5 🟨
□	Array Degraded	level 1 🟥
□	Illegal Access	level 1 🟥

To assign the same alarm level to multiple alarm types: select alarm types (1) and then click **Custom Alarm Level** (2). In the dialog box displayed, select the desired alarm level and then click **OK**.

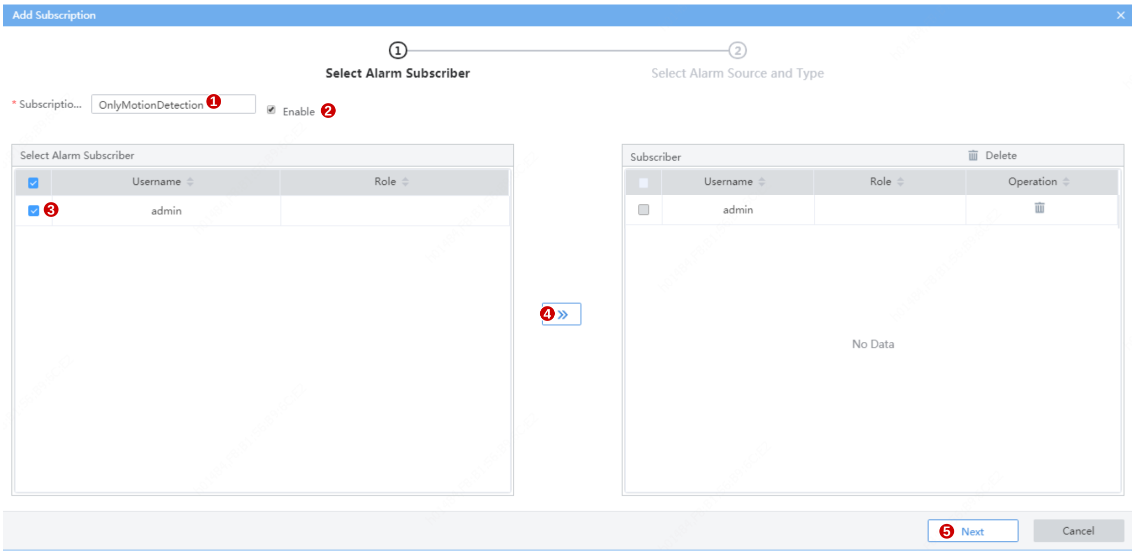
Alarm Subscription

Alarm Configuration > **Alarm Subscription**

Add an alarm subscription so that the subscriber(s) will only receive certain types of alarms from specified alarm source(s); irrelevant alarm messages will be filtered.

Click **Add** to add alarm subscription:

1. Select alarm subscriber.

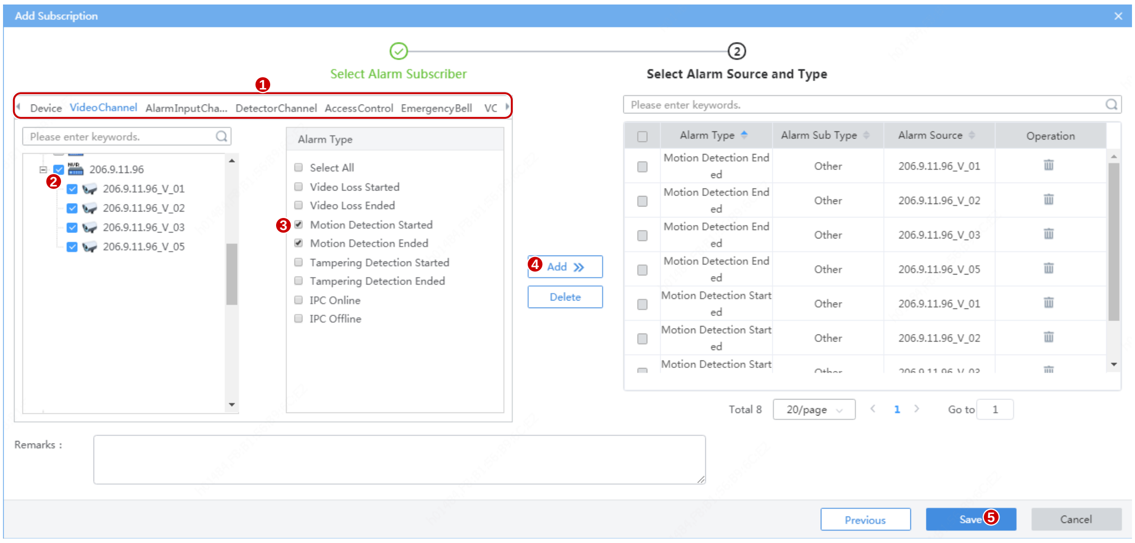


☑	Username	Role
☑	admin	

□	Username	Role	Operation
□	admin		🗑

No.	Description
1	The alarm subscription name must be unique in the system.
2	Alarm subscription is effective when the **Enable** checkbox is selected.
3	Select the alarm subscriber.

2. Select the alarm source and alarm type.



□	Alarm Type	Alarm Sub Type	Alarm Source	Operation
□	Motion Detection Ended	Other	206.9.11.96_V_01	🗑
□	Motion Detection Ended	Other	206.9.11.96_V_02	🗑
□	Motion Detection Ended	Other	206.9.11.96_V_03	🗑
□	Motion Detection Ended	Other	206.9.11.96_V_05	🗑
□	Motion Detection Started	Other	206.9.11.96_V_01	🗑
□	Motion Detection Started	Other	206.9.11.96_V_02	🗑
□	Motion Detection Start	Other	206.9.11.96_V_03	🗑

No.	Description
1	Select the alarm source type. **Note**: The types displayed may vary depending on the VMS model and version. The illustration is just an example.

No.	Description
2	Select the alarm source. Only alarms from the specified source will be sent to the subscriber.
3	Select the alarm type. Only alarms of the specified type(s) will sent to the subscriber.

3. The alarm subscription appears in the list and can be deleted, enabled or disabled as needed. Alarm subscription is not effective when disabled.

NOTE!

- Alarm subscription is enabled by default. If disabled, the client cannot receive any alarm messages, even if alarm subscription is configured.
- By default, a non-subscriber receives all alarm messages. To block all alarm messages for the user, add the user as an alarm subscriber without configuring any alarm source. Click **Save** directly at the **Select Alarm Source and Type** step.
- All alarms, including the subscribed and filtered, can be found on **History** tab on the **Alarm Records** page at the Software Client.

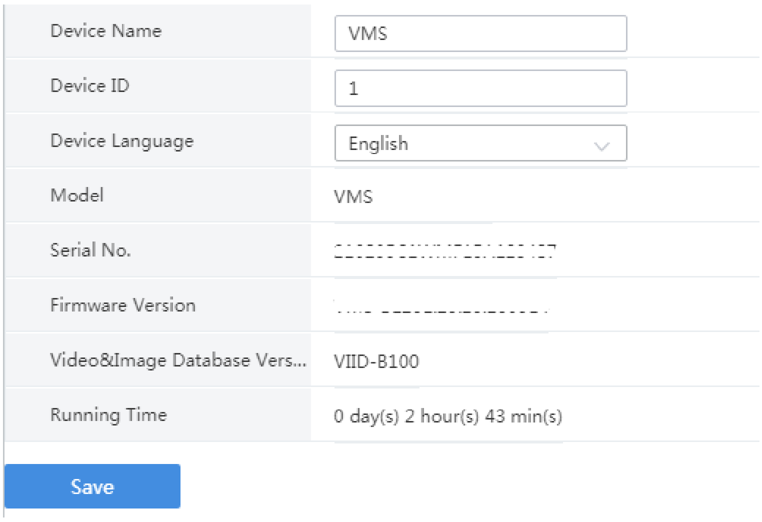
4 System Configuration

Basic Configuration

Basic

System > **Basic** > **Basic**

Configure the basic information of the VMS, including device name, system language; view device information including device model, serial number, firmware version, Video&Image Database version, and running time.



Device Name	VMS
Device ID	1
Device Language	English
Model	VMS
Serial No.	[redacted]
Firmware Version	[redacted]
Video&Image Database Vers...	VIID-B100
Running Time	0 day(s) 2 hour(s) 43 min(s)

NOTE!

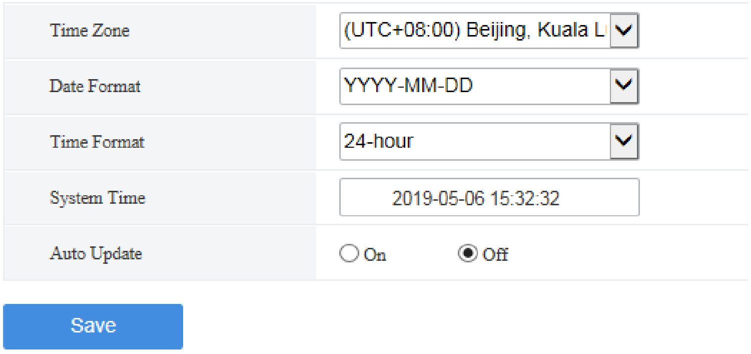
- Currently device ID is not in use.
- The **Running Time** shows how long the VMS has been running since its latest startup. This can be used to determine when a restart has occurred.

Date & Time

System > **Basic** > **Time**

Configure time for the VMS, including time zone, date and time format, and system time.

Auto Update: If enabled, an NTP server must be configured. The system time of the VMS syncs with the NTP server.



Time Zone	(UTC+08:00) Beijing, Kuala L
Date Format	YYYY-MM-DD
Time Format	24-hour
System Time	2019-05-06 15:32:32
Auto Update	○ On ● Off

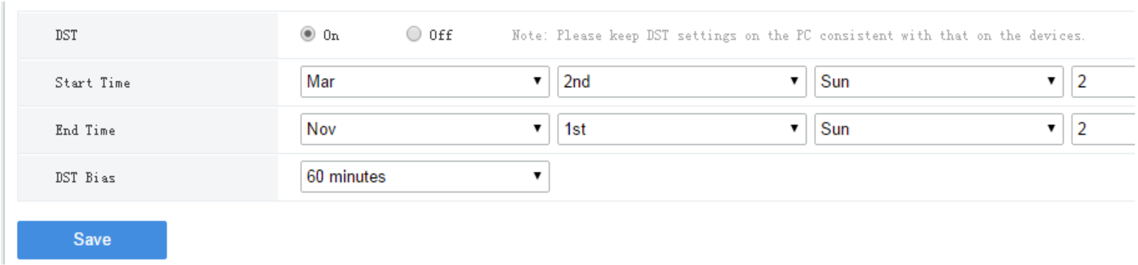
NOTE!

The PC Web client provides the **Sync with Computer** feature. When this feature is enabled, the system time of the VMS syncs with the PC's system time.

DST

System > **Basic** > **DST**

Set DST properly if your country or area uses the Daylight Saving Time (DST).

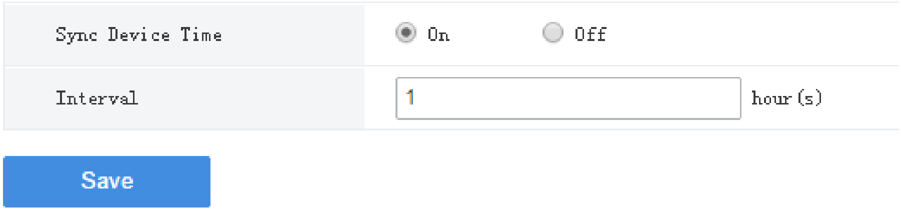


DST	● On ○ Off	Note: Please keep DST settings on the PC consistent with that on the devices.		
Start Time	Mar	2nd	Sun	2
End Time	Nov	1st	Sun	2
DST Bias	60 minutes			

Time Sync

System > **Basic** > **Time Sync**

This function is disabled by default. To enable this function, select **On**, set an appropriate interval, and then click **Save**. The VMS syncs time to all the directly connected devices under it immediately, including IPC, NVR, encoder and decoder (not including devices connected via an NVR), and then syncs time to devices at the set interval.



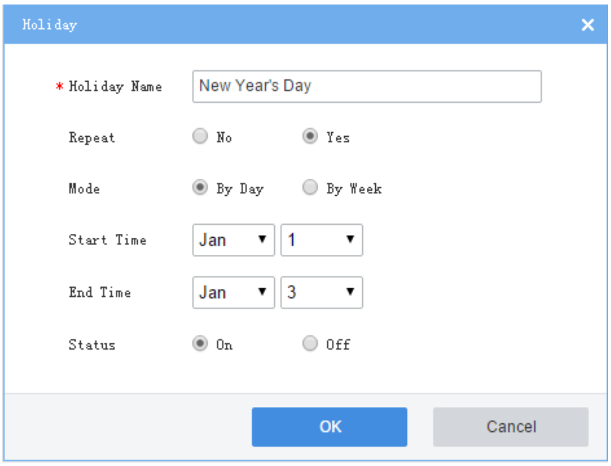
Sync Device Time ● On ○ Off

Interval 1 hour(s)

Holiday

System > **Basic** > **Holiday**

Holiday is used by time templates for alarm configuration. The holiday name must be unique in the system.



Holiday

* Holiday Name New Year's Day

Repeat ○ No ● Yes

Mode ● By Day ○ By Week

Start Time Jan 1

End Time Jan 3

Status ● On ○ Off

Disk Configuration

Disk Management

System > **Disk** > **Disk**

View disk info (slot number, device, disk status, and space usage), format disks (click ⊘), modify disk property.

Advanced Configuration

System > **Disk** > **Advanced**

Set the policy that the VMS adopts when recording space is used up:

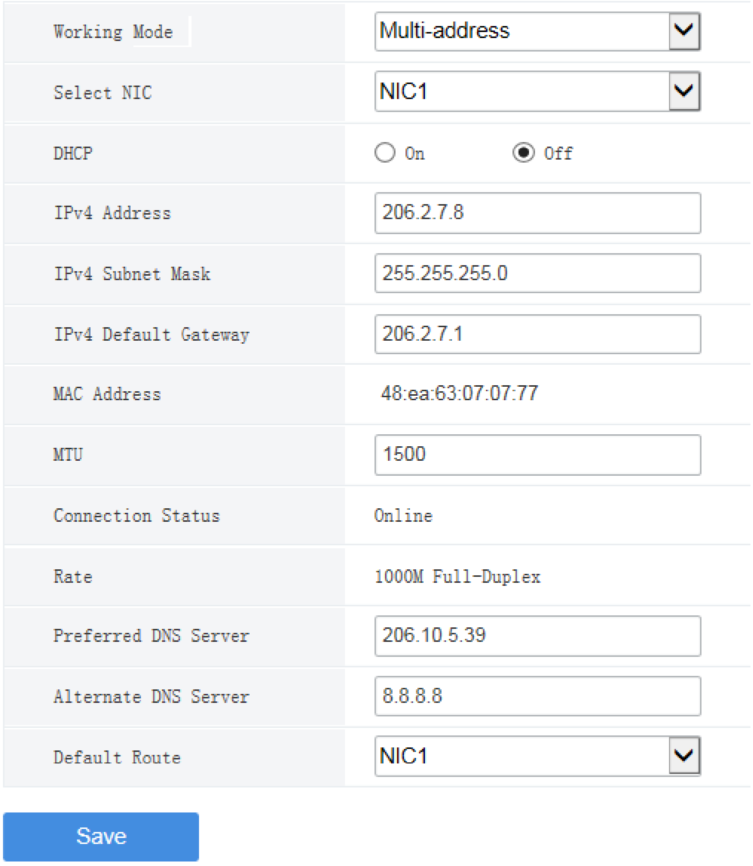
- Overwrite: Earliest recordings will be overwritten by new recordings when space is used up.
- Stop: Recording stops when space is used up.

Network Configuration

TCP/IP

System > **Network** > **TCP/IP**

Set TCP/IP parameters in different working modes, including IP obtainment (static or DHCP), IP address, subnet mask, default gateway, MTU, preferred and alternate DNS server, and default route.



Working Mode	Multi-address
Select NIC	NIC1
DHCP	○ On ● Off
IPv4 Address	206.2.7.8
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	206.2.7.1
MAC Address	48:ea:63:07:07:77
MTU	1500
Connection Status	Online
Rate	1000M Full-Duplex
Preferred DNS Server	206.10.5.39
Alternate DNS Server	8.8.8.8
Default Route	NIC1

NOTE!

- Network configurations are isolated among different working modes.
- Switching the working mode will restart the device and clear all custom routes.
- The configured IPv4 addresses of the NICs must belong to different network segments.

- Working mode

  Multi-address: Default mode. The Network Interface Cards (NICs) work independently with different IP addresses.

  Load Balance: NICs that make up a virtual NIC use the same IP and work together to share the network load.

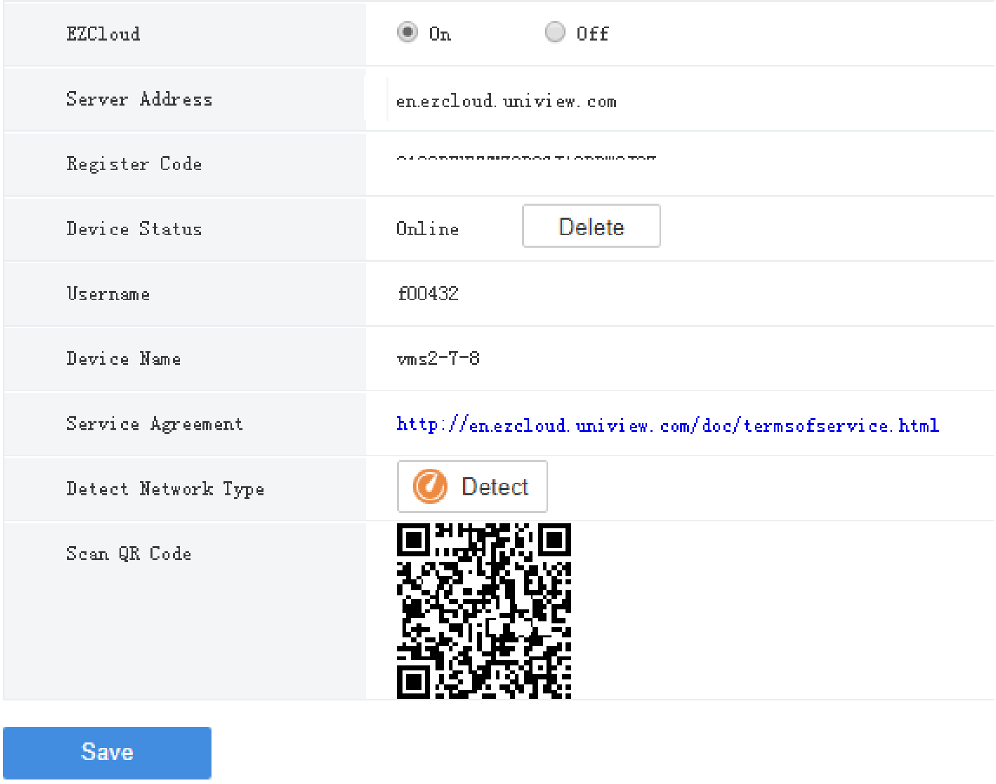
  Net Fault-tolerance: NICs that make up a virtual NIC use the same IP and work as a backup to each other. If either NIC becomes faulty, the other takes over.

- DHCP: Use a DHCP server to automatically assign an IP address.
- IPv4 Address: VMS' IP address. Users access the system at this address from a Web or software client.
- DNS server: Domain Name Server, which resolves a domain name into an IP address.
- Default Route: Specifies the default NIC that the VMS uses to send data. The default route may be different from the NIC set in the Select NIC drop-down list.

EZCloud

System > **Network** > **EZCloud**

EZCloud is intended for remote surveillance and is disabled by default. You may enable EZCloud and use the register code to register the VMS at the EZCloud website. If the **Device Status** is **Online**, you can use the cloud account to access the VMS.



EZCloud	● On ○ Off
Server Address	en.ezcloud.uniview.com
Register Code	[illegible]
Device Status	Online Delete
Username	f00432
Device Name	vms2-7-8
Service Agreement	http://en.ezcloud.uniview.com/doc/termsofservice.html
Detect Network Type	Detect
Scan QR Code	

- Register Code: Each VMS has a unique register code which is used to add the VMS to cloud.
- Device Status: If the status is **Online**, you may use the cloud account to access the VMS; Clicking **Delete** will delete the device from cloud.
- Username: Account name used to register the VMS at the cloud website.
- Device Name: Cloud name of the device.
- Detect Network Type: Click **Detect** to detect the NAT type, IP address type and firewall of the network.
- Scan QR Code: Scan the QR code with the mobile client to add the VMS to cloud.

NOTE!

When connected to EZCloud, the VMS is remotely accessible from the computer software client or EZView on the Internet. It is recommended that the VMS has a public IP address or is connected to the Internet through single network address translation (NAT).

DDNS

System > **Network** > **DDNS**

DDNS (Dynamic Domain Name Service) associates a changing IP address to a fixed domain name and allows users to access the device by visiting the fixed domain name instead of the changing IP address. Three DDNS services are available:

DynDNS

You need to complete registration at DynDNS official website first. After completing the registration, complete settings on this page. When device status is Online, you can access the VMS using the domain name.

No-IP

You need to complete registration at the No-IP official website first. After completing the registration, complete settings on this page. When device status is Online, you can access the VMS using the domain name.

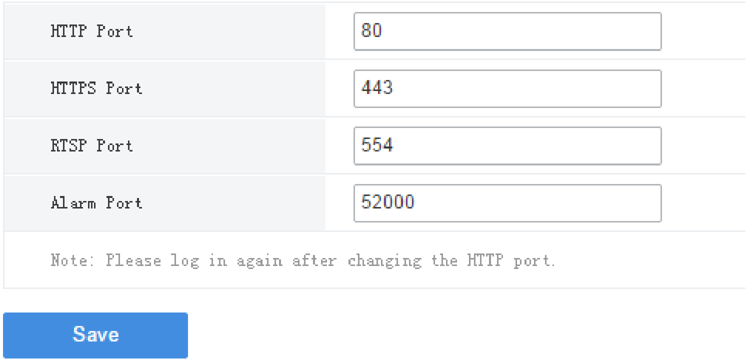
EZDDNS

- The default server address is en.ezcloud.uniview.com.
- The default port is 80.
- Domain name: Enter a domain name (e.g., VMS2) and then click **Check** to verify. If the domain name is usable, click **Save**. If the device status is Online, you can access the device using the automatically generated device address (e.g., en.ezcloud.uniview.com/vms2).

Port

System > **Network** > **Port**

Configure HTTP, HTTPS, RTSP and alarm ports.



HTTP Port	80
HTTPS Port	443
RTSP Port	554
Alarm Port	52000

Note: Please log in again after changing the HTTP port.

Port Mapping

System > **Network** > **Port**

Use port mapping (UPnP or Manual) to configure mapping relations between internal and external ports.

The VMS supports two port mapping modes:

- UPnP

  Auto: The VMS automatically negotiates external ports with the router. If an external port is already in use, the VMS will negotiate with the router again with another port number.

  Manual: Specify external ports manually. If the specified port is already in use, the VMS will not try again with another port, and port mapping will fail.

- Manual: Usually this mode is used when the router does not support UPnP. Complete settings on the router first and then fill in the settings on this page.

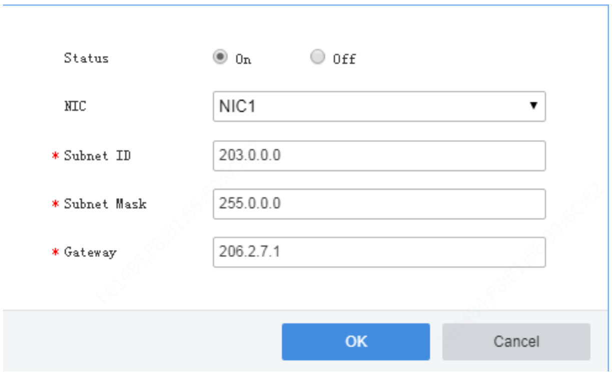
NOTE!

- By default port mapping is disabled.
- Enable UPnP in the router first. UPnP requires the router's support.

Custom Route

System > **Network** > **Custom Route**

Add static routes to interconnect the VMS with destination networks. Up to 100 custom routes are allowed. You need to choose the NIC and set the subnet ID, subnet mask and gateway. A custom route is enabled by default and can be disabled.



Status	● On ○ Off
NIC	NIC1
* Subnet ID	203.0.0.0
* Subnet Mask	255.0.0.0
* Gateway	206.2.7.1

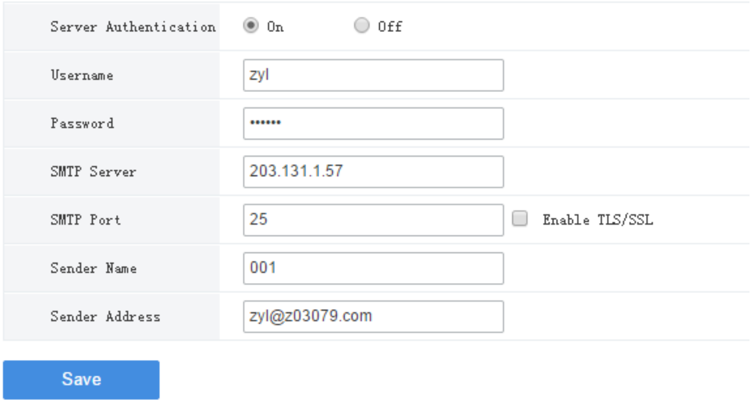
NOTE!

Changing the NIC's working mode will clear all the existing custom routes.

Email

System > **Network** > **Email**

Email configuration must be completed before all email-related functions (such as alarm-triggered email) can work properly.



Server Authentication	● On ○ Off
Username	zyl
Password	••••••
SMTP Server	203.131.1.57
SMTP Port	25 □ Enable TLS/SSL
Sender Name	001
Sender Address	zyl@z03079.com

NOTE!

- Enter the correct username and password after enabling (SMTP) server authentication.
- To encrypt data transmission between the VMS and the SMTP server, select TLS/SSL.
- You may need to change the SMTP port accordingly after enabling TLS/SSL.

Protocols & Interconnection

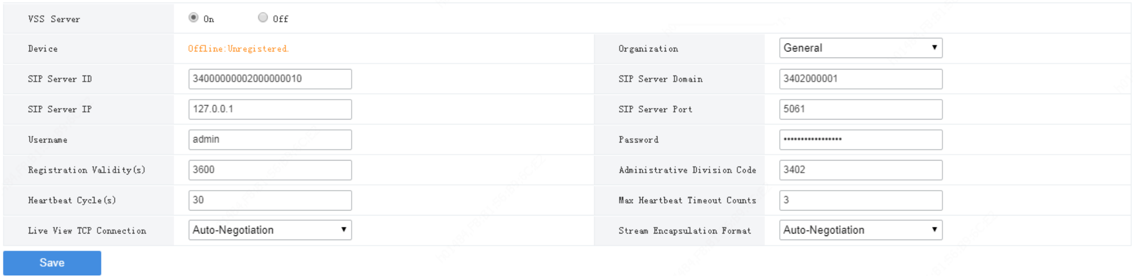
VSS Server

System > **Network** > **Protocols & Interconnection** > **VSS Server**

Configure VSS server parameters to connect the VMS to a higher-level management platform. When the configuration is complete, you can manage the VMS on the platform and perform live view, playback, and alarm subscription on channels under the VMS.

In VSS server configuration, SIP server refers to the higher-level management platform.

1. Complete basic settings

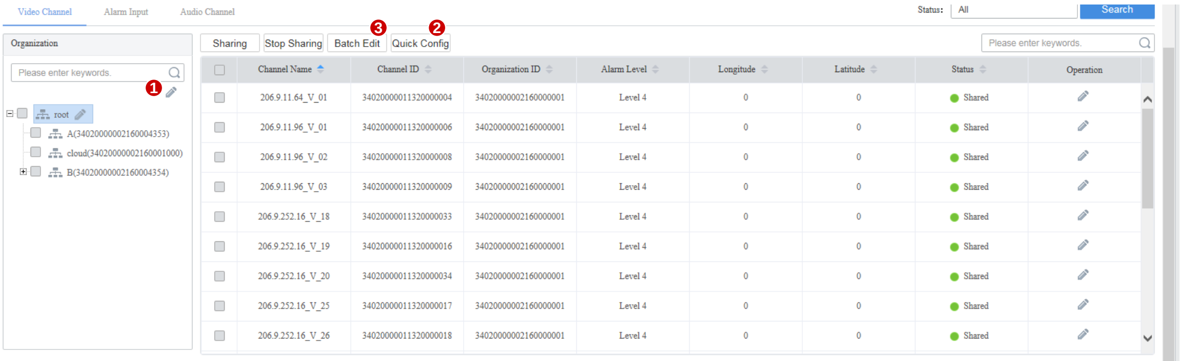


VSS Server	● On ○ Off		
Device	Offline:Unregistered.	Organization	General ▾
SIP Server ID	34000000002000000010	SIP Server Domain	3402000001
SIP Server IP	127.0.0.1	SIP Server Port	5061
Username	admin	Password	•••••••••••••••••
Registration Validity(s)	3600	Administrative Division Code	3402
Heartbeat Cycle(s)	30	Max Heartbeat Timeout Counts	3
Live View TCP Connection	Auto-Negotiation ▾	Stream Encapsulation Format	Auto-Negotiation ▾

- SIP Server ID: ID of the platform server (obtained from the server).
- SIP Server IP: IP address of the platform server (obtained from the server).
- Organization: The drop-down list shows the General organization and all the custom organizations that you have created. You need to click **Save** after choosing a different organization from the list. The organization tree in the lower left corner shows the organization that you have chosen.
- SIP Server Domain: Domain ID of the platform server.
- SIP Server Port: Port assigned on the platform server.
- Heartbeat Cycle: Keepalive cycle between the VMS and the platform.
- Max Heartbeat Timeout Counts: Max number of times that communication times out between the VMS and the platform. Communication stops automatically when it reaches the max count.

2. Share channels with higher-level management platform

When channels are shared successfully with the higher-level management platform, operators can search these channels on the platform and subscribe to alarms of these channels. When sharing is stopped, the channels will be deleted from the higher-level management platform



□	Channel Name	Channel ID	Organization ID	Alarm Level	Longitude	Latitude	Status	Operation
□	206.9.11.64_V_01	34020000011320000004	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.11.96_V_01	34020000011320000006	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.11.96_V_02	34020000011320000008	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.11.96_V_03	34020000011320000009	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.252.16_V_18	34020000011320000033	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.252.16_V_19	34020000011320000016	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.252.16_V_20	34020000011320000034	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.252.16_V_25	34020000011320000017	34020000002160000001	Level 4	0	0	● Shared	✎
□	206.9.252.16_V_26	34020000011320000018	34020000002160000001	Level 4	0	0	● Shared	✎

1. Select the desired organization from the **Organization** drop-down list and then click **Save**. The organization appears on the organization tree.
2. Select the desired channel type to share: video channel, alarm input channel or audio channel.
3. Edit organization IDs on the organization tree. You can select multiple organizations and click **Batch Edit** (see 1 in the figure) to edit in batches.
4. Click **Quick Config** (see 2 in the figure) to assign channel IDs to channels without channel IDs. Set the basic code, and then the system will create and assign channel IDs based on the basic code.
5. You can select channels and click **Batch Edit** (see 3 in the figure) to edit channel IDs in batches.

NOTE!

- Chanel ID: 8-character center code + 2-character industry code + 3-character type code + 7-digit sequence number (SN).
- Basic code: The system creates new channel IDs based on the basic code that you set and assigns automatically. The basic code includes three parts: the first part is the default value which you may change as needed; the second part is generated automatically according to the channel type and cannot be edited; the third part is the sequence number that needs to be set.
- The **Quick Config** function only assigns new channel IDs to channels without channel ID and does not change any existing channel IDs.
- When you edit an organization ID on the organization tree, make sure each organization ID is unique in the local domain and is NOT identical with any organization ID or any other channel ID.

6. After being assigned a channel ID, a channels' status is displayed as **Shared**, the channel can be discovered on the higher-level platform, and the higher-level platform can subscribe to alarms from this channel.
7. To stop sharing channels, select the channels and click **Stop Sharing**. When sharing is stopped, the status changes to **Unshared**, and the channels are deleted from the higher-level platform.

NOTE!

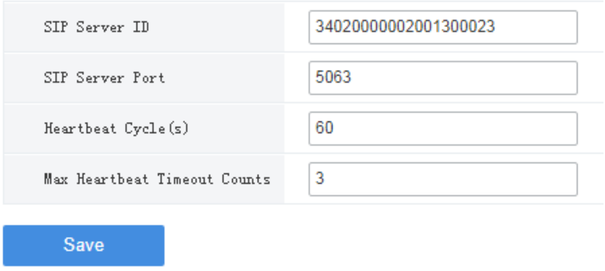
An audio channel cannot be shared or unshared like a video channel. An audio channel's status (Shared or Unshared) is consistent with that of the corresponding video channel. That is to say, sharing (or stop sharing) a video channel also shares (or stops sharing) the corresponding audio channel.

VSS Local

Configure VSS local parameters to connect devices such as IPC and NVR to the VMS. In VSS local configuration, SIP server refers to the VMS.

System > **Network** > **Protocols & Interconnection** > **VSS Local**

- SIP Server ID: VSS ID of the VMS.
- SIP Server Port: VSS port assigned on the VMS.
- Heartbeat Cycle: Keepalive cycle between the VMS and the IPC/NVR devices.
- Max Heartbeat Timeout Counts: Max number of times that communication times out between the VMS and IPC/NVR devices. Communication stops automatically when it reaches the max count.



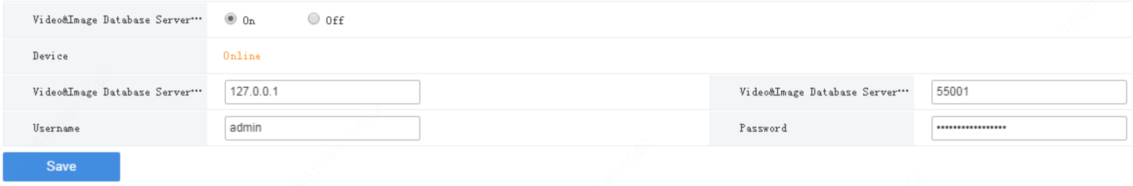
SIP Server ID	34020000002001300023
SIP Server Port	5063
Heartbeat Cycle(s)	60
Max Heartbeat Timeout Counts	3

Video&Image Database

System > **Network** > **Protocols & Interconnection** > **Video&Image Database Config**

Video&Image database configuration includes server configuration and local configuration.

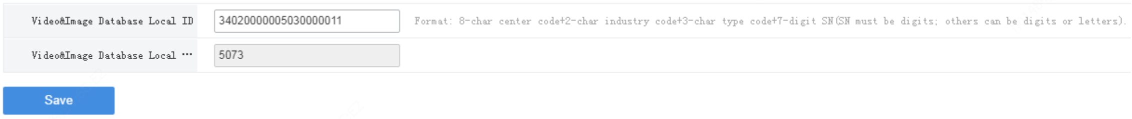
Video&Image Database Configuration



Video&Image Database Server···	● On ○ Off		
Device	Online		
Video&Image Database Server···	127.0.0.1	Video&Image Database Server···	55001
Username	admin	Password	•••••••••••••••••

- Device: The device is displayed as "Online" when the VMS is successfully connected to the Video&Image Database server.
- Video&Image Database Server IP: IP address of the Video&Image Database server.
- Video&Image Database Server Port: Port number of the Video&Image Database server.
- Username/password: The username and password used to connect to the Video&Image Database server.

Video&Image Database Configuration



Video&Image Database Local ID	34020000005030000011	Format: 8-char center code+2-char industry code+3-char type code+7-digit SN(SN must be digits; others can be digits or letters).
Video&Image Database Local ···	5073	

- Video&Image Database Local ID: Device ID of the VMS that you use when adding the VMS to the Video&Image Database server.
- Video&Image Database Local Port: 5073. This port must be set on the license plate recognition camera or face recognition camera.

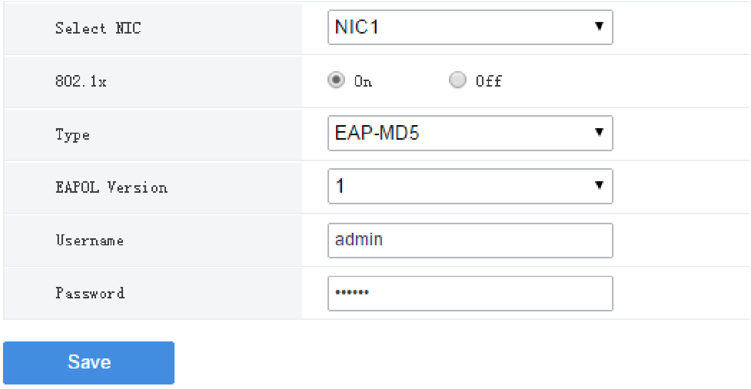
Security Configuration

802.1x

System > **Security** > **802.1x**

Enable **802.1x** to control access to the device with username and password set in the network switch.

- You may select an NIC to enable 802.1x; authentication is independent among NICs. **Binding 1** and **Binding 2** are displayed if the working mode of the selected NIC is **Load Balance** or **Net Fault-tolerance**.
- Type: Protocol type, currently only EAP-MD5.
- EAPOL Version: 1 for 802.1x-2001, and 2 for 802.1x-2004.
- Username and password: Used for authentication. Authentication succeeds when the entered username and password match that on the authenticator (such as Ethernet switch).



Select NIC	NIC1 ▾
802.1x	● On ○ Off
Type	EAP-MD5 ▾
EAPOL Version	1 ▾
Username	admin
Password	••••••

NOTE!

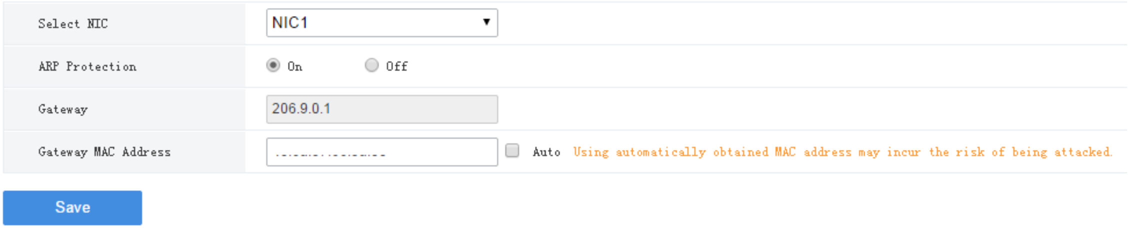
802.1x must also be properly configured on the authenticator (such as Ethernet switch).

ARP Protection

System > **Security** > **ARP Protection**

Enable **ARP Protection** to protect the device from potential ARP attacks by verifying the gateway's MAC address in access requests.

Select **Auto** to obtain an MAC address automatically, or fill in an MAC address manually.



Select NIC	NIC1 ▾
ARP Protection	● On ○ Off
Gateway	206.9.0.1
Gateway MAC Address	[illegible] □ Auto Using automatically obtained MAC address may incur the risk of being attacked.

NOTE!

Please make sure the function is enabled and the MAC address is set (either manually or automatically) before ARP attacks are inflicted. Any changes made during the attacks may fail the protection.

HTTPS

System > **Security** > **HTTPS**

Enable HTTPS (HTTP Secure) function by creating a private certificate or uploading a signed certificate. In HTTPS, the communication protocol is encrypted by Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

- Private: Uses a private certificate which is not signed by a trusted authority.
- Request: Uses a certificate issued by a trusted authority.

After a certificate is created and HTTPS is enabled, you may use https://device IP to access the device.

NOTE!

- If a private certificate has been created, you have to delete it before you can create another certificate.
- If a request has been created, you have to delete it before you can create another request.
- A certificate cannot be deleted when HTTPS is enabled. Disable HTTPS and then click **Save**.

Telnet

System > **Security** > **Telnet**

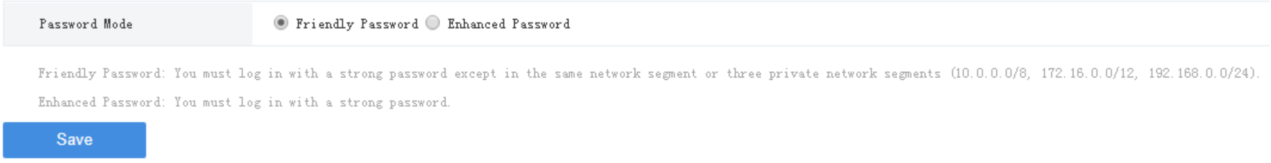
Access the device through Telnet for maintenance.

Secure Password

System > **Security** > **Secure Password**

The **Friendly Password** mode is enabled by default. In this mode, access with a weak password is allowed from the same network segment or on three private network segments.

When the **Enhanced Password** mode is enabled, access the software client with a weak password is forbidden; the user will be forced to change the weak password to a strong one on the Web client; and it is not allowed to set a weak password when adding a user or change a user's password to a weak one.



Password Mode ● Friendly Password ○ Enhanced Password

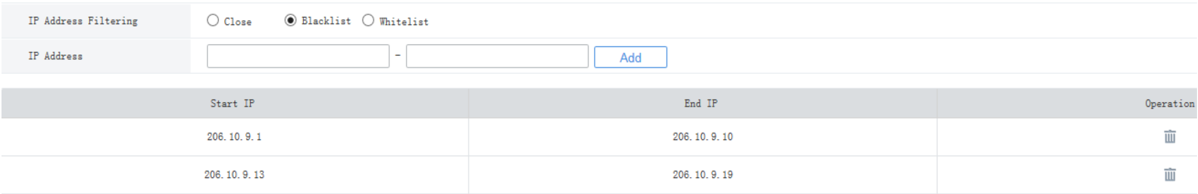
Friendly Password: You must log in with a strong password except in the same network segment or three private network segments (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24).

Enhanced Password: You must log in with a strong password.

IP Address Filtering

System > **Security** > **IP Address Filtering**

Use blacklist/whitelist to forbid or allow login from certain IP addresses only.



IP Address Filtering ○ Close ● Blacklist ○ Whitelist

IP Address: ____ - ____

Start IP	End IP	Operation
206.10.9.1	206.10.9.10	🗑
206.10.9.13	206.10.9.19	🗑

- Blacklist: When enabled, login from the specified IP addresses is forbidden.
- Whitelist: When enabled, login only from the specified IP addresses are allowed.

NOTE!

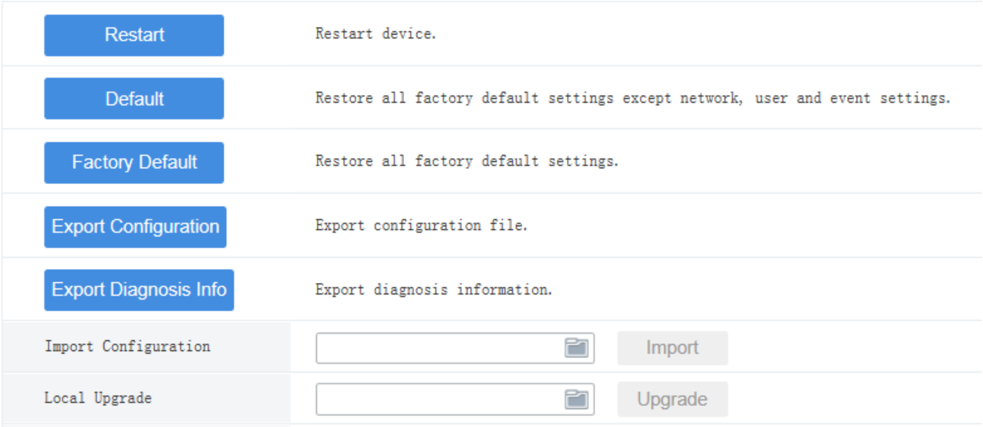
- Blacklist and whitelist cannot be enabled at the same time.
- Blacklist/whitelist is effective to IP-based logins.
- You can click a field in the list to edit an IP address.

Maintenance

System Maintenance

System > **Maintenance** > **Maintenance**

Restart the VMS, restore default configurations, import or export configurations, export diagnosis info, and perform a local upgrade. Connect a USB storage device if you operate on the local client.



Restart	Restart device.	
Default	Restore all factory default settings except network, user and event settings.	
Factory Default	Restore all factory default settings.	
Export Configuration	Export configuration file.	
Export Diagnosis Info	Export diagnosis information.	
Import Configuration		Import
Local Upgrade		Upgrade

- Default: Restore all factory settings except network, user and event settings. Note: Except **IP Address Filtering**, all the other settings under the **Security** tab will be maintained.
- Factory Default: Restore all factory default settings.
- Export Configuration: Export current configurations to a backup file, and use this file to restore configurations when necessary.
- Export Diagnosis Info: Export diagnosis info of the VMS.
- Import Configuration: Restore configurations by importing a backup configuration file. The VMS will restart.
- Local Upgrade: Upgrade the VMS version by using upgrade files saved on a USB storage device. The VMS will restart to complete the upgrade.

NOTE!

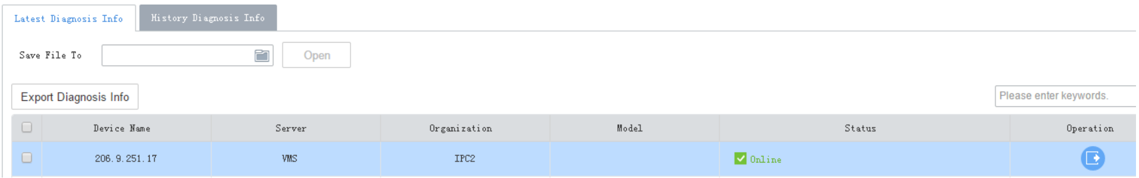
- The PC Web client provides the **Plug-in Log Path** feature. You may click **Open** to view plugin logs, or click the folder icon to customize the path. The text box and the button are grayed out if no plugin is installed or if your Web browser does not support a plugin.
- When using IE9 or higher on the PC Web client, you cannot upgrade the VMS by loading a local upgrade file if no plugin is installed.

Device Diagnosis Info

System > **Maintenance** > **Device Diagnosis Info**

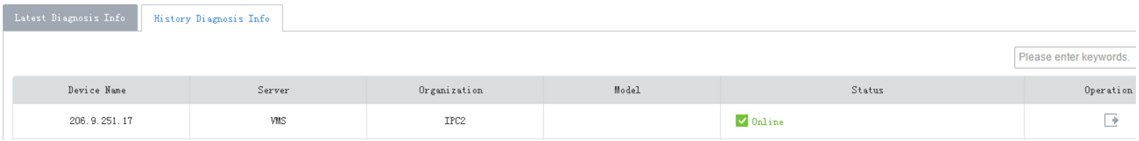
Click to export diagnosis information of devices (NVR and camera) directly connected to the VMS, including latest and history diagnosis info.

Latest diagnosis info can be exported only when the device is online.



□	Device Name	Server	Organization	Model	Status	Operation
□	206.9.251.17	VMS	IPC2		☑ Online	

To export history diagnosis info, the NVR must be online (the camera doesn't have to). History diagnosis info refers to diagnosis info of up to the last 15 days.



Device Name	Server	Organization	Model	Status	Operation
206.9.251.17	VMS	IPC2		☑ Online	

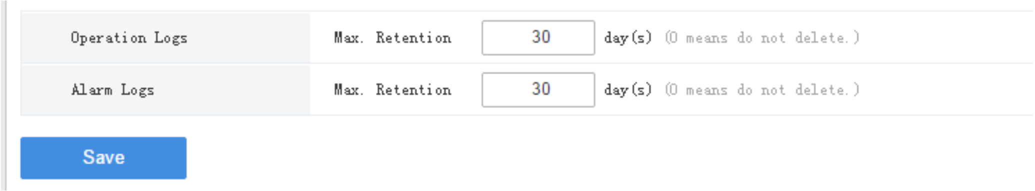
NOTE!

This feature is not available to devices connected via VSS and third-party devices.

Delete Logs

System > **Maintenance** > **Delete Logs**

Set the VMS to delete operation and alarm logs automatically. Logs that have been saved for a certain period will be deleted automatically. The default maximum retention time is 30 days. Entering 0 means logs will not be deleted automatically.



Operation Logs	Max. Retention	30	day(s) (0 means do not delete.)
Alarm Logs	Max. Retention	30	day(s) (0 means do not delete.)

Packet Capture

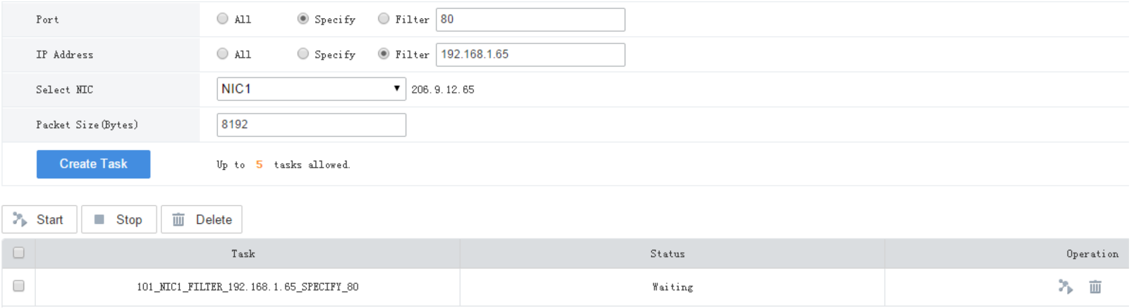
System > **Maintenance** > **Packet Capture**

Capture packets for troubleshooting or analysis.

Set conditions (port number, IP address, NIC and packet size) to capture or filter packets of specified port and/or IP address.

After conditions are set, click **Create Task**. Up to 5 tasks are allowed. The created tasks are listed. You may click to delete a task.

Click ▶ to start the task, click ■ to stop, and then click ⇥ to export captured packets to your computer. You need to export manually every time a task is completed.



Port	○ All	● Specify	○ Filter	80
IP Address	○ All	○ Specify	● Filter	192.168.1.65
Select NIC	NIC1 ▾	206. 9. 12. 65		
Packet Size(Bytes)	8192			
Create Task	Up to 5 tasks allowed.			

□	Task	Status	Operation
□	101_NIC1_FILTER_192. 168. 1. 65_SPECIFY_80	Waiting	

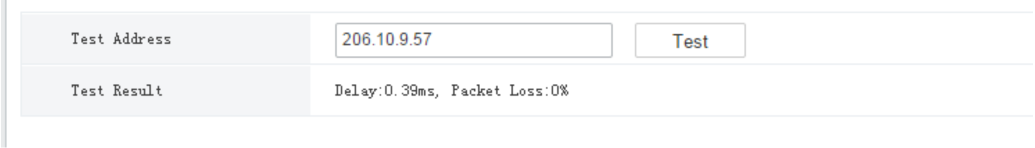
NOTE!

A file is generated for each packet capture task with a max size limit (around 19.1M). When the file size reaches the limit, the packet capture task stops automatically (note: the status does not change and it is still displayed as **Ongoing** when the task stops in this way).

Network Detect

System > **Maintenance** > **Net Detect**

Test a domain name or an IP address by filling in the field and clicking **Test**. The test result indicates whether there is a connection and the connection status (delay and packet loss rate) if connected.

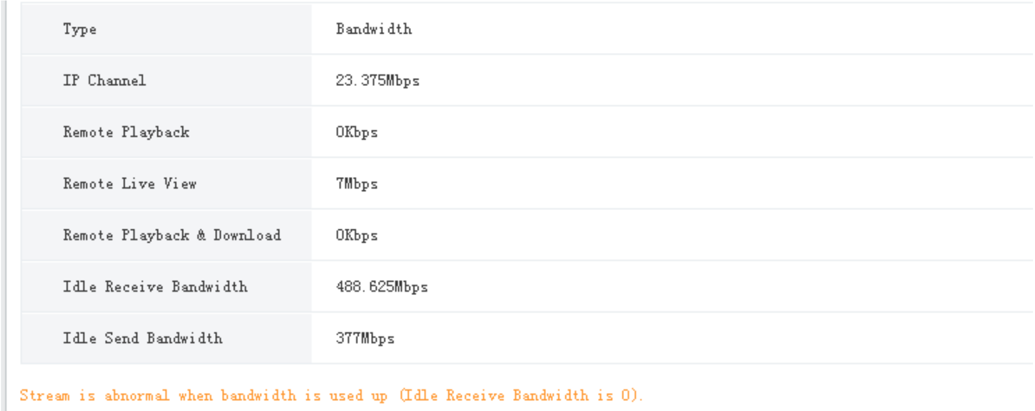


Test Address	206.10.9.57
Test Result	Delay:0.39ms, Packet Loss:0%

Bandwidth Usage

System > **Maintenance** > **Bandwidth Usage**

View network bandwidth usage statistics, including bandwidth used by connected IP cameras, used for remote playback, remote live view, remote playback and download, and idle receive and send bandwidth.



Type	Bandwidth
IP Channel	23.375Mbps
Remote Playback	0Kbps
Remote Live View	7Mbps
Remote Playback & Download	0Kbps
Idle Receive Bandwidth	488.625Mbps
Idle Send Bandwidth	377Mbps

Stream is abnormal when bandwidth is used up (Idle Receive Bandwidth is 0).

- IP Channel: Bandwidth usage when the VMS receives live video streams from devices (e.g., camera or NVR).

- Remote Playback: Bandwidth usage when the VMS receives recorded video streams from devices (NVR) (such as when a client computer plays recordings saved on the NVR).
- Remote Live View: Bandwidth usage when the VMS sends live video streams (such as when a client computer or video wall plays live video).
- Remote Playback & Download: Bandwidth usage when the VMS sends recorded video streams (such as when a client computer or video wall plays recorded video or during recording download).

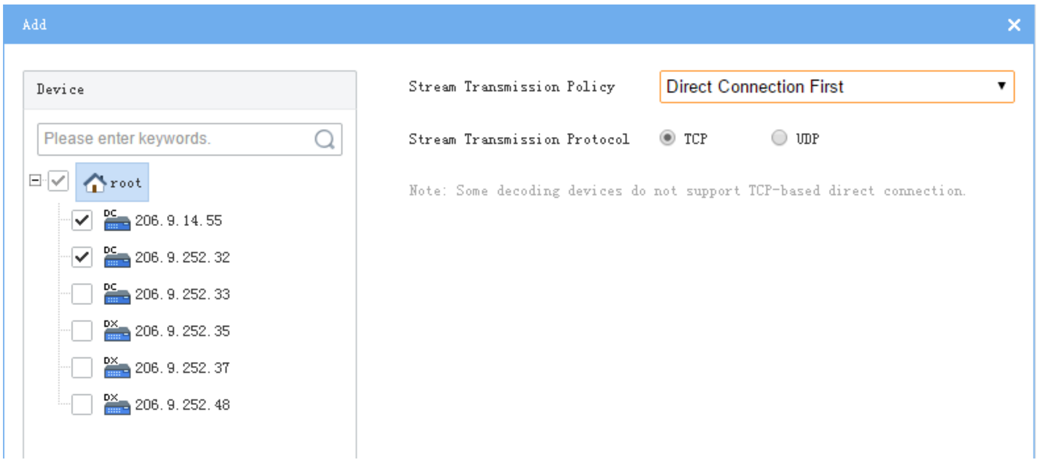
Stream Transmission Policy

System > **Maintenance** > **Stream Transmission Policy**

The Direct Connection First policy is effective on an LAN where the VMS collaborates with Uniview IPCs or NVRs.

If the policy is set to **Direct Connection First**, the VMS will determine whether conditions are satisfied (e.g., remaining output bandwidth of IPC/NVR) for direct transmission when starting streams. If conditions are satisfied, streams will be directly transmitted from IPC/NVR to the decoder, reducing bandwidth consumption of the VMS. If conditions are not satisfied for direct transmission, streams will be transmitted via the VMS.

If the policy is set to **Forwarding First**, streams will always be transmitted via the VMS from IPC/NVR to the decoder.



Add ✕

Device

Please enter keywords

☑ root
- ☑ DC 206.9.14.55
- ☑ DC 206.9.252.32
- □ DC 206.9.252.33
- □ DX 206.9.252.35
- □ DX 206.9.252.37
- □ DX 206.9.252.48

Stream Transmission Policy: Direct Connection First ▾

Stream Transmission Protocol: ● TCP ○ UDP

Note: Some decoding devices do not support TCP-based direct connection.

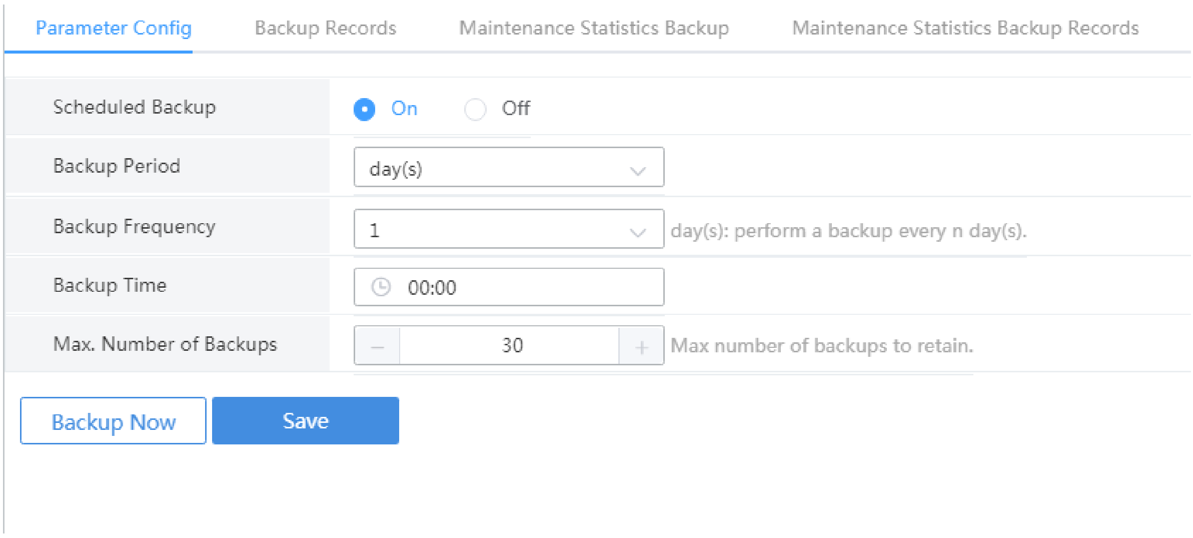
NOTE!

Some decoders do not support TCP-based direct connection. The settings are not effective even though you have set so on the page.

Data Backup

System > Maintenance > Data Backup

Back up database so that VMS configurations can be quickly restored by using a data backup when necessary.


Parameter Config
Backup Records
Maintenance Statistics Backup
Maintenance Statistics Backup Records
Backup Now
Save

Scheduled Backup	● On ○ Off
Backup Period	day(s)
Backup Frequency	1 day(s): perform a backup every n day(s).
Backup Time	00:00
Max. Number of Backups	30 Max number of backups to retain.

Configure scheduled backup

Configure scheduled backup on the **Parameter Config** tab so the VMS backs up databases automatically in accordance with the set period, frequency and time.

- Scheduled Backup: Select **On** to enable this function.
- Backup Period: Choose to back up by day, week or month.

  By day: Set backup frequency, that is to perform a backup every *n* days.

  By week: Choose the days of a week on which a backup will be performed.

  By month: Choose the days of a month on which a backup will be performed.
- Backup Time: Set the time to perform a backup.
- Max. Number of Backups: Set the maximum number of backup files. Up to 30 backups are allowed. When the number of backups reaches the maximum number, new backups will overwrite old backups.

Backup manually

On the **Parameter Config** tab, click **Backup Now** to perform a backup manually. A backup record appears on the **Backup Records** tab.

View backup records

View scheduled and manual backup records on the **Backup Records** tab. You can click ⇥ in the **Operation** column to export a backup file.

Use a backup to restore configurations

On the **Backup Records** tab, choose a backup record and then click ⟳ in the **Operation** column. A message appears indicating the device will restart in order to complete this operation. Click **Yes** to proceed.

Back up maintenance statistics

Create tasks to automatically back up maintenance statistics.

On the **Maintenance Statistics Backup** tab, click **Add** to create a task. Set backup period, backup frequency and backup time (see Configure scheduled backup). You can choose device type (such as encoding device, decoding device), device status (such as online/offline), export type (device or channel). You need to add recipients to receive the backup file. If the mail sending failed, a record will be generated on the **Maintenance Statistics Backup Record** tab (no record is generated if mail sending is successful). You can select one or more records and export.

Map Configuration

System > Map Config

To use image maps on the software client, select **Image Map**. To use the online map on the software client, select **Online Map** and then set longitude, latitude and initial zoom level.

NOTE!

Changing the map mode (**Image Map** or **Online Map**) will cause the software client to restart in order to apply the new setting.

5 Statistics

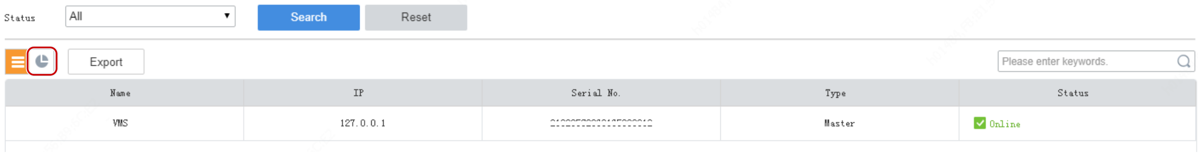
View operation statistics of the server (VMS) and the connected devices, search alarm logs of the server and devices, search operation logs of the server.

Server Statistics

Server Status

Statistics > Server > Server Status

View VMS information, including server name, IP address, serial number and status (online or offline), and export information to a CSV file. You can switch the list to a pie chart and place the mouse pointer on the pie chart to view the number and percentage.



Status: All

Name	IP	Serial No.	Type	Status
VMS	127.0.0.1	[illegible]	Master	✓ Online

S.M.A.R.T. Test

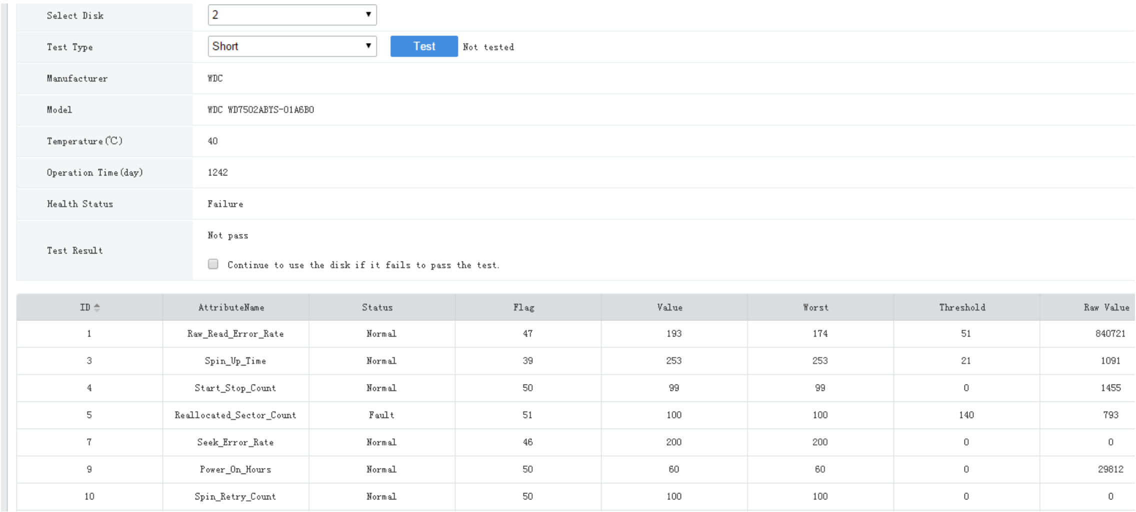
Statistics > **Server > S.M.A.R.T. Test**

Test the current health status of disks and view reference statistics after the test is finished.

The system provides three test types:

- Short: A short test checks less items than an extended test and it takes less time.
- Extended: An extended test checks more thoroughly than a short test and it takes longer time.

- Conveyance: A conveyance test mainly checks for data transmission problems.



Select Disk	2 ▾
Test Type	Short ▾ Test Not tested
Manufacturer	WDC
Model	WDC WD7502ABYS-01A6B0
Temperature(℃)	40
Operation Time(day)	1242
Health Status	Failure
Test Result	Not pass □ Continue to use the disk if it fails to pass the test.

ID	AttributeName	Status	Flag	Value	Worst	Threshold	Raw Value
1	Raw_Read_Error_Rate	Normal	47	193	174	51	840721
3	Spin_Up_Time	Normal	39	253	253	21	1091
4	Start_Stop_Count	Normal	50	99	99	0	1455
5	Reallocated_Sector_Count	Fault	51	100	100	140	793
7	Seek_Error_Rate	Normal	46	200	200	0	0
9	Power_On_Hours	Normal	50	60	60	0	29812
10	Spin_Retry_Count	Normal	50	100	100	0	0

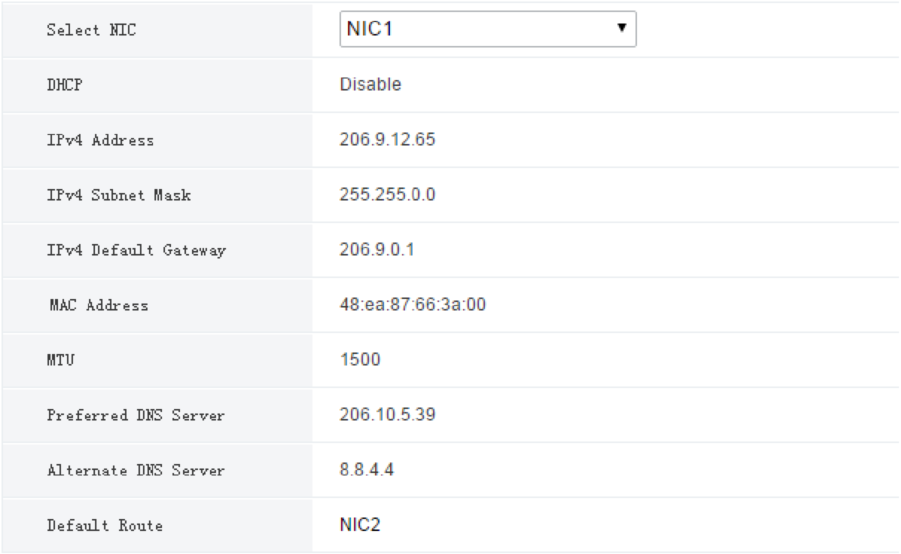
NOTE!

It is recommended to replace the disk if **Health Status** is not **Healthy**.

Network

Statistics > **Server** > **Network**

Select an NIC to view its configurations. For details, see TCP/IP.



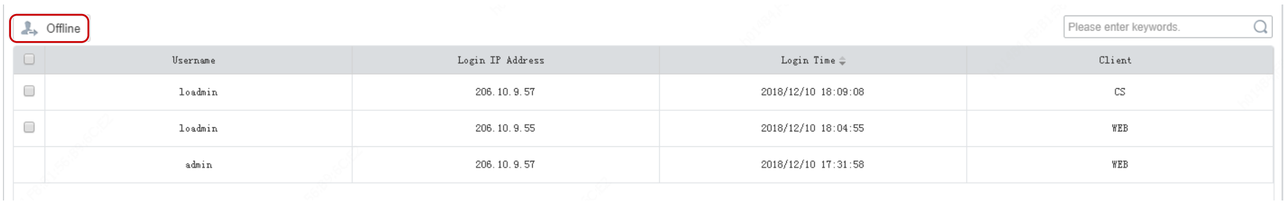
Select NIC	NIC1 ▾
DHCP	Disable
IPv4 Address	206.9.12.65
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	206.9.0.1
MAC Address	48:ea:87:66:3a:00
MTU	1500
Preferred DNS Server	206.10.5.39
Alternate DNS Server	8.8.4.4
Default Route	NIC2

Online User

Statistics > Server > Online User

View information about current online users, including username, client IP address, login time, and client type (WEB for Web client and CS for software client).

Admin can force other users to log out by selecting the target user(s) and clicking **Offline**. The target user(s) are logged out.

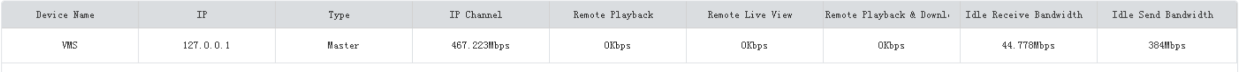


□	Username	Login IP Address	Login Time	Client
□	loadmin	206.10.9.57	2018/12/10 18:09:08	CS
□	loadmin	206.10.9.55	2018/12/10 18:04:55	WEB
	admin	206.10.9.57	2018/12/10 17:31:58	WEB

Bandwidth

Statistics > **Server** > **Bandwidth**

View the current bandwidth usage of the VMS. See Bandwidth Usage.

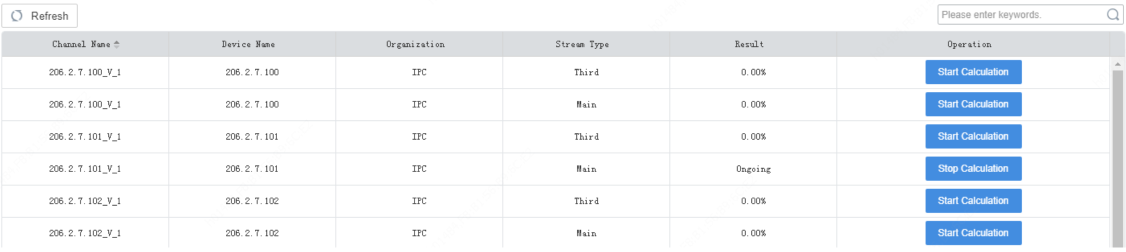


Device Name	IP	Type	IP Channel	Remote Playback	Remote Live View	Remote Playback & Downl:	Idle Receive Bandwidth	Idle Send Bandwidth
VMS	127.0.0.1	Master	467.223Mbps	0Kbps	0Kbps	0Kbps	44.778Mbps	384Mbps

Packet Loss

Statistics > Server > Packet Loss

View the packet loss rate of channels from which the VMS is receiving streams. Click **Start Calculation** and **Stop Calculation** buttons.



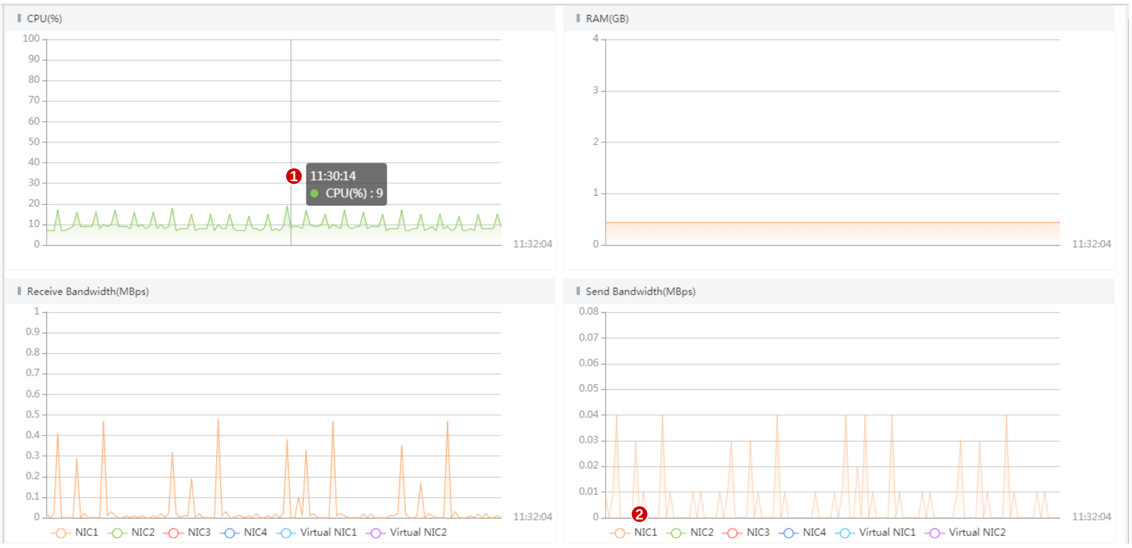
Channel Name	Device Name	Organization	Stream Type	Result	Operation
206.2.7.100_V_1	206.2.7.100	IPC	Third	0.00%	Start Calculation
206.2.7.100_V_1	206.2.7.100	IPC	Main	0.00%	Start Calculation
206.2.7.101_V_1	206.2.7.101	IPC	Third	0.00%	Start Calculation
206.2.7.101_V_1	206.2.7.101	IPC	Main	Ongoing	Stop Calculation
206.2.7.102_V_1	206.2.7.102	IPC	Third	0.00%	Start Calculation
206.2.7.102_V_1	206.2.7.102	IPC	Main	0.00%	Start Calculation

Server Performance

Statistics > Server > Server Performance

View the current CPU usage, RAM (physical memory) usage, and receive (input) and send (output) bandwidth of the VMS.

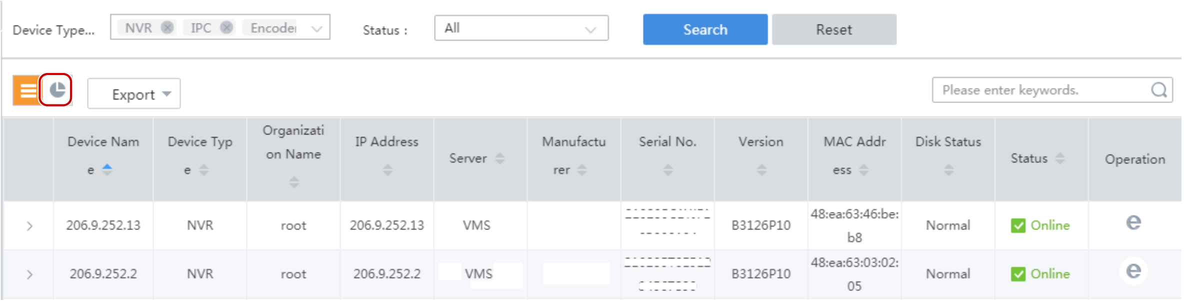
The Web client starts calculation when you open the page and displays statistics of the recent 240 seconds. Place the mouse pointer anywhere on the chart (see 1 in the figure below) to view details at the specific point. If more than one NIC is in use, statistics of the NICs are shown in different colors. You may click under x-axis (see 2 in the figure below) to collect statistics of certain NICs only. The statistics are cleared when you switch to another page.



Device Statistics

Statistics > **Device**

Search device statistics by device type and device status. Export search results to a CSV file. You can switch the list to a pie chart and place the mouse pointer on the chart to view the number and percentage.



	Device Name	Device Type	Organization Name	IP Address	Server	Manufacturer	Serial No.	Version	MAC Address	Disk Status	Status	Operation
>	206.9.252.13	NVR	root	206.9.252.13	VMS		[illegible]	B3126P10	48:ea:63:46:be:b8	Normal	☑ Online	e
>	206.9.252.2	NVR	root	206.9.252.2	VMS		[illegible]	B3126P10	48:ea:63:03:02:05	Normal	☑ Online	e

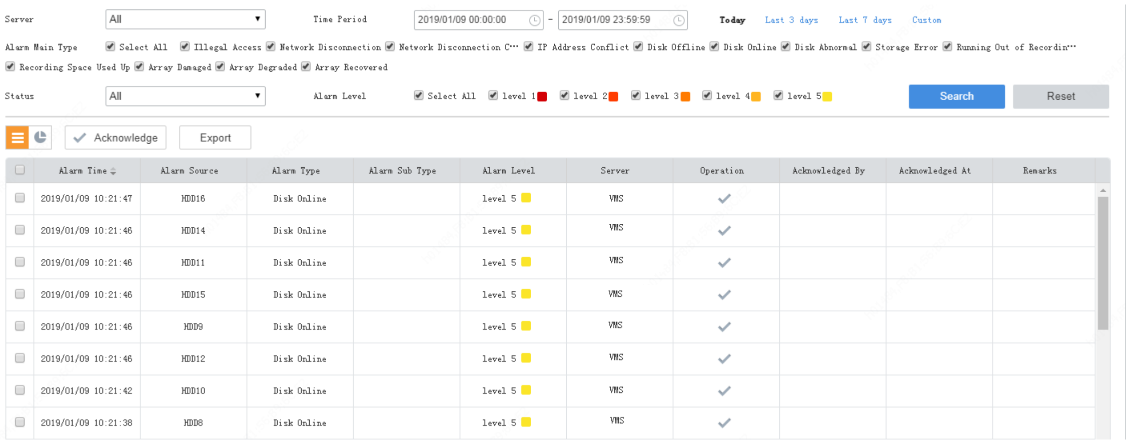
Logs

Search and export alarm logs of the VMS and devices; search and export operation logs of the VMS.

Server Alarm Logs

Statistics > Log > Server Alarm Logs

Search, acknowledge or export alarm logs of the VMS server. You can switch the list to a diagram.



Server: All

Time Period: 2019/01/09 00:00:00 - 2019/01/09 23:59:59

Alarm Main Type: ☑ Select All ☑ Illegal Access ☑ Network Disconnection ☑ Network Disconnection C··· ☑ IP Address Conflict ☑ Disk Offline ☑ Disk Online ☑ Disk Abnormal ☑ Storage Error ☑ Running Out of Recordin··· ☑ Recording Space Used Up ☑ Array Damaged ☑ Array Degraded ☑ Array Recovered

Status: All

Alarm Level: ☑ Select All ☑ level 1🟥 ☑ level 2🟥 ☑ level 3🟧 ☑ level 4🟧 ☑ level 5🟨

□	Alarm Time	Alarm Source	Alarm Type	Alarm Sub Type	Alarm Level	Server	Operation	Acknowledged By	Acknowledged At	Remarks
□	2019/01/09 10:21:47	HDD16	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:46	HDD14	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:46	HDD11	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:46	HDD15	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:46	HDD9	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:46	HDD12	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:42	HDD10	Disk Online		level 5 🟨	VMS	✓			
□	2019/01/09 10:21:38	HDD8	Disk Online		level 5 🟨	VMS	✓			

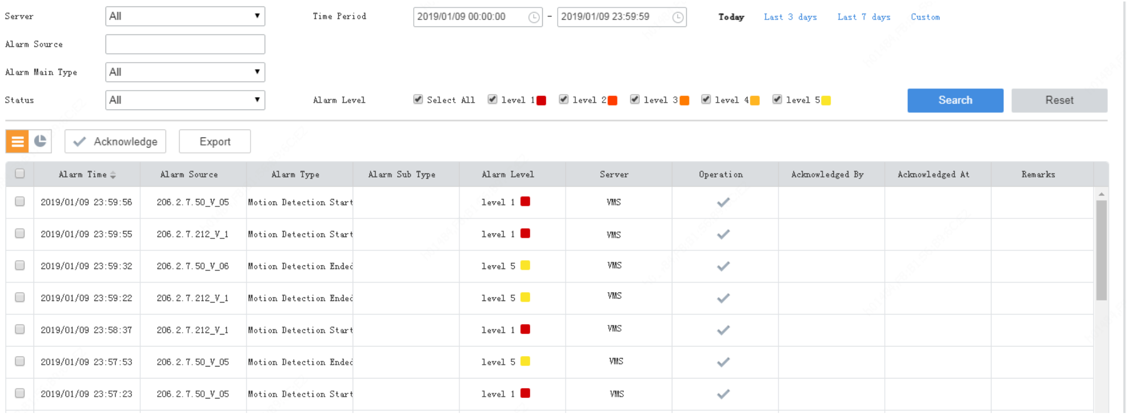
NOTE!

The acknowledge operation is irreversible. Acknowledged status cannot be revoked.

Device Alarm Logs

Statistics > Log > Device Alarm Logs

Search, acknowledge and export alarm logs of devices managed by the VMS.



Server: All

Time Period: 2019/01/09 00:00:00 - 2019/01/09 23:59:59

Alarm Source:

Alarm Main Type: All

Status: All

Alarm Level: ☑ Select All ☑ level 1🟥 ☑ level 2🟥 ☑ level 3🟧 ☑ level 4🟧 ☑ level 5🟨

□	Alarm Time	Alarm Source	Alarm Type	Alarm Sub Type	Alarm Level	Server	Operation	Acknowledged By	Acknowledged At	Remarks
□	2019/01/09 23:59:56	206.2.7.50_V_05	Motion Detection Start		level 1 🟥	VMS	✓			
□	2019/01/09 23:59:55	206.2.7.212_V_1	Motion Detection Start		level 1 🟥	VMS	✓			
□	2019/01/09 23:59:32	206.2.7.50_V_06	Motion Detection Endec		level 5 🟨	VMS	✓			
□	2019/01/09 23:59:22	206.2.7.212_V_1	Motion Detection Endec		level 5 🟨	VMS	✓			
□	2019/01/09 23:58:37	206.2.7.212_V_1	Motion Detection Start		level 1 🟥	VMS	✓			
□	2019/01/09 23:57:53	206.2.7.50_V_05	Motion Detection Endec		level 5 🟨	VMS	✓			
□	2019/01/09 23:57:23	206.2.7.50_V_05	Motion Detection Start		level 1 🟥	VMS	✓			

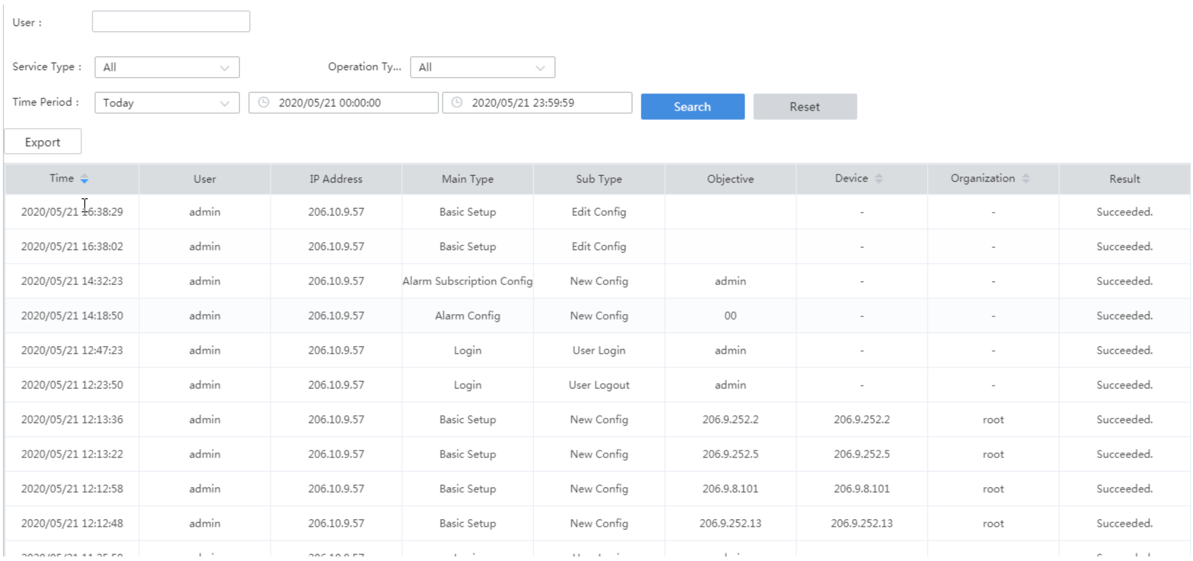
NOTE!

The acknowledge operation is irreversible. Acknowledged status cannot be revoked.

Operation Logs

Statistics > Log > Operation Logs

Search and export user operation logs.



User :

Service Type : All

Operation Ty... All

Time Period : Today 2020/05/21 00:00:00 2020/05/21 23:59:59

Time	User	IP Address	Main Type	Sub Type	Objective	Device	Organization	Result
2020/05/21 16:38:29	admin	206.10.9.57	Basic Setup	Edit Config		-	-	Succeeded.
2020/05/21 16:38:02	admin	206.10.9.57	Basic Setup	Edit Config		-	-	Succeeded.
2020/05/21 14:32:23	admin	206.10.9.57	Alarm Subscription Config	New Config	admin	-	-	Succeeded.
2020/05/21 14:18:50	admin	206.10.9.57	Alarm Config	New Config	00	-	-	Succeeded.
2020/05/21 12:47:23	admin	206.10.9.57	Login	User Login	admin	-	-	Succeeded.
2020/05/21 12:23:50	admin	206.10.9.57	Login	User Logout	admin	-	-	Succeeded.
2020/05/21 12:13:36	admin	206.10.9.57	Basic Setup	New Config	206.9.252.2	206.9.252.2	root	Succeeded.
2020/05/21 12:13:22	admin	206.10.9.57	Basic Setup	New Config	206.9.252.5	206.9.252.5	root	Succeeded.
2020/05/21 12:12:58	admin	206.10.9.57	Basic Setup	New Config	206.9.8.101	206.9.8.101	root	Succeeded.
2020/05/21 12:12:48	admin	206.10.9.57	Basic Setup	New Config	206.9.252.13	206.9.252.13	root	Succeeded.

NOTE!

For operation logs of playing live or recorded video on video wall, the objective is in this format: video wall name/screen number/window number. If video wall name/screen number/window number is followed by "-", the information following "-" indicates encoding channel/stream type by default (if not modified by user). For example, -203.130.1.35-1/0, where 203.130.1.35-1 indicates the 1st encoding channel of the encoding device with the IP address 203.130.1.35; 0: main stream (1: sub stream, 2: third stream).

6 Access Control

Permissions

Access Control > Permissions

Manage time templates, door groups and access permissions.

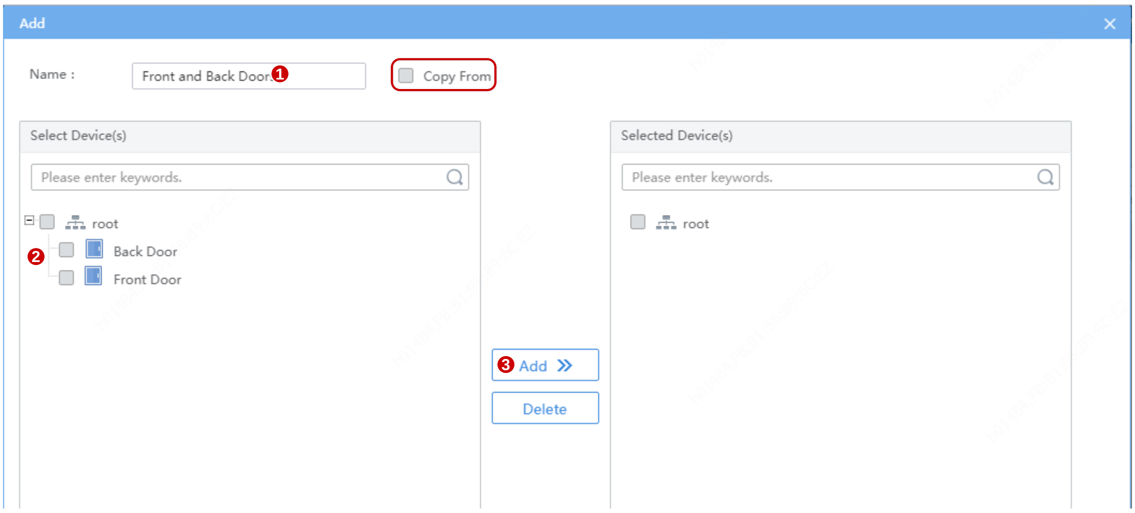
Time Template

Use a time template to restrict access time. You will need to choose a time template when configuring access permissions.

All-day is the default template in the system which can be edited but cannot be deleted. Using this template means there are no restrictions on access time. See User Time Template in User Management. The configuration steps are similar.

Door Group

A door group is a group of doors, which provides convenience when you assign access permissions. Doors must be added first at **Basic** > **Device**. See Access Controller and Door Channel for details.



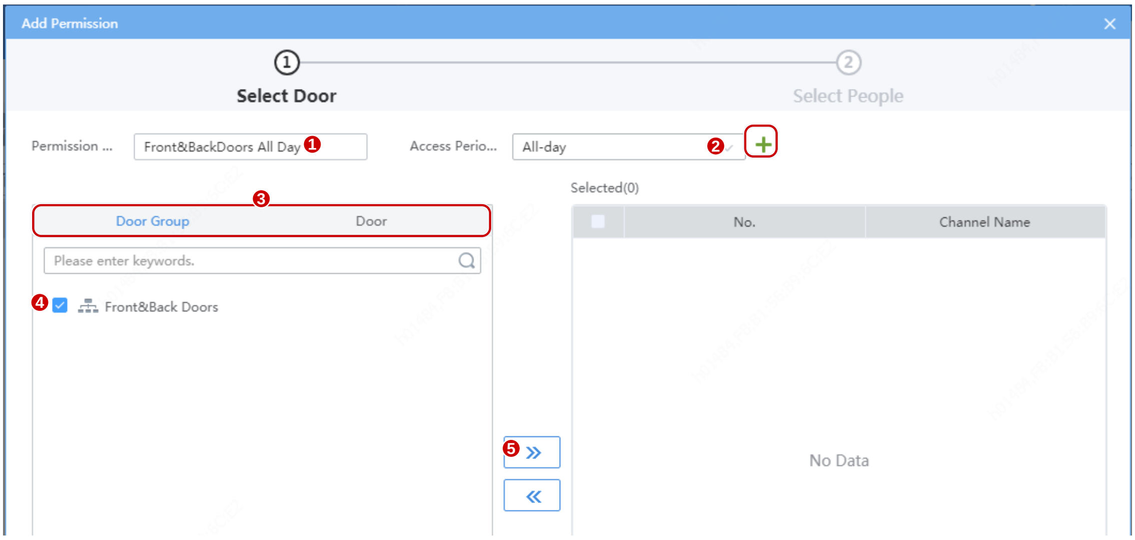
Note!

You can select **Copy From** and copy settings from an existing door group.

Assign Access Permission

Assign permissions so the specified persons have access to the specified doors during the specified time.

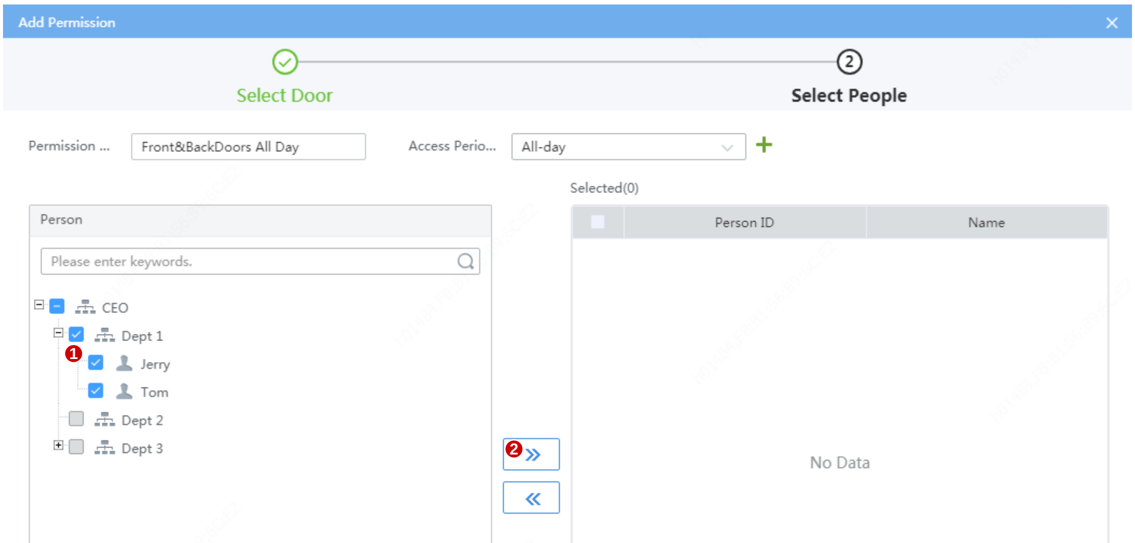
1. Select doors.



NOTE!

- Step 2: You can choose an existing time template or create a new one to restrict access time.
- Step 3: You can click the **Door Group** or **Door** tab and then select door group(s) or door(s) to grant access permission.

2. Select person(s) to assign permissions to.



Add Permission

Select Door — Select People

Permission ...: Front&BackDoors All Day

Access Perio...: All-day

Person

Please enter keywords.

- ☐ CEO
  - ☑ Dept 1
    - ☑ Jerry
    - ☑ Tom
  - ☐ Dept 2
  - ☐ Dept 3

Selected(0)

☐	Person ID	Name

No Data

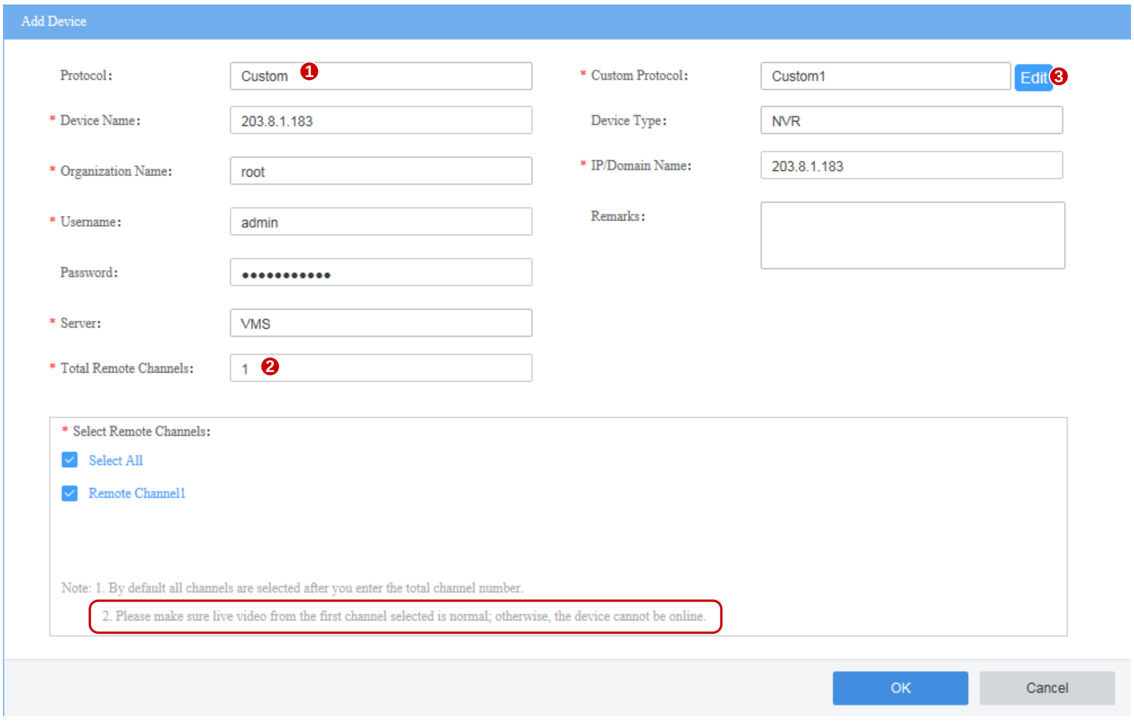
3. Click **Save**.

4. Click in the **Operation** column to check whether permissions are assigned successfully.

7 Appendix A Add a Device Using RTSP

Connect IPC or NVR via RTSP for live view.

1. Click **Add** and complete the required settings.



Add Device

Protocol: Custom

* Custom Protocol: Custom1

* Device Name: 203.8.1.183

Device Type: NVR

* Organization Name: root

* IP/Domain Name: 203.8.1.183

* Username: admin

Remarks:

Password: ●●●●●●●●●●●

* Server: VMS

* Total Remote Channels: 1

* Select Remote Channels:

☑ Select All

☑ Remote Channel1

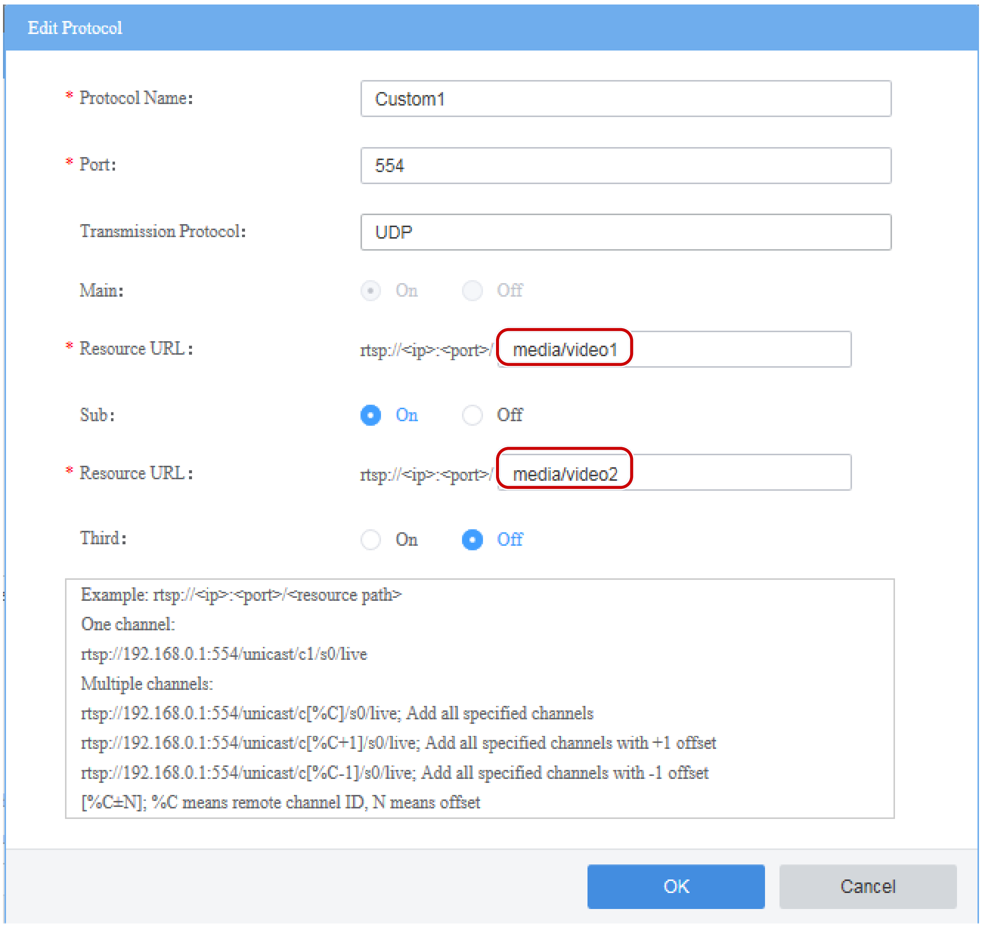
Note: 1. By default all channels are selected after you enter the total channel number.

2. Please make sure live video from the first channel selected is normal; otherwise, the device cannot be online.

NOTE!

- The **Protocol** must be set to **Custom**.
- **Total Remote Channels**: Set **1** for IPC, and fill in with the actual channel number for an NVR. Make sure live video from the first channel selected is normal; otherwise, the device cannot go online.

2. Click **Edit** and complete other settings.



Edit Protocol

* Protocol Name: Custom1

* Port: 554

Transmission Protocol: UDP

Main: ● On ○ Off

* Resource URL: rtsp://<ip>:<port>/ media/video1

Sub: ● On ○ Off

* Resource URL: rtsp://<ip>:<port>/ media/video2

Third: ○ On ● Off

Example: rtsp://<ip>:<port>/<resource path>
One channel:
rtsp://192.168.0.1:554/unicast/c1/s0/live
Multiple channels:
rtsp://192.168.0.1:554/unicast/c[%C]/s0/live; Add all specified channels
rtsp://192.168.0.1:554/unicast/c[%C+1]/s0/live; Add all specified channels with +1 offset
rtsp://192.168.0.1:554/unicast/c[%C-1]/s0/live; Add all specified channels with -1 offset
[%C±N]; %C means remote channel ID, N means offset

NOTE!

The **Resource URL** must be set in accordance with the format defined by the device manufacturer. The settings in the above figure are just an example.

3. When the device is added and gets online, you can play live video on the client.

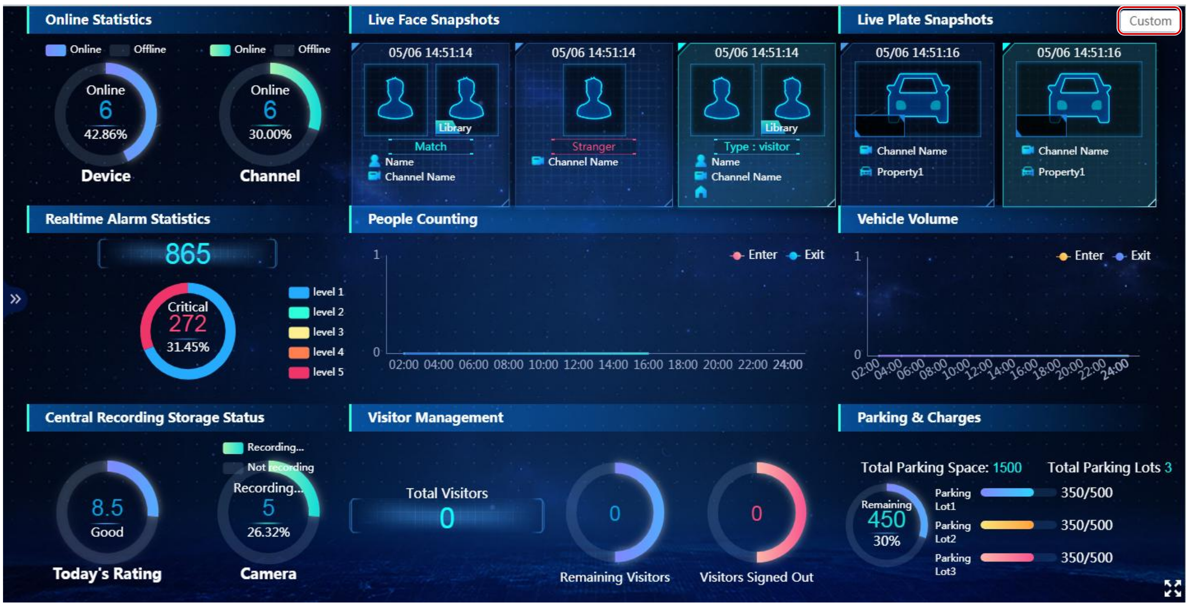
8 Appendix B Customize Comprehensive Management Dashboard

Customize the comprehensive management dashboard including the data modules displayed and the dashboard layout.

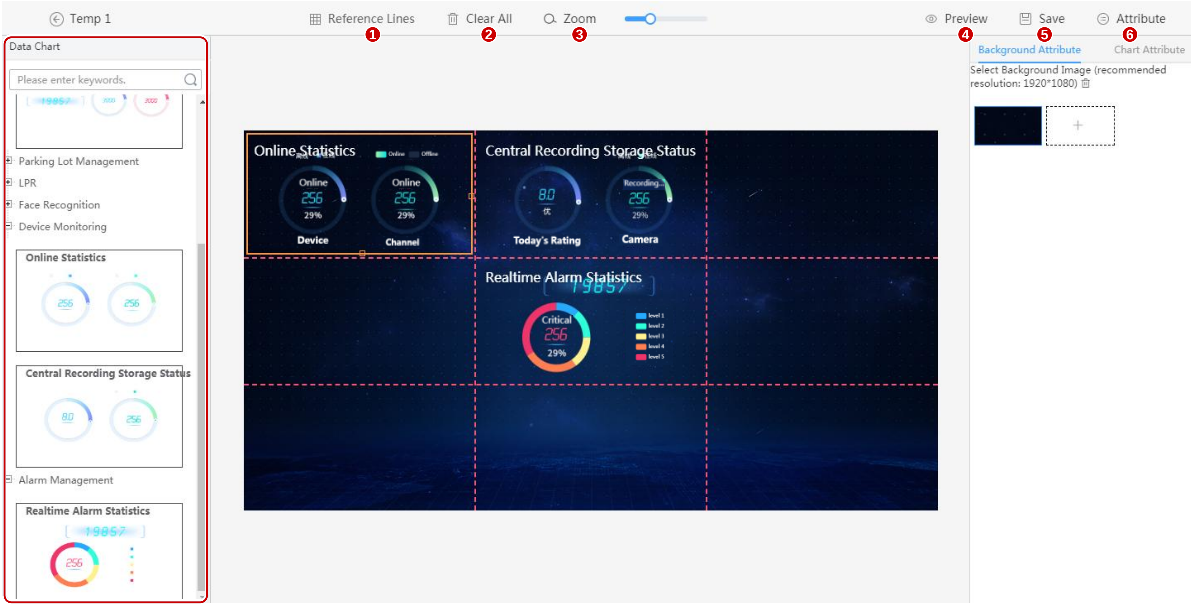
NOTE!

The figure below is only an example. The actual data modules displayed may vary depending on your device model and firmware version.

1. Click the expand button («) on the right side on the home page.
2. Click the **Custom** button in the top right corner.



3. Click ⊕ and then set the template name.
4. In the **Data Chart** area on the left, click to expand the nodes and find the data modules you want to display, and then drag the data modules to the desired positions on the panel, for example, **Online Statistics**, **Realtime Alarm Statistics**.

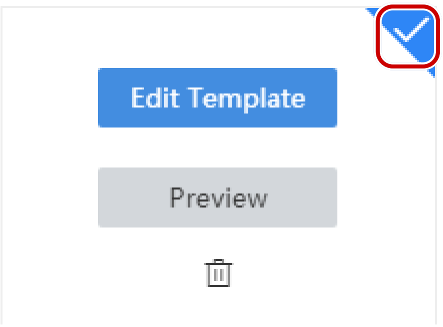


Some buttons are described as follows:

- Reference Lines: Select or customize the red dotted lines on the panel.
- Clear All: Click to remove all the data modules that are currently displayed on the panel.
- Zoom: Drag the slider to adjust the display ratio.
- Preview: Click to preview the customized dashboard.
- Save: Click to save the settings.
- Attribute: Set background attribute (background image) and chart attribute (whether to display chart title, such as Online Statistics).

5. When you complete the settings, click **Save**.

6. To enable the template, move the mouse cursor onto the template and then click in the top right corner (blue background means that the template is enabled).


Edit Template
Preview