Video Management Server
Web Manager
User Manual

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 Introduction 1

2 Login 1

3 Basic Configuration 1

Organization Management 1

General Organization 2

Custom Organization 2

User Management 4

Role 4

User 6

User Time Template 6

Person Management 7

Device Management 8

Encoding Device 8

Decoding Device 10

Smart Device 11

Network Keyboard 12

Cloud Device 12

Access Controller 13

Access Gateway 14

Alarm Control 15

Access Control 15

Encoding Channel 16

Decoding Channel 16

Alarm Channel 17

Detector Channel 17

Door Channel 18

External Alarm 18

Link Resource 19

Server Management 20

Central Server 20

Distributed Server 21

Allocate Resource 22

Batch Configuration 22

Batch Change Passwords 22

Batch Shut Down NVRs 23

Batch Scramble Streams 23

Batch Configure Encoding Parameters 24

Recording Schedule 25

Time Template 25

Recording Schedule 27

4 Alarm Configuration 28
Alarm Configuration 28
Time Template 31
Contacts 31
Custom Alarm Level 31
Alarm Subscription 32
5 Recording Backup 33
Auto Backup 33
Local Backup 35
6 System Configuration 36
Basic Configuration 36
Basic 36
Date & Time 37
DST 37
Time Sync 38
Holiday 38
Disk Configuration 38
Array Configuration 38
Disk Management 40
Network Disk 41
Capacity Allocation 41
Disk Group Property 42
Advanced Configuration 43
Network Configuration 43
TCP/IP 43
P2P 44
DDNS 45
Port 45
Port Mapping 46
Custom Route 46
Email 47
Protocols & Interconnection 47
VSS Server 47
VSS Local 49
Video&Image Database 49
Security Configuration 50
802.1x 50
ARP Protection 50
HTTPS 51
Telnet 51
Secure Password 51
IP Address Filtering 52
Maintenance 52
System Maintenance 52

Device Diagnosis Info ····· 53
Delete Logs ····· 53
Packet Capture ····· 54
Network Detect ····· 54
Bandwidth Usage ····· 54
Stream Transmission Policy ····· 55
Data Backup ····· 56
Master/Slave Switch ····· 57
Master to Slave ····· 57
Slave to Master ····· 57
Change Master Server ····· 58
Configure Hot Standby ····· 58
Map Configuration ····· 59
7 Video Service ····· 59
Live Video ····· 59
Start Live Video ····· 59
Stop Live Video ····· 60
Live Video Operations ····· 60
Playback ····· 61
Glossary ····· 61
Search Recording ····· 61
Playback Control ····· 62
Recording Download ····· 63
Local Settings ····· 65
8 Statistics ····· 66
Server Statistics ····· 66
Server Status ····· 66
S.M.A.R.T. Test ····· 66
Network ····· 67
Online User ····· 67
Bandwidth ····· 68
Packet Loss ····· 68
Server Performance ····· 68
Storage Capacity ····· 69
Recording Status ····· 70
Device Statistics ····· 70
Logs ····· 71
Server Alarm Logs ····· 71
Device Alarm Logs ····· 71
Operation Logs ····· 72
9 Access Control ····· 72
Permissions ····· 72
Time Template ····· 72
Door Group ····· 73

Assign Access Permission ····· 73
10 Appendix A Add a Device Using RTSP ····· 74
11 Appendix B Customize Comprehensive Management Dashboard ····· 76

1 Introduction

The Video Management Server (referred to as VMS hereinafter) is a new generation video management device designed to meet security surveillance needs from small and medium-sized businesses.

The VMS offers three access methods. This manual describes how to use the Web Manager.

Method	Description
Web Manager	Use a Web browser to access the VMS to manage, configure devices and services and perform maintenance operations. Simple video service is available on the Web Manager.
Client Software	Access the VMS through the client software installed on your computer to perform service operations.
Mobile app	Access the VMS through the app for live view, playback and device management.

2 Login

Use a Web browser to log in to the VMS:

1. Open your Web browser and then enter the VMS' IP address in the address bar, e.g., 192.168.1.60.
2. Enter the username and password to log in. The default username/password: admin/123456.
3. Change the password after login.

CAUTION!

- Set a strong password when you are logged in. A strong password consists of at least eight characters including digits, upper case and lower case letters, and special characters. For security concerns, access from the Internet using a weak password will be denied until a strong password is set on the LAN.
- If you forgot your password, click **Forgot Password** above the **Login** button and follow the on-screen instructions to obtain a temporary password. The temporary password is applicable to admin and invalid on a Local Area Network (LAN) on the current day. Please reset the password when logged in.

3 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 can 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 from which 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

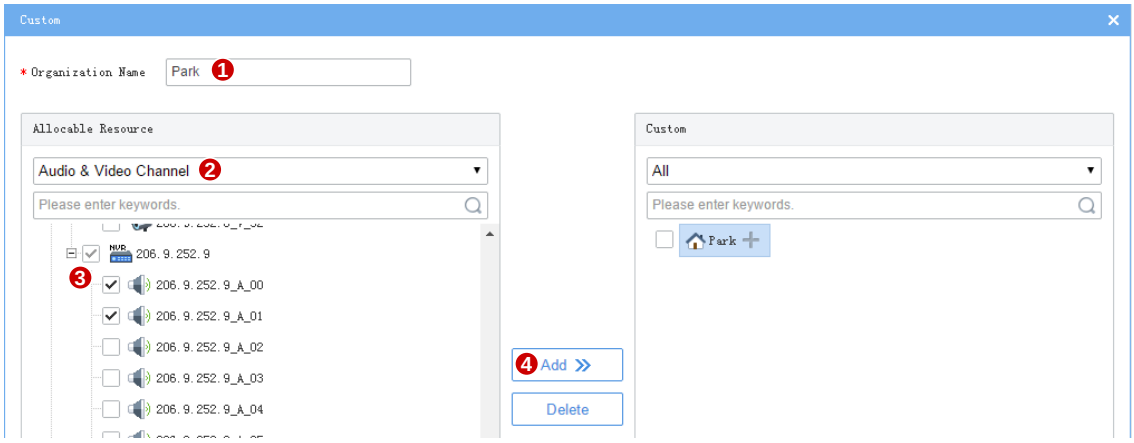
Basic > **Organization** > **Custom**

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

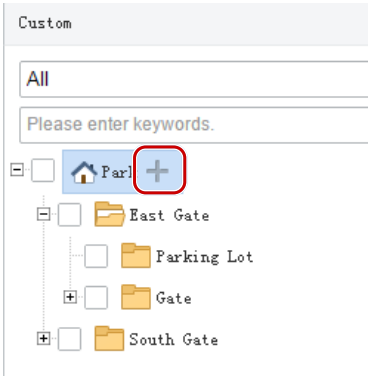
- Assign cameras under an NVR to different organizations.
- Assign cameras under different NVRs to one organization.
- Assign a camera to different organizations at the same time.
- Assign a custom organization to a role, so that users with this role can access certain resources on the software client.
- Assign resources of different types (e.g., audio & video channel) to different organizations.

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

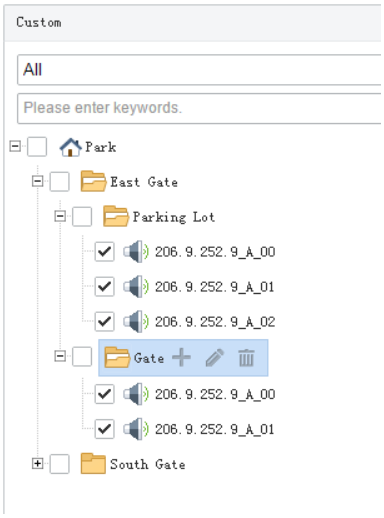
1. Enter a name. The organization name appears on the right.
2. (Optional) Select resource type (Audio & Video Channel). Enter keywords to filter if necessary.



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.

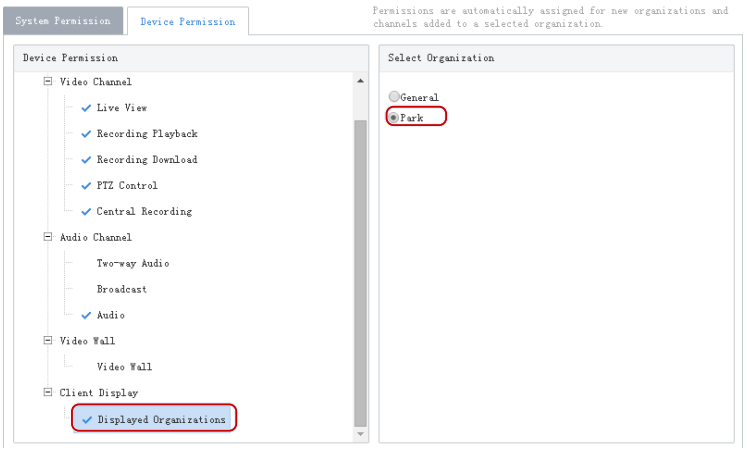


5. Click an organization on the right, select resources on the left, and then click **Add**. The selected resources are allocated to the organization. A resource can be allocated to multiple organizations (see figure below).



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.



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

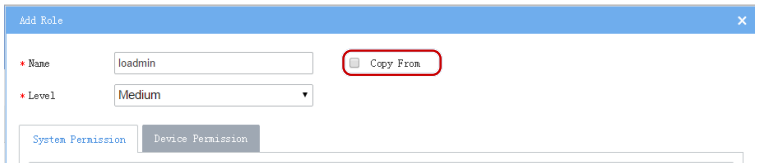
Basic > **User** > **Role**

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

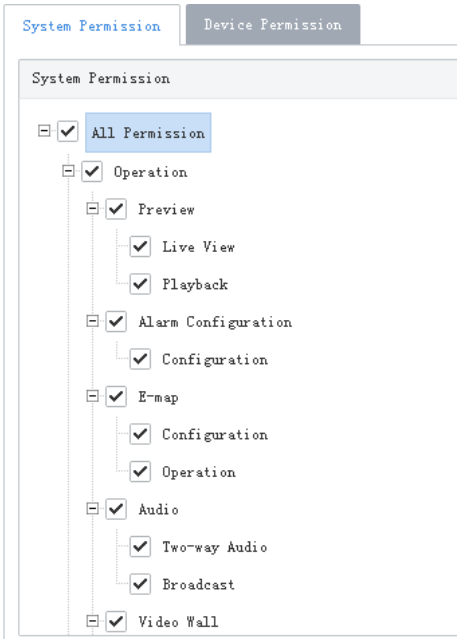
- **System Permission**: including operation permission (on software client) and management permissions (on Web Manager).
- **Device Permission**: Permission to access functions when using a device. You need to select permissions and specify allowed organizations or channels.
- **Level**: Used to differentiate 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:

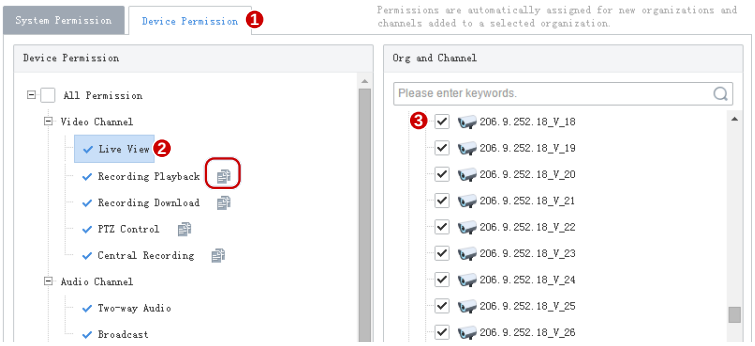
1. Enter the role name.
2. Select a level.
3. (Optional) Select **Copy From**. The existing roles in the system are listed. Select a role and then edit permissions for the new role based on the selected role. Permissions of the selected role will not change.



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**.



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



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.

NOTE!

- Click to edit a role. Changes made to a role automatically apply to users who have this role.
- Click to delete a role. After a role is deleted, the permission(s) that the role includes are revoked from user(s) who have this role.
- The affected users need to log in again after permissions are changed.

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.

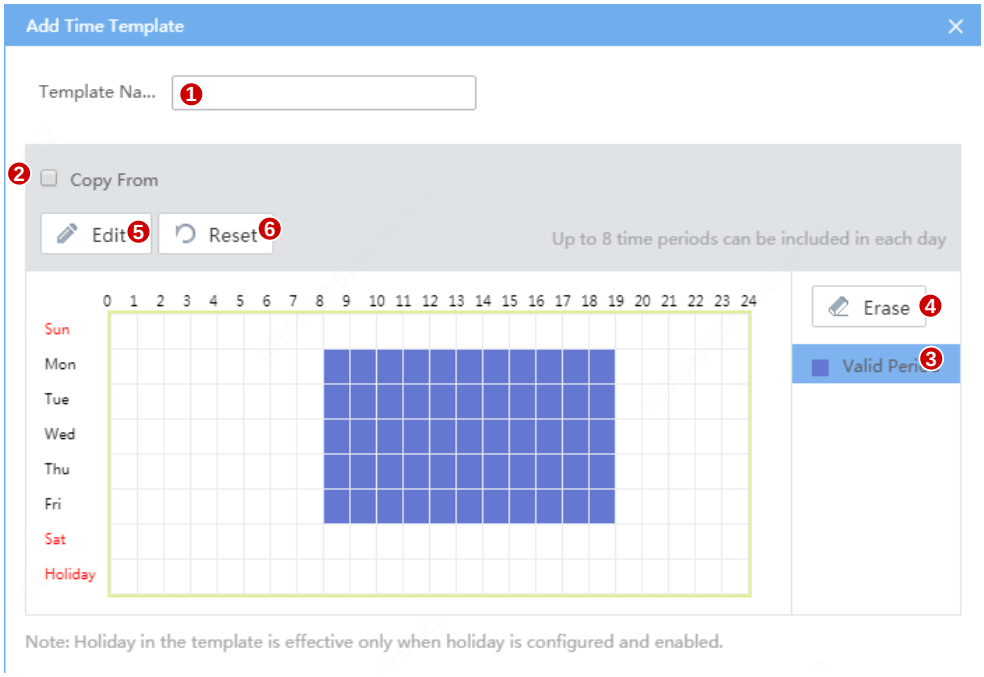
User Time Template

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.

Tip!

- All-day is the default template in the system, which you can edit but cannot delete. Using this template means there are no restrictions on login time.
- Up to 8 periods are allowed each day.
- Before configuring a valid period for holidays, you must add and enable holidays at **System** > **Basic** > **Holiday**; otherwise, the configured valid period will not be effective for the holiday.

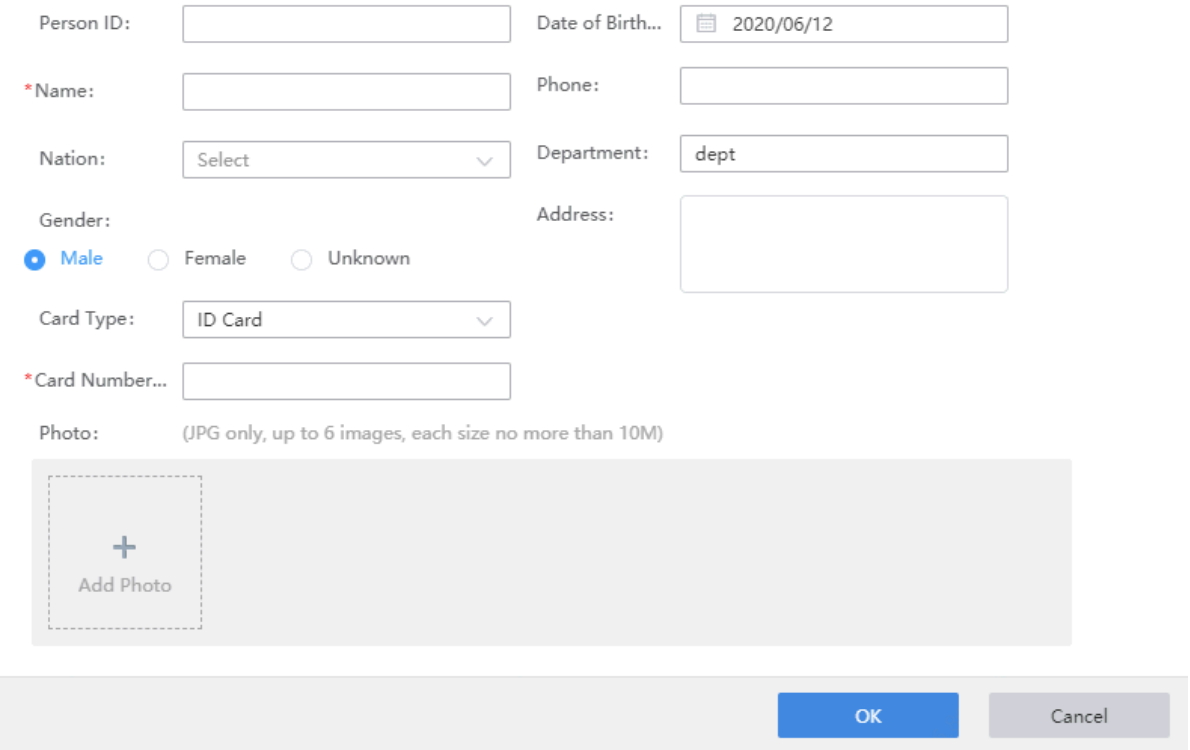


No.	Description
1	Enter a unique template name.
2	Optional. Select the checkbox and then choose an existing template to copy settings from.
3	Click the button, and then click or drag on the grid to draw a schedule. Purple means login is allowed, and white means login is forbidden.
4	Click the button, and then click or drag on the grid to erase.
5	Click to set more precisely. After settings are completed for one day, you can use the **Copy To** feature to apply the same settings to other day(s): select the day(s) and then click **Copy**.
6	Click to erase all settings on the grid.

Person Management

Basic > **Person**

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



Device Management

Encoding Device

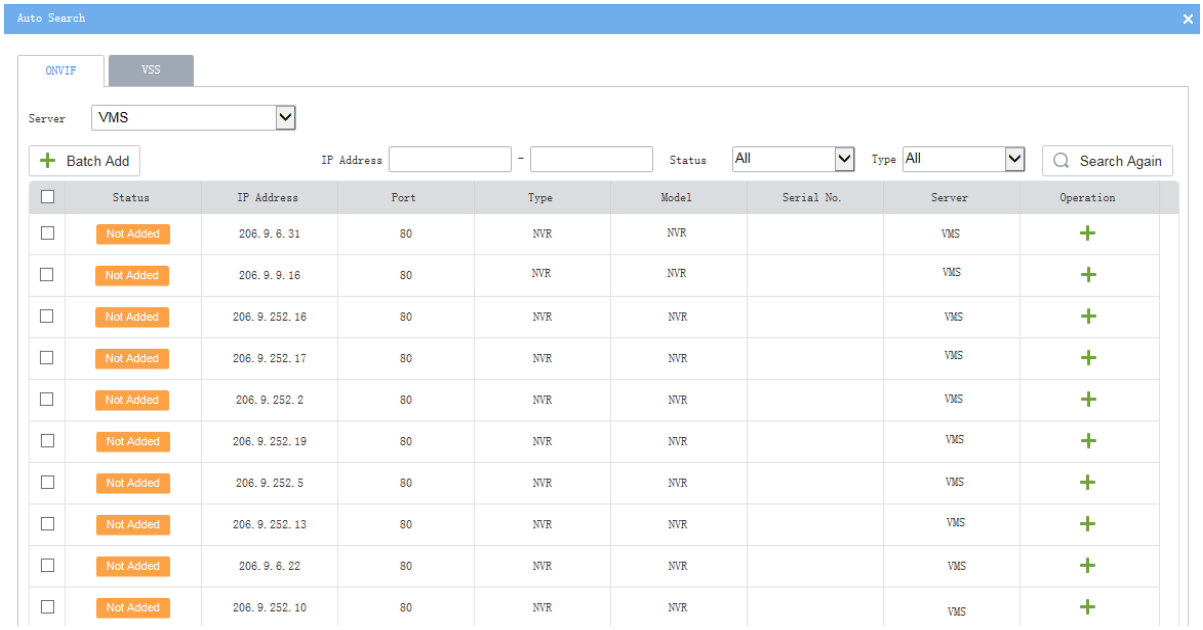
Basic > **Device** > **Device > Encoding Device**

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.



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:

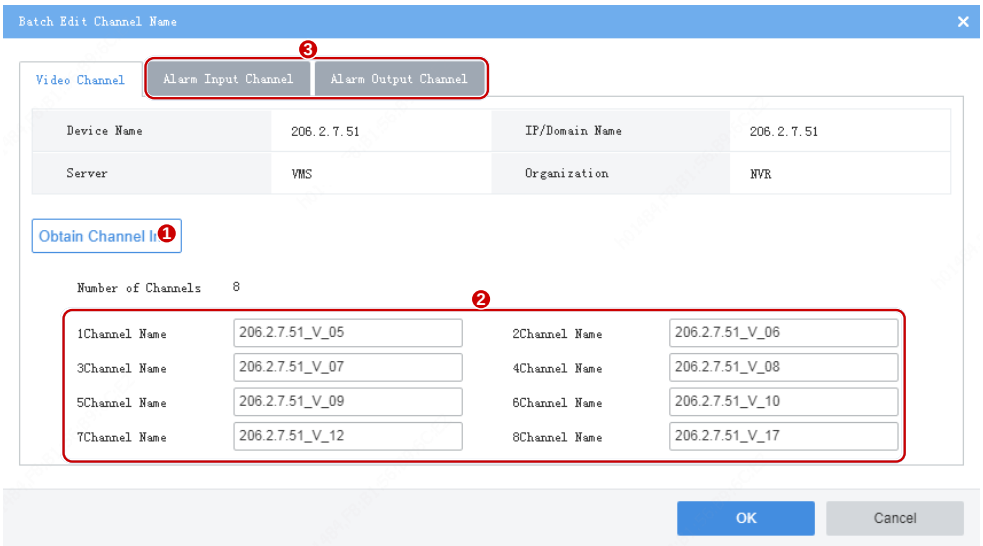
- **Server**: Search devices under the specified server (in master/slave configuration).
- **IP**: Search devices within the specified IP range.
- Filter devices by status (added or not) and type (IPC, NVR).
- Click the **VSS** tab to search for VSS devices only. You need to complete VSS configuration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



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

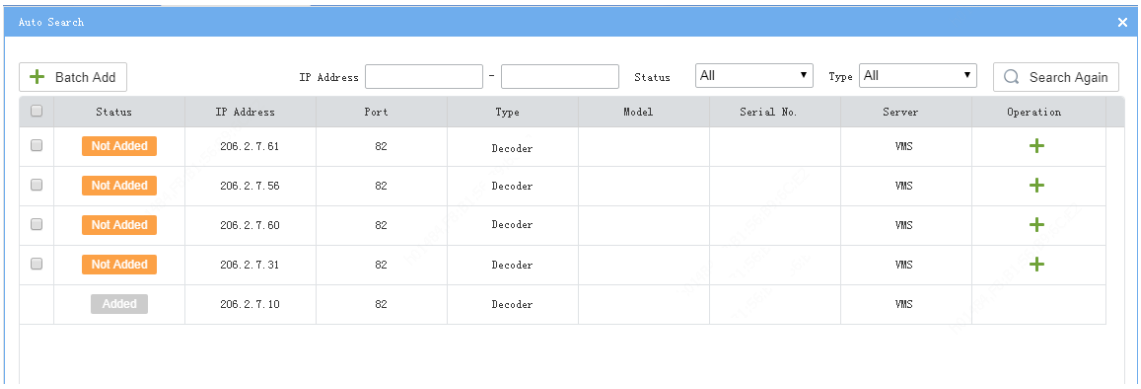
Basic > **Device** > **Device > Decoder**

Decoding devices include the VMS' built-in decoder, decoding card (sold separately), and external decoding device.

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.



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.
- If a decoding card is installed, then DC_2 or DC_3 is displayed as **Online**, depending on the installation slot (DC_2 for SLOT0, and DC_3 for SLOT1). You may rename the device by clicking .

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.

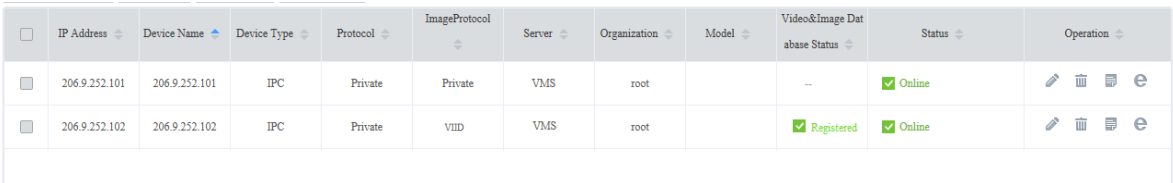
1. Click the **Auto Search** or **Add** button to add devices (see Encoding Device).

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; otherwise, 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	
206.9.252.102	206.9.252.102	IPC	Private	VIID	VMS	root		Registered	Online	

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

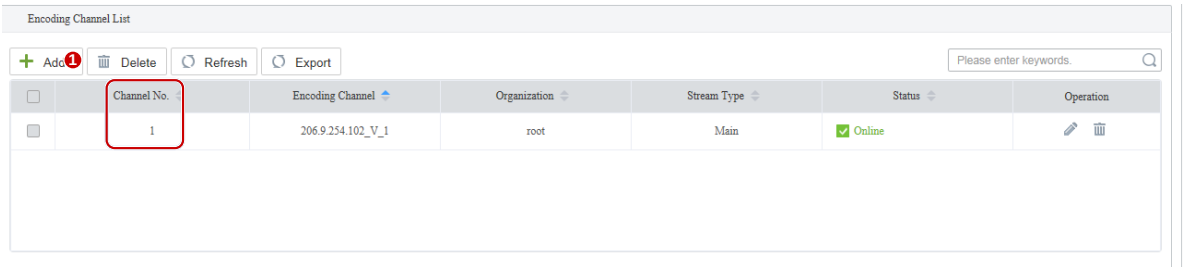
Basic > **Device** > **Device > Network Keyboard**

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

NOTE!

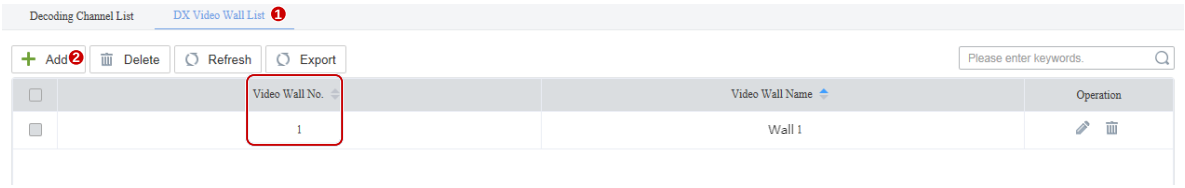
First refer to the Network Keyboard User Manual to set up the keyboard, including its registration with the VMS (by inputting the VMS' IP/port on the keyboard). And then follow the steps below to specify the video channel(s), decoding channel(s) or video wall(s) that you want to control using the keyboard.

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



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

3. To use the keyboard with a DX video wall or a decoding card 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).



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.

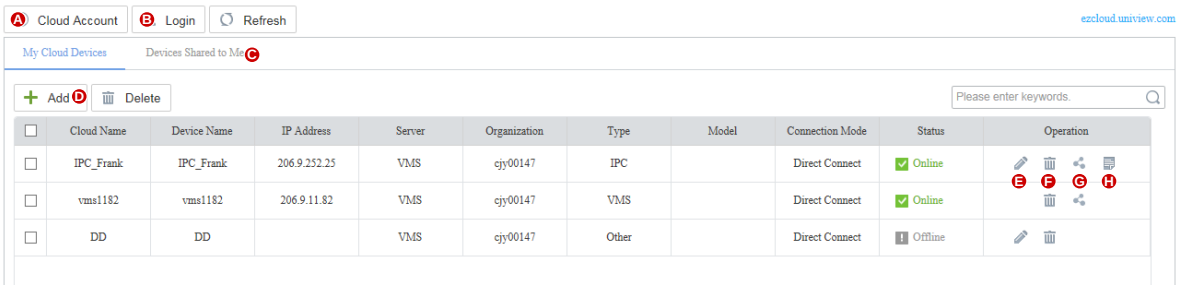
Cloud Device

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 P2P 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.



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. You can specify the server in master/slave configuration. 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 and change the server that the device belongs to (in master/slave configuration). 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 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**.

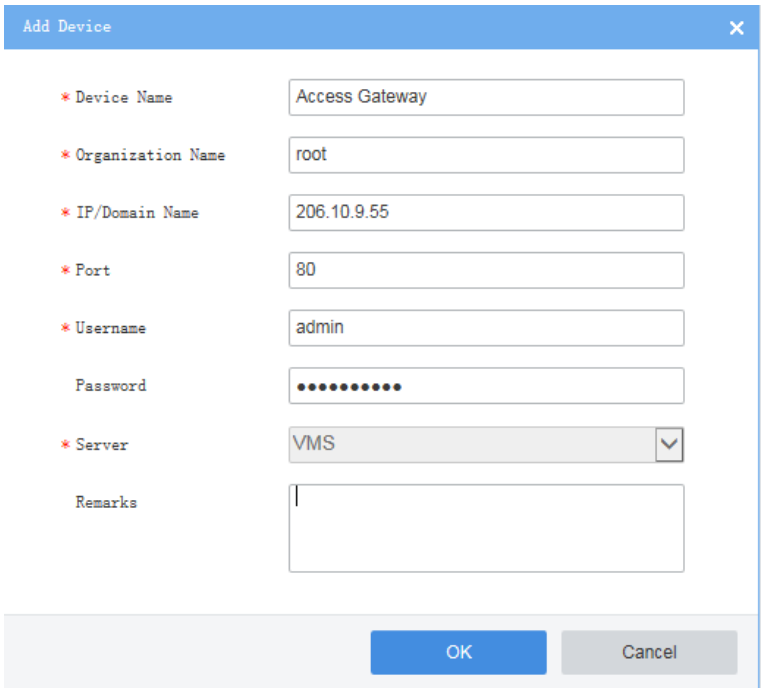
1. Click the **Auto Search** or **Add** button to add devices (see Encoding Device).
2. Make sure you select the correct access control type and set the correct IP/port.
3. Check whether the device status is **Online**. A door channel is added automatically if the added access controller is online.

Access Gateway

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

Add an access gateway 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 Guard Agent User Manual for more information about the access gateway.

1. Click **Add**.



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 access gateway.
- The **Password** is the password of the access gateway.

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!

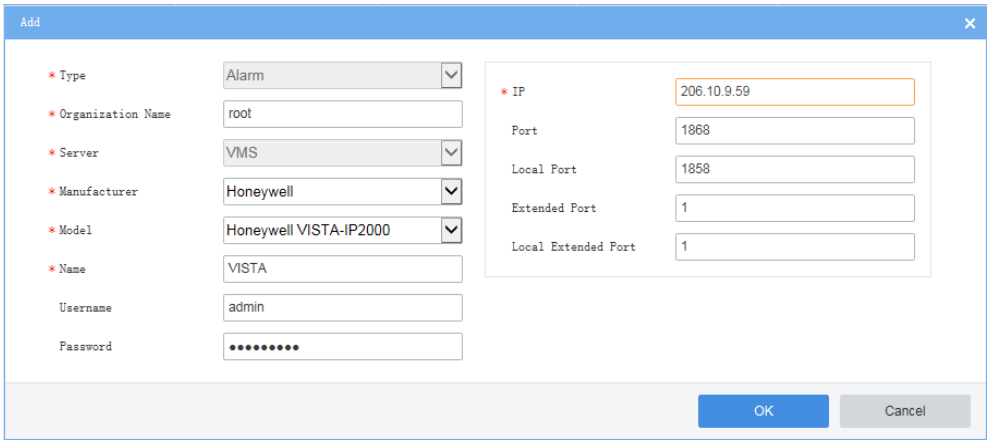
For alarm controllers and access controllers that are connected to the VMS via gateway, you cannot add their channels directly on the VMS' Web client; they can only be added on the access gateway.

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.



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.

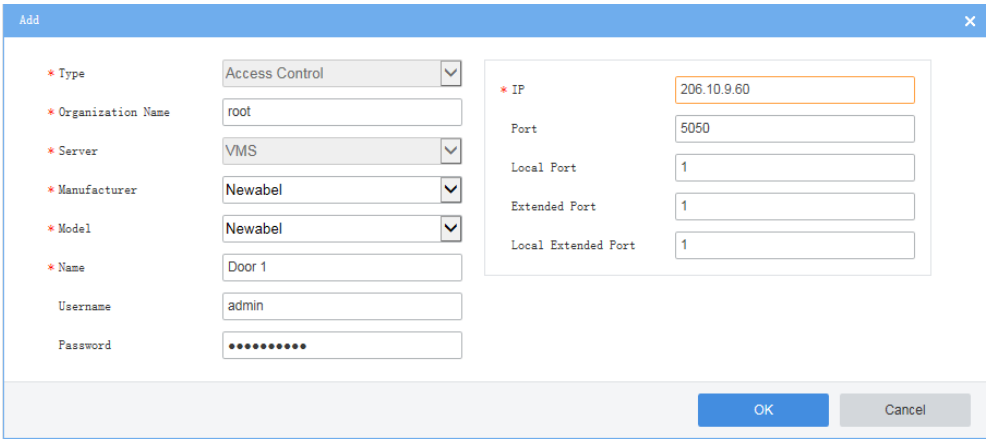
3. The added alarm controller is displayed as **Online** if it is connected.

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.



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	
206.2.7.14_V_1	206.2.7.14	1	IPC	Online	
206.2.7.15_V_1	206.2.7.15	1	IPC	Online	
206.2.7.22_V_1	206.2.7.22	1	IPC	Online	
206.2.7.16_V_1	206.2.7.16	1	IPC	Online	
206.2.7.17_V_1	206.2.7.17	1	IPC	Online	
206.2.7.18_V_1	206.2.7.18	1	IPC	Online	
206.2.7.43_V_1	206.2.7.43	1	IPC	Online	
206.2.7.42_V_1	206.2.7.42	1	IPC	Online	
206.2.7.35_V_1	206.2.7.35	1	IPC	Online	
206.2.7.59_V_1	206.2.7.59	1	IPC	Online	

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	
206.2.7.10_D_2	206.2.7.10	2	root	1080P60	16	Online	
206.2.7.10_D_3	206.2.7.10	3	root	1080P60	16	Online	
206.2.7.10_D_4	206.2.7.10	4	root	1080P60	16	Online	
206.2.7.10_D_5	206.2.7.10	5	root	1080P60	16	Online	
206.2.7.10_D_6	206.2.7.10	6	root	1080P60	16	Online	
206.2.7.10_D_7	206.2.7.10	7	root	1080P60	16	Online	
206.2.7.10_D_8	206.2.7.10	8	root	1080P60	16	Online	

NOTE!

DC_1_VGA, DC_1_HDMI1 and DC_1_HDMI2 are the decoding channels of the VMS' internal decoder DC_1.

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.

Alarm Input Channel (1) Alarm Output Channel | Batch Config (3) | Please enter keywords.

Channel Name	Device	Device ID	Organization	Channel Type	Status	Operation (2)	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.

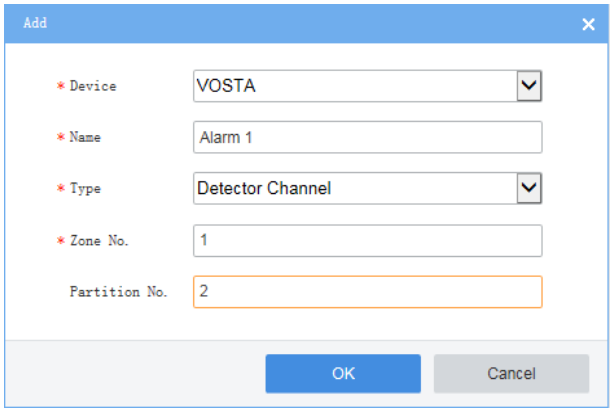
Tip!

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

Detector Channel

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

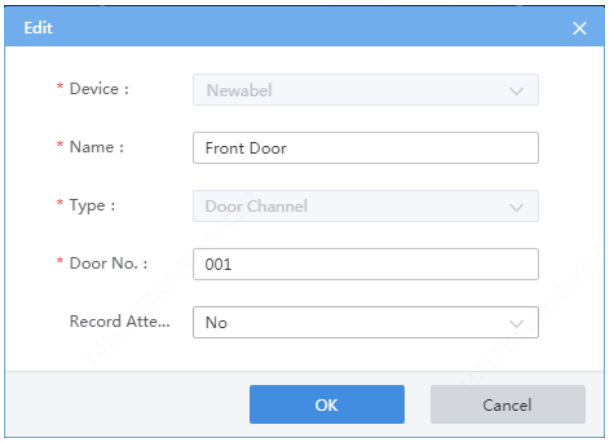
Add detector channels, zones or partitions to an alarm control device on the VMS.



Door Channel

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

A door channel is automatically added when an 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.



External Alarm

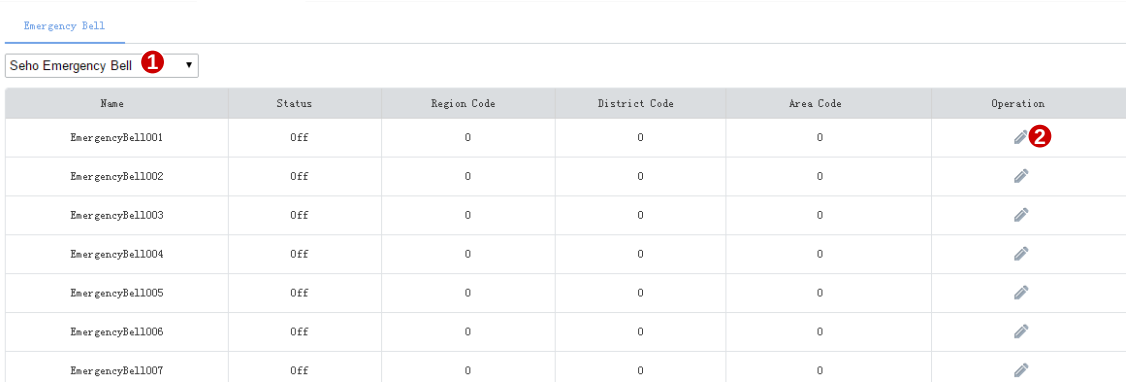
Basic > **Device** > **External Alarm**

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, recording, buzzer or email.

NOTE!

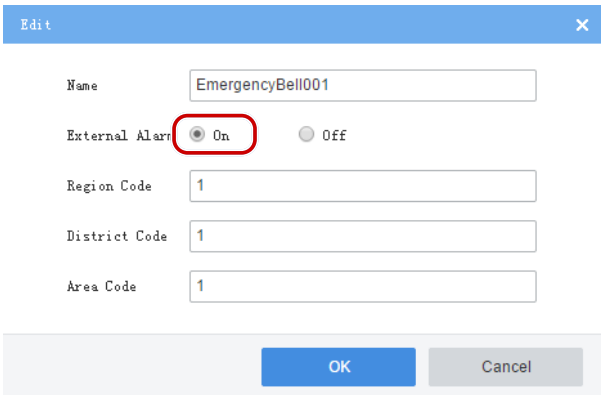
First link the emergency bell to the VMS by setting the VMS' IP and port on the emergency bell. Two emergency bell types are supported (Seho and Hitec). For Seho, the port number is 25000, and for Hitec, the port number is 9010.

1. Select an emergency bell and then configure.



Name	Status	Region Code	District Code	Area Code	Operation
EmergencyBell001	Off	0	0	0	
EmergencyBell002	Off	0	0	0	
EmergencyBell003	Off	0	0	0	
EmergencyBell004	Off	0	0	0	
EmergencyBell005	Off	0	0	0	
EmergencyBell006	Off	0	0	0	
EmergencyBell007	Off	0	0	0	

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



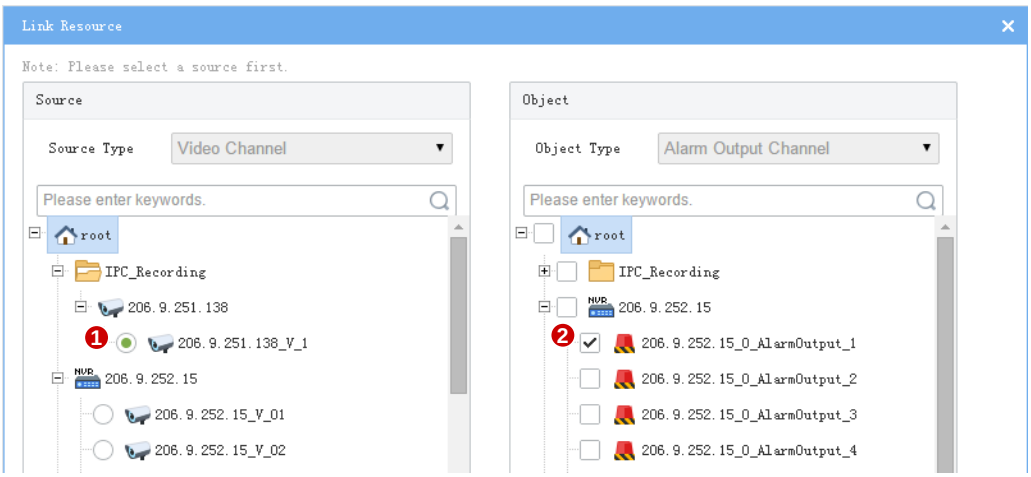
3. Configure actions to trigger. See Alarm Configuration.
4. Configure actions to trigger on the software client. See Alarm Configuration of the *Software Client User Manual*.

Link Resource

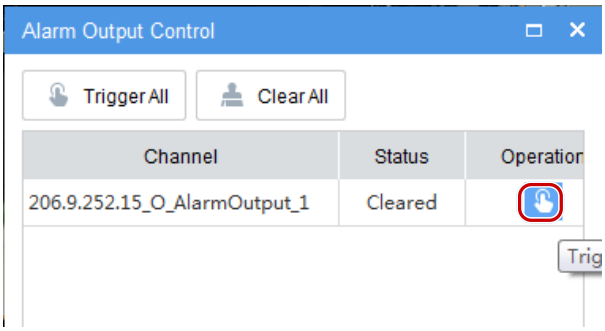
Basic > **Device** > **Link Resource**

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**.



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).



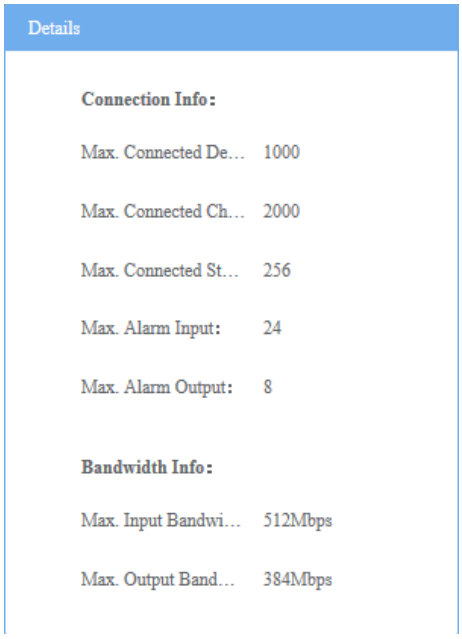
Server Management

View information and status of the central server (primary and secondary servers) and distributed server (slave server); specify working and backup slave servers; allocate device resources to master and slave servers.

Central Server

Basic > **Server** > **Central Server**

View info and status of the central server(s). Click to view connection and bandwidth info.

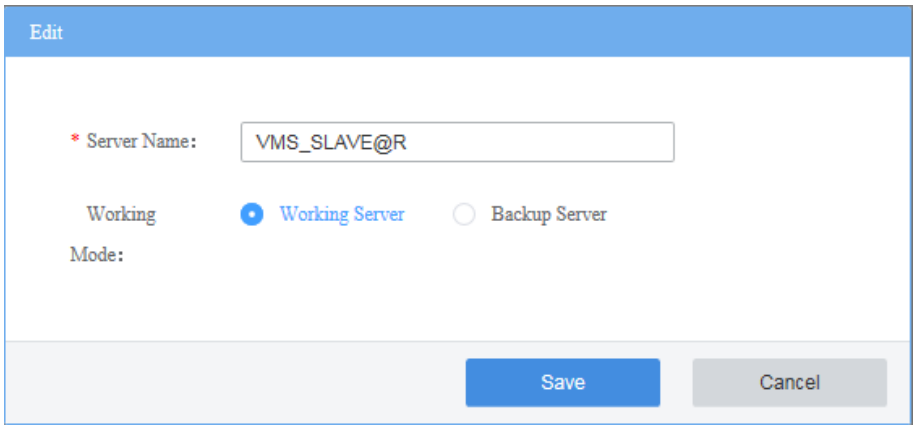


Distributed Server

Basic > **Server** > **Distributed Server**

View info and status of the slave server(s); delete a slave server from a master server; configure working and backup slave servers.

- To view the connection and bandwidth info of a slave server, click .
- To delete a slave server, click .
- To set the working mode of a slave server, click and then select **Working Server** or **Backup Server**.



Backup slave server(s) are standby in case any working slave server fails or becomes offline. If a working slave server fails or is offline (**Working Status** changes from **Normal** to **Failure**), an idle backup slave server

takes over (**Working Status** changes from **Idle** to **Taking over**). When the working server recovers to **Normal** status, it takes back over, and the backup server syncs data to the working server.

NOTE!

- Only admin can change the working mode, and changing the working mode will clear all data on the server and restart the server. However, the working mode cannot be changed if any devices exist under the server.
- A backup server can take over one working server at a time.
- Currently the backup server cannot automatically transfer recordings back to the working server.
- The backup server does not support Automatic Network Replenishment (ANR), recording backup, locking or tagging recordings.

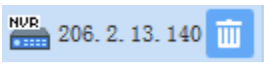
Allocate Resource

Basic > **Server** > **Allocate Resource**

Allocate devices (including cloud devices) to master or slave servers for load balance.

- Drag device(s) to the intended master or slave VMS.
- Click **Auto Assign** to assign all devices automatically.
- Click **Restore** to restore the original status displayed when the page was loaded.

Tip!

- On the device list of a slave server, deleting a device by clicking the **Delete** button (e.g., 

) removes the device from the current slave server and assigns it to the master server.
- A backup slave server is displayed only when its status is **Taking over**.

Batch Configuration

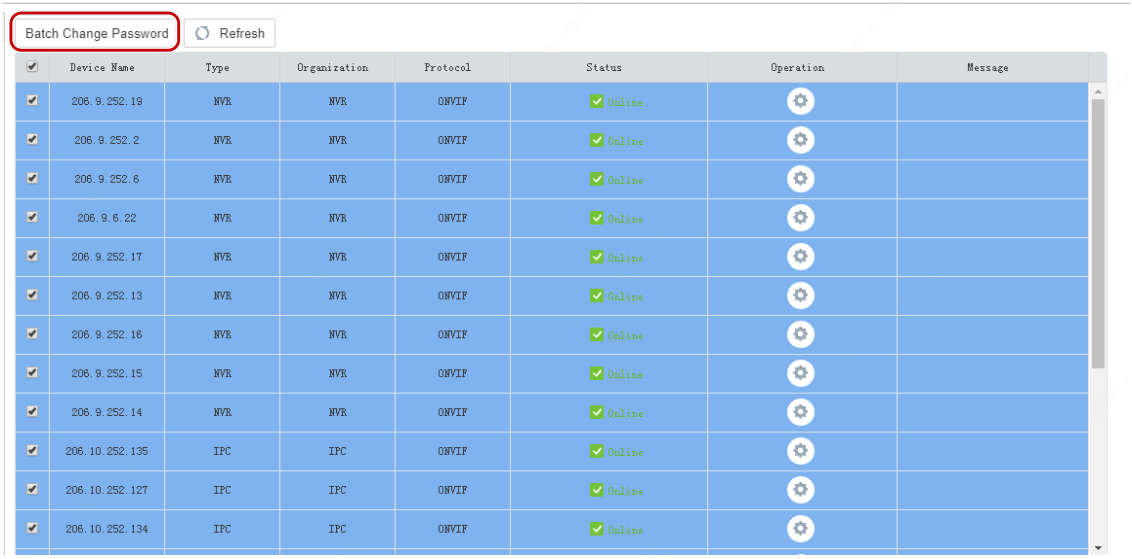
Batch Change Passwords

Basic > Batch Config> Batch Change Password

Batch change passwords of NVRs under the master or slave VMS server. For NVRs under a slave server, their passwords can only be changed from the master server.

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**.



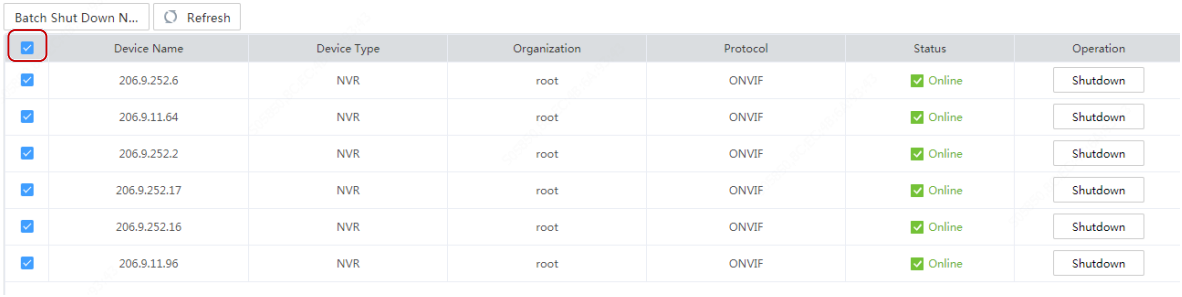
2. Enter the new passwords and then click **OK**.

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.



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

NOTE!

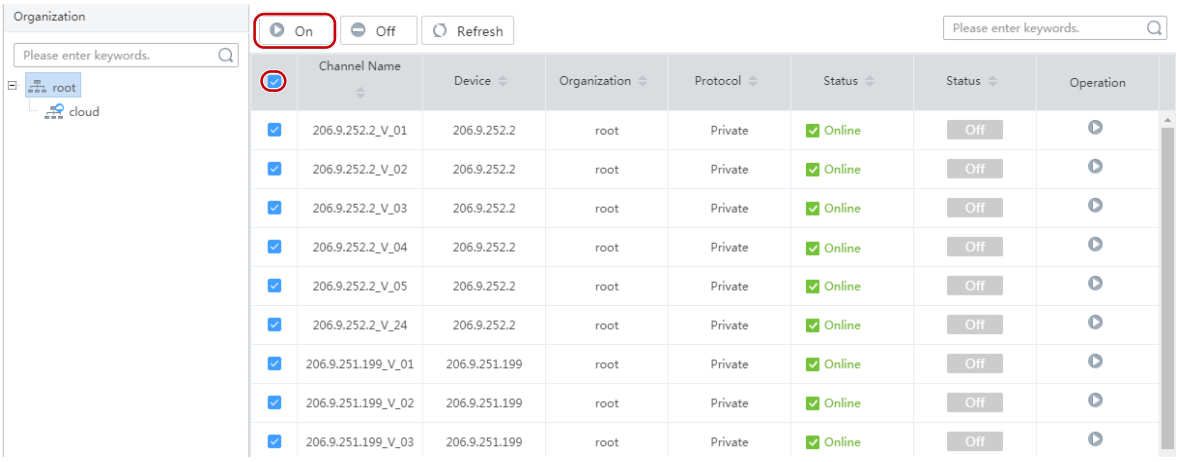
- This function is available to certain NVR versions. A message appears if the function is unavailable.
- This function is not available if the NVR is connected to the VMS via the VSS protocol.

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.



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!

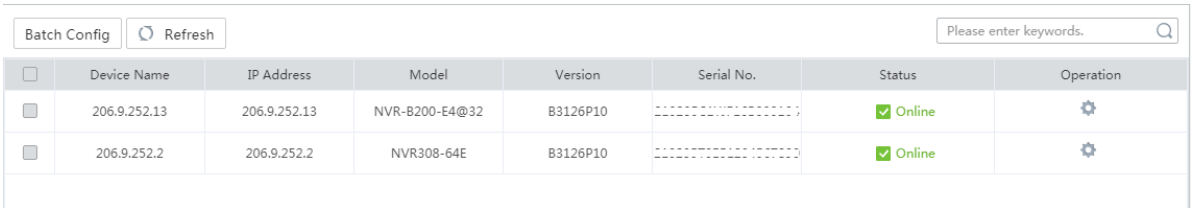
This function is available to devices connected via the private protocol.

Batch Configure Encoding Parameters

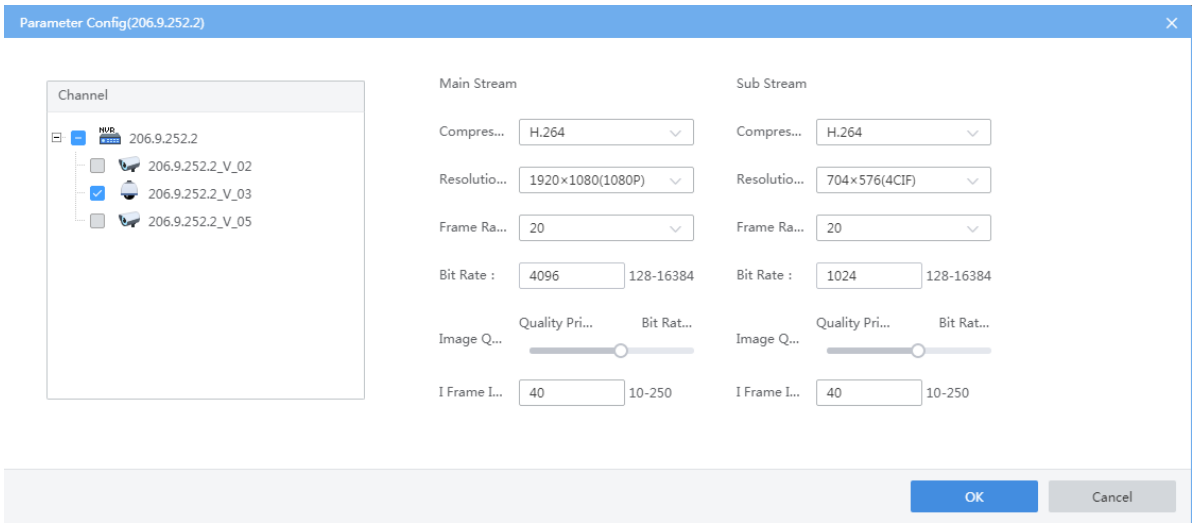
Basic > Batch Config > Batch Config Encoding Parameters

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**.



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.



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

Recording Schedule

Use recording schedules to customize recording operations for different cameras during specified time periods.

Time Template

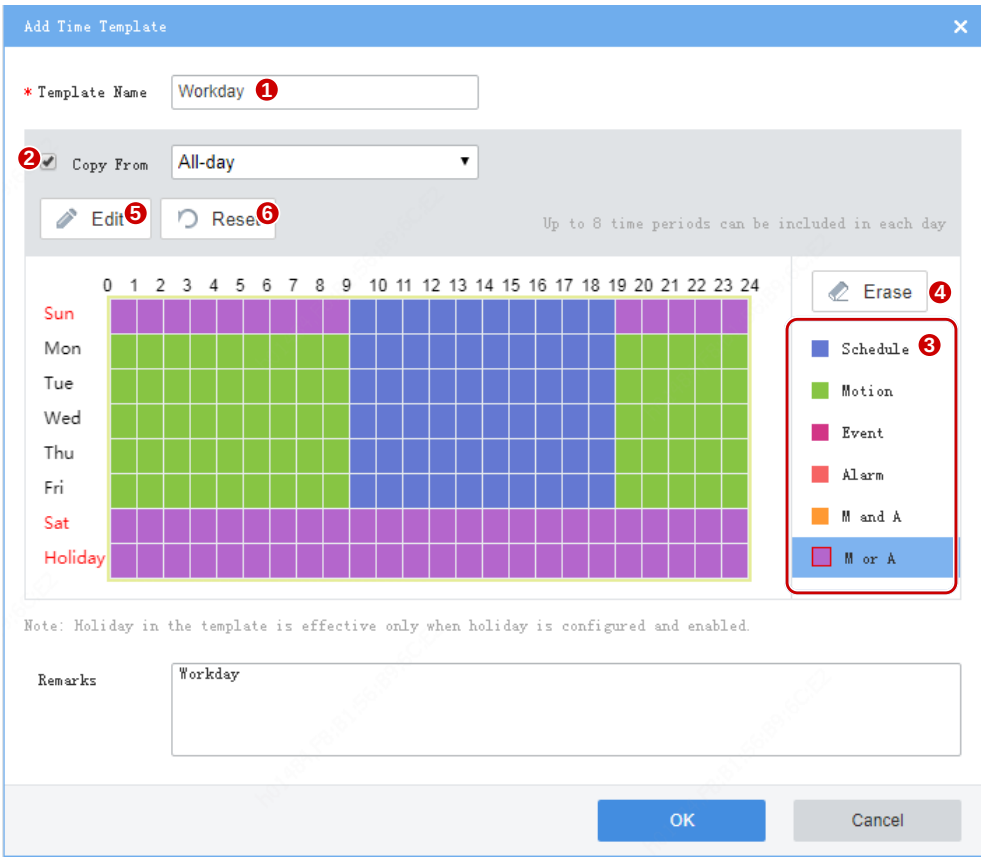
Basic > **Recording Schedule** > **Time Template**

Each recording schedule uses a time template to specify recording time and policy. The system provides a default template (All-day) which records video 24/7. You can customize time templates for your recording schedules.

NOTE!

- The default template can be renamed but cannot be deleted.
- A holiday in a time template is effective only when the holiday is configured and enabled (**System** > **Basic** > **Holiday**). See Holiday.

1. Click **Add**, and then follow the steps to create a time template.



No.	Description
1	The template name must be unique in the system.
2	Select the checkbox and then select an existing template from the drop-down list, so you can edit based on the template without configuring from scratch. The template selected will not be altered.
3	Click a type (e.g., Schedule) and then drag or click on the grid.
4	Click the button and then drag or click on the grid to delete settings.
5	Click to set more precisely. After settings are completed for one day, you can use the **Copy To** feature to apply the same settings to other day(s): select the day(s) and then click **Copy**.
6	Click to erase all settings on the grid.

2. Refer to the table below for the meanings of recording schedule types.

Type	Description
Schedule	Record video according to the time set in the schedule.
Motion	Record video when Motion Detection occurs.
Event	Record video when video loss, audio detection or an alarm other than the following occurs: motion detection, tampering detection, alarm input, auto tracking, defocus detection, and scheduled recording failure.
Alarm	Record video when tampering detection, alarm input, auto tracking, defocus detection or

Type	Description
	scheduled recording failure occurs.
M and A	M for Motion Detection and A for Alarm. Record video when motion detection AND an alarm specified in the Alarm category (e.g., tampering detection) occur simultaneously.
M or A	M for Motion Detection and A for Alarm. Record video when motion detection OR an alarm specified in the Alarm category (e.g., tampering detection) occurs.

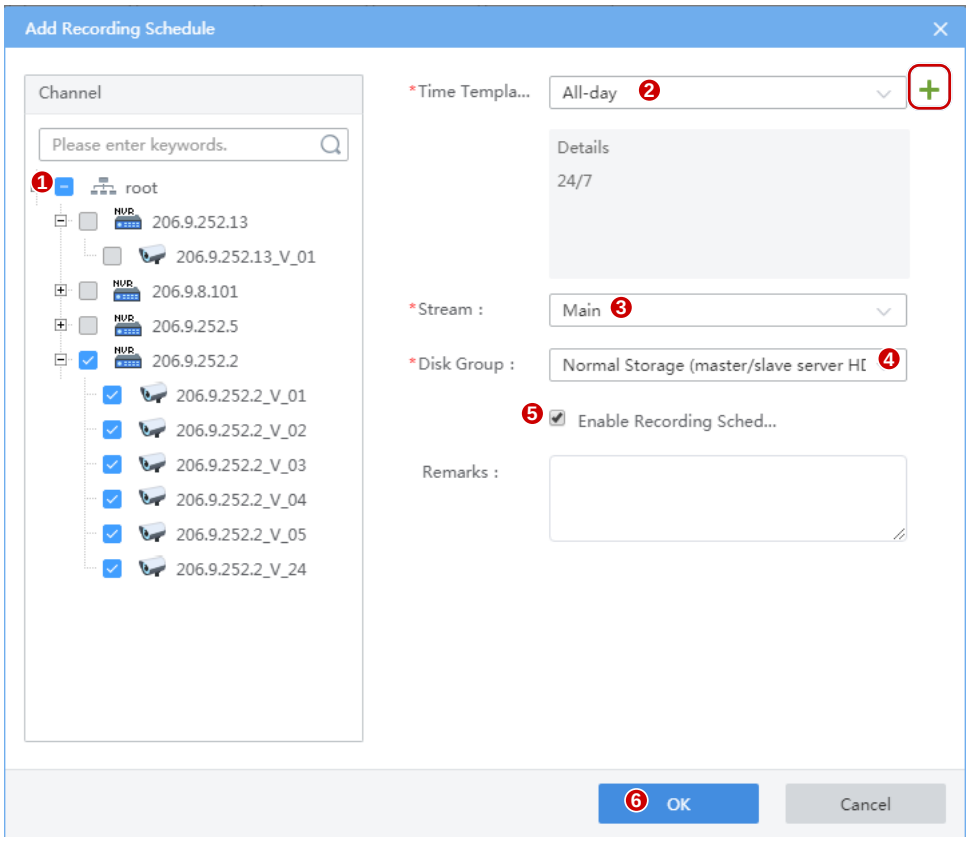
3. The new time template appears in the list and can be edited or deleted as needed.

Recording Schedule

Basic > **Recording Schedule** > **Recording Schedule**

Create a recording schedule so the VMS can record videos from specified cameras according to the set schedule, recording type, stream type, etc.

Click **Add**, and then follow the steps to add a recording schedule.



1. Select camera(s).
2. Select a time template, or click + to create one. See Time Template.
3. Select a stream type to record.
4. Select a disk group: normal storage or IPSAN.

5. By default **Enable Recording Schedule** is selected. Clearing the checkbox will disable the recording schedule.
6. Click **OK**.

NOTE!

- Before you set recording as a trigger action, make sure a correct recording schedule has been configured and enabled for the linked camera; otherwise, recording cannot be triggered as expected. For more details, see Alarm Configuration.
- The VMS supports Automatic Network Replenishment (ANR). For an ANR-enabled camera (including NVR-connected camera), if network connection is interrupted during its recording schedule, video will be saved to the camera's onboard SD card or NVR during the interruption and will be transferred automatically to the VMS when network connection is recovered.
- For third-party cameras, if the stream type selected is an unsupported video stream (e.g., MJPEG), recording will fail, and the **Diagnosis** column on the **Recording Schedule** page will indicate "unsupported encoding format".

4 Alarm Configuration

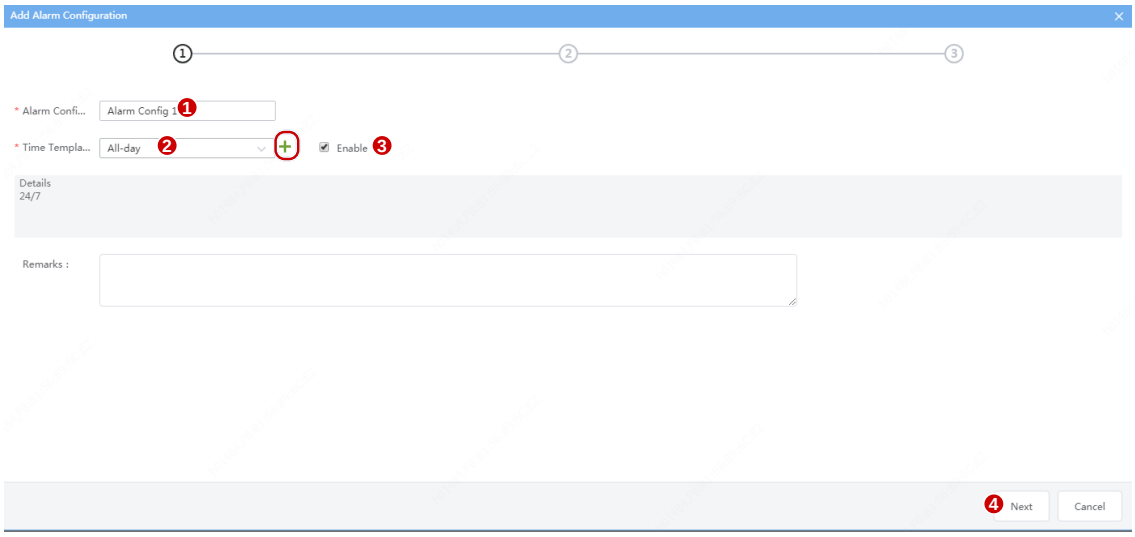
Configure alarms so that certain alarms at the specified source(s) will trigger actions such as recording, buzzer, email and snapshot.

Alarm Configuration

Alarm Configuration > **Alarm Configuration**

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

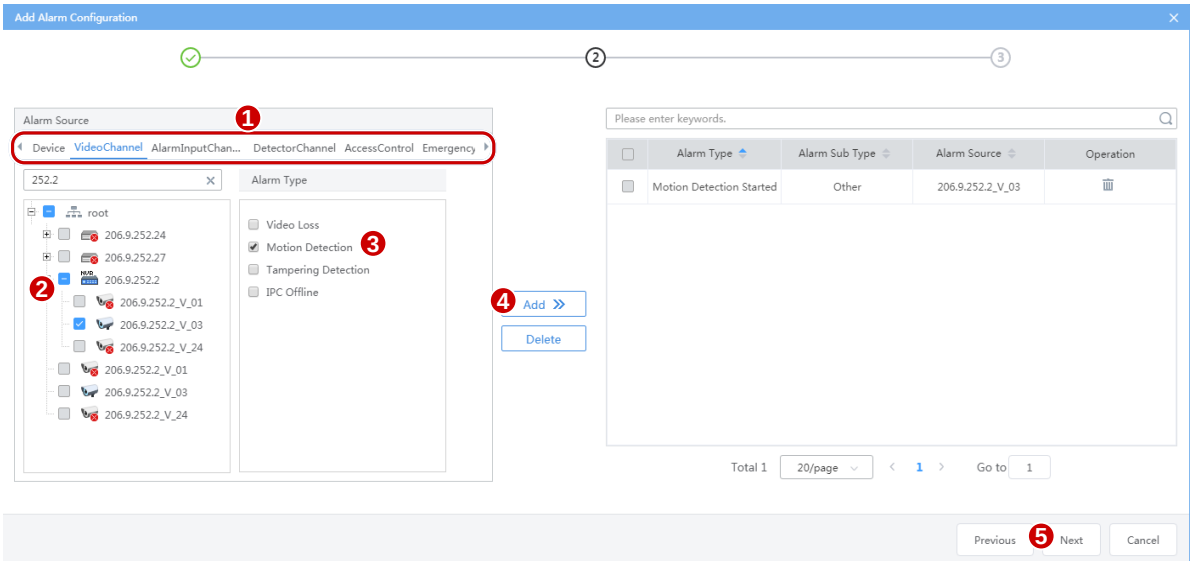
1. Complete settings including the alarm configuration name, time template, etc.



No.	Description
1	The alarm configuration name must be unique in the system.

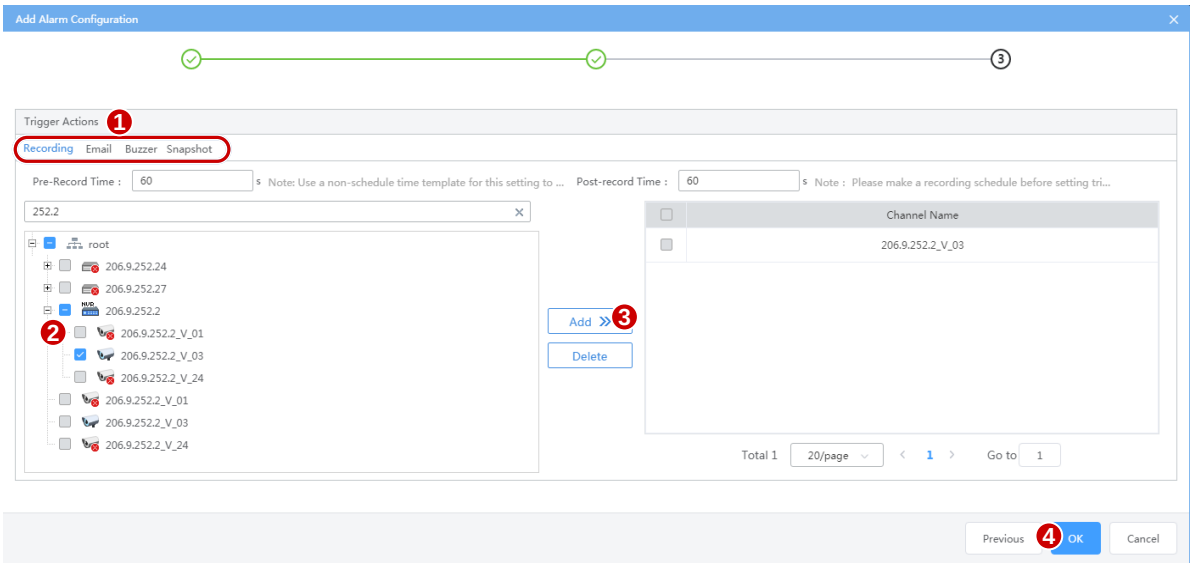
No.	Description
2	Select a time template, or click + to create one. The alarm configuration is effective during the time set in the time template.
3	The alarm configuration is effective when the **Enable** checkbox is selected.

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.



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.
2	Select alarm source(s).
3	Select alarm type(s).

3. Set action(s) to trigger and object(s) to link. 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.



No.	Description
1	Set action(s) to trigger.
2	Set object(s) to link.
3	Configure the action(s) to trigger (see table below).

Table 4-1 Configure Alarm-Triggered Actions

Action	Description
Recording	• **Pre-Record Time**: When configured, the set time will be included in the start time of an alarm recording. For example, **Pre-Record Time** is set to 10 seconds, and an alarm occurs at 12:00:00, then the start time of the alarm recording is 10 seconds before 12:00, which is 11:59:50. • **Post-Record Time**: For alarms that clear automatically, such as motion detection and video loss, the post-record time means how long recording continues after the alarm is cleared; for alarms that cannot clear automatically, such as IP conflict and failed login attempt, the post-record time means how long the recording lasts after the alarm occurs. **Note**: In order for alarm-triggered recording to work, you must set and enable a recording schedule for the linked object(s) (see Recording Schedule).
Email	You need to complete email settings (see Email).
Buzzer	Select the **Buzzer** checkbox to enable buzzer.

Action	Description
Snapshot	The following alarm types support alarm-triggered snapshot: Motion Detection, Video Loss, Alarm Input, Tampering Detection, Audio Detection, IPC Offline, Cross Line Detection, Intrusion Detection, Face Detection, Scene Change Detection, Defocus Detection, Face Recognition Match Alarm, Face Recognition Not Match Alarm, People Gathering, Auto Tracking, Loitering Detection, Vehicle Recognition Match Alarm, Vehicle Recognition Not Match Alarm, Enter Area, Leave Area, Object Removed, Fire Detection Alarm, Human Body Detection Alarm, Zone Alarm, Duress Alarm, Bypass Operation, Tamper Alarm, Tamper Alarm Cleared. **Note**: In order for alarm-triggered snapshot to work, image space must be allocated for the linked object(s). See Capacity Allocation. Alarm-triggered snapshot does not support the capture and upload of images of license plates or vehicles.

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. See Time Template in Recording Schedule for reference.

Contacts

Alarm Configuration > **Contacts**

Add a valid email address in **Contacts** as recipient before setting email as a triggered action. You can verify the configurations by clicking **Test email**.

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 (red) represents the severest.

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.

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**.

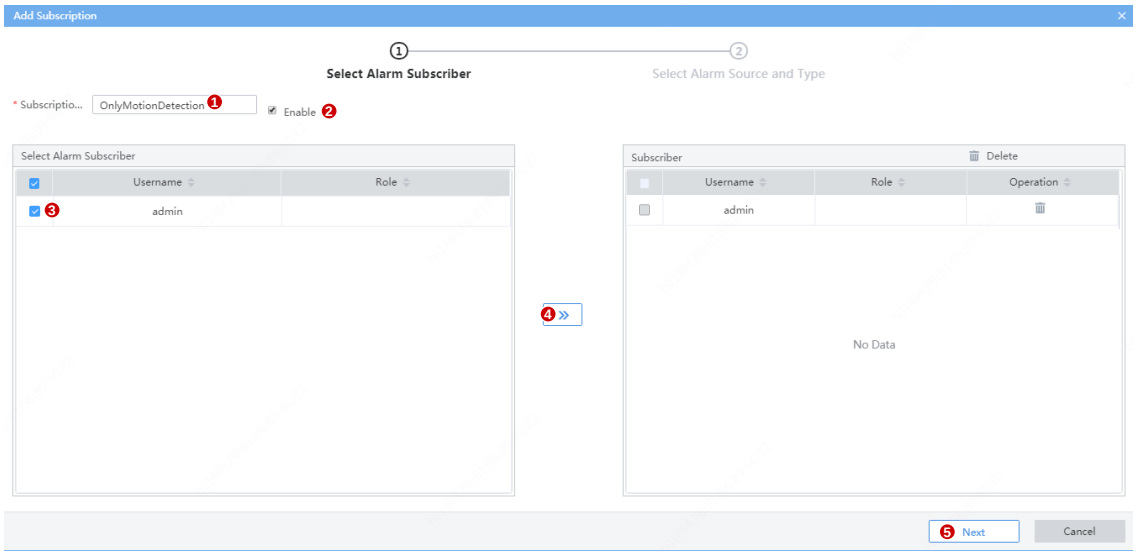
Alarm Subscription

Alarm Subscription > **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.

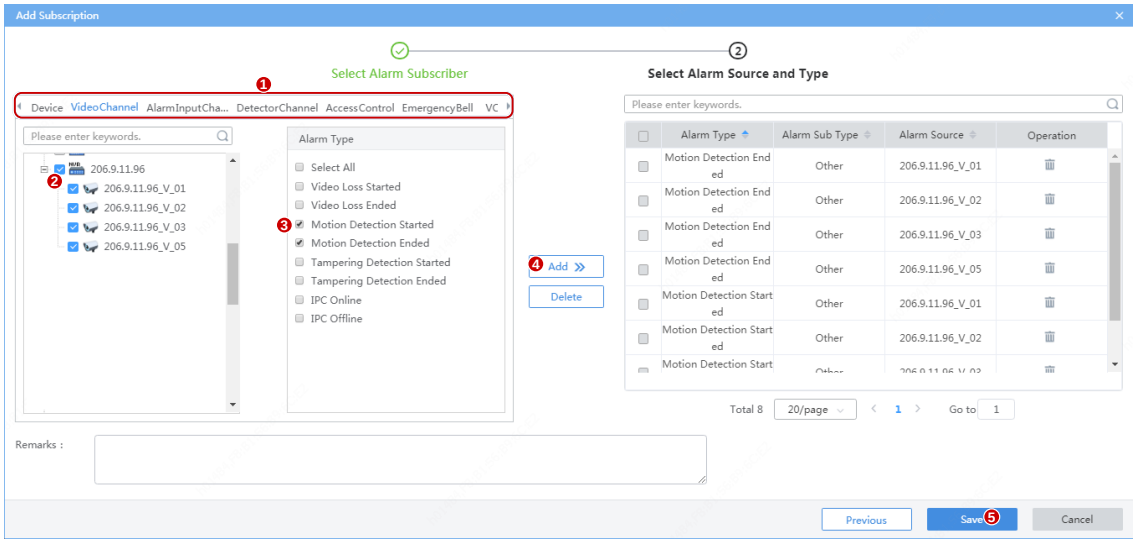
Click **Add** to add alarm subscription:

1. Select alarm subscriber.



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.



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.
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 Sound 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.

5 Recording Backup

Auto Backup

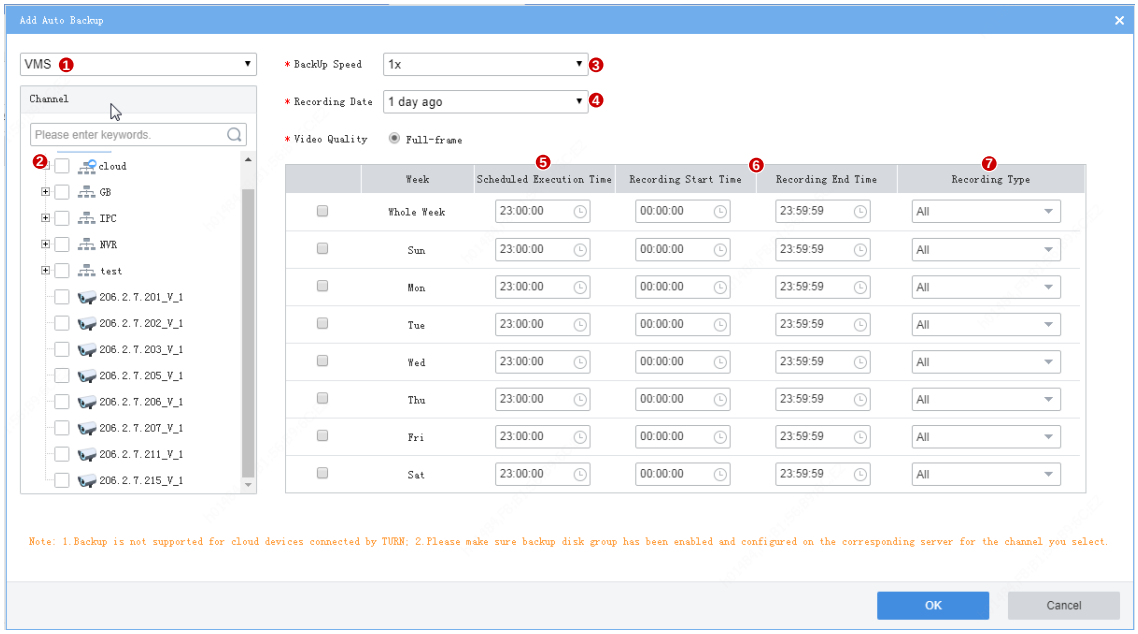
Recording Backup > **Auto Backup**

Create tasks to automatically replicate recordings from NVRs or onboard SD cards of cameras to the VMS.

NOTE!

- You need to configure storage for backup use on the platform first (see Capacity Allocation and Disk Group Property).
- Automatic backup is not available for cloud devices connected by TURN (see connection mode under **Basic** > **Device** > **Cloud Device**).

1. Click **Add**, and then follow the steps to create an auto backup task.



No.	Description
1	Select a server. You can choose master server or slave server if a slave server is configured. If a slave server is to perform the backup, you need to configure disk groups on the slave server.
2	Select the channels for which you want to automatically back up recordings.
3	A higher backup speed consumes more storage capacity.
4	Specifies the date of recordings to back up. For example, if you choose **1 day ago**, then the task that executes on Monday backs up recordings of Sunday. The platform cannot back up recordings of the current day in this way.
5	Scheduled time to execute a task. Tasks are executed one by one. If a task cannot be executed at the schedule time, it waits.
6	**Recording Start Time** and **Recording End Time** specify which part of a video to back up.
7	User can choose to back up certain types of recordings, for example, manual recording, motion.

VMS' Storage Capacity is 256 (unit: channel)
Storage Consumption = Consumption by Recording Schedules + Consumption by Backup Schedules

VMS' Storage Capacity is 256 (unit: channel)	
Consumption by recording schedule = number of recording schedules For example, 2 recording schedules consumes 2. *Remarks:* *A recording schedule, regardless of being enabled or not, regardless of whether its time template covers a whole day, consumes 1.*	Consumption by backup schedules = number of backup schedules * backup speed * recording types *Remarks:* • *Backup speed 1/2/4/8x consumes 1/2/4/8* • *Recording type refers to Normal and Event. Event includes Manual Recording, Motion, Alarm Input, Video Loss and Audio Exception* • *Each Normal type consumes 1; n Normal types consume n.* • *Each Event type consumes 0.2, n Event types consume n*0.2.* • *Each Normal+Event consumes 1.* *Remarks:* • *For devices added via the VSS protocol, the recording type always consumes 1, regardless of how many recording types are configured.*

NOTE!

If a message appears indicating that the backup task has exceeded the storage capacity, please go to **Statistics** > **Server** > **Storage Capacity** to view storage usage (see Storage Capacity).

2. The created backup task appears in the list. You can pause, edit, or delete a task or view task details.

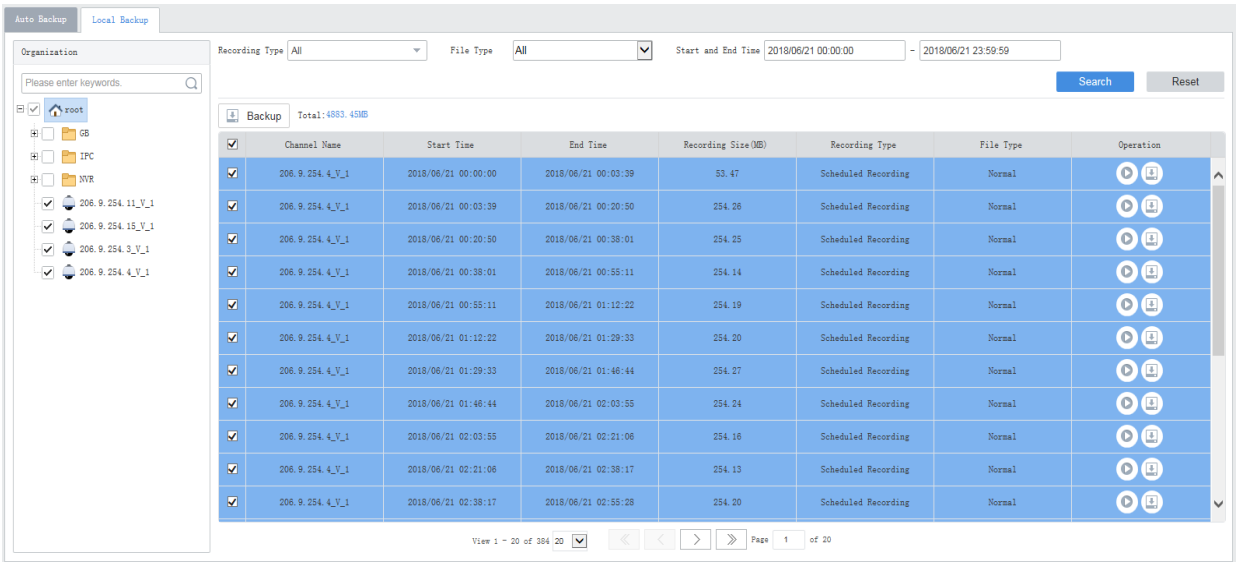
NOTE!

- Editing a schedule (e.g., recording end time) after a backup task has started does not change the current task; the changed settings take effect when next time a task is created.
- If backup is interrupted unexpectedly (for example, because the NVR is disconnected), you may use **Batch Resume** to restart the interrupted backup after the interruption is eliminated.

Local Backup

Recording Backup > **Local Backup**

Save recordings manually to a USB drive plugged in to the VMS. You may format the USB drive in advance or format it on the Web.



1. Select channels on the left, and then set search conditions on the right, including recording type, file type, time period, and then click **Search**.
2. (Optional) Click buttons in the **Operation** column to play or back up a recording file.
3. Select files to back up. The space required for the backup is displayed next to the **Backup** button. Click the button.
4. On the page displayed, set the backup task and path; you may also:

- Create new folders in the USB drive.
- Edit or delete exiting files or folders in the USB drive.
- Format the USB drive into NTFS or FAT32 format.
- View the total space and remaining space of the USB drive.

5. Click **OK**.
6. Click the **Backup Management** button ( ) in the top right corner to view backup tasks or delete a backup task in progress.

6 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.	
Firmware Version	VMS-B1101.19.10.190716
Video&Image Database Version	VIID-B100
Running Time	0 day(s) 4 hour(s) 29 min(s)

Save

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.

- Sync with Computer: If selected, the VMS syncs its time with that of the client computer.
- Auto Update: If enabled, an NTP server must be configured. The system time of the VMS syncs with the NVT server.

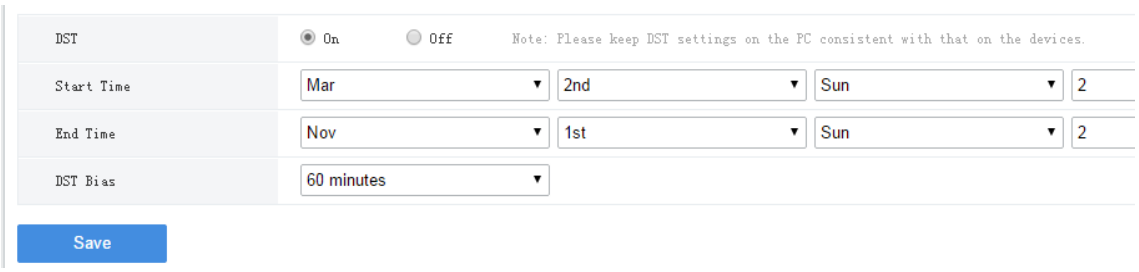
Time Zone	(UTC+08:00) Beijing, Kuala L
Date Format	YYYY-MM-DD
Time Format	24-hour
System Time	2017-12-13 15:27:52 Sync with Computer
Auto Update	On Off

Save

DST

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

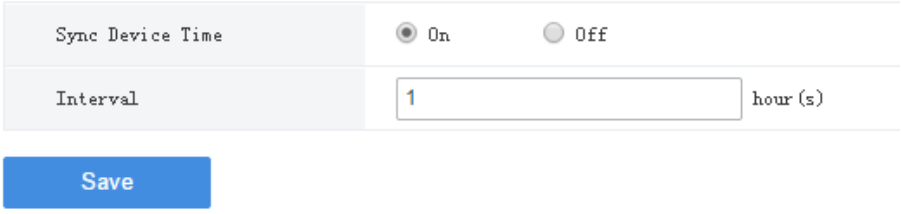
Set DST properly if your country or area uses the Daylight Saving Time (DST).



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 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.

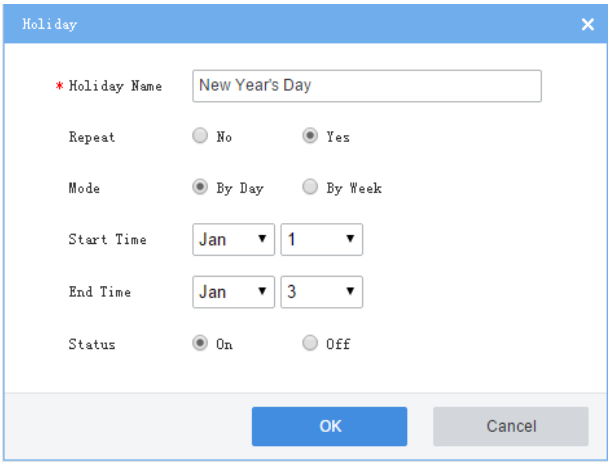


Holiday

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

Holiday is used by time templates (see Time Template) for recording and alarm configuration. Specify holidays to make time templates more flexible and accurate.

The holiday name must be unique in the system.



Disk Configuration

Manage hard disks (or HDD or disks) on the VMS, a disk enclosure, or IPSAN.

Array Configuration

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

Turn on/off RAID mode, create RAID, view RAID info, configure hot spare disk, and rebuild array.

Create an array

1. Turn on RAID mode, and then click **One-click Create** or **Manual Create**.

Table 6-1 Creating RAID by One-click Create or Manual Create

One-click Create	Manual Create
Create RAID1 and RAID5.	Create RAID0, RAID1, RAID5, RAID6, RAID10, RAID50 and RAID60.
Automatically name array(s) in ARRAY*n* format, e.g., ARRAY1.	Arrays are named by user (must be unique).
Automatically create array(s) based on the number of hard disks available: • 2 HDDs: RAID1 • 3 HDDs: RAID5 (no hot spare) • 4-8 HDDs: RAID5 (1 hot spare) • 9-16 HDDs: 2 RAID5 (1 hot spare)	• User sets array type manually. • For RAID50 and RAID60, user must set sub-array disks and select disks properly. The total number of selected disks must be an integer multiple of sub-array disks, and the multiple is greater than 1.

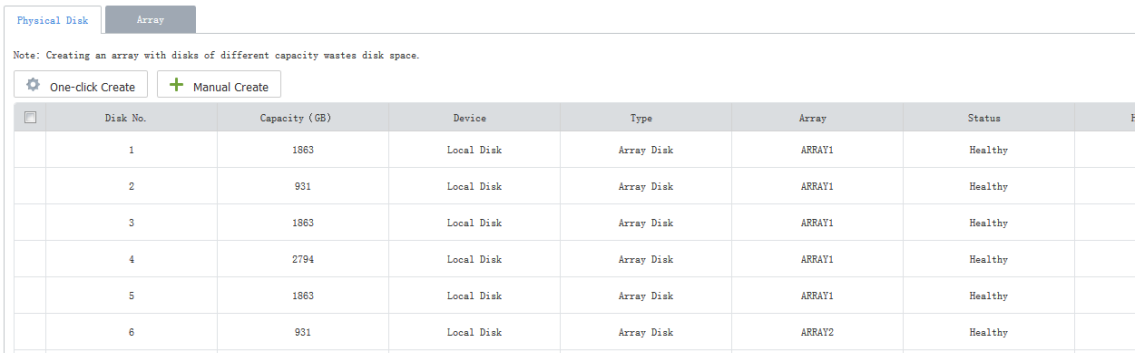
Note:

- *Creating an array will format disks automatically.*
- *The disk with the largest capacity is chosen as the hot spare disk; if multiple such disks exist, the last disk will be chosen as the hot spare disk.*
- *When creating two RAID5, if the total disk number is an odd number (N), then each RAID5 has (N-1)/2 disks; if N is an even number, then the number of disks in the two RAID5 are N/2 and N/2-1.*
- *The disks used to create an array must belong to one device: VMS or disk expansion unit (DEU for short; if configured), which means, you cannot create an array using disks from VMS and DEU; and you cannot create an array using disks from DEU A and DEU B.*

Table 6-2 Supported RAID Types and Corresponding Disks

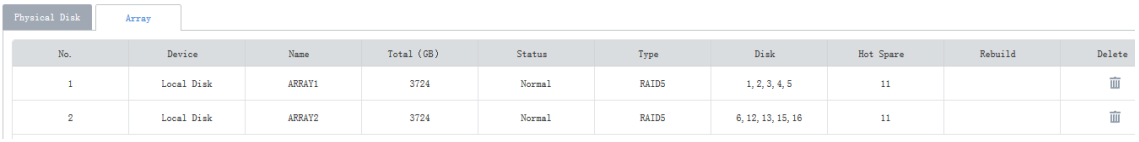
RAID Type	HDDs
RAID0	2-8
RAID1	2
RAID5	3-8
RAID6	4-8
RAID10	4-16
RAID50	6-16
RAID60	8-16

2. When any array is created, click the **Physical Disk** tab to view array disk info. To turn a hot spare disk into a normal disk, click , To set a hot spare disk, click .



Disk No.	Capacity (GB)	Device	Type	Array	Status
1	1863	Local Disk	Array Disk	ARRAY1	Healthy
2	931	Local Disk	Array Disk	ARRAY1	Healthy
3	1863	Local Disk	Array Disk	ARRAY1	Healthy
4	2794	Local Disk	Array Disk	ARRAY1	Healthy
5	1863	Local Disk	Array Disk	ARRAY1	Healthy
6	931	Local Disk	Array Disk	ARRAY2	Healthy

3. Click the **Array** tab to view the created arrays.



No.	Device	Name	Total (GB)	Status	Type	Disk	Hot Spare	Rebuild	Delete
1	Local Disk	ARRAY1	3724	Normal	RAID5	1, 2, 3, 4, 5	11		
2	Local Disk	ARRAY2	3724	Normal	RAID5	6, 12, 13, 15, 16	11		

Delete an array

On the **Array** tab, click in the **Delete** column to delete an array. All data on the array will also be deleted.

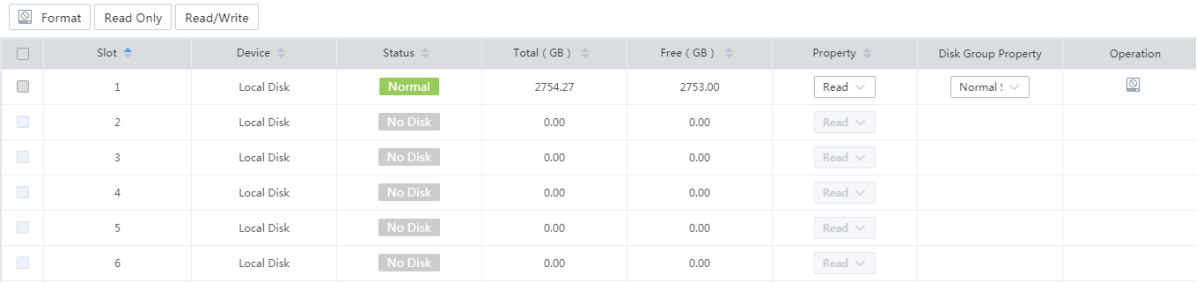
Rebuild an array

If a hot spare disk is available and its capacity is greater than or equal to the smallest disk in the array, the system will start rebuilding the array in 10 minutes after a disk in an array fails. If no such disk is detected by the system, you need to select a replacement disk and rebuild the array manually. The capacity of the replacement disk must be greater than or equal to the smallest disk in the array.

Disk Management

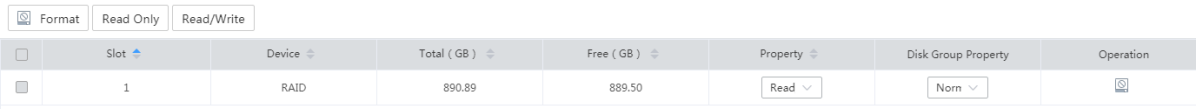
System > **Disk** > **Disk**

- View disk info (slot number, device, disk status, and space usage), format disks (click), modify disk property. The **Device** column indicates if it is a local disk of the VMS or belongs to a disk expansion unit.



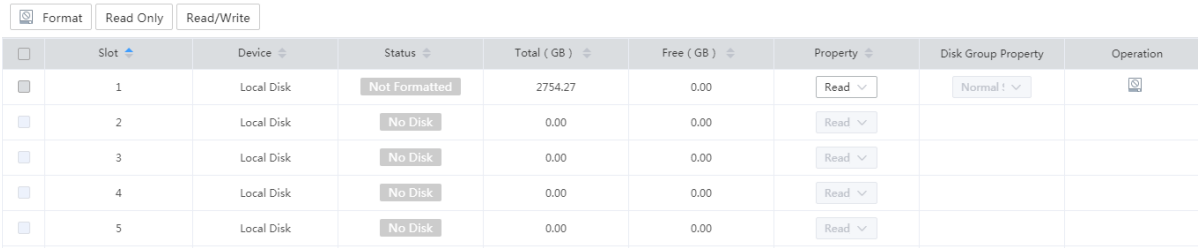
Slot	Device	Status	Total (GB)	Free (GB)	Property	Disk Group Property	Operation
1	Local Disk	Normal	2754.27	2753.00	Read	Normal	
2	Local Disk	No Disk	0.00	0.00	Read		
3	Local Disk	No Disk	0.00	0.00	Read		
4	Local Disk	No Disk	0.00	0.00	Read		
5	Local Disk	No Disk	0.00	0.00	Read		
6	Local Disk	No Disk	0.00	0.00	Read		

- When RAID mode is turned on with array(s) created, you can view array disk information, format disks, modify disk property. This page is empty when there is no array.



Slot	Device	Total (GB)	Free (GB)	Property	Disk Group Property	Operation
1	RAID	890.89	889.50	Read	Norn	

- When RAID mode is turned off with undeleted array(s), the disk status is displayed as **Not Formatted**. You must format the disk before you can use it for storage.



Network Disk

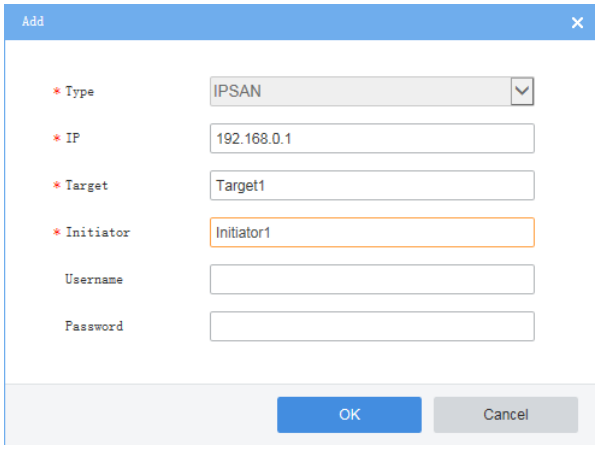
System > **Disk** > **Network Disk**

Configure IPSAN. After the configuration is complete, you can assign IPSAN storage at **Disk** > **Capacity**.

NOTE!

- You must complete configuration (such as service IP address) and create Targets and Initiators on the IPSAN console first.
- IPSAN smaller than 2G is unusable even if it is added successfully.

1. Click **Add** and complete settings in the dialog box.



- IP: IP address of the management or service interface of the IPSAN, which must match that configured on the IPSAN console.
- Initiator: Initiator that you have created on the IPSAN console.
- Target: Target that you have created on the IPSAN console.
- Username/password: For authentication; not required if authentication is disabled on the IPSAN console.

2. Click **OK**.
3. Format disks or modify disk property as needed.

Capacity Allocation

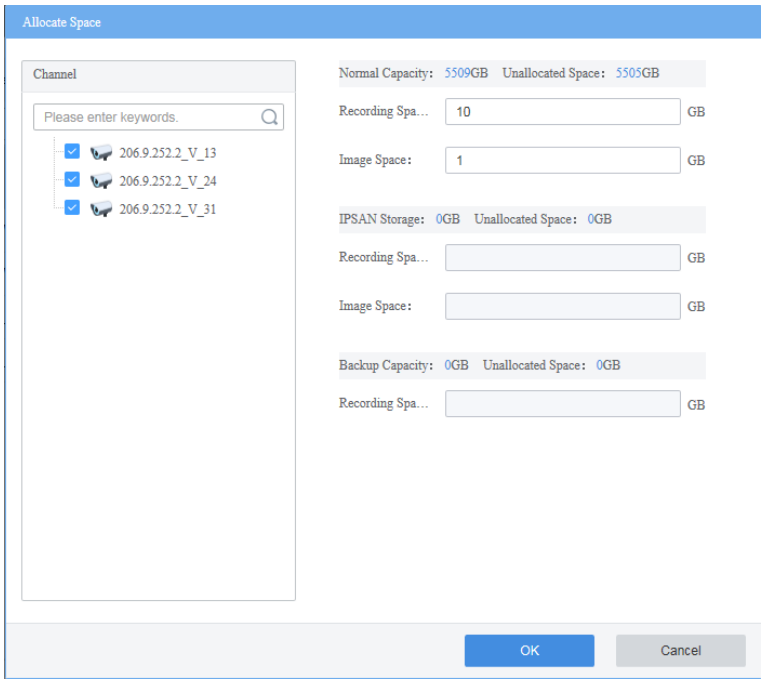
System > **Disk** > **Capacity**

Allocate space to store videos and snapshots from cameras. The total storage space assignable depends on configurations in Disk Management and Network Disk.

NOTE!

- Cameras with no space allocated share the free space.
- If the **Allocate** button is grayed out, check whether it is because you have turned on RAID mode but hasn't created any array.

1. Click **Allocate**, select cameras and then enter the space to assign.



- Normal Capacity: Allocate space for normal storage.
- IPSAN Storage: Allocate IPSAN storage.
- Backup Capacity: Allocate space for backup storage.
- Recording Space: Used for recordings.
- Image Space: Used for alarm-triggered snapshots.

2. Results appear in the list. Click or in the column to delete or edit.

Disk Group Property

System > **Disk** > **Disk Group Property**

View capacity of normal storage, backup storage, and IPSAN.

Disk Group No.	Capacity (GB)	Property
1	891	Normal Storage

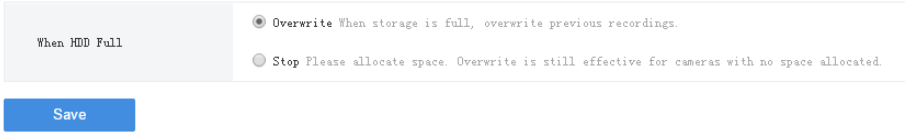
- Normal Storage: Used to store recordings for specified cameras.
- Backup Storage: Used to automatically back up recordings from specified NVRs.
- IPSAN: Network disk that you have added.

Advanced Configuration

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

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

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



NOTE!

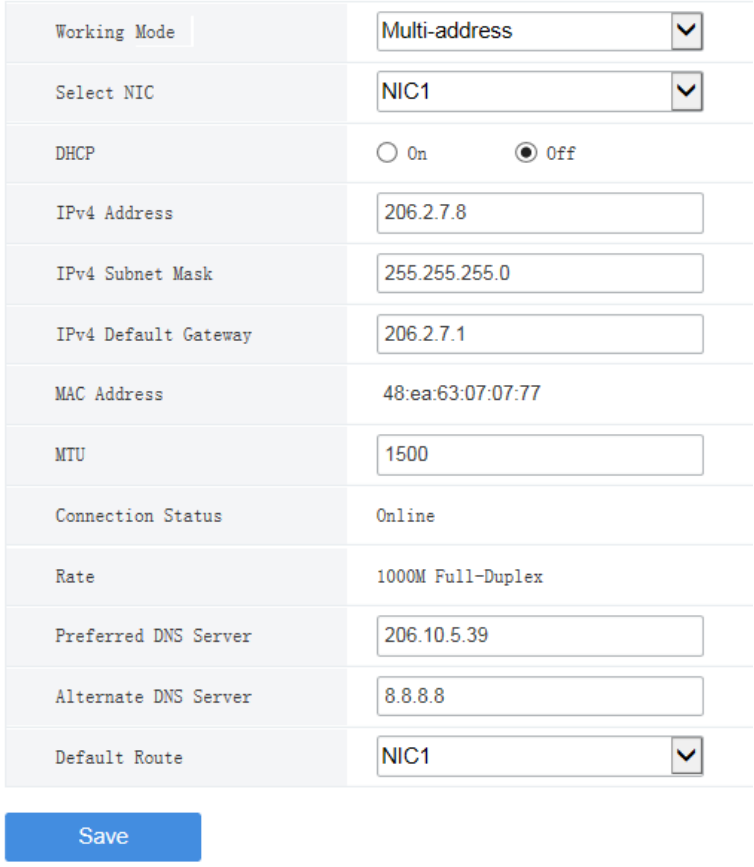
The **Stop** mode is effective only when space is allocated. That is to say, for a camera that no space is allocated, its recording will still be overwritten even if you have set **When HDD Full** to **Stop**. So allocate space appropriately to avoid undesired video loss.

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 servers, and default route.



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.

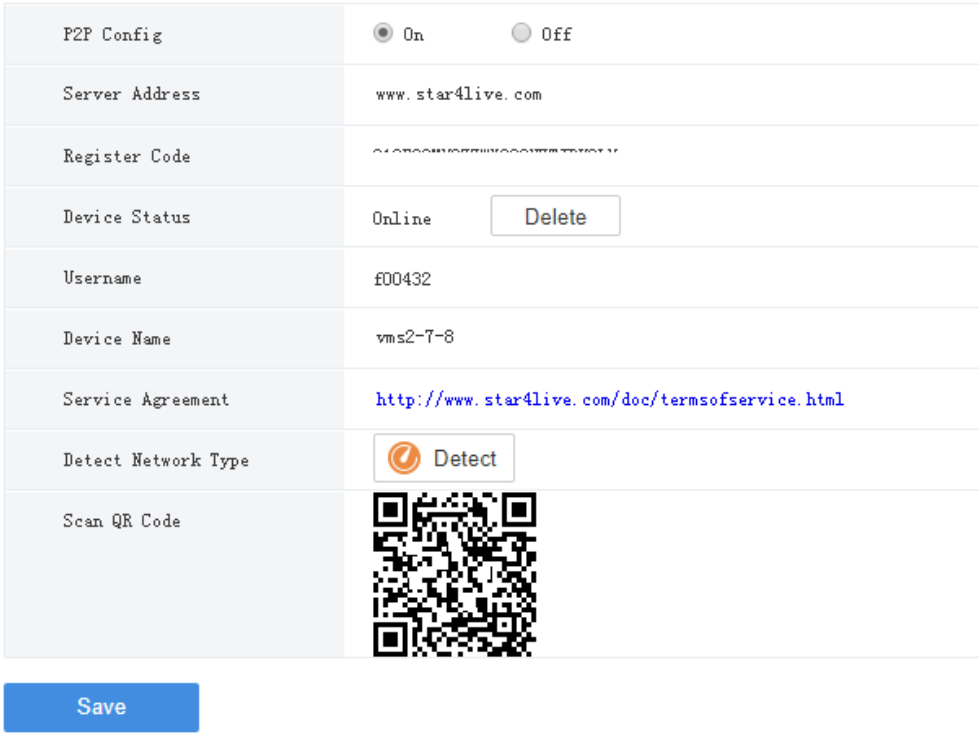
  Load Balance: NICs that make up a virtual NIC use the same IP and work together to share the network load.

  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.

P2P

System > **Network** > **P2P**

P2P is intended for remote surveillance and is disabled by default. You may enable P2P and use the register code to register the VMS at the cloud website. If the **Device Status** is **Online**, you can use the cloud account to access the VMS (see the Login chapter in the *Software Client User Manual*).



- 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 P2P, the VMS is remotely accessible from a PC or mobile client over 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. DDNS is disabled by default.

Three DDNS services are available:

DynDNS

You need to complete registration at the DynDNS official website first. After completing the registration, complete settings on this page, including the server address, port number, and username/password. When the 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, including the server address, port number, and username/password. When the device status is **Online**, you can access the VMS using the domain name.

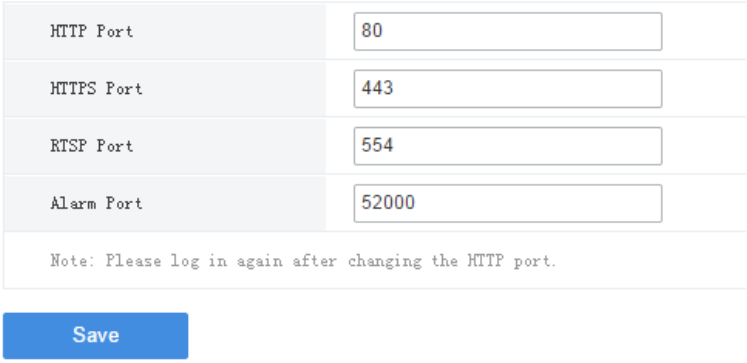
EZDDNS

- The default server address is www.star4live.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. 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., www.star4live.com/vms2).

Port

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

Configure HTTP, HTTPS, RTSP and alarm ports.



Port Mapping

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

Use port mapping 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!

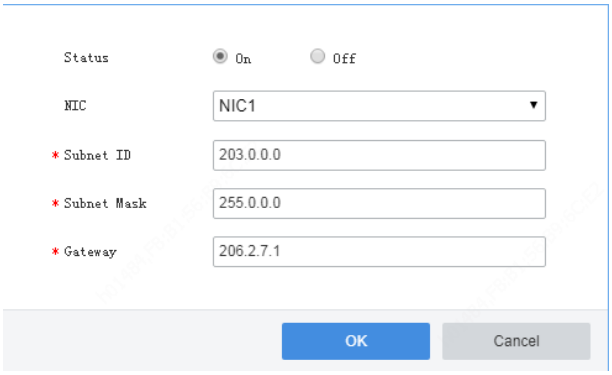
- By default port mapping is disabled.
- Enable UPnP in the router first before you setting UPnP on this page. UPnP requires the router's support.

Custom Route

System > **Security** > **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.



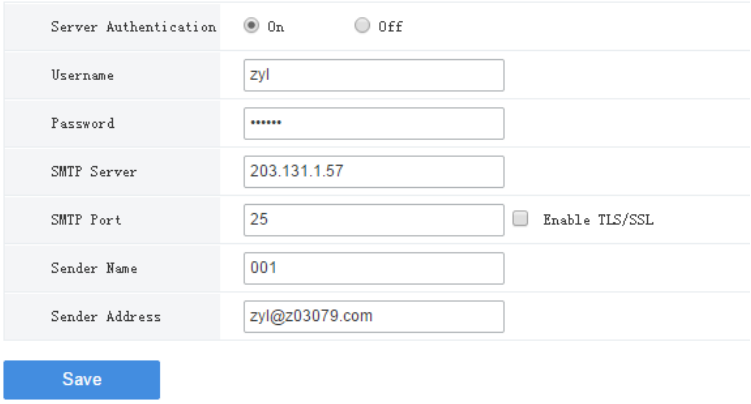
NOTE!

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

Email

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

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



NOTE!

- Enter the correct username and password after enabling (SMTP) server authentication.
- When **Enable TLS/SSL** is selected, data communication between the VMS and the SMTP server is encrypted.
- You may need to change the SMTP port accordingly after enabling TLS/SSL.

Protocols & Interconnection

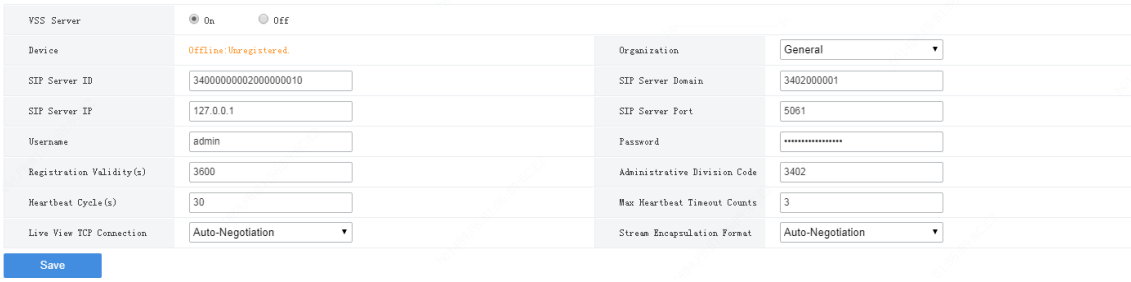
VSS Server

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 live view, play back, and subscribe alarms from channels under the VMS.

The SIP server below refers to the higher-level management platform.

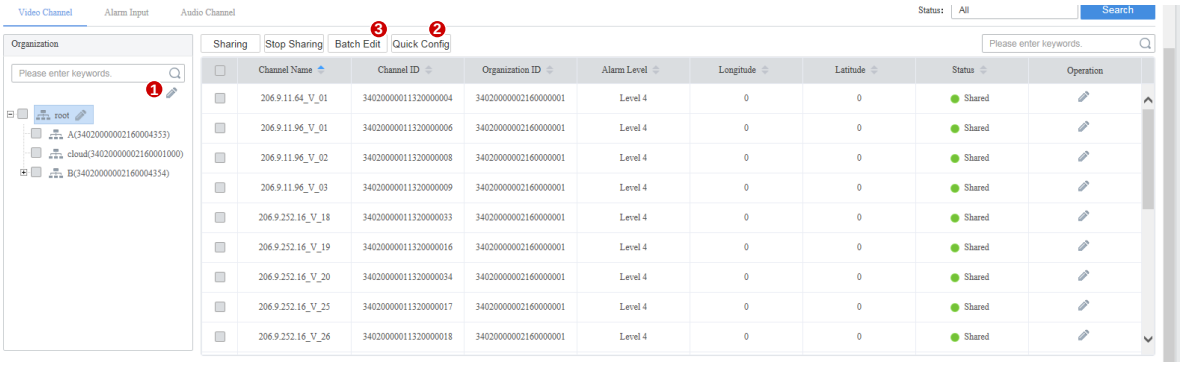
1. Complete basic settings



- 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 between the VMS and the platform times out. Communication stops automatically when it reaches the max count.

2. Share channels with a 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.



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!

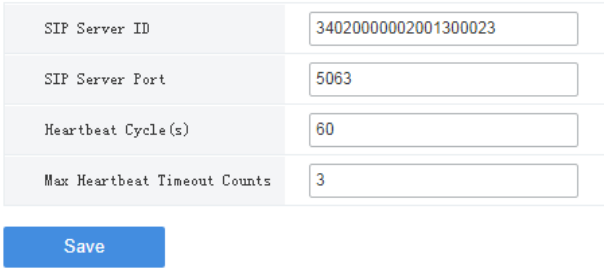
An audio channel cannot be shared or unshared like a video channel. An audio channel's status (Shared or Unshared) is consistent with that of the corresponding video channel. That is to say, sharing (or stop sharing) a video channel also shares (or stops sharing) the corresponding audio channel.

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.

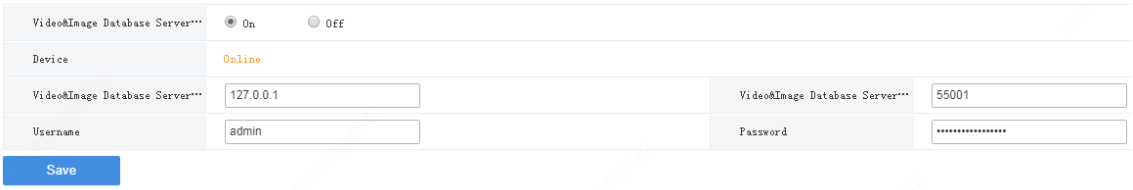


Video&Image Database

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

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

Video&Image Database Configuration



- 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: 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.

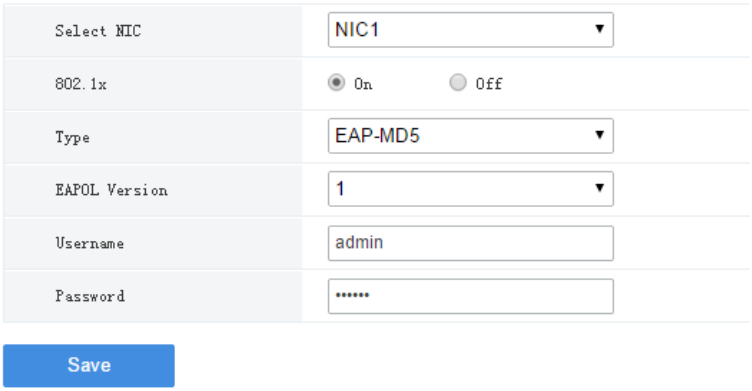
Security Configuration

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).



NOTE!

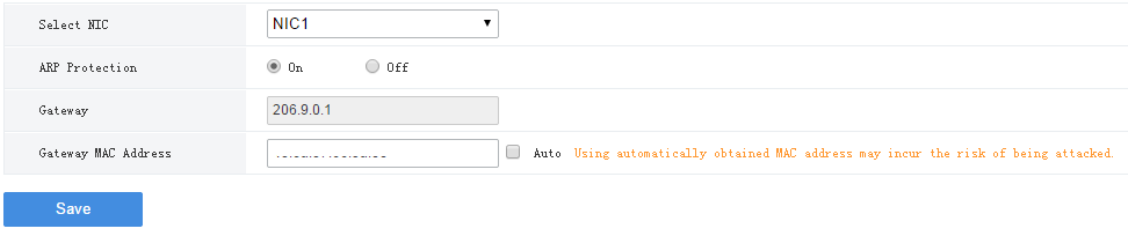
802.1x must also be properly configured on the authenticator (such as Ethernet switch).

ARP Protection

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

Enable **ARP Protection** and bind the IP of the VMS' gateway to the gateway's MAC address to prevent spoofing attacks that impersonate the gateway.

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



NOTE!

ARP protection is effective only when it is enabled and configured before an ARP attack occurs. Protection may fail if you edit the gateway MAC address during an attack.

HTTPS

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

Enable HTTPS (HTTP Secure) 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**

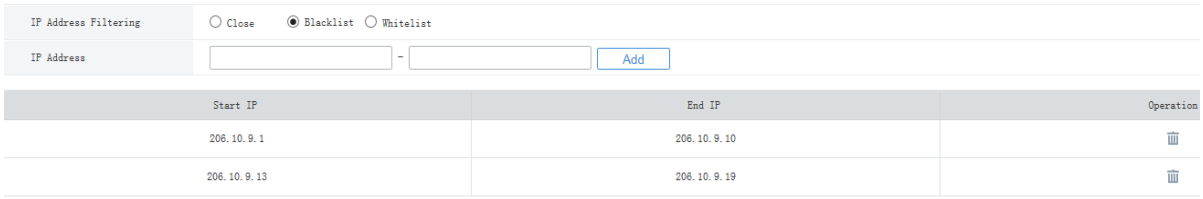
The **Friendly Password** mode is enabled by default. In this mode, access with a weak password is allowed from the same network segment or on three private network segments.

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.

IP Address Filtering

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

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



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

NOTE!

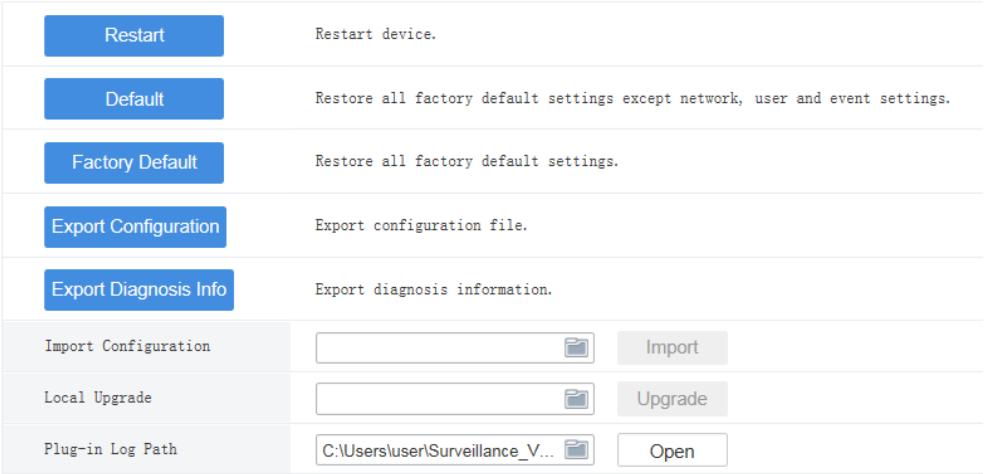
- Blacklist and whitelist cannot be enabled at the same time.
- Blacklist/whitelist is effective to IP-based logins.
- You can click a field in the list to edit an IP address.

Maintenance

System Maintenance

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

Restart the VMS, restore default configurations, import or export configurations, export diagnosis info, and perform a local upgrade.



- 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 the computer. The VMS will restart to complete the upgrade.
- Plug-in Log Path: Click **Open** to view plugin logs. Click the folder icon ( ) to customize the path. The text box and the button are grayed out if no plugin is installed or the Web browser does not support a plugin.

NOTE!

For IE9 and higher, you cannot upgrade the VMS by loading an upgrade file without the plugin installed.

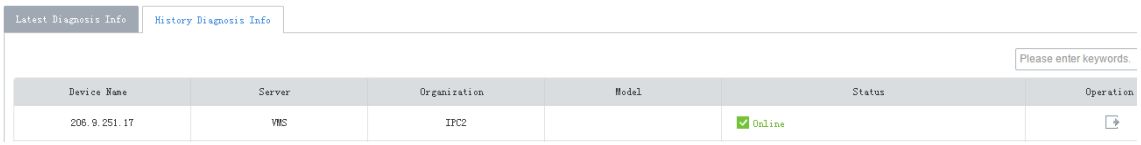
Device Diagnosis Info

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.

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.



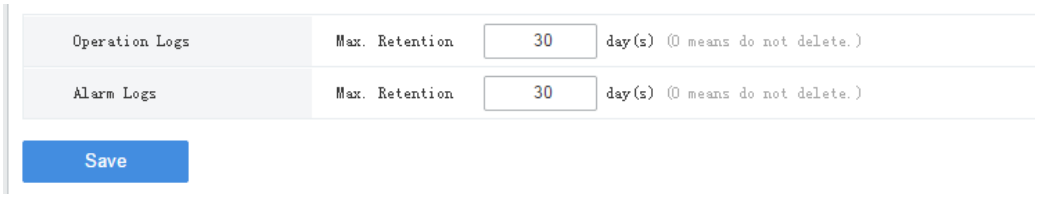
NOTE!

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.



Packet Capture

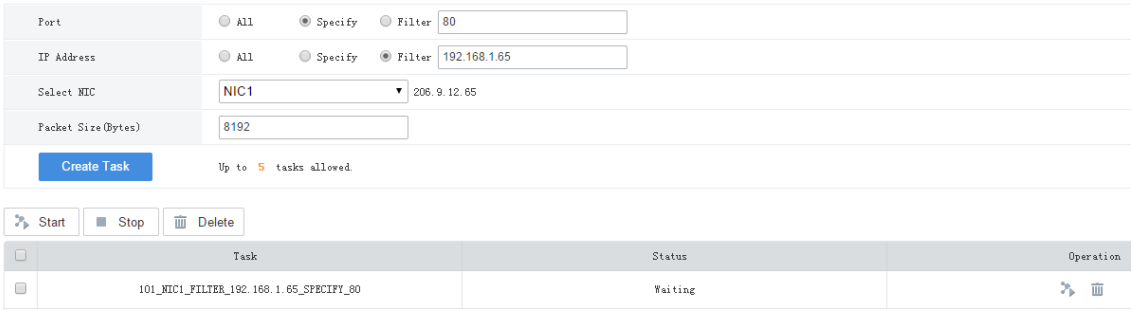
System > **Maintenance** > **Packet Capture**

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.



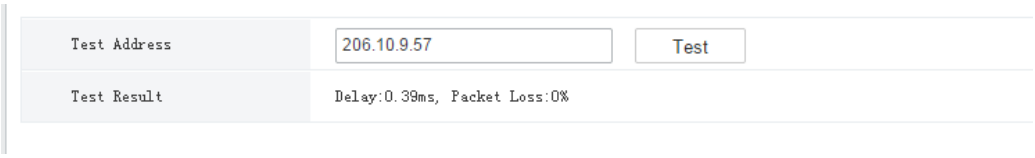
NOTE!

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**

Enter a domain name or an IP address and then click **Test**. The test result will indicate whether the network is connected, and the connection status (including delay and packet loss rate) if connected.



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).

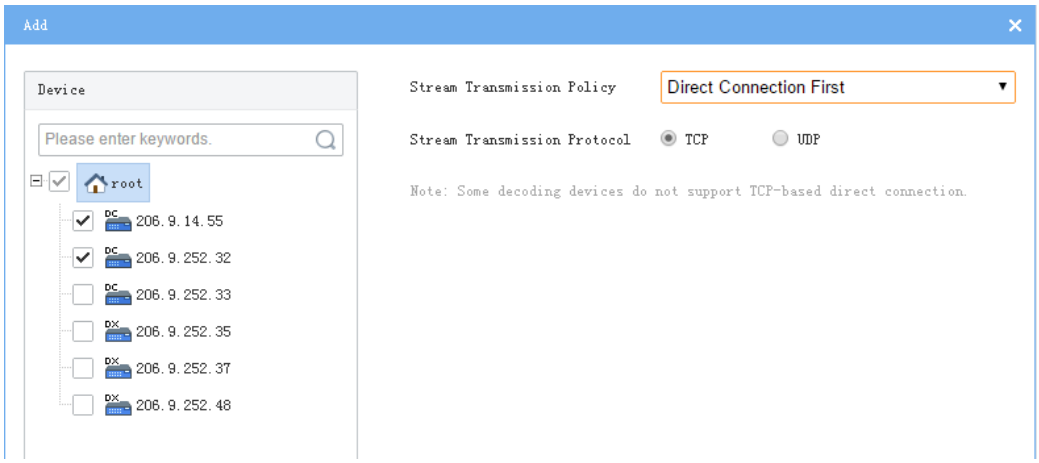
Stream Transmission Policy

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

The Direct Connection First policy is effective on an LAN where the VMS collaborates with certain 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, avoiding 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.



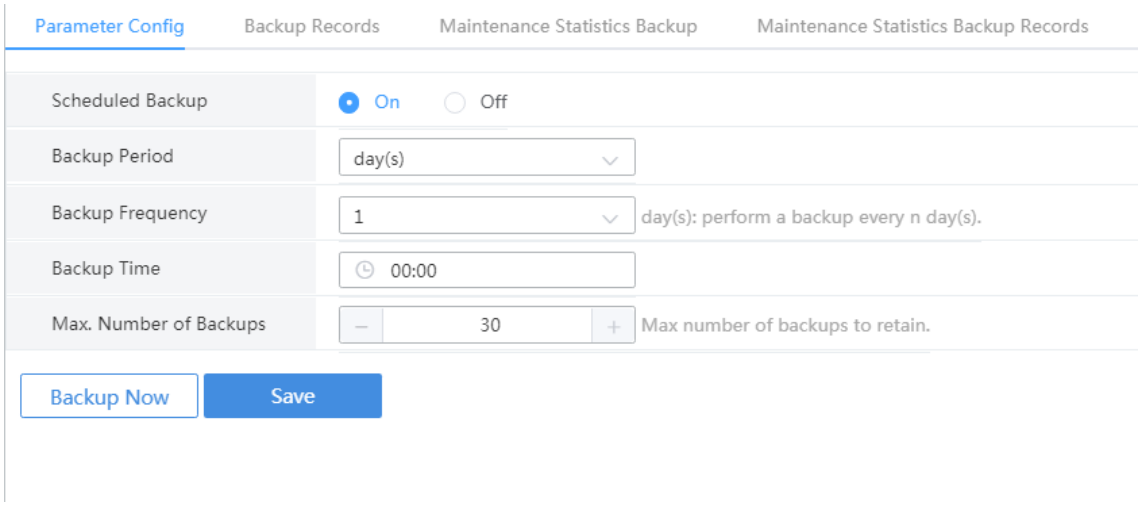
NOTE!

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.



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.

Master/Slave Switch

System > **Master/Slave Switch**

Configure hot standby to improve system reliability; configure master/slave to expand storage and transfer performance. Switch master/slave VMS or change the master VMS for a slave VMS.

Master to Slave

NOTE!

- To add a slave server, access its Web manager, switch to slave mode, and then enter the master server's IP address.
- If the software versions of the master/slave VMSes do not match, you need to upgrade the version first.
- A master/slave switch will clear data, restart the VMS, and reset the password to the default.
- The maximum number of slave VMSes is specified. No more slave VMS can be added when the max number is reached.
- Users cannot access the slave VMS from the software client.

1. Set **Master/Slave Switch** to **Slave**, and then enter the master server's IP address.
2. Click **Save**. If it succeeds, the slave server's status is displayed as **Online**.

Slave to Master

Set **Master/Slave Switch** to **Master** and then click **Save**.

Change Master Server

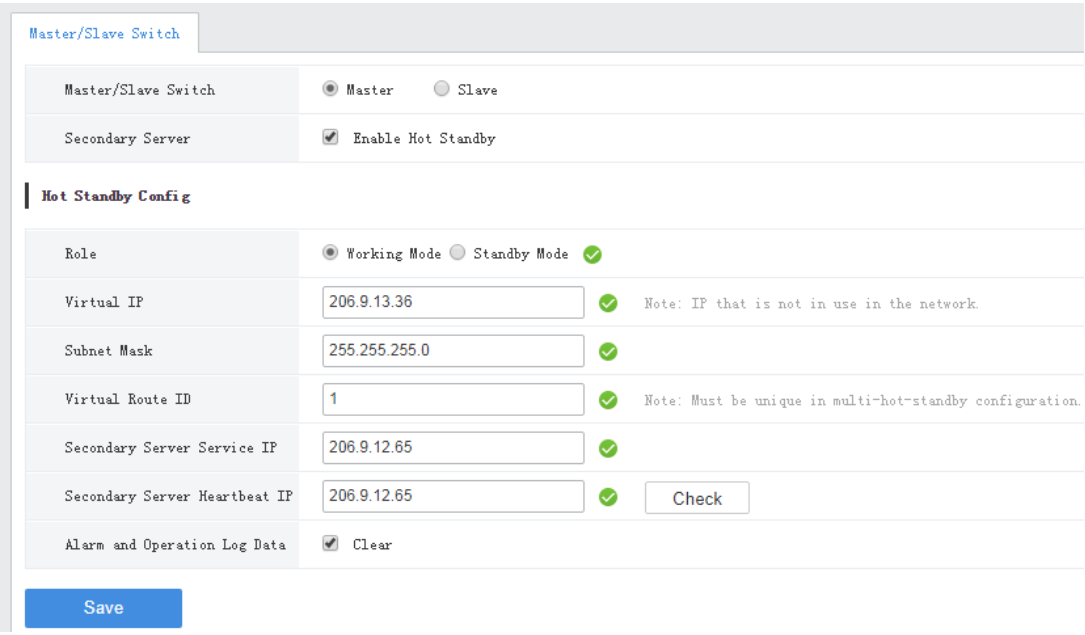
Enter the new master server's IP address and then click **Save**.

Configure Hot Standby

Set a working mode for the central server.

NOTE!

- It is only necessary to configure hot standby on one server (primary or secondary).
- Clearing the **Enable Hot Standby** checkbox will disable hot standby.
- When hot standby is enabled, certain configurations and operations are masked or unavailable on the secondary server's Web manager; and the secondary server is inaccessible from the software client.
- The secondary server takes over when the primary server is down. When the primary server is recovered, video recorded during the takeover will be migrated automatically to the primary server. For security, it is strongly recommended to recover the server immediately.
- If master/slave and hot standby are both configured, make sure the **Master IP Address** is set to the **Virtual IP** on the Web manager of the slave server(s).
- You need to disable hot standby before switching to slave mode.



1. Click **Master**, select **Enable Hot Standby**. Take working mode as an example.

- Secondary Server: Enable/disable hot standby.
- Role: Specify a working mode for the server.
- Virtual IP: Must be an IP that is not in use on the network. When configured successfully, the virtual IP can be used to access the Web and software clients.
- Virtual route ID: (must be unique) Used to differentiate different hot standby configurations on the same network.
- Secondary Server Service IP: IPv4 address of the secondary server (see TCP/IP).

- Secondary Server Heartbeat IP: Same as the service IP, which is used for heartbeat detection between the primary and secondary servers. If no heartbeat is detected within a certain period, the secondary server automatically switches to primary server.
- Check: Check validity of the settings. You can save the settings only when they are checked valid.
- Alarm and Operation Log Data: Selecting **Clear** will improve the speed of synchronization between the primary and secondary servers.

2. Click **Save**.

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.

7 Video Service

View live video and play recordings on the Web manager. You may need to download and install the latest plug-in.

NOTE!

- If the **Playback** and **Local Settings** pages are not displayed, please install the recommended Web browser versions and install the plug-in.
- The Web client can play H.264 video without the plugin, but it will hide the **Playback** and **Local Settings** pages.

Live Video

Video Service > **Live View**

Start Live Video

- Double-click an online camera or drag it to a window to start live video.
- Drag an organization or an NVR to a window to start video. The layout changes automatically if more cameras are selected than windows displayed.

TIP!

- When live video starts, the camera icon changes, (e.g., from to).
- Clicking a playing window will highlight the corresponding camera on the list (e.g.,

).
- Live video stops automatically when you switch to other pages of the Web Manager.

Stop Live Video

- Click in the window's upper right corner.
- To stop all videos, click on the toolbar.
- Live video stops automatically when you switch to other pages of the Web Manager.

Live Video Operations

Use the toolbar at the bottom. Some buttons on the toolbar are only effective to the currently selected window, and the buttons may vary with camera.

No.	Description
A	Set screen layout. Up to 25 windows allowed.
B	Close video in all windows.
C	Frame rate, bit rate, resolution, compression format, packet loss rate of video playing in current window (example).
D	Take a snapshot and save it to the PC. The storage path is configurable (see Local Settings).
E	Local recording. Click to stop. The storage path is configurable (see Local Settings).
F	Digital zoom. When enabled, drag the mouse to draw an area on the image to zoom in on, and then use the wheel scroll to zoom in or out. Click to disable.
G	Adjust the output sound volume on PC or mute.
H	Adjust video settings, including brightness, saturation, contrast and sharpness.
I	Select a stream type to play: main stream, sub stream, third stream. **Note:** The stream type available may vary with camera. An unsupported stream type (e.g., MJPEG video stream) is not displayed.
J	Set display ratio: stretch or scale.
K	Play in full screen. Press <**Esc**> to exit.

For a PTZ camera, you may click the on the right border of the window to display the PTZ control panel and control the PTZ.

Button	Description
	Control rotation directions or stop rotation. ***Note:*** You may also use the mouse to change the surveillance direction in the live view window: move the mouse pointer toward the side of the window you want to view; when the pointer changes shape (like ▶), click the mouse button to move, or press and hold the mouse button to keep moving. The camera will rotate in that direction. Release the button to stop.
	Adjust focus and zoom. ***Note:*** You may also click anywhere on the image and then use the scroll wheel to zoom in or out.
	Adjust rotation speed. Nine speed levels are available.
	Rotate the camera to the intended position and then click to add as a preset. To go to a preset, click . To delete a preset, click .
	Enable or disable the wiper (if equipped).

Playback

Video Service > **Playback**

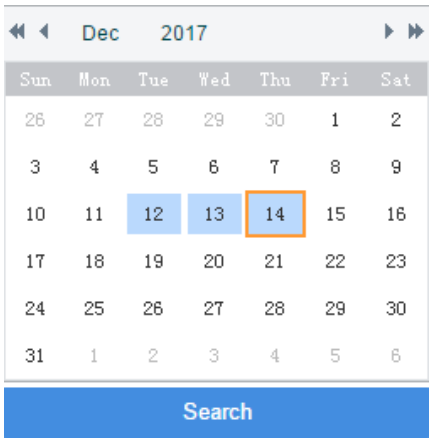
Glossary

- Center recording: Recording that is stored on the VMS.
- Device recording: Recording that is stored on an NVR.
- Video channel: A video channel corresponds to a camera.
- Normal recording: Video recorded according to a recording schedule.
- Event recording: Recording triggered by an event (e.g., an alarm).

Search Recording

1. Click **Center** or **Device**.
2. Select camera(s) (up to 16). Enter keywords to filter if necessary.

The calendar shows recording status of the current month. Blue means normal recording, red means event recording, and white means no recording (see figure below).



3. Select a date with recordings.
4. Click **Search**.

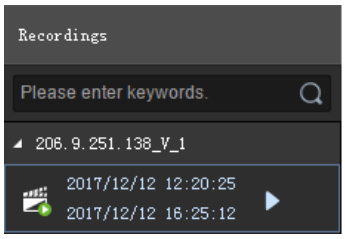
Search results are shown on the timeline (as known as progress bar) and the **Recordings** list on the right. Different recording types are shown with different colors on the timeline: blue for normal (scheduled), and red for event (alarm).

TIP!

The timeline and the file list shows search results for the currently selected window. Click another window to view corresponding search results.

Playback Control

Double-click a recording in the **Recordings** list on the right, or click the **Play** button ( ), which appears when the pointer rests on a file.



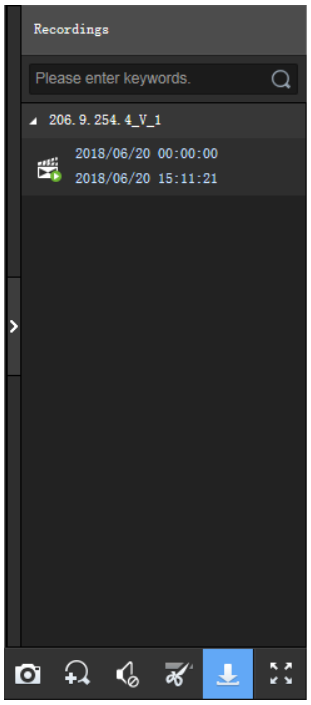
During playback, use the toolbar at the bottom of the window. Some buttons on the toolbar are effective to the currently selected window.

No.	Description
A	Set screen layout, up to 16 windows.
B	Close all windows.
C/F	Rewind by frame, forward by frame.
D	Pause/resume
E	Stop
G	Adjust playback speed. Multiple options are available. + means playing forward, - means playing backward.
H	Take a snapshot and save it to the PC. The storage path is configurable (see Local Settings).
I	Digital zoom. When enabled, drag the mouse to draw an area on the image to zoom in on, and then use the scroll wheel to zoom in or out. Click to disable.
J	Adjust the output sound volume on PC or mute.
K	Clip video to download: click , click on the timeline to locate the end, and then click .
L	Download recording. Click in the upper right corner to view and manage recording download tasks. See Recording Download for details.
M	Play in full screen. Press <Esc> to exit.
N	Camera name.
O	Progress of playing (with date and time on the top).
P	Indicating recording: blue for normal recording, red for event recording.
Q	Corresponding time where the mouse pointer rests.
R	Calendar button. Click to search recordings for other dates.

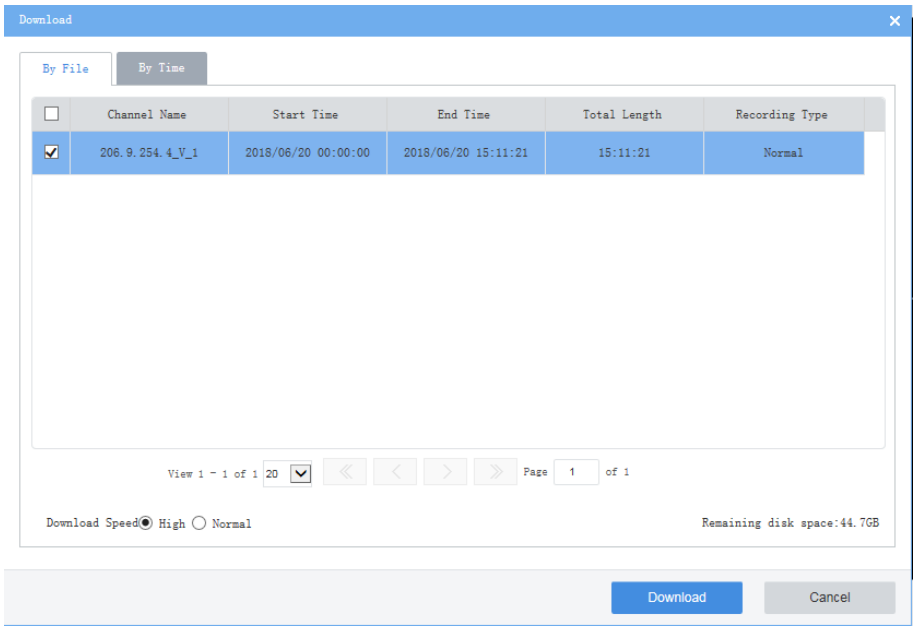
Recording Download

Download recordings from the VMS to your computer.

1. Click on the toolbar.



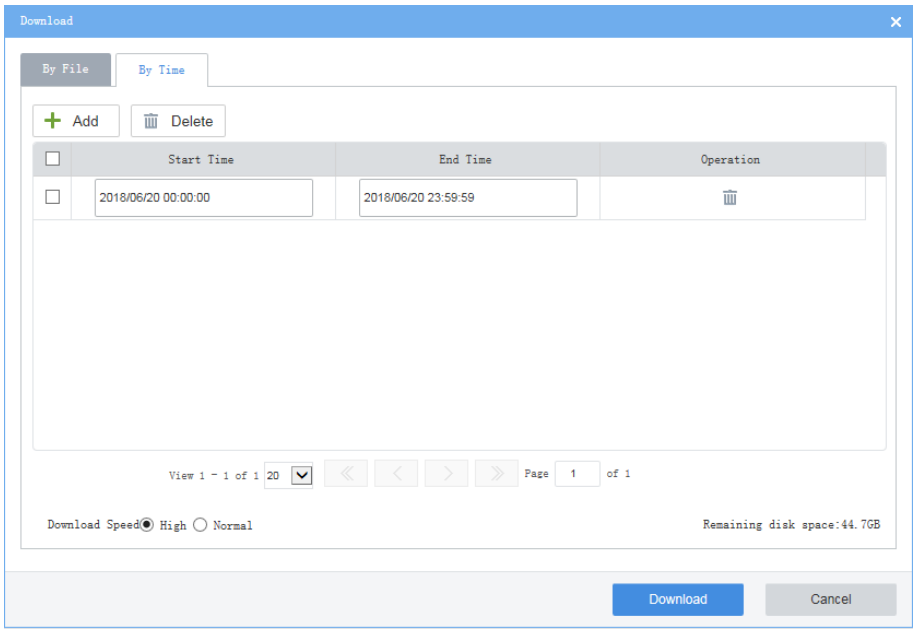
2. Select recording(s) to download and then click **Download**.



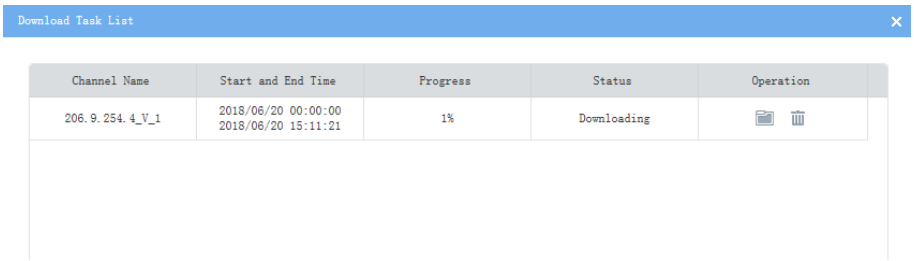
3. To download recordings of specified period, click the **By Time** tab, and then set the start and end times. Click **Add** to add download tasks. Select the tasks and then click **Download**.

TIP!

- The downloaded recordings are named in **channel name_start time_end time** format in the specified directory, for example, 206.9.9.19_V_1_S20180115000001_E20180115000721.mp4.
- If a channel name contains a special character such as asterisk (*) or question mark (?), the special character will be displayed as underline (_) in the filename. If the channel name is ended with two or more spaces or dots (.), the last space or dot (.) will also be displayed as underline in the filename.



4. To view download progress, open the recording folder or manage download tasks, click in the page's upper right corner.



Local Settings

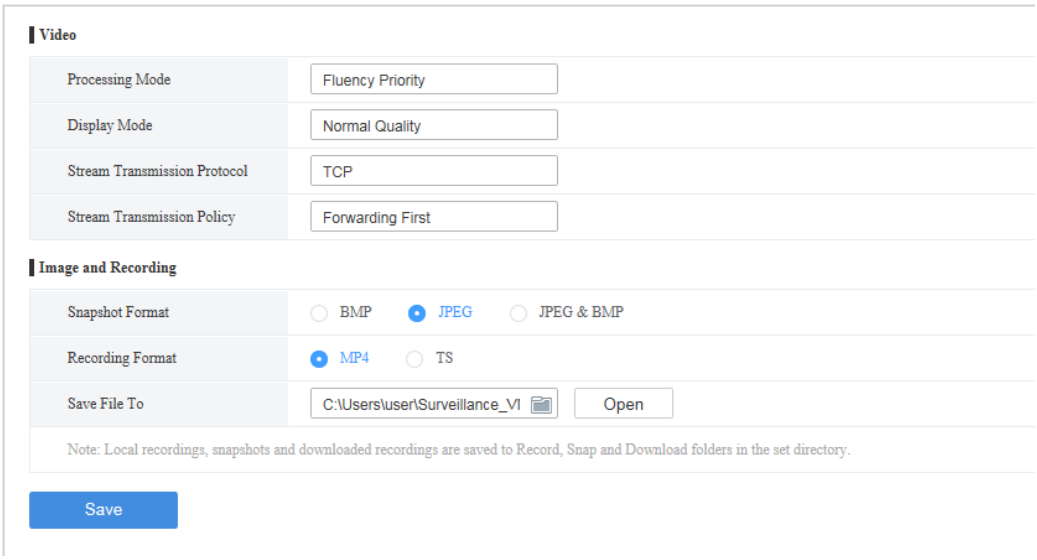
Video Service > **Local Settings**

Set local settings include video processing mode, display mode, snapshot/recording formats and storage locations.

The **Direct Connection First** policy is effective on a local area network (LAN) where the VMS collaborates with certain 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 client, avoiding 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 client.



8 Statistics

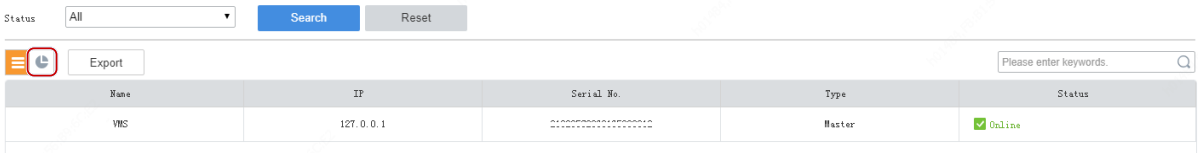
View operation statistics of the server (VMS) and the connected devices, search alarm logs of the server and devices, search operation logs of the server.

Server Statistics

Server Status

Statistics > Server > Server Status

View master/slave VMS information, including server name, IP address, serial number, server type (master or slave) 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.



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.

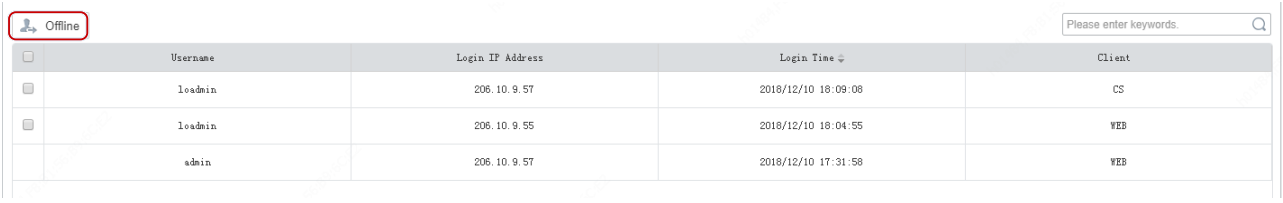
Select NIC	NIC1
DHCP	Disable
IPv4 Address	206.9.12.65
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	206.9.0.1
MAC Address	48:ea:87:66:3a:00
MTU	1500
Preferred DNS Server	206.10.5.39
Alternate DNS Server	8.8.4.4
Default Route	NIC2

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.



Bandwidth

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

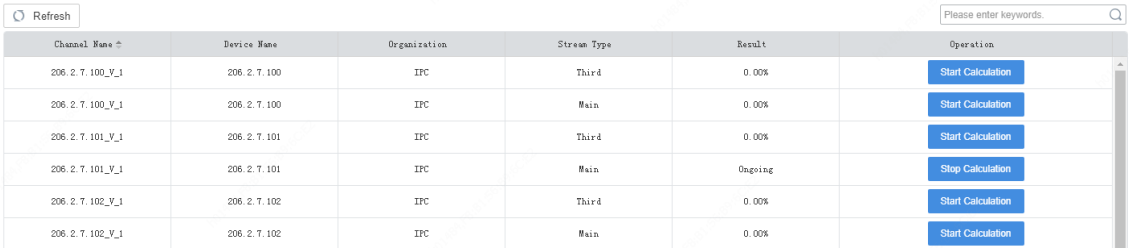
View the current bandwidth usage of the master/slave VMS. See Bandwidth Usage.

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.



Server Performance

Statistics > Server > Server Performance

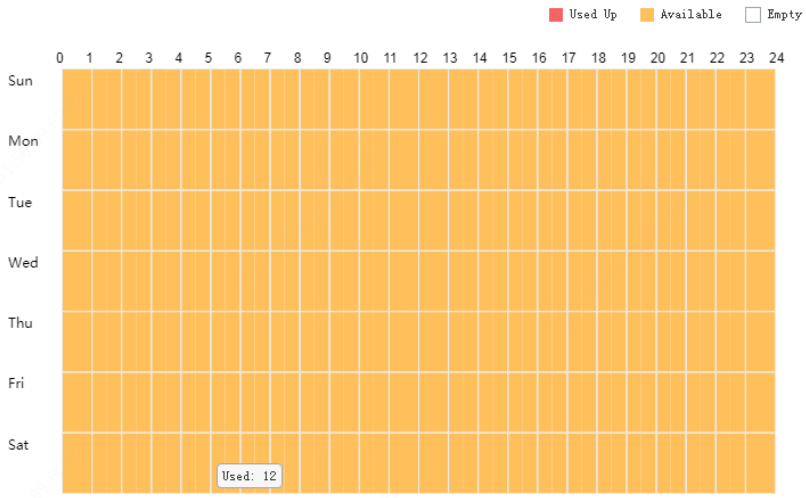
View the current CPU usage, RAM (physical memory) usage, and receive (input) and send (output) bandwidths of the VMS.

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.

Storage Capacity

Statistics > Server > Storage Capacity

If the system indicates full storage capacity when you are configuring a recording schedule (**Basic** > **Recording Schedule**) or recording backup (**Recording Backup** > **Auto Backup**), you can analyze the usage of storage capacity on this page and then alter the current recording schedules or recording backup accordingly to free up certain storage capacity.



The vertical axis means days (Sunday to Saturday), and the horizontal axis means time (00:00 to 24:00, divided into 48 segments). Three colors represent three different statuses. And by placing the mouse pointer on the diagram you can view the used storage capacity of the corresponding period.

- Red: No idle storage capacity, and no recording schedule or recording backup schedule is allowed during this period.
- Yellow: Idle storage capacity, and recording schedule or recording backup schedule is allowed during this period.
- White: No storage capacity has been used during this period, and you can configure recording schedule and recording backup.

If the system indicates full storage capacity, try the following to release storage capacity.

Service Type	Try
Recording schedule (**Basic** > **Recording Schedule**)	Delete unnecessary recording schedules.
Recording Backup (**Recording Backup** > **Auto Backup**)	● Deselect unnecessary recording types. The more recording types you choose, the more storage capacity will be used. ● Alter the selected recording types. The Normal type uses more storage capacity than other recording types. ● Alter backup times, for example, from seven days a week to three days a week. ● Alter recording start time and recording end time to reduce same backup periods every day. ● Lower the backup speed. A higher backup speed uses more storage capacity than a lower backup speed.

NOTE!

Both recording schedule and recording backup consume storage capacity. When storage capacity is used up, you may alter recording schedule to release storage capacity for recording backup; likewise, you may also alter recording backup schedule to release storage capacity for recording schedule.

Recording Status

Statistics > **Server** > **Recording**

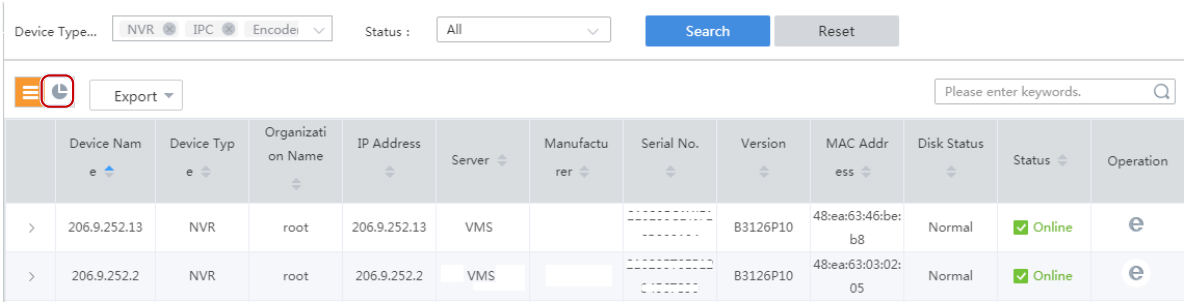
Search recording statistics by recording status and recording type. Export search results to a CSV file. You can switch the list to a pie chart and place the mouse pointer on the chart to view the number and percentage.

Channel Name	Device Name	Organization	Recording Type	Status	Diagnosis	Recording Spac	Stream Type	Frame Rate(fps	Bit Rate(Kbps)	Resolution
206.2.7.102_V_1	206.2.7.102	IPC	Normal Recording	Recording...	Normal	324	Main	30	5146	1920x1080(1080P)
206.2.7.104_V_1	206.2.7.104	IPC	Normal Recording	Recording...	Normal	329	Main	30	5104	1920x1080(1080P)
206.2.7.114_V_1	206.2.7.114	IPC	Normal Recording	Recording...	Normal	323	Main	30	3926	1280x960(960P)
206.2.7.113_V_1	206.2.7.113	IPC	Normal Recording	Recording...	Normal	163	Main	25	1966	1280x720(720P)
206.2.7.112_V_1	206.2.7.112	IPC	Normal Recording	Recording...	Normal	328	Main	30	5139	1920x1080(1080P)
206.2.7.111_V_1	206.2.7.111	IPC	Normal Recording	Recording...	Normal	328	Main	30	5238	1920x1080(1080P)
IP Camera 03	206.2.7.4	GB	Normal Recording	Recording...	Normal	309	Main	25	5103	1920x1080(1080P)
206.2.7.100_V_1	206.2.7.100	IPC	Normal Recording	Recording...	Normal	324	Main	30	5137	1920x1080(1080P)
206.2.7.101_V_1	206.2.7.101	IPC	Normal Recording	Recording...	Normal	324	Main	30	4025	1920x1080(1080P)

Device Statistics

Statistics > **Device**

Search device statistics by device type and device status. Export search results to a CSV file.



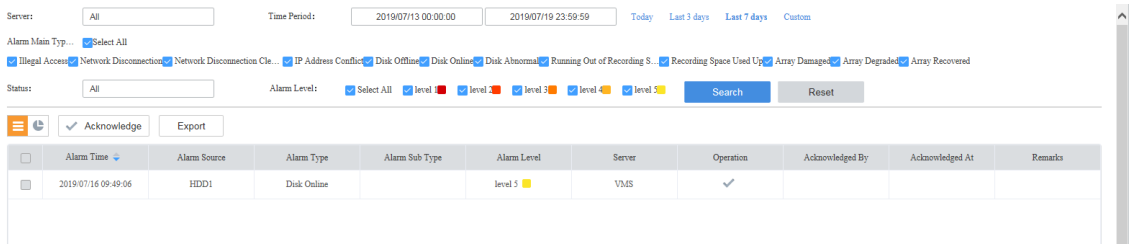
Logs

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.



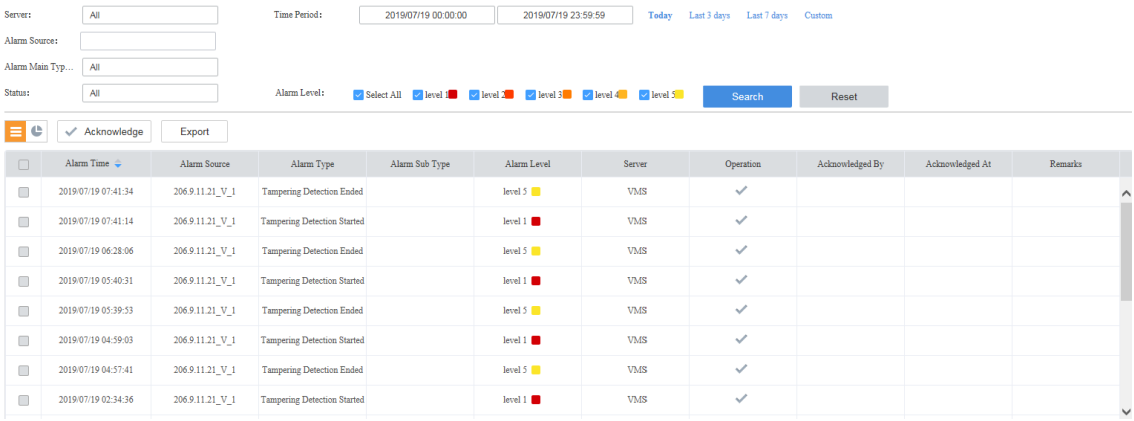
NOTE!

The acknowledge operation is irreversible. The 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.



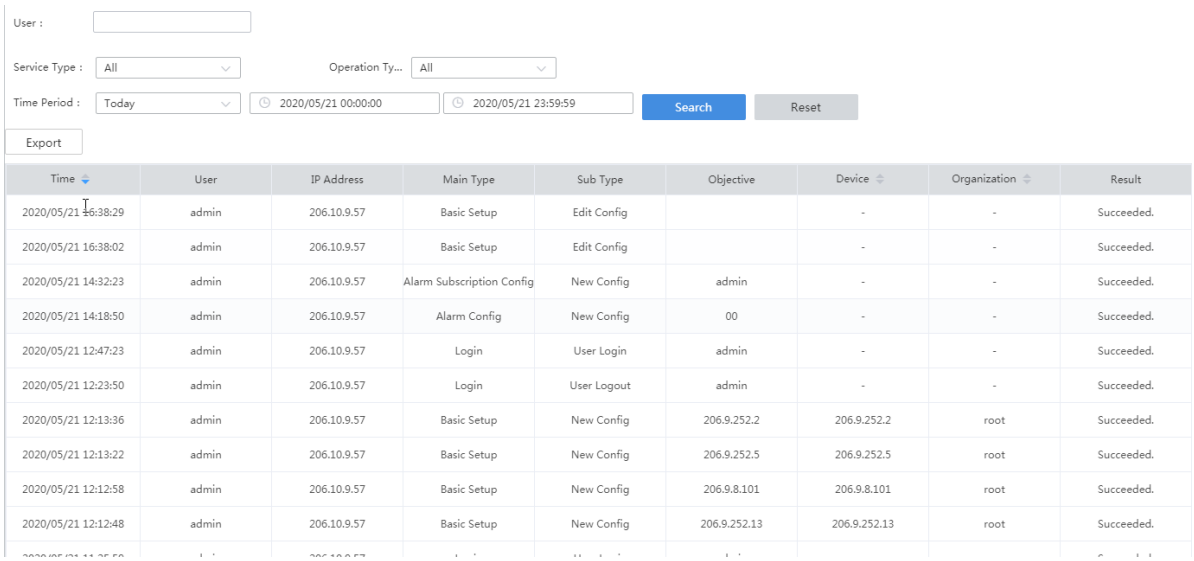
NOTE!

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

Operation Logs

Statistics > **Log** > **Operation Logs**

Search and export user operation logs.



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).

9 Access Control

Permissions

Access Control > Permissions

Manage time templates, door groups and access permissions.

Time Template

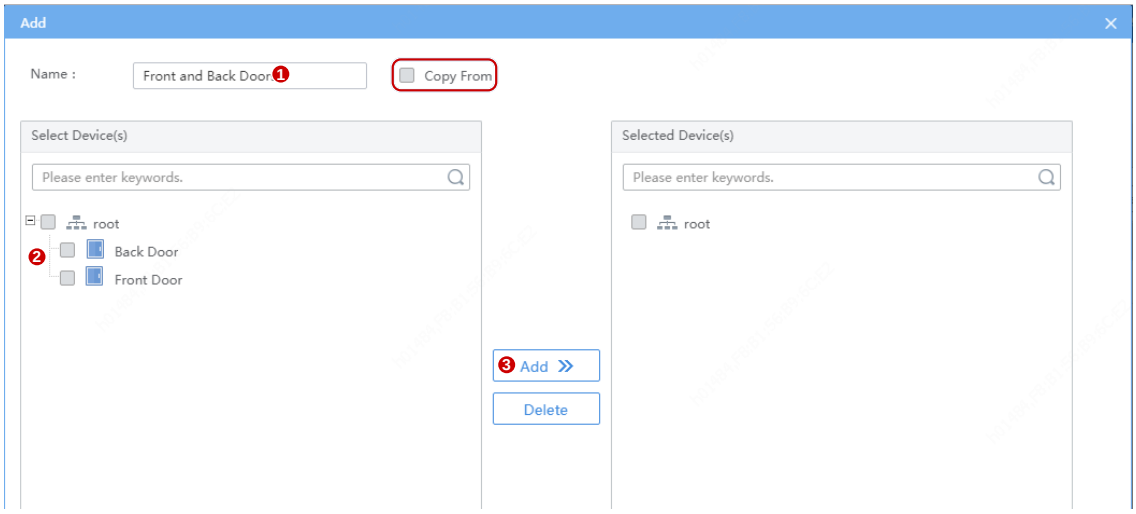
Use a time template to restrict access time. You will need to choose a time template when configuring access permissions.

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.



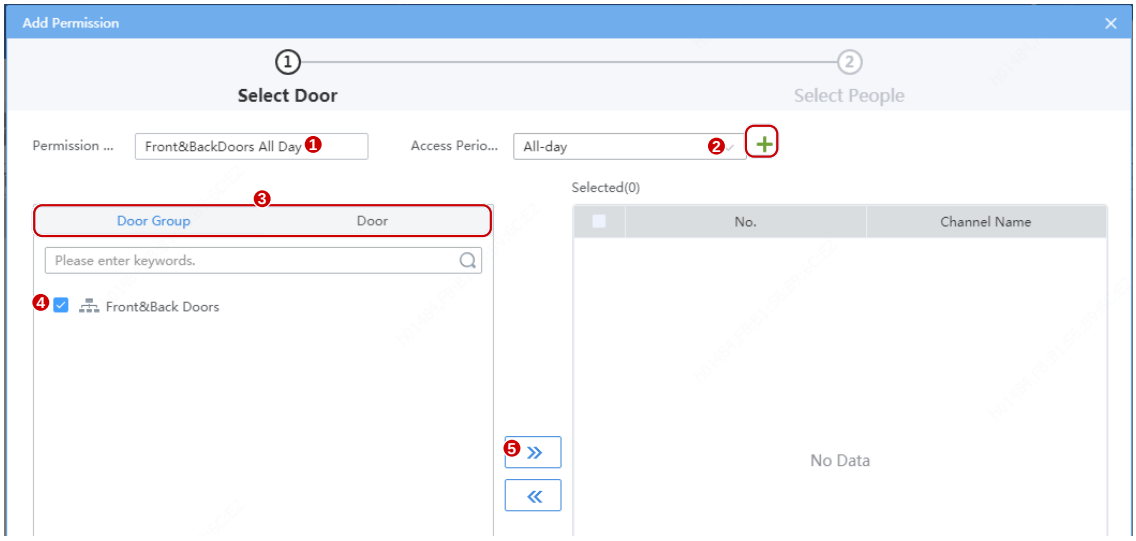
Note!

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.

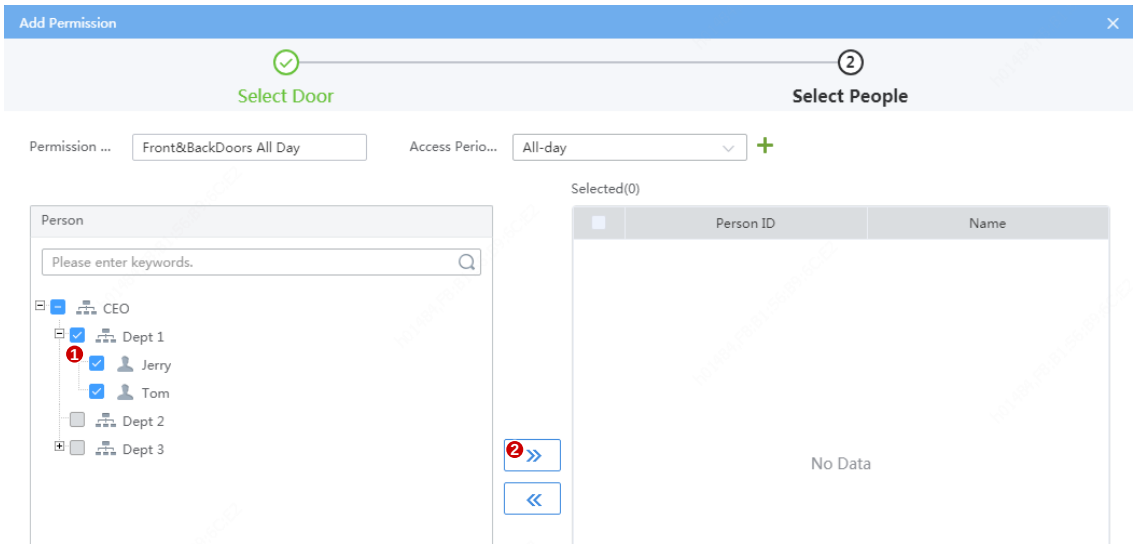
1. Select doors.



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.



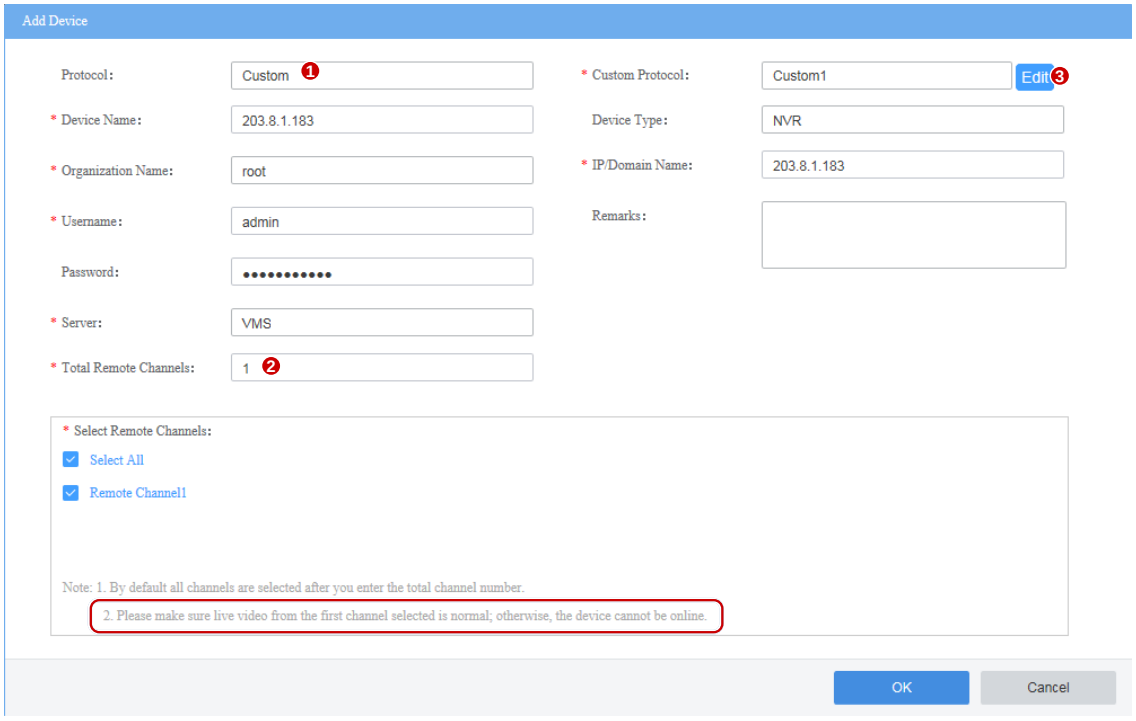
3. Click **Save**.

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

10 Appendix A Add a Device Using RTSP

Connect IPC or NVR via RTSP for live view.

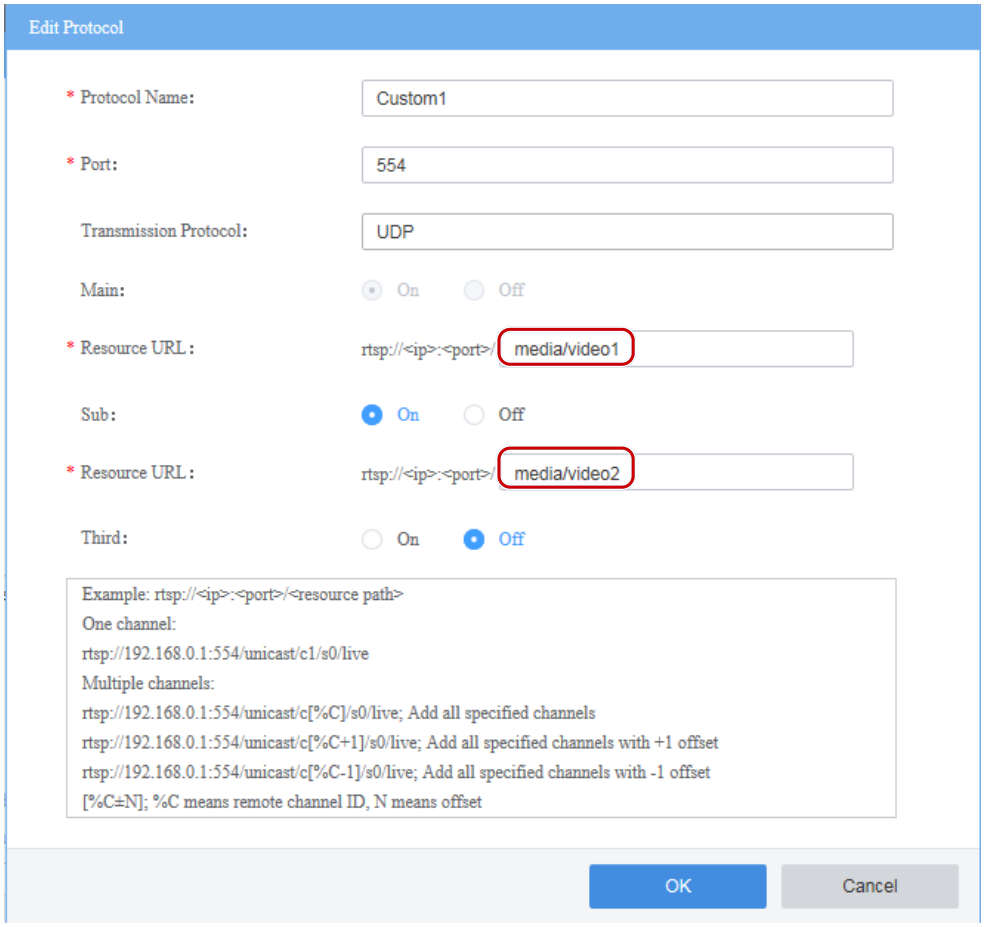
1. Click **Add** and complete the required settings.



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.



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.

11 Appendix B Customize Comprehensive Management Dashboard

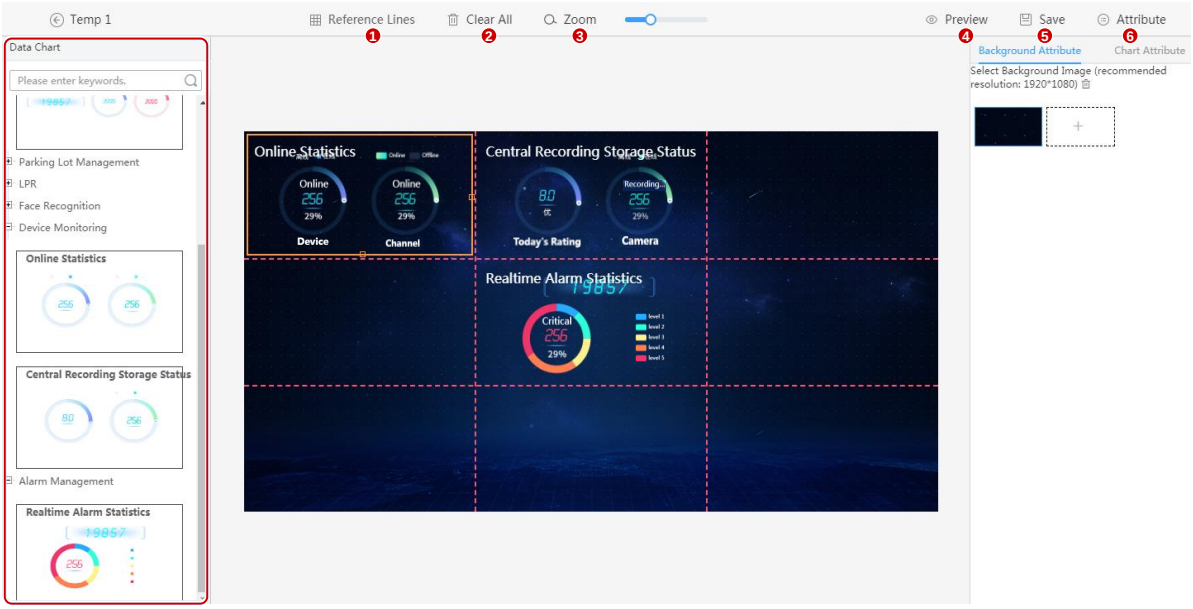
Customize the comprehensive management dashboard including the data modules displayed and the dashboard layout.

NOTE!

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

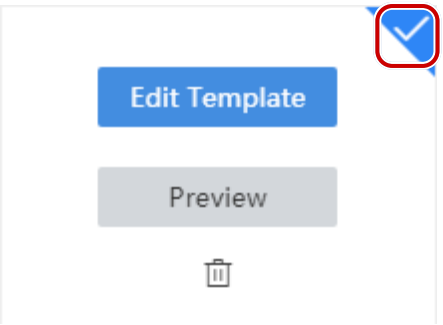
1. Click the expand button ( ) on the right side on the home page.
2. Click the **Custom** button in the top right corner.

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**, **Central Recording Storage Status**, and **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).