

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	2
General Organization	2
Custom Organization	2
User Management	4
Role	4
User	6
User Time Template	7
Device Management	8
Device	8
Channel	15
External Alarm	17
Link Resource	18
Server Management	18
Central Server	18
Distributed Server	19
Allocate Resource	19
4 Service Configuration	20
Recording Schedule	20
Time Template	20
Recording Schedule	22
Alarm Configuration	23
Alarm Configuration	23
Time Template	24
Contacts	24
Custom Alarm Level	25
Alarm Subscription	25
Recording Backup	26
Auto Backup	26
Local Backup	28
5 System Configuration	29
Basic Configuration	29
Basic	29
Date & Time	30
DST	30
Time Sync	30
Holiday	31
Disk Configuration	31

Array Configuration	31
Disk Management	33
Network Disk	34
Capacity Allocation	34
Disk Group	35
Advanced Configuration	35
Network Configuration	36
TCP/IP	36
EZCloud	37
DDNS	38
Port	38
Port Mapping	38
Email	39
VSS Server	39
VSS Local	41
Video&Image Database	41
Custom Route	42
Security Configuration	43
802.1x	43
ARP Protection	43
HTTPS	44
Telnet	44
Secure Password	44
IP Address Filtering	44
Maintenance	45
System Maintenance	45
Device Diagnosis Info	46
Delete Logs	46
Packet Capture	46
Network Detect	47
Bandwidth Usage	47
Stream Transmission Policy	48
Master/Slave Switch	48
Master to Slave	49
Slave to Master	49
Change Master Server	49
Configure Hot Standby	49
Batch Configuration	50
Batch Change Passwords	50
6 Video Service	51
Live Video	51
Start Live Video	51
Stop Live Video	52
Live Video Operations	52
Playback	53

Glossary	53
Search Recording	53
Playback Control	54
Recording Download	55
Local Settings	57
7 Statistics	57
General View	57
View the Numbers of Online/Offline Servers or Devices	58
View Info about Online/Offline Servers or Devices	58
View History Alarm Statistics of Servers or Devices	59
Server Statistics	60
Server Status	60
S.M.A.R.T. Test	60
Network	61
Online User	61
Bandwidth	61
Packet Loss	61
Server Performance	62
Storage Capacity	62
Recording Status	64
Device Statistics	64
Log	65
Server Alarm Logs	65
Device Alarm Logs	65
Operation Logs	66

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.

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 a mobile app for live view, playback and device management.

This manual describes how to use the Web Manager.

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. 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 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** on top of the **Login** button and then obtain a temporary password to log in. The temporary password is usable only to admin on a Local Area Network (LAN), and it is valid on the current day only. Please reset the password when logged in.
-

3 Basic Configuration

Basic configuration includes:

- [Organization Management](#): Configure general and custom organizations to manage devices.
- [User Management](#): Configure roles and assign permissions.
- [Device Management](#): Manage devices, channels, external alarms and link resources.

- [Server Management](#): View the basic info and status of central servers (primary and secondary servers) distributed servers (slave servers), allocate resources.

Organization Management

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



Organization management includes:

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

General Organization

Basic > Organization > General

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

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



NOTE!

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

Custom Organization

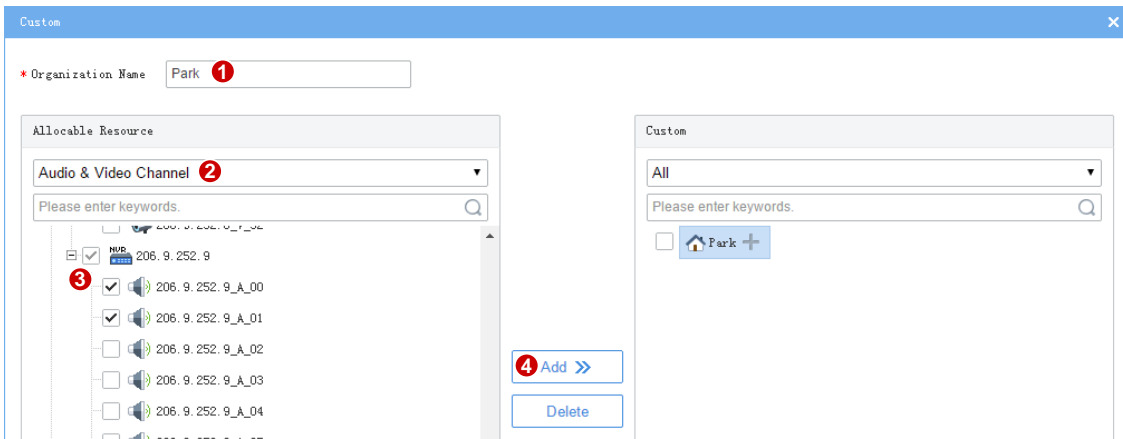
Basic > Organization > Custom

Custom organization provides a flexible way to manage devices by allowing you to:

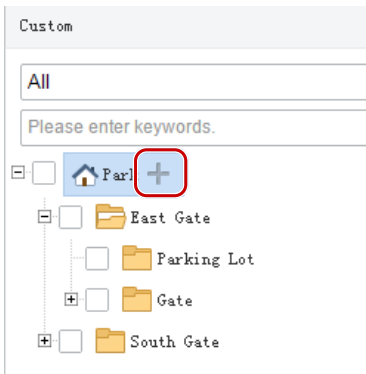
- Assign cameras under an NVR to different organizations.
- Assign cameras under different NVRs to one organization.
- Assign a camera to different organizations at the same time.
- Assign a custom organization to a role, so that users with this role can access certain resources on the software client.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

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

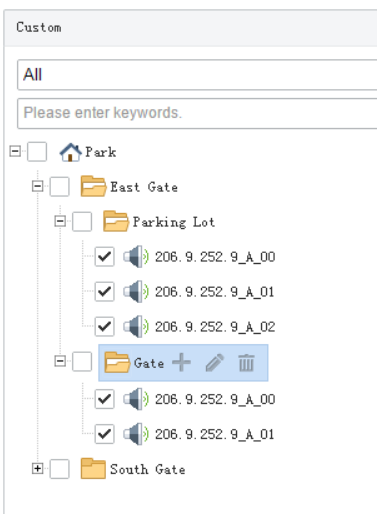
1. Enter a name. The organization name appears on the right.
2. (Optional) Select resource type (Audio & Video Channel). Enter keywords to filter if necessary.



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).



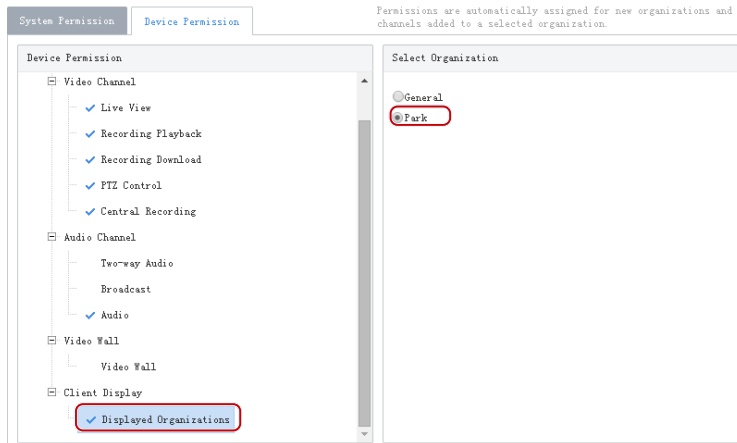
6. Click **OK**.



NOTE!

Operations to add, edit and delete organizations take effect immediately. Changes will be saved even if you click **Cancel**.

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 and management permissions. 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

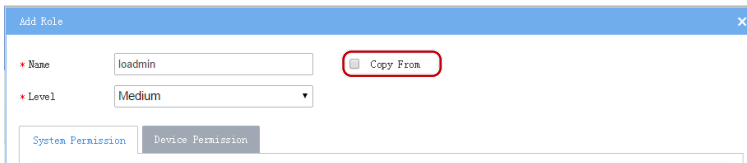
Roles are used to limit user's permissions, including:

- **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.

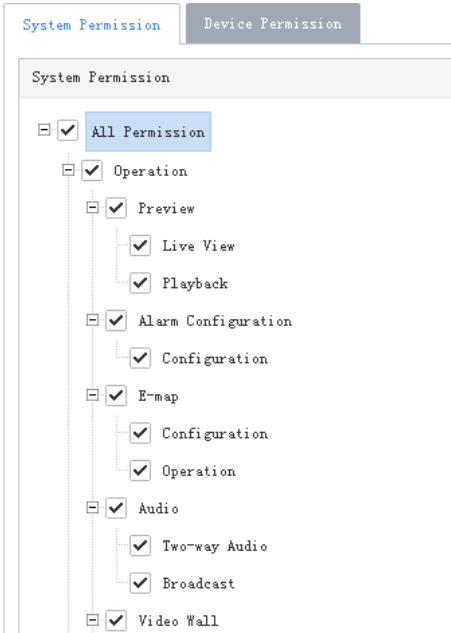
Click **Add** to add a new role:

1. Enter the role name.
2. Select a level.

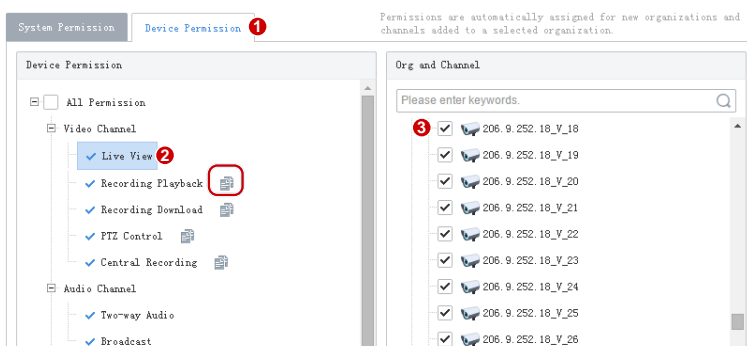
- (Optional) Select **Copy From**. The existing roles in the system are listed. Select a role and then edit permissions for the new role based on the selected role. Permissions of the selected role will not change.



- 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**.






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

User

Basic > User > User


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




NOTE!



The admin user cannot be edited, deleted or locked.

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

- Username: Must be unique in the system and cannot change once set.
- Role: Up to 16 roles are allowed for a user. The user will have all the permissions included in the roles assigned.
- Password: Used to access the system.
- Valid Date: Specify the period during which the user have access to the system.
- Time Template: See User Time Template.
- Click  to expand and enter more details.

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

- Click  to change roles, valid date and time template.

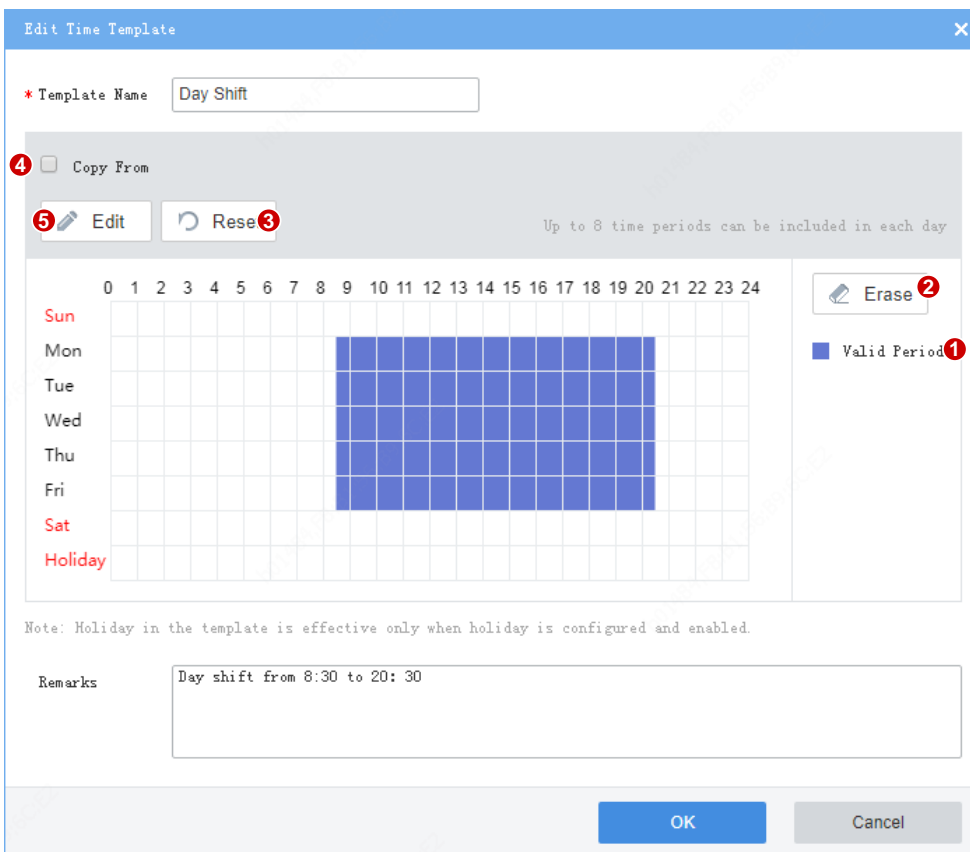
- Click  to change the user's password. The new password takes effect at the user's next login. Only admin can change other users' passwords.
- Click  to delete a user. A user who is logged in will be forced out of the system when deleted.

User Time Template

Basic > User > User Time Template

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

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



The screenshot shows the 'Edit Time Template' window. At the top, there's a text input for 'Template Name' with the value 'Day Shift'. Below it is a checkbox labeled 'Copy From' with a red '4' next to it. There are two buttons: 'Edit' with a red '5' and 'Reset' with a red '3'. A note says 'Up to 8 time periods can be included in each day'. The main area is a calendar grid with days of the week (Sun to Sat) and hours (0-24). A blue shaded area covers the hours 8:30 to 20:30 from Monday to Friday. To the right of the grid is an 'Erase' button with a red '2' and a legend for 'Valid Period' with a red '1'. Below the grid is a 'Remarks' text area containing 'Day shift from 8:30 to 20:30'. At the bottom are 'OK' and 'Cancel' buttons.

Draw a user time template:

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

- To apply the same settings to another day (e.g., Saturday), select the check box (1) and then click **Copy (2)**.

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Holiday
No.			Start Time			End Time	
1			08:30:00			20:30:00	
2							
3							
4							
5							
6							
7							
8							

Copy To: Select All

Sun Mon Tue Wed Thu Fri Sat Holiday

Copy **2**

OK Cancel

Device Management

Manage devices, channels, external alarms; link resources.

Before you start service operations on the software client, you need to add devices on the Web client first.

The VMS supports the following device types:

- Encoding device: IPC (IP camera or camera for short), NVR (Network Video Recorder), and encoder.
- Decoding devices: Built-in decoder, decoding card, and external decoding devices.
- Access gateway
- Smart device
- Network keyboard
- Cloud devices: Devices under cloud account(s).
- Alarm control: Alarm panel, alarm control panel (name may vary depending on the manufacturer).
- Access control: Door access control (or controller).

Device


Basic > Device > Device

Encoding Device

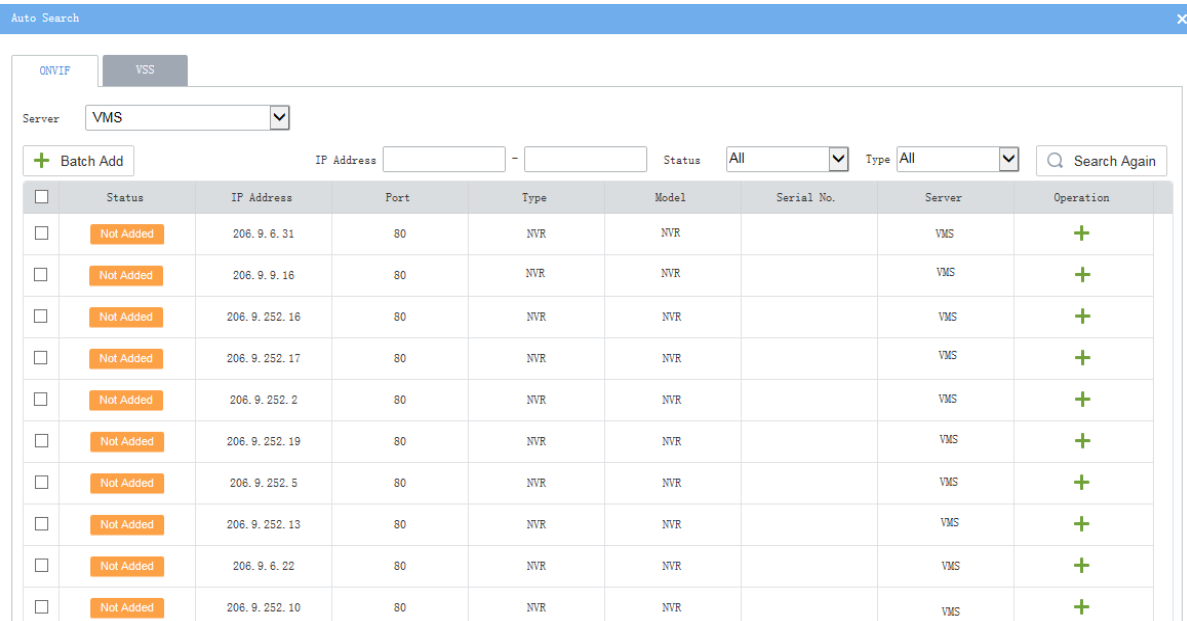
Encoding devices include encoder, IPC, and NVR.

1. Click the **Encoding Device** tab.
2. Click **Auto Search**. Encoding devices on the same network with the VMS are discovered.

To add an encoding device with known IP/domain, click **Add**.

3. On the device list, click  for the device to add. Check the settings and then click **OK**.

To add devices with same configurations (server, protocol, organization, username/password), select the checkbox for these devices and click then **Batch Add**.



<input type="checkbox"/>	Status	IP Address	Port	Type	Model	Serial No.	Server	Operation
<input type="checkbox"/>	Not Added	206.9.6.31	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.9.16	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.16	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.17	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.2	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.19	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.5	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.13	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.6.22	80	NVR	NVR		VMS	+
<input type="checkbox"/>	Not Added	206.9.252.10	80	NVR	NVR		VMS	+

4. You may search again with set conditions:

- **Server:** Search devices under the specified server. Selectable 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.




5. Check device status after they are added.


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.

6. Do the following as needed:

- To sync channel info (channel name) 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. You can view the updated channel info at **Basic > Device > Channel**.

- : Edit device info, including protocol, device type, device name, organization, IP/domain, port, username, password, and server.
- : Delete a device from the VMS.
- : Open the device's Web page.


- : Update channel names displayed on the VMS (click **Obtain Channel Info**), or edit channel names on the VMS (not on device); view alarm input/output channel information.

Decoding Device

Add decoding devices to convert media streams received on the network into video playable on a video wall. Decoding devices include the VMS' built-in decoder, decoding card (sold separately), and external decoding device.




NOTE!

If a decoding card is installed, DC_2 or DC_3 is Online (DC_2 for SLOT0, and DC_3 for SLOT1). You may rename the device for easier recognition by clicking .


IP Address	Device Name	Type	Protocol	Organization	Model	Status	Operation
127.0.0.1	DC_1	Built-in Decoder	Private	root	VMS	Online	
127.0.0.1	DC_2	Decoding card	Private	root	DC_HDMI_6	Online	
127.0.0.1	DC_3	Decoding card	Private	root	-	Offline	

1. Click the **Decoder** tab.
2. Click **Auto Search**. Decoding devices on the same network with the VMS are discovered. To add a device with known IP/domain, click **Add**.




3. On the device list, click  for the device to add. Check the settings and then click **OK**.
To add devices with same configurations (protocol, organization, username/password), select the checkbox for the devices and then click **Batch Add**.
4. You may search again with set conditions:

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

 **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.

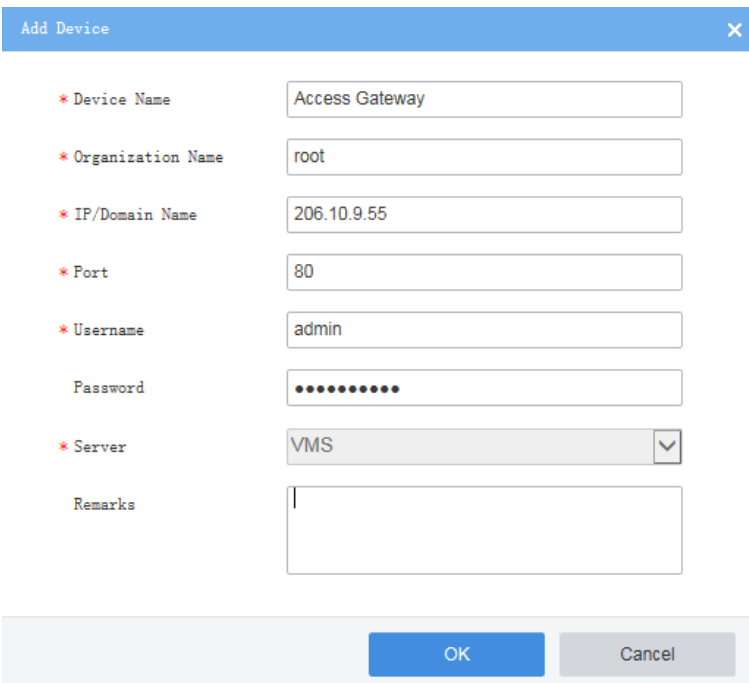
6. Do the following as needed:

-  : Edit device info, including protocol, device name, organization, IP/domain, port, username/password.
-  : Delete a device from the VMS.
-  : Open the device's Web page.

Access Gateway

Click the **Access Gateway** tab to add an access gateway (EZAgent), so the VMS can receive alarms from alarm control panels and door access controls, and users can arm/disarm zones, bypass/unbypass partitions, and open/close doors on the software client.

1. Click **Add**.




The screenshot shows a dialog box titled "Add Device" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- * Device Name: Access Gateway
- * Organization Name: root
- * IP/Domain Name: 206.10.9.55
- * Port: 80
- * Username: admin
- Password: (masked with 10 dots)
- * Server: VMS (dropdown menu)
- Remarks: (empty text area)

At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel".

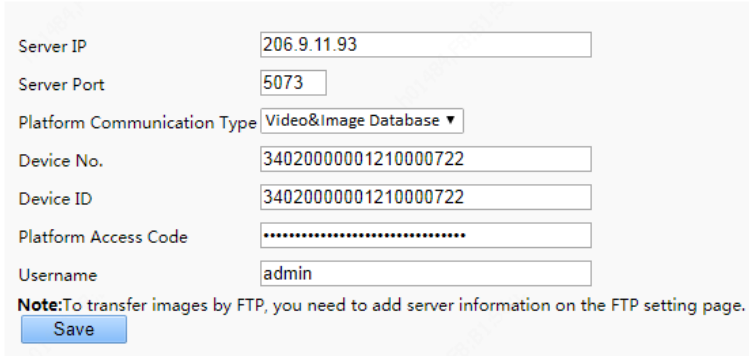
2. Complete settings in the dialog box. Some are described below:

- Device name: Set as needed for easy recognition.
- IP/Domain Name: IP address/domain name of the PC where the EZAgent server is installed.
- Port: 80
- Username: admin

- Password: Password of the EZAgent server.
3. Click **OK**. The access gateway appears online on the device list. You may click  to edit settings.

Smart Device

Smart devices refer to LPR cameras and face recognition cameras. Complete Video&Image Database configuration on the cameras at **System > Server > Intelligent Server** (the menu may vary with camera version) first, and then add smart devices in the same way as you add other encoding devices.

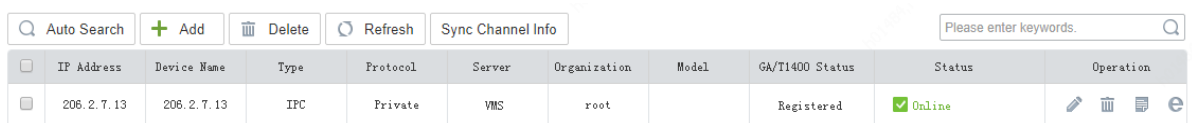






- Server IP: IP address of the VMS.
- Server Port: 5073
- Platform Communication Type: Video&Image Database
- Device No.: Set according to the format specified for the video&image database.
- Platform Access Code/Username: Used for connecting camera to the VMS.

After you complete the settings, add cameras on the VMS by **Auto Search** or **Add** (see [Encoding Device](#) for detailed steps).

- Auto Search: Cameras on the same network with the VMS are discovered.
- Add: Add a camera with known IP/domain.

When cameras are added and registered successfully, the **Registered** status is displayed. See [Video&Image Database](#) for more information.



IP Address	Device Name	Type	Protocol	Server	Organization	Model	GA/T1400 Status	Status	Operation
206.2.7.13	206.2.7.13	IPC	Private	VMS	root		Registered	Online	   

Network Keyboard

Add a network keyboard and use it to control PTZ cameras, set screen/window, or play video on a video wall. You need to enter the VMS' IP address and port number on the keyboard first. See the keyboard user guide for details.

Cloud Device




NOTE!



If an NVR has been added on the VMS via 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.

Click the **Cloud Device** tab, and log in to a cloud account to add, delete, edit and share cloud devices.

- Log in to cloud account: Click **Login** and then enter your cloud account info (or click **Register** to sign up). When logged in, your cloud account appears on the tree on the left, and cloud devices under this account are listed on the right. You may log in to multiple cloud accounts and manage devices under them.
- Add cloud device(s). Click **Add** to add the device to an online cloud account (cannot add VMS). The added device appears in the cloud device list. If connected, the device status is displayed as **Online**.

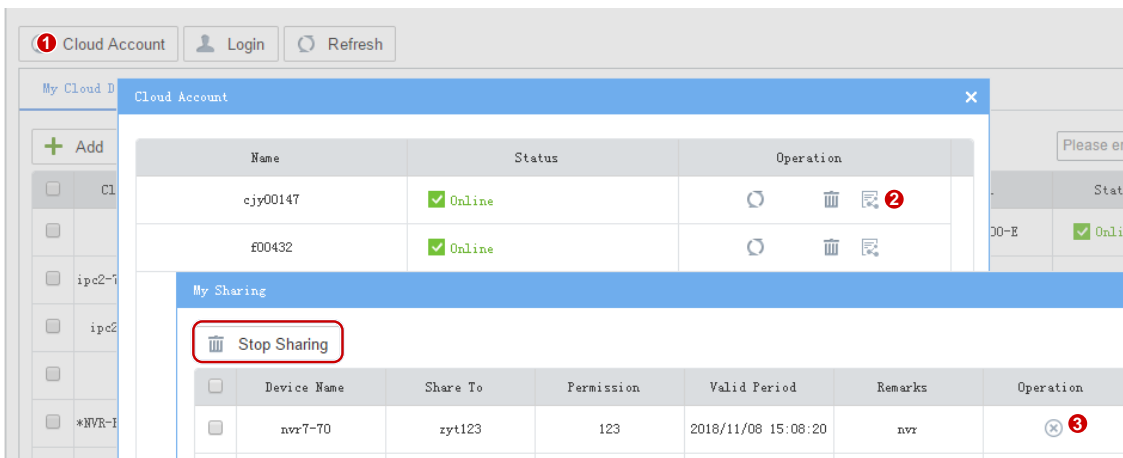
Cloud Name	Device Name	IP Address	Server	Organization	Type	Model	Connection Mod	Status	Operation
NVRclouddemo	NVRclouddemo	208.10.5.38	VMS	x03077	Other		Direct Connect	Online	[Edit] [Delete] [Share] [Print]

- Edit cloud device. Click  in the **Operation** column. If **Sync to Cloud** is selected, the changed name will be synced to cloud; otherwise, only the name saved on the VMS is changed. You can change the server in master/slave configuration.

- Delete cloud device from a cloud account. Click  in the **Operation** column, or select multiple items and click the **Delete** button.
- Share online cloud device: Click  in the **Operation** column to share an online device with other cloud accounts. You may set a sharing period and select a user to specify the permissions of the cloud account. The user and its permissions are configured on the shared device.
- Click **Cloud Account** to view and manage cloud accounts on the VMS.

Name	Status	Operation
cjoy00147	Online	[Refresh] [Delete] [Share]
f00432	Online	[Refresh] [Delete] [Share]

- View sharing from a cloud account and cancel sharing. Sharing can be cancelled by clicking the **Stop Sharing** button.




- To cancel sharing from other cloud accounts, click the **Devices Shared to Me** tab, select items and then click the **Stop Sharing** button.

Alarm Control

Add alarm controllers such as alarm control panels, so you can arm/disarm zones and bypass/unbypass partitions on the software client.

- Click **Add**.

- Complete settings in the dialog box. Some are described below:
 - Manufacturer and model: Choose correctly according to your alarm control device.
 - Name: Set as needed for easy recognition.
 - Username/password: Required if you want to arm/disarm or bypass/unbypass on the software client.
 - IP: IP address of the alarm control panel.
 - Port: Keep the default.
- Click **OK**. The alarm control appears online on the device list. You may click  to edit settings.

Access Control

Add access controllers so you can open or close doors on the software client.



- Click **Add**.
















- Manufacturer and model: Choose according to your access control device.
 - Name: Set as needed for easy recognition.
 - Name/password: Required if you want to open/close doors on the software client.
 - IP: IP address of the access control device.
 - Port: Keep the default.
2. Click **OK**.



Channel

Basic > Device > Channel

Channels include encoding channel, decoding channel, alarm input/output channel.

- Click the **Encoding Channel** tab to view encoding channels of the encoding devices you have added. Click an organization on the tree on the left to list encoding channels under the organization on the right. You may click some table headers (e.g., Channel Name) to sort the list. Click  to edit channel name. If a device is online, you may click  to open the Web page of the device to which the channel belongs; for example, to open the Web page of the NVR device.

Channel Name	Device	Device ID	Organization	Status	Operation
206.9.15.15_V_1	206.9.15.15	1	root	 Online	 
206.9.251.109_V_1	206.9.251.109	1	root	 Online	 
206.9.251.110_V_1	206.9.251.110	1	root	 Online	 
206.9.251.111_V_1	206.9.251.111	1	IPC2	 Online	 
206.9.251.112_V_1	206.9.251.112	1	IPC2	 Online	 

- Click the **Decoding Channel** tab to view decoding channels of the decoding devices you have added. Click an organization on the tree on the left to list decoding channels under the organization on the right. You may click some table headers (e.g., Channel Name) to sort the list. Click  to edit channel name. If a device is online, you may click  to open the Web page of the device to which the channel belongs.

Channel Name	Device	Device ID	Organization	Resolution (default)	Split Screen (max)	Status	Operation
DC_1_HDMI1	DC_1	1	root	SIGAB0	64	<input checked="" type="checkbox"/> Online	
DC_1_HDMI2	DC_1	2	root	SIGAB0	64	<input checked="" type="checkbox"/> Online	
DC_1_VGA	DC_1	3	root	SIGAB0	36	<input checked="" type="checkbox"/> Online	



NOTE!

VGA, HDMI1 and HDMI2 are decoding channels of the VMS' internal decoder DC_1.

- Click the **Alarm Channel** tab to view alarm input and output channels of the devices you have added. Click an organization on the tree on the left to list alarm channels under the organization on the right.

Select the **Alarm Input Channel** or **Alarm Output Channel** check box to filter the list. Click to edit channel name, alarm type or default status, or select multiple channels and click **Batch Config**.

Channel Name	Device	Device ID	Organization	Channel Type	Status	Operation	Type
206.9.15.15_0_relay_ou	206.9.15.15	1	root	Alarm Output Channel	<input checked="" type="checkbox"/> Online		N.O.
206.9.15.15_I_0	206.9.15.15	1	root	Alarm Input Channel	<input checked="" type="checkbox"/> Online		N.O.
206.9.15.15_I_1	206.9.15.15	2	root	Alarm Input Channel	<input checked="" type="checkbox"/> Online		N.O.
206.9.251.112_0_relay_	206.9.251.112	1	IPC2	Alarm Output Channel	<input checked="" type="checkbox"/> Online		N.O.



Tip!

- N.O. means normally open, and N.C. means normally closed.
- For an alarm output channel, **Delay** means the duration of the changed status before the default status is restored.

- Click the **Detector Channel** tab to add zones or partitions to an alarm control device.

Add
✕

* Device:

* Name:

* Type:

* Zone No.:

Partition No.:

- Click the **Door Channel** tab to add doors to a door access control device.

Add [X]

* Device: Newabel [v]

* Name: Door 1

* Type: Door Channel [v]

* Door No.: 01

OK Cancel

External Alarm

Basic > Device > External Alarm

Connect emergency bells to the VMS so that 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.

1. First link the emergency bell to the VMS by setting IP and port number of the VMS on the emergency bell. Currently only two emergency bell types are supported (Seho and Hitec). For Seho, the port number is 25000, and for Hitec, the port number is 9010.
2. Select an emergency bell and then configure.

Emergency Bell

Seho Emergency Bell 1

Name	Status	Region Code	District Code	Area Code	Operation
EmergencyBell001	Off	0	0	0	2
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	

3. Enable external alarm so emergency alarms will trigger actions. Set the three codes properly. The VMS uses the combination to identify an emergency bell.

Edit [X]

Name: EmergencyBell001

External Alarm: On Off

Region Code: 1

District Code: 1

Area Code: 1

OK Cancel

4. Configure alarm-triggered actions including recording, email and buzzer at **Service > Alarm**. See [Alarm Configuration](#).

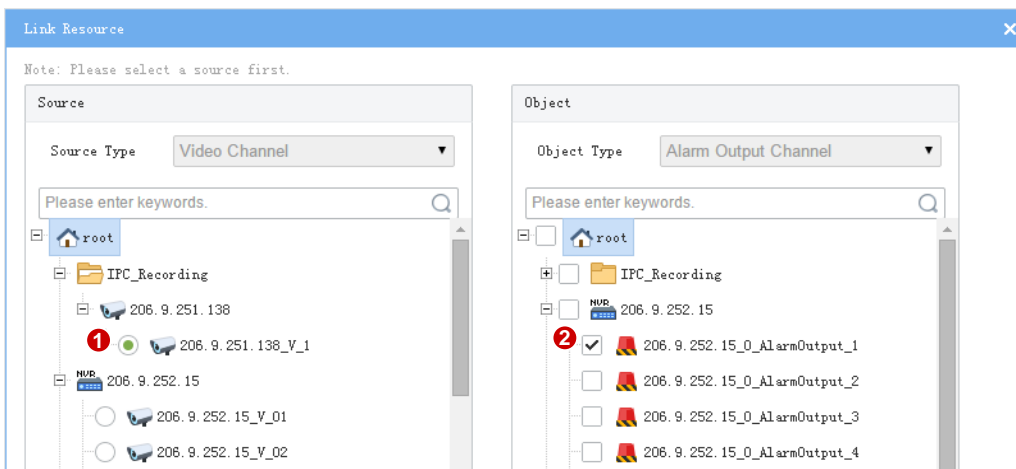
- Configure alarm-triggered actions including live view, preset (for PTZ cameras), alarm output, and alarm to video wall on the software client. See Alarm Configuration of the *Software Client User Manual*.


Link Resource

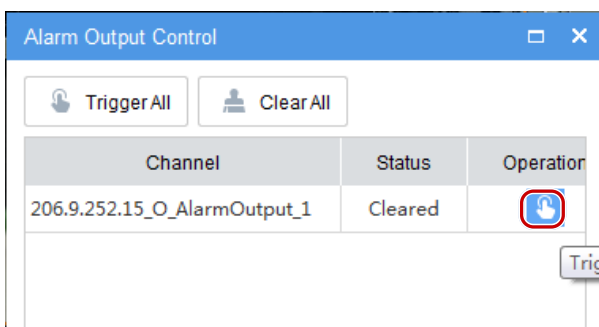
Basic > Device > Link Resource

By linking a source (video channel) to an object (alarm output channel), you can trigger alarm output manually on the software client.

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



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



Server Management

View information and status of the central servers (primary and secondary server) and distributed server (slave server); 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.

Details ✕

Connection Info

Max. Connected Devices 1000

Max. Connected Channels 2000

Max. Connected Storage 256

Max. Alarm Input 24

Max. Alarm Output 8

Bandwidth Info





Max. Input Bandwidth 512Mbps




Max. Output Bandwidth 384Mbps

Distributed Server

Basic > Server > Distributed Server

View info and status of the slave server; delete a slave server from a master server.

Name	IP	Serial No.	Type	Status	Operation
Slave	206.2.7.8	210235C2063185006277	Slave	 Offline - The slave server is not	  

- Click  to view connection and bandwidth info.
- Click  to rename a slave server.
- Click  to delete a slave server.

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 the slave server, a delete button appears when the mouse pointer moves close to a device (e.g., ). Clicking the button removes the device from the slave server and assigns it to the master server.

4 Service Configuration

Service configuration includes:

- [Recording Schedule](#): Configure recording schedules so the VMS records video in accordance with the set time and policy.
- [Alarm Configuration](#): Configure alarms to trigger specified actions; custom alarm levels.
- [Alarm Subscription](#): Configure alarm subscriptions so alarm subscribers only receive certain alarm messages; irrelevant alarm messages are filtered.
- [Recording Backup](#): Automatically back up recordings on an NVR to the VMS, or manually save recordings on the VMS to a USB drive.

Recording Schedule

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

Time Template

Service > Recording Schedule > Time Template

Each recording schedule uses a time template which specifies time and recording policy. All-day is the default time template in the system, by which video is recorded 24/7. You may change its name, but cannot delete this template.

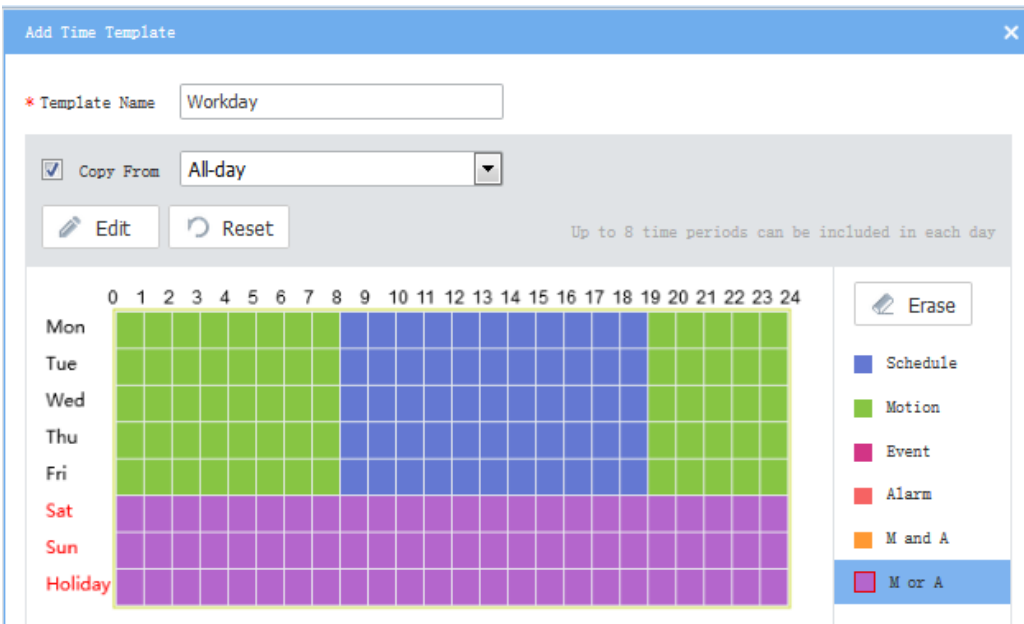
Click **Add** to create a time template:

1. Enter the template name, e.g., Workday. The template name must be unique in the system. A name that is easy to identify is recommended.
2. (Optional) Select **Copy From** and select a template from the drop-down list. Edit based on this template.
3. Click a type (e.g., Motion) under the **Erase** button and then drag the mouse to draw on the template. Use the **Erase** or **Reset** button to clear some or all settings. The types are described as follows.

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.

Type	Description
Alarm	Record video when tampering detection, alarm input, auto tracking, defocus detection or 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.

Example:



- Click **Edit** to set precisely, for example, to set schedule to 8:30-19:30 (currently 8:00-19:00) for Monday. The time periods must not overlap. Use the copy function to copy the same settings to other days.

Mon	Tue	Wed	Thu	Fri	Sat	Sun	Holiday
No.	Start Time	End Time	Plan Type				
1	00:00:00	08:30:00	Motion				
2	08:30:00	19:30:00	Schedule				
3	19:30:00	23:59:59	Motion				

- Click **OK**. The new time template is available when you add or edit a recording schedule.



NOTE!

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


Recording Schedule

Service > Recording Schedule > Recording Schedule

Assign a time template to cameras so that the VMS records video for the cameras according to the time template.

Click **Add** to add a recording schedule:

The screenshot shows the 'Add Recording Schedule' dialog box. On the left, a list of camera channels is displayed, with checkboxes next to each. Channels 206.9.252.6_V_18, 206.9.252.6_V_19, 206.9.252.6_V_20, and 206.9.252.6_V_21 are checked. On the right, the 'Time Template' is set to 'All-day', and a green plus icon is visible next to it. The 'Stream' is set to 'Main' and the 'Disk Group' is set to 'Normal Storage'. The 'Enable Recording Schedule' checkbox is checked. At the bottom, there are 'OK' and 'Cancel' buttons.

1. Select camera(s).
2. Select a time template; or click  to create one. See [Time Template](#).
3. Select a stream type.
4. Select a disk group: normal storage or IPSAN.
5. By default **Enable Recording Schedule** is selected. Clearing the check box will disable the recording schedule.
6. Click **OK**.



NOTE!

- Before setting 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.


Alarm Configuration

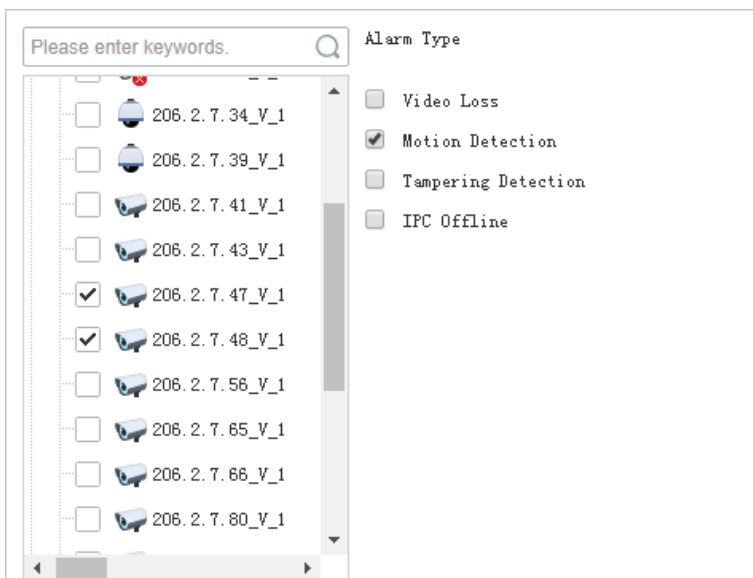
Configure alarms so that certain alarms at specified sources will trigger actions such as recording, buzzer and emails.

Alarm Configuration

Service > Alarm Configuration > Alarm Configuration

Click **Add** to add alarm configuration:

1. Enter a name (must be unique). A name that is easy to identify is recommended.
2. Select a time template (or click  to create one).
3. Set the alarm source, including type, specific source, and alarm type. When an alarm of the specified type (e.g., motion detection) occurs at the alarm source (i.e. cameras selected below), it will trigger the object to perform specified action(s).



The screenshot shows a web interface for configuring alarms. At the top, there is a search bar with the placeholder text "Please enter keywords." and a magnifying glass icon. Below the search bar is a list of camera sources, each with a checkbox and a camera icon. The sources are labeled with IP addresses and video streams: 206.2.7.34_V_1, 206.2.7.39_V_1, 206.2.7.41_V_1, 206.2.7.43_V_1, 206.2.7.47_V_1, 206.2.7.48_V_1, 206.2.7.56_V_1, 206.2.7.65_V_1, 206.2.7.66_V_1, and 206.2.7.80_V_1. The checkboxes for 206.2.7.47_V_1 and 206.2.7.48_V_1 are checked. To the right of the list is a section titled "Alarm Type" with four options: Video Loss, Motion Detection, Tampering Detection, and IPC Offline. The "Motion Detection" option is checked.

4. Set object(s) and action(s) to trigger. When an alarm of the specified type occurs at the alarm source, the object performs specified actions (e.g., recording).

Trigger Actions

[Recording](#) [Email](#) [Buzzer](#)

Please enter keywords.

- 206.2.7.30_V_1
- 206.2.7.34_V_1
- 206.2.7.39_V_1
- 206.2.7.41_V_1
- 206.2.7.43_V_1
- 206.2.7.47_V_1
- 206.2.7.48_V_1
- 206.2.7.56_V_1
- 206.2.7.65_V_1
- 206.2.7.66_V_1

Pre-Record Time s

Post-record Time s

Note: Please make a recording schedule before setting triggered recording.



NOTE!

- You can set **Pre-Record Time** and **Post-Record Time** for alarm-triggered 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.
- 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 recording lasts after the alarm occurs.
- To trigger recording, a recording schedule must be set for the object camera (see [Recording Schedule](#)). To trigger email, you also need to complete email settings (see [Email](#)). To trigger buzzer, you need to select buzzer.

5. Enter a description in the **Remarks** field.
6. Click **OK**.

Time Template

Service > Alarm Configuration > Time Template

Configure time templates for alarm configuration. See [Time Template](#) for reference.

Contacts

Service > Alarm Configuration > Contacts

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

Click **Test email** to test.



NOTE!

An email server must be configured before testing the email. For details, see [Email](#).

Custom Alarm Level

Service > Alarm Configuration > Custom Alarm Level

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

Select an alarm level from the drop-down list for the alarm type. The setting is saved directly.




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

Alarm Subscription

Service > Alarm Subscription > Alarm Subscription

Add alarm subscribers to receive certain types of alarm messages from specified alarm sources; irrelevant alarm messages will be filtered.

Click **Add** to add alarm subscription:

1. Enter a subscription name (must be unique). A name that is easy to identify is recommended.
2. Select the user and then click . The user is added as an alarm subscriber. Click **Next**.
3. Select alarm source(s) and type(s). Different alarm source types have different alarm types. Configure all alarm sources and alarm types as needed. The following takes video channel as an example.

Video Channel

Please enter keywords.

<input checked="" type="checkbox"/>		206.9.15.15_V_1
<input checked="" type="checkbox"/>		206.9.251.109_V_1
<input checked="" type="checkbox"/>		206.9.251.110_V_1
<input checked="" type="checkbox"/>		206.9.251.133_V_1
<input checked="" type="checkbox"/>		206.9.251.142_V_1
<input checked="" type="checkbox"/>		206.9.251.143_V_1
<input checked="" type="checkbox"/>		206.9.251.147_V_1
<input type="checkbox"/>		206.9.251.164_V_1
<input type="checkbox"/>		206.9.251.168_V_1
<input type="checkbox"/>		206.9.251.172_V_1
<input type="checkbox"/>		206.9.251.176_V_1

Alarm Type

- Select All
- Video Loss Started
- Video Loss Ended
- Motion Detection Started
- Motion Detection Ended
- Tampering Detection Started
- Tampering Detection Ended
- Scheduled Recording Failure
- Scheduled Recording Failure Cleared
- IPC Online
- IPC Offline

4. Click **Save**.



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.

Recording Backup

Auto Backup

Service > Recording Backup > Auto Backup

Create a task to schedule the automated replication of recordings from an NVR or an onboard SD card of a camera to the VMS.

You need to configure storage for backup use first (see [Capacity Allocation](#) and [Disk Group](#)).

Note: Auto backup is not available for cloud devices connected by TURN (see connection mode under **Basic > Device > Cloud Device**).

1. Click **Add**. Select channel(s) and set task parameters. Some parameters are described as follows.

- Recording Date: Specifies the date of recordings to back up (cannot back up recordings of the current day). For example, if you choose 1 day ago, then the task that executes on Monday backs up recordings of Sunday.
 - Scheduled Execution Time: Tasks execute one by one in each schedule. A task is waiting if it cannot execute at the scheduled time.
 - Recording Start Time and Recording End Time: Specifies the recording to back up.
 - Recording Type: User can choose certain types of recordings to back up, for example, manual recording, motion.
2. A message will appear on the screen if the backup task exceeds the VMS' storage capacity; in this case, please go to **Statistics > Server > Storage Capacity** to view storage usage (see [Storage Capacity](#)). The created backup task appears in the list.

<input type="checkbox"/>	Device Name	Channel Name	Status	Operation
<input type="checkbox"/>	206.9.252.14	206.9.252.14_V_01	Backing up	
<input type="checkbox"/>	206.9.252.14	206.9.252.14_V_02	No task	

- The **Status** column shows task status; for example, No task means no task is being executed.
- Click to pause an on-going schedule.
- Click to edit a schedule.
- Click to delete a schedule.

NOTE!

Editing a schedule (e.g., recording end time) after a backup task has started does not change the current task; the changed settings become effective when next time a task is created.

- Click to view task details of a schedule. Clicking deletes a task.

No.	Status	Progress	Start Time	End Time	Operation
1	Backing up	<div style="width: 7%;"><div style="width: 7%;"></div></div> 7%	2018-04-07 01:00:00	2018-04-07 02:00:00	


If backup is interrupted for some reason (for example, NVR is disconnected), you may use **Batch Resume** to restart the interrupted backup after the cause of interruption is eliminated.

Local Backup

Service > 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.

The screenshot shows the 'Local Backup' interface. On the left, there is a tree view of the organization structure with folders for 'root', 'GB', 'IPC', and 'NVR'. Below this is a search bar. On the right, there are search filters for 'Recording Type' (All), 'File Type' (All), and 'Start and End Time' (2018/06/21 00:00:00 - 2018/06/21 23:59:59). A 'Search' button and a 'Reset' button are present. Below the filters, a 'Backup' button is shown with 'Total: 4883.45MB'. The main area contains a table of recordings with columns for Channel Name, Start Time, End Time, Recording Size (MB), Recording Type, File Type, and Operation. The table lists 20 recordings for channel 206.9.254.4_V_1. At the bottom, there is a pagination control showing 'View 1 - 20 of 204 20' and 'Page 1 of 20'.

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 existing 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.

5 System Configuration

System configuration includes:

- [Basic Configuration](#): Basic device info, time and time synchronization, DST, and holiday configuration.
- [Disk Configuration](#): Array configuration, disk management, network disk, capacity configuration, disk group, and advanced configuration.
- [Network Configuration](#): Basic network settings, cloud, DDNS, port, port mapping, email, VSS, and Video&Image database, custom route.
- [Security Configuration](#): Includes 802.1x, ARP protection, HTTPS, Telnet, secure password, and IP address filtering.
- [Maintenance](#): Restart or restore VMS, collect device diagnosis info, log cleanup, capture packets, detect network, network bandwidth usage, and stream transmission policy.
- [Master/Slave Switch](#): Configure hot standby, switch master/slave VMS.
- [Batch Configuration](#): Change device passwords in batches.

Basic Configuration

Basic

System > Basic > Basic Setup

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.	C:-----:-----
Firmware Version	B1118P10
Video&Image Database Version	VIID-B100
Running Time	1 day(s) 19 hour(s) 27 minute(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 system time of the VMS syncs 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 NTP server.

Time Zone	(UTC+08:00) Beijing, Kuala Li ▼
Date Format	YYYY-MM-DD ▼
Time Format	24-hour ▼
System Time	2017-12-13 15:27:52 ⌚ <input type="checkbox"/> Sync with Computer
Auto Update	<input type="radio"/> On <input checked="" type="radio"/> Off

Save

DST

System > Basic > DST

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

DST	<input checked="" type="radio"/> On <input type="radio"/> Off	Note: Please keep DST settings on the PC consistent with that on the devices.		
Start Time	Mar ▼	2nd ▼	Sun ▼	2
End Time	Nov ▼	1st ▼	Sun ▼	2
DST Bias	60 minutes ▼			

Save

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.

Sync Device Time	<input checked="" type="radio"/> On <input type="radio"/> Off
Interval	<input type="text" value="1"/> hour (s)

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, including:

- [Array Configuration](#): turn on/off RAID mode, create RAID by **One-click Create** or **Manual Create**.
- [Disk Management](#): view disk info such as slot, status and space usage, modify disk property (read-only or read/write), and format disks.
- [Network Disk](#): Add IPSAN, format disk, modify disk property.
- [Capacity Allocation](#): allocate VMS or IPSAN disk space for recording storage.
- [Disk Group](#): configure disk group property.
- [Advanced Configuration](#): overwrite or stop recording when the assigned space on the VMS is used up.

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 5-1 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 ARRAYn format, e.g., ARRAY1.	Arrays are named by user (must be unique).
Automatically create array(s) based on the number of hard disks available: <ul style="list-style-type: none"> • 2 HDDs: RAID1 • 3 HDDs: RAID5 (no hot spare) • 4-8 HDDs: RAID5 (1 hot spare) • 9-16 HDDs: 2 RAID5 (1 hot spare) 	<ul style="list-style-type: none"> • 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 even number (N), then each RAID5 has $(N-1)/2$ disks; if N is an odd 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 5-2 Supported RAID Types and Corresponding Disks

RAID Type	HDD (pcs)
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 .

Physical Disk Array

Note: Creating an array with disks of different capacity wastes disk space.


One-click Create + Manual Create

<input type="checkbox"/>	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.

							Total: 19562 GB F
	Format	Read Only	Read/Write				
	Slot ↑	Device	Status	Total (GB)	Free (GB)	Property	Operation
	1	Local Disk	Normal	1863.02	1861.75	Read/Write	
	2	Local Disk	Normal	931.51	930.25	Read/Write	
	3	Local Disk	Normal	1863.02	1861.75	Read/Write	
	4	Local Disk	Normal	2794.52	2792.00	Read/Write	
	5	Local Disk	Normal	1863.02	1861.75	Read/Write	
	6	Local Disk	Normal	931.51	930.25	Read/Write	

- 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.

							Total: 7450 GB F
	Format	Read Only	Read/Write				
	Slot ↑	Device	Total (GB)	Free (GB)	Property	Operation	
	1	Array Disk	3724.55	3718.25	Read/Write		
	2	Array Disk	3724.55	3723.25	Read/Write		

- 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.

							Total: 19562 GB F
	Format	Read Only	Read/Write				
	Slot ↑	Device	Status	Total (GB)	Free (GB)	Property	Operation
	1	Local Disk	Not Formatted	1863.02	1863.02	Read/Write	
	2	Local Disk	Not Formatted	931.51	931.51	Read/Write	
	3	Local Disk	Not Formatted	1863.02	1863.02	Read/Write	
	4	Local Disk	Not Formatted	2794.52	2794.52	Read/Write	
	5	Local Disk	Not Formatted	1863.02	1863.02	Read/Write	
	6	Local Disk	Not Formatted	931.51	931.51	Read/Write	

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.

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- * Type: IPSAN (dropdown menu)
- * IP: 192.168.0.1 (text input)
- * Target: Target1 (text input)
- * Initiator: Initiator1 (text input)
- Username: (empty text input)
- Password: (empty text input)

At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel" (grayed out).

- 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

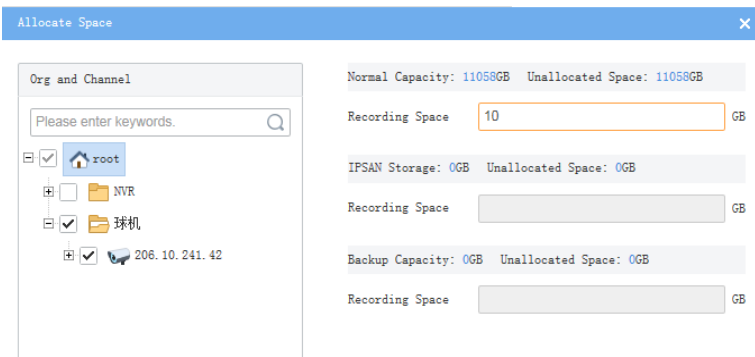
Allocate recording storage space for cameras. The total storage space assignable depends on configurations in [Disk Group](#) and [Network Disk](#).





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

Disk Group

System > Disk > Disk Group

1. On the **Disk List** tab, select or view property in the **Disk Group Property** drop-down list:
 - Normal Storage: used to store recordings for specified cameras.
 - Backup Storage: used to automatically back up recordings on specified NVRs.
 - IPSAN: added network disks.

Disk No. ↑	Total (GB)	Free (GB)	Type	Status	Disk Property	Disk Group Property
1	16764.87	8984.25	Array Disk		Read/Write	Backup Storage ▼
2	13038.49	13036.50	Array Disk		Read/Write	Normal Storage ▼
3	19659.01	16340.25	Array Disk		Read/Write	Normal Storage ▼
4	6517.97	6516.25	Array Disk		Read/Write	Normal Storage ▼
5	11175.85	11173.75	Array Disk		Read/Write	Normal Storage ▼
0-1	2000.00	254.50	Network Disk	Normal	Read/Write	IPSAN ▼
0-2	2000.00	271.00	Network Disk	Normal	Read/Write	IPSAN ▼
0-3	2000.00	506.00	Network Disk	Normal	Read/Write	IPSAN ▼
0-4	2000.00	351.25	Network Disk	Normal	Read/Write	IPSAN ▼
0-5	3000.00	737.75	Network Disk	Normal	Read/Write	IPSAN ▼

2. After configuration is complete, click the **Disk Group Property** tab to view capacity of normal storage, backup storage, and IPSAN.
3. Allocate storage at **Disk > Capacity**.

Advanced Configuration

System > Disk > Advanced

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

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

When HDD Full

Overwrite When storage is full, overwrite previous recordings.
 Stop Please allocate space. Overwrite is still effective for cameras with no space allocated.

Save



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 server, and default route.

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

Save



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 must belong to different network segments.

- Working mode

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

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


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

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

EZCloud

System > Network > EZCloud

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

EZCloud	<input checked="" type="radio"/> On <input type="radio"/> Off
Server Address	en.ezcloud.uniview.com
Register Code	XXXXXXXXXXXXXXXXXXXX
Device Status	Online <input type="button" value="Delete"/>
Username	f00432
Device Name	vms2-7-8
Service Agreement	http://en.ezcloud.uniview.com/doc/termsofservice.html
Detect Network Type	<input type="button" value="Detect"/>
Scan QR Code	

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

- Scan QR Code: Scan the QR code with the mobile client to add the VMS to cloud.

DDNS

System > Network > DDNS

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

DynDNS

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

No-IP

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

EZDDNS

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

Port

System > Network > Port

Configure HTTP, HTTPS, RTSP and alarm ports.

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
RTSP Port	<input type="text" value="554"/>
Alarm Port	<input type="text" value="52000"/>

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

Save

Port Mapping

System > Network > Port

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

The VMS supports two port mapping modes:

- UPnP

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

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

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



NOTE!

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

Email

System > Network > Email

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

Server Authentication	<input checked="" type="radio"/> On <input type="radio"/> Off
Username	<input type="text" value="zyl"/>
Password	<input type="password" value="*****"/>
SMTP Server	<input type="text" value="203.131.1.57"/>
SMTP Port	<input type="text" value="25"/> <input type="checkbox"/> Enable TLS/SSL
Sender Name	<input type="text" value="001"/>
Sender Address	<input type="text" value="zyl@z03079.com"/>



NOTE!

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

VSS Server

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

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

Complete basic settings

VSS Server	<input checked="" type="radio"/> On <input type="radio"/> Off		
Device	Offline:Unregistered	Organization	General
SIP Server ID	3400000002000000010	SIP Server Domain	3402000001
SIP Server IP	127.0.0.1	SIP Server Port	5061
Username	admin	Password	*****
Registration Validity(s)	3600	Administrative Division Code	3402
Heartbeat Cycle(s)	30	Max Heartbeat Timeout Counts	3
Live View TCP Connection	Auto-Negotiation	Stream Encapsulation Format	Auto-Negotiation

[Save](#)

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

Share channels with higher-level management platform

For channels that are shared with the higher-level management platform, operators can search these channels on the platform and subscribe to alarms of these channels.

The screenshot shows a web interface for channel management. At the top, there are tabs for 'Video Channel', 'Alarm Input', and 'Audio Channel'. A 'Status' dropdown is set to 'All' and a 'Search' button is present. Below the tabs, there is a 'Quick Config' button and a warning message: 'Quick Config is effective only to channels with an empty Channel ID.' A search bar is also visible. On the left, an 'Organization' tree is shown with a search bar and a list of organizations including 'root (34020000002160000001)', 'GB (34020000002160000005)', 'IPC (34020000002160000004)', 'WVS (34020000002160000003)', 'POE (34020000002160000045)', 'test (34020000002160000050)', and 'ZJB (34020000002160000053)'. The main area displays a table of channels with columns for Channel Name, Channel ID, Organization ID, Alarm Level, Longitude, Latitude, Status, and Operation. The table contains 7 rows of data, all with a 'Shared' status.

Channel Name	Channel ID	Organization ID	Alarm Level	Longitude	Latitude	Status	Operation
206.2.7.207	3402000001321302742	34020000002160000005	Level 4	0	0	Shared	
206.2.7.213_V_1	34020000011320000001	34020000002160000004	Level 4	0	0	Shared	
206.2.7.214_V_1	34020000011320000002	34020000002160000004	Level 4	0	0	Shared	
206.2.7.212_V_1	34020000011320000003	34020000002160000004	Level 4	0	0	Shared	
206.2.7.204_V_1	34020000011320000004	34020000002160000004	Level 4	0	0	Shared	
206.2.7.211_V_1	34020000011320000005	34020000002160000004	Level 4	0	0	Shared	

1. Select the desired organization from the **Organization** drop-down list and then click **Save**. The organization appears on the organization tree.
2. Select the desired channel type to share: video channel, alarm input channel or audio channel.
3. Click **Quick Config** to assign channel IDs to channels with no channel IDs. Set the basic code, and then the system will create and assign channel IDs based on the basic code.



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 with no 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 channel ID or any other organization ID.

4. After being assigned channel IDs, the channels are in **Shared** status, you can search and find these channels on the higher-level platform and subscribe to alarms of these channels.
5. To stop sharing certain channels, select channels and click **Stop Sharing**. When sharing is stopped, the status changes to **Unshared**, and the higher-level platform cannot receive subscribed alarms of these channels.



NOTE!

An audio channel's sharing status 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 > VSS Local

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

SIP Server ID	<input type="text" value="34020000002001300023"/>
SIP Server Port	<input type="text" value="5063"/>
Heartbeat Cycle(s)	<input type="text" value="60"/>
Max Heartbeat Timeout Counts	<input type="text" value="3"/>

Video&Image Database

System > Network > Video&Image Database Config

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

Video&Image Database Configuration

Video&Image Database Server...	<input checked="" type="radio"/> On <input type="radio"/> Off		
Device	Online		
Video&Image Database Server...	<input type="text" value="127.0.0.1"/>	Video&Image Database Server...	<input type="text" value="55001"/>
Username	<input type="text" value="admin"/>	Password	<input type="password" value="*****"/>
<input type="button" value="Save"/>			

- 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	<input type="text" value="34020000005030000011"/>	Format: 8-char center code+2-char industry code+3-char type code+7-digit SN(SN must be digits; others can be digits or letters).
Video&Image Database Local ...	<input type="text" value="5073"/>	
<input type="button" value="Save"/>		

- 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.

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.

Status	<input checked="" type="radio"/> On <input type="radio"/> Off
NIC	<input type="text" value="NIC1"/>
* Subnet ID	<input type="text" value="203.0.0.0"/>
* Subnet Mask	<input type="text" value="255.0.0.0"/>
* Gateway	<input type="text" value="206.2.7.1"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	



NOTE!

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

Security Configuration

802.1x

System > Security > 802.1x

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

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

Select NIC	NIC1
802.1x	<input checked="" type="radio"/> On <input type="radio"/> Off
Type	EAP-MD5
EAPOL Version	1
Username	admin
Password	*****

[Save](#)



NOTE!

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

ARP Protection

System > Security > ARP Protection

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

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

Select NIC	NIC1
ARP Protection	<input checked="" type="radio"/> On <input type="radio"/> Off
Gateway	206.9.0.1
Gateway MAC Address <input type="checkbox"/> Auto <small>Using automatically obtained MAC address may incur the risk of being attacked.</small>

[Save](#)



NOTE!

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

HTTPS

System > Security > HTTPS

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

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

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



NOTE!

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

Telnet

System > Security > Telnet

Access the device through Telnet for maintenance.

Secure Password

System > Security > Secure Password

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

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

Password Mode Friendly Password Enhanced Password

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

Save

IP Address Filtering

System > Security > IP Address Filtering

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

Start IP	End IP	Operation
206.10.9.1	206.10.9.10	
206.10.9.13	206.10.9.19	

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



NOTE!

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

Maintenance

System Maintenance

System > Maintenance > Maintenance

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

Restart	Restart device.
Default	Restore all factory default settings except network, user and event settings.
Factory Default	Restore all factory default settings.
Export Configuration	Export configuration file.
Export Diagnosis Info	Export diagnosis information.
Import Configuration	<input type="text"/> Import
Local Upgrade	<input type="text"/> Upgrade
Plug-in Log Path	C:\Users\user\Surveillance_V... Open

- **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 using version files saved on the computer. The VMS will restart.
- **Plug-in Log Path:** Click **Open** to view plugin logs. Click the folder icon () to set 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 load 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.

Latest Diagnosis Info | History Diagnosis Info


Save File To:

Export Diagnosis Info

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

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

Latest Diagnosis Info | History Diagnosis Info

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

Delete Logs

System > Maintenance > Delete Logs

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

Operation Logs	Max. Retention	<input type="text" value="30"/>	day(s) (0 means do not delete.)
Alarm Logs	Max. Retention	<input type="text" value="30"/>	day(s) (0 means do not delete.)

Packet Capture




System > Maintenance > Packet Capture

Capture packets for troubleshooting or analysis.

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

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

click  to delete a task.

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

Port	<input type="radio"/> All <input checked="" type="radio"/> Specify <input type="radio"/> Filter <input type="text" value="80"/>
IP Address	<input type="radio"/> All <input type="radio"/> Specify <input checked="" type="radio"/> Filter <input type="text" value="192.168.1.65"/>
Select NIC	<input type="text" value="NIC1"/> 206.9.12.65
Packet Size (Bytes)	<input type="text" value="8192"/>

Create Task Up to 5 tasks allowed.

<input type="checkbox"/>	Task	Status	Operation
<input type="checkbox"/>	101_NIC1_FILTER_192.168.1.65_SPECIFY_80	Waiting	



NOTE!

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

Network Detect

System > Maintenance > Net Detect

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

Test Address	<input type="text" value="206.10.9.57"/>	<input type="button" value="Test"/>
Test Result	Delay:0.39ms, Packet Loss:0%	

Bandwidth Usage

System > Maintenance > Bandwidth Usage

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

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

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

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

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

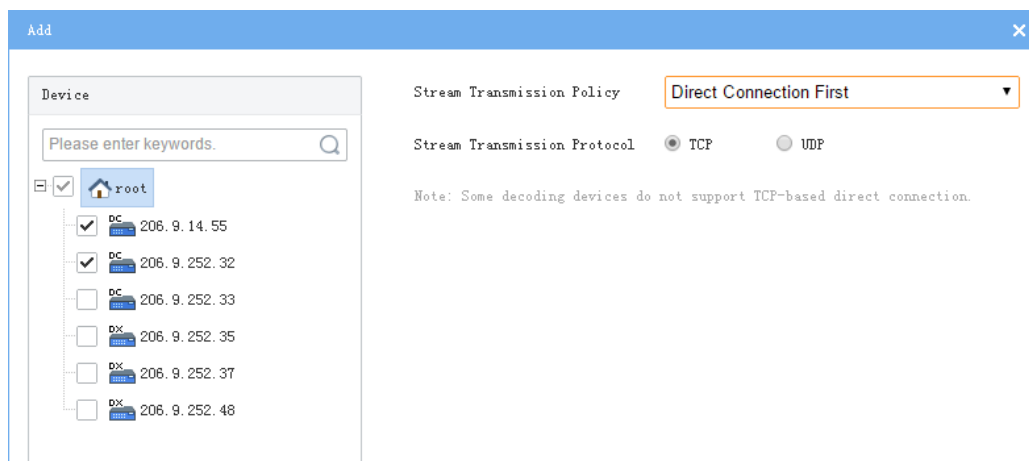
Stream Transmission Policy

System > Maintenance > Stream Transmission Policy

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

If the policy is set to **Direct Connection First**, the VMS will determine whether conditions are satisfied (e.g., remaining output bandwidth of IPC/NVR) for direct transmission when starting streams. If conditions are satisfied, streams will be directly transmitted from IPC/NVR to the decoder, saving 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.

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!

- Add a slave server on its Web manager (switch to slave mode and then enter the master's IP address).
 - If the software versions of the master/slave VMS 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 VMS is specified. After the max number is reached, no more slave VMS can be added.
 - The slave VMS is inaccessible 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 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).
 - Clear the **Enable Hot Standby** check box 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.
-

Master/Slave Switch	
Master/Slave Switch	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Secondary Server	<input checked="" type="checkbox"/> Enable Hot Standby
Hot Standby Config	
Role	<input checked="" type="radio"/> Working Mode <input type="radio"/> Standby Mode <input checked="" type="checkbox"/>
Virtual IP	<input type="text" value="206.9.13.36"/> <input checked="" type="checkbox"/> <small>Note: IP that is not in use in the network.</small>
Subnet Mask	<input type="text" value="255.255.255.0"/> <input checked="" type="checkbox"/>
Virtual Route ID	<input type="text" value="1"/> <input checked="" type="checkbox"/> <small>Note: Must be unique in multi-hot-standby configuration.</small>
Secondary Server Service IP	<input type="text" value="206.9.12.65"/> <input checked="" type="checkbox"/>
Secondary Server Heartbeat IP	<input type="text" value="206.9.12.65"/> <input checked="" type="checkbox"/> <input type="button" value="Check"/>
Alarm and Operation Log Data	<input checked="" type="checkbox"/> Clear
<input type="button" value="Save"/>	

- 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 client.
 - 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: Select **Clear** will improve the speed of synchronization between the primary and secondary servers.
- Click **Save**.

Batch Configuration

System > Batch Config

Batch Change Passwords

Batch change passwords of NVRs under the master or slave VMS server.

This function is not available to VSS devices and cloud devices. For devices under a slave server, their passwords can only be changed from the master server.

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

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

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

6 Video Service

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



NOTE!

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.,  206.9.252.15_V_01).
- 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


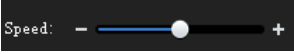




Use the toolbar at the bottom. Some buttons on the toolbar are only effective to the currently selected window, and the buttons may vary with camera.



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 stream type: main stream, sub stream, third stream (may vary with camera).
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

Button	Description
	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  .

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).

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Search


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

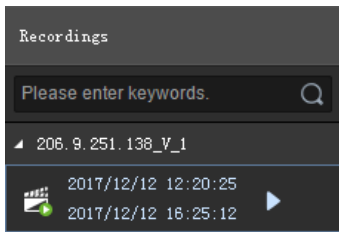
Search results are shown on the timeline (as known as progress bar) and the **Recordings** list on the right. Different recording types are shown with different colors on the timeline: blue for normal (scheduled), and red for event (alarm).

 **TIP!**

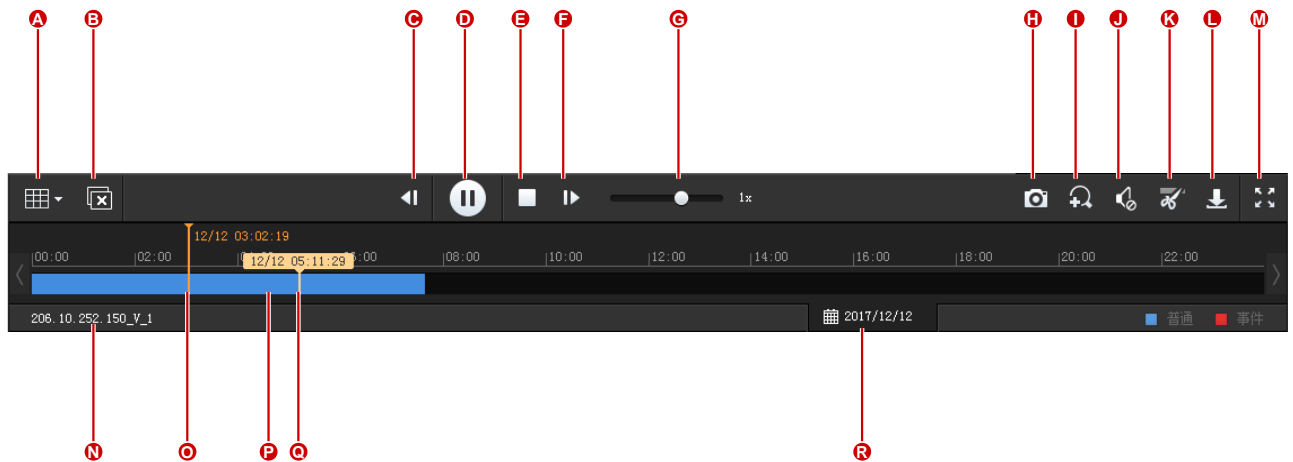
The timeline and the file list shows search results for the currently selected window. Click another window to view corresponding search results.

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.



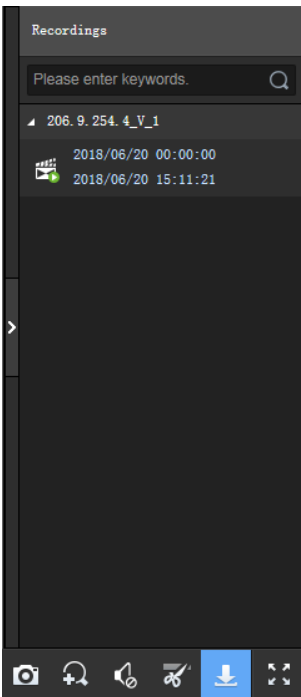
No.	Description
A	Set screen layout, up to 16 windows.
B	Close all windows.
C/F	Rewind by frame, forward by frame.
D	Pause/resume,
E	Stop
G	Adjust playback speed. Multiple options. + means playing forward, - means playing backward.
H	Take a snapshot and save it to the PC. The storage path is configurable (see Local Settings).
I	Digital zoom. When enabled, drag the mouse to draw an area on the image to zoom in on,

No.	Description
	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.

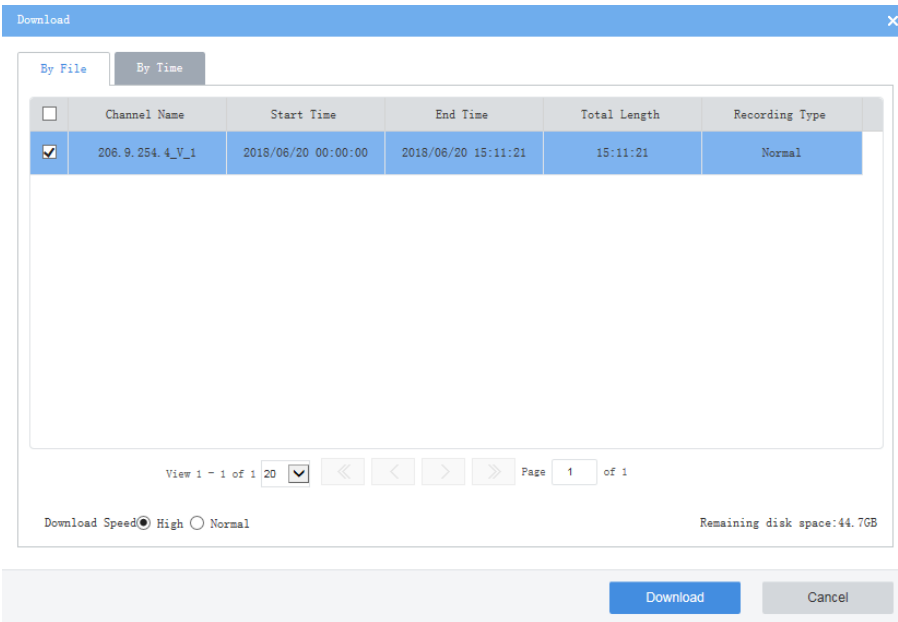
Recording Download

Download recordings from the VMS to your computer.

1. Click  on the toolbar.



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

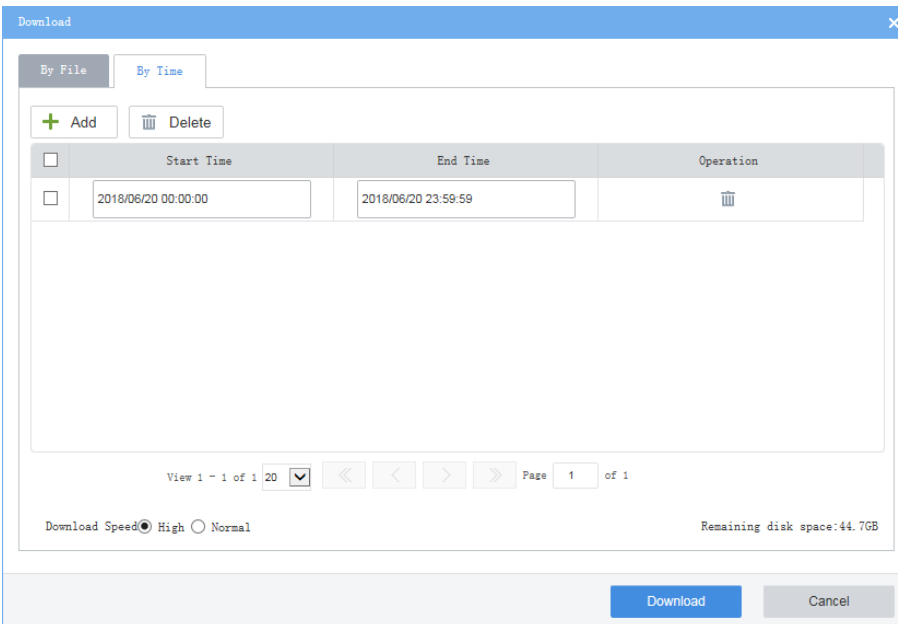



3. To download recordings of specified period, click the **By Time** tab, and then set the start and end times. Click **Add** to add download tasks. Select the tasks and then click **Download**.





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.

Channel Name	Start and End Time	Progress	Status	Operation
206.9.254.4_V_1	2018/06/20 00:00:00 2018/06/20 15:11:21	1%	Downloading	 

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 an LAN where the VMS collaborates with Uniview IPCs or NVRs.


If the policy is set to **Direct Connection First**, the VMS will determine whether conditions are satisfied (e.g., remaining output bandwidth of IPC/NVR) for direct transmission when starting streams. If conditions are satisfied, streams will be directly transmitted from IPC/NVR to the client, saving 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.

Video

Processing Mode	Fluent
Display Mode	Normal Quality
Stream Transmission Protocol	TCP
Stream Transmission Policy	Forwarding First

Image and Recording

Snapshot Format	<input type="radio"/> BMP <input checked="" type="radio"/> JPEG <input type="radio"/> JPEG & BMP
Recording Format	<input checked="" type="radio"/> MP4 <input type="radio"/> TS
Save File To	<input type="text" value="C:\Users\"/>  <input type="button" value="Open"/>

Note: Local recordings, snapshots and downloaded recordings are saved to Record, Snap and Download folders in the set directory.

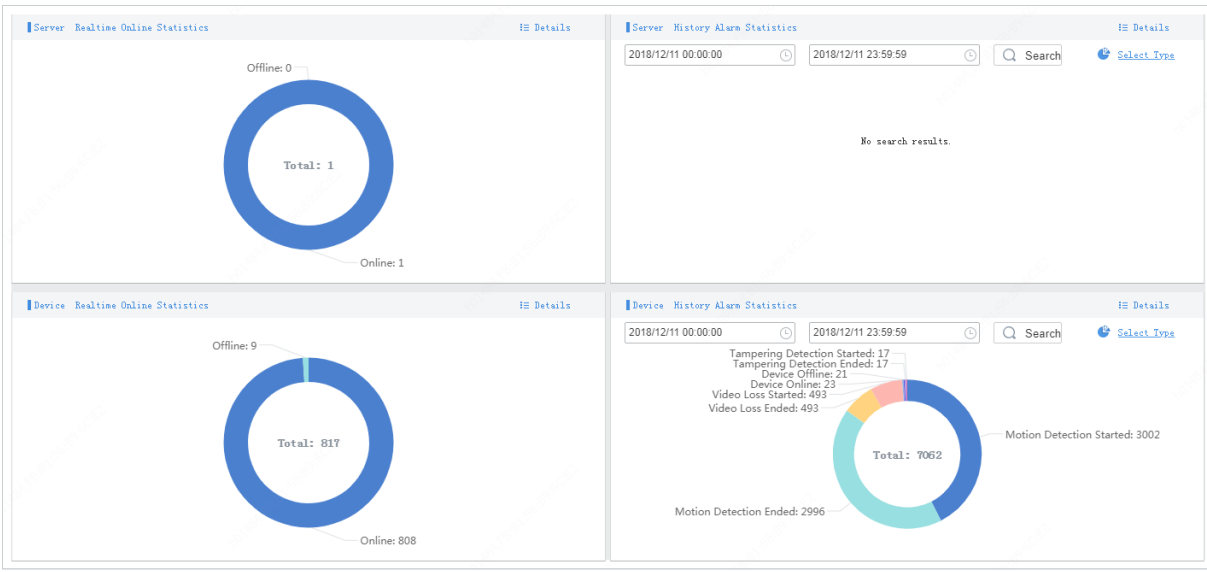
7 Statistics

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.

General View

Statistics > General View

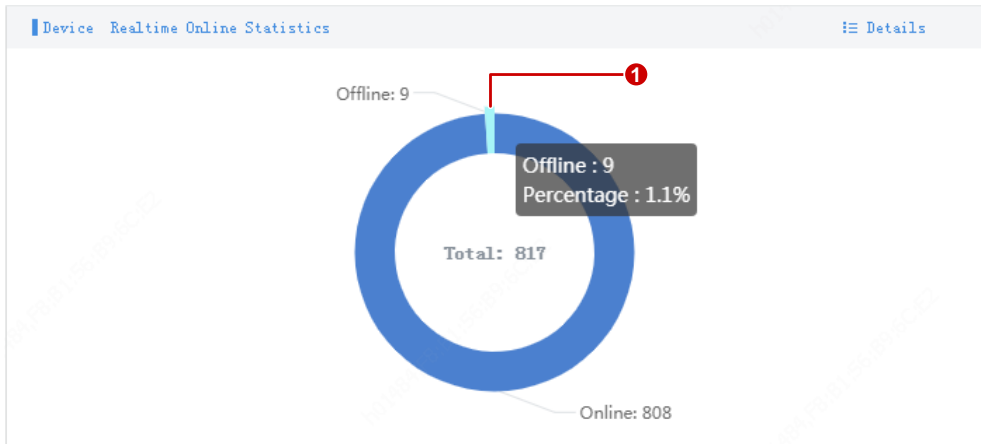
Have a general view of current online/offline status and history alarm statistics of the VMS server(s) and the connected devices.



View the Numbers of Online/Offline Servers or Devices

Place the mouse pointer on the chart in the **Server Realtime Online Statistics** or **Device Realtime Online Statistics** area to view the numbers and percentages of online and offline servers or devices.

For example, place the mouse pointer on the position (1) as illustrated in the figure below to view the number of offline devices and the percentage.



View Info about Online/Offline Servers or Devices

Click on the pie chart in the **Server Realtime Online Statistics** or **Device Realtime Online Statistics** area to view details on the corresponding page.

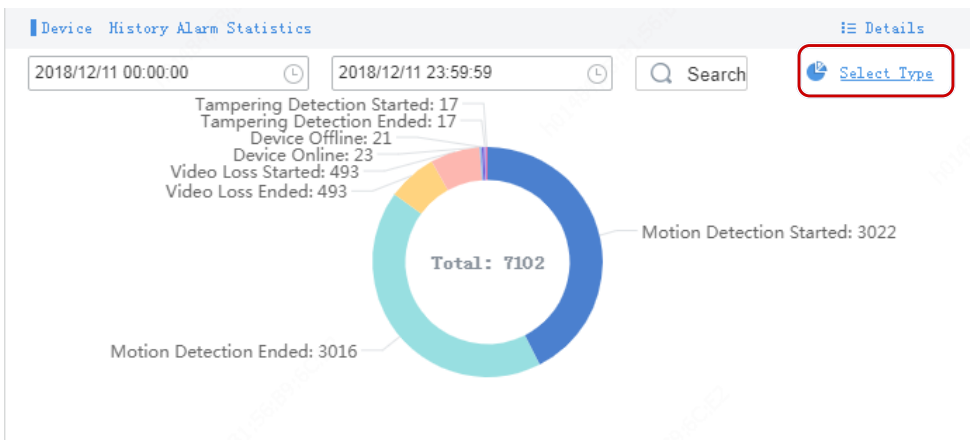
For example, click on the position (1) as illustrated in the above figure to view details about offline devices on the **Device** page. Clicking **Details** in the top right corner also opens the **Device** page, as shown below.

Device Name	Type	Organization No.	IP Address	Server	Serial No.	Version	MAC Address	Disk Status	Status	Operation
DC_2	Decoder	root	127.0.0.1	VMS				No Disk	Offline	
DC_3	Decoder	root	127.0.0.1	VMS				No Disk	Offline	
206.9.12.65	NVR	root	206.9.12.65	VMS				No Disk	Offline	
206.9.10.52	NVR	root	206.9.10.52	VMS				No Disk	Offline - I	
206.9.252.36	Decoder	root	206.9.252.36	VMS				No Disk	Offline - I	
206.9.252.56	Decoder	root	206.9.252.56	VMS				No Disk	Offline - I	
206.9.252.47	Decoder	root	206.9.252.47	VMS				No Disk	Offline - I	
206.9.10.44	Decoder	root	206.9.10.44	VMS				No Disk	Offline - C	
206.9.9.23	Decoder	root	206.9.9.23	VMS				No Disk	Offline - C	

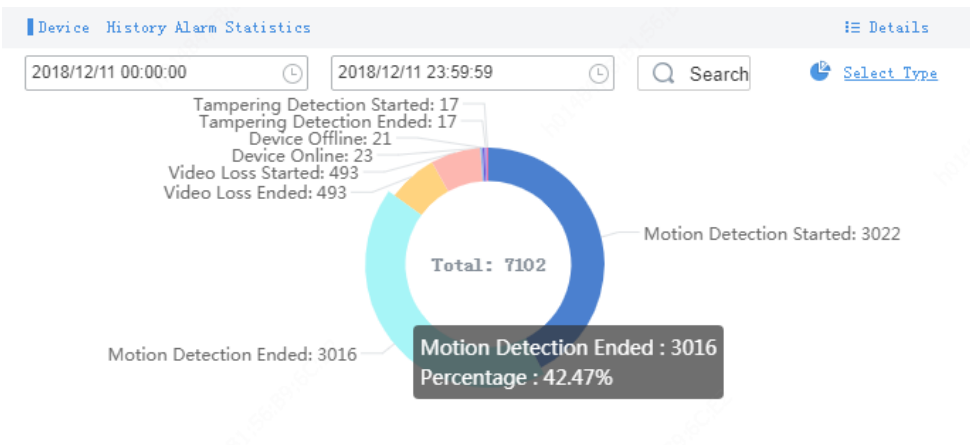
View History Alarm Statistics of Servers or Devices

View history alarms in the **Server History Alarm Statistics** or **Device History Alarm Statistics** area. Set a period as needed. Click **Select Type** to select alarm types (up to 8) you want to view.

For example. The pie chart below shows the total number of device alarms and the numbers of specified alarms reported during the set period.



Place the mouse pointer on the pie chart to view the number of alarms (e.g., Motion Detection Ended) and its percentage.



Click on the pie chart to view details. For example, click on the Motion Detection Ended part on the pie chart to view detailed information about Motion Detection Ended alarms on the **Device Alarm Logs** page.

<input type="checkbox"/>	Alarm Time	Alarm Source	Alarm Type	Alarm Sub Type	Alarm Level	Server	Operation	Acknowledged By	Acknowledged At	Remarks
<input type="checkbox"/>	2018/12/11 15:41:37	206.10.252.151_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:40:26	206.10.252.169_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:40:16	206.10.252.151_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:40:05	206.10.252.151_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:39:35	206.10.252.169_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:39:33	206.10.252.151_V_1	Motion Detection Ended		level 5	VMS	✓			
<input type="checkbox"/>	2018/12/11 15:38:46	206.10.252.151_V_1	Motion Detection Ended		level 5	VMS	✓			

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.

Name	IP	Serial No.	Type	Status
VMS	127.0.0.1	XXXXXXXXXXXXXXXXXXXX	Master	Online

S.M.A.R.T. Test

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

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

The system provides three test types:

- **Short:** A short test checks less items than an extended test and it takes less time.
- **Extended:** An extended test checks more thoroughly than a short test and it takes longer time.
- **Conveyance:** A conveyance test mainly checks for data transmission problems.

Select Disk	2
Test Type	Short <input type="button" value="Test"/> Not tested
Manufacturer	WDC
Model	WDC WD7502ABTS-01A6B0
Temperature (°C)	40
Operation Time (day)	1242
Health Status	Failure
Test Result	Not pass <input type="checkbox"/> 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 offline by selecting the target user(s) and clicking **Offline**. The target user(s) are logged out.

<input type="checkbox"/>	Username	Login IP Address	Login Time	Client
<input type="checkbox"/>	loadmin	206.10.9.57	2018/12/10 18:09:08	CS
<input type="checkbox"/>	loadmin	206.10.9.55	2018/12/10 18:04:55	WEB
<input type="checkbox"/>	admin	206.10.9.57	2018/12/10 17:31:58	WEB

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.

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

Server Performance

Statistics > Server > Server Performance

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

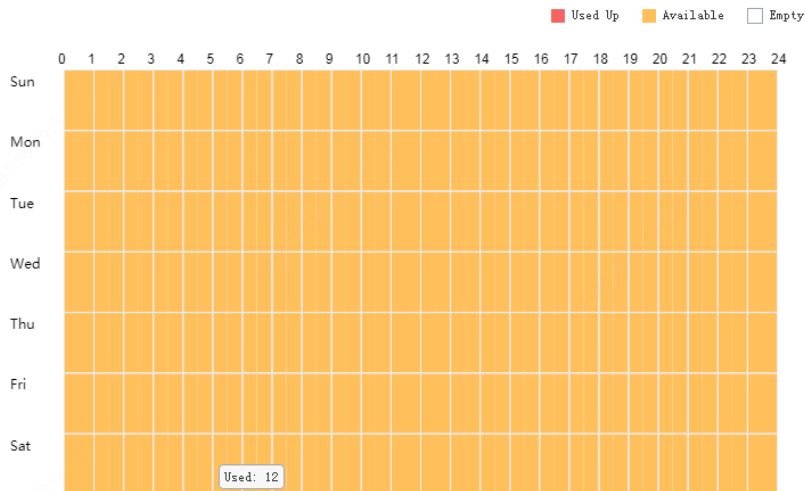
The Web client starts calculation when you open the page and displays statistics of the recent 240 seconds. Place the mouse pointer anywhere on the chart (see 1 in the figure below) to view details at the specific point. If more than one NIC is in use, statistics of the NICs are shown in different colors.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



Storage Capacity

Statistics > Server > Storage Capacity

If the system indicates full storage capacity when you are configuring a recording schedule (**Service > Recording Schedule**) or recording backup (**Service > 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 (Service > Recording Schedule)	Delete unnecessary recording schedules.
Recording Backup (Service > Recording Backup > Auto Backup)	<ul style="list-style-type: none"> ● 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.



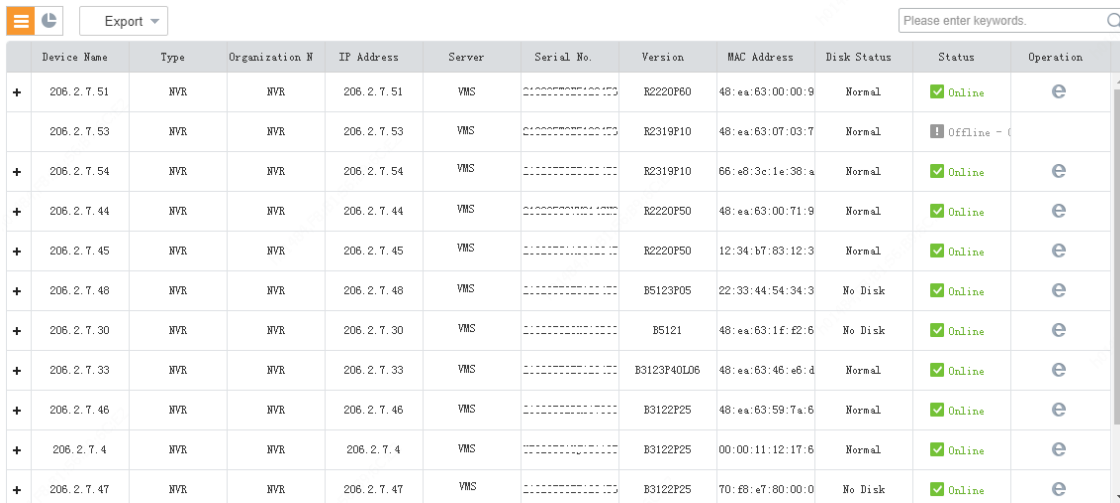
The table displays recording statistics for various channels. It includes columns for Channel Name, Device Name, Organization, Recording Type, Status, Diagnosis, Recording Spac, Stream Type, Frame Rate (fps), Bit Rate (Kbps), and Resolution. The Status column shows 'Recording...' for all entries.

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

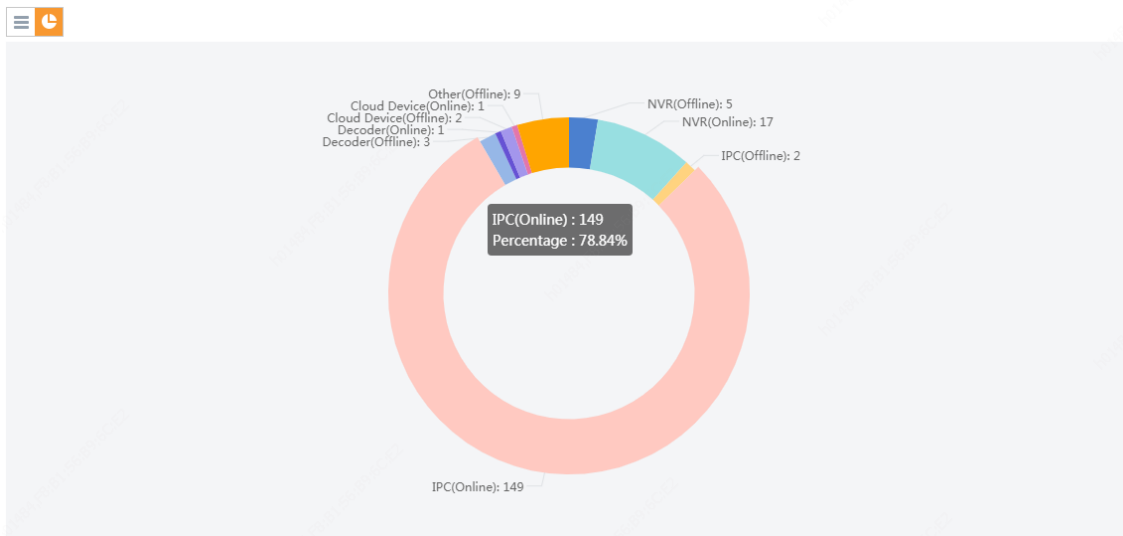
Search device statistics by device type and device status. Export search results to a CSV file.



The table displays device statistics for various devices. It includes columns for Device Name, Type, Organization, IP Address, Server, Serial No., Version, MAC Address, Disk Status, Status, and Operation. The Status column shows 'Online' for most devices, with one 'Offline' and one 'No Disk'.

Device Name	Type	Organization	IP Address	Server	Serial No.	Version	MAC Address	Disk Status	Status	Operation
206.2.7.51	NVR	NVR	206.2.7.51	VMS	...	R2220P60	48:ea:63:00:00:9	Normal	Online	e
206.2.7.53	NVR	NVR	206.2.7.53	VMS	...	R2319P10	48:ea:63:07:03:7	Normal	Offline	e
206.2.7.54	NVR	NVR	206.2.7.54	VMS	...	R2319P10	66:e8:3c:1e:38:a	Normal	Online	e
206.2.7.44	NVR	NVR	206.2.7.44	VMS	...	R2220P50	48:ea:63:00:71:9	Normal	Online	e
206.2.7.45	NVR	NVR	206.2.7.45	VMS	...	R2220P50	12:34:b7:83:12:3	Normal	Online	e
206.2.7.48	NVR	NVR	206.2.7.48	VMS	...	B5123P05	22:33:44:54:34:3	No Disk	Online	e
206.2.7.30	NVR	NVR	206.2.7.30	VMS	...	B5121	48:ea:63:1f:e2:6	No Disk	Online	e
206.2.7.33	NVR	NVR	206.2.7.33	VMS	...	B3123P40L06	48:ea:63:46:e6:d	Normal	Online	e
206.2.7.46	NVR	NVR	206.2.7.46	VMS	...	B3122P25	48:ea:63:59:7a:6	Normal	Online	e
206.2.7.4	NVR	NVR	206.2.7.4	VMS	...	B3122P25	00:00:11:12:17:6	Normal	Online	e
206.2.7.47	NVR	NVR	206.2.7.47	VMS	...	B3122P25	70:f8:e7:80:00:0	No Disk	Online	e

You can switch the list to a pie chart and place the mouse pointer on the chart to view the number and percentage.



Log

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

Server Alarm Logs

Statistics > Log > Server Alarm Logs

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

Server: Time Period: - **Today** Last 3 days Last 7 days Custom

Alarm Main Type: Select All Illegal Access Network Disconnection Network Disconnection C... IP Address Conflict Disk Offline Disk Online Disk Abnormal Storage Error Running Out of Recordin...

Recording Space Used Up Array Damaged Array Degraded Array Recovered

Status: Alarm Level: Select All level 1 level 2 level 3 level 4 level 5

Acknowledge

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



NOTE!

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

Device Alarm Logs

Statistics > Log > Device Alarm Logs

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

Server: All Time Period: 2019/01/09 00:00:00 - 2019/01/09 23:59:59 Today Last 3 days Last 7 days Custom

Alarm Source: Alarm #Main Type: All Status: All Alarm Level: Select All level 1 level 2 level 3 level 4 level 5 Search Reset

Acknowledge Export

Alarm Time	Alarm Source	Alarm Type	Alarm Sub Type	Alarm Level	Server	Operation	Acknowledged By	Acknowledged At	Remarks
2019/01/09 23:59:56	206.2.T.50_V_05	Motion Detection Start		level 1	VMS	✓			
2019/01/09 23:59:55	206.2.T.212_V_1	Motion Detection Start		level 1	VMS	✓			
2019/01/09 23:59:32	206.2.T.50_V_06	Motion Detection Endec		level 5	VMS	✓			
2019/01/09 23:59:22	206.2.T.212_V_1	Motion Detection Endec		level 5	VMS	✓			
2019/01/09 23:58:37	206.2.T.212_V_1	Motion Detection Start		level 1	VMS	✓			
2019/01/09 23:57:53	206.2.T.50_V_05	Motion Detection Endec		level 5	VMS	✓			
2019/01/09 23:57:23	206.2.T.50_V_05	Motion Detection Start		level 1	VMS	✓			



NOTE!

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

Operation Logs

Statistics > Log > Operation Logs

Search and export user operation logs.

User: Service Type: All Operation Type: All Time Period: Today 2019/01/09 00:00:00 - 2019/01/09 23:59:59 Search Reset

Export

Time	User	IP Address	Main Type	Sub Type	Objective	Result
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmOutput_B3_1	Succeeded.
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmOutput_B4_1	Succeeded.
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmInput_B3_2	Succeeded.
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmInput_B3_1	Succeeded.
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmInput_B4_2	Succeeded.
2019/01/09 11:09:30	SYSTEM	127.0.0.1	Basic Setup	Delete Config	AlarmInput_B4_1	Succeeded.
2019/01/09 11:04:58	admin	206.10.20.222	Login	User Login	admin	Succeeded.
2019/01/09 11:00:22	admin	206.10.9.57	Basic Setup	Edit Config		Succeeded.
2019/01/09 10:59:46	admin	206.10.20.37	Login	User Login	admin	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).