

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 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. So please see the actual display on your device.
- 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
Device Management	7
Device	7
Channel	11
External Alarm	12
Link Resource	13
Server Management	13
Central Server	13
Distributed Server	14
Allocate Resource	14
4 Service Configuration	15
Recording Schedule	15
Time Template	15
Recording Schedule	16
Alarm Configuration	17
Alarm Configuration	17
Time Template	19
Contacts	19
Custom Alarm Level	19
Alarm Subscription	19
Recording Backup	20
5 System Configuration	22
Basic Configuration	22
Device	22
Date & Time	22
DST	23
Time Sync	23
Holiday	23
Network Configuration	24
TCP/IP	24
EZCloud	25
DDNS	26

Port	27
Port Mapping.....	27
Email	27
VSS.....	28
Security Configuration	29
802.1x	29
ARP Protection	30
HTTPS.....	30
Secure Password	31
Maintenance	31
Maintenance	31
Device Diagnosis Info	32
Delete Logs	32
Packet Capture	32
Network Detect	33
Bandwidth Usage.....	33
Stream Transmission Policy.....	34
Master/Slave Switch	34
Master to Slave.....	34
Slave to Master.....	35
Change Master Server.....	35
Configure Hot Standby	35
6 Video Service	36
Live Video	36
Start Live Video.....	36
Stop Live Video	36
Live Video Operations	37
Playback	38
Glossary	38
Search Recording.....	38
Playback Control.....	39
Recording Download	40
Local Settings	42
7 Statistics	42
Server Statistics.....	42
Server Status.....	42
Network	43
User	43
Bandwidth	43
Device Statistics	43
Device	43
Channel.....	44
Log.....	44
Alarm Logs	44

Operation Logs45

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 an 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), specify working and backup slave servers, and 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 IPC under the same NVR may only belong to the same organization.
- Custom organization: Provides a much 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

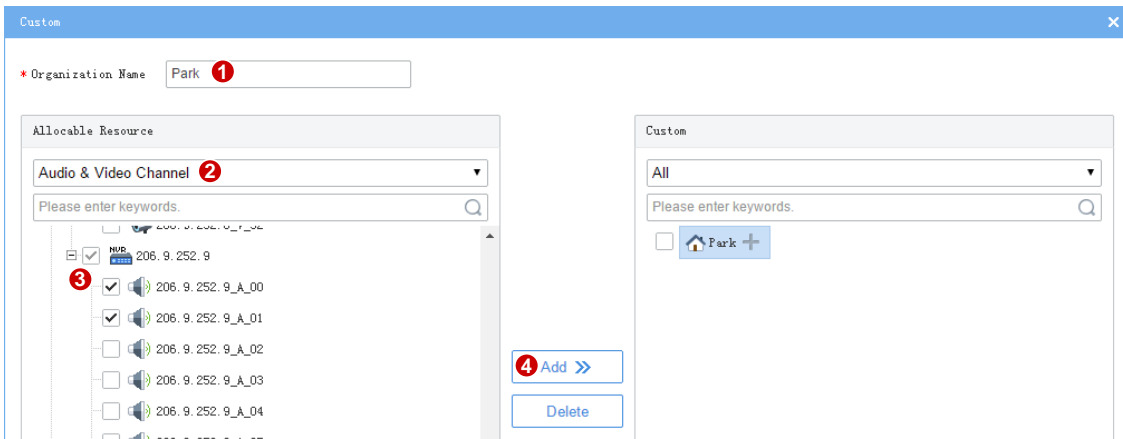
Basic > Organization > Custom

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

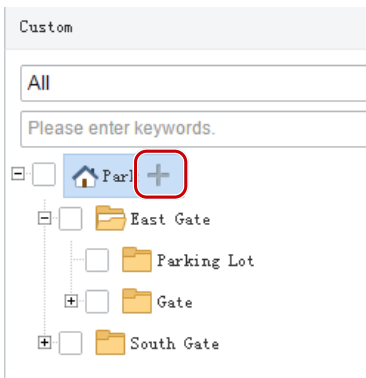
- Assign cameras under an NVR to different organizations.
- Assign cameras under different NVRs to one organization.
- Assign a camera to different organizations at the same time.
- Assign a custom organization to a role, so that users with this role can access certain resources on the software client.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

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

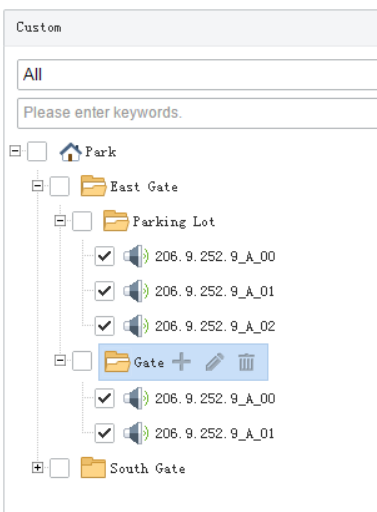
1. Enter a name. The organization name appears on the right.
2. (Optional) Select resource type (Audio & Video Channel). Enter keywords to filter if necessary.



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 right to the root organization 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).



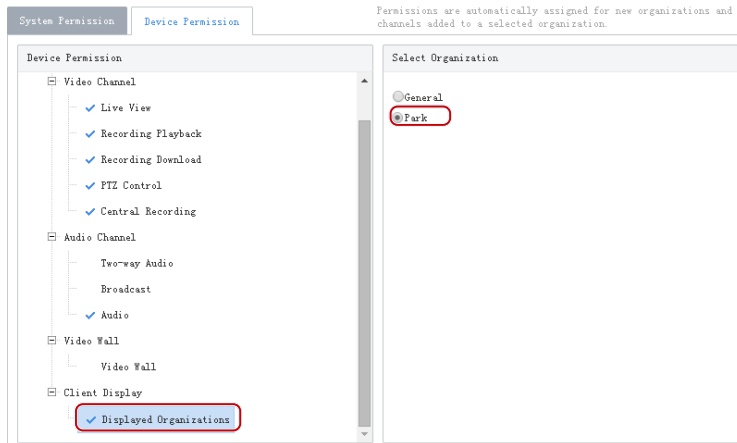
6. Click **OK**.



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

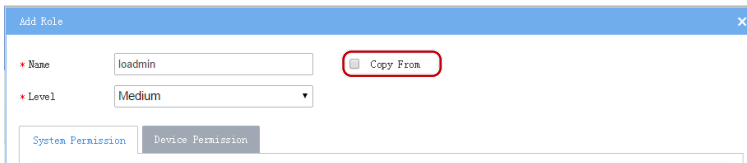
Roles are used to limit user's permissions, including:

- **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.

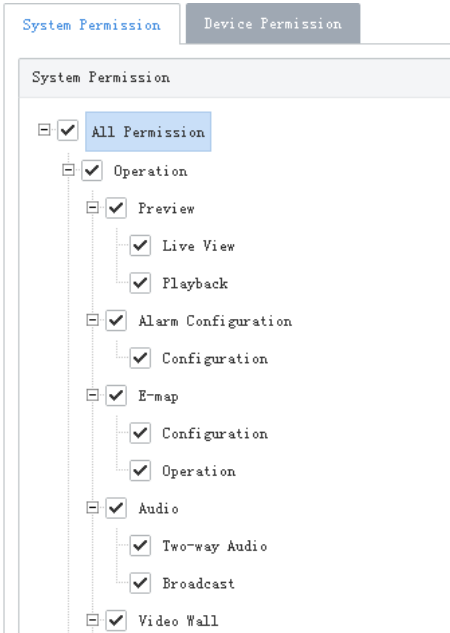
Click **Add** to add a new role:

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

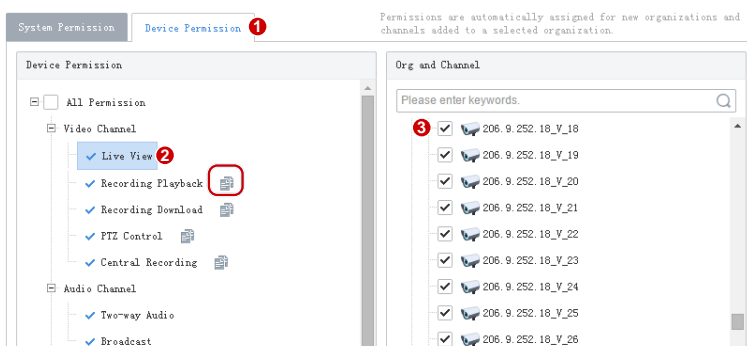
- (Optional) Select **Copy From**. The existing roles in the system are listed. Select a role and then edit permissions for the new role based on the selected role. Permissions of the selected role will not change.



- 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 permission on the left and then select channels 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 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


Control a user's permissions in the VMS by specifying roles. Lock a user's account so the user cannot log in.



NOTE!




The admin user cannot be edited or deleted.

Click **Add** to add a user.

1. Enter the username. A username must be unique in the system and cannot be changed once set.
2. Select role(s) to assign. The user will have all the permissions included in the role(s) assigned.
3. Enter the password, which the user will use to access the VMS.
4. (Optional) Click  to expand and enter more details.
5. Click **OK** to save the settings.

The user list lists all the users in the system, including username, role(s), and current status (online/offline). Click the buttons in the list to manage users:

- Click  to edit roles.

- Click  to change password. The new password is effective at the next login. Only admin can change other users' passwords.
- Click  to lock a user. A locked user cannot log in before being unlocked.
- Click  to delete a user. A user who is logged in will be forced out of the system.

Device Management

Manage devices, channels, external alarms; link resources.

The VMS supports the following device types:


- Encoding device: IPC (IP camera or camera for short), NVR (Network Video Recorder), and encoder.
- Decoding devices
- Network keyboard
- Cloud devices

Device

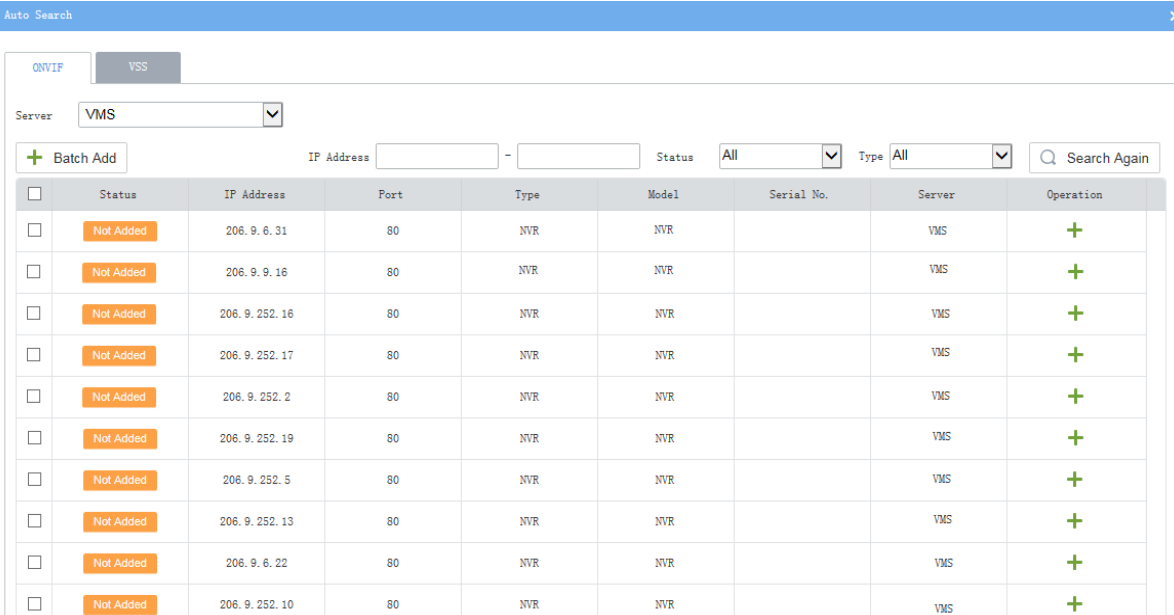
Basic > Device > Device

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**.








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

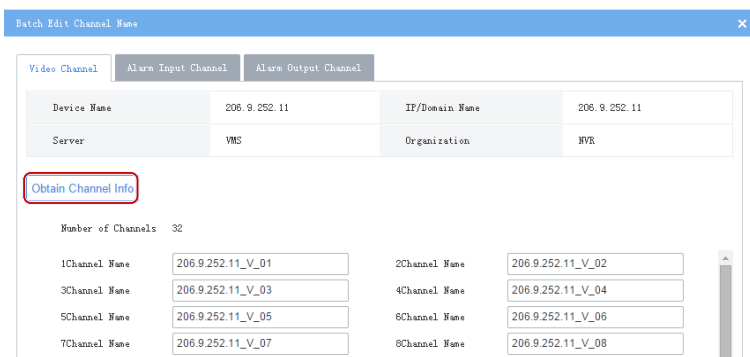
4. You may search again with set conditions:
 - **Server:** Search devices under the specified server. Selectable in master/slave configuration.
 - **IP:** Search devices within the specified IP range.
 - Filter devices by status (added or not) and type (IPC, NVR).
 - Click the **VSS** tab to search 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

1. Click the **Decoder** tab. Click an organization on the tree on the left to list decoding devices under the organization on the right.
2. Choose a way to add decoding devices:
 - Auto-Search: Search decoding devices on the same LAN with the VMS. Use an IP address range, device status and device type to narrow search results. Click  to add a device; or select multiple devices and click **Batch Add**.

Status	IP Address	Port	Type	Model	Serial No.	Operation
Not Added	206.9.14.55	82	Decoder			+
Not Added	206.9.252.32	82	Decoder			+

- Add: Select a protocol, enter device information, and then click **OK**. Information required may vary depending on the protocol you select. The following takes ONVIF as an example.

Protocol	ONVIF
Type	Decoder
* Device Name	Decoder
* Organization Name	root
* IP/Domain Name	206.9.252.37
* Port	82
* Username	admin
Password	
Remarks	

Network Keypad

Click the **Network Keypad** tab to add a network keyboard and use it to control PTZ camera, set screen/window, or play video on a video wall. You need to enter the VMS's IP address and port number on the keyboard first. See the keypad 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 Devices** 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.
- Add cloud device. 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**.

My Cloud Devices Devices Shared to Me

+ Add Delete Please enter keywords. 🔍

	Cloud Name	Device Name	IP Address	Server	Organization	Type	Model	Status	Operation
<input type="checkbox"/>	IPC	IPC	206.2.T.29	VMS	f00432	IPC		✔ Online	✎ 🗑️ ➦

- 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.

Edit ✕



* Device Name

Cloud Account

Server

Sync to Cloud

OK Cancel

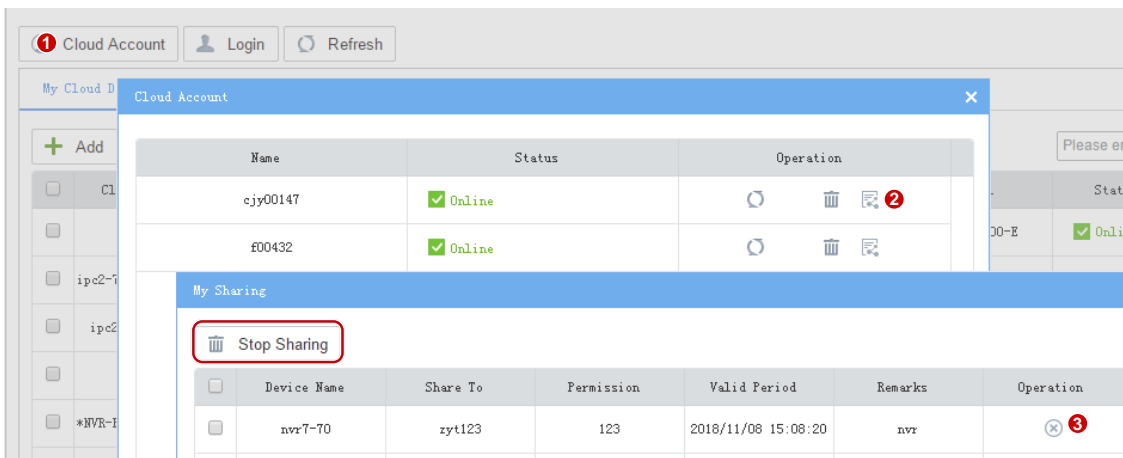
- Delete cloud device. Click  in the **Operation** column, or select multiple items and click the **Delete** button.
- Share online cloud device with other cloud accounts: Click  in the **Operation** column, set a sharing period and select a user to specify the permissions of the cloud account. The user and permissions are configured on the devices, not on the VMS.
- Click **Cloud Account** to view and manage cloud accounts on the VMS.

 Login Refresh

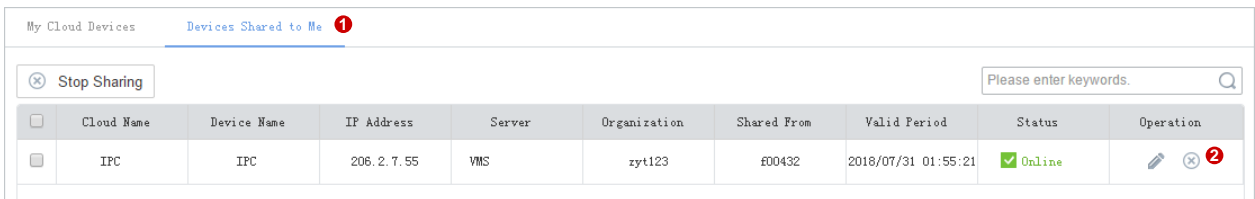
My Cloud D Cloud Account ✕

	Name	Status	Operation
<input type="checkbox"/>	cjy00147	✔ Online	🔄 🗑️ 📄
<input type="checkbox"/>	f00432	✔ Online	🔄 🗑️ 📄

- 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 account, click **Devices Shared to Me** and then click **Stop Sharing**.
















Channel

Basic > Device > Channel

Channels include encoding channel, decoding channel, alarm channel.

- Click the **Encoding Channel** tab. 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. 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.
- Click the **Alarm Channel** tab. Click an organization on the tree on the left to list alarm channels under the organization on the right. Use the check boxes to filter the display. Click  to edit channel name, alarm type or default status, or select multiple channels and click **Batch Edit**.

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	Online		N.O.
206.9.15.15_I_0	206.9.15.15	1	root	Alarm Input Channel	Online		N.O.
206.9.15.15_I_1	206.9.15.15	2	root	Alarm Input Channel	Online		N.O.
206.9.251.112_0_relay_	206.9.251.112	1	IPC2	Alarm Output Channel	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.

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, 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
✕

Name

External Alarm On Off

Region Code

District Code

Area Code

OK

Cancel

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

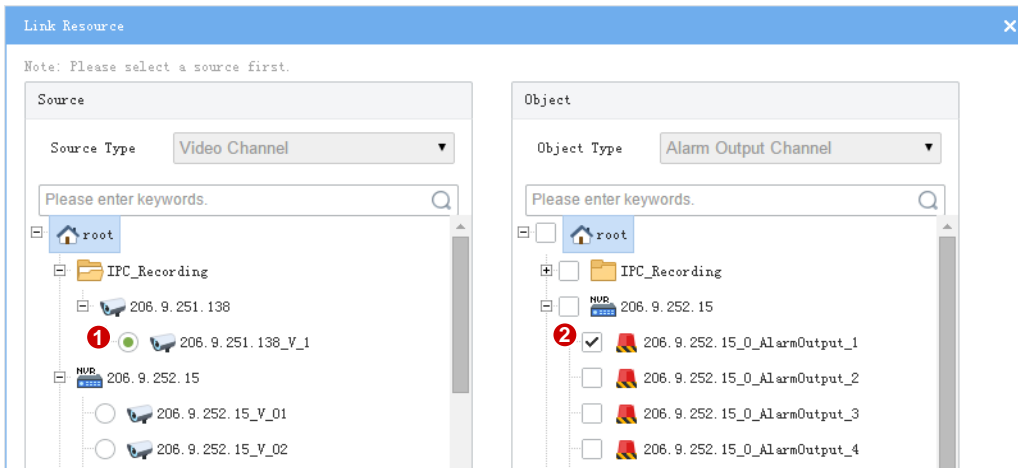
- Configure alarm-triggered actions including live view, preset (for PTZ cameras), alarm output, and alarm to video wall on the software client. See Alarm Configuration of the *Software Client User Manual*.


Link Resource

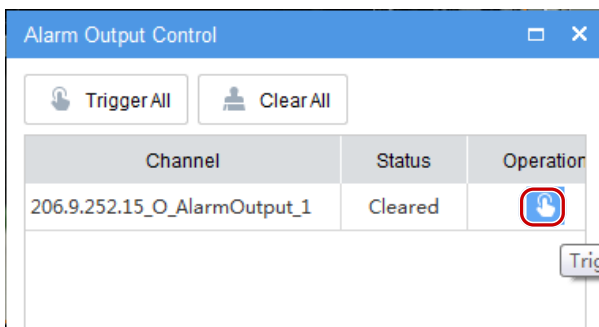
Basic > Device > Link Resource

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 central server (primary and secondary server) and distributed server (slave server), specify working and backup slave servers; allocate device resources to master and slave servers.

Central Server





















Basic > Server > Central Server




View info and status of central server. Click  to view connection and bandwidth info.

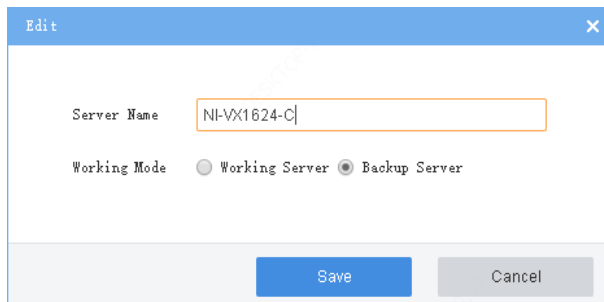
Distributed Server

Basic > Server > Distributed Server

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

Name	IP	Serial No.	Type	Working Mode	Working Status	Status	Operation
NI-VX1624-C	192.168.206.3	210235C1L1J18B000005	Slave	Backup Server	Idle	 Online	  
206.5	192.168.206.5	210235C1SUJ18B000049	Slave	Working Server	Normal	 Online	  
10.253	192.168.10.253	210235C1DWJ181000003	Slave	Working Server	Normal	 Online	  
206.4	192.168.206.4	210235C1SUJ18B000045	Slave	Working Server	Failure	 Offline - The slave ser	  
206.2	192.168.206.2	210235C1L1J18B000020	Slave	Working Server	Normal	 Online	  

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



Backup slave server(s) are standby in case any working slave server fails or becomes offline. If a working slave server fails or is offline (Working Status changes from "Normal" to "Failure"), an idle backup slave server takes over (Working Status changes from "Idle" to "Taking over"). When the working server recovers to "Normal" status, it takes back over, and the backup server syncs data to the working server.



NOTE!

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

Allocate Resource

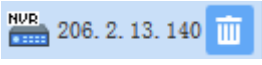
Basic > Server > Allocate Resource

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

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



Tip!

- In 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.
- Backup slave servers are displayed only when they are in "Taking over" status.

4 Service Configuration

Service configuration includes:

- [Recording Schedule](#): Configure recording schedules so video will be recorded 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 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	Constant recording according to the schedule.
Motion	Trigger recording by motion.

Type	Description
Event	Trigger recording by an event (such as video loss).
Alarm	Trigger recording by an alarm.
M and A	Trigger recording by motion AND an alarm.
M or A	Trigger recording by motion OR an alarm.

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	00:00:00				08:30:00			
End Time					19:30:00			
Plan Type	Motion				Schedule			
Start Time	19:30:00				23:59:59			
Plan Type	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](#).

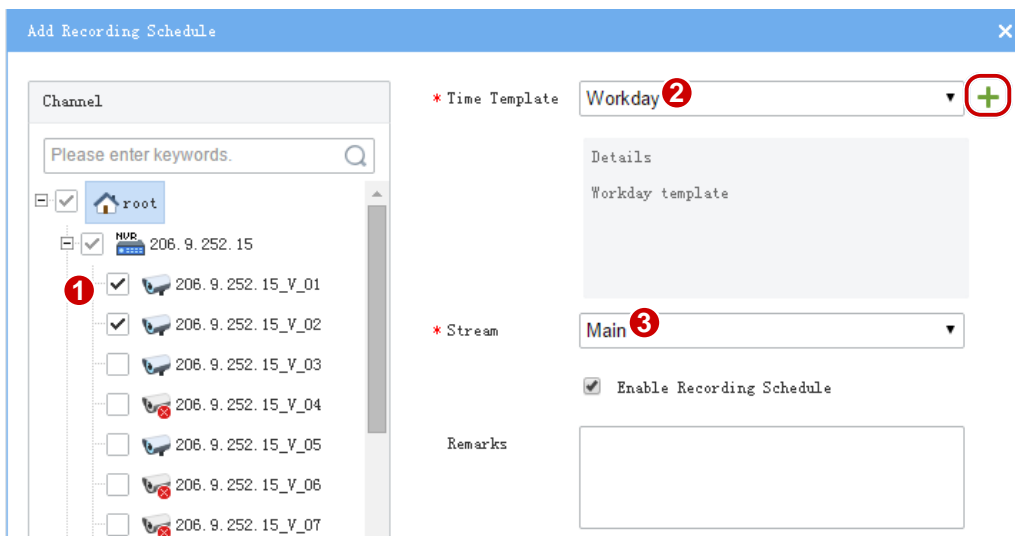
Recording Schedule

Service > Recording Schedule > Recording Schedule

Assign a time template to cameras so that video will be recorded for the cameras according to the time template.

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

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



5. 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, if network connection is interrupted during its recording schedule, video will be saved to the camera's onboard SD card before network connection is recovered; and the video saved on the SD card will be transferred automatically to the slave VMS when network connection is recovered.


Alarm Configuration

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

Please enter keywords.

Alarm Type

- Video Loss
- Motion Detection
- Tampering Detection
- IPC Offline

- 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
- 206.2.7.80_V_1

- 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

Please enter keywords.

Pre-Record Time

s

Note: Use a non-schedule time template for this setting to take effect.

Post-record Time

s

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

- 206.2.7.102_V_1
- 206.2.7.103_V_1
- 206.2.7.104_V_1
- 206.2.7.105_V_1
- 206.2.7.106_V_1
- 206.2.7.107_V_1
- 206.2.7.108_V_1
- 206.2.7.109_V_1
- 206.2.7.110_V_1
- 206.2.7.111_V_1
- 206.2.7.112_V_1



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](#)).

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

Time Template

Service > Alarm Configuration > Time Template

Configure time templates for alarm configuration. For details, 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.

Alarm Type	Alarm Level
Running Out of Recording Space	level 1 ■
Recording Space Used Up	level 1 ■
Device Online	level 5 ■
Device Offline	level 1 ■
Array Damaged	level 1 ■
Disk Online	level 5 ■
Array Degraded	level 1 ■
Disk Offline	level 1 ■
Disk Abnormal	level 1 ■

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

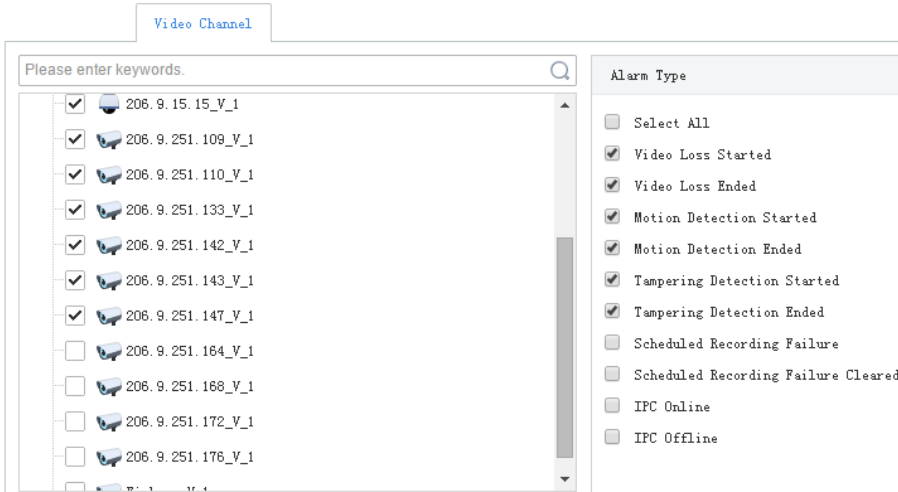
Service > Alarm Subscription > Alarm Subscription

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.



The screenshot shows a configuration window titled "Video Channel". On the left, there is a search bar "Please enter keywords." and a list of video channels. Each channel entry consists of a checkbox, a camera icon, and an IP address followed by a channel ID (e.g., "206.9.15.15_V_1"). The first seven channels have their checkboxes checked. On the right, there is a section titled "Alarm Type" with a list of alarm types, each with a checkbox. The checked items are: "Video Loss Started", "Video Loss Ended", "Motion Detection Started", "Motion Detection Ended", "Tampering Detection Started", and "Tampering Detection Ended". Other unchecked items include "Select All", "Scheduled Recording Failure", "Scheduled Recording Failure Cleared", "IPC Online", and "IPC Offline".

4. Click **Save**.



NOTE!

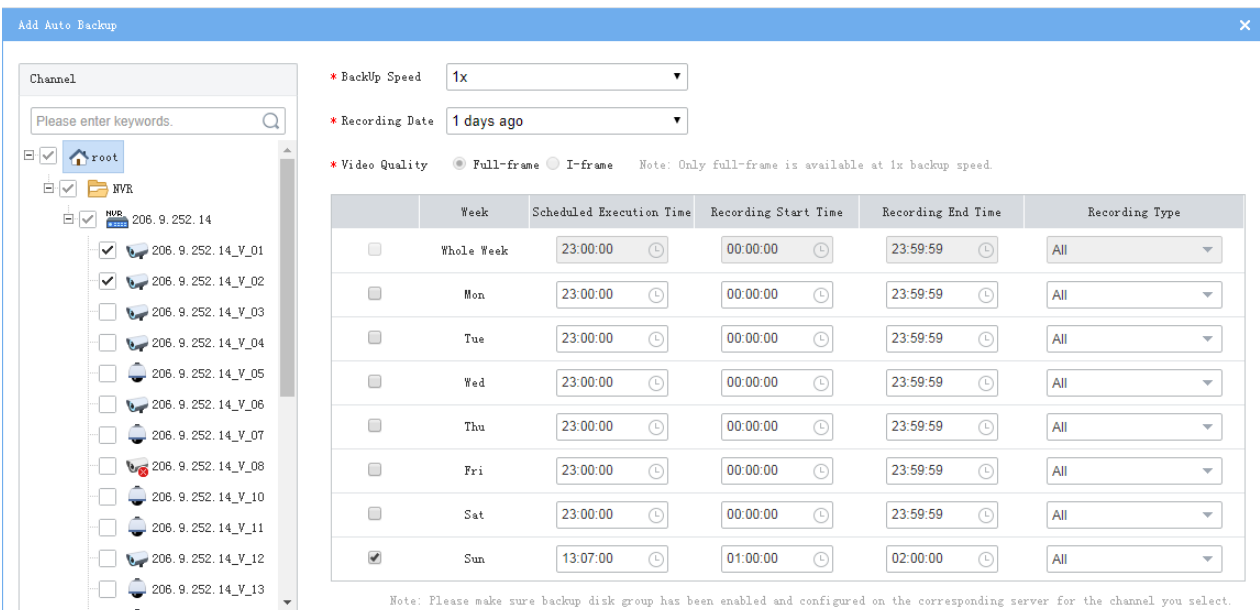
- Alarm subscription is enabled by default. If disabled, the client cannot receive any alarm messages, even if alarm subscription is configured.
- By default, a non-subscriber receives all alarm messages. To block all alarm messages for the user, add the user as an alarm subscriber without configuring 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

Service > Recording Backup > Auto Backup

Create a task to automatically replicate recordings stored on an NVR to a slave VMS according to schedule.

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



Add Auto Backup

Channel

Please enter keywords.

- * Backup Speed: 1x
- * Recording Date: 1 days ago
- * Video Quality: Full-frame I-frame Note: Only full-frame is available at 1x backup speed.

	Week	Scheduled Execution Time	Recording Start Time	Recording End Time	Recording Type
<input type="checkbox"/>	Whole Week	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Mon	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Tue	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Wed	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Thu	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Fri	23:00:00	00:00:00	23:59:59	All
<input type="checkbox"/>	Sat	23:00:00	00:00:00	23:59:59	All
<input checked="" type="checkbox"/>	Sun	13:07:00	01:00:00	02:00:00	All

Note: Please make sure backup disk group has been enabled and configured on the corresponding server for the channel you select.

- **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.
- **Video Quality:** Choose Full-frame to make a full backup; or choose I-frame to only back up I-frames. Full-frame backup requires more storage.
- **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. The backup task papers 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	

5 System Configuration

System configuration includes:

- [Basic Configuration](#): Basic device info, time and time synchronization, DST, and holiday configuration.
- [Network Configuration](#): Basic network settings, cloud, DDNS, port, port mapping, VSS and email.
- [Security Configuration](#): Includes 802.1x, ARP protection, and HTTPS.
- [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.

Basic Configuration

Device

System > Basic > Basic Setup

Configure basic information of the VMS, including device name, ID and language; view device model, serial number and firmware version.


Device Name	<input type="text" value="VMS"/>
Device ID	<input type="text" value="1"/>
Device Language	<input type="text" value="English"/>
Model	VMS
Serial No.	-----
Firmware Version	B1115

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	1 <input type="text"/> hour (s)

Save

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.

Network Configuration

TCP/IP

System > Network > TCP/IP

The IP address can be static or obtained through DHCP. Three working modes are available:

- **Multi-address:** (Default mode) The static IP address information of each NIC card of the device can be set respectively.
- **Load Balance:** Available for two or more NIC cards. Network traffic will be diverged to the logical card with lighter load.
- **Net Fault-tolerance:** Available for two or more NIC cards. One logical card works at a time. The other stands by for redundancy and comes into operation when the working one fails.



NOTE!

- Network configuration is independent among different working modes.
- Under **Load Balance** and **Net Fault Tolerance** modes, NIC cards will be bound into logical cards whose IP address can be customized.
- The IPv4 addresses of the NICs must belong to different network segments.

Working Mode	Multi-address ▼
Select NIC	NIC1 ▼
DHCP	<input type="radio"/> On <input checked="" type="radio"/> Off
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 ▼


[Save](#)

- DHCP: With a DHCP server configured, enabling DHCP will automatically obtain an IP address for the VMS.
- IPv4 Address: VMS' IP address. Use this address to access the VMS from a Web or software client.
- DNS Server: Domain Name Server, which resolves a domain name into an IP address.
- Default Route: 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) can associate 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

VSS configuration includes VSS server configuration and VSS local configuration. When configuration is complete, the VMS can connect IPC/NVR devices and connect to higher management platform (referred to as the platform for short in this section) via SIP.

In VSS server configuration, SIP server refers to the platform. In VSS local configuration, SIP server refers to the VMS.

VSS Server

System > Network > VSS Server

- 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).
- 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.

Click **Quick Config** to assign IDs to video channels, alarm input channels and cloud devices automatically.



CAUTION!

The Quick Config function assigns new channel IDs to ALL channels based on the basic code you set, which means, the existing channel IDs (if any) will be cleared and reassigned.

In the dialog box displayed, enter the basic code, and then click **OK**. Channel IDs generate automatically in ascending order based on the basic code you entered.

ID format: 8-character center code + 2-character industry code + 3-character type code + 7-digit Serial Number (SN).

In the dialog box, the basic ID consists of three parts, for example, 24020001+132+0000001. The first part (e.g., 24020001) is the default value which you may edit; the second (e.g., 132) is generated automatically based on the channel type and cannot be edited; the third (e.g., 0000001) is a serial number which you may set as needed.

The screenshot shows the VSS Server configuration interface. At the top, there are radio buttons for 'On' and 'Off'. Below is a form with various fields: 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 (3600), Administrative Division Code (3402), Heartbeat Cycle (30), Max Heartbeat Timeout Counts (3), Live View TCP Connection (Auto-Negotiation), and Stream Encapsulation Format (Auto-Negotiation). A 'Save' button is present. Below the form is a 'Quick Config' section with a table of channels.

Channel Name	Channel ID	Organization ID	Alarm Level	Longitude	Latitude	Operation
206.9.251.168_V_1	34020000011320000001	34020000002160000003	Level 4	0	0	
206.9.251.133_V_1	34020000011320000002	34020000002160000003	Level 4	0	0	
206.9.251.143_V_1	34020000011320000003	34020000002160000003	Level 4	0	0	
206.9.252.6_V_05	34020000011320000004	34020000002160000004	Level 4	0	0	

VSS Local

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.

The screenshot shows the VSS Local configuration form with the following fields:

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

A 'Save' button is located at the bottom of the form.

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 **Bind 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**.

Secure Password

System > Security > Secure Password

Friendly Password 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 Enhanced Password is enabled, using a weak password to access the software client 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 add a user with weak password or change the password to a weak one.

Password Mode	<input checked="" type="radio"/> Friendly Password	<input type="radio"/> Enhanced Password
<p>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).</p> <p>Enhanced Password: You must log in with a strong password.</p>		
<input type="button" value="Save"/>		

Maintenance

Maintenance

System > Maintenance > Maintenance

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

<input type="button" value="Restart"/>	Restart device.
<input type="button" value="Default"/>	Restore all factory default settings except network, user and event settings.
<input type="button" value="Factory Default"/>	Restore all factory default settings.
<input type="button" value="Export Configuration"/>	Export configuration file.
<input type="button" value="Export Diagnosis Info"/>	Export diagnosis information.
Import Configuration	<input type="text"/> <input type="button" value="Import"/>
Local Upgrade	<input type="text"/> <input type="button" value="Upgrade"/>

- **Default:** Restore all factory default settings except network, user and event 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.




NOTE!

The following operations require admin permissions: Export Configuration, Import Configuration, Export Diagnosis Info and Local Upgrade.

Device Diagnosis Info

System > Maintenance > Device Diagnosis Info

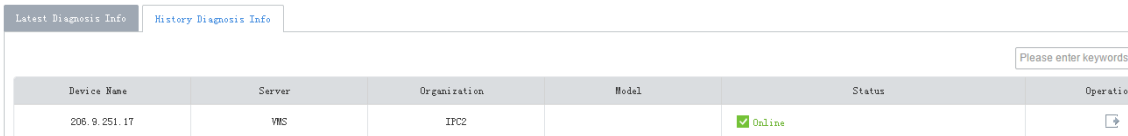
Click  to export diagnosis information of devices (NVR and camera) directly connected to the VMS, including latest and history diagnosis info.


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



Device Name	Server	Organization	Model	Status	Operation
206.9.251.17	VMS	IPC2		Online	

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

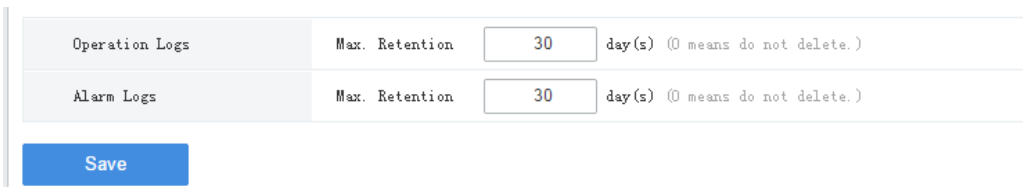


Device Name	Server	Organization	Model	Status	Operation
206.9.251.17	VMS	IPC2		Online	

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.

[Start](#)
[Stop](#)
[Delete](#)

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



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.

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"/>	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	61.5Mbps
Remote Playback	0Kbps
Remote Live View	106.625Mbps
Remote Playback & Download	0Kbps
Idle Receive Bandwidth	962.5Mbps
Idle Send Bandwidth	1941.375Mbps

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

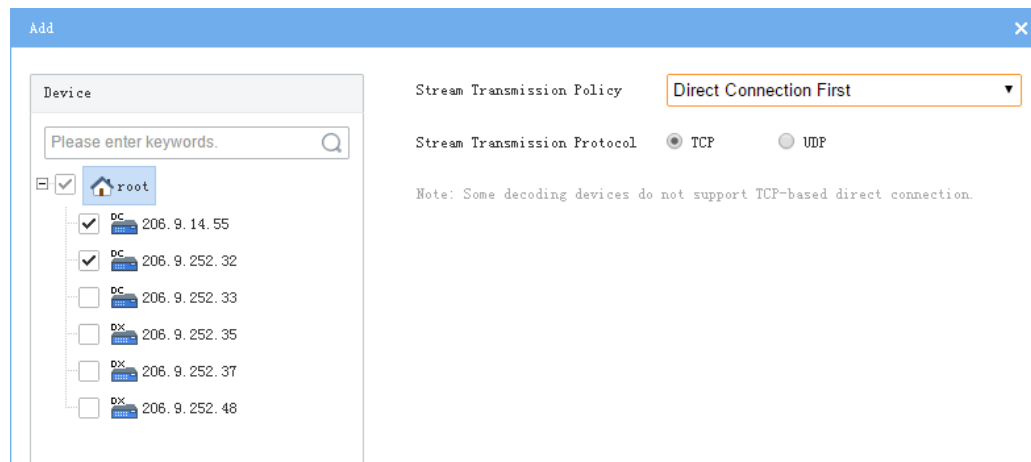
- IP Channel: Bandwidth usage when VMS receives live video streams from devices (e.g., camera or NVR).

- 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

Set the stream transmission policy and protocol, so that when conditions (including sufficient output bandwidth of the encoding device) are met, streams are directly transmitted with the chosen protocol to the decoding device without being forwarded via the VMS, which improves reliability and timeliness of data transmission.



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 ✔
Virtual IP	<input type="text" value="206.9.13.36"/> ✔ Note: IP that is not in use in the network.
Subnet Mask	<input type="text" value="255.255.255.0"/> ✔
Virtual Route ID	<input type="text" value="1"/> ✔ Note: Must be unique in multi-hot-standby configuration.
Secondary Server Service IP	<input type="text" value="206.9.12.65"/> ✔
Secondary Server Heartbeat IP	<input type="text" value="206.9.12.65"/> ✔ <input type="button" value="Check"/>
Alarm and Operation Log Data	<input checked="" type="checkbox"/> Clear

1. Click **Master**, select **Enable Hot Standby**. Take working mode as an example.
- Secondary Server: Enable/disable hot standby.
- Role: Specify a working mode for the server.

- Virtual IP: Must be an IP that is not in use on the network. When configured successfully, the virtual IP can be used to access the Web and software 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.
2. Click **Save**.

6 Video Service

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

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. If more cameras are selected than windows displayed, the layout will change automatically.



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 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.

Button	Description
	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

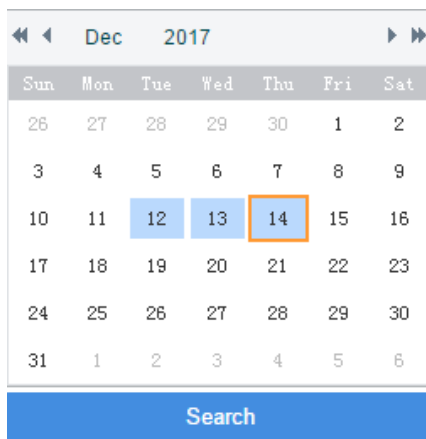
Glossary

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

Search Recording

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

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



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


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

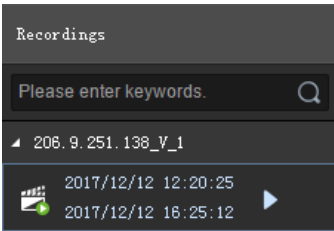


TIP!

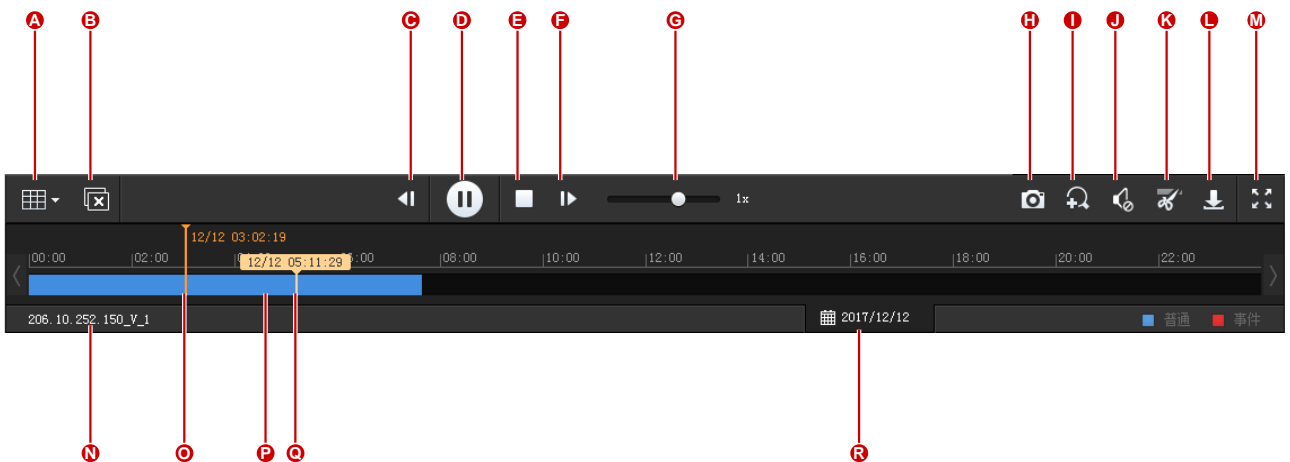
The timeline and the file list shows search results for the currently selected window. Click another window to view corresponding search results.


Playback Control




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



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



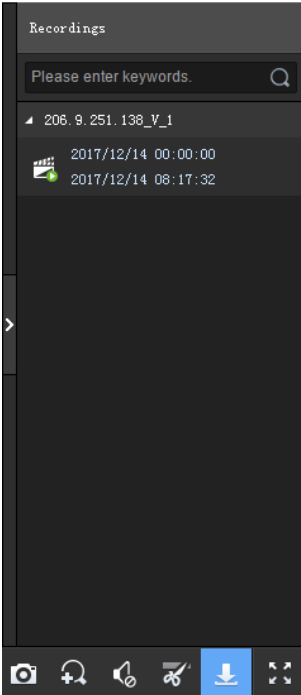
No.	Description
A	Set screen layout, up to 16 windows.
B	Close all windows.
C/F	Rewind by frame, forward by frame.
D	Pause/resume,
E	Stop
G	Adjust playback speed. Multiple options. + means play forward, - means play backward.
H	Take a snapshot and save it to the PC. The storage path is configurable (see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

No.	Description
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.

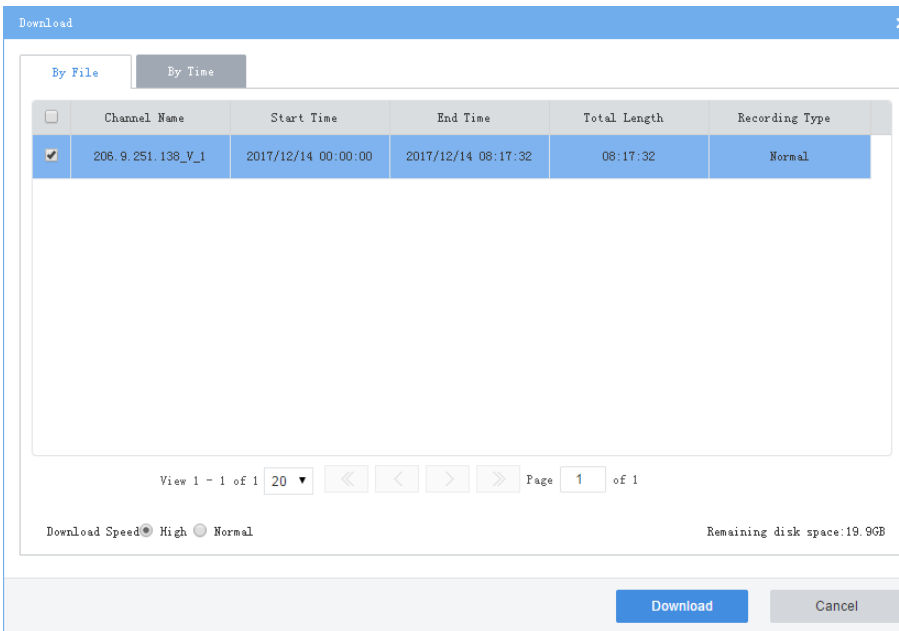
Recording Download

Download recordings from the VMS to your computer.

1. Click  on the toolbar.



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

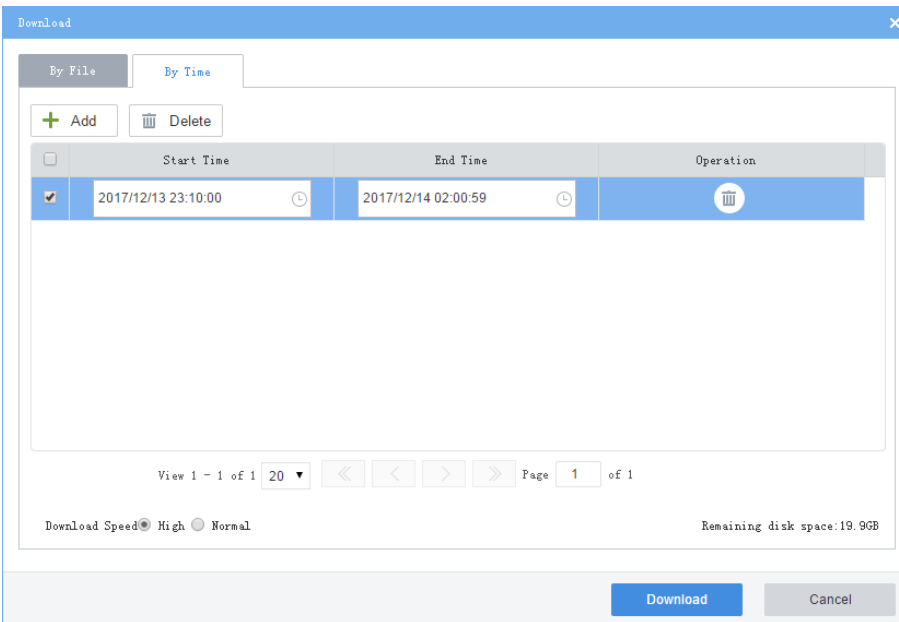



3. To download recordings of specified period, click the **By Time** tab, and then set the start and end times. Click **Add** to add download tasks. Select the tasks and then click **Download**.




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 or manage download tasks, click  in the page's upper right corner.

Channel Name	Start and End Time	Progress	Status	Operation
206.9.251.138_V_1	2017/12/13 23:10:00 2017/12/14 02:00:59	0%	Downloading	

Local Settings

Video Service > Local Settings


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

To improve reliability and timeliness of data transmission, set the media transmission policy and choose the preferred transmission protocol, so that if conditions (including sufficient output bandwidth of the encoding device) are met, streams are directly transmitted with the preferred protocol to the client computer without being forwarded via the VMS.

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 statistics of the VMS system, connected devices, and logs.

Server Statistics

Server Status

Statistics > Server > Server Status

View information about master and/or slave VMS, including device name, IP address, serial number, type (master or slave), and status (online or offline).

Name	IP	Serial No.	Type	Status
VMS	127.0.0.1	Master	<input checked="" type="checkbox"/> Online

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

User

Statistics > Server > User

View information about existing users, including username, login IP address, login time, and current status.

Username	Login IP Address	Login Time	Status
admin	206.10.9.57	2017/12/11 11:27:24	<input checked="" type="checkbox"/> Online
admin	206.10.9.57	2017/12/11 11:14:31	<input checked="" type="checkbox"/> Online
admin	206.9.5.20	2017/12/11 10:57:51	<input checked="" type="checkbox"/> Online

Bandwidth

Statistics > Server > Bandwidth

View real-time bandwidth usage of the master/slave VMS. See [Bandwidth Usage](#).

Device Name	IP	Type	IP Channel	Remote Playback	Remote Live View	Remote Playback & Download	Idle Receive Bandwidth	Idle Send Bandwidth
VMS	127.0.0.1	Master	52.625Mbps	0Kbps	92.125Mbps	0Kbps	971.375Mbps	1955.875Mbps

Device Statistics

Device

Statistics > Device > Device

Type: Status:

Device Name	Type	Organization Name	IP Address	Status	Operation
206.9.251.109	Encoding Device	root	206.9.251.109	Online	e
Fisheye	Encoding Device	root	206.2.5.103	Online	e
206.9.251.172	Encoding Device	root	206.9.251.172	Online	e
206.9.251.176	Encoding Device	root	206.9.251.176	Online	e
206.9.251.168	Encoding Device	root	206.9.251.168	Online	e
206.9.251.164	Encoding Device	root	206.9.251.164	Online	e
206.9.251.142	Encoding Device	root	206.9.251.142	Online	e

Channel

Statistics > Device > Channel

Channel Type: Status:

Channel Name	Device Name	Organization Name	Channel Type	Status
206.9.251.109_V_1	206.9.251.109	root	Encoding Channel	Online
Fisheye_V_1	Fisheye	root	Encoding Channel	Online
206.9.251.143_V_1	206.9.251.143	root	Encoding Channel	Online
206.9.251.110_V_1	206.9.251.110	root	Encoding Channel	Online
206.9.251.172_V_1	206.9.251.172	root	Encoding Channel	Online
206.9.251.142_V_1	206.9.251.142	root	Encoding Channel	Online

Log

Search and export alarm and operation logs of the VMS.

Alarm Logs

Statistics > Log > Alarm Logs

Search alarm logs by a combination of conditions including server, alarm type, alarm source, alarm status and time period. Click **Acknowledge** to confirm selected alarm(s) and add remarks as needed.

Alarm Logs | Operation Logs

Server:

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

Alarm Main Type:

Alarm Source: Status:

Time Period: -

<input type="checkbox"/>	Alarm Time	Alarm Source	Alarm Type	Alarm Sub Type	Alarm Level	Server	Operation	Acknowledged By	Acknowledged At
<input type="checkbox"/>	2017/12/11 15:50:24	206.9.254.100_V_6	Video Loss Ended		level 2	VMS	✓		
<input type="checkbox"/>	2017/12/11 15:50:20	206.9.254.100_V_2	Video Loss Ended		level 2	VMS	✓		



NOTE!

Acknowledged alarms cannot be revoked.

Operation Logs

Statistics > Log > Operation Logs

Search operation logs by a combination of conditions including user, service type, operation type, and time period.

Time	User	IP Address	Main Type	Sub Type	Objective	Result
2017/12/11 15:28:08	admin	206.10.9.57	Live View	User Stop Operation	206.9.251.138_V_1	Succeeded.
2017/12/11 15:24:48	SYSTEM	127.0.0.1	Login	User Logout	admin	Succeeded.
2017/12/11 15:07:48	SYSTEM	127.0.0.1	Login	User Logout	admin	Succeeded.
2017/12/11 15:06:42	admin	206.10.9.57	Live View	User Start Operation	206.9.251.138_V_1	Succeeded.
2017/12/11 15:02:03	admin	206.9.12.60	Login	User Login	admin	Succeeded.
2017/12/11 14:53:48	SYSTEM	127.0.0.1	Login	User Logout	admin	Succeeded.
2017/12/11 14:29:51	admin	206.9.12.60	Login	User Logout	admin	Succeeded.
2017/12/11 14:26:43	admin	206.9.12.60	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).