Video Management Server Web Manager

User Manual

V2.07

Contents

1 Overview

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

Note:
We recommend that you open no more than two tabs on the browser when using the local Web client. Too many tabs open will consume extra memory and cause the browser to exit.

2 Login

Use a Web browser to log in to the VMS:

- Enter the username and password to log in. The default username/password: admin/123456.

  Note:
  If the VMS has configured with AD Domain and Domain Users are imported, the domain users can log in with the imported domain username/password.

- It is recommended to change the password after login.

Important:

- Set a strong password at first login. A strong password consists of 9-32 characters and includes at least three of the following types: upper case letters, lower case letters, special characters, and digits.
- Admin can set contact information at first login. Contact information is used to retrieve the login password and is not compulsory. Contact information can also be set and modified any time later by clicking in User.
- If you forgot your password, click **Forgot Password** above the **Login** button and follow the on-screen instructions to obtain a temporary password. The temporary password is applicable to admin and valid on a Local Area Network (LAN) on the current day. Please reset the password when logged in.

3 Basic Configuration

Add and manage persons, users, organizations, devices, servers, and recording schedules on the VMS. It supports batch configuration.

3.1 Organization Management

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

Organization management includes:

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

General Organization

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

1. Click **Add** to create a general organization.
2. Enter a name and select a parent organization (by default is **root**).
3. Click **OK**.
4. The new organization appears on the organization tree on the left and the list on the right. It also appears in the organization name drop-down list from which you can select when adding or editing a device.

5. In the organization list, click or to edit or delete an organization.

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

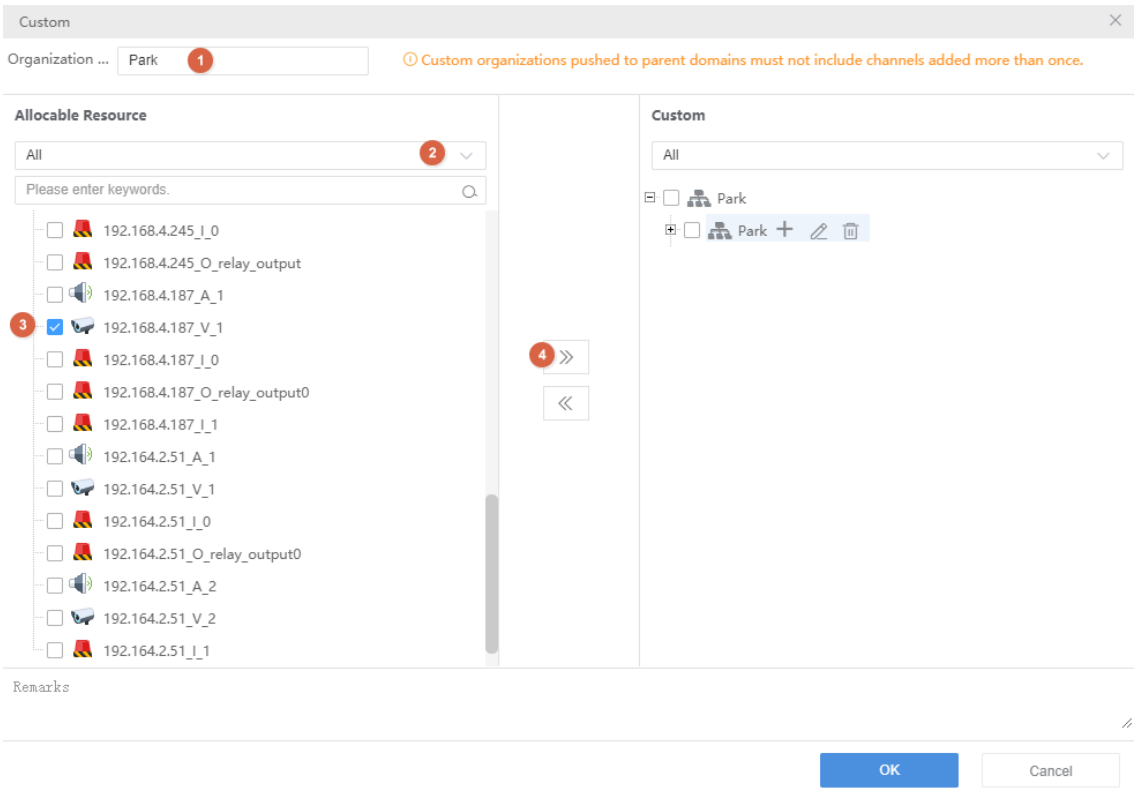
Custom Organization

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

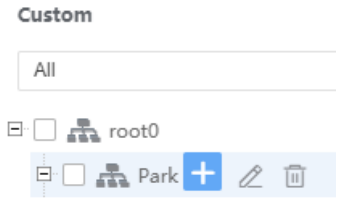
Custom organization provides a flexible way to manage devices and allows you to:

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

1. Click **Add** to create a custom organization:
2. Enter a name. The organization name appears on the right.
3. (Optional) Select resource type (Audio & Video Channel). Enter keywords to filter if necessary.



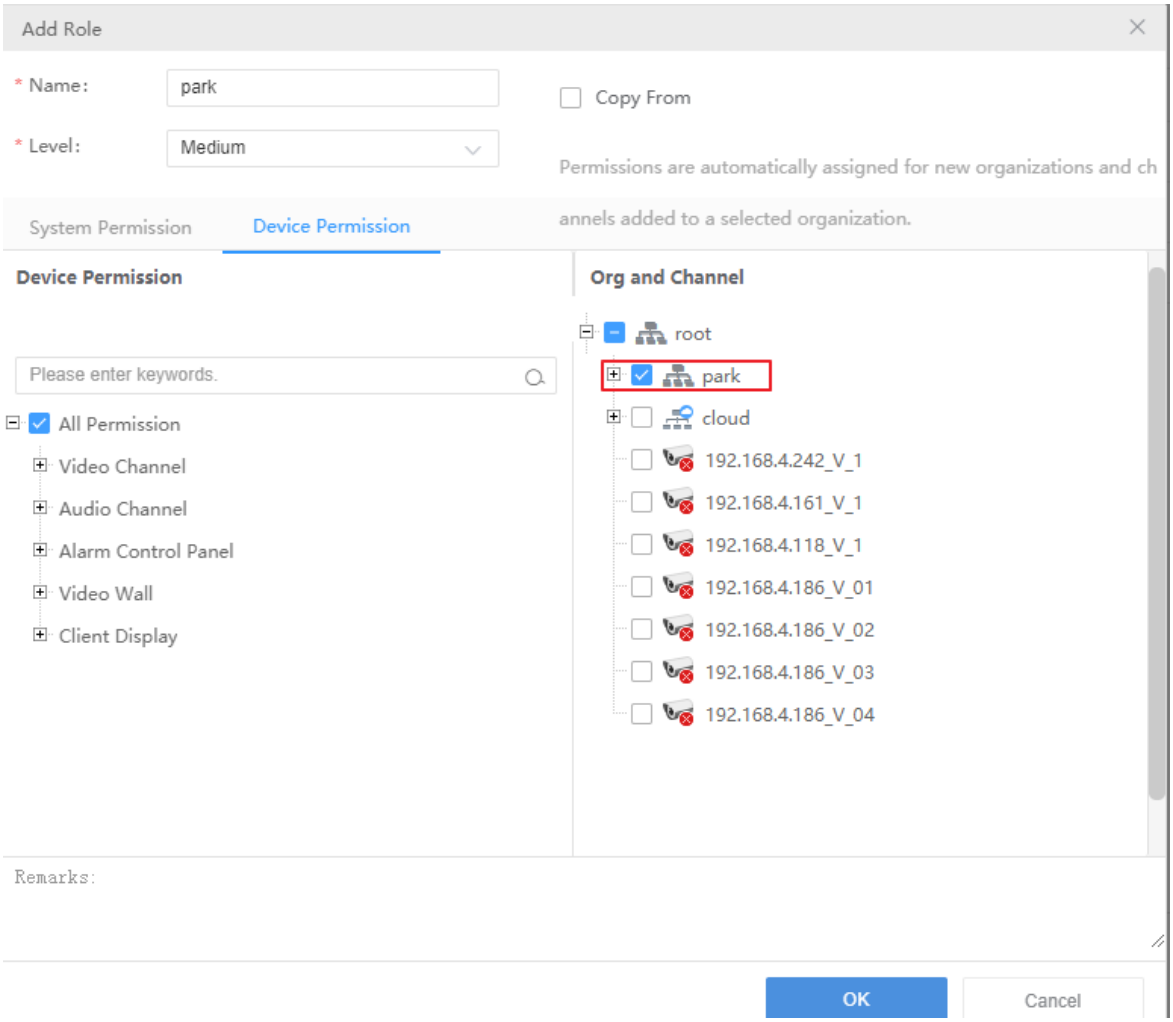
4. To allocate resources to the root organization (e.g., park), select resources on the left, click the organization name on the right, and then click **Add**.
5. To add a new organization, click the add sign (+) and then enter a name in the field. The tree updates automatically. Add all the needed organizations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



6. 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.

7. Click **OK**.

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



Note:

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

3.2 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.

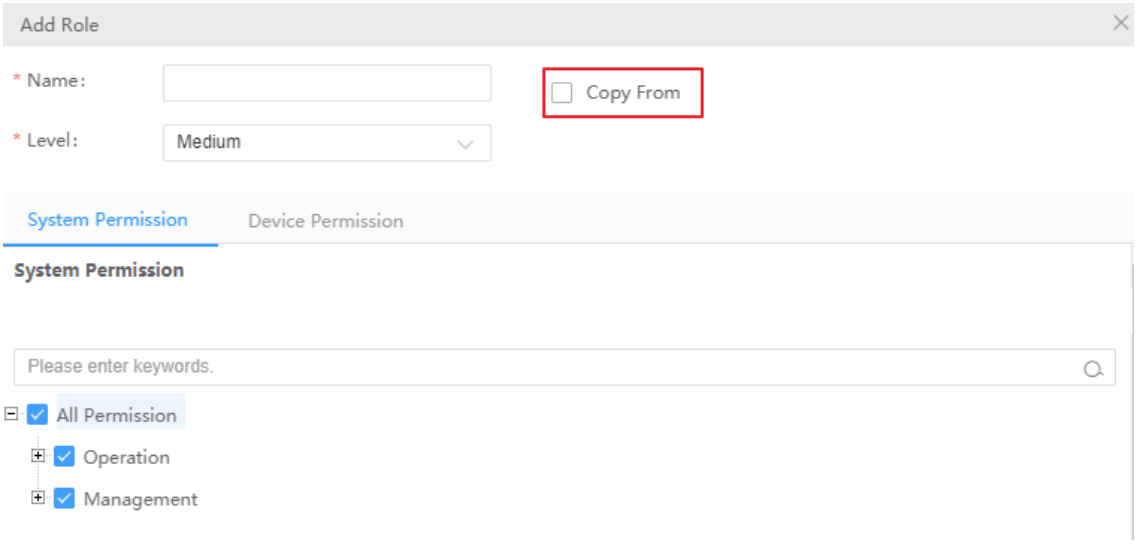
Role

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

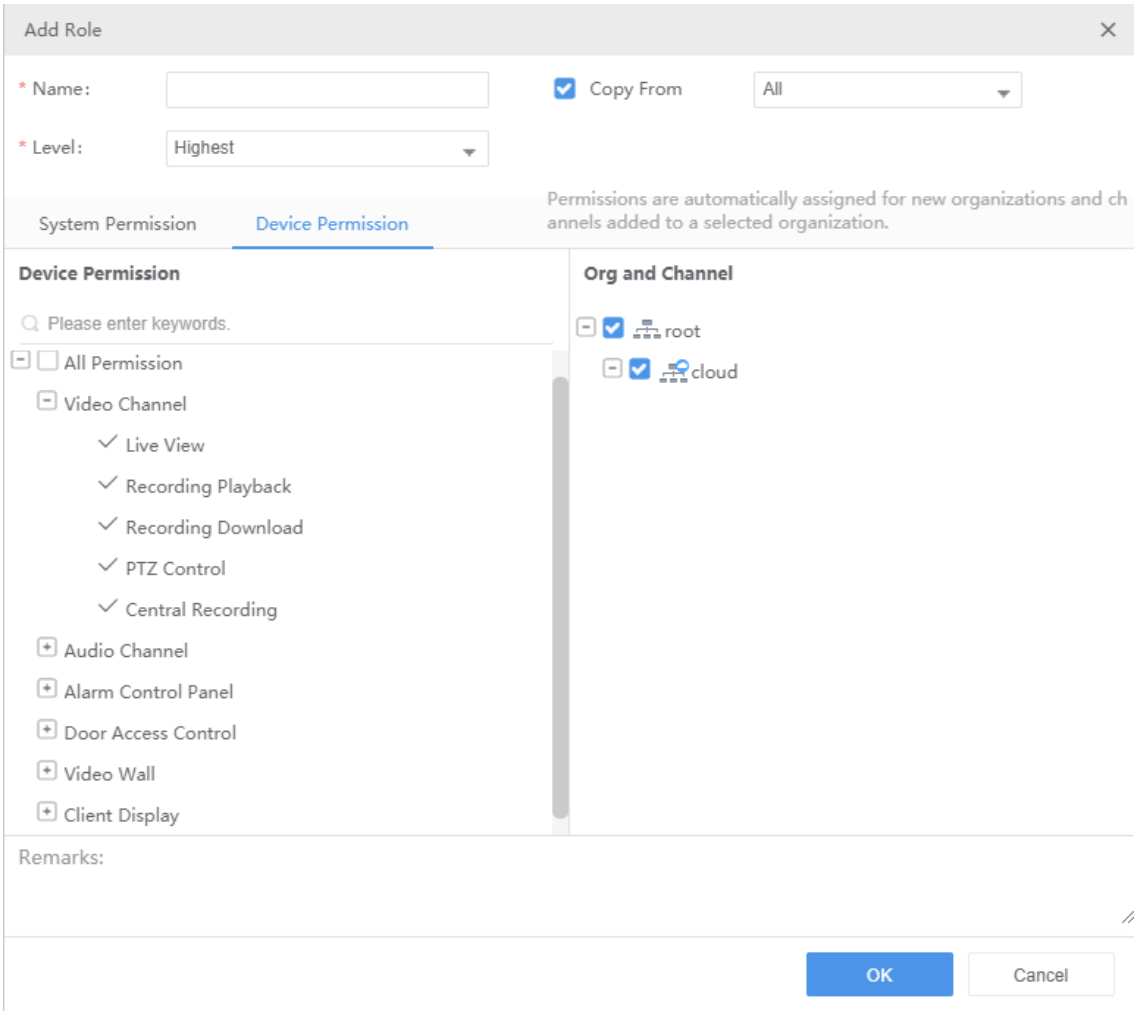
Roles are used to limit user's permissions, including:

- **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.

1. Click **Add** to add a new role.
2. Enter the role name.
3. Select a level.
4. (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.



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



Note:

- 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.
- 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.

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

User

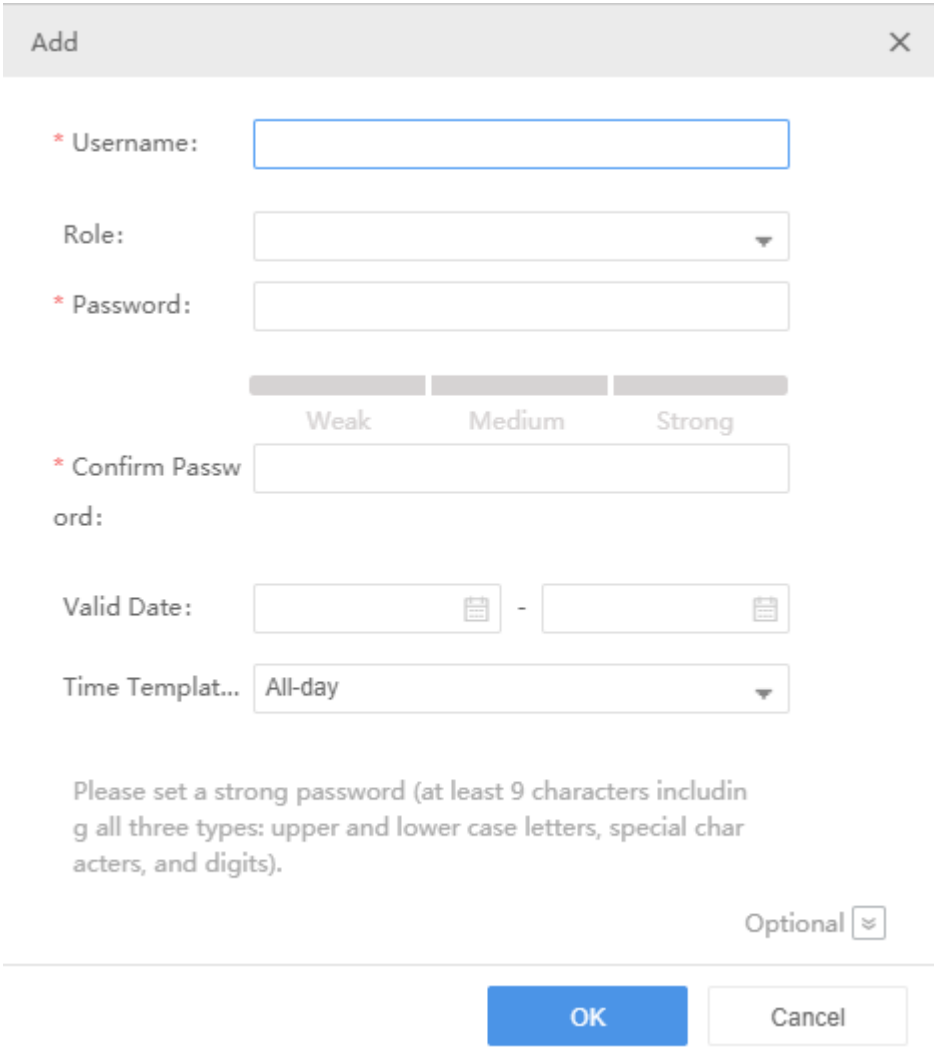
Basic > **User** > **User**

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

Note:
The admin user cannot be edited, deleted or locked.

Add users or import domain users.

- Add User:
  1. Click **Add** to add a user.



2. Set the following parameters.
   - 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 VMS.
   - Valid Date: Specify the period during which the user have access to the VMS.
   - Time Template: See User Time Template.
   - Click to expand and enter more details.
3. Click **OK**.

- Import Domain User: After the VMS is connected to the AD domain, you can import domain users so that the domain users can access the VMS by domain username/password. To configure AD domain, click **Links** > **AD Domain Configuration**.
  1. Click **Import Domain User**.
  2. Select the target domain users from the lelft organization of the domain server, and click .
  3. Set user status and permissions.
     - User status: Users only in normal state can access the VMS.
     - Role: Up to 16 roles are allowed for a user. The user will have all the permissions included in the roles assigned.
     - Valid Date: Specify the period during which the user have access to the VMS.
     - Time Template: See User Time Template.

4. Click **OK**.

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

- Click to change roles, valid date and time template. Admin can only modify contact information.
- 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.
- Click **Sync Domain User Info** to update the domain user information to the latest on the domain server. This feature is only available to the server with AD domain configuration.

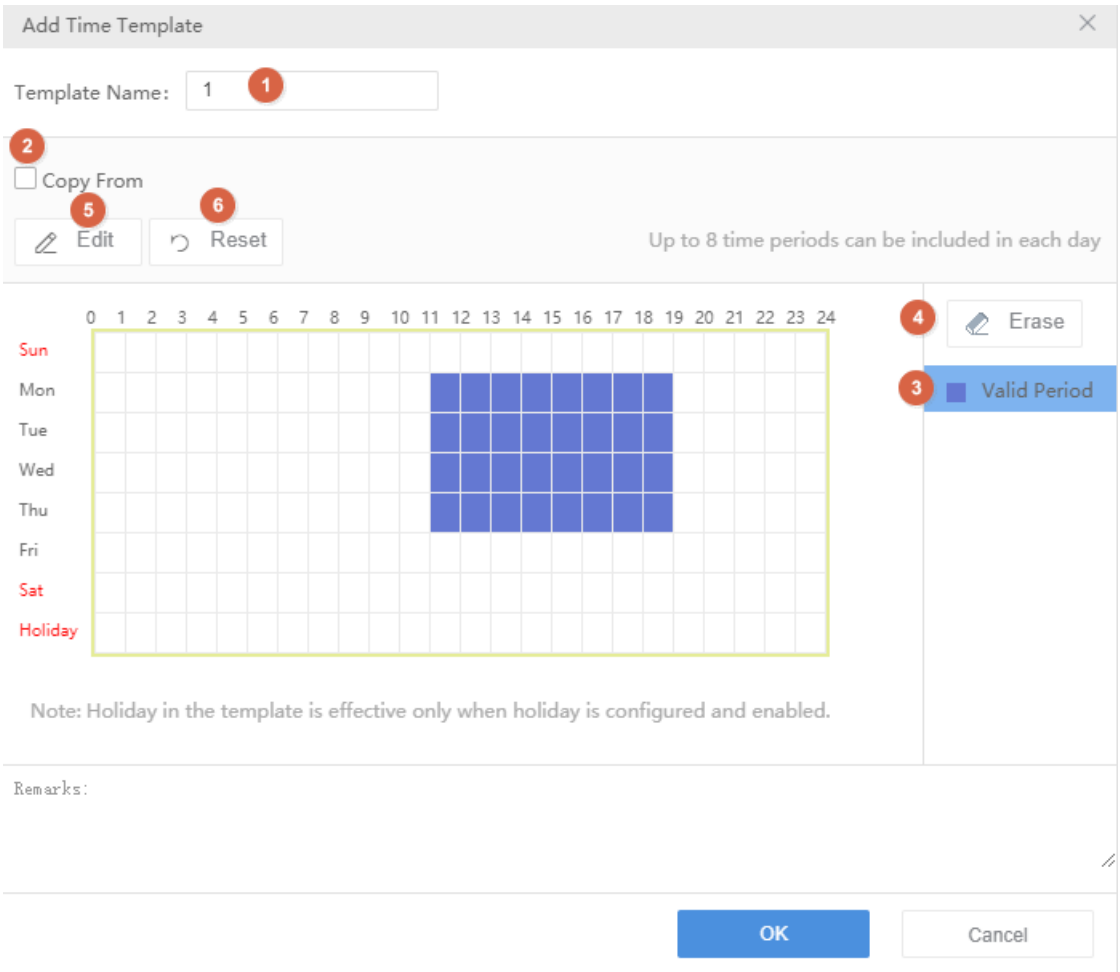
User Time Template

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.

Note:

- All-day is the default template in the system, which you can edit but cannot delete. Using this template means there are no restrictions on login time.
- Up to 8 periods are allowed each day.



No.	Description
1	Enter a unique template name.
2	Optional. Select the checkbox and then choose an existing template to copy settings from.

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

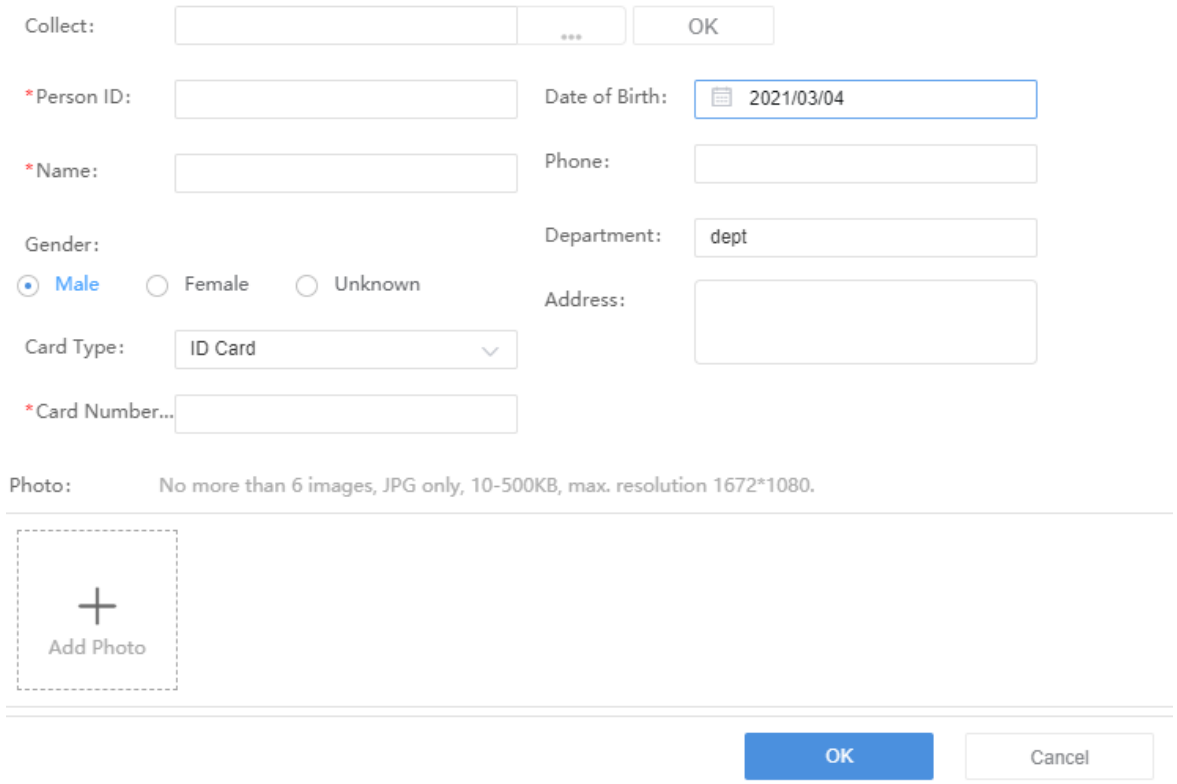
3.3 Person Management

Add people for room & resident management, access control verification, etc.

You need to install the WebAssist plug-in when adding people for the first time. Please log in again after installation.

3.3.1 Basic Info

Add or import the basic information of a person.

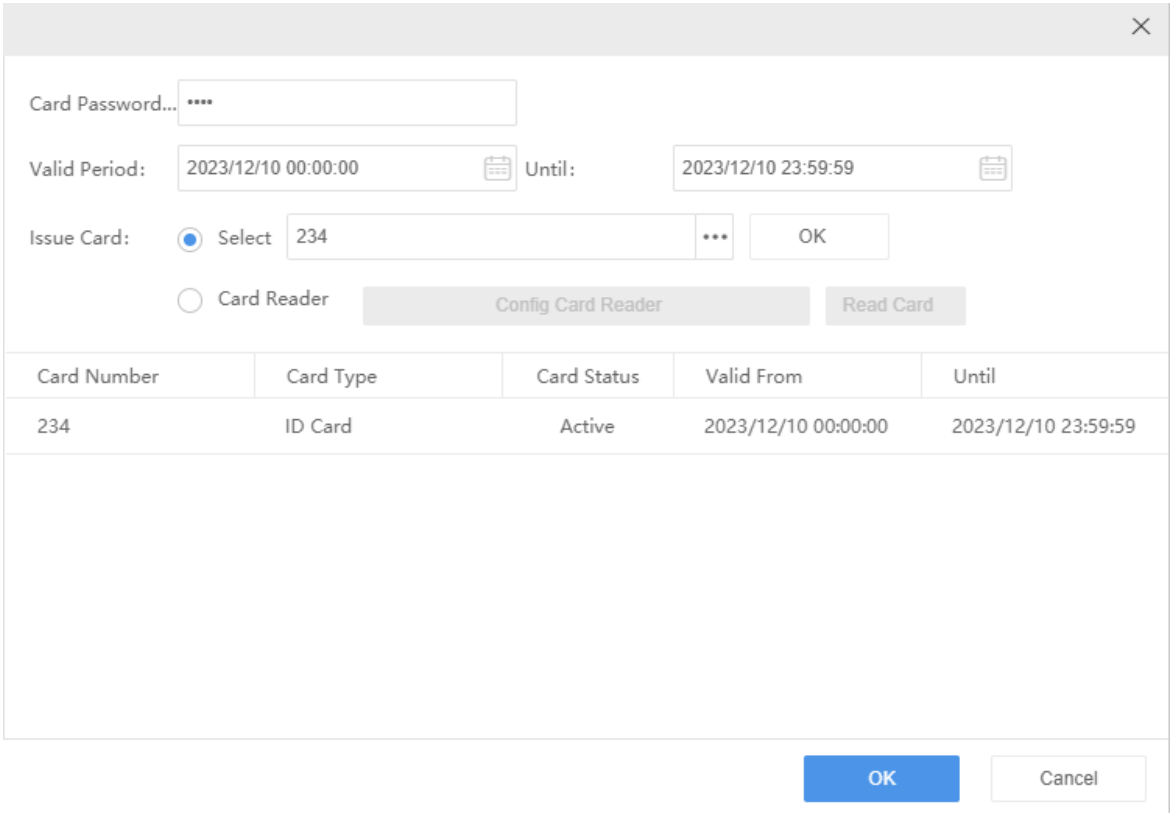


3.3.2 Card

Assign access control cards to personnel, set password and valid period for the card. You can select the card number manually or use the card enroller to read the card number.

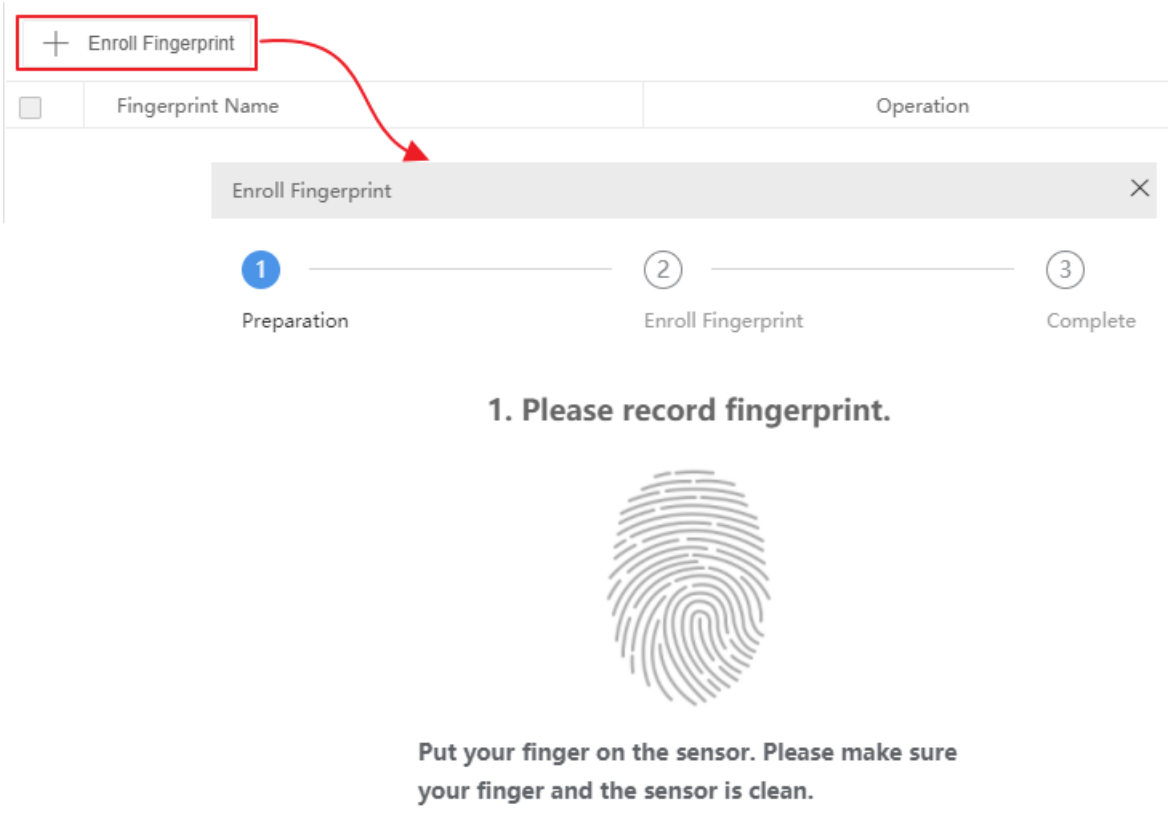
To select the card number manually, you need to add the card number in **Access Control** > **Card** > **Blank** first. After selecting the card number, click **OK**.

To read the card number using a card enroller, click **Config Card Enroller**, select the card type, click **Read Card**, and then the card number will be automatically read into the platform.



3.3.3 Fingerprint

You can enroll personnel fingerprints (used for access control verification). Up to 10 fingerprints are allowed for each person.



1. Connect the fingerprint enrollment device to the computer where the client is installed.
2. Click **Enroll Fingerprint**, and then follow the on-screen instructions to enroll the fingerprint.

Subsequent Operations

If you want to use the fingerprint verification on the access control, you need to configure the access control device.

1. Go to **Access Control** > **Permissions** > Check Template to add a check template and select the verification method as **Fingerprint**.
2. Go to **Basic Configuration** > **Device Management** > **Channel** > Door Channel to configure the 1:N matching threshold, personnel library, and check template.

3.4 Device Management

3.4.1 Encoding Device

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

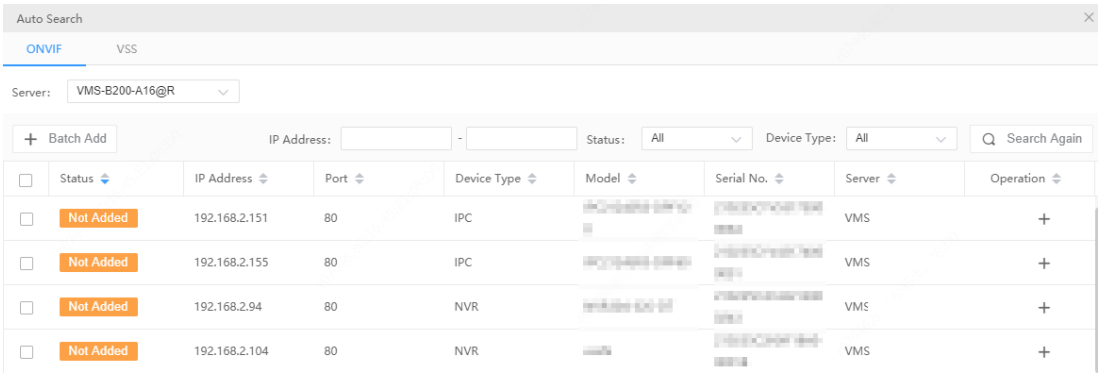
Encoding devices include IPC, NVR and encoder.

Note:

- To add a device with a known IP or domain name, click the **Add** button.
- To add an IPC or NVR for live view using RTSP, click **Add**, and select **Custom** from the **Protocol** drop-down list. For detailed steps, see Add a Device Using RTSP.

Choose one way to add devices.

- Add one by one: Add a device by IP address/domain name.
  1. Click **Add**.
  2. Enter the device information, and click **OK**.
- Auto Search: Search devices on the same subnet with the VMS.
  1. Click **Auto Search**. Encoding devices on the same subnet with the VMS are discovered.



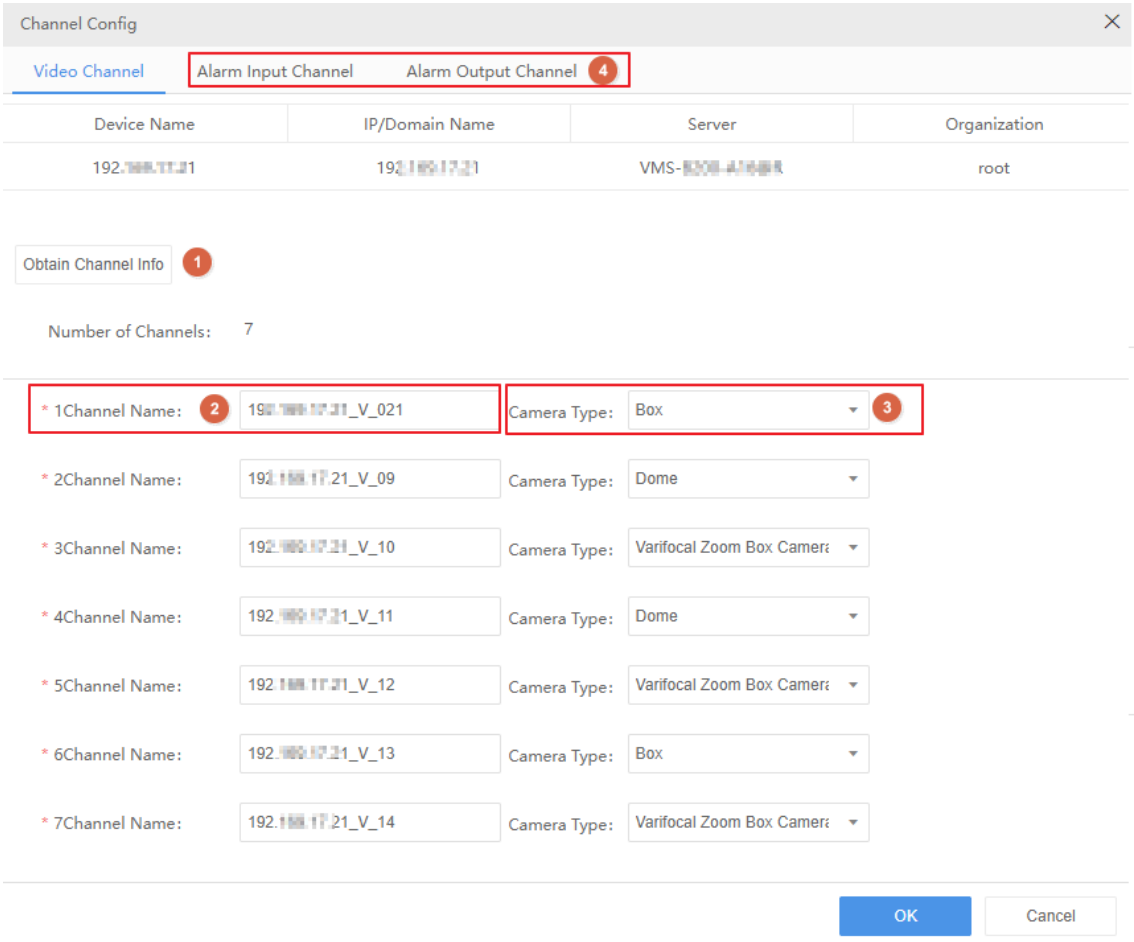
Note:
NVR devices cannot be added via ONVIF.

  2. To add a device, click ＋. To add multiple devices with the same configurations including server, protocol, organization, and username/password, select checkboxes for these devices and click **Batch Add**.
  3. You may search again using the following conditions:
     - Server: Search devices under the specified server.
     - IP address: 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 (see VSS Server and VSS Local for details).
  4. Check device status.

Note:
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.

Other Operations

- Export: Click **Export** to export the device list.
- Edit: Click the corresponding in the **Operation** column, or select the device and then click **Edit** on the top to edit device information.
- Delete: Click the corresponding in the **Operation** column, or select the device and then click **Delete** on the top to delete the device.
- Obtain channel information: Click the corresponding in the **Operation** column. A page as shown below appears.
  - (1) Click **Obtain Channel Info** to get channel information from the device (e.g., an NVR).
  - (2) Rename the channels displayed on the VMS, the change does not affect the channel names saved on the device (e.g., NVR).
  - (3) Select camera type. Different camera types are represented by distinct icons in the resource tree: box camera , dome camera , varifocal zoom box camera .
  - (4) View alarm input and output channels .



- Go to a device's Web interface: Click the corresponding in the **Operation** column to open the device's Web page.
- Sync channel information: Select devices, and then click **Sync Channel Info** on the top of the device list to synchronize channel information (channel names) from the selected devices to the VMS (for example, after channel names are changed on the NVR). You can view the updated channel information at **Basic** > **Device** > **Channel** > **Encoding Channel**.

3.4.2 Smart Device

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

Add smart devices (IPC/NVR/AIBox/EIA) to operate functions such as Face Recognition, LPR, and Mix Traffic Detection on the software client.

Face recognition and LPR

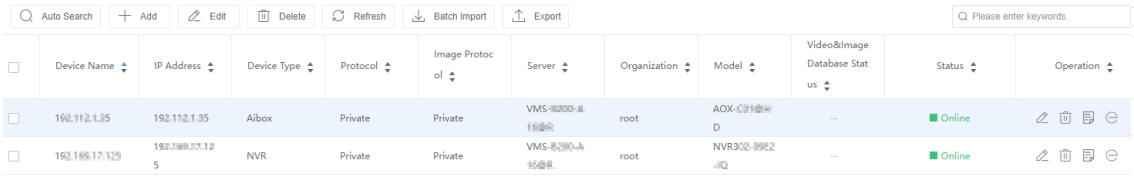
Add smart devices to operate the Face Recognition and LPR modules on the software client.

1. Add devices (see Encoding Device for details).

   Note:
   About setting the **Image Protocol** parameter:

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

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



Mixed traffic detection

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

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

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

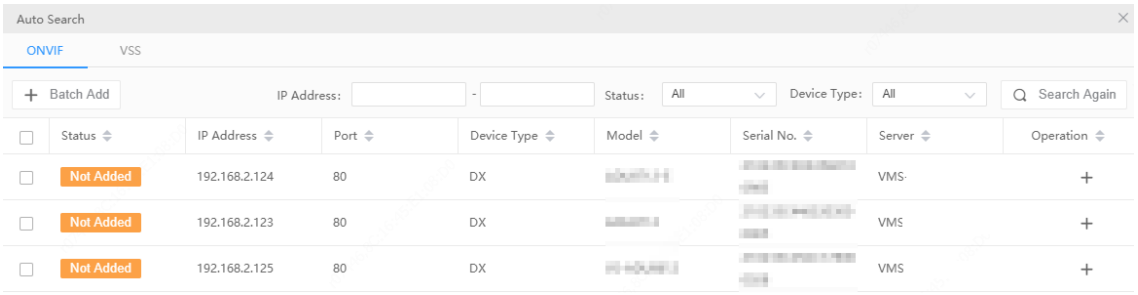
Click **Export** to export the device list.

3.4.3 Decoding Device

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

Note:
To add devices one by one or in batches, see Encoding Device for details.

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



2. Click ＋ for the device to add. To add devices with the same configurations (protocol, organization, username/password), select checkboxes for the devices and then click **Batch Add**.
3. You may set the following conditions and search again:
   - **IP**: Search devices within the specified IP range.
   - Filter devices by status (added or not) and type (decoder, DX).
4. Check device status.

Note:
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.

Click **Export** to export the device list.

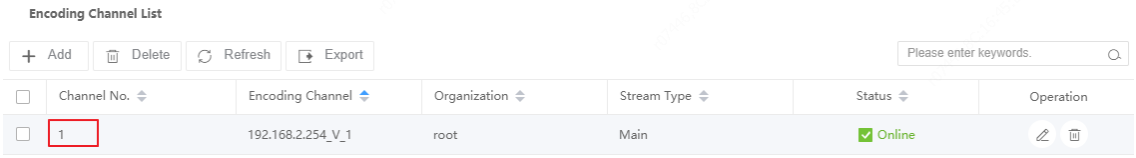
3.4.4 Network Keyboard

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

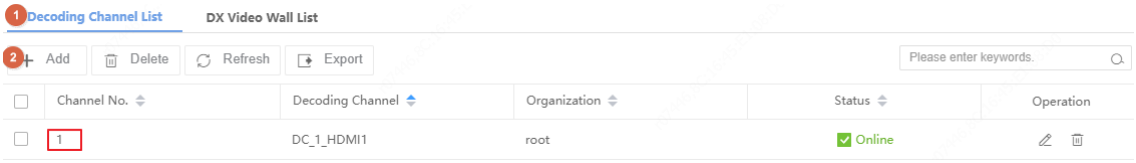
Add a network keyboard to use with a video wall to split windows, zoom in or out, adjust focus, and control the PTZ.

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

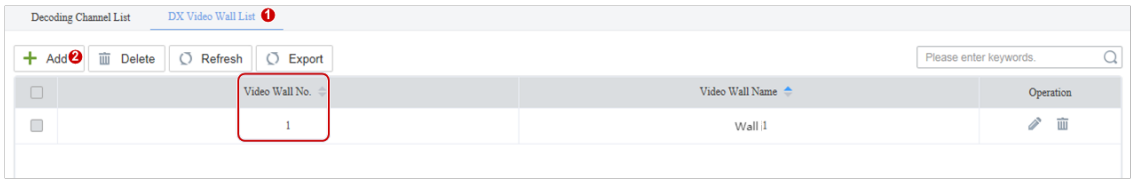
1. Add video channels (cameras). Each video channel is assigned a channel number (e.g., 1).



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



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



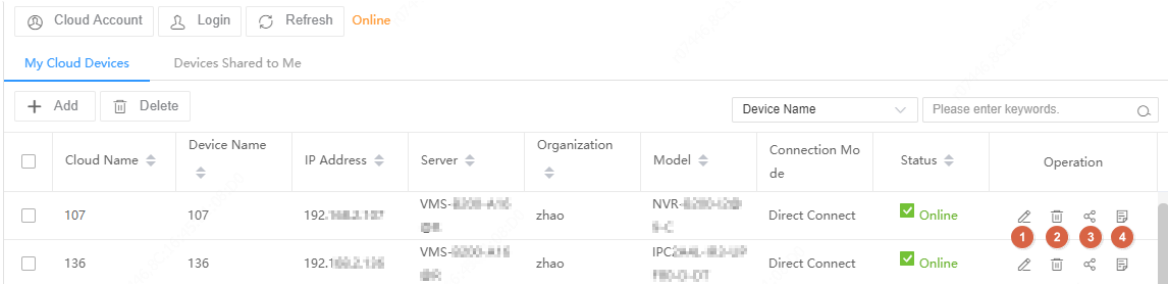
4. After the above steps are completed, you can start video on the video wall by entering the assigned channel numbers and video wall number on the keyboard.

3.4.5 Cloud Device

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

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

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

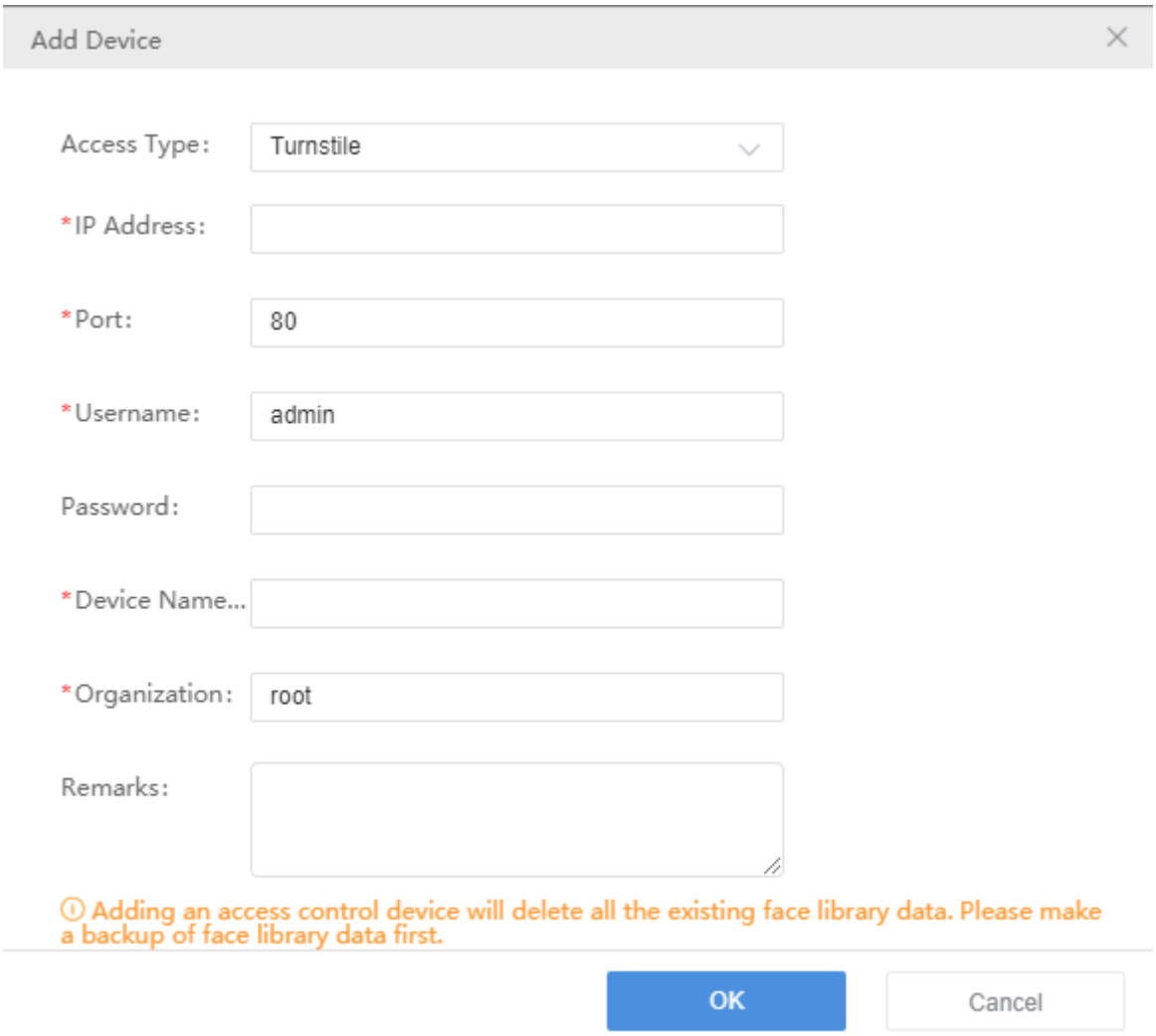


Purpose	Description
Log in to a cloud account	Enter your cloud account info to log in. When login succeeds, the cloud account appears on the tree on the left, and the existing devices under the cloud account are listed on the right. Login to multiple cloud accounts is allowed. You can click a cloud account on the tree to view devices under this account.
Manage cloud accounts	Manage cloud accounts on the VMS. You can refresh the status, log out of a cloud account, view shared devices, and cancel sharings.
Add cloud device	Add devices to specified online account(s). The device name and register code are required. The added devices are listed on the **My Cloud Devices** tab and are displayed as **Online** if they are successfully logged in. VMS cannot be added here.
Edit cloud device (1)	Rename a device. If the **Sync to Cloud** checkbox is selected, the new device name will be synced to cloud; otherwise, only the name saved on the VMS is changed.
Delete cloud device (2)	Delete a device from a cloud account.
Share cloud device (3)	Share device(s) with other cloud account(s). You need to specify a valid period for the sharing and assign permissions by selecting an existing user created on the device to share.
View cloud devices shared from other cloud accounts	View device(s) shared with you from other cloud account(s). You can stop a sharing proactively.
Obtain channel info (4)	Obtain channel info of a cloud device, edit channel names.

3.4.6 Access Controller

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

Add **Uniview** turnstiles, face recognition access controllers, ER-SR 1 series access controllers, ER-SR 2 series access controllers, Face/ID enrollment terminal to operate the Access Control module on the software client.



- Add devices (see Encoding Device for details).

  Note:

  If the ER-SR 1 series access controller is not on the same network segment as the platform, you can edit its network configuration by following the steps below:

  1. Connect the access controller's network cable to the platform's NIC.
  2. Click **Auto Search** to find the access controller.
  3. Click for the access controller in the **Operation** column. A dialog box appears.
  4. Modify the IP address and gateway address of the access controller to match the network segment of the platform.
  5. Click **OK**. Reconnect the access controller to its original network, then you can search the device in the platform.

- Make sure you select the correct access control type and set the correct IP/port.
- Check whether the device status is **Online**. A door channel is added automatically if the added access controller is online.

  Note:

  - A door channel will be deleted automatically if you delete the access controller.
  - After a face/ID enrollment terminal is added, you can select the device to collect person information remotely when you add a person in Basic Info. The collected information can be uploaded into the platform automatically.

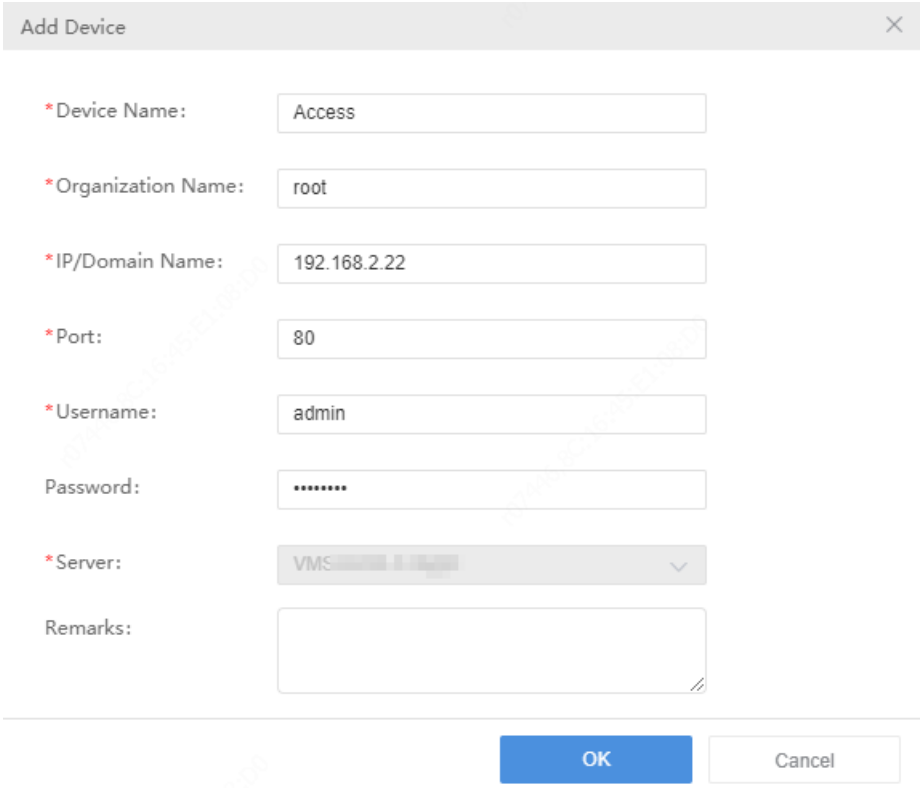
Click **Export** to export the device list.

3.4.7 Access Gateway

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

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

1. Click **Add**.
   Complete settings in the dialog box.



Note:

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

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

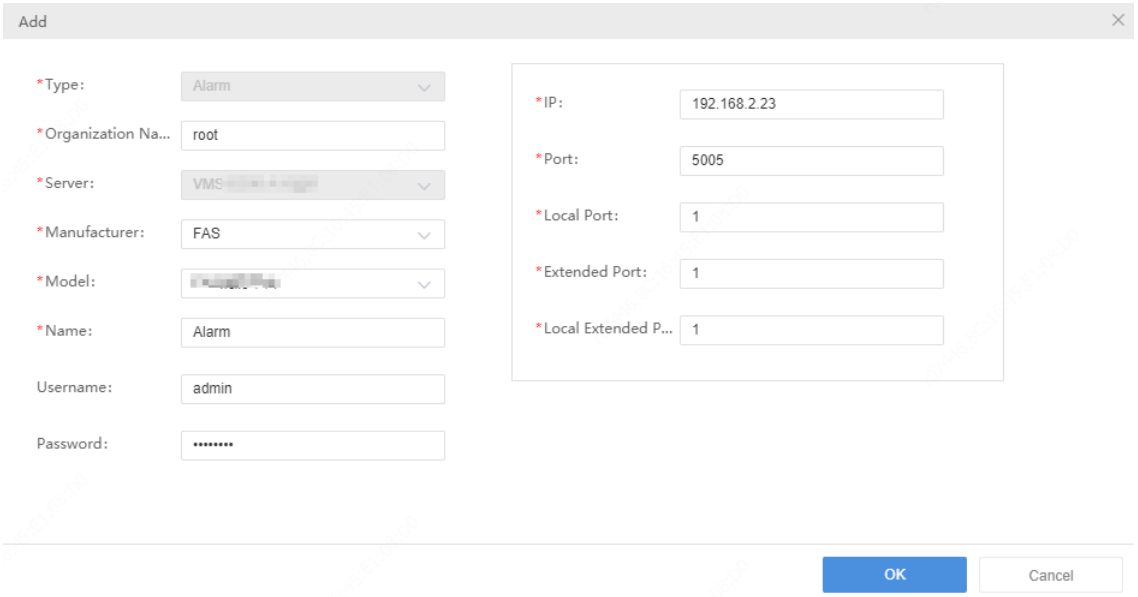
Note:
For alarm controllers and access controllers that are connected to the VMS via gateway, you cannot add their channels directly on the VMS' Web client; they can only be added on the EZAgent.

3.4.8 Alarm Control

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

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

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



Note:

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

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

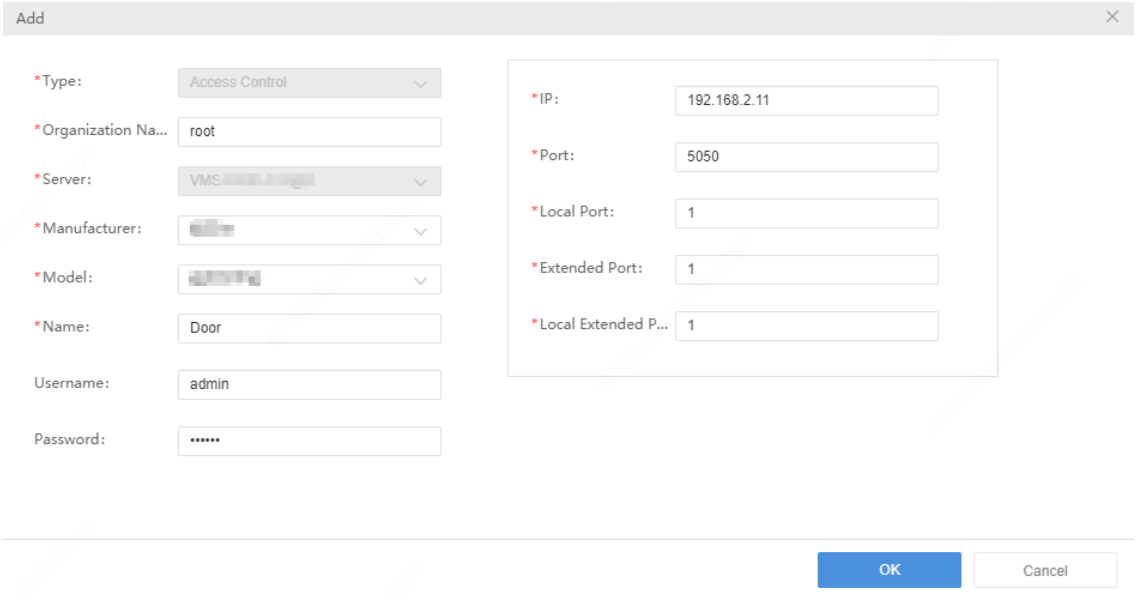
To customize alarm types reported by Uniview alarm controllers, click **Links** > **Custom Alarm**.

3.4.9 Access Control

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

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

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



Note:

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

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

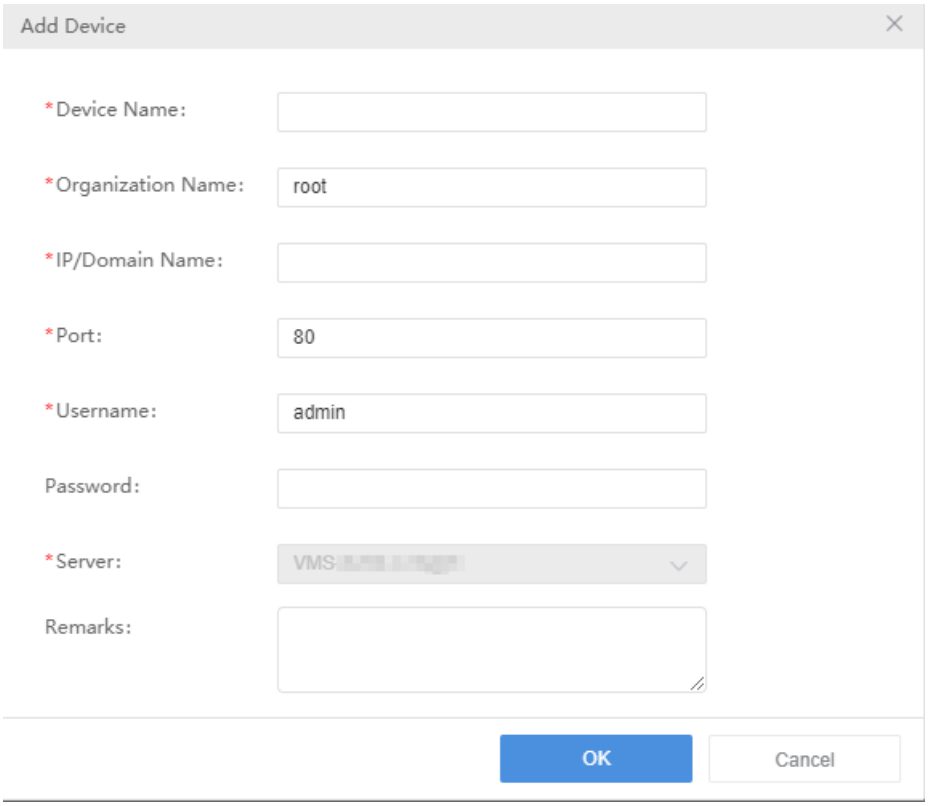
   To customize alarm types reported by Uniview alarm controllers, click **Links** > **Custom Alarm**.

3.4.10 Security Gateway

Basic > **Device** > **Device** > **Security Gateway**

Add an security gateway so the VMS can receive alarms from security gateway.

1. Click **Add**.
   Complete settings in the dialog box.

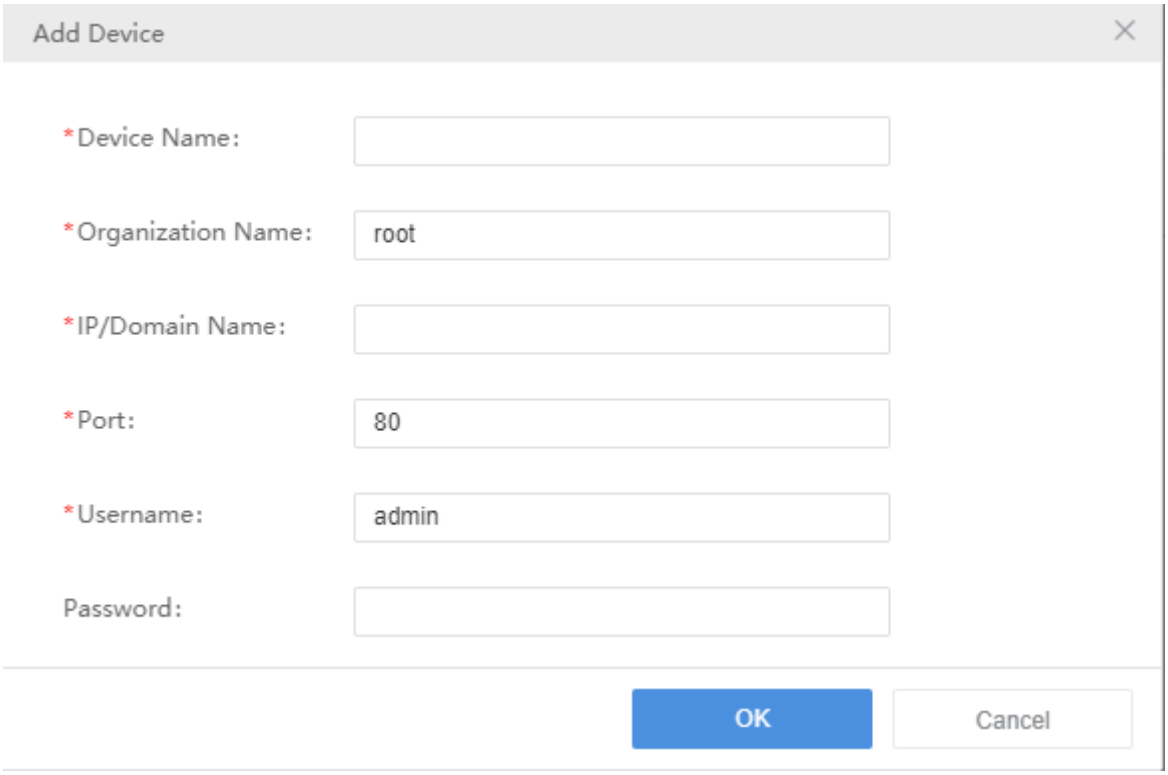


2. The added security gateway is displayed as **Online** if it is connected.

3.4.11 Entrance & Exit Device

Basic > **Device** > **Entrance & Exit Device**

Add and manage entrance & exit devices in parking lots. After configuration, you can operate the Parking Lot module on the software client.



To add a device, click **Auto Search** or **Add** (For more details, see Encoding Device).

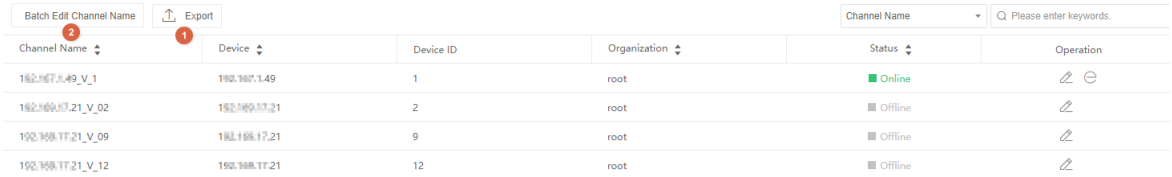
3.4.12 Channel

Encoding Channel

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

- View channel status.
- Click to open the Web page of the encoding device.
- Click to edit channel name and select camera type.

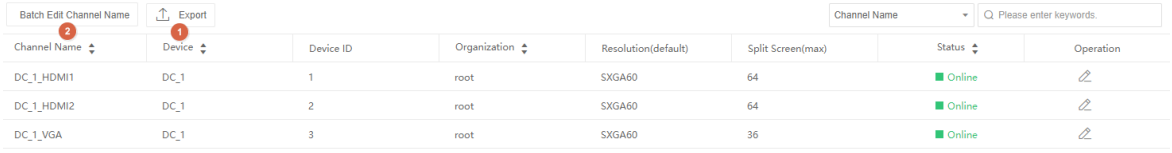
Note:
Different camera types are represented by distinct icons in the resource tree: box camera, dome camera, varifocal zoom box camera.



Decoding Channel

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

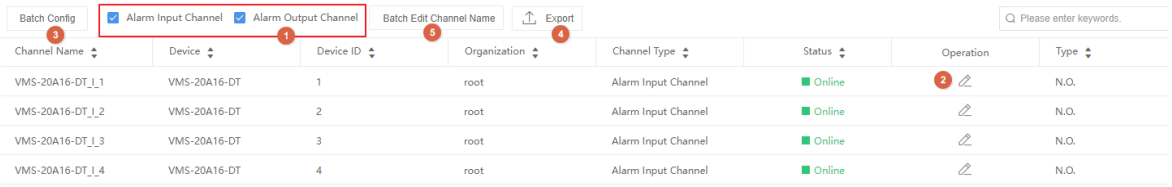
- View channel status and capability.
- Click to edit channel name.



Alarm Channel

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

- View alarm input and output channels. You can select the checkbox(es) (1) to display the corresponding type(s) only.
- Edit channel names or alarm types (N.O. or N.C.) in the **Operation** column (2). The alarm input channel can be enabled or disabled. For the alarm output channel, you can edit **Delay** to set the duration of the changed status before the default status is restored. You can click the **Batch Config** button (3) to configure settings in batches.

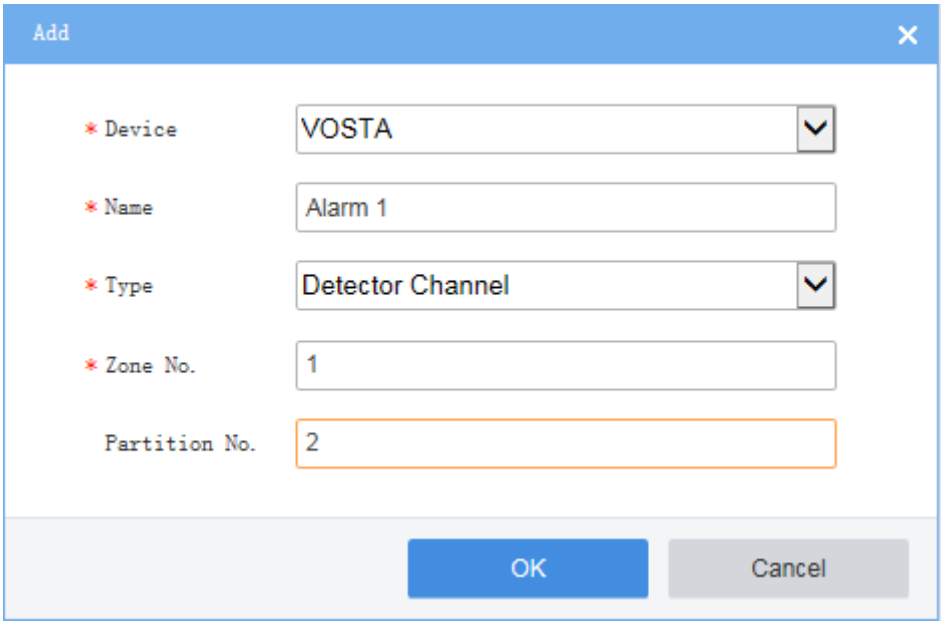


Note:
N.O. means normally open, and N.C. means normally closed.

Detector Channel

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

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

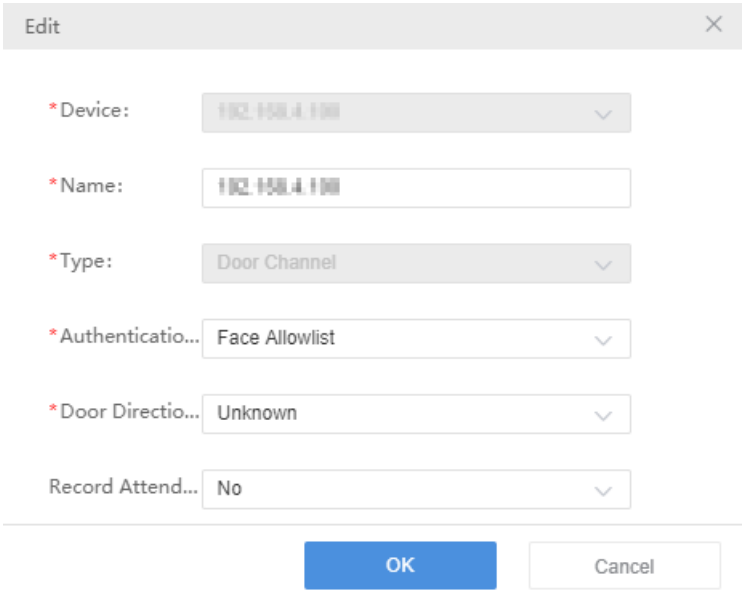


Door Channel

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

A door channel is automatically added when a Uniview access control device is added successfully. For third-party access controllers, door channels need to be added manually.

You can set the channel name, authentication mode/door opening mode, door number, door direction, and whether to record attendance, etc. (The actual configuration items may vary with device type, Please refer to the actual interface.)

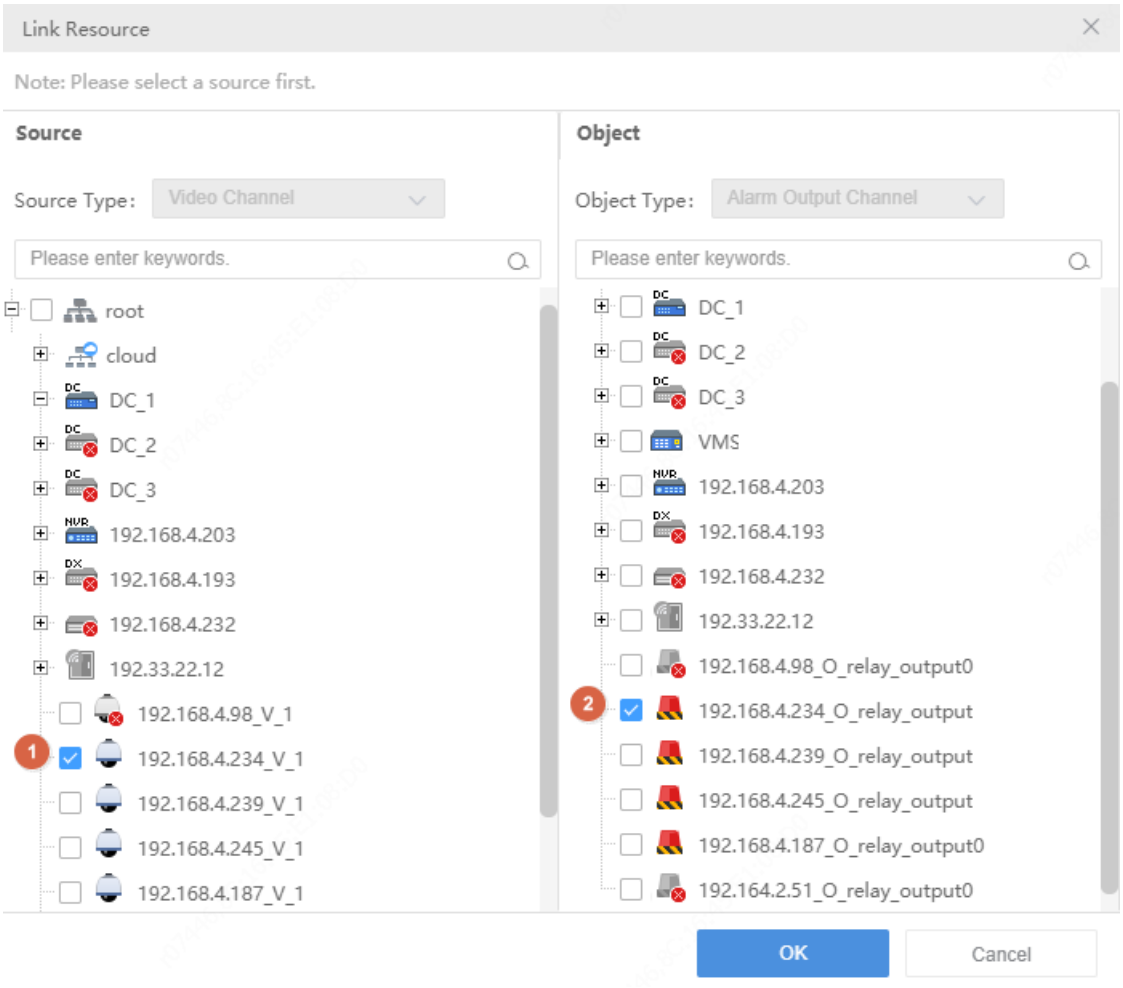


3.4.13 Link Resource

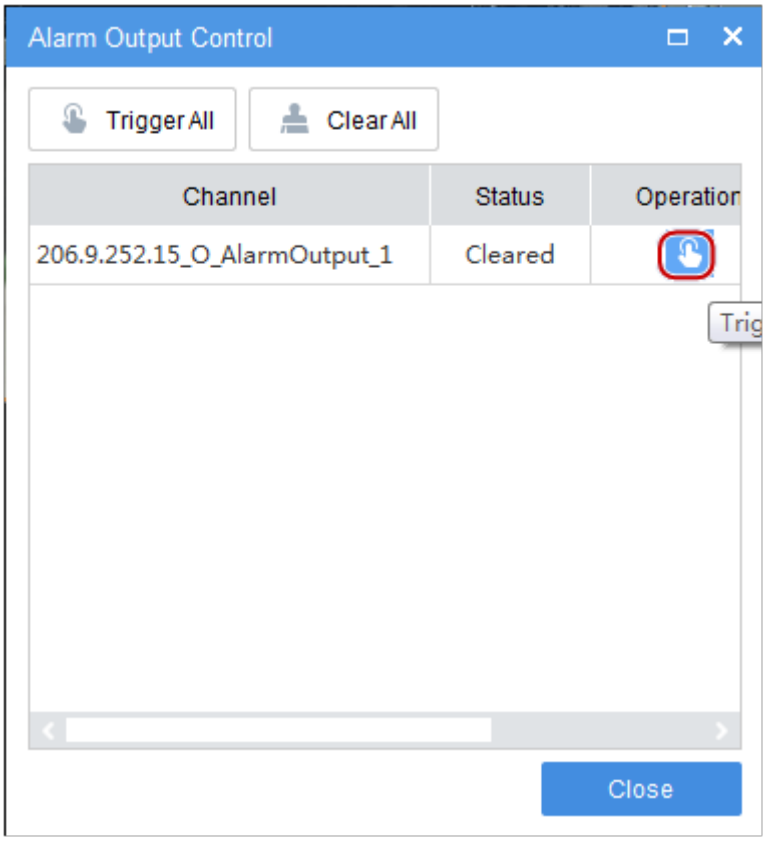
Basic > **Device** > **Link Resource**

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

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



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



3.5 Batch Configuration

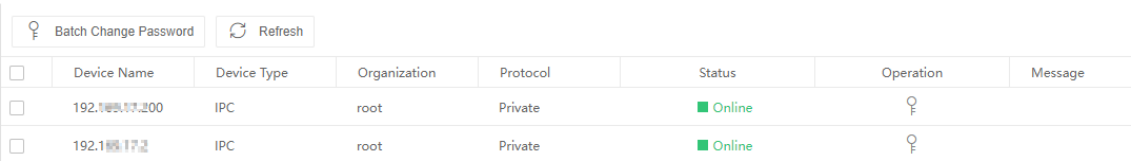
3.5.1 Batch Change Passwords

Basic > Batch Config> Batch Change Password

Batch change passwords of IPCs or NVRs.

This function is not available to VSS devices and cloud devices.

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



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

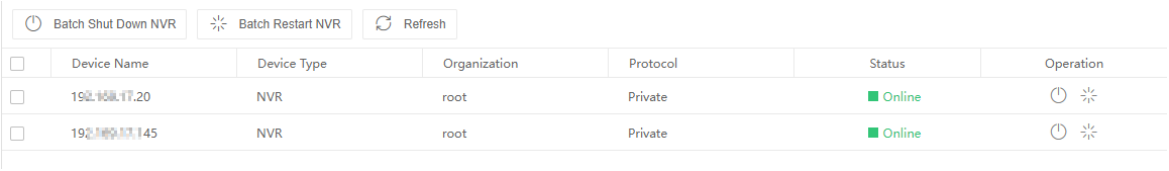
3.5.2 Batch Operate NVRs

Basic > Batch Config > Batch Operate NVRs

Shut down or restart online NVRs in batches.

Note:

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



Shutdown

1. Choose to shut down NVRs one by one or in batches.
   - Batch shutdown: Select NVRs in the device list, and then click **Batch Shut Down NVR**.
   - Shut down one by one: Click the corresponding for the NVR.
2. Click the **Refresh** . The selected NVR(s) disappear from the page.

Restart

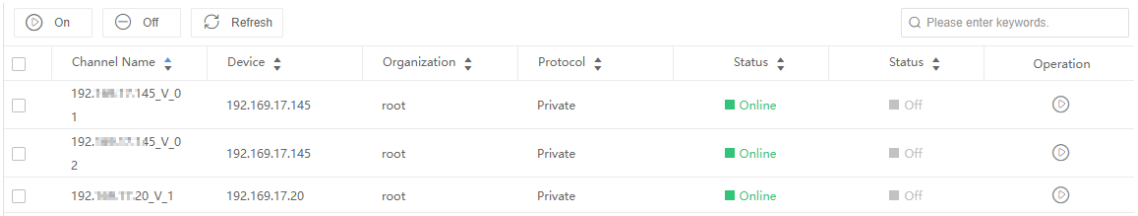
1. Choose to restart NVRs one by one or in batches.
   - Batch restart: Select NVRs in the device list, and then click **Batch Restart NVR**.
   - Restart one by one: Click the corresponding for the NVR.
2. Click **OK** in the pop-up window to restart. The NVR status is **Offline** during restart.
3. Wait until the NVR(s) complete restart, and then click the **Refresh**. The status of the restarted NVR(s) will be **Online**.

3.5.3 Batch Scramble Streams

Basic > Batch Config > Batch Scramble Streams

Scramble video streams to enhance data security.

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



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

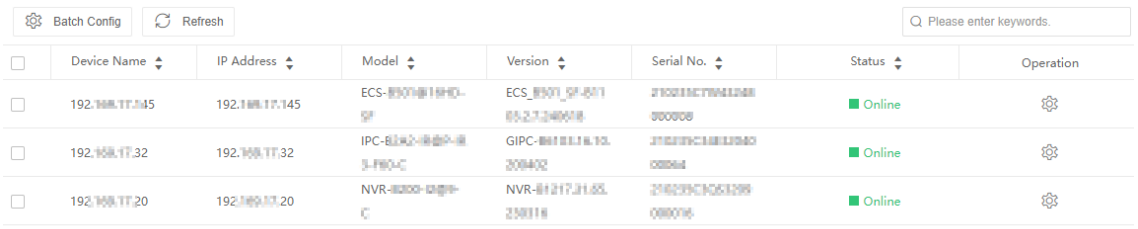
> **Note:**
> This function is available to devices connected via the private protocol.

3.5.4 Batch Configure Encoding Parameters

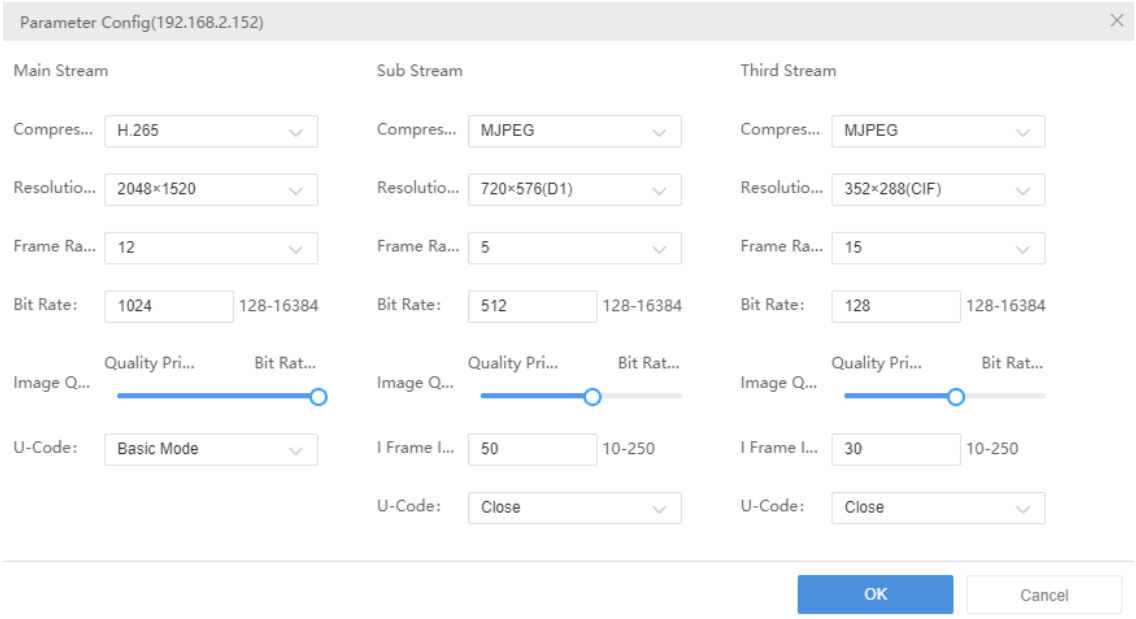
Basic > Batch Config > Batch Config Encoding Parameters

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

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



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



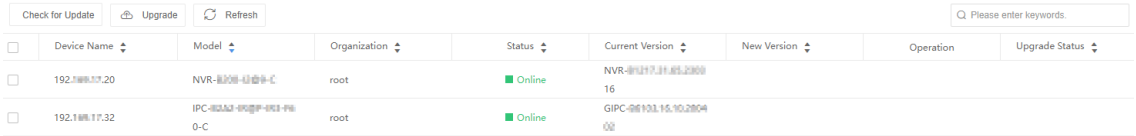
3. Click **OK** to save the configurations.

3.5.5 Upgrade Devices

Basic > **Batch Config** > **Device Upgrade**

Upgrade devices.

1. Choose the organization on the left-side organization tree.
2. Select the devices you want to upgrade, click **Check for Update**. The new version, if available, will be displayed in the **New Version** column.
3. Click **Upgrade** to upgrade the devices.



3.6 Recording Schedule

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

Note: This function is not available to VMS-10A1.

3.6.1 Time Template

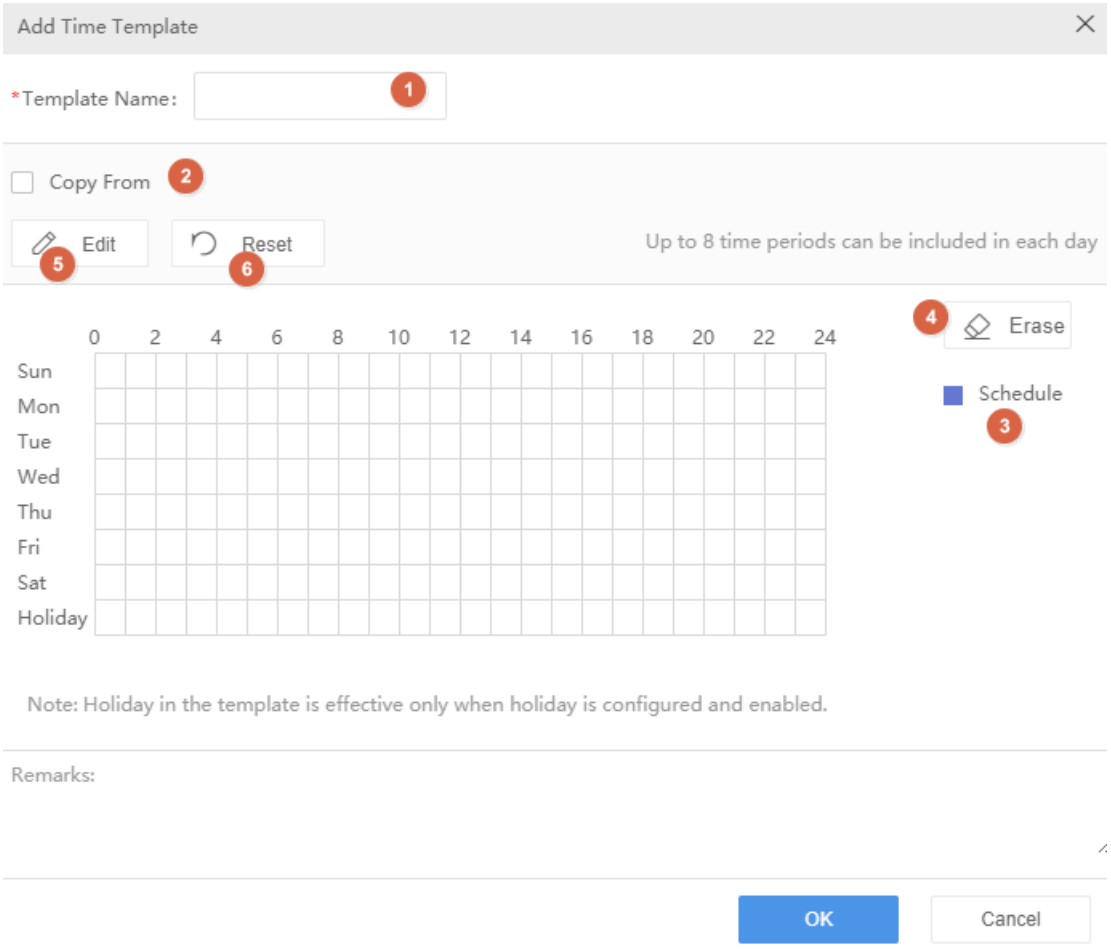
Basic > **Recording Schedule** > **Time Template**

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

Note:

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

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



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

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

Type	Description
Schedule	Record video according to the time set in the schedule.

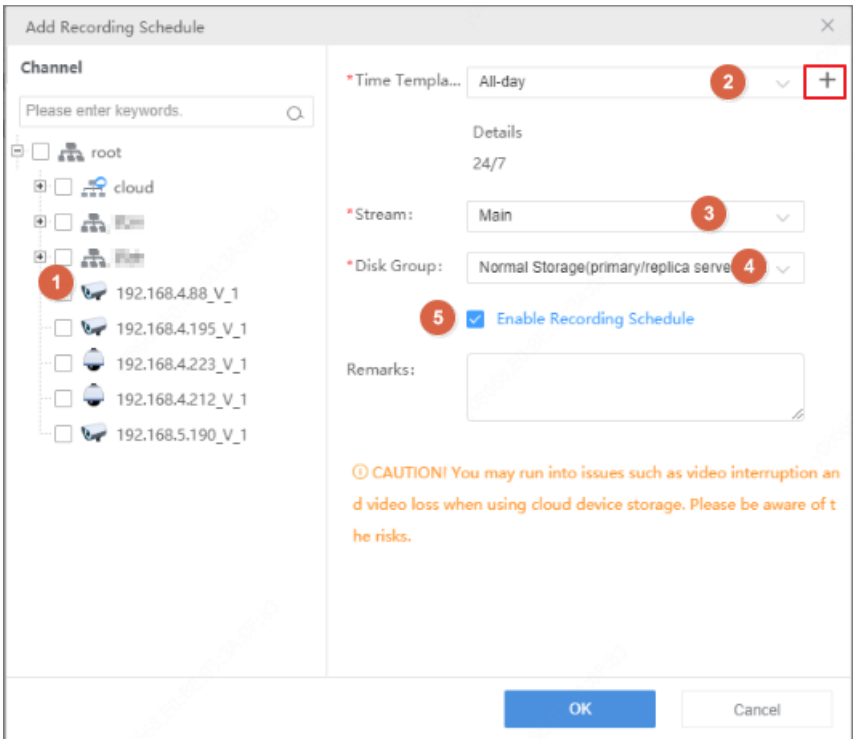
The new time template appears in the list and can be edited or deleted as needed.

3.6.2 Recording Schedule

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

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

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



2. Select camera(s).
3. Select a time template, or click to create one. See Time Template.
4. Select a stream type to record.
5. Select a disk group: normal storage or IPSAN.
6. By default **Enable Recording Schedule** is selected. Clearing the checkbox will disable the recording schedule.
7. Enter a description for the recording schedule in the **Remarks** field.
8. Click **OK**. The new recording schedule appears in the list.

Note:

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

Other operations

- Edit a recording schedule: Click the corresponding in the **Operation** column, or select the recording schedule and then click **Edit** on the top, and then modify the recording schedule. Click **OK** to save the settings when you complete.
- Enable a recording schedule: Click the corresponding in the **Operation** column, or select the recording schedule and then click **On** on the top. The recording schedule takes effect when enabled.
- Disable a recording schedule: Click the corresponding in the **Operation** column, or select the recording schedule and then click **Off** on the top. The recording schedule does not take effect when disabled.
- Delete a recording schedule: Click the corresponding in the **Operation** column, or select the recording schedule and then click **Delete**.

- Quick navigation: Click **Links** on the top, and then choose **Recording** or **Allocate Space** from the drop-down list to navigate to the corresponding page.

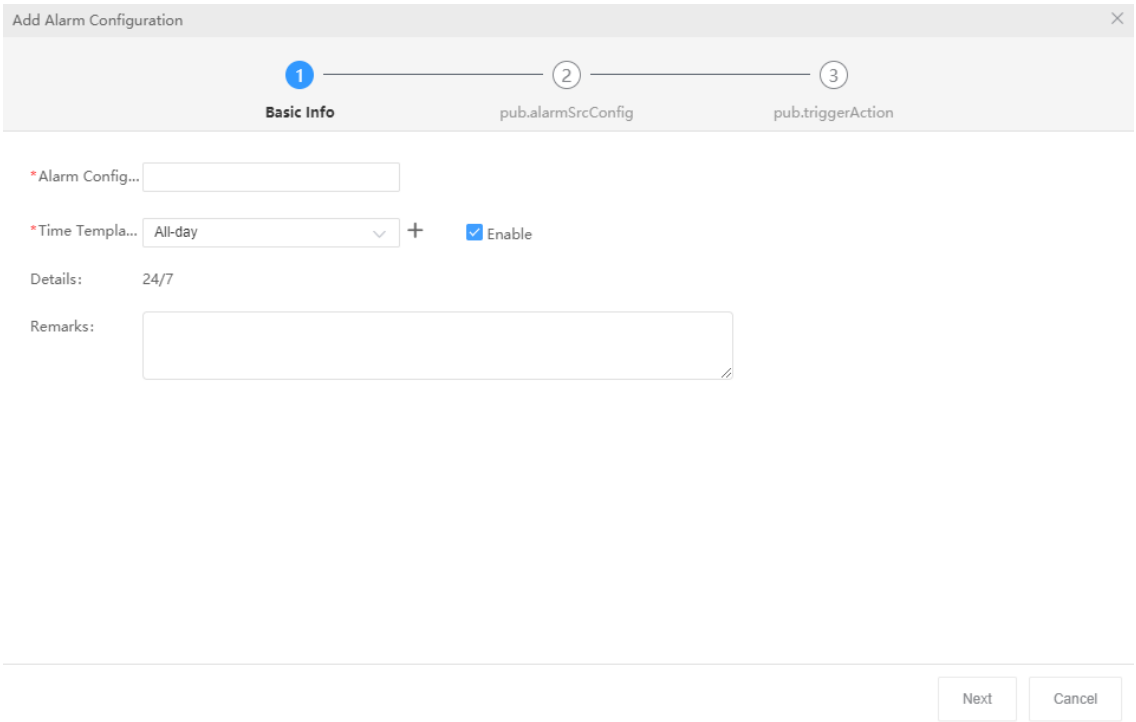
4 Alarm Configuration

Configure time templates, alarms, linkage actions, and alarm subscription so the specified actions will be triggered and the specified users will be alerted when an alarm occurs. Linkage actions include recording, email, and snapshot. You can also customize alarm levels to assign different severity levels to different alarm types.

4.1 Alarm Configuration

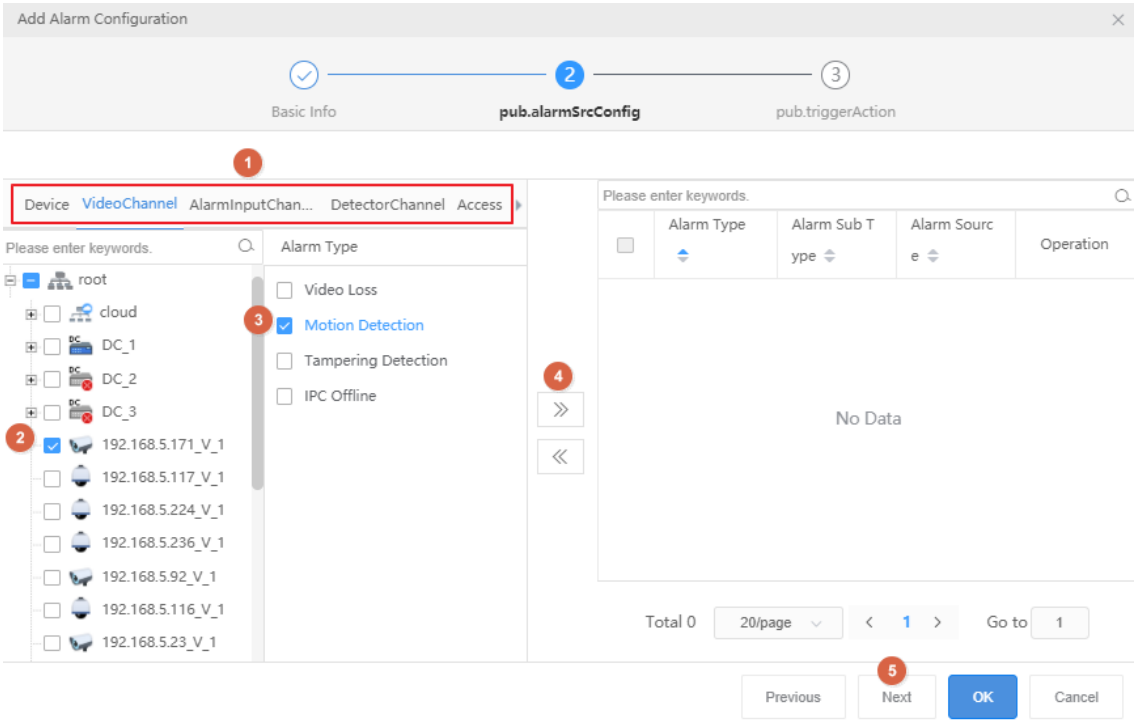
Alarm Configuration > **Alarm Configuration**

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



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

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



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

3. Set action(s) to trigger and object(s) to link. When an alarm of the specified type occurs at the alarm source, the linked object(s) will perform the specified action(s). To trigger email, you also need to complete email settings (see Email). To trigger buzzer, select **Enable Buzzer**. When an alarm of the specified type occurs at the alarm source, the linked object(s) will perform the specified action(s).

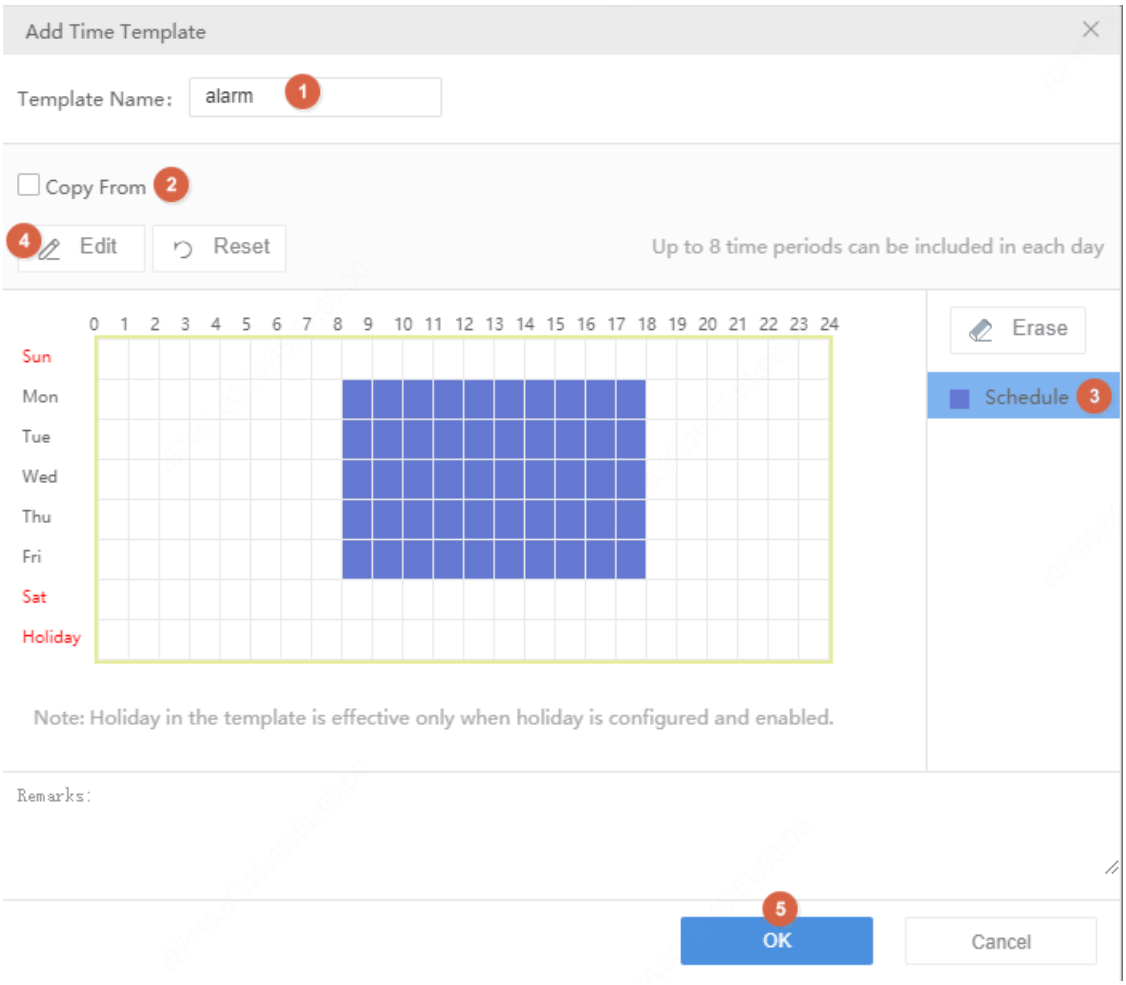
The alarm configuration appears in the list and can be deleted, enabled or disabled as needed. Alarm configuration is not effective when disabled.

4.2 Time Template

Alarm Configuration > **Time Template**

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

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



2. 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.
3. (Optional) Select **Copy From** and select a template from the drop-down list. Edit based on this template.
4. Click **Schedule** on the right and then drag the mouse to draw on the template. Use the **Erase** or **Reset** button to clear some or all settings.
5. To set precisely, click **Edit**. After completing the schedule for a day, you may copy the settings to other days by selecting the day(s) and clicking **Copy**.
6. Click **OK**.

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

4.3 Email Records

Alarm Configuration > **Email Records**

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

Click **Test email** to test.

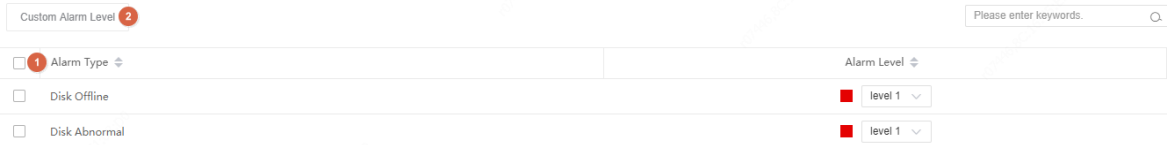
Note:
An email server must be configured before testing the email. For details, see Email.

4.4 Custom Alarm Level

Alarm Configuration > **Custom Alarm Level**

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

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



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

4.5 Alarm Subscription

Subscribe to specified alarm types from specified devices so that only alarms of interest will be pushed to the client.

Type	Description	Difference
Client Alarm Subscription	Subscribes to real-time alarms of interest for client's users.	• Filters real-time alarms only; all historical alarms can still be viewed. • Needs to specify alarm notification recipients. • When enabled, the subscription will be effective for all periods.
Device Alarm Subscription	Subscribes to alarms from devices of interest.	• Applies to both real-time alarms and historical alarms. • Applies to all users. • You can set the effective time period.

The two subscription types can be configured with only one or both.

When configured at the same time, the **Device Alarm Subscription** rule has higher priority, that is:

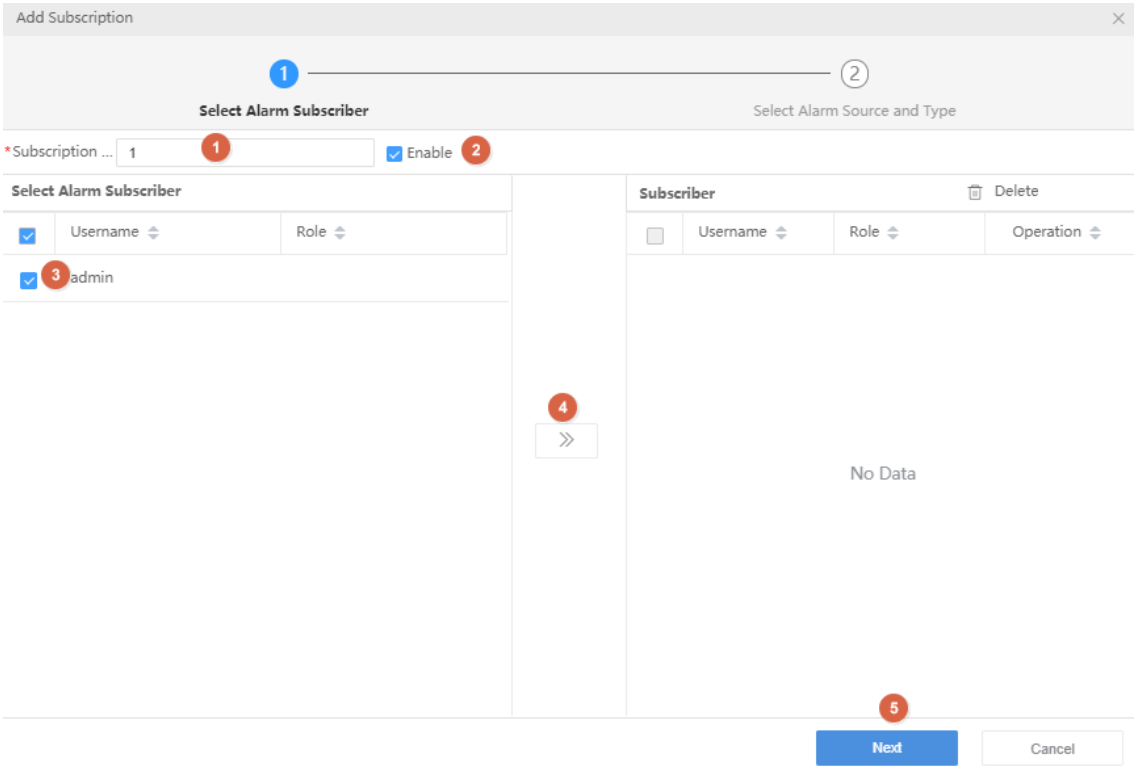
- When **Device Alarm Subscription** subscribes to a certain alarm, the specified users can receive the alarm only when **Client Alarm Subscription** also subscribes to that alarm; otherwise, they cannot receive the alarm.
- If **Device Alarm Subscription** filters a certain alarm type, even if **Client Alarm Subscription** has subscribed to that alarm, the specified users cannot receive the alarm.

4.5.1 Client Alarm Subscription

Alarm Subscription > **Client** >**Alarm Subscription**

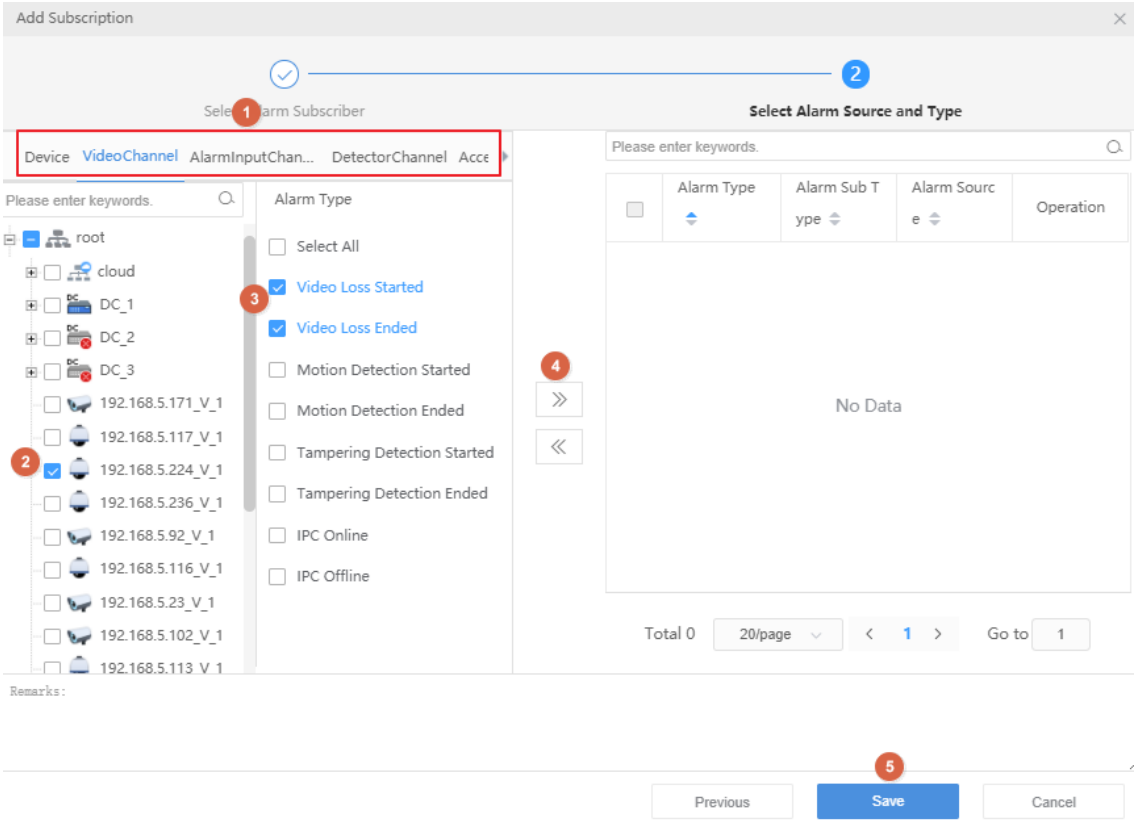
Add alarm subscription to allow specified users to only receive real-time alarm messages of specified types reported by specified alarm sources; other alarm messages will be filtered out (historical records of filtered alarms can still be queried).

1. Click **Add** to add alarm subscription.
2. Select alarm subscriber.



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

3. Select the alarm source and alarm type.



No.	Description
1	Select the alarm source type.

No.	Description
	Note: The types displayed may vary depending on the VMS model and version. The illustration is just an example.
2	Select the alarm source. Only alarms from the specified source will be sent to the subscriber.
3	Select the alarm type. Only alarms of the specified type(s) will sent to the subscriber.

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

Note:

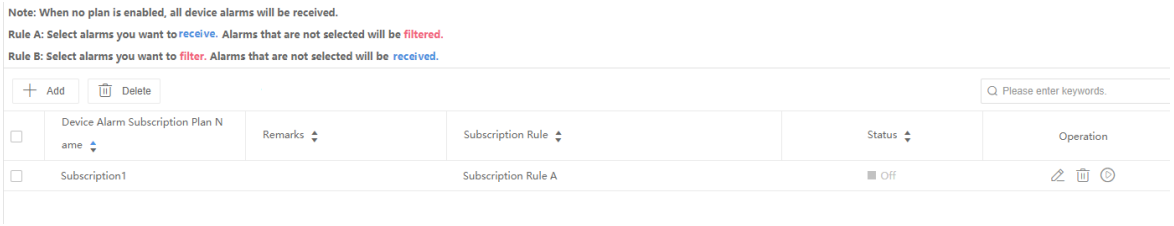
- Alarm subscription is enabled by default. If disabled, the client cannot receive any alarm messages, even if alarm subscription is configured.
- By default, a non-subscriber receives all alarm messages. To block all alarm messages for the user, add the user as an alarm subscriber without configuring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

4.5.2 Device Alarm Subscription

Alarm Subscription > **Device**>**Alarm Subscription**

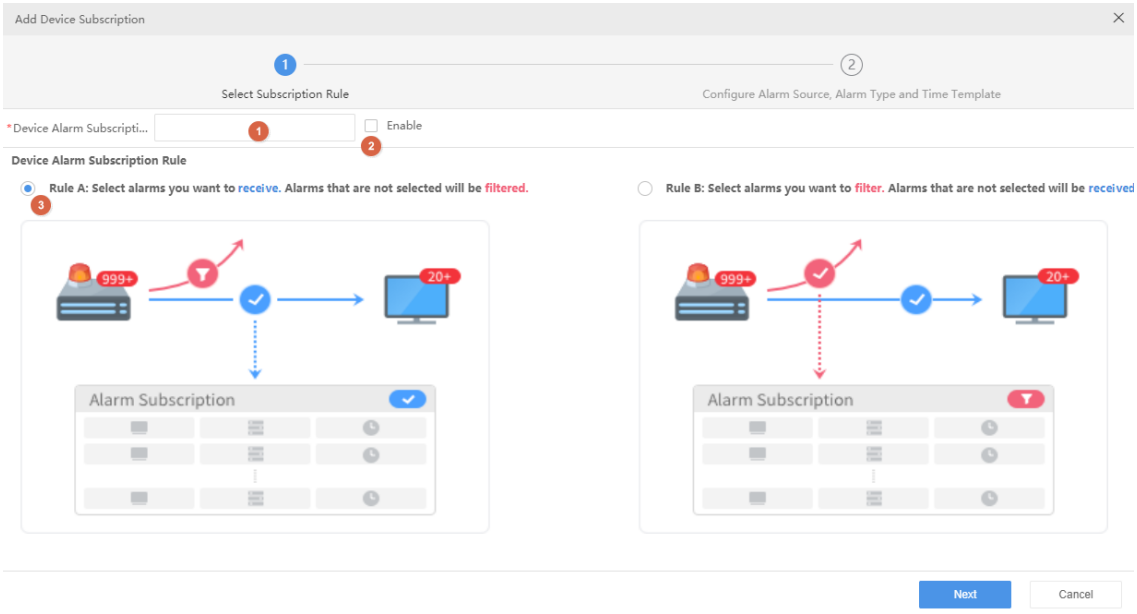
By configuring device alarm subscription rules, it is possible to receive only the alarms of interest and filter out the alarms that are not of interest (filtered alarms will not be saved in the historical alarm records). The effective time period can be set when subscribing to device alarms.

- Rute A: Select alarms you want to receive. Alarms that are not selected will be filtered.
- Rute B: Select alarms you want to filter. Alarms that are not selected will be received.



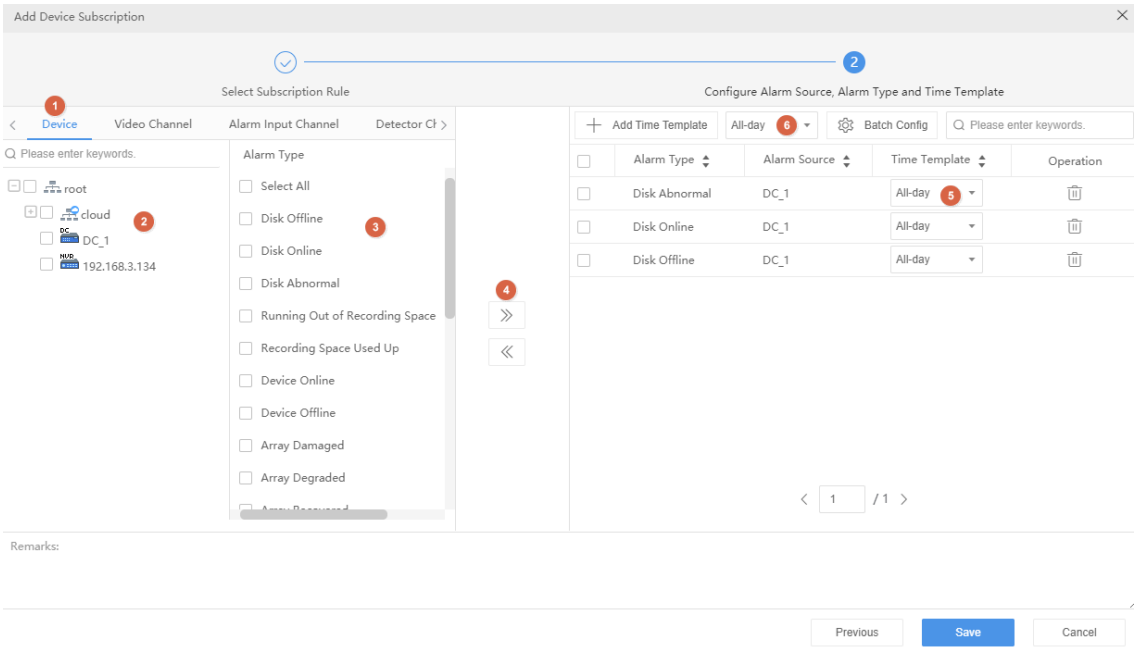
Add device subscription

1. Click **Add** to add device subscription.



No.	Description
1	The device subscription name must be unique in the system.
2	Device subscription is effective when the **Enable** checkbox is selected. You can also choose not to select **Enable** and enable it later as needed.
3	Select **Rute A** or **Rute B**.

2. Click **Next** to configure the alarm source, alarm type, and time template.



No.	Description
1	Select the alarm source type. **Note:** The types displayed may vary depending on the VMS model and version. The illustration is just an example.
2	Select the alarm source. Only alarms from the specified source will be received.
3	Select the alarm type. Only alarms of the specified type(s) will be received. **Note:** Different alarm sources support different types of alarms.
4	Click "**>>**" to add the selected alarm sources and alarm types to the right list.
5	Select the time template to only subscribe to alarms within the allowed time period. **Note:** • Customize time templates: click **Add Time Template**, follow the instructions for the operation, see Time Template. • Batch configuration: Select a time template at ⑥, click **Batch Configuration**, and the time template will be applied to all alarm types.

3. Click **Save**.

Manage device subscription

- Enable/Disable: click enable / disable device subscription.

Note:

- Only the enabled subscription will take effect.
- Only one subscription can be enabled at a time. If there is already a subscription enabled, enabling a new subscription will deactivate the existing plan.

- Edit: Click to edit subscription.
- Delete: Click , or select subscriptions and click **Delete** to delete items.

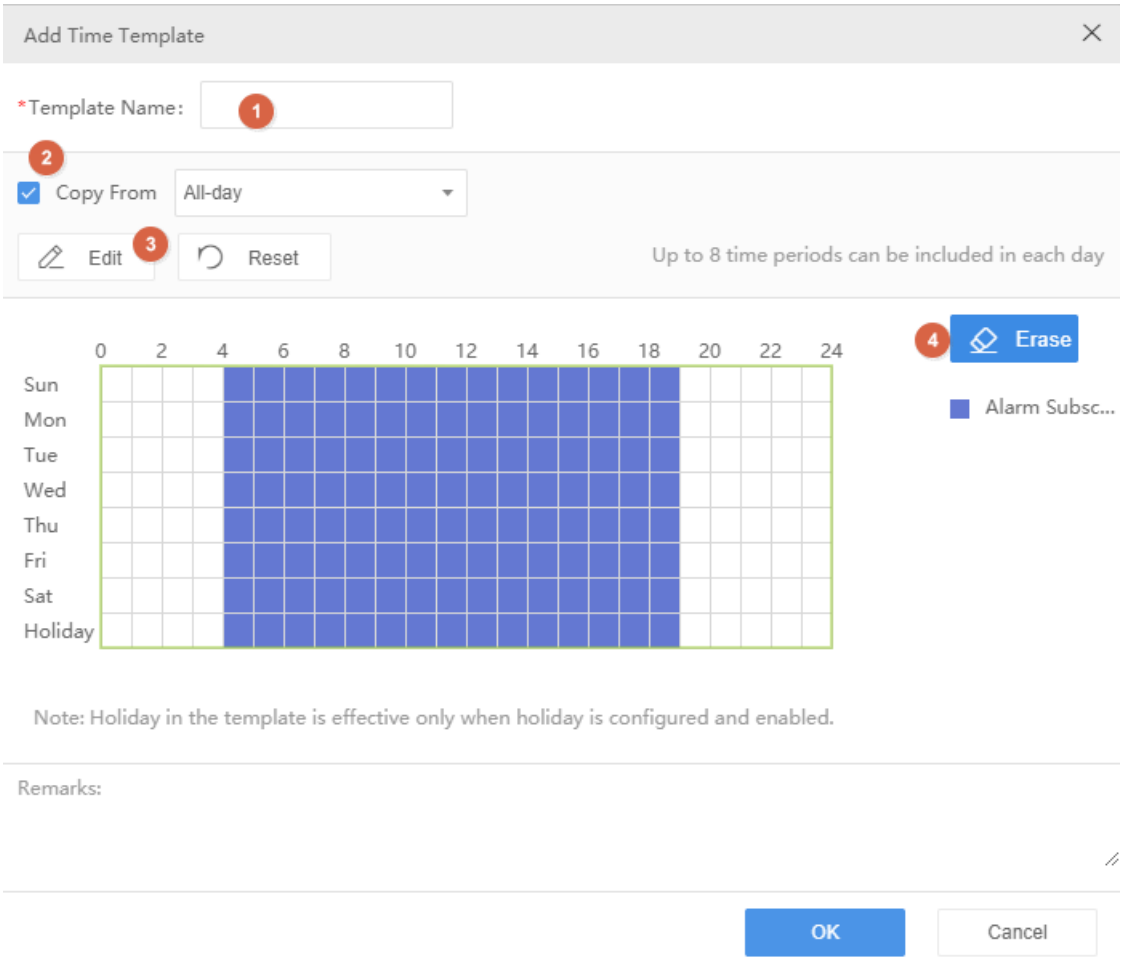
Time Template

Alarm Subscription>Device>Time Template

Note: The created time templates in this page are exclusively for "Device Alarm Subscription" and will not affect other functions that require time templates.

Support pre-creating time templates and configuring the effective time of alarm subscriptions, so that time templates can be quickly applied when subscribing to alarms.

1. Click **Add** to create a time template.



No.	Description
1	Template names cannot be duplicated.
2	Select **Copy From** and select a template from the drop-down list. Edit based on this template. The existing template will not be modified.
3	To set precisely, click **Edit**. After completing the schedule for a day, you may copy the settings to other days by selecting the day(s) and clicking **Copy**. **Note:** A holiday in a time template is effective only when the holiday is configured and enabled (**System** > **Basic** > **Holiday**). See Holiday.
4	Click **Erase** to use the cursor to drag and erase the unnecessary time periods on the time grid.

2. Click **OK**.

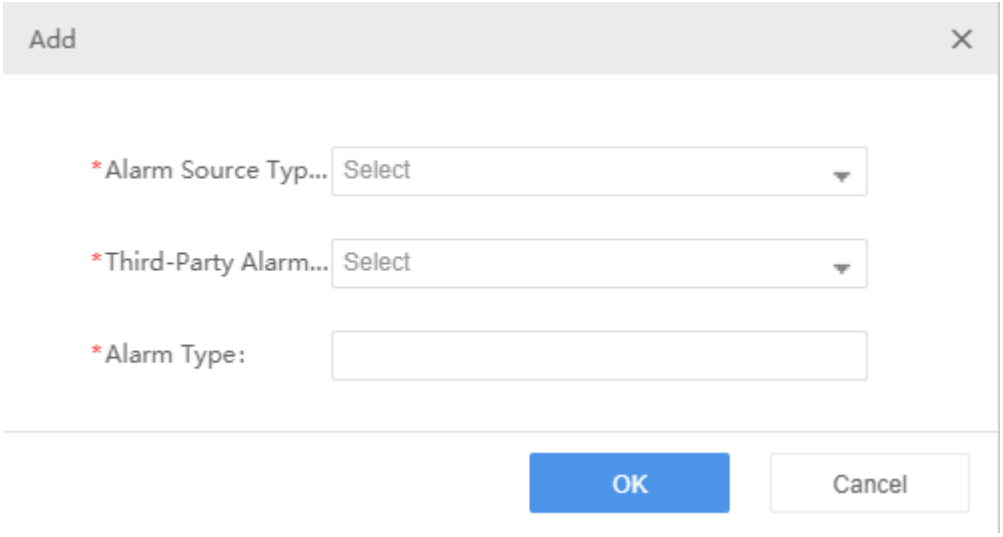
4.6 Custom Alarm

4.6.1 Custom Alarm

Alarm Configuration > **Custom Alarm**> **Custom Alarm**

Customize alarms reported by alarm control panel or access control.

1. Click **Add**.
2. Customize alarms as needed.



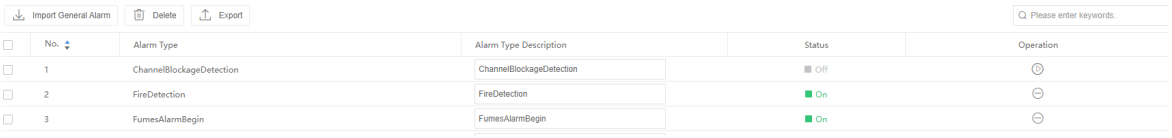
Item	Description
Alarm Source Type	Choose alarm control panel or access control.
Third-Party Alarm Type	Select the alarm type of the alarm source.
Alarm Type	Customize the alarm type displayed on the VMS.

3. Click **OK**. The default custom alarm level is 1, and you may change it at Custom Alarm Level.

4.6.2 General Alarm

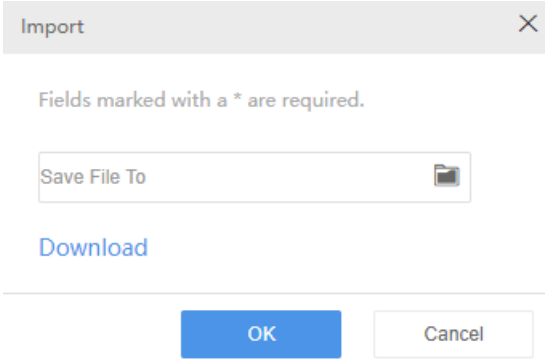
Alarm Configuration > **Custom Alarm** > **General Alarm**

Add device side's (AIBox/EIA) alarm types to the platform so that you can receive alarms reported by these kinds of devices.



Import General Alarm

1. Click **Import General Alarm**. The **Import** page appears. Click **Download** to obtain the import template.



2. Fill in the relevant information for alarm types in the template. Up to 256 alarm types are allowed in a template.

No. (*)	Alarm Type (1 to 64 characters)	Alarm Type Description (1 to 64 characters)	Status (0-Off, 1-On)

   - Alarm Type: Enter the alarm name that is consistent with the alarm type on the device side.
   - Alarm Type Description: Set the alarm name to be displayed on the platform as needed.
   - Status: 0 - disabled, 1 - enabled. The platform can receive this type of alarm only when the status is enabled.
3. On the **Import** page, click to upload the modified template from local.
4. Click **OK**.

Enable/Disable General Alarm

The platform can receive this type of alarm only then the alarm status is enabled.

In the alarm list, click the corresponding / in the **Operation** column to enable/disable the alarm type.

Edit Alarm Type Description

Edit the description in the input box directly, and then click on any blank area to save.

Delete General Alarm

Select general alarm(s) in the list, and click **Delete**.

Export General Alarm

Click **Export** to export the general alarm list into a .CSV file.

5 Recording Backup

Note: This function is not available to VMS-10A1.

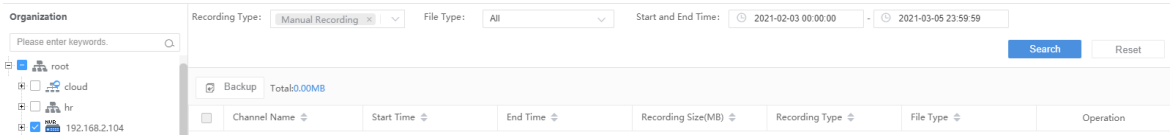
Back up recordings manually or automatically to PC for safety.

You can create backup tasks to back up recordings of specified types according to a schedule.

5.1 Local Backup

Recording Backup > **Local Backup**

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



1. Select channels on the left, and then set search conditions on the right, including recording type, file type, time period, and then click **Search**.
2. (Optional) Click buttons in the **Operation** column to play or back up a recording file.
3. Select files to back up. The space required for the backup is displayed next to the **Backup** button. Click the button.
4. On the page displayed, set the backup task and path; you may also:
   - Create new folders in the USB drive.
   - Edit or delete exiting files or folders in the USB drive.
   - Format the USB drive into NTFS or FAT32 format.

- View the total space and remaining space of the USB drive.

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

6 System Configuration

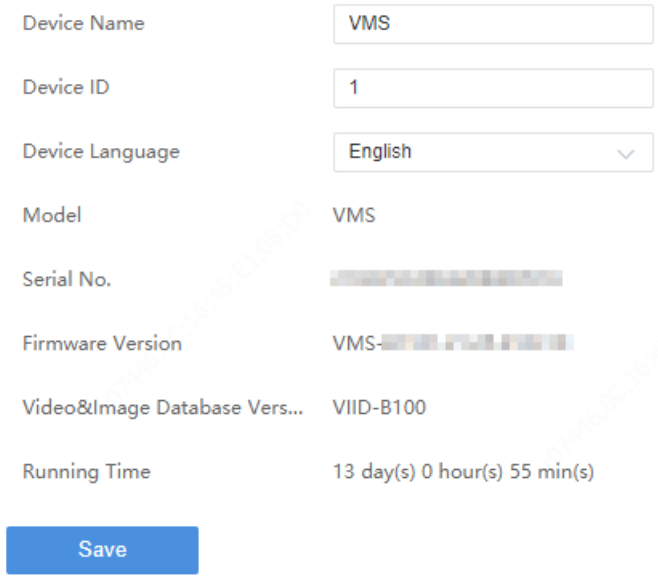
System configuration configures general parameters of system (time, holidays, HDD, network, etc.) and includes basic configuration, disk configuration, network configuration, protocols & interconnection, security configuration, system maintenance, and map configuration.

6.1 Basic Configuration

6.1.1 Basic

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

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



Note:

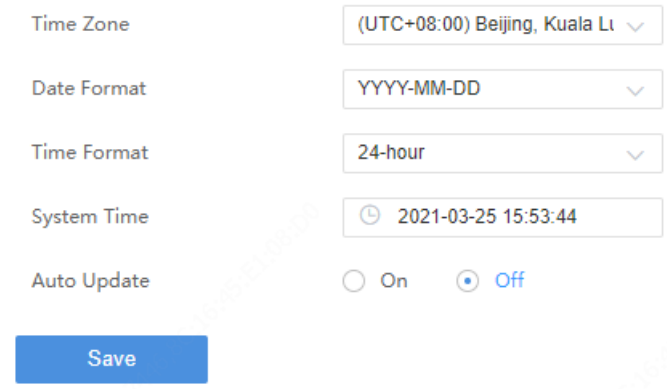
- Currently device ID is not in use.
- The **Running Time** shows how long the VMS has been running since its latest startup. This can be used to determine when a restart has occurred.

6.1.2 Date & Time

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

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

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

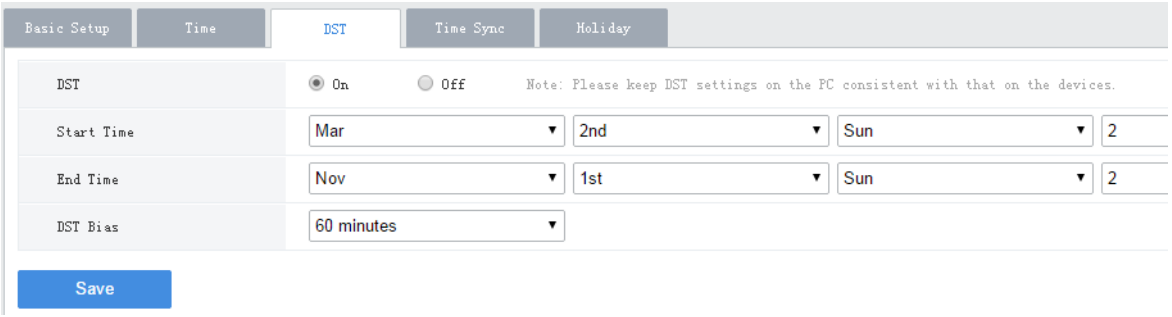


Note:
The PC Web client provides the **Sync with Computer** feature. When this feature is enabled, the system time of the VMS syncs with the PC's system time.

6.1.3 DST

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

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



6.1.4 Time Sync

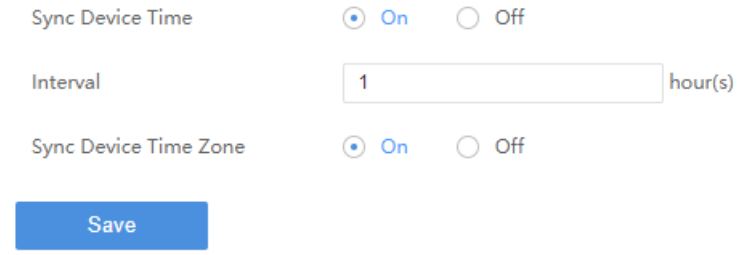
System > **Basic** > **Time Sync**

This function is disabled by default. When **Sync Device Time** and **Sync Device Time Zone** are enabled, the VMS syncs time and time zone to all the directly connected devices under it immediately, including IPC, NVR, encoder and decoder (not including devices connected via an NVR).

1. To enable **Sync Device Time**, select **On** and set an appropriate interval.

2. Enable **Sync Device Time Zone** as needed when **Sync Device Time** is on.

3. Click **Save**. The VMS will sync the PC's time to devices immediately and then repeat this operation at the set interval.

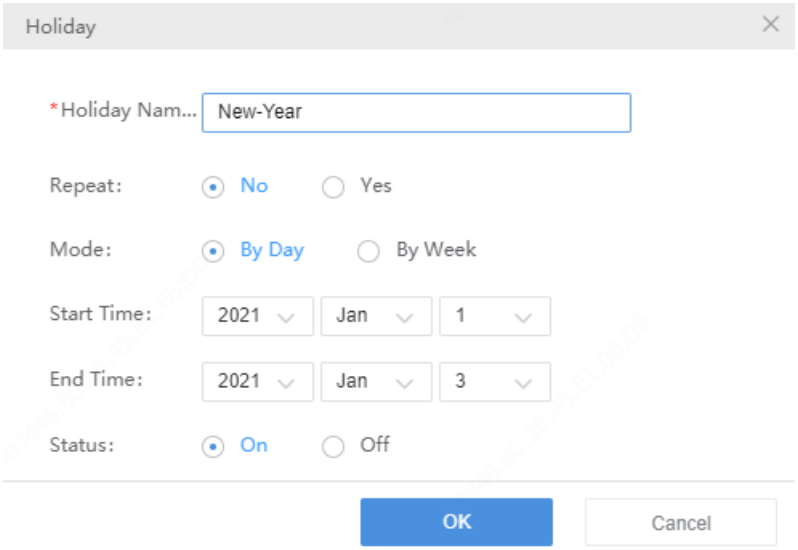


6.1.5 Holiday

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.

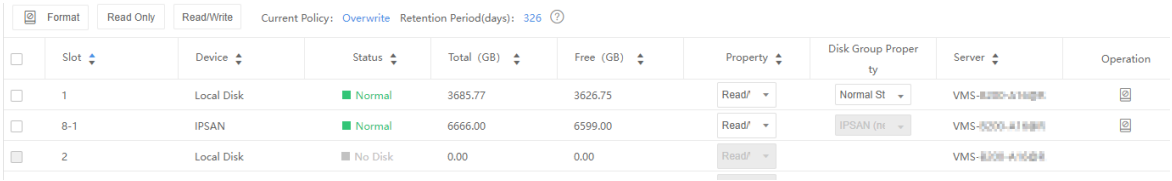
The holiday name must be unique in the system.



6.2 Disk Configuration

6.2.1 Disk Management

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



- View disk info: slot number, device (local disk or network disk), status, and space usage etc.

  Note:
  Images are stored on the disk in slot 1. Please ensure that there is a disk in slot 1 and is in normal status.

- View remaining storage days: When the storage policy is set to **Stop**, the system will calculate the estimated recording days; when the storage policy is set to **Overwrite**, the system will calculate the retention period in days.
- Configure read&write property: Select **Read Only**/**Read/Write** for the disk from the property selectbox, or select disk(s) and click **Read Only**/**Read/Write** above the list.
- Configure disk group property: Select **Normal Storage**/**Backup Storage** for the disk group from the disk group property selectbox.
- Format: Click for the disk, or select disk(s) to be formatted and click **Format** above the list.

  Note:
  - 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.
  - Formatting will erase all recordings stored on the disk.

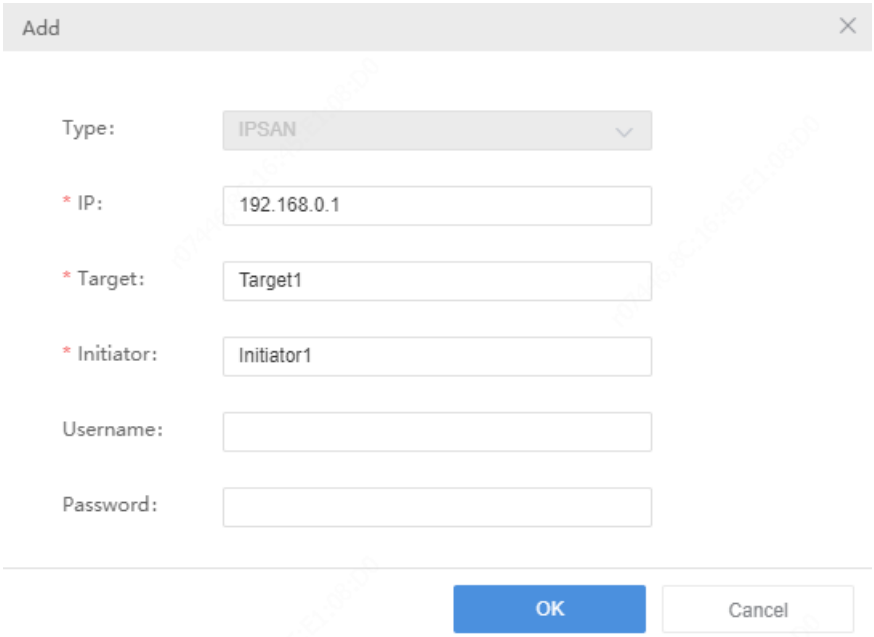
6.2.2 Network Disk

Note: This function is not available to VMS-10A1.

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

1. 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.



- 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.

6.2.3 Allocate Space

Note: This function is not available to VMS-10A1.

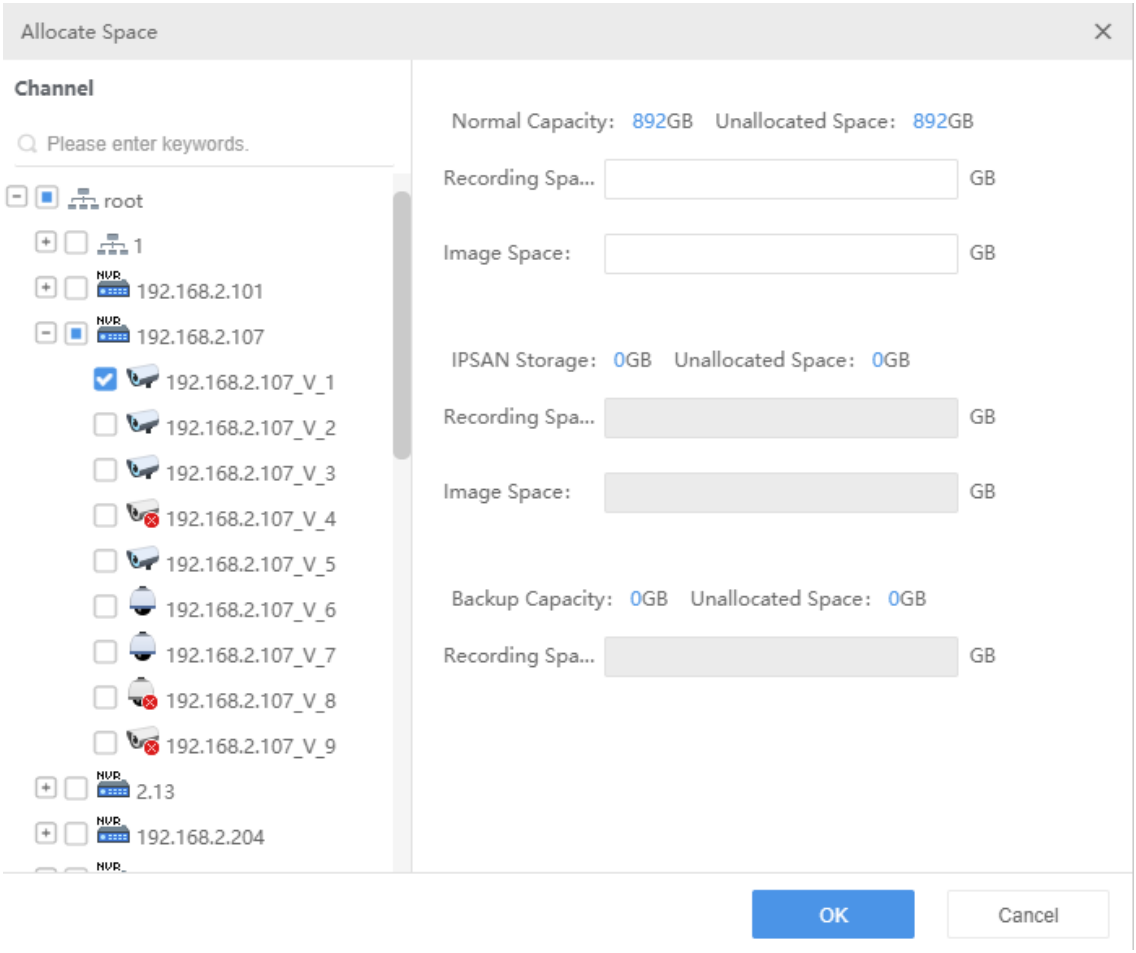
System > **Disk** > **Allocate Space**

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

Note:

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

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



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

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

6.2.4 Disk Group Property

Note: This function is not available to VMS-10A1.

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

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

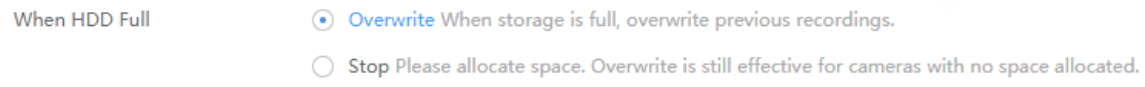
Disk Group No.	Capacity (GB)	Property
1	0	Normal Storage

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

6.2.5 Advanced Configuration

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

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



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

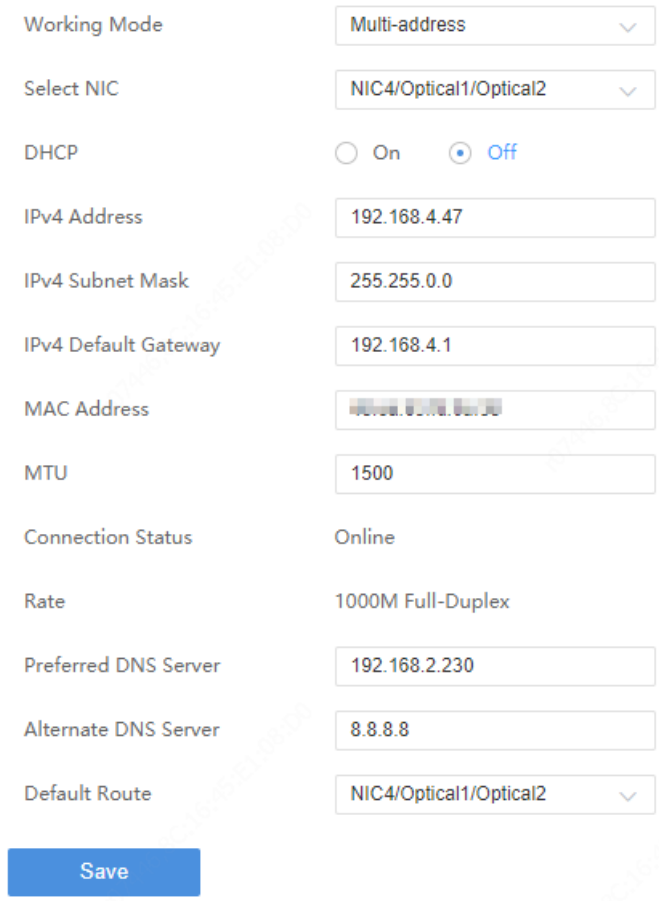
Note:
The **Stop** mode is effective only when space is allocated. That is to say, for a camera that no space is allocated, its recording will still be overwritten even if you have set **When HDD Full** to **Stop**. So allocate space appropriately to avoid undesired video loss.

6.3 Network Configuration

6.3.1 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.



Note:

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

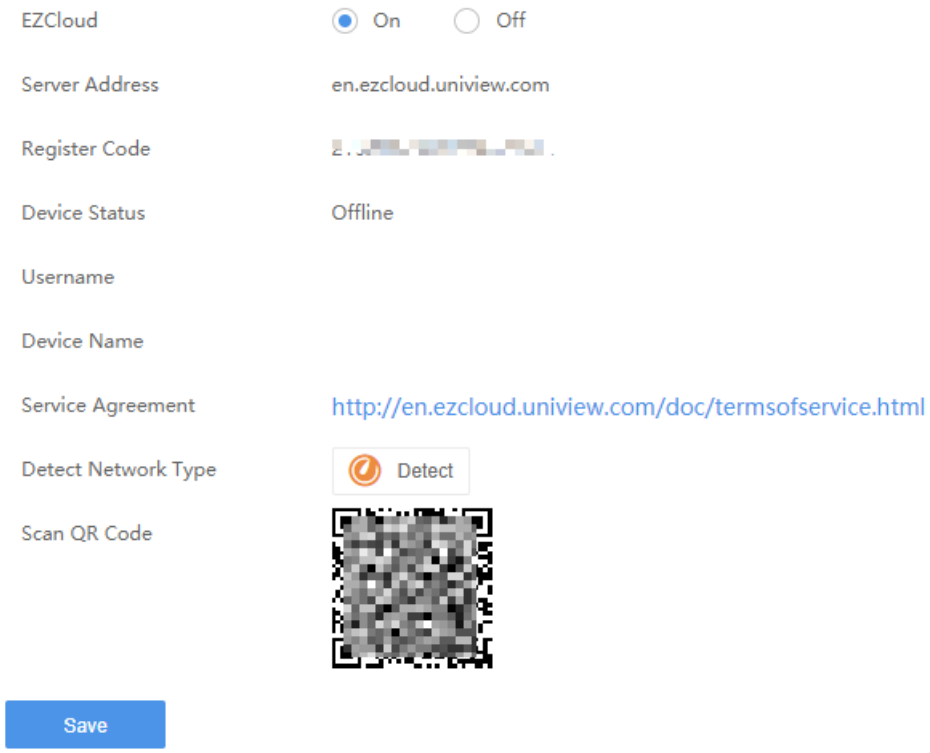
- Working mode
  - Multi-address: Default mode. The Network Interface Cards (NICs) work independently with different IP addresses.
  - Load Balance: NICs that make up a virtual NIC use the same IP and work together to share the network load.

    - Net Fault-tolerance: NICs that make up a virtual NIC use the same IP and work as a backup to each other. If either NIC becomes faulty, the other takes over.
- DHCP: Use a DHCP server to automatically assign an IP address.
- IPv4 Address: VMS' IP address. Users access the system at this address from a Web or software client.
- DNS server: Domain Name Server, which resolves a domain name into an IP address.
- Default Route: Specifies the default NIC that the VMS uses to send data. The default route may be different from the NIC set in the Select NIC drop-down list.

6.3.2 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.



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

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

6.3.3 DDNS

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

DDNS (Dynamic Domain Name Service) associates a changing IP address to a fixed domain name and allows users to access the device by visiting the fixed domain name instead of the changing IP address. DDNS is disabled by default.

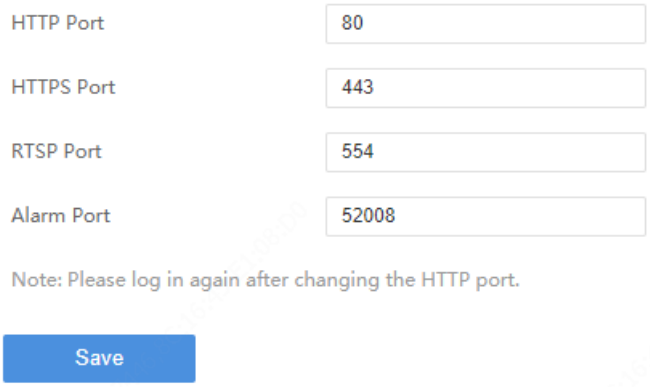
Three DDNS services are available:

- DynDNS: You need to complete registration at the DynDNS official website first. After completing the registration, complete settings on this page, including the server address, port number, and username/password. When the device status is **Online**, you can access the VMS using the domain name.
- No-IP: You need to complete registration at the No-IP official website first. After completing the registration, complete settings on this page, including the server address, port number, and username/password. When the device status is **Online**, you can access the VMS using the domain name.
- EZDDNS:
  - The default server address is 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. 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).

6.3.4 Port

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

Configure HTTP, HTTPS, RTSP and alarm ports.



6.3.5 Port Mapping

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

Use port mapping to configure mapping relations between internal and external ports.

The VMS supports two port mapping modes:

- UPnP:
  - Auto: The VMS automatically negotiates external ports with the router. If an external port is already in use, the VMS will negotiate with the router again with another port number.
  - Manual: Specify external ports manually. If the specified port is already in use, the VMS will not try again with another port, and port mapping will fail.
- Manual: Usually this mode is used when the router does not support UPnP. Complete settings on the router first and then fill in the settings on this page.

Note:

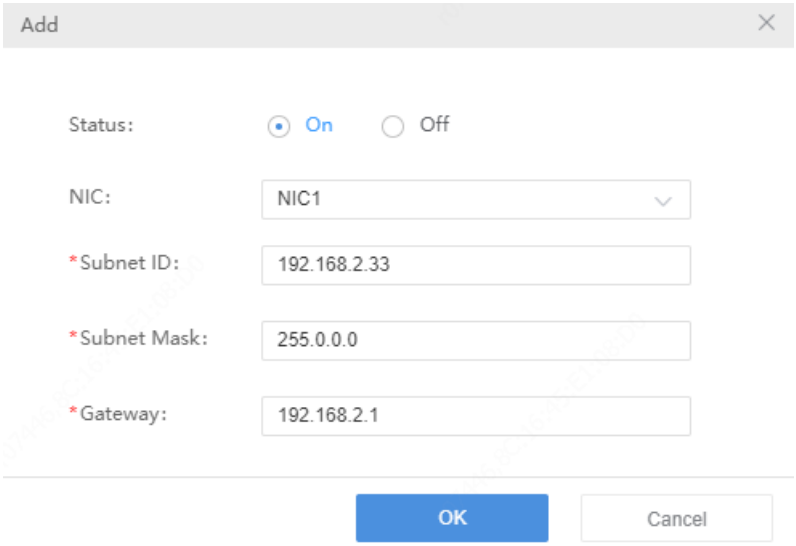
- By default port mapping is disabled.
- Enable UPnP in the router first before you setting UPnP on this page. UPnP requires the router's support.

6.3.6 Custom Route

System > **Security** > **Custom Route**

Add static routes to interconnect the VMS with destination networks. Up to 100 custom routes are allowed.

You need to choose the NIC and set the subnet ID, subnet mask and gateway. A custom route is enabled by default and can be disabled.

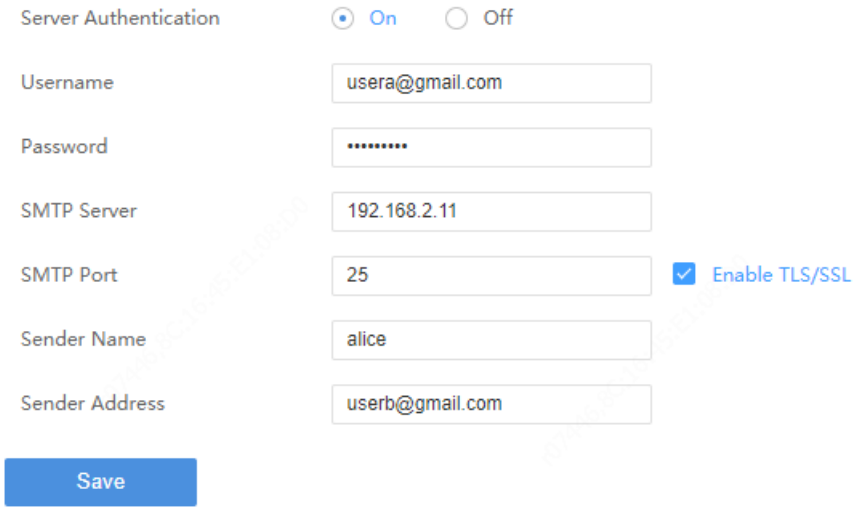


Note:
Changing the NIC's working mode will clear all the existing custom routes.

6.3.7 Email

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

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



Note:

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

6.3.8 AD Domain

System > **Network** > **AD Domain**

Introduction

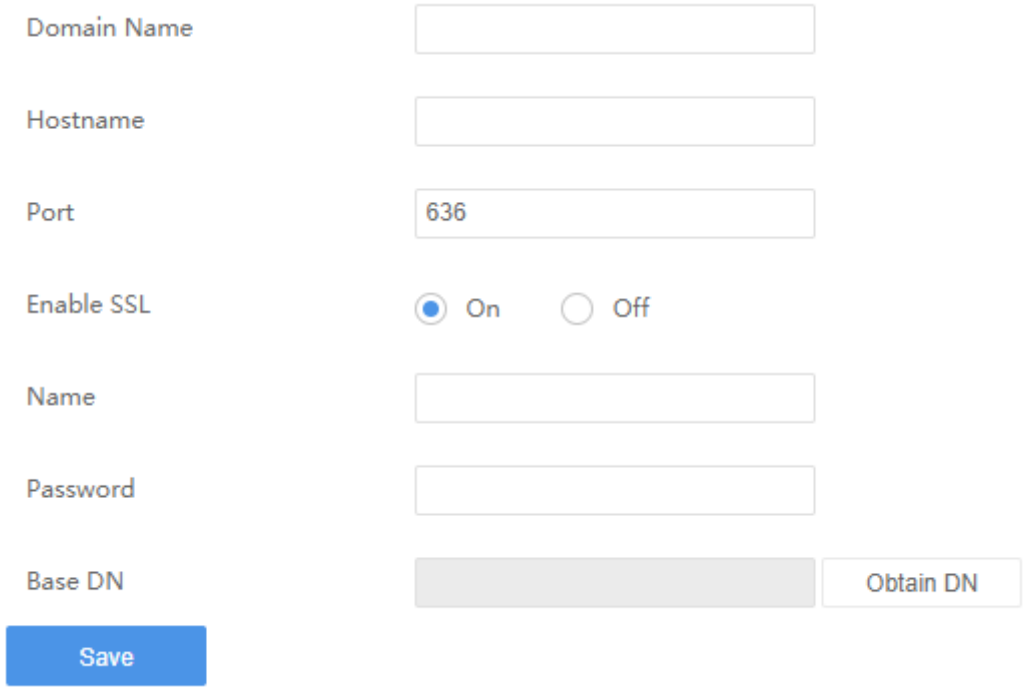
Active Directory Domain (AD Domain) is a Windows server directory that stores information about company computers, user accounts, groups, etc., serving as an organizational unit. It helps define security boundaries and

allows employees to log in using their domain accounts. All domain activities must comply with the company's security policies. With domain manager tools, companies can remotely manage and configure multiple domains for centralized control.

Once connected to an AD domain, administrators can set permissions for employees, allowing them to log in to this system with their AD domain accounts. This reduces the need for multiple usernames and passwords, ensuring secure and efficient login management.

Configuration Instructions

Connect the system to AD domain and realize unified management and permission control.



Item	Description
Domain Name	The AD domain name, obtained from the AD domain side.
Hostname	The IP address or the hostname of the AD domain server.
Port/Enable SSL	When SSL is enabled, data is encrypted using the SSL protocol for more secure transmission. The default port numbers differ when SSL is enabled or disabled. It is recommended to use the default port numbers.
Name/Password	The username and password of the AD domain administrator. **Note:** The user can interact with the domain using this credential. Do not change the user's password in the AD domain, as it may lead to authentication errors during domain user imports.
Base DN	Click **Obtain DN** to get the root directory name of the AD domain, which is used to search for the domain user list. After obtaining the correct base DN, click **Save**.

Subsequent Operations

Go to **Basic** > **User** > **User**, import domain users. Then, they can log in to this system using their domain username.

Note:
When domain users log into this system, the username format on the Login page is **Domain Name\Username**.

6.4 Protocols & Interconnection

6.4.1 VSS Server

VSS Server

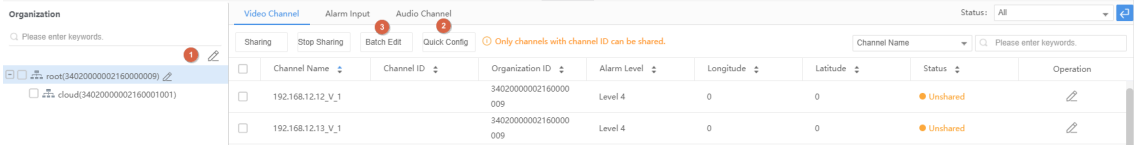
System > **Network** > **Protocols & Interconnection** > **VSS Server**

Configure VSS server parameters to connect the VMS to a higher-level management platform. When the configuration is complete, you can manage the VMS on the platform and live view, play back, and subscribe alarms from channels under the VMS.

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

- Complete basic settings

  - SIP Server ID: ID of the platform server (obtained from the server).
  - SIP Server IP: IP address of the platform server (obtained from the server).
  - Organization: The drop-down list shows the General organization and all the custom organizations that you have created. You need to click **Save** after choosing a different organization from the list. The organization tree in the lower left corner shows the organization that you have chosen.
  - SIP Server Domain: Domain ID of the platform server.
  - SIP Server Port: Port assigned on the platform server.
  - Heartbeat Cycle: Keepalive cycle between the VMS and the platform.
  - Max Heartbeat Timeout Counts: Max number of times that communication between the VMS and the platform times out. Communication stops automatically when it reaches the max count.
- Share channels with a higher-level management platform
  When channels are shared successfully with the higher-level management platform, operators can search these channels on the platform and subscribe to alarms of these channels. When sharing is stopped, the channels will be deleted from the higher-level management platform.



  1. Select the desired organization from the **Organization** drop-down list and then click **Save**. The organization appears on the organization tree.
  2. Select the desired channel type to share: video channel, alarm input channel or audio channel.
  3. Edit organization IDs on the organization tree. You can select multiple organizations and click **Batch Edit** (see 1 in the figure) to edit in batches.
  4. Choose one way to configure channel ID.
     - Click in the **Operation** column for the target channel, and then enter the channel ID.
     - Select the desired channels, click **Quick Config** (see 2 in the figure) to assign channel IDs to channels without channel IDs. Set the basic code, and then the system will create and assign channel IDs based on the basic code. This feature is not effective to channels that already have channel ID.
  5. You can select channels and click **Batch Edit** (see 3 in the figure) to edit channel IDs in batches.

Note:

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

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

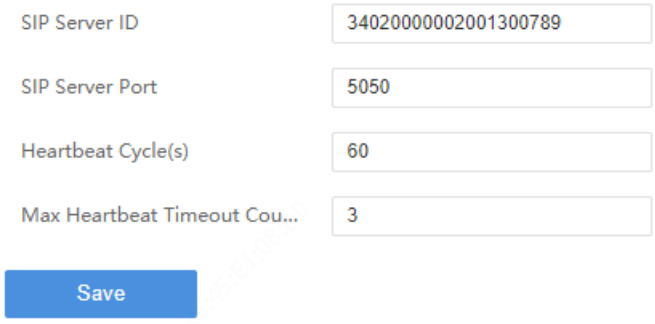
Note:
An audio channel cannot be shared or unshared like a video channel. An audio channel's status (Shared or Unshared) is consistent with that of the corresponding video channel. That is to say, sharing (or stop sharing) a video channel also shares (or stops sharing) the corresponding audio channel.

VSS Local

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

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

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



6.4.2 Video&Image Database

System > **Network** > **Protocols & Interconnection** > **VIID**

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

Video&Image Database Configuration

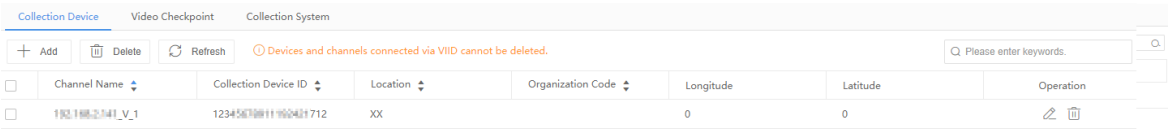
- Device: The device is displayed as "Online" when the VMS is successfully connected to the Video&Image Database server.
- Server Address: IP address of the Video&Image Database server.
- Server Port: Port number of the Video&Image Database server.
- Username/password: The username and password used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

Video&Image Database Configuration

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

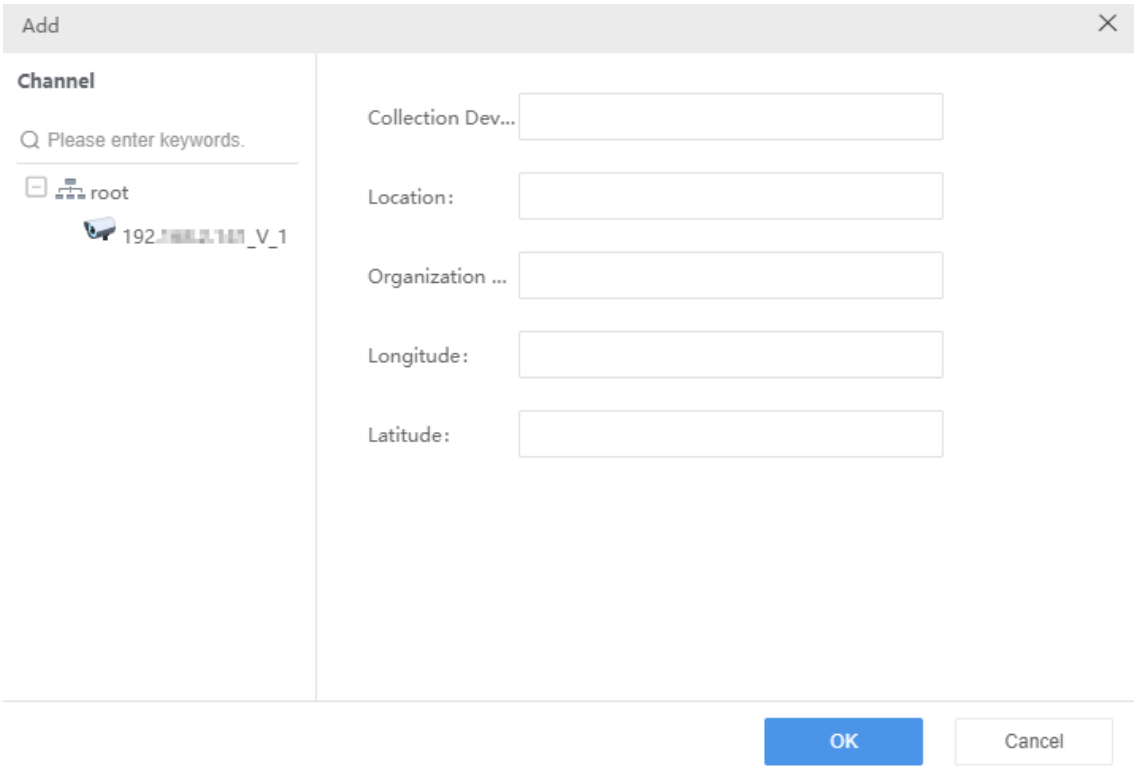
Add collection device/video checkpoint/collection system to the VMS.

You can search the added channels on the upper management platform and perform operations such as alarm subscription.



Taking collection device as an example, video checkpoint/collection system are added in a similar way.

1. Click **Add**.



Note:

- For collection device and video checkpoint, only smart devices, access control devices and channels under smart NVR connected via private protocol are displayed in the **Add** page.
- For collection system, only smart NVRs connected via private protocol are displayed in the **Add** page.

2. Set device ID, location and organization code according to the requirement.
   - Device ID: The configured device ID is used to distinguish the device on the platfrom.
   - Location: The place of the target device, for example, XX community.
   - Organization code: Enter 12 characters to distinguish the device's location.

- Longitude/latitude: Enter the longitude and latitude of the device's installation location.

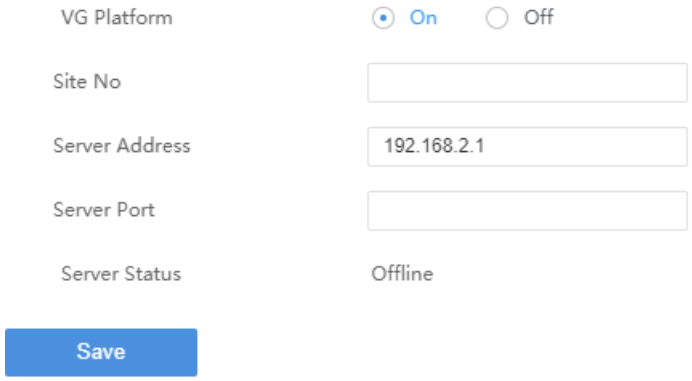
3. Click **OK**.

Note:
Please configure the collection system ID of the smart NVR before configuring its channels.

6.4.3 VG Platform

VG platform is disabled by default and needs to enabled if you want to perform Video Guard authentication.

Complete the settings correctly and then click **Save**. Connection succeeds when the server status changes to **Online**.



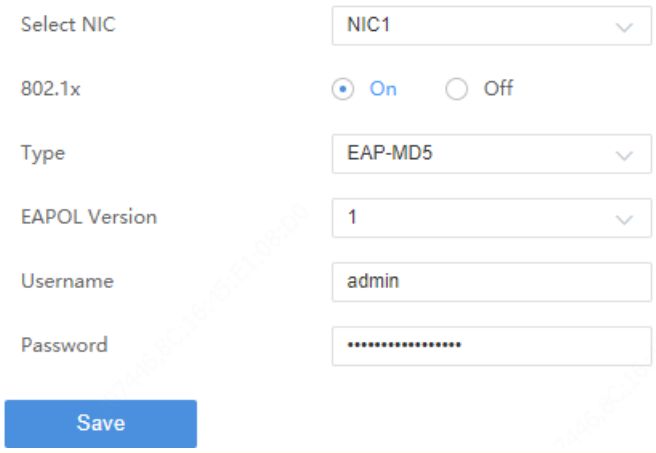
6.5 Security Configuration

6.5.1 802.1x

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

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

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



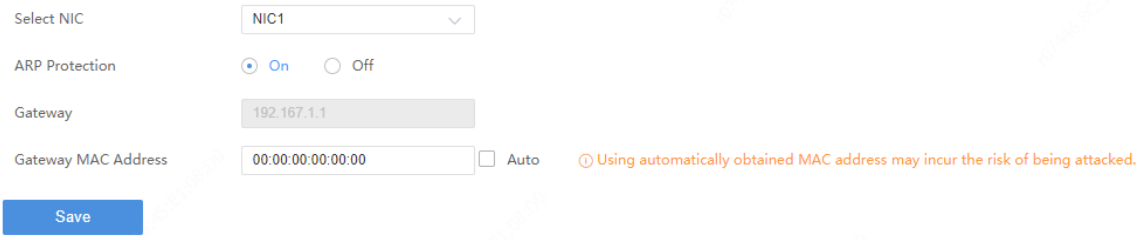
Note:
802.1x must also be properly configured on the authenticator (such as Ethernet switch).

6.5.2 ARP Protection

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

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

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



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

6.5.3 HTTPS

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

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

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

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

Note:

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

6.5.4 SSH

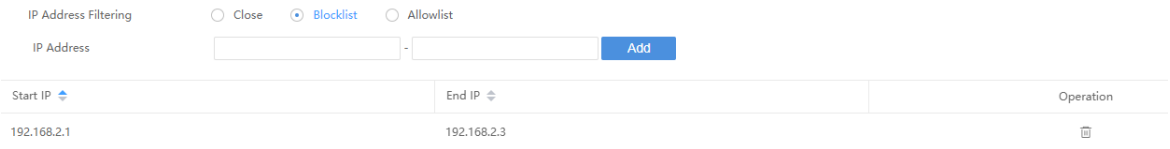
System > Security > SSH

Enable or disable SSH (Secure Shell).

6.5.5 IP Address Filtering

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

Use blocklist/allowlist to forbid or allow login from certain IP addresses only.



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

Note:

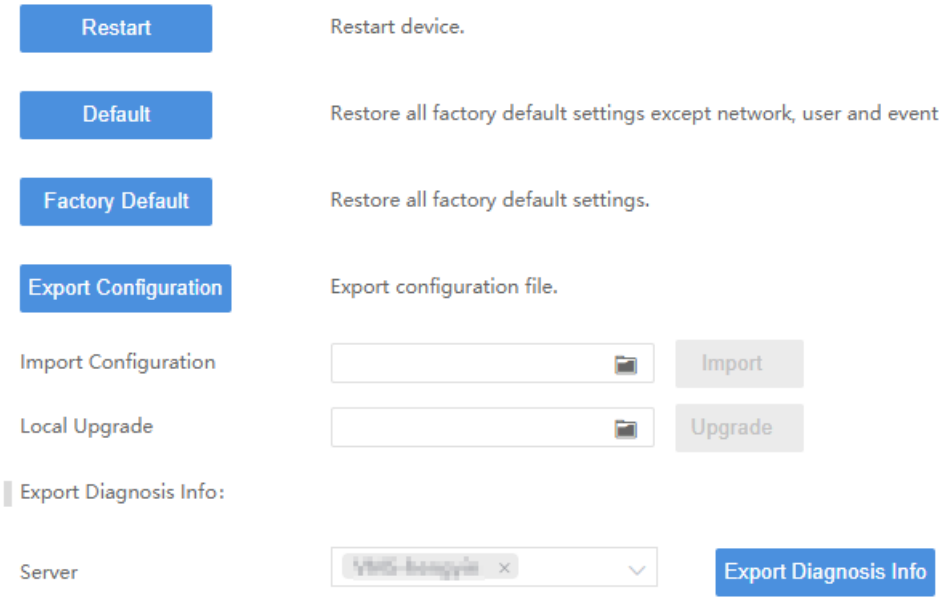
- Blocklist and Allowlist cannot be enabled at the same time.
- Blocklist/allowlist is effective to IP-based logins.
- You can click a field in the list to edit an IP address.

6.6 Maintenance

6.6.1 System Maintenance

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

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



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

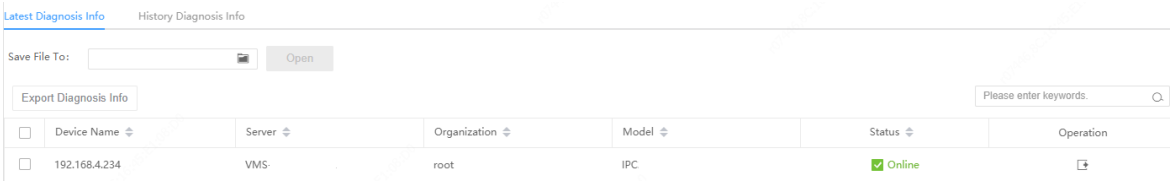
Note:
The PC Web client provides the **Plug-in Log Path** feature. You may click **Open** to view plugin logs, or click the folder icon to customize the path. The text box and the button are grayed out if no plugin is installed or if your Web browser does not support a plugin.

6.6.2 Device Diagnosis Info

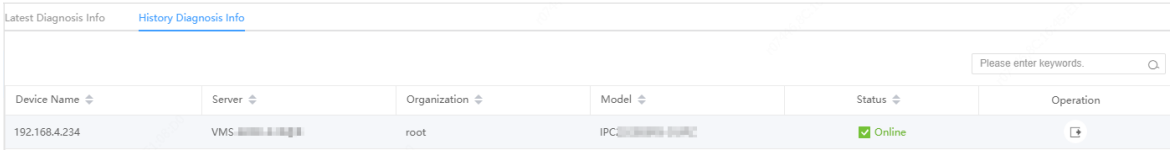
System > **Maintenance** > **Device Diagnosis Info**

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

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



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



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

6.6.3 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.

6.6.4 Packet Capture

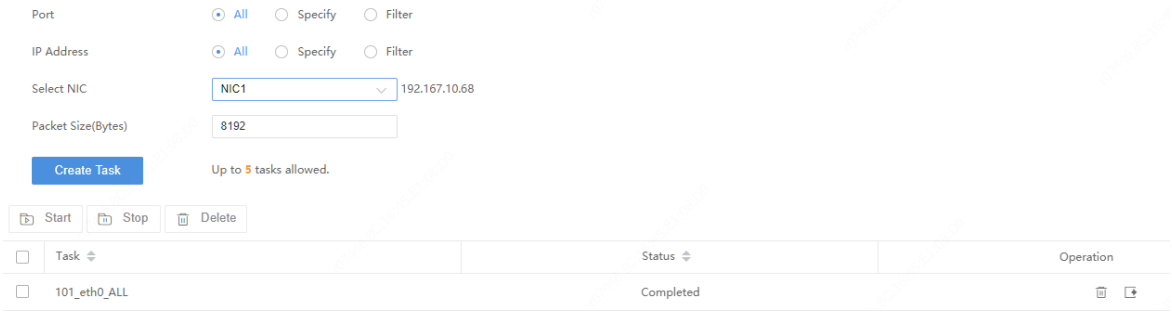
System > **Maintenance** > **Packet Capture**

Capture packets for troubleshooting or analysis.

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

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

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

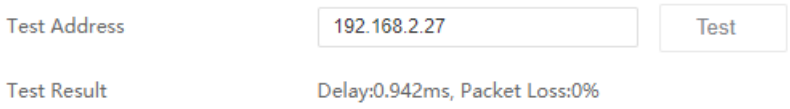


Note:
A file is generated for each packet capture task with a max size limit (around 19.1M). When the file size reaches the limit, the packet capture task stops automatically (note: the status does not change and it is still displayed as **Ongoing** when the task stops in this way).

6.6.5 Network Detect

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

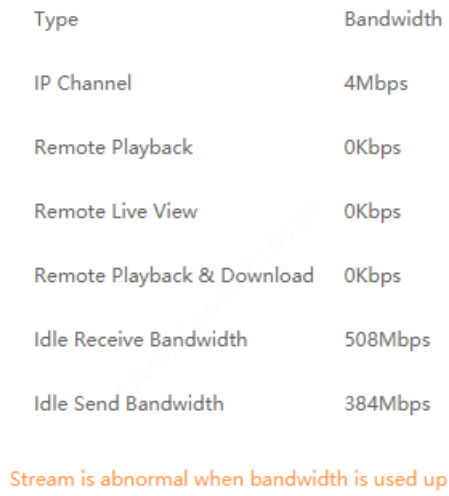
Enter a domain name or an IP address and then click **Test**. The test result will indicate whether the network is connected, and the connection status (including delay and packet loss rate) if connected.



6.6.6 Network Statistics

System > **Maintenance** > **Network Statistics**

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.



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).

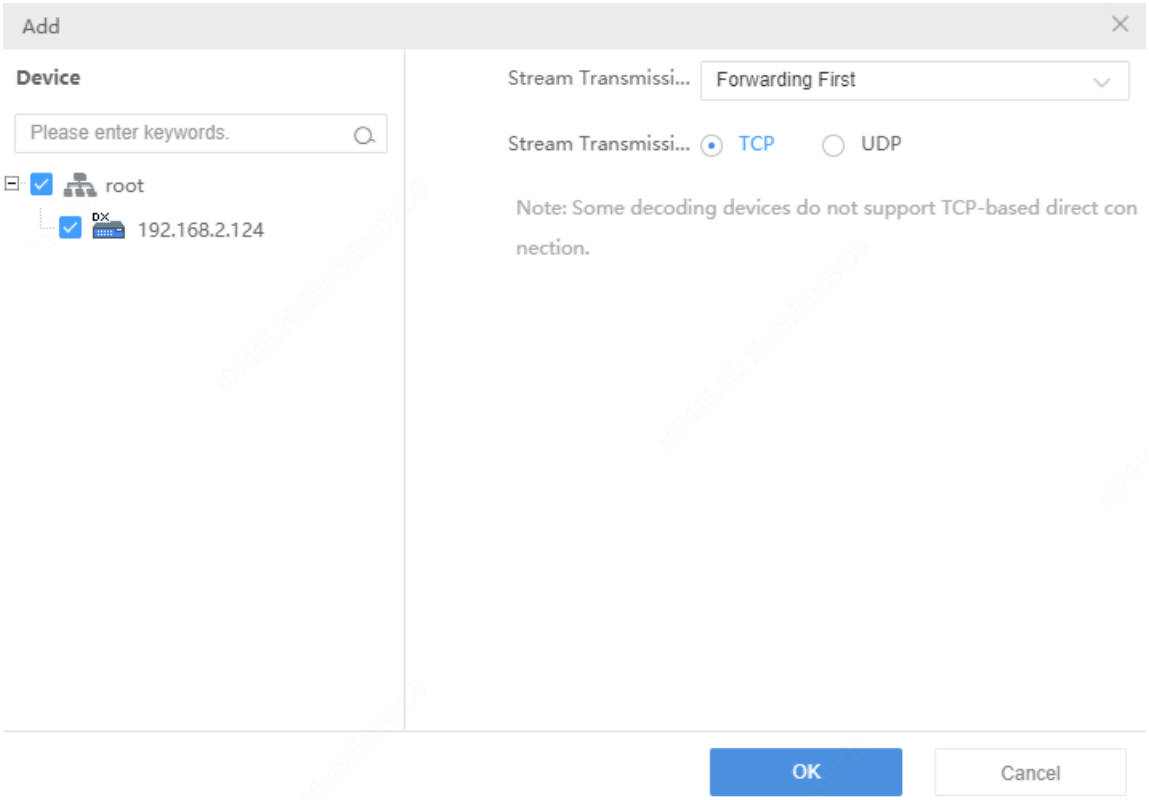
6.6.7 Stream Transmission Policy

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, avoiding bandwidth consumption of the VMS. If conditions are not satisfied for direct transmission, streams will be transmitted via the VMS.

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

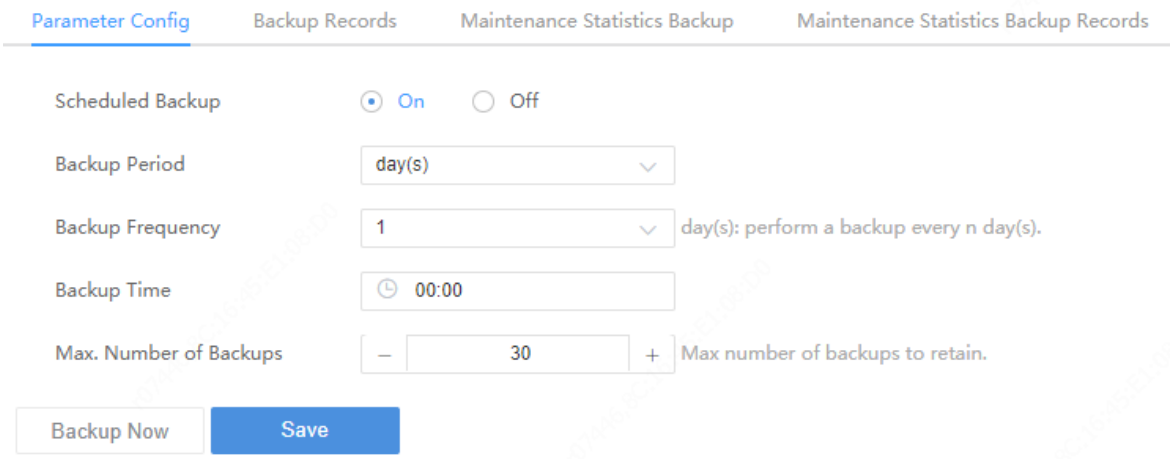


Note:
Some decoders do not support TCP-based direct connection. The settings are not effective even though you have set so on the page.

6.6.8 Data Backup

System > Maintenance > Data Backup

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



Configure scheduled backup

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

- Scheduled Backup: Select **On** to enable this function.
- Backup Period: Choose to back up by day, week or month.
  - By day: Set backup frequency, that is to perform a backup every *n* days.
  - By week: Choose the days of a week on which a backup will be performed.
  - By month: Choose the days of a month on which a backup will be performed.

- Backup Time: Set the time to perform a backup.
- Max. Number of Backups: Set the maximum number of backup files. Up to 30 backups are allowed. When the number of backups reaches the maximum number, new backups will overwrite old backups.

Backup manually

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

View backup records

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

Use a backup to restore configurations

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

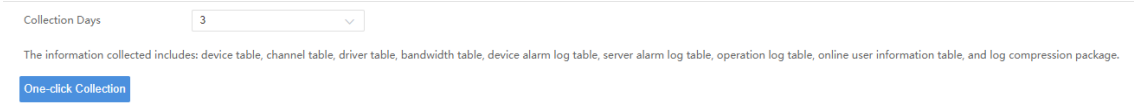
Back up maintenance statistics

Create tasks to automatically back up maintenance statistics.

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

6.6.9 One-click Collection

1. Select the number of days to collect.
2. Click **One-click Collection** to collect the related information.



6.7 Map Configuration

System > Map Config

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

Note:
Only image map is available on the local client.

7 Statistics

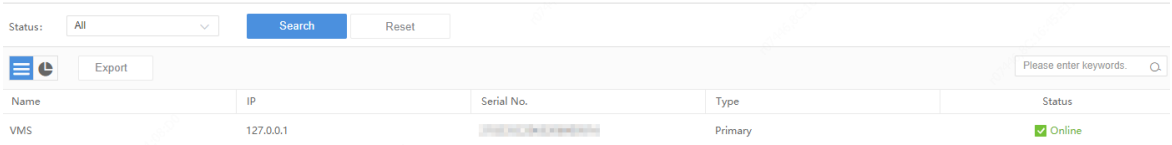
View server statistics, device statistics, and logs. Server statistics include server status, online status, and network parameters.

7.1 Server Statistics

7.1.1 Server Status

Statistics > Server > Server Status

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



7.1.2 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:

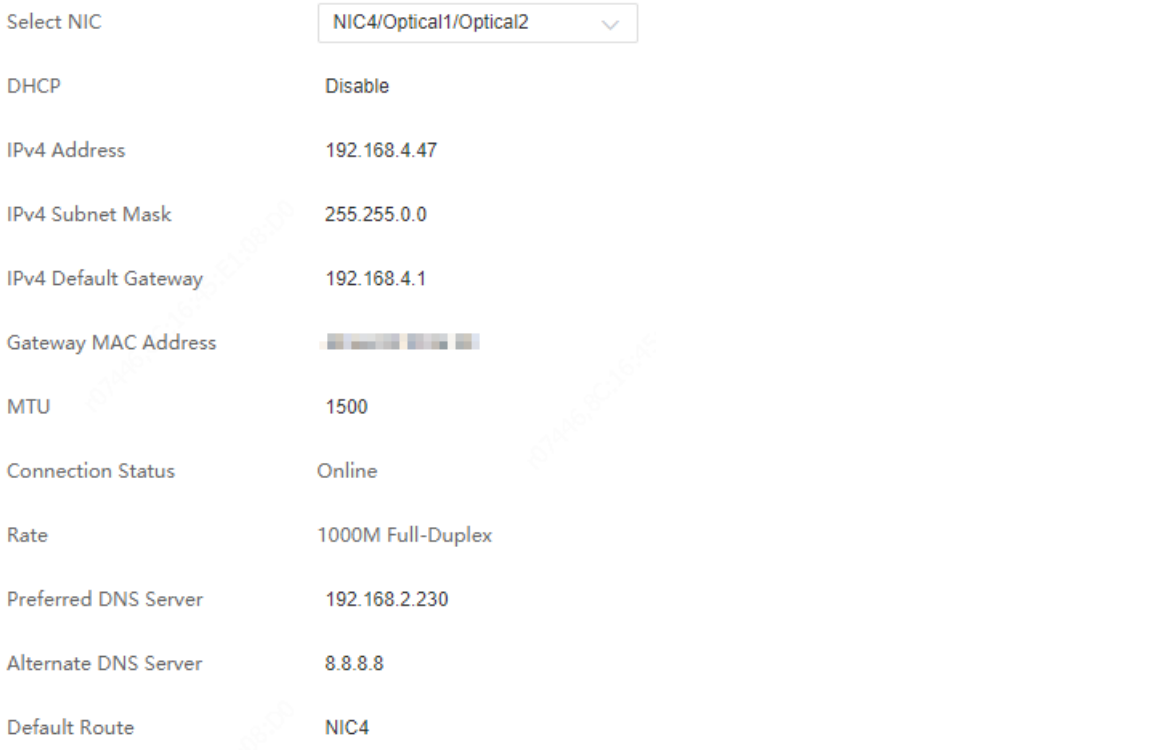
- Short: A short test checks less items than an extended test and it takes less time.
- Extended: An extended test checks more thoroughly than a short test and it takes longer time.
- Conveyance: A conveyance test mainly checks for data transmission problems.

Note:
It is recommended to replace the disk if **Overall Evaluation** is not **Healthy**.

7.1.3 Network

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

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

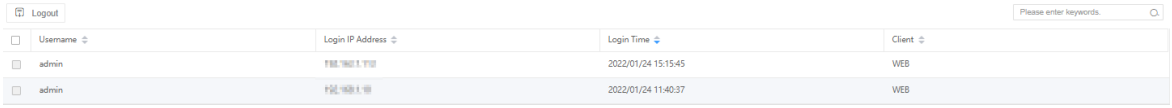


7.1.4 Online User

Statistics > Server > Online User

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

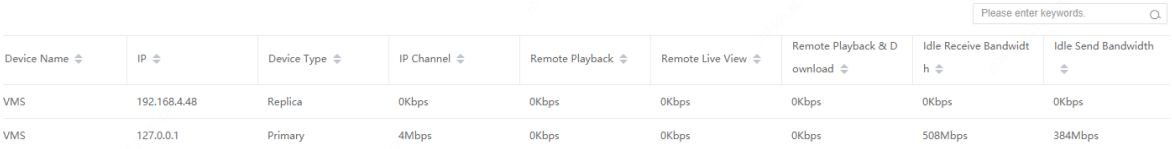
Admin can force other users to log out by selecting the target user(s) and clicking **Logout**. The target user(s) are logged out.



7.1.5 Bandwidth

Statistics > Server > Bandwidth

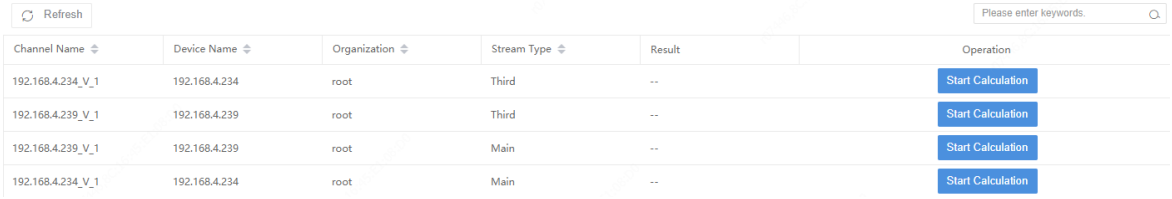
View the current bandwidth usage of the VMS. See Network Statistics.



7.1.6 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.



7.1.7 Server Performance

Statistics > Server > Server Performance

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

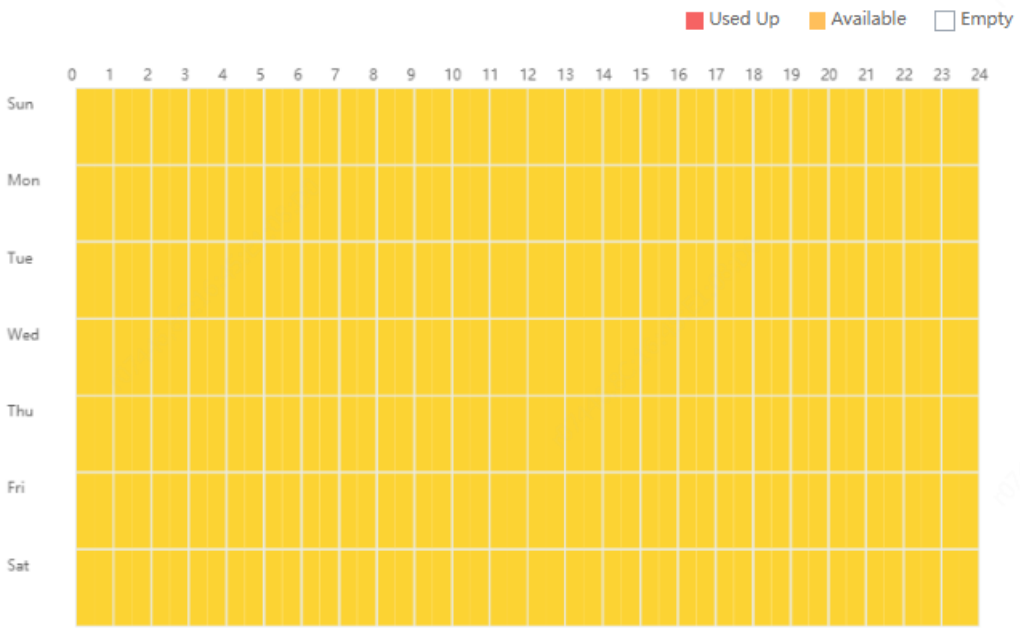
The Web client starts calculation when you open the page and displays statistics of the recent 240 seconds. Place the mouse pointer anywhere on the chart (see 1 in the figure below) to view details at the specific point. If more than one NIC is in use, statistics of the NICs are shown in different colors.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

7.1.8 Storage Capacity

Note: This function is not available to VMS-10A1.

Statistics > Server > Storage Capacity

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



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

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

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

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

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

7.1.9 Recording Status

Note: This function is not available to VMS-10A1.

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.

7.2 Device Statistics

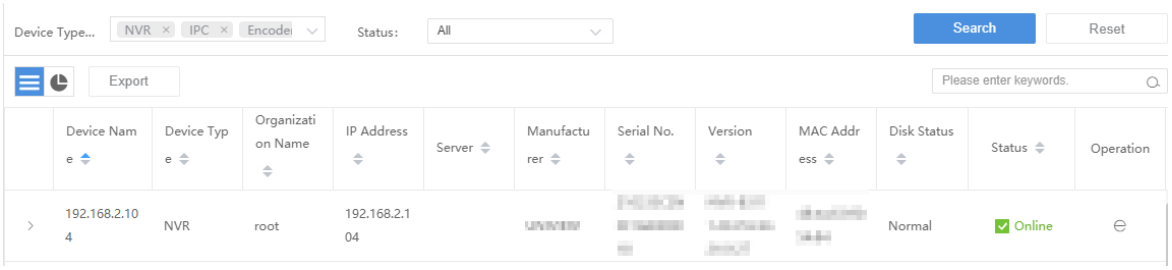
Device Status

Statistics > **Device** > **Device**

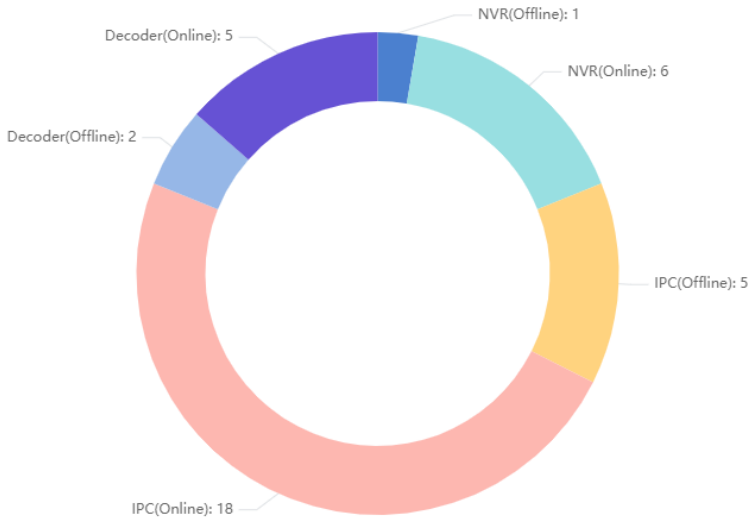
Choose the organization on the left-side organization tree. Search device statistics by device type or device status.

Click › on the left side of the device list to view the online/offline status of channels under a device.

Export search results 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.



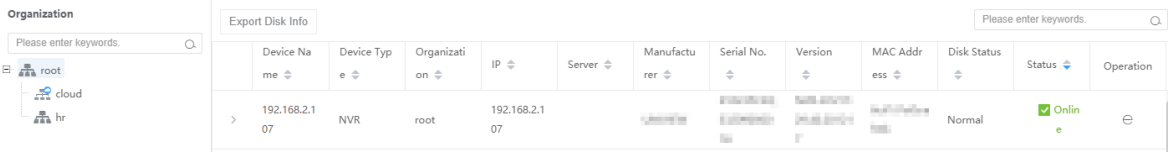
Device Disk Status

Statistics > **Device** > **Device Disk Status**

Choose the organization on the left-side organization tree. You can search a device by entering the device name in the top right corner.

Click › on the left side of the device list to view the online/offline status of a hard disk.

Click **Export Disk Info** to export information about online disks on the current page to a CSV file.



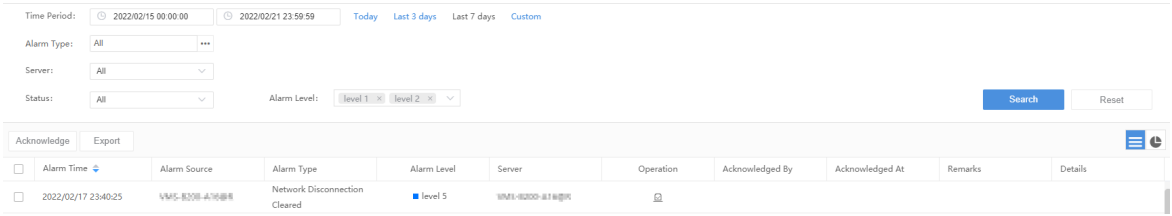
7.3 Logs

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

7.3.1 Server Alarm Logs

Statistics > Log > Server Alarm Logs

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

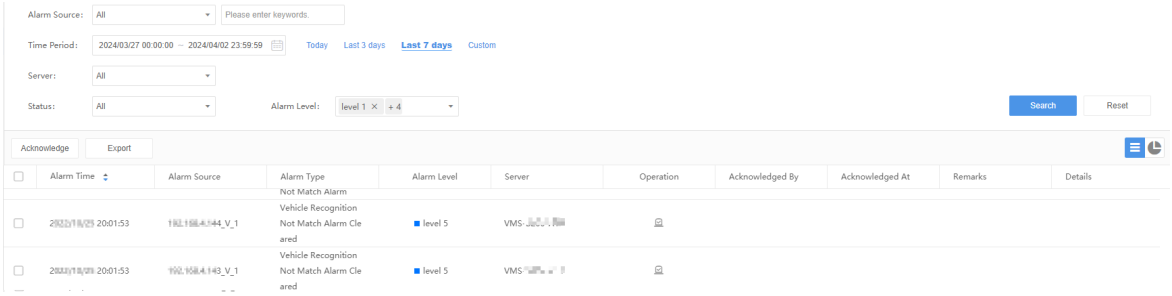


Note:
The acknowledge operation is irreversible. The Acknowledged status cannot be revoked.

7.3.2 Device Alarm Logs

Statistics > Log > Device Alarm Logs

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



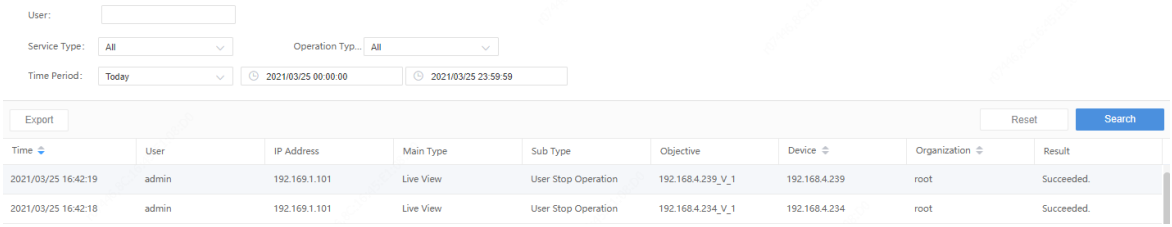
Note:

- For **Alarm Source**, when selecting **All**, you can search for alarm sources by keywords (supports fuzzy matching); when selecting a specific type, you can specify the alarm source and select the alarm type.
- The acknowledge operation is irreversible. The acknowledged status cannot be revoked.

7.3.3 Operation Logs

Statistics > Log > Operation Logs

Search and export user operation logs.



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).

8 Access Control

Manage access control devices, assign access permissions, and cards.

Use this function to achieve access control and personnel management by configuring door groups, time templates, and binding cards for persons to assign access permissions.

8.1 Permissions

Access Control > Permissions

Manage time templates, door groups and access permissions.

8.1.1 Time Template

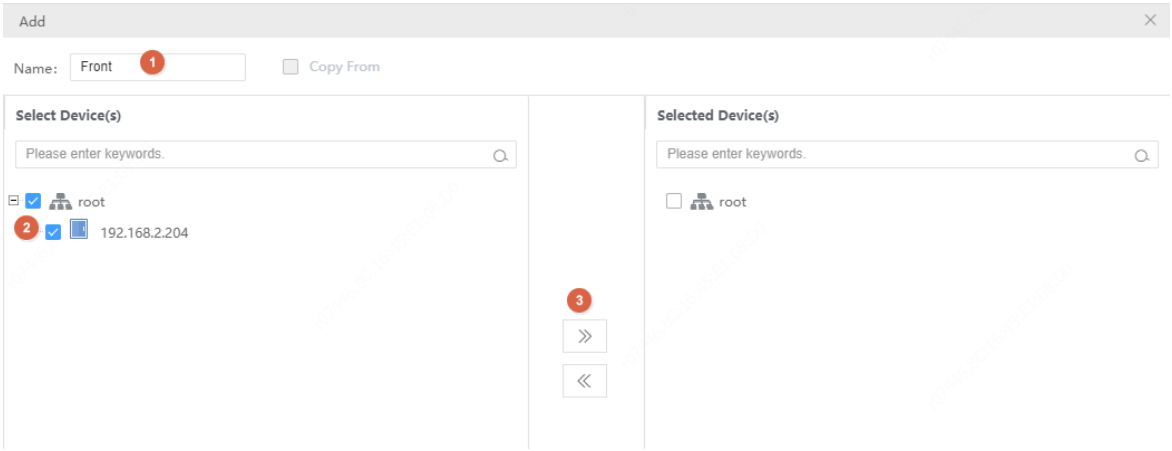
Use a time template to restrict access time. You will need to choose a time template when configuring access permissions.

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

See User Time Template in User Management. The configuration steps are similar.

8.1.2 Door Group

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

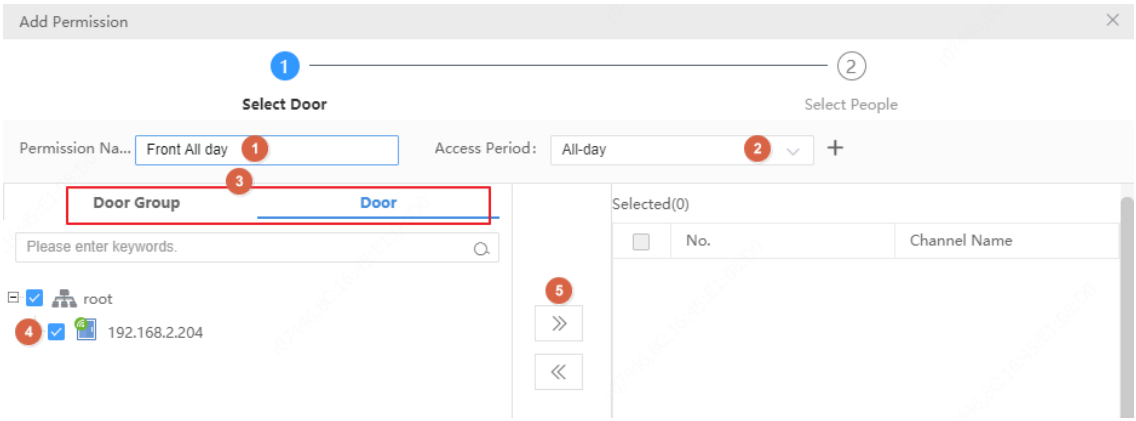


Note:
You can select **Copy From** and copy settings from an existing door group.

8.1.3 Assign Access Permission

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

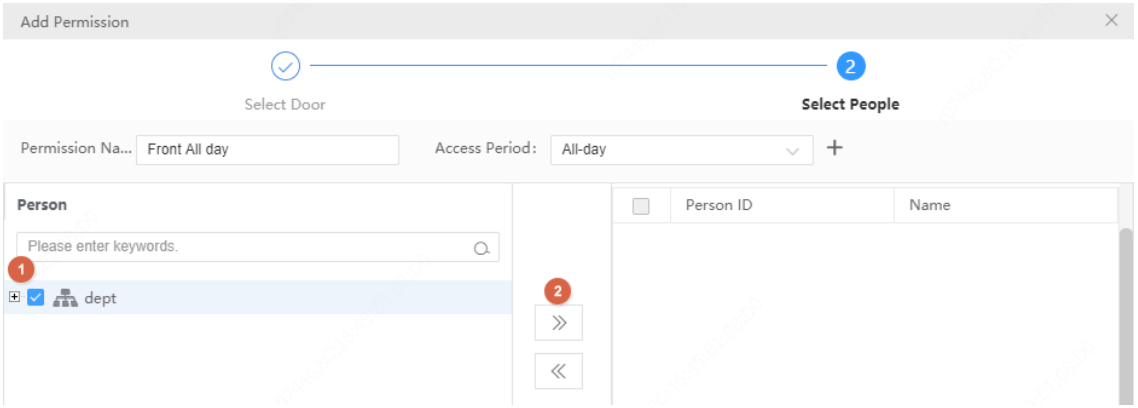
1. Select doors.



Note:

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

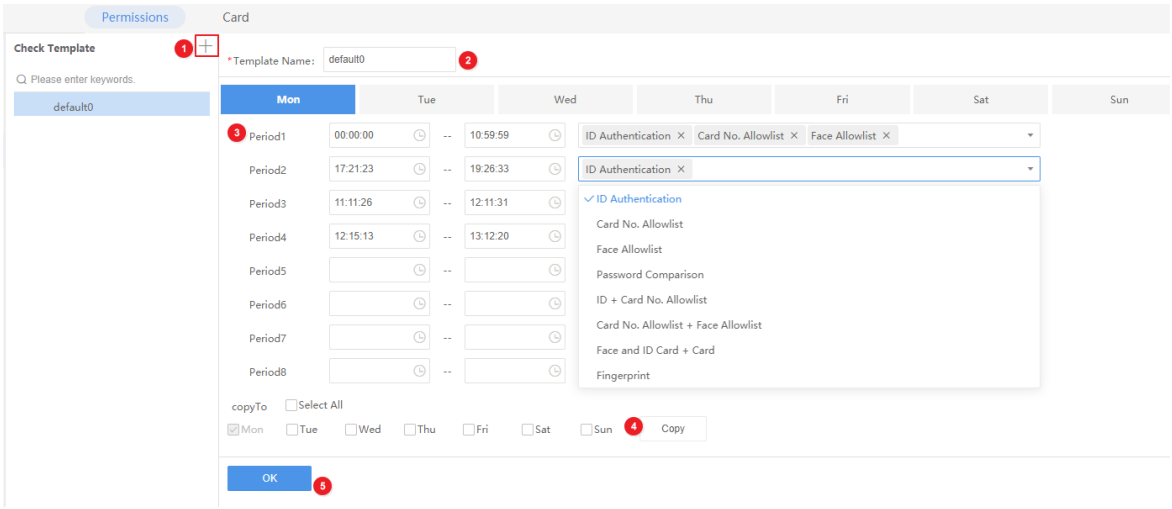
2. Select person(s) to assign permissions to.



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

8.1.4 Check Template

The check template (verification template) is used to set different access control verification methods for different time periods. You can directly associate the check template with the door channel when configuring the channel.



1. Click **+** to add a new check template, or select an existing check template on the left and edit based on it.
2. Set the template name.
3. Set the verification time period(s) and verification method(s) for each day.
4. After completing settings for a day, you can select other days and click **Copy** to copy the settings to those days.
5. Click **OK**.

8.2 Card Management

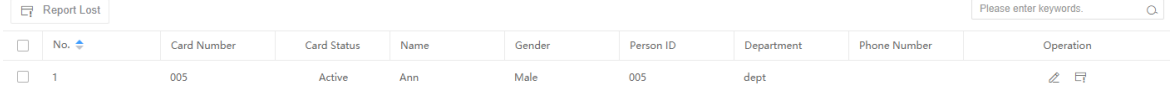
Access Control>Card

View cards of different status, report lost cards and activate suspended cards.

Active card

Access Control>Card>Active

Active cards are cards that are usable. You can change the valid period of an active card or report lost.

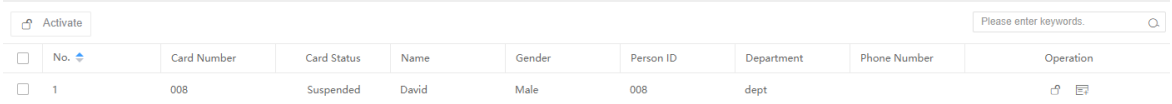


Suspended card

Access Control>Card>Suspended

Cards are suspended when they are reported lost. Suspended cards are unusable until being activated.

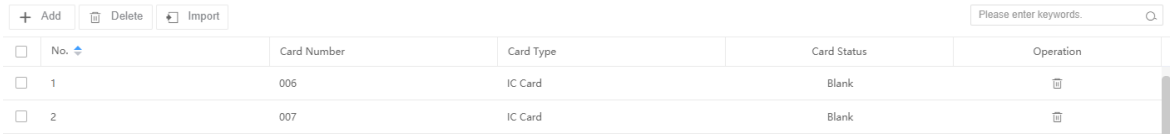
A suspended card can also be replaced by another card. A suspended card is cancelled when it is replaced.



Blank card

Access Control>Card>Blank

Blank cards are cards that are not assigned. Click **Add** or **Import** to add blank cards.



Cancelled card

Access Control>Card>Cancelled

A suspended card is cancelled when it is replaced by another card. Cancelled cards are unusable.

9 Appendix

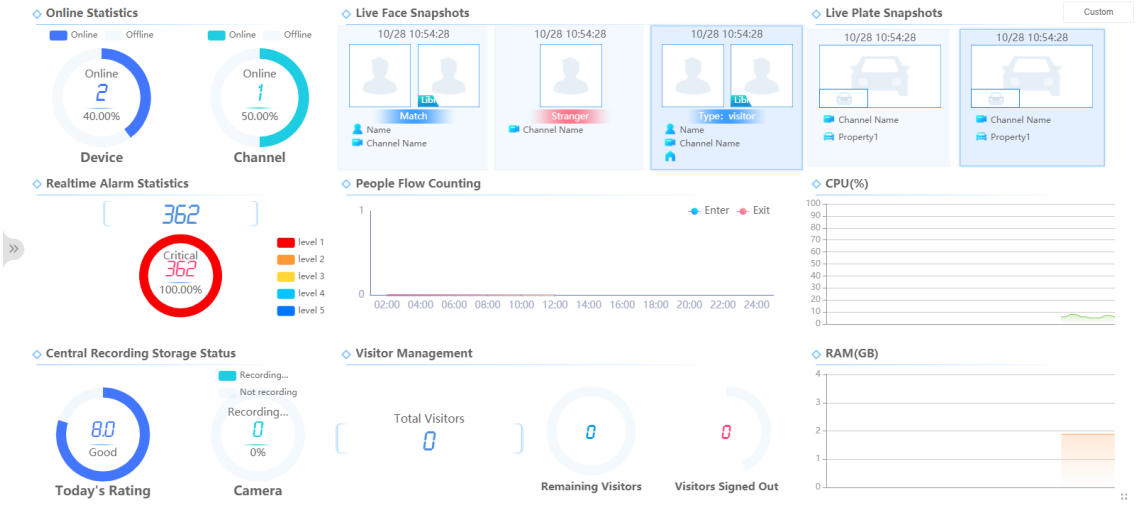
9.1 Customize Comprehensive Management Dashboard

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

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

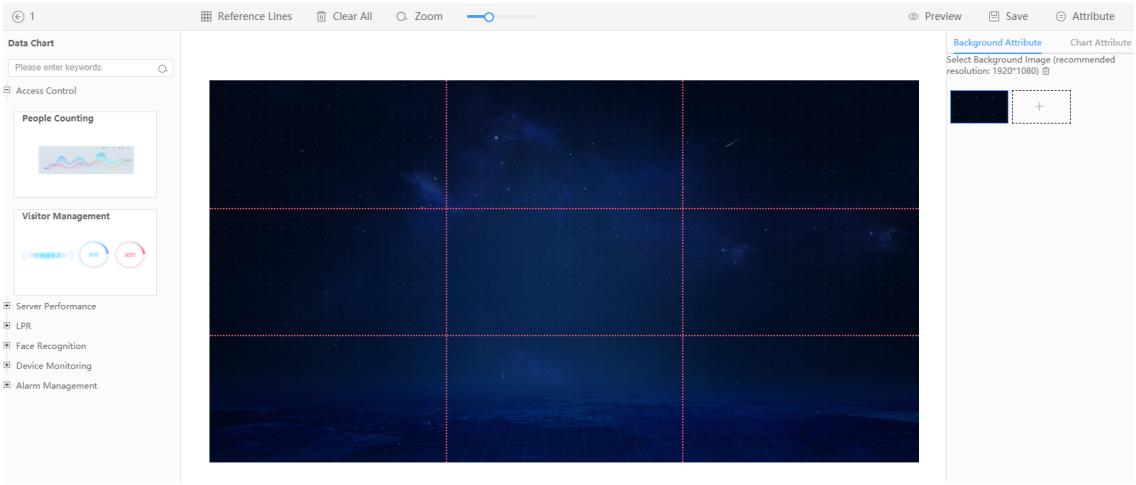
1. Click the expand button ( ) on the right side on the home page.

2. Click the **Custom** button in the top right corner.



3. Click  and then set the template name.

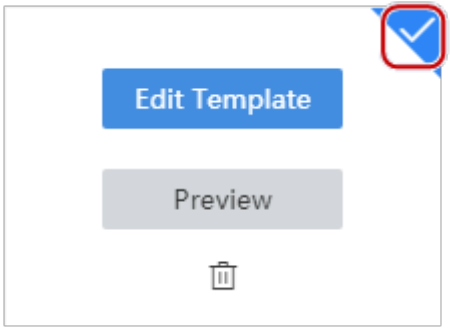
4. In the **Data Chart** area on the left, click to expand the nodes and find the data modules you want to display, and then drag the data modules to the desired positions on the panel, for example, **Online Statistics**, **Central Recording Storage Status**, and **Realtime Alarm Statistics**.



Some buttons are described as follows:

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

5. When you complete the settings, click **Save**.
6. To enable the template, move the mouse cursor onto the template and then click in the top right corner (blue background means that the template is enabled).



9.1.1 Data Chart

Access control

- People counting: Count people coming and leaving in the current day. Hover your mouse over a line to view the corresponding data. The line chart refreshes every two hours.
- Visitor statistics: Count the total number of visitors and the currently present in the day.

Server performance

- RAM usage: View the server's RAM usage. Statistics start to display when the dashboard opens, and statistics of up to the latest 180 seconds are displayed. Hover your mouse over the chart to view statistics.
- CPU usage: Refer to descriptions of RAM usage.

License plate recognition (LPR)

View the captured license plates with relevant information including the capture time, captured image, and channel name.

Face recognition

View face comparison information, including time, degree of match, face library image, captured image, name, and channel name.

Device monitoring

- Online/offline status: View information about online/offline devices and channels. Hover your mouse over the pie chart to view the percentage and quantity. Click the device chart to view detailed device information at **Statistics** > **Device** > **Device Status**. Click the channel chart to view detailed channel information at **Device** > **Channel** > **Encoding Channel**.
- Central recording storage status: View channels' video recording status such as recording, not recording. Hover your mouse over a slice to view the percentage. Click the camera chart to view detailed recording information at **Statistics** > **Server** > **Recording**. The pie chart refreshes every 30 minutes.

Alarm management

Different colors indicate different levels of alarms and the quantities. Hover your mouse over the pie chart to view the quantity and percentage. Click the pie chart to view detailed alarm information at **Statistics** > **Log** > **Device Alarm Logs**. The pie chart refreshes every minute.