X-VMS Web Client

User Manual

Legal Information

User Manual

About this Manual

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.
Please use this user manual under the guidance of professionals.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL OUR COMPANY, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. OUR COMPANY SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, OUR COMPANY WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.
IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
⚠ **Danger**	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
⚠ **Caution**	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 About This Document

This user manual is intended for the administrator of the system.

The manual guides you to establish and configure the surveillance system. Follow this manual to perform the installation of the system, activation of VSM, access of the system, and configuration of the surveillance task via the provided Web Client, etc. To ensure the properness of usage and stability of the system, refer to the contents below and read the manual carefully before installation and operation.

Chapter 2 Introduction

The system is developed for central management of video monitoring system and features flexibility, scalability high reliability, and powerful functions.

The system provides the central management, information sharing, convenient connection, and multi-service cooperation. It is capable of adding devices for management, live view, storage and playback of video files, alarm linkage, access control, time and attendance, face comparison, and so on.

Note

The displayed modules on the home page vary with the License you purchased. For detailed information, contact our technical support.

The complete system contains the following modules. You can install the modules according to actual needs. Refer to ***Installation and Uninstallation*** for the detailed installation instructions of the system.

Module	Introduction
VSM (Video Surveillance Management)	• Provide the unified authentication service for connecting with the clients and servers. • Provide the centralized management for the users, roles, permissions, devices, and services. • Provide the configuration interface for surveillance and management module. • Provide the log management and statistics function.
Streaming Service (Optional)	Provide forwarding and distributing the audio and video data of live view.

The following table shows the provided clients for accessing or managing system.

Client	Introduction
Control Client	Control Client is a C/S software which provides multiple operating functionalities, including real-time live view, PTZ control, video playback and downloading, alarm receiving, log query, and so on.
Web Client	Web Client is a B/S client for managing system. It provides multiple functionalities, including device management, area management, recording schedule settings, event configuration, user management, and so on.
Mobile Client	Mobile Client is the software designed for getting access to the system via Wi-Fi, 3G, and 4G networks with mobile device. It fulfills the functions of the devices

Client	Introduction
	connected to the system, such as live view, remote playback, PTZ control, and so on.

Chapter 3 Getting Started

The following content describes the tasks typically involved in setting a working system.

Verify Initial Configuration of Devices and other Servers

Before doing anything on system, make sure the devices (camera, DVR, recording server, and so on) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to connect the devices to the system via network.

Install System

Refer to ***Installation and Uninstallation*** for the detailed installation steps.

Open Web Client and Login

Refer to ***Login for First Time for admin User*** .

Activate License

Refer to ***Manage License*** .

Add Devices to System and Configure Area

The system can quickly scan your network for relevant devices (camera, DVR, and so on), and add them to your system. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to ***Manage Resource*** and ***Manage Area*** .

Configure Recording Settings

You can record the video files of the cameras on the storage device according to the configured recording schedule. The schedule can be set as continuous, alarm triggered, or command triggered as desired. Refer to ***Configure Recording*** .

Configure Event and Alarm

The camera exception, device exception, server exception, and alarm input can trigger linkage actions in the system. Refer to ***Configure Event and Alarm*** .

Configure Users

Specify who should be able to access your system, and how. You can set the different permissions for the users to limit the operation of the system. Refer to ***Manage Role and User*** .

Chapter 4 Installation and Uninstallation

Install the service modules on your servers or PCs to build your X-VMS.

Two installation packages are available for building your system.

Basic Installation Package

Contains all the modules to build the system, including Video Surveillance Management (VSM) Service, Streaming Service, and Control Client.

Control Client Installation Package

Contains the Control Client module only.

Note

The VSM Service and Streaming Service cannot be installed on the same PC.

4.1 Install Module

Two installation methods are available for building the modules.

Typical Mode

Install all the service modules (except the Streaming Service) and client.

Custom Mode

Select the installation directory and modules to be installed as desired.

4.1.1 Install Service Module in Custom Mode

During installation in custom mode, you can select the installation directory and install the specified service modules as desired.

Perform this task when you want to install service module in custom mode.

Steps

1. Double-click (X-VMS) to enter the Welcome panel of the InstallShield Wizard.
2. Click **Next** to start the InstallShield Wizard.
3. Read the License Agreement.
    - Click **I accept the terms of the license agreement** and continue.
    - Click **I do not accept the terms of the license agreement** to cancel the installation.
4. Select **Custom** as setup type and click **Next**.
5. **Optional:** Click **Change...** and select a proper directory as desired to install the module(s).
6. Click **Next** to continue.
7. Select the module(s) you want to install and click **Next**.

Note

The VSM Service and Streaming Service cannot be installed on the same PC.

In this way, you can install the service and client modules to different PCs or servers as desired.

8. **Optional:** Select the hot spare mode if you select to install VSM service in the previous step.
   - Select **Normal** if you do not need to build a hot spare system.
   - Select **Mirror Hot Spare** to build a mirror hot spare system. There are two VSM servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real time. When the host server fails, the spare server switches into operation without interruption, thus increasing the reliability of the system.
   - Select **Shared Storage Hot Spare** to build a shared storage hot spare system. There are two VSM servers and one HDD (installed on another server) in the hot spare system: host server, spare server, and the selected HDD. When the host server works, the data is stored in the HDD. When the host server fails, the spare server switches into operation and will take over the HDD to use the same data file.

   Note

   For building the hot spare system, contact our technical support engineer.

9. Click **Install**.

   A panel indicating progress of the installation will display.

10. Read the post-install information and click **Finish** to complete the installation.

    Note

    You can check **Run Web Client** to open the login page of Web Client via web browser automatically. If the settings of your web browser block opening the login page, follow the prompt on the web browser to allow the proper display of the page.

4.1.2 Install Service Module in Typical Mode

You can install all the service modules (except the Streaming Service) and client on one PC or server.

Perform this task when you want to install service module in typical mode.

Steps

1. Double-click (X-VMS) to enter the welcome panel of the InstallShield Wizard.
2. Click **Next** to start the InstallShield Wizard.
3. Read the License Agreement.
   - Click **I accept the terms of the license agreement** and continue.
   - Click **I do not accept the terms of the license agreement** to cancel the installation.
4. Select **Typical** as setup type and click **Next**.
5. **Optional:** Click **Change...** and select a proper directory as desired to install the module.

6. Click **Next** to continue.
7. **Optional:** Select the hot spare mode if you select to install VSM service in the previous step.
   - Select **Normal** if you do not need to build a hot spare system.
   - Select **Mirror Hot Spare** to build a mirror hot spare system. There are two VSM servers in the hot spare system: host server and spare server. When the host server works, the data in host server is copied to the spare server in real time. When the host server fails, the spare server switches into operation without interruption, thus increasing the reliability of the system.
   - Select **Shared Storage Hot Spare** to build a shared storage hot spare system. There are two VSM servers and one HDD (installed on another server) in the hot spare system: host server, spare server, and the selected HDD. When the host server works, the data is stored in the HDD. When the host server fails, the spare server switches into operation and will take over the HDD to use the same data file.

   Note

   For building the hot spare system, contact our technical support engineer.

8. Read the pre-install information, and click **Install** to begin the installation.

   A panel indicating progress of the installation will display.
9. Read the post-install information and click **Finish** to complete the installation.

   Note

   You can check **Run Web Client** to open the login page of Web Client via web browser automatically. If the settings of your web browser block opening the login page, follow the prompt on the web browser to allow the proper display of the page.

4.2 Install Control Client

You must install X-VMS Control Client on your computer before you can access the system via Control Client.

Perform this task when you want to install the Control Client.

Steps

1. Double-click (X-VMS_Client) to enter the welcome panel of the InstallShield Wizard.
2. Click **Next** to start the InstallShield Wizard.
3. **Optional:** Click **Browse** and select a proper directory on your computer to install the Control Client.
4. Click **Next** to continue.
5. Read the pre-install information and click **Install** to begin the installation.

   A panel indicating progress of the installation will display.
6. Read the post-install information and click **Finish** to complete the installation.

4.3 Uninstall Module

Two uninstallation modes are available for uninstalling the modules.

All Modules Uninstallation

You can remove the entire system from PC or server, including surveillance service software, related installation files, and the Control Client.

Specific Modules Uninstallation

You can remove the specific modules of the system from PC or server, such as VSM, Streaming Service, or the Control Client.

4.3.1 Uninstall All Modules

The entire system contains the surveillance service software, related installation files, and the Control Client. You can remove the entire system from your PC or server if you don't need it.

Before You Start

- Deactivate the activated VSM before removing the VSM, so that the License can be used for activating another VSM. See ***Deactivate License - Online*** or for details.
- Exit all system modules and the system Service Manager.

Perform this task when you want to remove the entire system.

Steps

Note

The following procedures of standard system module removal may be slightly different according to the different OS versions.

1. Select **Control Panel** in Windows' Start menu.
   - If using Category view, find the Programs category, and click **Uninstall a program**.
   - If using Small icons or Large icons view, select **Programs and Features**.
2. Right-click the system you want to remove in the list of currently installed programs.
3. Select **Uninstall** and follow the removal instructions.

   Note

   For uninstalling the VSM, a dialog will pop up to ask you whether to keep the database. If you choose to keep the database, the resource and configuration data will be saved and can be used when you install the system on this hardware server later.

4.3.2 Uninstall Specific Module

You can remove the specific module of system, such as VSM, Streaming Service, or the Control Client, from your PC or server if you don't need it.

Before You Start

- Deactivate the activated VSM before removing the VSM, so that the License can be used for activating another VSM. See ***Deactivate License - Online*** or for details.
- Exit all system modules and the system Service Manager.

Perform this task when you want to remove the specific module of system.

Steps

Note

The following procedures of standard system module removal may be slightly different according to the different OS versions.

1. Select **Control Panel** in Windows' Start menu.
   - If using Category view, find the Programs category, and click **Uninstall a program**.
   - If using Small icons or Large icons view, select **Programs and Features**.
2. Right-click the system you want to remove in the list of currently installed programs.
3. Select **Change** and the InstallShiled Wizard pops up.
4. Select **Modify** and click **Next** to continue.
5. Uncheck the module(s) you want to uninstall and click **Next**.
6. Click **Uninstall** and follow the removal instructions.

   Note

   For uninstalling the VSM, a dialog will pop up to ask you whether to keep the database. If you choose to keep the database, the resource and configuration data will be kept and can be used when you install the system on this hardware server for next time.

   The selected modules will be installed and the unselected modules will be removed.

4.4 Service Manager

After successfully installing the service module(s), you can run the Service Manager and perform the related operations of service, such as starting, stopping, or restarting the service.

Perform this task when you need to run the Service Manager and perform the related operations.

Steps

1. Right-click and select **Run as Administrator** to run the Service Manager.

Note

The displayed items vary with the service modules you selected for installation.

2. **Optional:** Perform the following operation(s) after starting the Service Management.

   Stop All
   Click **Stop All** to stop all the service.

   Restart All
   Click **Restart All** to run the service again.

   Stop Specific Service
   Select one service and click ⊖ to stop the service.

   Edit Service
   Click the service name to edit the port of the service.

   Note

   If the port number of the service is occupied by other service, the port No. will be shown in red. You should change the port number to other value before the service can work properly.

   Open Service Location
   Select one service and click 📁 to go to the installation directory of the service.

3. **Optional:** Check **Auto-Launch** to enable launching the Service Manager automatically after the PC started up.

Note

If the auto-launch function is not enabled, all the service modules you installed cannot run automatically after the server started up.

Chapter 5 Login

You can access and configure the system via web browser directly, without installing any client software on the your computer.

5.1 Recommended Running Environment

The following is recommended system requirement for running Web Client.

CPU

Intel Pentium IV 3.0 GHz and above

Memory

1 GB and above

Video Card

RADEON X700 Series

Web Browser

Internet Explorer 10/11 and above (32-bit), Firefox 32 and above (32-bit), Google Chrome 35 and above (32-bit)

Note

You should run the web browser as administrator.

5.2 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

5.2.1 Login for First Time for admin User

By default, the system predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Perform this task when you access the system for the first time.

Steps

1. In the address bar of the web browser, enter the address of the PC running VSM (Video Surveillance Management) service and press **Enter** key.

Example

If the IP address of PC running VSM is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

Note

- You should set the transfer protocol before accessing the VSM. For details, refer to ***Set Transfer Protocol*** .
- You should set the VSM's IP address before accessing the VSM via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the password and confirm password for the admin user in the pop-up Create Password window.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**. For setting minimum password strength, refer to ***Manage System Security*** .

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

3. Click **OK**.

   Web Client home page displays after you successfully creating the admin password.

Result

After you logging in, the Site Name window opens and you can set the site name for the current system as you want.

Note

You can also set it in **System → Site Name** . See ***Set Site Name*** for details.

5.2.2 First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

Perform this task when you need to access the system as normal user for the first time.

Steps

1. In the address bar of the web browser, input the address of the PC running VSM (Video Surveillance Management) service and press the **Enter** key.

   Example

   If the IP address of PC running VSM is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the VSM's IP address in WAN Access of System Configuration before accessing the VSM via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

   Note

   Contact the administrator for the user name and initial password.

3. Click **Login** and the **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

   The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***Manage System Security*** .

   Caution

   The password strength of the device can be checked by the system. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

5.3 Login via Web Client

You can access the system via web browser and configure the system.

Perform this task when you need to access the system via Web Client.

Steps

1. In the address bar of the web browser, input the address of the PC running VSM (Video Surveillance Management) service and press **Enter** key.

   Example

   If the IP address of PC running VSM is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the VSM's IP address in WAN Access of System Configuration before accessing the VSM via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.
3. Click **Login** to log in to the system.

   Note

   - If failed password attempt of current user is detected, you are required to input the verification code. The failed password attempts from current client, other client, and other address will all require the verification code.
   - The failed password attempt and verification code attempt from current client, other client (e.g., Control Client), and other address will all be accumulated. Your IP address will be locked for a specified period of time after specific number of failed password or verification code attempts detected. For setting failed login attempts and locking duration, refer to ***Manage System Security*** .
   - The account will be frozen for 30 minutes after 5 failed password attempts. The failed password attempts from current client, other clients (e.g., Control Client), and other addresses will all be accumulated.
   - The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***Manage System Security*** .
   - If your password is expired, you will be asked to change your password when login. For setting maximum password age, refer to ***Manage System Security*** .

Result

Web Client home page displays after you successfully logging in to the system.

5.4 Change Password for Reset User

When the normal user's password is reset to the initial password by admin user, he/she should change the initial password and set a new password when logging into X-VMS via the Web Client.

Perform this task when you need to access the system via the Web Client by normal user whose password has been reset to the initial one.

Steps

1. In the address bar of the web browser, enter the address of the PC running VSM (Video Surveillance Management) service and press **Enter** key.

   Example

   If the IP address of PC running VSM is 172.6.21.96, and you should enter http://172.6.21.96 or https://172.6.21.96 in the address bar.

   Note

   You should configure the VSM's IP address in WAN Access of System Configuration before accessing the VSM via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

   Note

   The initial password for normal user is Abc123.

3. Click **Login** and a **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

   The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***Manage System Security*** .

   Caution

   The password strength of the device can be checked by the system. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

5.5 Forgot Password

If you forgot the your account's password, you can reset the password and set a new password.

Perform this task when you forgot the user's password.

Steps

1. Open the login page.
2. Enter a user name in the User Name field.
3. Click **Forgot Password**.
4. Set the new password for the user.
   - For admin user, enter the activation code, new password, and confirm password in the Reset Password window.
   - For normal user, if the email address is set when adding the user and email server is tested successfully, click **Get Code**, and then you will receive an email with the verification code in your email address. Within 10 minutes, enter the received verification code, new password, and confirm password to set the new password for the normal user.

     Note

     If the email address is not set for the normal user, contact the admin user to reset the password for you and change the password when login. See ***Reset Password for Normal User*** for details.
   - For domain user, contact the admin user to reset the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***Manage System Security*** .

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **OK**.

Chapter 6 Web Control

For accessing the Web Client via web browser, you must install a web control on the PC on which you access the Web Client when performing some functions, e.g., live view, playback, and searching online devices. Web Client automatically asks you to install the web control when you want to access the corresponding functions, and you can follow the prompts to install it on the PC.

Chapter 7 Wizard

The wizard can guide you to go through the basic operations of the system, including adding the encoding devices, adding access control devices, configuring event parameters, and managing the users.

Click on Home page to enter the Start Wizard page.

Video

You can add the active online encoding devices in the same local subnet with the Web Client, add the devices by IP address, IP segment, or port segment, and import cameras in batch, etc. See ***Manage Encoding Device*** for detailed configuration.

Access Control

You can add the access control devices to the system for further operations, and set the access permission for persons to access the door, etc. See ***Manage Access Control Device*** for detailed configuration.

Event

You can configure the detected events with linkage actions for notification. For example, when motion is detected, it will trigger a user-defined event. See ***Configure Event and Alarm*** for detailed configuration.

User

You can add multiple user accounts to the system for accessing through Web Client, Control Client, or Mobile Client, and you are allowed to assign different roles for different users. The roles can be specified with different permissions. Refer to ***Manage Role and User*** for detailed configuration.

Chapter 8 Manage License

After installing X-VMS, you have a temporary License for a specified number of cameras and limited functions. To ensure the proper use of X-VMS, you can activate the VSM to access more functions and manage more devices. If you do not want to activate the VSM now, you can skip this chapter and activate the system later.

Two types of License are available for X-VMS:

- **Base:** You need to purchase at least one basic License to activate the X-VMS.
- **Expansion:** If you want to increase the capability of your system (e.g., connect more cameras), you can purchase an expanded License to get additional features.

Note

- Only the admin user can perform the activation, update, and deactivation operation.
- If you encounter any problems during activation, update, and deactivation, please send the server logs to our technical support engineers.

8.1 Activate License - Online

If the VSM to be activated can properly connect to the Internet, you can activate the VSM in online mode.

Perform this task when you need to activate the License in online mode.

Steps

1. Log in to X-VMS via the Web Client. Refer to ***Login via Web Client*** .
2. Click **Online Activation** in the License area to open the License configuration window.
3. Enter the activation code received when you purchased your License.

   Note

   If you have purchased more than one Licenses, you can click + and enter other activation codes.

4. **Optional:** Set the **Hot Spare** switch to **ON** and input the required parameters if you want to build a hot spare system.

   Note

   - You must select Hot Spare mode when you install the system. For details, refer to ***Install Module*** .
   - For how to build the hot spare system, please contact our technical support engineers.

5. Click **OK**

Result

The prompt **Operation completed** will appear when the License is activated.

8.2 Update License - Online

As your project grows, you may need to increase the connectable number of resources (e.g., cameras) for your X-VMS. If the VSM to be updated can properly connect to the Internet, you can update the License in online mode.

Before You Start

Contact your dealer or our sales team to purchase a License for additional features

Perform this task when you need to update your License in online mode.

Steps

1. Log in to X-VMS via the Web Client. Refer to ***Login via Web Client*** for details.
2. Click **Update License** at the License area to open the update panel.
3. Enter the activation code received when you purchase your License.

Note

If you have purchased more than one Licenses, you can click + and enter other activation codes.

4. Click **Update**.

Result

The prompt **Operation completed** will appear when the VSM is successfully updated.

8.3 Deactivate License - Online

If you want to run the VSM on another PC or server, you should deactivate the VSM first and then activate the other VSM again. If the VSM to be deactivated can properly connect to the Internet, you can deactivate the License in online mode.

Perform this task when you need to deactivate License in online mode.

Steps

1. Log in to X-VMS via the Web Client. Refer to ***Login via Web Client*** .
2. Click **Deactivate License** in the License area to open the deactivation panel.
3. Click **Online Deactivation** and check the activation code(s) to be deactivated.
4. Click **OK** to deactivate the license.

Result

The prompt **Operation completed** will appear when the VSM is successfully deactivated. You can activate another VSM with the License.

Chapter 9 Manage Resource

X-VMS supports multiple resource types, such as encoding device, access control device, Remote Site, decoding device and Smart Wall. After adding them to the system, you can manage them, configure required settings and perform further operations. For example, you can add encoding devices for live view, playback, recording settings, event configuration, etc., add access control devices for access control, time and attendance management, etc., add Remote Site for central management of multiple systems, add Recording Server for storing the videos, add Streaming Server for getting the video data stream from the server, and add Smart Wall for displaying decoded video on smart wall.

9.1 Create Password for Inactive Device(s)

Because of simple default password, the devices may be accessed by the unauthorized user easily. For more security purpose, the default password is not provided for some devices. You are required to create the password to activate them before adding them and performing some operations on them via the system . Besides activating the device one by one, you can also deal with multiple ones at the same time. The devices which are activated in a batch will have the same password

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- This function should be supported by the device. Make sure the devices you want to activate support this function.

Perform this task when you need to activate the detected online devices. Here we take creating password for the encoding device as an example.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

   Note

   - For access control devices, click **Physical View → Access Control Device** to enter the access control device management page.
   - For security control devices, click **Physical View → Security Control Device** to enter the security control device management page.
   - For decoding devices, click **Physical View → Smart Wall** . On the Decoding Device area, click **Add** and check **Online Devices** as Adding Mode.

   The detected online devices list in the online device area.
2. View the device status (shown on Security column) and select one or multiple inactive devices.

3. Click ○ to open the Device Activation window.
4. Create a password in the password field, and confirm the password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Click **Save** to create the password for the device.

   An **Operation completed.** message is displayed when the password is set successfully.
6. Click ✓ in the Operation column of the device and change its IP address, subnet mask, and gateway to the same subnet with your computer if you need to add the device to the system. Refer to ***Edit Online Device's Network Information*** .

9.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with VSM server or Web Client, can be detected by X-VMS. For the detected online devices, you can edit their network information as desired via X-VMS remotely and conveniently. For example, change the device IP address due to the changes of the network.

Before You Start
For some devices, you must activate it before editing its network information. Refer to ***Create Password for Inactive Device(s)*** for details.

Perform this task when you need to edit the network information for the detected online devices. Here we take editing encoding device as an example.

Steps
1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

ℹ **Note**

- For access control devices, click **Physical View → Access Control Device** to enter the access control device management page.
- For security control devices, click **Physical View → Security Control Device** to enter the security control device management page.
- For decoding devices, click **Physical View → Smart Wall** . On the Decoding Device area, click **Add** and check **Online Devices** as Adding Mode.

2. In the Online Device area, select a network type.

Server Network

The detected online devices in the same local subnet with the VSM server will list in the Online Device area.

Local Network

The detected online devices in the same local subnet with the Web Client will list in the Online Device area.

3. View the device status (shown on Security column) and click ✎ in the Operation column of an active device.
4. Change the required parameters, such as IP address, device port, HTTP port, subnet mask, and gateway.

Note

The parameters may vary for different device types.

5. Click ✓ .
6. Enter device's password.
7. Click **Save**.

9.3 Manage Encoding Device

The encoding devices (e.g., camera, NVR, DVR) can be added to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations based on the added devices, such as live view, video recording, and event settings,

9.3.1 Add Online Device

The system can perform an automated detection for available encoding devices in the network where the Web Client or VSM server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add an Online Device

When you want to add one of the detected online devices at present or add a few of these devices with different user names and passwords, you need to select single device every time to add it to X-VMS. The IP address, port number and user name will be recognized automatically, which may reduce some manual operations in a way.

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to add single one detected online device.

Steps

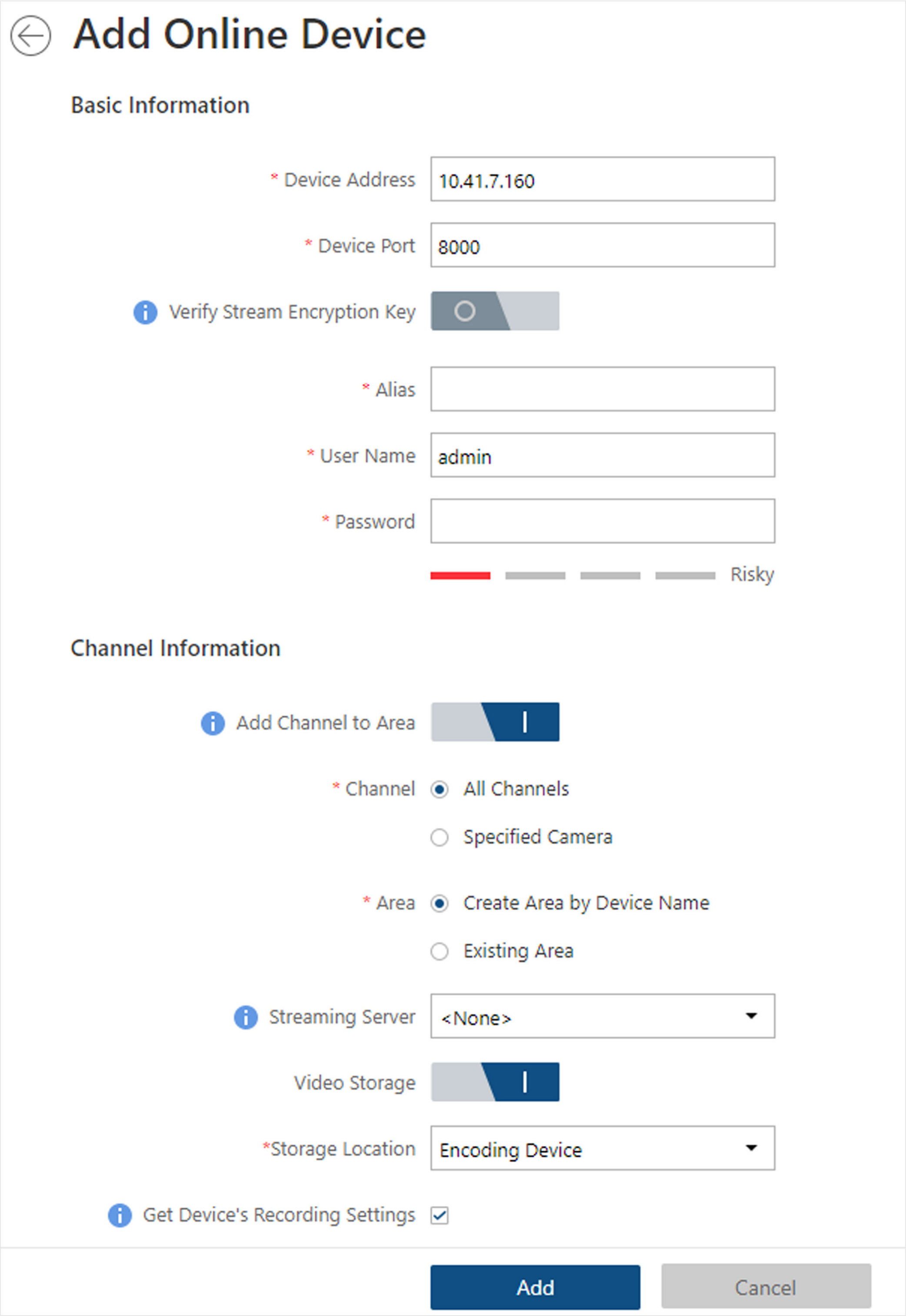
1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, select the active device to be added.
4. Click **Add to Device List** to open the Add Online Device window.



Add Online Device

Basic Information

* Device Address: 10.41.7.160

* Device Port: 8000

Verify Stream Encryption Key: ○

* Alias:

* User Name: admin

* Password:

Risky

Channel Information

Add Channel to Area: I

* Channel: ● All Channels ○ Specified Camera

* Area: ● Create Area by Device Name ○ Existing Area

Streaming Server: <None>

Video Storage: I

*Storage Location: Encoding Device

Get Device's Recording Settings: ☑

Figure 9-1 Add Online Device Window

5. Set the required information.

Device Address

The IP address of the device, which is shown automatically.

Device Port

The port number of the device, which is shown automatically. The default is 8000.

Verify Stream Encryption Key

You can set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in VSM server for security purpose.

Note

This function should be supported by the devices. Refer to the User Manual of the device for getting key.

Alias

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the cameras.

7. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.

8. **Optional:** If you choose to add channels to area, enable the **Video Storage** function and select the storage location for recording.

Encoding Device

The video files will be stored in the device according to the configured recording schedule.

Hybrid Storage Area Network

The video files will be stored in the Hybrid Storage Area Network according to the configured recording schedule.

Cloud Storage Server

The video files will be stored in the Cloud Storage Server according to the configured recording schedule.

pStor

According to the configured recording schedule, the video files will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

Note

- For adding the encoding device by domain name, the video files can only be stored in the local storage of the device.
- Configure the Hybrid Storage Area Network, Cloud Storage Server or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server or pStor.

9. Set the quick recording schedule for added channels.
   - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
   - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
10. Click **Add**.
11. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device.

Note

For detailed operation steps about remote configuration, see the user manual of the device.

Change Password Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Add Online Devices in a Batch

For the detected online encoding devices, if they have the same user name and password, you can add multiple devices to X-VMS at a time. The devices added by this method will be set as the same channel information, which you can edit later if required.

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to add the detected online devices in a batch.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, check the active device(s) to be added.
4. Click **Add to Device List** to open the Add Online Device dialog.
5. **Optional:** Set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field.

   Then when starting live view or remote playback of the camera, the client will verify the key stored in VSM server for security purpose.

Note

This function should be supported by the devices. Refer to the user manual of the device for getting key.

6. Enter the same user name and password.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the cameras.

8. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when starting live view on the smart wall.

9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online devices in a batch.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.3.2 Add Device by IP Address or Domain Name

When you know the IP address or domain name of the device to add, you can add the devices to your system by specifying the IP address (or domain name), user name, password, and other related parameters.

Before You Start

Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add device by IP address or domain name.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **IP/Domain** as the adding mode.
4. Set the required information, including access protocol, device address, device port, stream encryption key, alias, user name, and password.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   The IP address or domain name of the device.

   Device Port

   By default, the device port No. is 8000.

   Verify Stream Encryption Key

You can set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in VSM server for security purpose.

Note

This function should be supported by the devices. Refer to the User Manual of the device for getting key.

Alias

Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the cameras.

6. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.

7. **Optional:** If you choose to add channels to area, enable the **Video Storage** function and select the storage location for recording.

Encoding Device

The video files will be stored in the device according to the configured recording schedule.

Hybrid Storage Area Network

The video files will be stored in the Hybrid Storage Area Network according to the configured recording schedule.

Cloud Storage Server

The video files will be stored in the Cloud Storage Server according to the configured recording schedule.

pStor

According to the configured recording schedule, the video files will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

Note

- For adding the encoding device by domain name, the video files can only be stored in the local storage of the device.
- Configure the Hybrid Storage Area Network, Cloud Storage Server or pStor in advance, or its storage location cannot display in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server or pStor.

8. Set the quick recording schedule for added channels.
   - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
   - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
9. Finish adding the device.
   - Click **Add** to add the encoding device and back to the encoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For detailed operation steps for the remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.3.3 Add Devices by IP Segment

When multiple encoding devices to add have the same port number, user name and password, but have different IP addresses within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start IP address to the end IP address for the devices in order to add them quickly.

Before You Start
Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **IP Segment** as the adding mode.
4. Enter the required information.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   Enter the start IP address and end IP address where the devices are located.

   Device Port

   The same port number of the devices. By default, the device port No. is 8000.

   Verify Stream Encryption Key

   You can set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in VSM server for security purpose.

   Note

   This function should be supported by the devices. Refer to the User Manual of the device for getting key.

   User Name

   The user name for administrator created when activating the device or the added non-admin users. When adding the device to X-VMS using the non-admin user, your permissions may restrict your access to certain features.

   Password

   The password required to access the device.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the channels.

6. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.

7. Finish adding the device.
   - Click **Add** to add the devices of which the IP addresses are between the start IP address and end IP address and back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.3.4 Add Devices by Port Segment

When multiple encoding devices to add have the same IP address, user name and password, but have different port numbers within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

Before You Start

Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you want to add devices by port segment.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **Port Segment** as the adding mode.
4. Set the required information.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   Enter the IP address to add the devices which have the same IP address.

   Device Port

   Enter the start port No. and the end port No.

   Verify Stream Encryption Key

   You can set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored in VSM server for security purpose.

   Note

   This function should be supported by the devices. Refer to the user manual of the device for getting key.

   User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the channels.

6. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected streaming server when displaying live view on the smart wall.

7. Finish adding the device.
   - Click **Add** to add the devices of which the port No. is between the start port No. and end port No. and back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other devices.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password	Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.3.5 Add Device by Guarding Vision

You can add the encoding devices which have been added to the Guarding Vision account to the system.

Before You Start

Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add device by Guarding Vision.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **Guarding Vision** as the adding mode.
4. Enter the required information.

   Guarding Vision Server Address

   Enter the address of the Guarding Vision service. By default, it's ***https://open.ezvizlife.com***.

   appKey

   Enter the appKey of Guarding Vision service.

   appSecret

   Enter the appSecret of Guarding Vision service.

   Verify Stream Encryption Key

   Set the **Verify Stream Encryption Key** switch to ON, and enter stream encryption key in **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the camera, the client will verify the key stored in the VSM server for security purpose.

   This function should be supported by the devices. Refer to the User Manual of the device for getting key.

   Device List

   Click **Get Device** to display the devices added to the account, select the device, and input the device's user name and password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Set the **Add Channel to Area** switch to ON to import the channels of the added devices to an area.

   Note

   - You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the channels.

6. **Optional:** If you choose to add channels to area, select a Streaming Server to get the video stream of the channels via the server.

   Note

   You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.

7. Finish adding the device.
   - Click **Add** to add the encoding device and back to the encoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.3.6 Add Devices in a Batch

When there are a batch of devices to add to X-VMS , you can edit the predefined template containing the required device information, and import it to add multiple devices at a time. This is also a highly effective methods if you set up several similar systems.

Before You Start

Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by importing the template which contains information of multiple devices.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.
2. Click **Add** to enter the Add Encoding Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
6. Click ⋯ and select the template file.
7. Finish adding devices.
   - Click **Add** to add the devices and back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other devices.
8. **Optional:** Perform the following operations after adding devices in a batch.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.4 Manage Access Control Device

You can add the access control devices to the system for access permission configuration, time and attendance management, etc.

9.4.1 Add Online Device

The active online access control devices in the same local subnet with the current Web Client or VSM server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add Single Online Device

You can add the detected online access control devices, and here we introduce the process for adding single one device.

Before You Start

- Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Perform this task when you need to add single one detected online device.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the current Web Client will list in the Online Device area.

Note

For the DS-K5600 face recognition series, the displayed online devices are different according to the working mode setting. Refer to ***Set Working Mode*** for details.

3. In the Online Device area, select the active device to be added .
4. Click **Add to Device List** to open the Add Online Device window.
5. Enter the required information.

Note

The device's IP address can be automatically shown in **Device Address** field.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Set the **Add Channel to Area** switch to ON to import the access points of the added device to an area.

Note

- You can import all the access points or the specified access point(s) of the device to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import access points to area, you cannot perform the further configurations for the access points.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Application Settings

After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon ❗ will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

Add Online Devices in a Batch

For the detected online access control devices, if they have the same password for the same user name, you can add multiple devices at a time.

Before You Start

- Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Perform this task when you need to add the detected online devices in a batch.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. In the Online Device area, select a network type.

Server Network

The detected online devices in the same local subnet with the VSM server will list in the Online Device area.

Local Network

The detected online devices in the same local subnet with the Web Client will list in the Online Device area.

Note

For the DS-K5600 face recognition series, the displayed online devices are different according to the working mode setting. Refer to ***Set Working Mode*** for details.

3. In the Online Device area, select the active devices to be added.
4. Click **Add to Device List** to open the Add Online Device window.
5. Enter the required information.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Set the **Add Channel to Area** switch to ON to import the access points of the added devices to an area.

Note

- You can create a new area by the device name or select an existing area.
- If you do not import access points to area, you cannot perform the further operations for the access points.

7. Click **Add**.
8. Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Application Settings

After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon ❗ will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

9.4.2 Add Device by IP Address

When you know the IP address of the access control device to add, you can add the devices to your system by specifying the IP address, user name, password, and other related parameters.

Before You Start

Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by IP address.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **IP Address** as the adding mode.
4. Enter the required the information.

Note

By default, the device port No. is 8000.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the access points of the added devices to an area.

Note

- You can import all the access points or the specified access point(s) of the device to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you don't import access points to area, you cannot perform further operations for the access points.

6. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add next access control device.
7. Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Application Settings

After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon (!) will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

9.4.3 Add Devices by IP Segment

If the access control devices having the same user name and password, and their IP addresses are between the IP segment, you can specify the start IP address and the end IP address, user name, password, and other related parameters to add them.

Before You Start

Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by IP segment.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **IP Segment** as the adding mode.
4. Enter the required the information.

Note

By default, the device port No. is 8000.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the access points of the added devices to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - If you don't import access points to area, you cannot perform further operations for the access points.

6. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add next access control device.
7. Perform the following operations after adding the devices.

   Remote Configurations

   Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

   Note

   - For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
   - After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
   - For details about remote configuration, see the user manual of the device.

   Change Password

   Select the added device(s) and click 🔑 to change the password for the device(s).

   Note

   - If the devices have the same password, you can select multiple devices to change the password for them at the same time.

   Apply Application Settings

   After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon ❗ will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

9.4.4 Add Devices by Port Segment

If the access control devices having the same IP address, user name and password, and their port No. are between the port segment, you can specify the start port No. and the end port No., IP address, user name, password, and other related parameters to add them.

Before You Start

Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by port segment.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **Port Segment** as the adding mode.
4. Enter the required the information.

   ⚠ **Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the access points of the added devices to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - If you don't import access points to area, you cannot perform further operations for the access points.

6. Finish adding the device.
   - Click **Add** to add the access control device and back to the access control device list page.
   - Click **Add and Continue** to save the settings and continue to add next access control device.
7. Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Application Settings

After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon ❗ will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

9.4.5 Add Devices in a Batch

You can enter the access control device information to the predefined template to add multiple devices at a time.

Before You Start

Make sure the access control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices in a batch.

Steps

1. Click **Physical View → Access Control Device** to enter the Access Control Device Management page.
2. Click **Add** to enter the Add Access Control Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (CSV file) in your PC.

5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
6. Click … and select the template file.
7. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other devices.
8. Perform the following operations after adding devices in a batch.

Remote Configurations

Click ⚙ to edit the time parameters, reboot the device, restore the device, or set other configurations of the corresponding device.

Note

- For some access control devices, you can custom Wiegand communication rules for connecting the customized Wiegand card reader.
- After restoring the device, you need to apply the parameters in the system to the device (click **Apply Application Settings** on Access Control Device Management page).
- For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Apply Application Settings

After restoring the database or device's default configurations, if the parameters (such as anti-passback and opening door with first card) in the system are inconsistent with the parameters on the access control device(s), a red icon ❗ will be displayed on the right side of the **Apply Application Settings**. Click **Apply Application Settings** to clear the original data on the device and apply the current settings in system to the device(s).

9.5 Manage Security Control Device

You can add the security control devices to the system for managing partition, zone, arming/ disarming, handling alarms,etc.

The security control device includes the security control panel, panic alarm station, etc., which are widely applied to many scenarios.

A security control panel is used for monitoring arming zones, handling alarm signal from the triggers, and uploading alarm reports to the central alarm monitoring station. The security control panel is very important for preventing robbery, theft or other accidents.

A panic alarm station is mainly installed in the areas with the crowd or high incidence of cases, such as school, square, tourist attraction, hospital, supermarket gate, market, station, parking lot, etc. When the emergency happens or someone asks for help, the person can press panic button to send alarm to the monitoring center, and the operator in the center will take the appropriate actions. The panic alarm station helps to realize alarm aid in emergency.

9.5.1 Add Online Device

The active online security control devices in the same local subnet with the current Web Client or VSM server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add Single Online Device

You can add the detected online security control devices, and here we introduce the process for adding single one device.

Before You Start

- Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Perform this task when you need to add single one detected online device.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   As the default selection, the detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the current Web Client will list in the Online Device area.

3. In the Online Device area, select the active device to be added .
4. Click **Add to Device List** to open the Add Online Device window.
5. Enter the required information.

Note

The device's IP address can be automatically shown in **Device Address** field.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- You can select **Specified Alarm Input** and select alarm inputs to import to the area.
- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the further configurations for the channels.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the online device.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Add Online Devices in a Batch

For the detected online security control devices, if they have the same password for the same user name, you can add multiple devices at a time.

Before You Start

- Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Perform this task when you need to add the detected online devices in a batch.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, select the active devices to be added.
4. Click **Add to Device List** to open the Add Online Device window.
5. Enter the required information.

   ⚠ **Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
6. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- You can select **Specified Alarm Input** and select alarm inputs to import to the area.
- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the further configurations for the channels.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the online devices in batch.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.5.2 Add Device by IP Address

When you know the IP address of the security control device to add, you can add the devices to your system by specifying the IP address, user name, password, and other related parameters.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by IP address.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **IP Address** as the adding mode.
4. Enter the required the information.

Note

By default, the device port No. is 8000.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- You can select **Specified Alarm Input** and select alarm inputs to import to the area.
- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- Up to 64 alarm inputs can be imported in one area. If you don't import channels to area, you cannot perform further operations for the channels.

6. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
7. Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.5.3 Add Device by Guarding Vision

If the IP address You can add the security control devices which have been added to the Guarding Vision account to the system.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add device by Guarding Vision.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Guarding Vision** as the adding mode.
4. Enter the required information.

   Guarding Vision Server Address

   Enter the address of the Guarding Vision service. By default, it's ***https://open.ezvizlife.com***.

   appKey

   Enter the appKey of Guarding Vision service.

   appSecret

   Enter the appSecret of Guarding Vision service.

   Device List

   Click **Get Device** to display the devices added to the account, select the device, and enter the device's user name and password.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the further configurations for the channels.

6. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
7. **Optional:** Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.5.4 Add Device by IP Segment

If the security control devices having the same port No., user name and password, and their IP addresses are between the IP segment, you can specify the start IP address and the end IP address, port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by IP segment.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **IP Segment** as the adding mode.
4. Enter the required the information.

Note

By default, the device port No. is 8000.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the further configurations for the channels.

6. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
7. Perform the following operations after adding the devices.

Remote Configurations

Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.5.5 Add Device by Port Segment

If the security control devices having the same user name and password, and their port No. are between the port segment, you can specify the start port No. and the end port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices by port segment.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Port Segment** as the adding mode.
4. Enter the required the information.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Set the **Add Channel to Area** switch to ON to import the channels (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

   Note

   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform the further configurations for the channels.

6. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
7. Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.5.6 Add Device in a Batch

You can edit the predefined template with the security control device information to add multiple devices at a time.

Before You Start

Make sure the security control devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add devices in a batch.

Steps

1. Click **Physical View → Security Control Device** to enter the Security Control Device Management page.
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (CSV file) in your PC.
5. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
6. Click ··· and select the template file.
7. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other devices.
8. Perform the following operations after adding devices in a batch.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click 🔑 to change the password for the device(s).

Note

- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

9.6 Restore/Reset Device Password

If you forgot the password of the detected online devices, you can restore the device's default password or reset the device's password through the system. Then you can access the device or add it to the system using the password.

For detailed operations of restoring device's default password, refer to ***Restore Device's Default Password*** .

For detailed operations of resetting device's password, refer to ***Reset Device Password*** .

9.6.1 Reset Device Password

If you have forgotten your password you use to access online device, you can request to have a key file from your technical support and reset the device's password through the system.

Before You Start

- Make sure the devices (cameras, DVR, access control device, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to reset the device's password. Here we take the encoding device as an example.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

Note

- For access control devices, click **Physical View → Access Control Device** to enter the access control device management page.
- For decoding devices, click **Physical View → Smart Wall** . On the Decoding Device area, click **Add** and check **Online Devices** as Adding Mode.

The detected online devices list in the Online Device area.

2. In the Online Device area, view the device status (shown on Security column) and click icon in the Operation column of an active device.

   A dialog with import file and export file, password and confirm password fields opens.
3. Click **Export** to save the device file on your PC.
4. Send the file to our technical engineers.

Note

For the following operations about resetting the password, contact the technical support engineer.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

9.6.2 Restore Device's Default Password

For some encoding devices with old firmware version, if you forgot the password you use to access the online device, you can restore the device's default password through the system and then you must change the default password to a stronger one for better security.

Before You Start

- Make sure the devices (cameras, DVR, etc.) you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operations about activating devices.

Perform this task when you need to restore the device's default password.

Steps

1. Click **Physical View → Encoding Device** to enter the Encoding Device Management page.

   The detected online devices list in the Online Device area.
2. In the Online Device area, view the device status (shown on Security column) and click ↺ in the Operation column of an active device.

   A dialog with security code pops up.
3. Enter the security code and restore the default password of the selected device.

   Note

   Contact our technical support to obtain a security code.

What to do next

You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

9.7 Manage Remote Site

You can add other X-VMS without RSM (Remote Site Management) module to the X-VMS with RSM module as the Remote Site for central management.

After adding the Remote Site to the Central System, you can manage the Remote Site's cameras (such as live view and playback), add the Remote Site's configured alarms so that you can manage the alarms via the Central System, and set the recording schedule for the Remote Site's cameras and store the recorded video files in the Recording Server added to the Central System. You can also view the Remote Site's GIS location, hot spot, and hot region settings in Map module.

Remote Site

If the X-VMS doesn't have RSM module (based on the License you purchased), you can add it to the Central System as Remote Site.

Central System

If the X-VMS has RSM module (based on the License you purchased), you can add other Remote Sites to this system. This system and the added Remote Sites are called Central System.

Note

- The system with RSM module cannot be added to other Central System as Remote Site.
- If one Remote Site has been added to one Central System, it cannot be added to other Central System.

9.7.1 Add Remote Site by IP Address or Domain Name

When you know the IP address or domain name of the Remote Site to add, you can add the site to the Central System by specifying the IP address (or domain name), user name, password, and other related parameters.

Perform this task when you need to add Remote Site by IP address or domain name.

Steps

Note

When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. Enter the Add Remote Site page.
   - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.
3. Select **IP/Domain** as the adding mode.
4. Enter the required information.

   Site Address

   The IP address or domain name of the Remote Site.

   Site Port

   Enter the port No. of the Remote Site. By default, it's 80.

   Alias

   Edit a name for the Remote Site as desired. You can check **Synchronize Name** to synchronize the Remote Site's name automatically.

   User Name

   The user name for the Remote Site, such as admin user and normal user.

   Password

   The password required to access the Remote Site.

   Description

Optionally, you can enter the descriptive information for the Remote Site, such as location and deployment.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Enable receiving the alarms configured on the Remote Site.
   1) Set the **Select Alarm** switch to **ON** to display all the configured alarms on a Remote Site.
   2) **Optional:** Filter the configured alarms by the alarm source, triggering event, and alarm priority.
   3) Select the configured alarm(s).

   Note

   - After receiving the alarm from Remote Site, the alarm will be configured as alarm in Central System automatically. You can click **Default Configuration Rule** to view the imported alarms' default settings including alarm name, alarm priority, actions, etc.
   - You can view and edit alarms in Alarm module. For details about setting the alarm, refer to ***Configure Alarm*** .
6. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.

   Max. Number of Backups

   Define the maximum number of backup files available on the system.
7. **Optional:** Enable backing up the Remote Site's database in schedule.
   1) Set the **Scheduled Database Backup** switch to **ON**.
   2) Select how often to back up the database.

   Note

   If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

   3) Select what time of a day to start backup.
8. Finish adding the Remote Site.
   - Click **Add** to add the Remote Site and back to the Remote Site list page.
   - Click **Add and Continue** to save the settings and continue to add other Remote Sites.

9.7.2 Add Remote Site Registered to Central System

If the Remote Sites have been registered the Central System and the Central System also enabled the receiving site registration function, the registered Remote Sites will display in the site list. You can add them to the Central System by entering user names and passwords.

Before You Start

- The Remote Site must be registered to the Central System by itentering the Central System's network parameters (see ***Register to Central System*** for details).
- The Central System should enable the receiving site registration function (see ***Allow for Remote Site Registration*** for details).

Perform this task when you need to add the site which has registered to the Central System.

Steps

Note

When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.

1. Click **Remote Site Management** on home page to enter the Remote Site management page.
2. Enter the adding Remote Site page.
   - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.
3. Select **Site Registered to Central System** as the adding mode.

   The sites which have already registered to the Central System will display in the list.
4. Select the Remote Site(s) and enter the user name and password of the Remote Site(s).

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
   Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
5. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.
   Max. Number of Backups

   Define the maximum number of backup files available on the system.

Note

The value of maximum number of backups ranges from 1 to 5.

6. **Optional:** Back up the Remote Site's database in schedule.
   1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.
   2) Select how often to back up the database.

      Note

      If you select **Weekly** or **Monthly** for running the backup task, select which day to run.
   3) Select what time of the day to start backup.
7. Finish adding Remote Site.
   - Click **Add** to add the Remote Site and back to the Remote Site list page.
   - Click **Add and Continue** to save the settings and continue to add other Remote Sites.

9.7.3 Add Remote Sites in a Batch

When you want to add multiple Remotes Sites at a time for convenience, you can edit the predefined template by entering the sites' parameters and import the template to the Central System to add them.

Perform this task when you need to add Remote Sites in a batch.

Steps

Note

When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.

1. Click **Remote Site Management** on home page to enter the Remote Site management page.
2. Enter the adding Remote Site page.
   - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (CSV file) on your PC.
5. Open the exported template file and input the required information of the Remote Sites to be added on the corresponding column.
6. Click ··· and select the template file.
7. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.

   Max. Number of Backups

   Define the maximum number of backup files available on the system.
8. **Optional:** Back up the Remote Site's database in schedule.

1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.
2) Select how often to back up the database.

Note

If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

3) Select what time of the day to start backup.

9. Finish adding Remote Site.

- Click **Add** to add the Remote Site and back to the Remote Site list page.
- Click **Add and Continue** to save the settings and continue to add other Remote Sites.

9.7.4 Back Up Remote Site's Database to Central System

After adding the Remote Site, you can back up the database of the Remote Site to the Central System. The database backup can be performed according to the configured schedule or immediately. In case of the data deletion or corruption following a natural or human-induced disaster, you can recover the data to ensure the business continuity.

Perform this task when you need to back up the database of Remote Site in the Central System.

Steps

1. Click **Remote Site Management** on home page to open the Remote Site management page.

2. In the site list on the left, click the Remote Site name to view its details.

3. Click **Back Up Now** to back up the Remote Site's database manually.

Note

The backup file is stored in the **VSM Servers\VSM\Backup** of the installation path of the Central System.

4. **Optional:** Set the backup parameters and enable scheduled database backup if needed to back up the Remote Site's database regularly.

1) Click **Set Database Backup** to open the Set Database Backup dialog.
2) Set the **Scheduled Database Backup** switch as **ON** to enable the scheduled backup.
3) Select how often to back up the database.

Note

If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

4) Select what time of the day to start backup.
5) Set the **Maximum Number of Backups** to define the maximum number of backup files available on the system.

Note

The maximum number of the backups should be between 1 to 5.

6) Click **Save**.

Result

The backup file (including manual backup and scheduled backup) will display in the list, showing the file name and backup time.

9.7.5 Edit Remote Site

After adding the Remote Site, you can view and edit the added Remote Site's information and set its GPS location.

Perform this task when you need to edit the added Remote Site's details.

Steps

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. In the site list on the left, click the Remote Site name to view its details.
3. View and edit the basic information of the Remote Site, including IP address, port, alias, etc.

   Note

   You cannot edit the address and port of the site registered to the Central System.
4. In the original information field, view the Remote Site's site name, system ID, system version, and GPS location.

   Note

   If the GPS location is not configured, click **Configuration** to set its location in Map module. See ***Manage Map*** for details.
5. **Optional:** Click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

   Note

   The site must be online if you need to enter its Web Client.
6. Click **Save**.

9.7.6 View Remote Site's Changes

When there are changed resources on the Remote Site, such as newly added cameras, deleted cameras, and name changed cameras, you can view the changed resources and synchronize the resources in Central System with the Remote Site.

Perform this task when you need to view the Remote Site's changes.

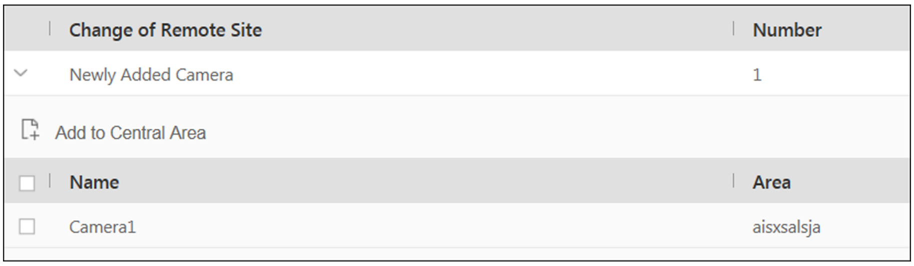
Steps

Note

The site should be online if you need to view the changed resources.

1. Click **Remote Site Management** on home page to open the Remote Site management page.
2. Click in the site list on the left to get the latest status of the Remote Sites.

   If the resources on the Remote Site are changed, a red dot will appear on the icon of Remote Site as .
3. Click the site name whose resources are changed to enter its details page.
4. Click **Changes of Remote Site** to view the changes.
5. When there are newly added cameras on the site, you can view the added cameras and add them to the area in Central System.
   1) If there are some newly added cameras on Remote Site, click **Newly Added Camera** to expand the newly added camera list.



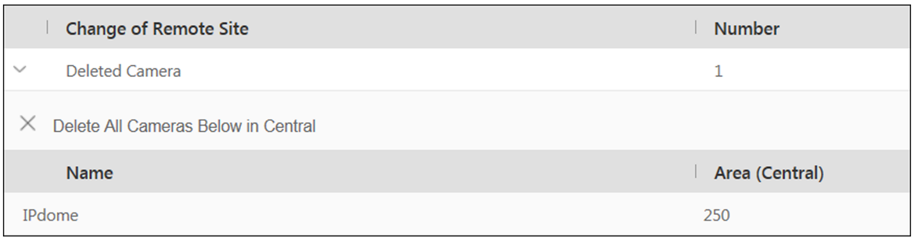
Change of Remote Site	Number
Newly Added Camera	1

Add to Central Area

□ Name	Area
□ Camera1	aisxsalsja

Figure 9-14 Changes of Remote Site

   You can view the camera name and area name on the Remote Site.
   2) Select the camera(s) and click **Add to Central Area** to synchronize the newly added cameras to the Central System.
   3) Select the area in the Central System.
   4) Click **Save**.
6. When there are some cameras deleted from the site, you can view the deleted cameras and remove them from Central System.
   1) If there are some cameras deleted from Remote Site, click **Deleted Camera** to expand the deleted camera list.



Change of Remote Site	Number
Deleted Camera	1

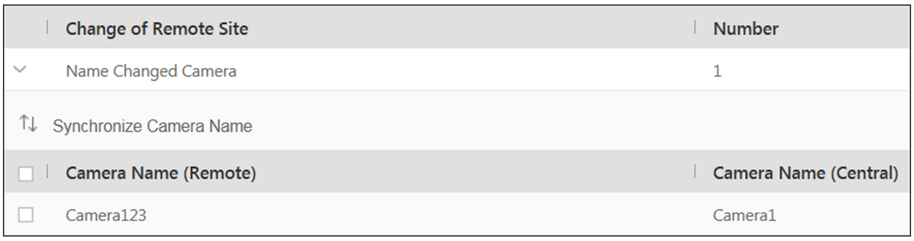
Delete All Cameras Below in Central

Name	Area (Central)
IPdome	250

Figure 9-15 Change of Remote Site

   You can view the camera name and its area in Central System.
   2) Click **Delete All Cameras Below in Central** to delete the deleted cameras in Central System.

7. When there are some cameras whose names are changed on the site, you can view the name changed cameras and synchronize them to Central System.
   1) If the name of camera of Remote Site is changed, click **Name Changed Camera** to expand the name changed camera list.



Change of Remote Site	Number
Name Changed Camera	1

⇅ Synchronize Camera Name

□ Camera Name (Remote)	Camera Name (Central)
□ Camera123	Camera1

Figure 9-16 Name Changed Camera

   You can view the camera names in Remote Site and Central System.

   2) Select the cameras and click **Synchronize Camera Name** to synchronize the camera name in Central System.

9.8 Manage Recording Server

You can add the Recording Server to the X-VMS for storing the video files. Currently, the Recording Server supports Hybrid Storage Area Network, Cloud Storage Server and pStor. You can also form an N+1 hot spare system with several Hybrid Storage Area Networks to increase the video storage reliability of X-VMS.

9.8.1 Manage Cloud Storage Server

You can add a Cloud Storage Server as a Recording Server to the X-VMS for storing the video files.

Import Service Component Certificate to Cloud Storage Server

For data security purpose, the Cloud Storage Server's certificate should be same with the VSM server's. Before adding the Cloud Storage Server to the system, you should import the certificate stored in the VSM server to the Cloud Storage Server first.

Before You Start

Make sure the Cloud Storage Server you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

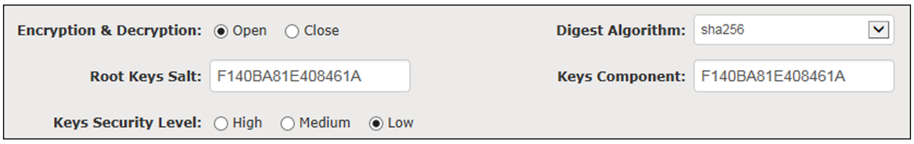
Perform this task when you need to import the service component certificate to the Cloud Storage Server.

Steps

Note

If the service component certificate is updated, you should export the new certificate and import it to the Cloud Storage Server again to update.

1. Click **System → Service Component Certificate** .
2. Click **Export** to export the certificate stored in the VSM server.
3. Log in the configuration page of the Cloud Storage Server via web browser.
4. Click **System → Configuration → Cloud Configuration** .
5. Input the root keys salt and keys component according to the parameters in the certificate you export in Step 3.



Encryption & Decryption: ● Open ○ Close

Digest Algorithm: sha256

Root Keys Salt: F140BA81E408461A

Keys Component: F140BA81E408461A

Keys Security Level: ○ High ○ Medium ● Low

6. Click **Set**.

What to do next

After importing the certificate to the Clout Storage Server, you can add the server to the system for management. See ***Add Cloud Storage Server*** for details.

Add Cloud Storage Server

You can add Cloud Storage Server as Recording Server to the X-VMS for storing the video files and pictures.

Before You Start

- Make sure the Cloud Storage Servers you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- You should import the service component certificate to the Cloud Storage Server first before adding it to the system. See ***Import Service Component Certificate to Cloud Storage Server*** for details.

Perform this task when you need to add Cloud Storage Server to the system.

Steps

1. Click **Physical View → Recording Server** to enter the recording server page.
2. Click **Add** to enter the adding server page.
3. Select **Cloud Storage Server**.
4. Enter the network parameters.

Address

The server's IP address in LAN that can communicate with VSM.

Control Port

The control port No. of the server. If it is not changed, use the default value.

Network Port

The network port No. of the server. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the server. If it is not changed, use the default value.

5. Enter the user's access key and secret key of the Cloud Storage Server for searching the video files stored in this Cloud Storage Server via the X-VMS Mobile Client or downloading pictures via Control Client.

Note

- You can download these two keys on the Cloud Storage Server's configuration page (click **Virtualizing → User Management**).
- For details about searching video files stored in Cloud Storage Server via Mobile Client, see *User Manual of X-VMS Mobile Client*.

6. **Optional:** Set the **Enable Picture Storage** switch to ON for storing pictures in this Cloud Storage Server.

Note

If this function is enabled, you need to set picture downloading port No., which is used to download pictures via Control Client.

7. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
8. Enter the alias, user name, and password of the server.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

9. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
10. **Optional:** Perform the following operations after adding the server:

Edit Server	Click **Alias** field of the server and you can edit the information of the server and view its storage and camera information.

Delete Server
Select the server(s) from the list, and click **Delete** to remove the selected server(s).

Configure Server
Click ⚙ , and the login interface of the Cloud Storage Server displays. You can log in and configure the Cloud Storage Server.

9.8.2 Add Hybrid Storage Area Network

You can add the Hybrid Storage Area Network as Recording Server to the X-VMS for storing the video files and pictures.

Before You Start
Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add Hybrid Storage Area Network to the system.

Steps

1. Click **Physical View → Recording Server** to enter the recording server page.
2. Click **Add** to enter the Add Recording Server page.
3. Select **Hybrid Storage Area Network**.
4. Enter the network parameters.

   Address

   The server's IP address in LAN that can communicate with VSM.

   Control Port

   The control port No. of the server. If it is not changed, use the default value.

   Network Port

   The network port No. of the server. If it is not changed, use the default value.
5. **Optional:** Enable picture storage function for storing pictures in this Hybrid Storage Area Network.
   1) Set the **Enable Picture Storage** switch to ON.
   2) Set picture downloading port No. for downloading pictures via Control Client. If the picture downloading port No. is not changed, use the default ones.
   3) Set signaling gateway port No.. If the picture downloading port No. is not changed, use the default ones.
   4) Enter the access key and secret key.

   Note

   The access key and secret key are used to download pictures via the Control Client. If required, you can contact our technical support to get them.
6. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.

7. Enter the alias, user name, and password of the server.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

8. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
9. **Optional:** Perform the following operations after adding the server:

   Edit Server Click **Alias** field of the server and you can edit the information of the server and view its storage and camera information.

   Delete Server Select the server(s) from the list, and click **Delete** to remove the selected server(s).

   Configure Server Click ⚙ , and the login interface of the Hybrid Storage Area Network displays. You can log in and configure the Hybrid SAN.

   One-Touch Configuration If the Hybrid Storage Area Network has not been configured with storage settings, click ⚙ to perform one-touch configuration before you can store the video files of the camera on the Hybrid Storage Area Network.

9.8.3 Add pStor

You can add pStor as Recording Server to the X-VMS for storing the video files and pictures.

Before You Start

Make sure the pStors you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Perform this task when you need to add pStor to the system.

Steps

1. Click **Physical View → Recording Server** to enter the recording server page.
2. Click **Add** to enter the adding server page.
3. Select **pStor**.
4. Enter the network parameters.

Address

The server's IP address in LAN that can communicate with VSM.

Control Port

The control port No. of the pStor. If it is not changed, use the default value.

Network Port

The network port No. of the pStor. If it is not changed, use the default value.

Signaling Gateway Port

The signaling gateway port No. of the pStor. If it is not changed, use the default value.

5. Enter the user's access key and secret key of the pStor for downloading pictures via Control Client.

Note

You can download these two keys on the pStor's Web Client page.

6. **Optional:** Set the **Enable Picture Storage** switch to ON for storing pictures in this pStor.

Note

If this function is enabled, you need to set picture downloading port No., which is used to download pictures via Control Client.

7. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
8. Enter the alias, user name, and password of the pStor.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

9. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
10. **Optional:** Perform the following operations after adding the server:

Edit Server	Click **Alias** field of the server and you can edit the information of the server and view its storage and camera information.

Delete Server Select the server(s) from the list, and click **Delete** to remove the selected server(s).

Configure Server Click ⚙ , and the login interface of the pStor displays. You can log in and configure the pStor.

9.8.4 Set N+1 Hot Spare

You can form an N+1 hot spare system with several Recording Servers. The system consists of several host servers and a spare server. When the host server fails, the spare server switches into operation, thus increasing the video storage reliability of X-VMS.

Before You Start

- At least two online Hybrid Storage Area Networks should be added to form an N+1 hot spare system.
- Make sure the Hybrid Storage Area Networks you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

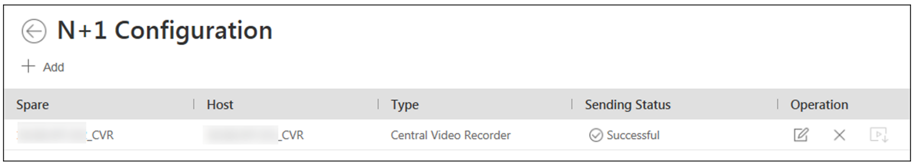
Perform this task when you need to set N+1 hot spare for the added Recording Servers.

Steps

Note

- The N+1 hot spare function is only supported by Hybrid Storage Area Networks.
- The spare server cannot be selected for storing videos until it switches to host server.
- The host server cannot be set as a spare server and the spare server cannot be set as a host server.

1. Click **Physical View → Recording Server → N+1 Hot Spare** to enter the N+1 Configuration page.



N+1 Configuration

+ Add

Spare	Host	Type	Sending Status	Operation
[redacted]_CVR	[redacted]_CVR	Central Video Recorder	Successful	

Figure 9-20 N+1 Configuration Page

2. Click **Add** to set the N+1 hot spare.
3. Select a Hybrid Storage Area Network in the Spare drop-down list to set as the spare server.
4. Select the Hybrid Storage Area Network(s) in the Host field as the host server(s).
5. Click **Add**.

   Note

   The recording schedules configured on the Hybrid Storage Area Network will be deleted after setting it as the spare Recording Server.

6. **Optional:** After setting the hot spare, you can do one or more of the following:

   Edit Click ✎ on the Operation column, and you can edit the spare and host settings.

   Delete Click × on the Operation column to cancel the N+1 hot spare settings.

   Note

   Canceling the N+1 hot spare will cancel all the host-spare associations and clear the recording schedule on the spare server.

7. **Optional:** If the host server sending the recording schedule to spare server failed, you can click ▷ on the Operation column to send the recording schedule on the host server to the spare one again.

9.9 Manage Streaming Server

You can add the Streaming Server to the X-VMS to get the video data stream from the Streaming Server, thus to lower the load of the device.

Note

For system which supports Remote Site Management, the cameras imported from Remote Site adopt the Streaming Server configured on the Remote Site by default. You are not required to add the Streaming Server to Central System and configure again.

9.9.1 Import Service Component Certificate to Streaming Server

For data security purpose, the Streaming Server's certificate should be same with the VSM server's. Before adding the Streaming Server to the system, you should import the certificate stored in the VSM server to the Streaming Server first.

Perform this task when you need to import the service component certificate to the Streaming Server.

Steps

Note

If the service component certificate is updated, you should import the new certificate to the Streaming Server again to update.

1. Log into the Web Client on the VSM server locally.

   You will enter the home page of the Web Client.
2. Enter **System → Service Component Certificate** .
3. Click **Export** to export the certificate stored in the VSM server.
4. Copy the certificate to the computer which has installed with Streaming Service.

5. Open the Service Manager, select the Streaming Service and click to import the certificate you exported in Step 3.

9.9.2 Add Streaming Server

You can add a Streaming Server to the system to forward the video stream.

Perform the following steps when you need to add a Streaming Server to the system.

Steps

1. Click **Physical View → Streaming Server** to enter the Streaming Server management page.
2. Click **Add** to enter the Add Streaming Server page.
3. Input the required information.

   Network Location

   Select **LAN IP Address** if the Streaming Server and the VSM are in the same LAN. Otherwise, select **WAN IP Address**.
4. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch as **ON** and set the corresponding parameters which are available when you access the server via WAN.

   Note

   The **Enable WAN Access** switch is available when you set Network Location as **LAN IP Address**.
5. Finish adding the streaming server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the server and continue to add other servers.

   The servers will be displayed on the server list for management after added successfully. You can check the related information of the added servers on the list.

9.10 Manage Smart Wall

Smart wall can provide security personnel with a rich visual overview of the areas you want to keep an eye on. Before displaying the video on smart wall, you need to set up smart wall firstly, and you can also edit, delete smart wall or manage decoding devices here.

This mainly includes the following:

- Decoding devices that can be added to the system and used for decoding the video stream from the encoding devices.
- Virtual smart wall that defines the layout and the name of the smart wall.
- Link between the decoding outputs of the decoding device and the windows of the smart wall.

9.10.1 Add Decoding Device

The decoding devices can be added to the system for linking with the smart wall. You can add online decoding devices with the IP addresses within VSM server's or Web Client's subnet, and can also add decoding devices by IP address, IP segment, or by port segment.

Add Online Decoding Device

The system can perform an automated detection for available decoding devices on the network where the Web Client or VSM server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Steps

Note

- For Google Chrome, you should install the SADP service according to the instructions and then the online device detection function is available.
- For Firefox, you should install the SADP service and import the certificate according to the instructions and then the online device detection function is available.

1. Click **Physical View → Smart Wall** to enter the smart wall management page.
2. Click **Add** on Decoding Device panel to enter the Add Decoding Device page.
3. Select **Online Devices** as Adding Mode.
4. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the VSM server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
5. Check the checkbox of the device(s) to be added.

Note

- For the inactive device, you need to create the password for it before you can add it properly. For detailed steps, see .
- If the detected devices have the same password and user name, you can add multiple devices at a time. Otherwise, you can add them one by one.

6. Enter the required information.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Finish adding the decoding device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
8. **Optional:** Perform the following operations after adding the decoding device.

   View Decoding Output

   Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

   Edit

   Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address.

   Remote Configurations

   Click ⚙ to set the remote configurations of the device.

   Note

   For detailed operations, see the user manual of the device.

   Delete

   Click × to delete the device.

Add Decoding Device by IP Address

When you know the IP address of the decoding device to add, you can add the device to your system by specifying IP address, user name, password and other related parameters. This adding mode requires you to add the devices one by one, so it is a good choice if you only want to add a few devices and know all the details mentioned above.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.
2. Click **Add** to enter the Add Decoding Device page.
3. Select **IP Address** as Adding Mode.
4. Enter the required information.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   The IP address of the device.

   Device Port

   The port number on which to scan. The default is 8000.

   If the device is located behind a NAT (Network Address Translation)-enabled router or a firewall, you may need to specify a different port number. In such cases, remember to configure the router/firewall so it maps the port and IP address used by the device.

   Alias

   Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
6. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit	Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address.
Remote Configurations	Click ⚙ to set the remote configurations of the device. **Note** For detailed operations, see the user manual of the device.
Delete	Click × to delete the device.

Add Decoding Devices by IP Segment

If multiple decoding devices to add have the same port number, user name and password, but have different IP addresses, which are within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start IP address to the end IP address for the devices in order to add them quickly.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.
2. Click **Add** to enter the Add Decoding Device page.

3. Select **IP Segment** as Adding Mode.
4. Enter the required information.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   Enter the start IP address and end IP address where the devices are located.

   Device Port

   The same port number of the devices. By default, the device port No. is 8000.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

⚠ Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
6. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit	Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address.
Remote Configurations	Click ⚙ to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete Click × to delete the device.

Add Decoding Devices by Port Segment

When multiple decoding devices to add have the same IP address, user name and password, but have different port numbers, which are within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

Before You Start

Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.
2. Click **Add** to enter the Add Decoding Device page.
3. Select **Port Segment** as Adding Mode.
4. Enter the required information.

   Access Protocol

   Select **Hikvision Protocol** to add the devices and select **ONVIF Protocol** to add the third-party devices.

   Device Address

   The same IP address where the devices are located.

   Device Port

   Enter the start port number and the end port number on which to scan.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to X-VMS using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   Caution

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your

password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Finish adding the device
- Click **Add** to add the decoding device and back to the decoding device list page.
- Click **Add and Continue** to save the settings and continue to add other decoding devices.

After adding the decoding device, the device will display in the list on Decoding Device panel.

6. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output
Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .

Edit
Click ✎ to edit the decoding device. You can modify the network location as LAN IP address or WAN IP address.

Remote Configurations
Click ⚙ to set the remote configurations of the device.

ℹ **Note**

For detailed operations, see the user manual of the device.

Delete
Click × to delete the device.

9.10.2 Configure Cascade

In some actual scenarios for large screen display, the screen number of the smart wall will exceed the decoding output number of one decoder, or the cross-decoder functions such as roaming and spanning are required. You can cascade two decoders with video wall controller to meet various display demands.

Before You Start

- Make sure the devices you are going to use are correctly installed and connected to the network as specified by the manufacturers. Such initial configuration is required in order to be able to connect the devices to the X-VMS via network.
- The decoders' interfaces have be connected with the video wall controller's using the matched wires.
- The decoders and video wall controller are added to the X-VMS. Refer to ***Add Decoding Device*** for details.

Perform this task when you need to configure cascade for the decoding devices as follows.

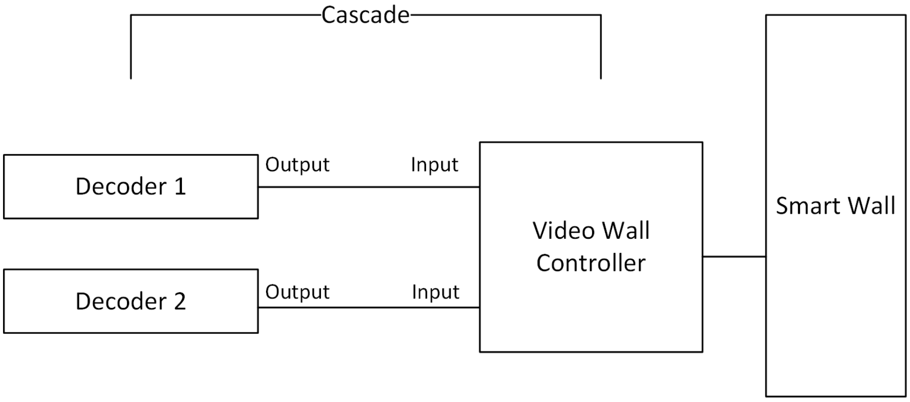


Figure 9-25 Cascade

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.

   The added decoding device(s) and the added smart wall will display.
2. Click ⧉ behind the added video wall controller to enter the Cascading page.

   Note

   Only video wall controller DS-CS10S and DS-C10S-T can support this function.
3. Select the signal channel of the video wall controller and click ⧉ .
4. Select the decoding output of the decoders to set it as the signal input of the video wall controller.

   Note

   If the decoders are cascaded with video wall controller, the spared decoding outputs of the decoders cannot be used to display on smart wall any more.
5. Click **Save** to save the cascade.

Result

After configuring cascade, you need to add a smart wall and link the decoding outputs of the video wall controller to display the signal outputs of the two decoders on the smart wall.

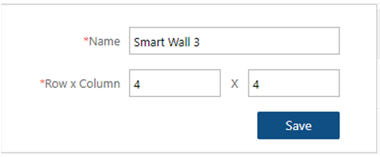
9.10.3 Add Smart Wall

You can add the smart wall to the system and configure its row and column.

Perform this task when you need to add a smart wall to the system.

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.
2. Click **Add** on Smart Wall panel to open the Add Smart Wall dialog.



*Name: Smart Wall 3

*Row x Column: 4 X 4

Figure 9-26 Add Smart Wall Dialog

3. Set the name for the smart wall.
4. Set the row number and the column number.
5. Click **Save**.
6. **Optional:** Perform the following operations after adding the decoding device.

Link Decoding Output with Window — For details about the operations, see ***Link Decoding Output with Window*** .

Edit Smart Wall — Edit the name of the smart wall.

Delete Smart Wall — Delete the smart wall.

9.10.4 Link Decoding Output with Window

After adding the decoding device and smart wall, you should link the decoding device's decoding output to the window of the smart wall.

Perform this task when you need to link the decoding output to the smart wall.

Steps

1. Click **Physical View → Smart Wall** to enter the smart wall management page.

   The added decoding device(s) and the added smart wall will display.
2. Click › in front of the decoding device to show the decoding outputs.
3. Click › in front of the smart wall to show the windows.
4. Drag the decoding output from the Decoding Device panel to the display window of the smart wall, to configure the one-to-one correspondence.
5. **Optional:** Click ☒ to release the linkage.

Chapter 10 Manage Area

X-VMS provides areas to manage the added resources in different groups. You can group the resources into different areas according to the resources' locations. For example, on the 1st floor, there mounted 64 cameras, 16 access points, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named 1st Floor) for convenient management. You can get the live view, play back the video files, and do some other operations of the devices after managing the resources by areas.

Note

If the current system is a Central System with a Remote Site Management module, you can also manage the areas on a Remote Site and add cameras on Remote Site into areas.

10.1 Add Area

You should add an area before managing the elements by areas.

10.1.1 Add Area for Current Site

You can add an area for current site to manage the devices.

Perform this task when you need to add an area for current site.

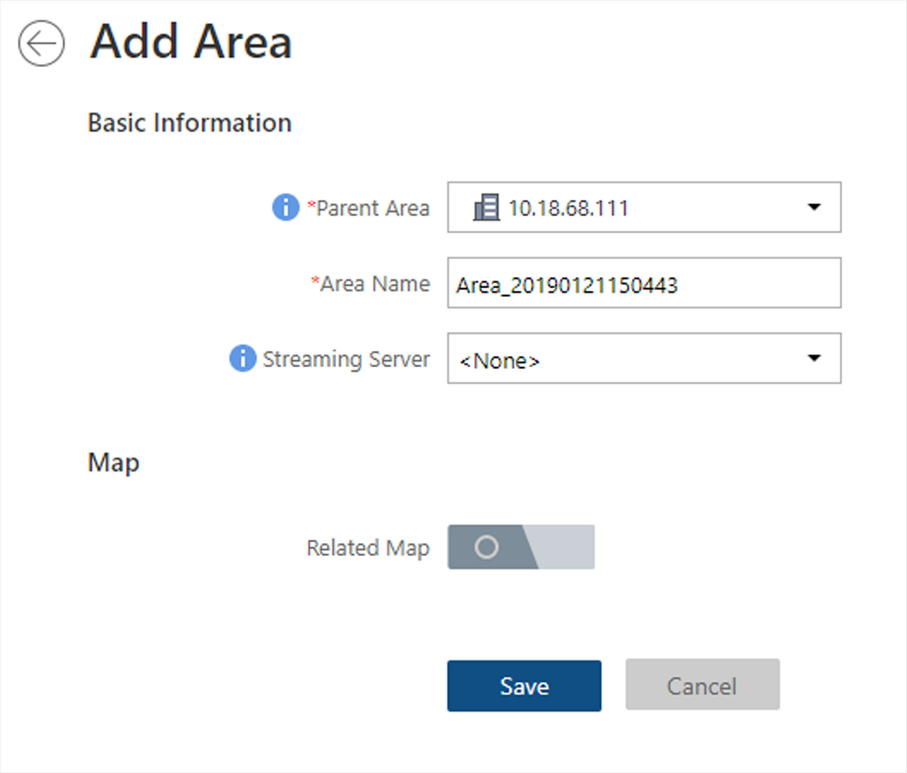
Steps

1. Click **Logical View** on the Home page to enter the Logical View page.
2. **Optional:** Select the parent area in the area list panel to add a sub area.

   Note

   - For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
   - The icon 🌐 indicates that the site is a current site.

3. Click + on the area list panel to open the Add Area window.



Add Area

Basic Information

*Parent Area: 10.18.68.111

*Area Name: Area_20190121150443

Streaming Server: <None>

Map

Related Map

Figure 10-1 Add Area for Current Site

4. Select the parent area to add a sub area.
5. Create a name for the area.
6. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
7. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** to display the area's resources on the smart wall via this Streaming Server.
8. **Optional:** Set the **Related Map** switch to ON and link e-map(s) to area. See ***Link E-Map to Area*** for details.
9. Click **Save**.
10. **Optional:** After adding the area, you can do one or more of the following:

Edit Area Click to edit the area.

Delete Area Click to delete the selected area.

Note

After deleting the area, the resources in the area (cameras, alarm inputs, alarm outputs, access points, and UVSSs) will be removed from the area, as well as the corresponding recording settings, event settings, and map settings.

Search Area Enter a keyword in the search field to search the area.

10.1.2 Add Area for Remote Site

You can add an area for Remote Site to manage the devices in the Central System.

Perform this task when you need to add area for the Remote Site.

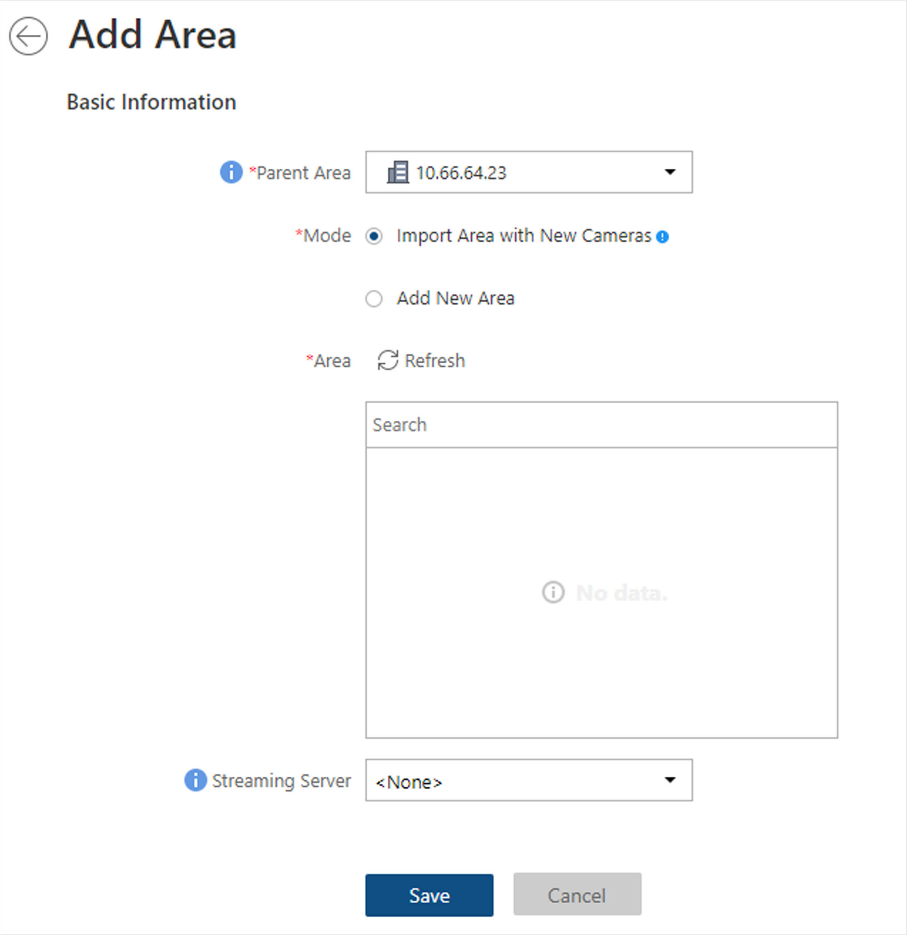
Steps

1. Click **Logical View** on the Home page to enter the Logical View page.
2. In the area list panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is Remote Site.

3. Click + on the area list panel to open the Add Area window.



Add Area

Basic Information

*Parent Area: 10.66.64.23

*Mode: ● Import Area with New Cameras ○ Add New Area

*Area: Refresh

Search

No data.

Streaming Server: <None>

Figure 10-2 Add Area for Remote Site

4. Select the parent area to add a sub area.
5. Set the adding mode for adding the area.

Import Area with New Cameras

If there are some cameras newly added to the areas on a Remote Site, you can import the areas as well as those newly added cameras. The areas with newly added cameras will display and you can select the areas to add.

Add New Area

Add a new area to the parent area.

6. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
7. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** if you want to display the area's resources on the smart wall via this Streaming Server.
8. Click **Save**.
9. After adding the area, you can do one or more of the following:

Edit Area Click ✎ to edit the area.

Delete Area Click 🗑 to delete the selected area.

Note

After deleting the area, the cameras will be removed from the area, as well as the corresponding recording settings and event settings.

Search Area Enter a keyword in the search field to search the area.

10.2 Add Element to Area

You can add elements including cameras, alarm inputs, alarm outputs, access points, and under vehicle surveillance systems into areas for management.

10.2.1 Add Camera to Area for Current Site

You can add cameras to areas for the current site. After managing cameras into areas, you can get the live view, play the video files, and so on.

Before You Start

The devices need to be added to the X-VMS for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Perform this task when you need to add current site's cameras to areas.

Steps

Note

One cameras can only belong to one area. You cannot add a camera to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding cameras to.

Note

- For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
- The icon 🌐 indicates that the site is current site.

3. Select the **Cameras** tab.
4. Click **Add** to enter the Add Camera page.
5. Select the device type as **Encoding Device** or **Security Control Device**.

Note

Some security control devices, such as the panic alarm stations, also contain the cameras.

6. Select the cameras to add.
7. **Optional:** Check **Get Device's Recording Settings** to obtain the recording schedule configured on the local device and the device can start recording according to the schedule.

Note

If the recording schedule configured on device is not continuous recording, it will be changed to event recording on the local device.

8. **Optional:** Check **Add to Map** to add the camera to the map.
9. Click **Add**.
10. **Optional:** After adding the cameras, you can do one or more of the followings

Get Camera Name	Select the cameras and click **Get Camera Name** to get the cameras' names from the device in a batch.
Move to Other Area	Select the cameras and click **Move to Other Area**. Then select the target area to move the selected cameras to and click **Move**.
Display Cameras of Child Areas	Check **Include Sub-area** to display the cameras of child areas.

10.2.2 Add Camera to Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can also add cameras from Remote Sites to areas in Central System for management.

Before You Start

Encoding devices need to be added to the X-VMS for area management. Refer to ***Manage Encoding Device*** for detailed configuration about adding devices.

Perform this task when you need to add Remote Site's camera to central area.

Steps

Note

Cameras can only belong to one area. You cannot add a camera to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added Remote Site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is Remote Site.

3. Select an area for adding elements to.
4. Click **Add** to enter the Add Camera page.
5. Select the cameras to add.

   Note

   Up to 64 cameras can be added to one area.

6. Click **Add**.
7. **Optional:** After adding the cameras, you can do one or more of the following:

   Synchronize Camera Name
   Select the cameras and click ⇅ to get the cameras' names from the device in a batch.

   Move to Other Area
   Select the cameras and click ⇱ . Then select the target area to move the selected cameras to and click **Move**.

   Display Cameras of Child Areas
   Select **Include Sub-area** to display the cameras of child areas.

10.2.3 Add Access Point to Area for Current Site

You can add access points to areas for the current site for management.

Before You Start

Access control devices need to be added to the X-VMS for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Perform this task when you need to add current site's access points to areas.

Steps

Note

One access point can only belong to one area. You cannot add a access point to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding access points to.

Note

- For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
- The icon 🌐 indicates that the site is current site.

3. Select the **Access Points** tab.
4. Click **Add** to enter the Add Access Point page.
5. Select the access point(s) to add.
6. **Optional:** Check **Get Access Point Name** to get the access point name from the device.
7. **Optional:** Check **Add to Map** to add the access point to the map.
8. Click **Add**.
9. **Optional:** After adding the access points, you can do one or more of the followings.

Get Access Point Name	Select the access points and click **Get Access Point Name** to get the access points' names from the device in a batch.
Move to Other Area	Select the access points and click **Move to Other Area**. Then select the target area to move the selected access points to and click **Move**.
Display Access Point of Child Areas	Check **Include Sub-area** to display the access points of child areas.

10.2.4 Add Alarm Input to Area for Current Site

You can add alarm inputs to areas for the current site for management.

Before You Start

Devices need to be added to the X-VMS for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Perform this task when you need to add current site's alarm inputs to areas.

Steps

Note

Alarm input can only belong to one area. You cannot add an alarm input to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding alarm inputs to.

Note

- For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
- The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Inputs** tab.

4. Click **Add** to enter the Add Alarm Inputs page.
5. Select the device type.
6. Select the alarm inputs to add.

Note

For the security control device, you need to select its zones as alarm inputs to add to the area.

7. **Optional:** Check **Add to Map** to add the alarm input to the map.
8. Click **Add**.
9. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

Move to Other Area	Select the alarm inputs and click **Move to Other Area**. Then select the target area to move the selected alarm inputs to and click **Move**.
Display Alarm Inputs of Child Areas	Check **Include Sub-area** to display the alarm inputs of child areas.

10.2.5 Link Alarm Inputs to Security Control Partition

After adding the security control device's zones to the system (called "alarm inputs" after added to the system), you should link them to different security control partitions in the system according to the relation between zones and partitions configured on the device. After grouping alarm inputs into security control partitions in the system, you can set one defense schedule for the alarm inputs in a security control partition. The defense schedule defines when and how to arm the alarm inputs in this security control partition. For example, area 1 is created for the first floor, and all the resources on the first floor are managed in area 1. If there is one security control device mounted on the first floor, you should add its zones into area 1 first, then link the zones (alarm inputs) into security control partitions and set a defense schedule to these security control partitions. After that, the zones (alarm inputs) can be armed according to the schedules respectively.

Before You Start

Make sure the security control device's zones are added to the system and grouped into areas. For details, refer to ***Add Alarm Input to Area for Current Site*** .

Steps

1. Click **Logical View** on the home page.
2. Select one area which contains alarm inputs you want to set a defense schedule for and click ✎ to enter the editing area page.
3. In the Security Control Partition field, click **Add**.
4. Create a name for the security control partition.
5. In the drop-down list of Alarm Input field, select a security control device.

   The alarm inputs of the security control device added to this area and haven't been added to any security control partitions are displayed.

6. Select the alarm inputs which you want to add to the security control partition.
7. Select a security control partition No. in the drop-down list which is gotten from the device you selected in Step 5.
8. **Optional:** Set a defense schedule for this partition, which defines how and when to arm the alarm inputs in the security control partition.

Note

For setting a new defense schedule, refer to ***Configure Defense Schedule Template*** .

9. Click **Add**.

10.2.6 Add Alarm Output to Area for Current Site

You can add alarm outputs to areas for the current site for management. When the alarm or event linked with the alarm output is detected, the alarm devices (e.g., the siren, alarm lamp, etc.) connected with alarm output will make actions. For example, when receiving the alarm out signal from the system, the alarm lamp will flash.

Before You Start

Devices need to be added to the X-VMS for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Perform this task when you need to add current site's alarm outputs to areas.

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding alarm outputs to.

Note

- For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
- The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Outputs** tab.
4. Click **Add** to enter the Add Alarm Outputs page.
5. Select the device type.
6. Select the alarm outputs to add.
7. **Optional:** Check **Add to Map** to add the alarm output to the map.
8. Click **Add**.
9. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

Move to Other Area	Select the alarm outputs and click **Move to Other Area**. Then select the target area to move the selected alarm outputs to and click **Move**.
Display Alarm Outputs of Child Areas	Check **Include Sub-area** to display the alarm outputs of child areas.

10.2.7 Add UVSS to Area for Current Site

You can add Under Vehicle Surveillance Systems (UVSSs) to areas for the current site for management.

Perform this task when you need to add Current Site's UVSSs to areas.

Steps

Note

UVSSs can only belong to one area. You cannot add a UVSS to multiple areas.

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area for adding UVSSs to.

   Note

   - For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
   - The icon 🌐 indicates that the site is current site.

3. Select the **Under Vehicle Surveillance Systems** tab.

   Note

   If the map function is enabled, you can click » and click **UVSSs**.

4. Click **Add** to enter the Add UVSS page.
5. Input the required information of UVSS.
6. Link cameras to the UVSS.
   1) Set **Relate Camera** switch to ON.
   2) Select the cameras.
7. Check **Add to Map** to add the UVSS on the map.
8. Click **Add**.

10.3 Edit Element in Area

You can edit the area's added elements, such as recording settings, event settings, and map settings for cameras, application settings, hardware settings, and attendance settings for doors, and so on.

10.3.1 Edit Camera for Current Site

You can edit basic information, recording settings, picture storage settings, event settings, and map settings of the camera for current site. You can also edit the face comparison group settings of the cameras which support face picture comparison.

Perform this task when you need to edit camera for current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Cameras** tab to show the added cameras.
5. Click **Name** column to enter the Edit Camera page.
6. Edit the camera's basic information, including camera name and protocol type.
7. **Optional:** Click ▶ to view the live view of the camera and hover over the window and click ▶ in the lower-right corner to switch to playback.

   Note

   The live view and playback functions in the camera details page are only supported by Internet Explorer.

8. Edit the recording settings of the camera. See ***Configure Recording*** for details.

   Note

   If no recording settings have been configured for the camera, you can click **Configuration** to set the parameters.

9. **Optional:** For cameras which support face picture comparison, you can edit the face comparison group settings.
   1) Set the person group for face comparison. You can delete the applied group and view the group details.

Note

If no face comparison group has been applied to the camera, you can click **Apply Face Configuration Group**. See ***Apply Face Comparison Group to Device*** for details.

2) Set the face comparison similarity threshold which affects the frequency and accuracy of face picture comparison alarm.

10. **Optional:** Set the **Picture Storage** switch to ON and select the storage location from the drop-down list for storing the pictures uploaded from the camera to the specified location.

Note

Refer to ***Configure Storage for Uploaded Pictures*** for details.

11. Edit the event settings of the camera. See ***Configure Event and Alarm*** for details.

Note

If no event settings have been configured for the camera, you can click **Configuration** to set the parameters.

12. Add the camera to the map.
    1)Set the **Add to Map** switch to ON.
    2)Select the icon style and name color for displaying the camera on the map.
13. **Optional:** Click **Configuration on Device** to set the remote configurations of the corresponding device if needed.

Note

For details about the remote configuration, refer to the user manual of the device.

14. Click **Save**.
15. **Optional:** Enter Edit Camera page again and click **Copy to** to select configuration item and copy the settings of this camera to other cameras.

10.3.2 Edit Access Point for Current Site

You can edit basic information, related cameras, application settings, hardware settings, access level, attendance settings, event settings, and map settings of the access point for current site.

Perform this task when you need to edit the access point for current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Access Points** tab to show the added access points.
5. Click Name column to enter the Edit Access Point page.
6. Edit the access point's basic information.

   Door Contact

   The door contact's connection mode.

   Exit Button Type

   The exit button connection mode.

   Open Duration(s)

   The time interval between the access point is unlocked and locked again.

   Extended Open Duration(s)

   The time interval between the access point is unlocked and locked again when the person's extended access function enabled.

   Door Open Timeout Alarm

   After enabled, if the access point has configured with event or alarm, when the door contact open duration has reached the limit, the event or alarm will be uploaded to the system.

   Duress Code

   If you enter this code on the card reader keypad, the Control Client will receive an duress event. It should be different with the super password and dismiss code.

   Super Password

   If you enter this password on the card reader keypad, you are exempted from all the remaining locked (Credential Failed), anti-passback, and first card authorization restrictions. It should be different with the duress code and dismiss code.

   Dismiss Code

   If you enter this code on the card reader keypad, the buzzer's beeping will be stopped. It should be different with the duress code and super password.

   Free Access Schedule

   During this schedule, the access point remains open. User can enter or exit via the access point without any credentials. For turnstile, you can set schedules for entrance and exist respectively.

7. Link the cameras to the access point, and you can view its live view, recorded video, captured pictures via the Control Client.

   Note

   Up to two cameras can be related to one access point.

8. Edit the application settings.

   Anti-passback

The person should exit via the access point in the anti-passback if he/she enters via the access point in the anti-passback. It minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. For setting the anti-passback rule, refer to ***Configure Anti-Passback Rules*** .

Open Door with First Card

After swiping the first card, the access point will remain unlocked or be authorized. The status depends on the card swiping times (odd or even). For odd, the access point will remain unlocked or be authorized. For even, it will exit the unlocked or authorized mode.

9. Edit the hardware settings.

1) Set the **Card Reader** switch to ON and set the card reader related parameters.

OK LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for OK core wire connection on the card reader mainboard.

Error LED Polarity

Only supported when the device is connected via Wiegand interface. The polarity for ERR core wire connection on the card reader mainboard.

Buzzer Polarity

Only supported when the device is connected via Wiegand interface. The polarity for buzzer connection on the card reader mainboard.

2) Set the card reader's access mode in normal time periods.

Note

The card reader's access modes should be supported by the device.

Example

If you select **Card**, you should open the access point by swiping the card all the time.

3) **Optional:** When you want to open the access point via another access mode in some special time periods, set the card reader's access mode and select the custom time period.

Example

If you select **Fingerprint** and **Weekend Schedule**, you should open the access point via fingerprint at weekends.

Note

You can add a custom schedule template and up to 3 time periods can be set for each day. See ***Set Access Control Schedule Template*** for details.

4) Set the **Min. Card Swipe Interval** switch to ON and set the interval.

Min. Card Swipe Interval

After enabled, you cannot swipe the same card again within the minimum card swiping interval.

5) Set the maximum time interval of pressing two keys on the keypad. If timed out, the first entry will be reset.
6) Set the **Failed Card Attempts Alarm** switch to ON and set the maximum failed attempts.

Failed Card Attempts Alarm

After enabled, if the access point has configured with event or alarm, when the number of excessive failed card swiping attempts has reached the limit, the event or alarm will be uploaded to the system.

Tampering Detection

After enabled, if the access point has configured with device tampered event or alarm, when the device body or panel is taken apart, the alarm will be triggered and sent to the system.

10. **Optional:** For the access point of the turnstile, set **Face Recognition Terminal** switch to ON and add the face recognition terminals to link the selected access point.
   1)Set the **Face Recognition Terminal** switch to ON to add the face recognition terminals.
   2)Click **Add** to enter Add Face Recognition Terminal page.
   3)Select **IP** or **Online Devices** as the adding mode, and set the required parameters, which may vary according to different terminals.
   4)Click **Add** to link the terminal to access point.

Note

After adding to the terminal list, you can edit, delete the devices, or do other further operations.

11. Add the access point to one access level.
12. Set the access point as attendance check point.
13. Edit the event settings of the access point. See ***Configure Event and Alarm*** for details.

Note

If no event settings have been configured for the access point, you can click **Configuration** to set the parameters.

14. Add the access point to the map.
   1)Set the **Add to Map** switch to ON.
   2)Select the icon style and name color for displaying the access point on the map.

Note

Up to 128 access points can be added to one map.

15. Click **Save**.
16. **Optional:** If required, enter the Edit Access Point page again and click **Copy to** to apply the current settings of the access point to other access point(s).

10.3.3 Edit Alarm Input for Current Site

You can edit basic information, event settings, and map settings of the alarm input for current site.

Perform this task when you need to edit alarm input for current site.

Steps

1. Click **Logical View** on the Home Page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Inputs** tab to show the added alarm inputs.
4. Click Name column to enter the Edit Alarm Input page.
5. Edit the alarm input name.
6. **Optional:** For the alarm input of the security control device, select **Detector Type** and **Zone Type** according to the actual deployment.
7. Edit the event settings of the alarm input. See ***Configure Event and Alarm*** for details.

   Note

   If no event settings have been configured for the alarm input, you can click **Configuration** to set the parameters.

8. Add the alarm input to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the alarm input on the map.
9. Click **Save**.

10.3.4 Edit Alarm Output for Current Site

You can edit basic information and map settings of the alarm output for current site.

Perform this task when you need to edit alarm output for current site.

Steps

1. Click **Logical View** on the Home Page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is current site.

3. Select the **Alarm Outputs** tab to show the added alarm outputs.
4. Click Name column to enter the Edit Alarm Output page.

5. Edit the alarm output name.
6. Add the alarm output to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the alarm output on the map.
7. Click **Save**.

10.3.5 Edit Under Vehicle Surveillance System for Current Site

You can edit basic information, related cameras, and map settings of the Under Vehicle Surveillance System (UVSS) for current site.

Perform this task when you need to edit UVSS for current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon 🌐 indicates that the site is current site.

3. Select an area.
4. Select the **Under Vehicle Surveillance Systems** tab to show the added UVSSs.

   Note

   If the map function is enabled, you should click » and click **UVSSs**.

5. Click Name column to enter the Edit UVSS page.
6. Edit the UVSS's basic information, such as IP address, port No., and so on.
7. Link cameras to the UVSS.
   1) Set the **Relate Camera** switch to ON.
   2) Select the camera(s).
8. Add the UVSS to the map.
   1) Set the **Add to Map** switch to ON.
   2) Select the icon style and name color for displaying the UVSS on the map.
9. Click **Save**.

10.3.6 Edit Element for Remote Site

If the current system is a Central System with Remote Site Management module, you can edit the cameras added from the Remote Site.

Perform this task when you need to edit the camera parameters for the Remote Site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.

2. In the area list panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a Remote Site.

3. Select an area to show its added cameras.
4. Click the Name field to edit the parameters of the cameras including basic information and recording settings.

Note

For recording settings, if no recording settings have been configured for the camera, click **Configuration** to set the parameters (for details, refer to ***Configure Recording for Cameras on Remote Site***).

5. **Optional:** Click ▶ to view the live view of the camera and hover over the window and click in the lower-right corner to switch to playback.

Note

The live view and playback functions in the camera details page are only supported by Internet Explorer.

6. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.
7. Click **Save**.

10.4 Remove Element from Area

You can remove the added cameras, alarm inputs, alarm outputs, doors, and Under Vehicle Surveillance Systems (UVSSs) from the area.

10.4.1 Remove Element from Area for Current Site

You can remove the added cameras, alarm inputs, alarm outputs, doors, and UVSSs from the area for current site.

Perform this task when you need to remove the element from the area for the current site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. Select an area in the area list panel to show its added elements.

Note

- For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
- The icon 🌐 indicates that the site is the current site.

3. Select the Cameras, Alarm Inputs, Alarm Outputs, Doors, or UVSSs tab to show the added elements.
4. Select the elements.
5. Click **Delete**.

10.4.2 Remove Element from Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can remove the added cameras from its area.

Perform this task when you need to remove the element from the area for the Remote Site.

Steps

1. Click **Logical View** on the Home page to enter the Area Management page.
2. In the area list panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon 🌐 indicates that the site is a Remote Site.

3. Select an area to show its added cameras.
4. Select the cameras.
5. Click **Delete**.
6. **Optional:** If ⊗ appears near the camera name, it means the camera has been deleted from the Remote Site. Hover the cursor over the ⊗ and click **Delete** to delete the camera from the area.

10.5 Configure Defense Schedule Template

The defense schedule defines the arming mode in different time periods for the partitions of the added security control devices. You can set a weekly schedule to schedule time periods for stay arming, instant arming, or away arming in one week. The system predefines two default defense schedule templates: All-day Template and Weekday Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page and enter **Schedule → Defense Schedule Template** page.
2. Click **Add** to enter the adding defense schedule template page.

Note

You can add up to 10 templates.

3. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

4. Select an arming mode and drag on the time bar to draw a time period.

   Note

   By default, the Time-based is selected.

   Instant Arming

   It is used when people leave the detection area. The zone will be immediately triggered when it detects event or alarm with no delay and notify the security personnel.

   Away Arming

   It is used when people leave the detection area. Event or alarms will be activated when the zone is triggered or tampered. For delayed zone, the alarm will not be activated when the zone detects triggering event during entry/exit delay.

   Stay Arming

   It is used when people stay inside the detection area. During stay arming, all the perimeter burglary detections (such as perimeter detector, magnetic contacts, curtain detector in the balcony) will be turned on. Meanwhile, the detectors inside the detection area are bypassed (such as PIR detectors). People can move inside the area and not trigger an event or alarm.

   Note

   Up to 8 time periods can be set for each day.

5. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
6. Finish adding the defense schedule template.
   - Click **Add** to add the template and back to the defense schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The defense schedule template will be displayed on the defense schedule template list.

7. **Optional:** Perform the following operations after adding the template.

View Template Details	Click the template to view its details.
Edit Template	Click ✎ in the Operation column to edit template details (except the template(s) in use).

Delete Template Click × in the Operation column to delete the template.

Delete All Templates Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

Chapter 11 Configure Recording

Recording settings are for defining when and how the recording starts with the pre-defined parameters. You can also configure the storage settings for storing imported pictures and uploaded pictures.

X-VMS provides four storage locations (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, or pStor) for storing the recorded video files of the cameras.

Encoding Device

The encoding devices, including the DVRs, NVRs, and network cameras, should provide storage devices such as the HDDs, Net HDDs, and SD/SDHC cards for video files. The newly installed storage devices need to be formatted. Go to the remote configuration page of the device (**Physical View → Configuration**), click **Storage → General** , select the HDD, Net HDD or SD/SDHC card, and click **Format** to initialize the selected storage device.

Hybrid Storage Area Network

Store the video files in the added Hybrid Storage Area Network. For details about adding Hybrid Storage Area Network, refer to ***Add Hybrid Storage Area Network*** .

Cloud Storage Server

Store the video files in the added Cloud Storage Server. For details about adding Cloud Storage Server, refer to ***Add Cloud Storage Server*** .

pStor

Store the video files in the added pStor, which is the storage access service used for managing local HDDs and logical disks. For details about adding pStor, refer to ***Add pStor*** .

11.1 Configure Recording for Cameras on Current Site

For the cameras on the current site, X-VMS provides four storage methods (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, or pStor) for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding camera to an area.

Before You Start

Encoding devices need to be added to the X-VMS for area management. Refer to ***Manage Resource*** for detailed configuration about adding devices.

Perform this task when you need to record videos for the cameras on the current site.

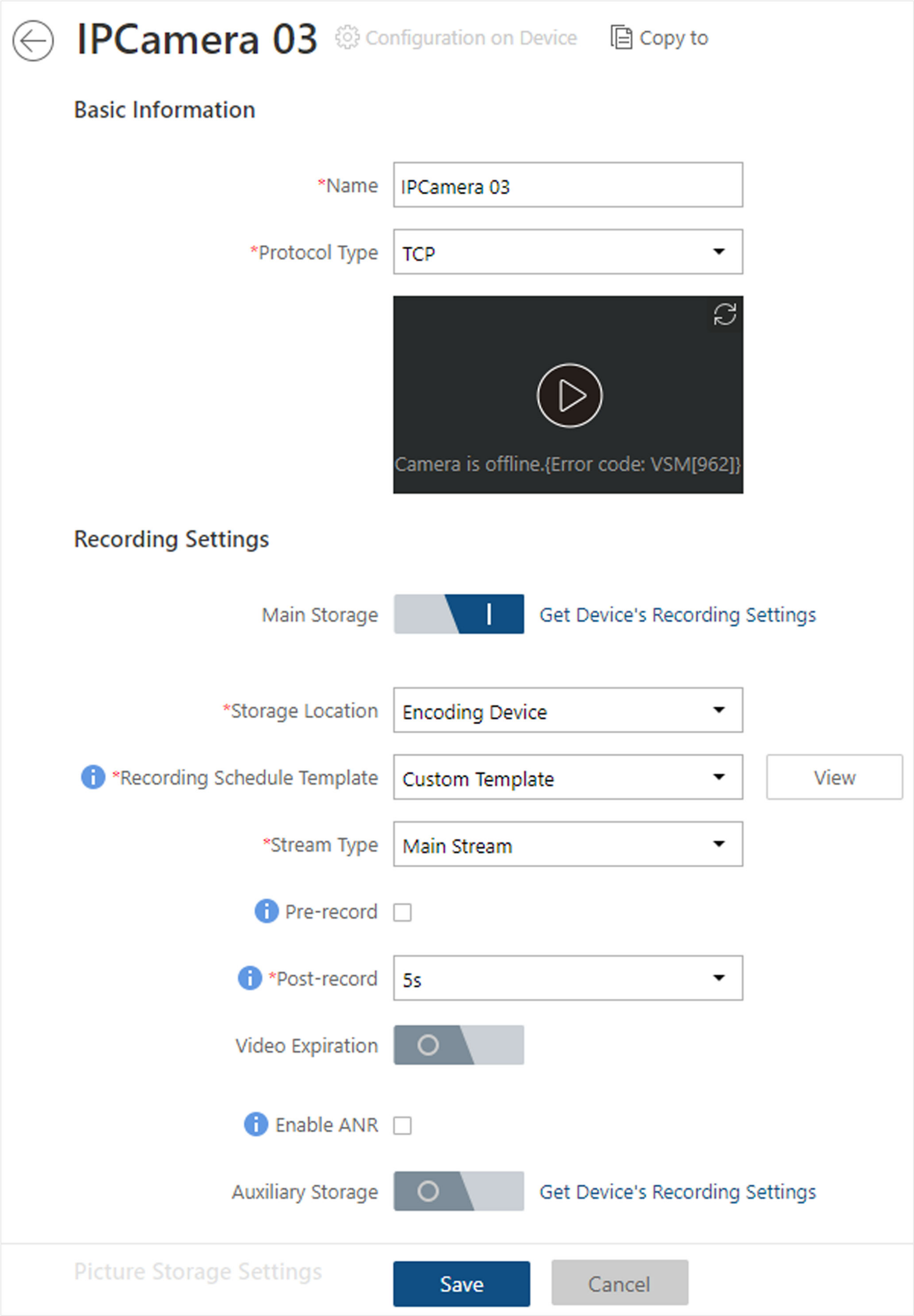
Steps

1. Enter the recording setting page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select an area to show its cameras.

Note

For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.

3) Select a camera and click the Name field to enter the Edit Camera page.



IPCamera 03

Basic Information

*Name: IPCamera 03

*Protocol Type: TCP

Camera is offline.{Error code: VSM[962]}

Recording Settings

Main Storage: ON — Get Device's Recording Settings

*Storage Location: Encoding Device

*Recording Schedule Template: Custom Template

*Stream Type: Main Stream

Pre-record: □

*Post-record: 5s

Video Expiration: OFF

Enable ANR: □

Auxiliary Storage: OFF — Get Device's Recording Settings

Figure 11-1 Edit Camera Page

2. Set the **Main Storage** switch to ON.
3. Select the storage location for storing the recorded video file.

Note

If you select **Hybrid Storage Area Network**, **Cloud Storage Server** or **pStor**, specify a server and (optional) select a Streaming Server to get the video stream of the camera via it.

4. Select the storage type and configure the required parameters.
   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

     Note

     If you choose **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.

     Recording Schedule Template

     Set the template which defines when to record the camera's video.

     All-Day Time-Based Template

     Record the video for all-day continuously.

     All-Day Event-Based Template

     Record the video when alarm occurs.

     Add New

     Set the customized template. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

     View

     View the template details.

     Note

     The event-based recording schedule can not be configured for the **Cloud Storage Server**, and the command-based recording schedule can not be configured for the **Cloud Storage Server** and **pStor**.

     Stream Type

     Select the stream type as main stream, sub-stream or dual-stream.

     Note

     For storing on Hybrid Storage Area Network, Cloud Storage Server or pStor, dual-stream is not supported.

     Pre-Record

     Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

     This field displays when the storage location is set as Encoding Device or pStor, and it is available for the camera that is configured with event-based recording.

Post-Record

Record video from periods following detected events.

This field displays when the storage location is set as Encoding Device or Hybrid Storage Area Network. It is available for the camera that is configured with event-based recording.

Video Expiration

If you select **Encoding Device** as the storage location , set Video Expiration switch to ON and enter expiration day(s).

Automatically delete the oldest videos after the specified retention period. This method allows you to define the longest time period to keep the videos as desired and the actual retention period for the videos depends on the allocated quota.

Enable ANR

If you select the **Encoding Device** or **Hybrid Storage Area Network** as the storage location, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network fails and transport the video to storage device when network recovers.

- Select **Scheduled Uploading** as the storage type to upload the recorded video files from the encoding device or pStor to the specified storage location according to scheduled period

Note

- Make sure you have configured recording schedule stored in the device local storage or pStor for auxiliary storage first. Otherwise, the schedule uploading is not configurable.
- The recordings can be uploaded only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server or pStor, or from pStor to another pStor.

Upload between

Specify the time period to upload the recorded video files to the specified storage location during the period.

Recording for Uploading

Select the recorded video file type to backup.

5. **Optional:** Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

Note

- If Cloud Storage Server, Hybrid Storage Area Network, or pStor is set as the auxiliary storage location, you can select **Real-Time Storage** to store recorded vide files or select **Scheduled Uploading** to upload recordings from the encoding device or pStor (main storage) to specified auxiliary storage location according to the scheduled period.
- Before setting **Scheduled Uploading**, make sure you have configured real-time recording schedule stored in device local storage or pStor for the main storage.
- The recordings can be uploaded only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server or pStor, or from pStor to another pStor.

6. Click **Save**.

11.2 Configure Recording for Cameras on Remote Site

You can set recording schedule to record the video of cameras on Remote Sites and stores in the Central System's Recording Servers (Hybrid Storage Area Network, Cloud Storage Server, or pStor).

Perform this task when you need to record videos for the cameras on the Remote Site.

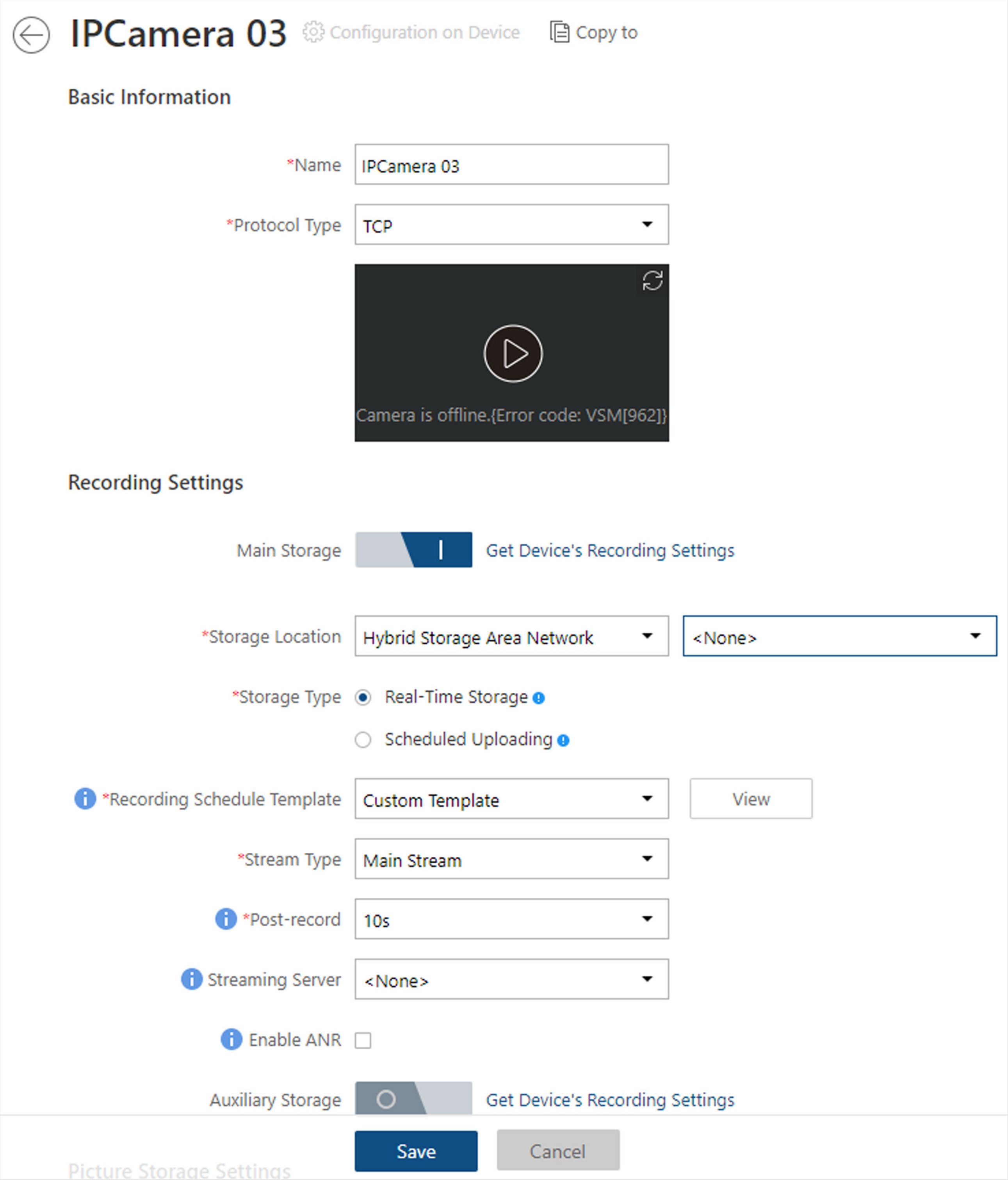
Steps

1. Enter the recording setting page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select the added Remote Site form the drop-down list.

   Note

   The icon 🌐 indicates that the site is Remote Site.

   3) Select an area to show its cameras.
   4) Select a camera and click the **Name** field to enter the Edit Camera page.
   5) In the Recording Settings area, set **Storage in Central System** switch to ON to show the recording setting area.



IPCamera 03 Configuration on Device Copy to

Basic Information

*Name: IPCamera 03

*Protocol Type: TCP

Camera is offline.{Error code: VSM[962]}

Recording Settings

Main Storage: on — Get Device's Recording Settings

*Storage Location: Hybrid Storage Area Network; <None>

*Storage Type: ● Real-Time Storage ○ Scheduled Uploading

*Recording Schedule Template: Custom Template — View

*Stream Type: Main Stream

*Post-record: 10s

Streaming Server: <None>

Enable ANR: □

Auxiliary Storage: off — Get Device's Recording Settings

Picture Storage Settings

Figure 11-2 Add Recording Settings Page

2. Select the storage location for storing the recorded video file.

Note

You can select **Hybrid Storage Area Network**, **Cloud Storage Server** or **pStor**, specify a server and (optional) select a Streaming Server to get the video stream of the camera via it.

3. Select the storage type and configure the required parameters.
   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

     Note

     If you choose **Encoding Device** as the storage location, you needn't select the storage type, but configure the following parameters as real-time storage settings by default.

     Recording Schedule Template

     Set the template which defines when to record the camera's video.

     All-Day Time-Based Template

     Record the video for all-day continuously.

     All-Day Event-Based Template

     Record the video when alarm occurs.

     Add New

     Set the customized template. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

     View

     View the template details.

     Stream Type

     Select the stream type as main stream, sub-stream or dual-stream.

     Note

     For storing on Hybrid Storage Area Network, Cloud Storage Server or pStor, dual-stream is not supported.

     Pre-Record

     Record video from periods preceding detected events. For example, when someone opens a door, you can see what happens right before the door opened.

     This field displays when the storage location is set as Cloud Storage Server, and it is available for the camera that is configured with event-based recording.

     Post-Record

     Start recording the video from periods following detected events.

     This field displays when the storage location is set as Hybrid Storage Area Network, and it is available for the camera that is configured with event-based recording.

Streaming Server

Optionally, select a **Streaming Server** to get the video stream of the camera via it.

Enable ANR

If you select the Storage Location as Hybrid Storage Area Network, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network disconnects and transport the video to Hybrid Storage Area Network when network recovers.

- Select **Scheduled Uploading** as the storage type and specify period, main/auxiliary storage, recording type and uploading speed to upload the recorded video files from the device local storage or pStor on the Remote Site to the specified storage location according to scheduled period.

Note

Make sure you have configured recording schedule stored on encoding device or pStor for the camera on the remote site.

4. Click **Save**.

11.3 Configure Storage for Imported Pictures

The pictures imported by the users, such as the original undercarriage pictures imported on Vehicle page, static map pictures, the face pictures in the person list, can be stored on the HDD of VSM server.

Before You Start

Make sure that you have at least 1GB free space for picture storage.

Perform this task when you need to store the imported pictures.

Steps

1. Log into the Web Client running on the VSM server.
2. Click **System → Storage → Storage on VSM Server** to enter the storage on VSM server page.

   Note

   This module displays when the current Web Client is running on VSM server.

   The disks of the VSM server are displayed with the free space and total capacity.
3. Select the HDD to store the imported pictures.
4. **Optional:** Set the **Restrict Quota for Pictures** switch to ON to allocate the quota for storing the pictures.
5. Click **Save**.

11.4 Configure Storage for Uploaded Pictures

The pictures uploaded from the devices, such as alarm triggered pictures, captured face pictures, and captured plate license pictures, can be stored on the HDD of VSM server, Hybrid Storage Area Network, Cloud Storage Server, or pStor.

Perform this task when you need to store the pictures uploaded from the devices.

Steps

1. Enter the picture storage setting page.
   1) Click **Logical View → Cameras** to enter the area management page.
   2) Select an area to show its cameras.

      Note

      For Central System with Remote Site Management module, you can select the current site (marked with 🌐 icon) from the drop-down site list to show its cameras.

   3) Select a camera and click the Name field to enter the Edit Camera page.
2. Set the **Picture Storage** switch to ON to enable the picture storage for the camera.
3. Select the storage location from the drop-down list.

   Note

   - If you select Video Surveillance Management, the pictures will be stored on the VSM server. Click **Configuration** to view the disk on VSM server and storage quota, which can be edited via the Web Client running on the VSM server. Refer to ***Configure Storage for Imported Pictures*** for details.
   - You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

4. Click **Save** to save the uploaded pictures to the specified location.

11.5 Configure Recording Schedule Template

Recording schedule is time arrangement for video recording. You can configure the recording schedules to record video in a certain period. Two default recording schedules are available: All-day Time-based Template and All-day Event-based Template. All-day Time-based Template can be used for recording videos for all day continuously, and All-day Event-based Template is for recording videos when alarm is triggered. You can also customize the recording schedule.

Perform this task when you need to customize the schedule to record the video files.

Steps

1. Click **System** on the home page and enter **Schedule → Recording Schedule Template** page.
2. Click **Add** to enter the adding recording schedule page.

Note

Up to 32 templates can be added.

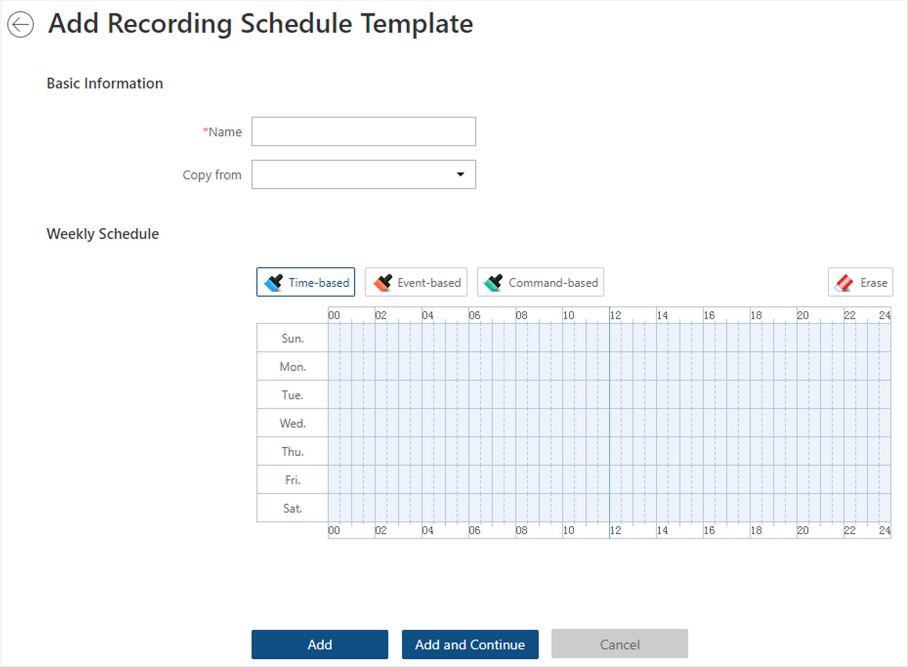


Figure 11-3 Adding Recording Schedule Template Page

3. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

4. Select a recording type and drag on the time bar to draw a time period.

Note

By default, the Time-based is selected.

Time-based

Continuous recording according to the time you arranged. The schedule time bar is marked with blue.

Event-based

The recording triggered by the alarm (e.g., alarm input alarm or motion detection alarm). The schedule time bar is marked with orange.

Command-based

The recording triggered by the ATM command. The schedule time bar is marked with green.

Note

Up to 8 time periods can be set for each day in the recording schedule.

5. **Optional:** Click **Erase** and click on the time bar to clear the drawn time period.
6. Finish adding the template.
   - Click **Add** to add the template and back to the recording schedule template list page.
   - Click **Add and Continue** to save the settings and continue to add other template.
7. **Optional:** Perform the following operations on the recording schedule template list page.

View Template Details
Click the template to check the detailed settings.

Edit Template
Click ✎ in the Operation column to edit template details (except the template(s) in use).

Delete Template
Click × in the Operation column to delete the template.

Delete All Templates
Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

Chapter 12 Configure Event and Alarm

You can set the linkage actions for the detected events and alarms. The detailed information of the events and alarms can be received and checked via the Control Client and the Mobile Client.

Event

Events can be divided into:

System-Monitored Event

The signal that resource (e.g., camera, device, server) sends when something occurs. System can trigger linkage actions (such as recording, capturing, sending email, etc.) to record the received event for checking.

Generic Event

The signal that resource (e.g., other software, device) sends when something occurs, and can be received in the form of TCP or UDP data packages, which the system can analyze, and generate events if they match configured expression.

User-Defined Event

The user-defined event can be used to:

- The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
- A user-defined event can trigger an alarm if configured.
- An alarm will be armed or disarmed when the user-defined event is triggered.
- An alarm can trigger a user-defined event as alarm actions.

Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. An alarm can trigger a series of linkage actions (e.g., popping up window) for notification and alarm handling.

Linkage Actions

You can set linkage actions for both events and alarms.

- An event's linkage actions are used to record the event details (such as recording and capturing) and trigger basic actions (such as linking access point to lock or unlock, triggering alarm output, sending email, etc.).
- An alarm's linkage actions are used to record the alarm details and provide the recipients multiple ways to view alarm information for alarm acknowledgment and handling, such as popping up alarm window, displaying on smart wall, audible warning, etc.

12.1 Configure System-Monitored Event

System-monitored event is the signal that resource (e.g., device, camera, server) sends when something occurs. System can receive and record event for checking, and can also trigger a series of linkage actions for notification. The event can also trigger an alarm for further notification and linkage actions (such as alarm recipients, pop-up window on the Control Client, displaying on the Smart Wall, etc.). You can check the event related video and captured pictures via the Control Client if you set the recording and capturing as event linkage.

It supports the following types of event:

- **Camera Event:** the video exception or the events detected in the monitoring area of the camera, such as motion detection, video loss, line crossing, and so on.
- **Access Point Event:** the access control event triggered at the access point, such as access event, door status event, etc.
- **Alarm Input Event:** the event triggered by the alarm input.
- **ANPR Event:** the license plate matched event and mismatched event detected by the ANPR camera or UVSS.
- **Person Event:** the face matched event and mismatched event detected by the facial recognition camera.
- **UVSS Event:** the event triggered by the UVSS, including getting online or offline.
- **Remote Site Event:** the event triggered by the added Remote Site, including site getting offline.
- **Device Event:** the event triggered by encoding device, access control device, and security control panel's exception.
- **Server Event:** the events triggered by Recording Server, Streaming Server, or X-VMS Server.
- **User Event:** the event triggered by system users, including user login and logout.
- **Generic Event:** the event triggered by the generic event added in the system.
- **User-Defined Event:** the event triggered by the user-defined event added in the system.

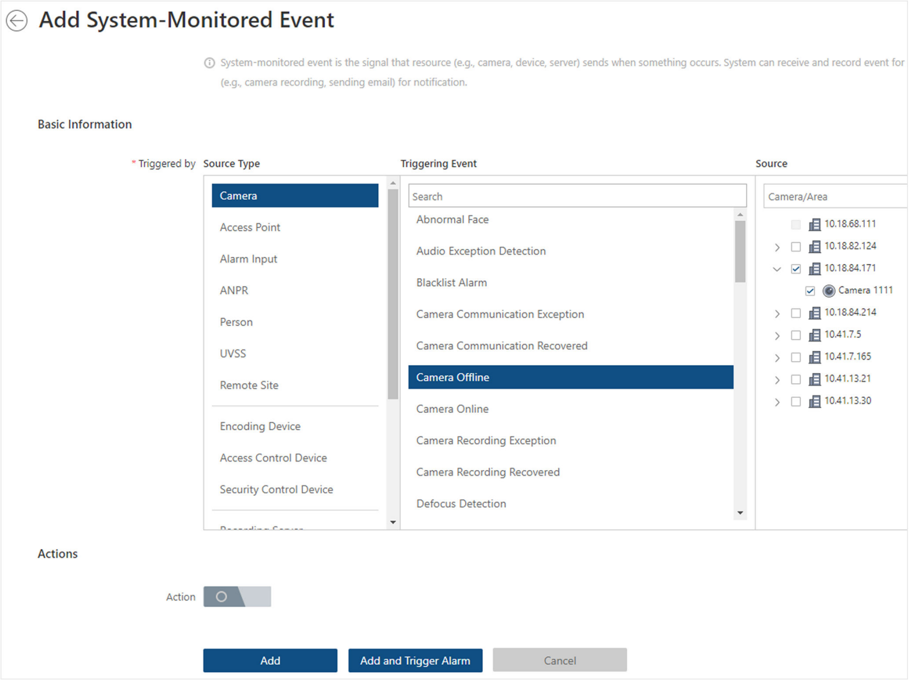
12.1.1 Add Event for Camera

You can add an event for the cameras on the current site. When the event is triggered on the camera, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the cameras in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.



Add System-Monitored Event

ⓘ System-monitored event is the signal that resource (e.g., camera, device, server) sends when something occurs. System can receive and record event for (e.g., camera recording, sending email) for notification.

Basic Information

* Triggered by

Figure 12-1 Add a System-Monitored Event

2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Camera**.

   Triggering Event

   The event detected on the camera will trigger a system-monitored event in the system.

   Source

   The specific camera(s) which can trigger this event.

3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The camera is armed during the arming schedule and the triggering event occurred on the camera during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Select the camera to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

- To trigger the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected event. Specify the number of seconds which you want to record video for after the event stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Select the camera(s) to record video when the event occurs and add tag to the event triggered video. The tagged video can be searched and checked via the Control Client.

- To trigger the source camera itself for tagged recording, select **Source Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

- To trigger the source camera itself for capturing pictures, select **Source Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** and select one camera for capturing pictures.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds to define when the camera will capture pictures for the event. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

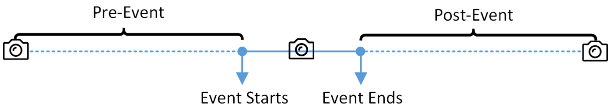


Figure 12-2 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm	Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters. **Note** For details, refer to ***Configure Alarm*** .
Delete Event	Select the event(s) and click **Delete** to delete the selected event(s).
Manage Invalid Event	If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.
Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.2 Add Event for Access Point

You can add an event for the access points in the system. When the event is triggered at the access point, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the access point in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Access Point**.

Triggering Event

The event detected at the access point will trigger the system-monitored event in the system.

Source

The specific access point(s) which can trigger this event.

3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

Arming Schedule Template

The access point is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

Note

For setting customized template, refer to ***Configure Arming Schedule Template*** .

Trigger Recording

Select the camera to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

- To trigger the access point's related camera(s) for recording, you can select **Source Related Camera** and select the storage location for storing the video files.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Select the camera to record video when the event occurs and add tag to the event triggered video. The tagged video can be searched and checked via the Control Client.

- To trigger the access point's related camera(s) for tagged recording, you can select **Source Related Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

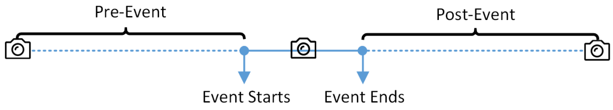


Figure 12-3 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.

- Click **Add** to add the event and back to the event list page.
- Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. Optional: Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.3 Add Event for Alarm Input

You can add an event for the alarm inputs in the system. When the alarm input is triggered, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the alarm inputs in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Alarm Input**.

   Triggering Event

   The event detected on the alarm input will trigger the system-monitored event in the system.

   Source

   The specific alarm input(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The alarm input is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera(s) to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

   Create Tag

Click **Add** to select the camera(s) to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

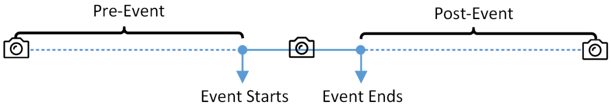


Figure 12-4 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.

- Click **Add** to add the event and back to the event list page.
- Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.4 Add Event for ANPR Camera

You can add an event for the cameras which have ANPR (Automatic Number-Plate Recognition) function (such as ANPR cameras and UVSS) in the system. When the recognized license plate numbers matched or mismatched with the license plate numbers in the vehicle list, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the ANPR camera in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **ANPR**.

   Triggering Event

   Select the vehicle list that will trigger the corresponding license plate matched/mismatched event.

   Source

   The specific ANPR camera(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The ANPR camera is armed during the arming schedule and the matched or mismatched license plate recognized during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Select the camera to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

- To trigger the source camera (when the source is ANPR camera) or trigger the source's related camera (when the source is UVSS) for recording, select **Source or Related Camera** and select the storage location for storing the video files.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Select the camera(s) to record video when the event occurs and add tag to the event triggered video. The tagged video can be searched and checked via the Control Client.

- To trigger the source camera (when the source is ANPR camera) or trigger the source's related camera (when the source is UVSS) for tagged recording, select **Source or Related Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

- To trigger the source camera (when the source is ANPR camera) or trigger the source's related camera (when the source is UVSS) for capturing pictures, select **Source or Related Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** (optional) and select one camera for capturing pictures.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

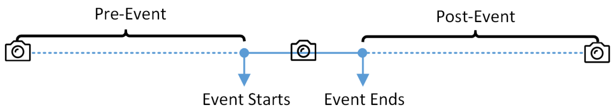


Figure 12-5 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.5 Add Event for Person

You can add a matched and mismatched event for the added face recognition camera in the system. When the camera recognizes a matched or mismatched person face, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the persons in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.

2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Person**.

   Triggering Event

   Select the face comparison group that will trigger the corresponding face matched/mismatched event.

   Source

   The specific camera(s) which can trigger this event.

3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The face recognition camera is armed during the arming schedule and the matched or mismatched person recognized during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Select the camera to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   - To trigger the face recognition camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
   - To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

   Create Tag

   Select the camera to record video when the event occurs and add tag to the event triggered video. The tagged video can be searched and checked via the Control Client.

- To trigger the face recognition camera itself for tagged recording, select **Source Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

- To trigger the face recognition camera itself for capturing pictures, select **Source Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** and select one camera for capturing pictures.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

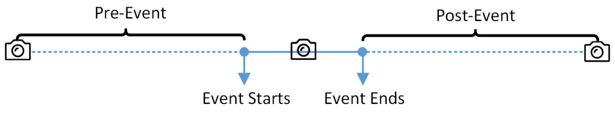


Figure 12-6 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

   Trigger Event as Alarm

   Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

   Note

   For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.6 Add System-Monitored Event for UVSS

You can add an event for the UVSS in the system. When the event is triggered on the UVSS, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the UVSS in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **UVSS**.

   Triggering Event

   The event detected on the UVSS and it will trigger the system-monitored event in the system.

   Source

   The specific UVSS(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The UVSS is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

- To trigger the UVSS's related camera(s) for recording, you can select **Source Related Camera** and select the storage location for storing the video files.
- To trigger other cameras, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Select the camera(s) to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

- To trigger the UVSS's related camera(s) for tagged recording, you can select **Source Related Camera** and select the storage location for storing the video files.
- To trigger other cameras for tagged recording, select **Specified Camera** and click **Add** to add other cameras. Select the storage location for storing the video files.

You can enter the name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

- To trigger the UVSS's related camera for capturing pictures, select **Source Related Camera**.
- To trigger other camera for capturing pictures, select **Specified Camera** (optional) and select one camera for capturing pictures.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

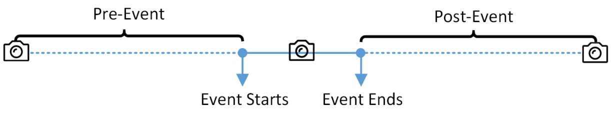


Figure 12-7 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

   Trigger Event as Alarm

   Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

   Note

   For details, refer to ***Configure Alarm*** .

   Delete Event

   Select the event(s) and click **Delete** to delete the selected event(s).

   Manage Invalid Event

   If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

   Delete All Invalid Events

   Click **Delete All Invalid Items** to delete all the invalid events in a batch.

   Filter Event

   Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.7 Add Event for Remote Site

You can add an event for the managed Remote Sites in the system. When the Remote Site gets offline, Central System can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the Remote Site's offline in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Remote Site**.

Triggering Event

If the Remote Site gets offline, it will trigger a system-monitored event in the Central System.

Source

The specific resource(s) which can trigger this event.

Note

For source type of generic event and user-defined event, you should select the configured generic event or user-defined event as the event source.

3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

Arming Schedule Template

The Remote Site is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

Note

For setting customized template, refer to ***Configure Arming Schedule Template*** .

Trigger Recording

Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

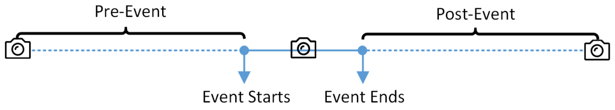


Figure 12-8 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.8 Add Event for Encoding Device

You can add an event for the encoding devices in the system. When the event is triggered on the device, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the encoding devices in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Encoding Device**.

   Triggering Event

   The event detected on the encoding devices will trigger the system-monitored event in the system.

   Source

   The specific encoding devices(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The event source is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera(s) to record video when the event occurs. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

   Create Tag

Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

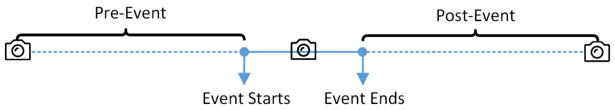


Figure 12-9 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.9 Add Event for Access Control Device

You can add an event for the access control devices in the system. When the event is triggered on the device, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the access control devices in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Access Control Device**.

   Triggering Event

   The event detected on the access control device will trigger a system-monitored event in the system.

   Source

   The specific access control device(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The access control device is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera(s) to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera(s) to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

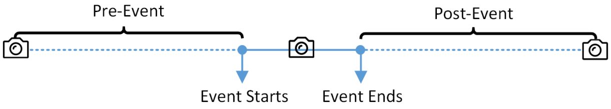


Figure 12-10 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm	Click in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.10 Add Event for Security Control Device

You can add an event for the security control device in the system. When the event is triggered on the device, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the security control device in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Security Control Device**.

   Triggering Event

   The event detected on the security control device will trigger the system-monitored event in the system.

   Source

   The specific security control device(s) which can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The security control device is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

Note

For setting customized template, refer to ***Configure Arming Schedule Template*** .

Trigger Recording

Click **Add** to select the camera(s) to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera(s) to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

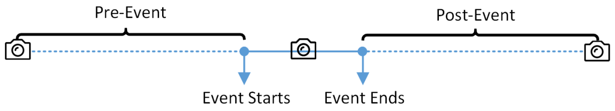


Figure 12-11 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.11 Add Event for Streaming Server or Recording Server

You can add an event for the added Streaming Servers and Recording Servers in the system. When the event is triggered on these servers, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the Streaming Server or Recording Server in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Streaming Server** or **Recording Server**.

Triggering Event

The event detected on the server will trigger a system-monitored event in the system.

Source

The specific server(s) which can trigger this event.

3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

Arming Schedule Template

The server is armed during the arming schedule and the triggering event occurred on the server during the arming schedule will trigger the configured linkage actions.

Note

For setting customized template, refer to ***Configure Arming Schedule Template*** .

Trigger Recording

Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

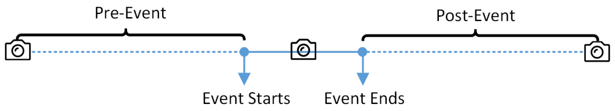


Figure 12-12 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.
5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events

Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event

Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.12 Add Event for X-VMS Server

You can set an event for the exception (including hardware exception and service exception) of the servers which have been installed with the X-VMS services (such as VSM service, third-party device access gateway, NGINX service, keyboard proxy service, smart wall management service, etc.). When the event is triggered, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the X-VMS Server in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **X-VMS Server**.

   Triggering Event

   The event detected on the X-VMS Server will trigger the system-monitored event in the system.

   Source

   Select **X-VMS Server** to trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The server is armed during the arming schedule and the triggering event occurred on the server during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

   Create Tag

   Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

   You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

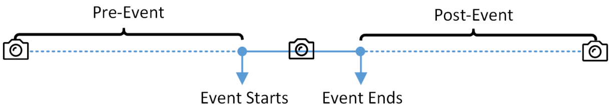


Figure 12-13 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm
Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event
Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event
If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events
Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event
Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.13 Add Event for User

You can add an event for the users in the system. When the user logs in or out, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the users in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **User**.

   Triggering Event

   The event detected on the event source and it will trigger the system-monitored event in the system.

   Source

   The specific user(s) who can trigger this event.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The user is armed during the arming schedule and the triggering event occurred on the event source during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

   Create Tag

Select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

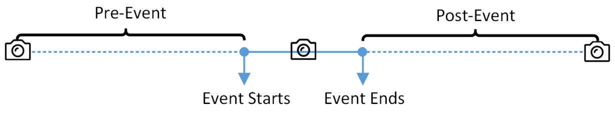


Figure 12-14 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
- Click **Add** to add the event and back to the event list page.
- Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. Optional: Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.14 Add Event for User-Defined Event

You can add an event for the added user-defined event in the system. When the user-defined event is triggered, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the user-defined event in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type and event source.

   Source Type

   Select the source type as **User-Defined Event**.

   Source

   Select the configured user-defined event as the event source.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The user-defined event is armed during the arming schedule and the user-defined event triggered during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

   Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

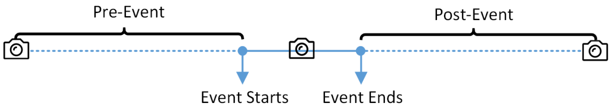


Figure 12-15 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manage Invalid Event

If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events	Click **Delete All Invalid Items** to delete all the invalid events in a batch.
Filter Event	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.15 Add Event for Generic Event

You can add an event for the added generic events in the system. When the generic event is triggered, system can receive and record event for checking and trigger a series of linkage actions (e.g., sending email) for notification.

Perform this task when you need to add a system-monitored event triggered by the generic event in the system.

Steps

1. Click **Event & Alarm → System-Monitored Event → Add** to enter the event adding page.
2. Configure the event's basic information, including source type, triggering event, and event source.

   Source Type

   Select the source type as **Generic Event**.

   Source

   Select the configured generic event as the event source.
3. **Optional:** Set the **Action** switch to on to set the linkage actions for the event.

   Arming Schedule Template

   The event is armed during the arming schedule and the generic event triggered during the arming schedule will trigger the configured linkage actions.

   Note

   For setting customized template, refer to ***Configure Arming Schedule Template*** .

   Trigger Recording

   Click **Add** to select the camera to record video when the event occurs. Select the storage location for storing the video files. You can play back the recorded video files when checking events in the Alarm & Event Search of the Control Client.

   View Pre-Event Video: If the camera has recorded video files before the event, you can view the video recorded from periods preceding the event. Specify the number of seconds which you want to view the recorded video for before the event starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

   Post-record: Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

Lock Video Files for: Set the days for protecting the video file from being overwritten.

Create Tag

Click **Add** to select the camera to record video when the event occurs and add tag to the event triggered video. Select the storage location for storing the video files. The tagged video can be searched and checked via the Control Client.

You can enter the tag name as desired. You can also click the button below to add the related information to the name.

Set the time range to define the tagged video length. For example, you can set to record the tagged video started from 5 seconds before the event and lasted until and 10 seconds after the event. The tagged video can be searched and checked via the Control Client.

Add the description to the tagged video as needed.

Capture Picture

Select one camera to capture pictures during the event, and you can view the captured pictures when checking event in the Alarm & Event Search of the Control Client.

Note

Only one camera can be set for capturing pictures.

Capture Picture When: Specify the number of seconds at which the camera will capture before/after the event starts/ends. After you set the number of seconds for pre/post-event, the camera will capture one picture at three time points respectively: at the configured seconds before the event starts, at the configured seconds after the event ends, and at the middle of the event (as shown in the picture below).

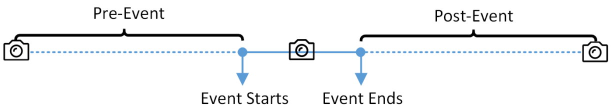


Figure 12-16 Capture Pictures

Note

The pre-event picture is captured from the camera's recorded video files. This pre-event capture function is only supported by the camera which is set to store the video files in the Recording Server (Cloud Storage Server, Hybrid SAN, or pStor).

Link Access Point

Select the access point(s) as the linkage target(s). You can set the access point action so that the access point will be unlocked, locked, remained unlocked, or remained locked when the event occurs.

Note

Up to 16 access points can be selected as event linkage.

Link Alarm Output

Select the alarm output (if available) and the external device connected can be activated when the event occurs.

Note

Up to 64 alarm outputs can be selected as event linkage.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the number of seconds in which the alarm output(s) will be closed automatically.

Trigger PTZ

Call the preset, patrol or pattern of the selected camera(s) when the event occurs.

Note

Up to 64 PTZ linkages can be selected as event linkage.

Send Email

Select an email template to send the event information according to the defined email settings. You can select **Add New** to create a new email template. For details, refer to ***Set Email Template*** .

Trigger User-Defined Event

Trigger user-defined event(s) when the system-monitored event is triggered.

Note

- Up to 16 user-defined events can be selected as event linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

4. Finish adding the event.
   - Click **Add** to add the event and back to the event list page.
   - Click **Add and Trigger Alarm** to trigger this event as an alarm for further notification. For details, refer to ***Configure Alarm*** .

   After adding the event, it displays on the event list, and you can view the event name, event source, and triggering event.

5. **Optional:** Perform the following operation(s) after adding the event.

Trigger Event as Alarm

Click 🔔 in the Operation column of system-monitored event settings page to set the alarm properties, recipients, actions, and other parameters.

Note

For details, refer to ***Configure Alarm*** .

Delete Event

Select the event(s) and click **Delete** to delete the selected event(s).

Manual Invalid Event
If ⊗ appears near the event name, it means the event is not supported by the device and it is invalid. You should hover the cursor over the ⊗ and click **Delete** on the tooltip and delete the event.

Delete All Invalid Events
Click **Delete All Invalid Items** to delete all the invalid events in a batch.

Filter Event
Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the events according to the conditions.

12.1.16 Edit System-Monitored Event

After adding the system-monitored event, you can edit the event settings and trigger the event as alarm.

Before You Start
Add the system-monitored event. See ***Configure System-Monitored Event*** for details.

Perform this task when you need to edit the added system-monitored event or trigger it as alarm.

Steps

1. Click **Event & Alarm** on home page.
2. Click **System-Monitored Event** tab to enter the event list page.
3. Click the event name to enter the event details page.
4. **Optional:** Perform the following operations to edit the event details.

   Configure Event on Device (If Supported)
   For some of the source types, click ⚙ to log in to the device and configure the event. See the user manual of the device for details.

   Edit Event Name
   Edit the event name as desired.

   Edit Actions
   Edit the event linkage action settings. For details, refer to ***Configure System-Monitored Event*** .
5. Save the event settings.
   - Click **Save** to save the event settings and back to the event list page.
   - Click **Save and Trigger Alarm** to save the event as alarm and enter the alarm settings page for setting alarm. See ***Configure Alarm*** for details.

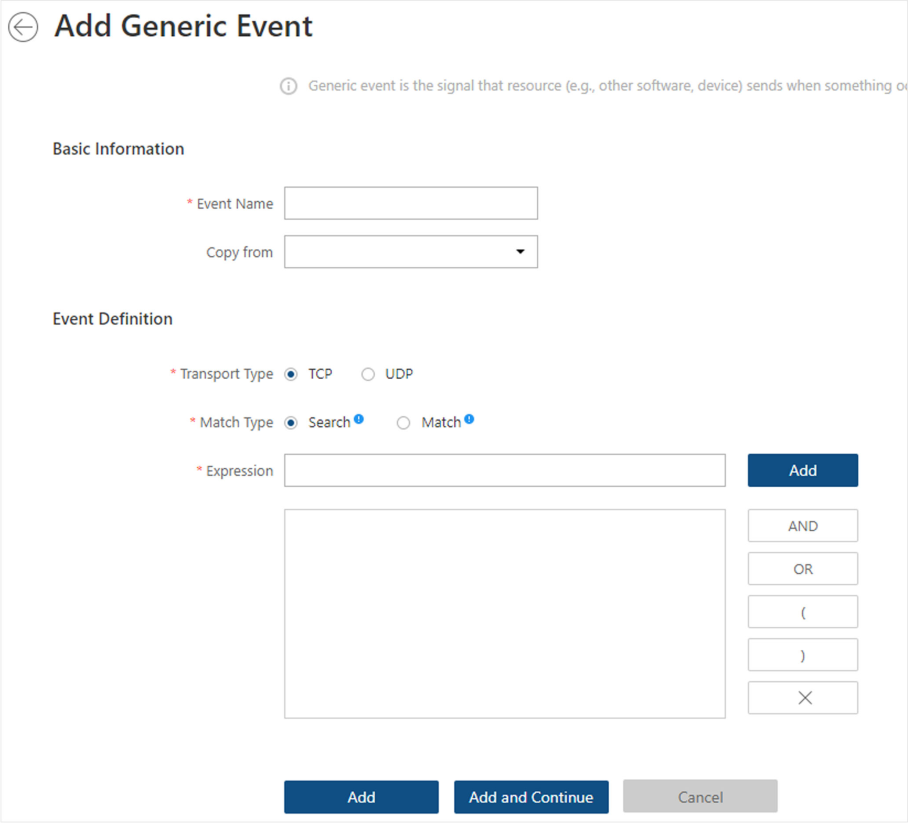
12.2 Configure Generic Event

You can customize the expression to create a generic event to analyze the received TCP and/or UDP data packages, and trigger events when specified conditions are met. In this way, you can easily integrate your system with a very wide range of external sources, such as access control systems and alarm systems.

Perform this task when you need to configure generic event.

Steps

1. Click **Event & Alarm → Generic Event** to enter the generic event settings page.
2. Click **Add** to enter the Add Generic Event page.



Generic event is the signal that resource (e.g., other software, device) sends when something o

Figure 12-18 Add Generic Event Page

3. Set a name for the event in the Event Name field.
4. **Optional:** Copy the settings from other defined generic events in the **Copy from** field.
5. Select **TCP** or **UDP** to analyze the packages using TCP or UDP protocol.
6. Select the matched type which indicating how particular your system should be when analyzing the received data packages:

   Search

   The received package must contain the text defined in the Expression field.

   For example, if you have defined that the received packages should contain "Motion" and "Line Crossing", the alarm will be triggered when the received packages contain "Motion", "Intrusion" and "Line Crossing".

   Match

   The received package must exactly contain the text defined in the Expression field, and nothing else.

7. Define the event rule for analyzing the received package in the Expression field.
   1) Enter the term which should be contained in the expression in the text field.
   2) Click **Add** to add it to the expression.

3) Click parenthesis or operator button to add it to the expression.
4) To add a term, parenthesis or operator to the expression, position the cursor inside the expression field in order to determine where a new item (term, parenthesis or the operator) should be included, and click Add or one of the parenthesis or operator buttons.
5) To remove an item from the expression, position the cursor inside the field in order to determine where an item should be removed, and click × . The item immediately to the left of the cursor will be removed.

The parenthesis or operator buttons are described in the following:

AND

You specify that the terms on both sides of the AND operator must be included.

For example, if you define the rule as "Motion" AND "Line Crossing" AND "Intrusion", the term Motion, and Line Crossing as well as the term Intrusion must be all contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with AND, the fewer events will be detected.

OR

You specify that any term should be contained.

For example, if you define the rule as "Motion" OR "Line Crossing" OR "Intrusion", any of the terms (Motion, Line Crossing, or Intrusion) must be contained in the received package for the conditions to be met.

Note

In generally, the more terms you combine with OR, the more events will be detected.

(

Add the left parenthesis to the rule. Parentheses can be used to ensure that related terms are processed together as a unit; in other words, they can be used to force a certain processing order in the analysis.

For example, if you define the rule as ("Motion" OR "Line Crossing") AND "Intrusion", the two terms inside the parentheses will be processed first, then the result will be combined with the last part of the rule. In other words, the system will first search any packages containing either of the terms Motion or Line Crossing, then it search the results to look for the packages that contained the term Intrusion.

)

Add the right parenthesis to the rule.

8. Finish adding the event.
- Click **Add** to add the event and back to the event list page.
- Click **Add and Continue** to save the event settings and continue to add event.

9. Optional: Perform the following operations after adding the event.

Edit Event Settings	Click the name in the Event Name column to edit the corresponding event settings.
Delete Event Settings	Check the event(s) and click **Delete** to delete the selected event settings.
Delete All Event Settings	Check the checkbox in the heading row, and click **Delete** to delete all the event settings.

12.3 Configure User-Defined Event

If the event you need is not in the provided system-monitored event list, or the generic event cannot properly define the event received from third-party system, you can customize a user-defined event.

Perform this task if you need to add a user-defined event.

Steps

1. Click **Event & Alarm → User-Defined Event** to enter the user-defined event management page.
2. Click **Add** to open the following window.

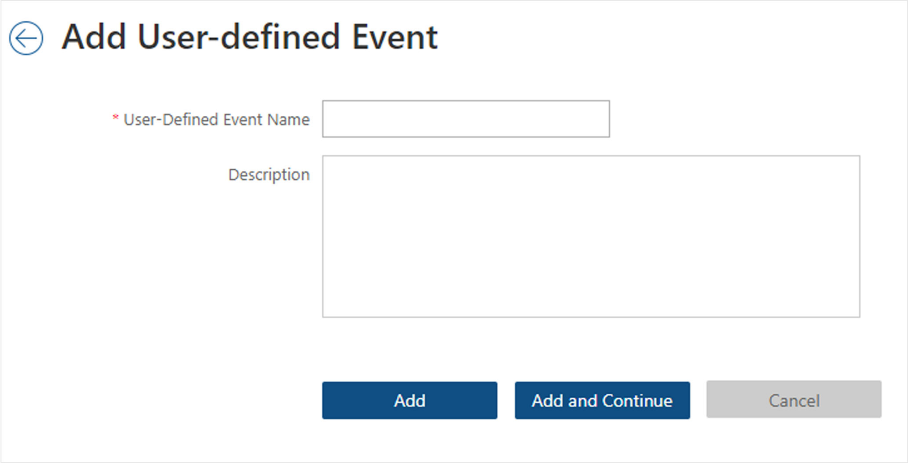


Figure 12-19 Add User-Defined Event

3. Create a name for the event.
4. **Optional:** Enter the description information to describe the event details.
5. Finish adding the event.
   - Click **Add** to add the event and go back to the event list page.
   - Click **Add and Continue** to add the event and continue to add other events.

   With the customized user-defined event, it provides the following functions:

   - The user can trigger a user-defined event manually in Monitoring and Alarm Center module on the Control Client when viewing the video or checking the alarm information.
   - A user-defined event can trigger an alarm if configured.

- You can define the arming time period by the user-defined event: An alarm's arming schedule will start or end when the user-defined event is triggered.
- An alarm can trigger a user-defined event as alarm actions.
- Integrate other third-party systems with X-VMS by using the data received from the third-party system. You can trigger the user-defined events outside the X-VMS. For details, contact our technical support.

Note

- For configuring the alarm source, arming schedule, and alarm action, refer to ***Configure Alarm*** .
- For triggering the user-defined event on the Control Client, refer to *User Manual of X-VMS Control Client*.

12.4 Configure Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly. Alarm can trigger a series of linkage actions (e.g., popping up window on the Control Client, showing the alarm details) for notification and alarm handling.

You can set the alarms for the resources on the current site.

If the system is a Central System with Remote Site Management module, you can also set the alarm for the camera on Remote Site which has configured with alarm, so that you can receive alarms in the Central System when the alarm is triggered.

You can set different linkage actions for the following alarms:

- Camera Alarm: the video exception or the events detected in the monitoring area of the cameras, such as motion detection, video loss, line crossing, etc.
- Access Point Alarm: the alarm triggered at the access points (door, lane, etc.), such as access event, door status event, etc.
- Alarm Input Alarm: the alarm triggered by the alarm inputs (including alarm inputs of encoding devices,.access control devices, and security control devices).
- ANPR Alarm: the alarm triggered when the license plates detected by the ANPR camera and UVSS matches or mismatches the vehicle information in vehicle list.
- Person Alarm: the alarm triggered when the person's face detected by the face recognition device matches or mismatches the face picture in the face comparison group.
- UVSS Alarm: the alarm trigger by the UVSS device, including device getting online and offline.
- Remote Site Alarm: the alarm triggered by the added Remote Site, including site getting offline.

Note

Remote Site alarm is available for the system with Remote Site Management module (based on the license you purchased).

- Device Exception: the alarm triggered by encoding device's, access control device's, or security control devices' exceptions.
- Server Exception: the alarm triggered by Recording Server, Streaming Server, or X-VMS Server.
- User Alarm: the alarm triggered by system users, including user login and logout.
- User-Defined Event: the alarm triggered by the configured user-defined event.
- Generic Event: the alarm triggered by the configured generic event.

Note

You can check the received alarm message via the Control Client. For details, see *User Manual of X-VMS Control Client*.

12.4.1 Alarm Settings

The system predefines several alarm priorities and alarm categories for basic needs. You can edit the predefined alarm priority and alarm category, and set customized alarm priority and alarm category according to actual needs.

Perform this task when you need to configure the alarm priority and alarm category.

Alarm Priority

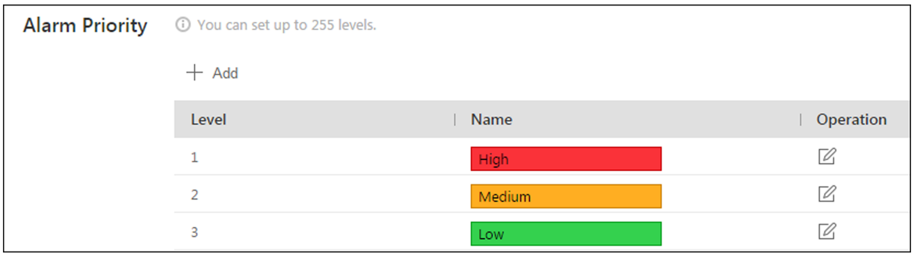
Define the priority for the alarm when add the alarm and filter alarms in the Control Client.

Alarm Category

Alarm category is used when the user acknowledges the alarm in the Control Client and categorises what kind of alarm it is, e,g., false alarm, or alarm to be verified. You can search the alarms by the alarm type in the Alarm Center of Control Client.

Steps

1. Click **Event & Alarm → Alarm → Alarm Settings** to enter the alarm settings page.
2. Set the alarm priority according to actual needs. By default, three kinds of alarm priority exist.



Alarm Priority ⓘ You can set up to 255 levels.

+ Add

Level	Name	Operation
1	High	✎
2	Medium	✎
3	Low	✎

Figure 12-20 Alarm Priority Page

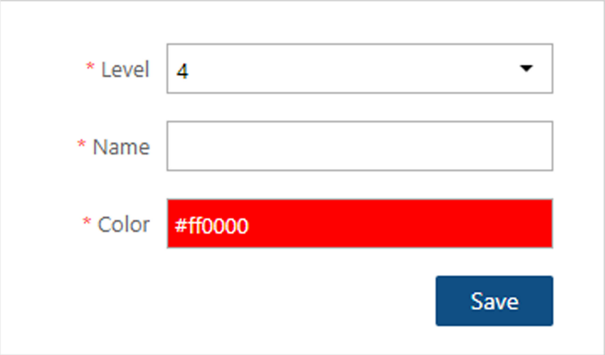
1) Click **Add** to add a customized priority.

Note

Up to 255 levels of alarm priority can be added. The priority levels can be used for sorting alarms in Alarm Center of Control Client.

2) Select a level No. for the priority.

3) Enter a descriptive name for the priority.
4) Select the color for the priority.



* Level: 4

* Name:

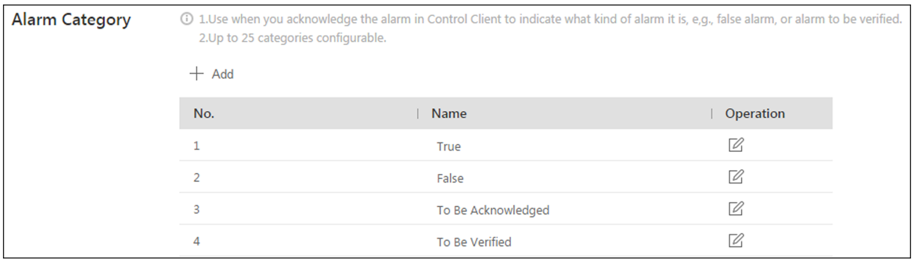
* Color: #ff0000

Figure 12-21 Alarm Priority Settings Window

5) Click **Save** to add the priority.

   The priority will be displayed on the alarm priority list.

3. Set the alarm category according to actual needs. By default, four alarm categories exist.



Alarm Category

ⓘ 1.Use when you acknowledge the alarm in Control Client to indicate what kind of alarm it is, e,g., false alarm, or alarm to be verified.
2.Up to 25 categories configurable.

No.	Name	Operation
1	True	✎
2	False	✎
3	To Be Acknowledged	✎
4	To Be Verified	✎

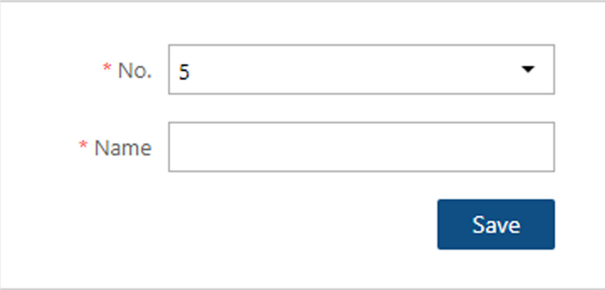
Figure 12-22 Alarm Category Page

1) Click **Add** to add the customized alarm category.

Note

Up to 25 alarm categories can be added.

2) Select a No. for the alarm category.
3) Enter a descriptive name for the alarm category.



* No.: 5

* Name:

Figure 12-23 Alarm Category Settings Window

4) Click **Save** to add the alarm category.

   The alarm category will be displayed on the alarm category list.

4. Perform the following operation(s) after adding alarm priority and category.

Edit Click ✎ to edit the alarm priority and category.

Note

You cannot edit the No. of predefined alarm priorities and categories.

Delete Click × to delete the alarm priority and category.

Note

You cannot delete the predefined alarm priorities and categories.

12.4.2 Add Alarm for Camera on Current Site

You can set alarms for added cameras on current site and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add a new alarm for cameras on current site.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set the source type as **Camera** in the **Triggered by** field.
3. Select a triggering event as the source for triggering the alarm.
4. In the site drop-down list, select the current site.
5. Select a specific camera for triggering the alarm.
6. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
7. Set the required information.

   Arming Schedule

   The camera is armed during the arming schedule and the event occurred during the arming schedule will be triggered as alarm and notify the user. It provides two types of arming schedule:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

8. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions.

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back these video files in the Alarm Center of the Control Client.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Alarm Video:** You can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to ***Add Hot Spot***). You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window and set the alarm video's stream type.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected

public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

9. Finish adding the alarm.
- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

The alarm will be displayed on the alarm list and you can view the alarm name and alarm status.

10. Optional: Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Click × in the Operation column to delete the alarm.

Delete All Alarms	Click **Delete All** to delete all the added alarm.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.
Disable All Alarms	Click **Disable All** to disable all the added alarms.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

12.4.3 Add Alarm for Camera on Remote Site

If the system is a Central System with Remote Site Management module (based on the license you purchased), you can also add the alarms configured for the cameras on the Remote Site to the Central System, and configure a series of linkage actions for notification in Central System when alarm is triggered.

Before You Start
You should configure the alarm for the camera on the Remote Site via the Remote Site's Web Client.

Perform this task if you need to add the alarms configured for the cameras on Remote Site to the Central System.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set the source type as **Camera** in the **Triggered by** field.
3. Select the alarm source.
   1) In the **Triggering Event** list, select the source event type.
   2) In the **Source** list, select a Remote Site from the drop-down list.

      The alarms configured on the Remote Site of the selected triggering event type will be displayed.
   3) Select the alarm configured on the Remote Site as the source to trigger an alarm in Central System.

   Note

   Please make the alarm configured on the Remote Site is enabled. The alarm will be effective after enabled on Remote Site and in Central System
4. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipient

Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm linkage actions.

Related Camera

If the selected alarm is configured with related camera on Remote Site, you can view its video files when checking the alarm in Central System.

Related Map

If the selected alarm is configured with related map on Remote Site, you can view the alarm source location when checking the alarm in Central System.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarms.

   The alarm will be displayed on the alarm list. You can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm
Click ✎ in the Operation column to edit the alarm.

Copy to Other Alarms
You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm
Click × in the Operation column to delete the alarm.

Delete All Alarms
Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms
Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm
Click ✓ in the Operation column to enable the alarm.

Enable All Alarms
Click **Enable All** to enable all the added alarms.

Disable Alarm
Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms
Click **Disable All** to disable all the added alarms.

Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

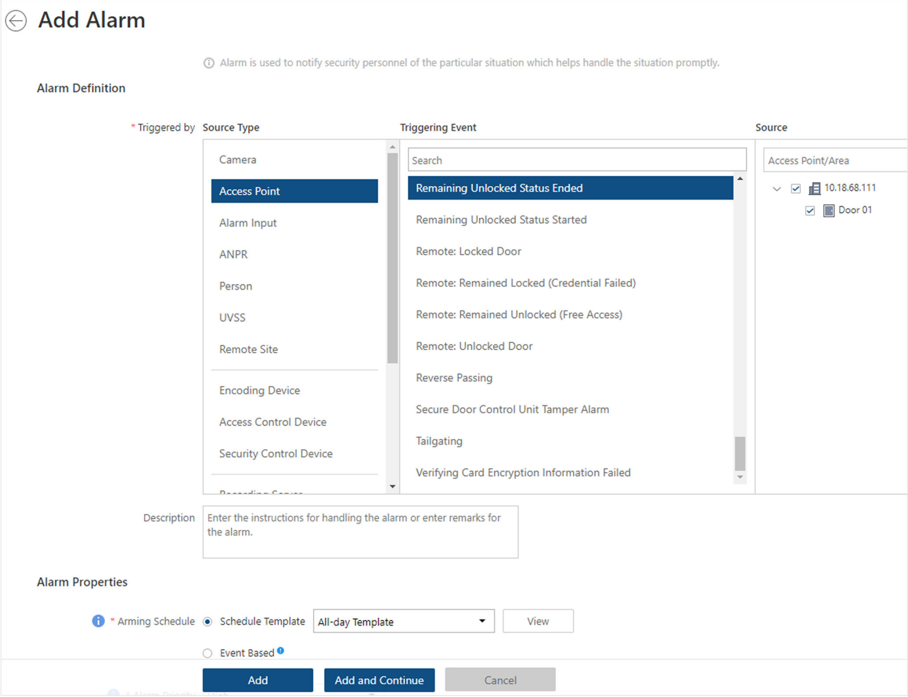
12.4.4 Add Alarm for Access Point

You can set alarms for the access points of the added access control devices and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add a new alarm for the access points.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by

Source Type	Triggering Event	Source
Camera	Search	Access Point/Area
Access Point	**Remaining Unlocked Status Ended**	☑ 10.18.68.111
Alarm Input	Remaining Unlocked Status Started	☑ Door 01
ANPR	Remote: Locked Door	
Person	Remote: Remained Locked (Credential Failed)	
UVSS	Remote: Remained Unlocked (Free Access)	
Remote Site	Remote: Unlocked Door	
Encoding Device	Reverse Passing	
Access Control Device	Secure Door Control Unit Tamper Alarm	
Security Control Device	Tailgating	
	Verifying Card Encryption Information Failed	

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule ● Schedule Template: All-day Template ▾ View

○ Event Based

Figure 12-26 Add Alarm for Access Point

2. Set the source type as **Access Point** in the **Triggered by** field.
3. Select a triggering event and a specific access point as the source for triggering the alarm.
4. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The access point is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedules are provided:

- **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipients

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- To relate the access point's related camera for recording, select **Source Related Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and Click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- For setting the access point's related camera in the Logical View, refer to ***Edit Access Point for Current Site*** .
- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

Select the map to show the alarm information and you should add the access point to the map as a hot spot (refer to ***Add Hot Spot***). You can check the map in the Alarm Center and Alarm & Event Search of the Control Client.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:**A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

6. Finish adding the alarm.

- Click **Add** to add the alarm and go back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.

7. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm
Click ✎ in the Operation column to edit the alarm.

Copy to Other Alarms
You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm
Click × in the Operation column to delete the alarm.

Delete All Alarms
Click **Delete All** to delete all the added alarm.

Delete All Invalid Alarms
Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm
Click ✓ in the Operation column to enable the alarm.

Enable All Alarms
Click **Enable All** to enable all the added alarms.

Disable Alarm
Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms
Click **Disable All** to disable all the added alarms.

Test Alarm
Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

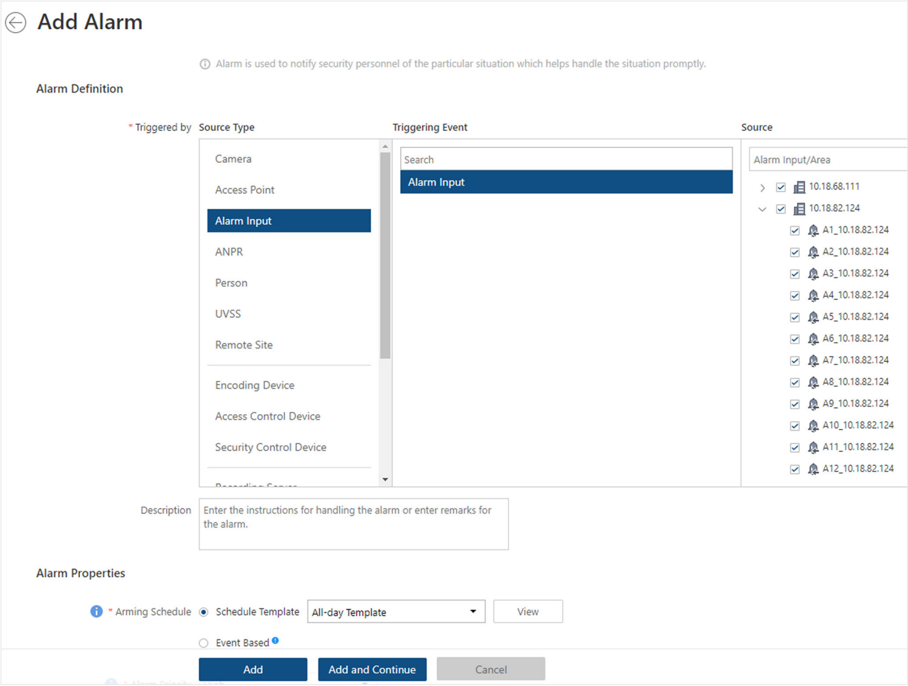
12.4.5 Add Alarm for Alarm Input

You can set alarm input alarm for alarm inputs of the added device and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add alarm for the alarm inputs of the added device.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: Alarm Input; Triggering Event: Alarm Input; Source: ☑ 10.18.68.111, ☑ 10.18.82.124, ☑ A1_10.18.82.124, ☑ A2_10.18.82.124, ☑ A3_10.18.82.124, ☑ A4_10.18.82.124, ☑ A5_10.18.82.124, ☑ A6_10.18.82.124, ☑ A7_10.18.82.124, ☑ A8_10.18.82.124, ☑ A9_10.18.82.124, ☑ A10_10.18.82.124, ☑ A11_10.18.82.124, ☑ A12_10.18.82.124

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template ○ Event Based

Figure 12-27 Add Alarm for Alarm Input

2. Set the source type as **Alarm Input** in the **Triggered by** field.
3. Select a specific alarm input as the source for triggering the alarm.
4. **Optional:** Enter the instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The alarm input is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user-defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.
6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

Select the map to show the alarm information and you should add the alarm input to the map as a hot spot (refer to ***Add Hot Spot***). You can check the map in the Alarm Center and Alarm & Event Search of Control Client.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and recorded video files when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.

- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.

8. Optional: Perform the following operation(s) after adding the alarm:

Edit Alarm

Click ✎ in the Operation column to edit the alarm.

Delete Alarm

Click × in the Operation column to delete the alarm.

Copy to Other Alarms

You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete All Alarms

Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms

Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm Click ⊘ in the Operation column to enable the alarm.

Enable All Alarms Click **Enable All** to enable all the added alarms.

Disable Alarm Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms Click **Disable All** to disable all the added alarms.

Test Alarm Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

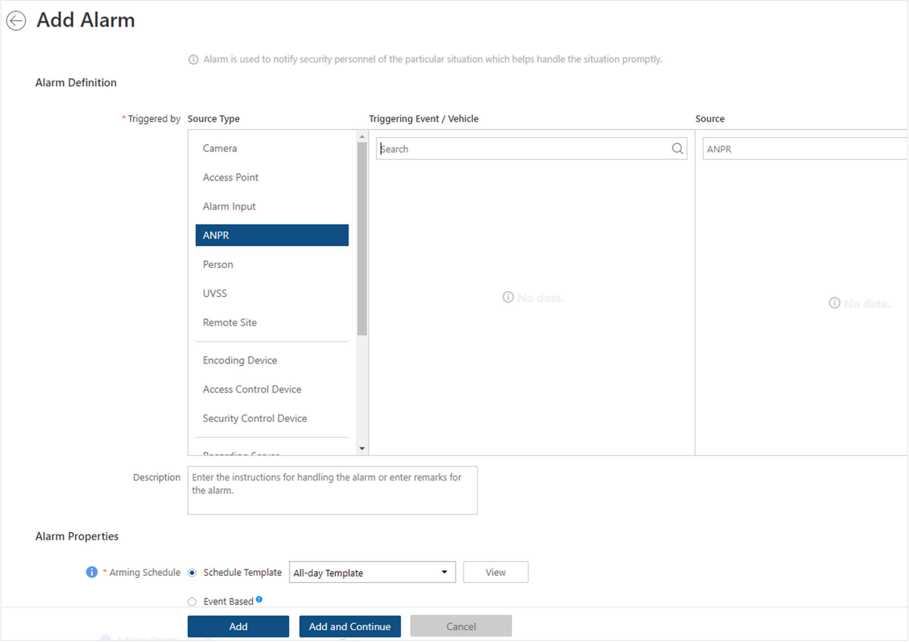
12.4.6 Add Alarm for ANPR Camera

You can set plate number matched and mismatched alarm for the added ANPR camera (including professional ANPR traffic cameras and camera in UVSS (under vehicle surveillance system)) and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add alarm for the added ANPR camera.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: ANPR; Source: ANPR

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template ○ Event Based

Figure 12-28 Add Alarm for ANPR Camera

2. Set the source type as **ANPR** in the **Triggered by** field.
3. Select a defined vehicle list as the source for matching or mismatching the license plate recognized by and then select a specific ANPR camera or UVSS camera as the source for triggering the alarm.

Note

Before setting ANPR alarm, vehicles information should be added for matching the license plate recognized by ANPR device. For adding vehicle list and vehicle information, refer to ***Manage Vehicle*** .

4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The device is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

   Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

   - To relate the source ANPR camera itself, or the UVSS's related camera for recording, select **Source or Source Related Camera** and select the storage location for storing the video files.
   - To relate other cameras, select **Specified Camera** and Click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
   - **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

Select the map to show the alarm information and you should add the camera or UVSS to the map as a hot spot (refer to ***Add Hot Spot***). You can check the map in the Alarm Center and Alarm & Event Search of Control Client.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarm.

   After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

   Edit Alarm
   Click ✎ in the Operation column to edit the alarm information.

   Copy to Other Alarms
   You can copy the current alarm's specified parameters to other added alarms for batch configuration.

   Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

   Specify the settings of the source alarm, select target alarm(s), and click **OK**.

   Delete Alarm
   Click × in the Operation column to delete the alarm.

   Delete All Alarms
   Click **Delete All** to delete all the added alarms.

   Delete All Invalid Alarms
   Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

   Enable Alarm
   Click ✓ in the Operation column to enable the alarm.

   Enable All Alarms
   Click **Enable All** to enable all the added alarms.

   Disable Alarm
   Click ⊖ in the Operation column to disable the alarm.

   Disable All Alarms
   Click **Disable All** to disable all the added alarms.

   Test Alarm
   Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

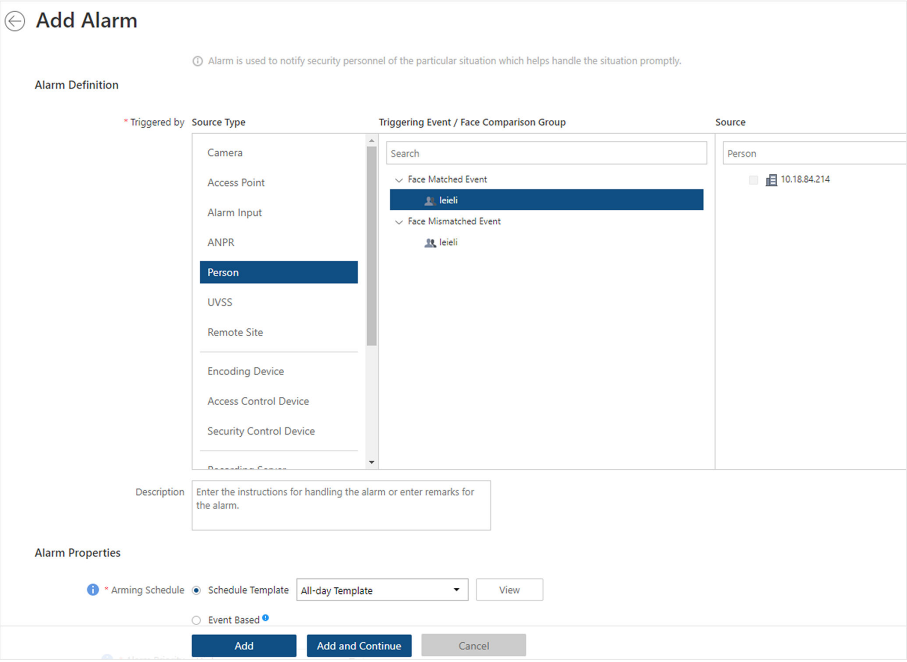
12.4.7 Add Alarm for Person

You can set face matched and mismatched alarm for the added face recognition camera and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add face matched or mismatched alarm for the person.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.



Add Alarm

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: Person

Triggering Event / Face Comparison Group: Face Matched Event: leieli

Source: 10.18.84.214

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template

○ Event Based

Figure 12-29 Add Alarm for Person

2. Set the source type as **Person** in the **Triggered by** field.
3. Select a face comparison group applied to the camera and select a specific face recognition camera as the source for matching or mismatching the person face recognized by the face recognition camera.

Note

For configuring the face comparison group and applying to the device, refer to ***Manage Face Comparison Group*** .

4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

The camera is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

Schedule Template

Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .

Event Based

Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipient

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

Select the related camera to record the alarm video when the alarm is triggered. You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- To relate the source camera itself for recording, select **Source Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and Click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to ***Add Hot Spot***). You can check the map in the Alarm Center and Alarm & Event Search of Control Client.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and recorded video files when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarm.

   After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

   Edit Alarm
   Click ✎ in the Operation column to edit the alarm.

   Copy to Other Alarms
   You can copy the current alarm's specified parameters to other added alarms for batch configuration.

   Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

   Specify the settings of the source alarm, select target alarm(s), and click **OK**.

   Delete Alarm
   Click × in the Operation column to delete the alarm.

   Delete All Alarms
   Click **Delete All** to delete all the added alarm.

   Enable Alarm
   Click ✓ in the Operation column to enable the alarm.

   Enable All Alarms
   Click **Enable All** to enable all the added alarms.

   Disable Alarm
   Click ⊖ in the Operation column to disable the alarm.

   Disable All Alarms
   Click **Disable All** to disable all the added alarms.

   Delete All Invalid Alarms
   Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

   Test Alarm
   Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

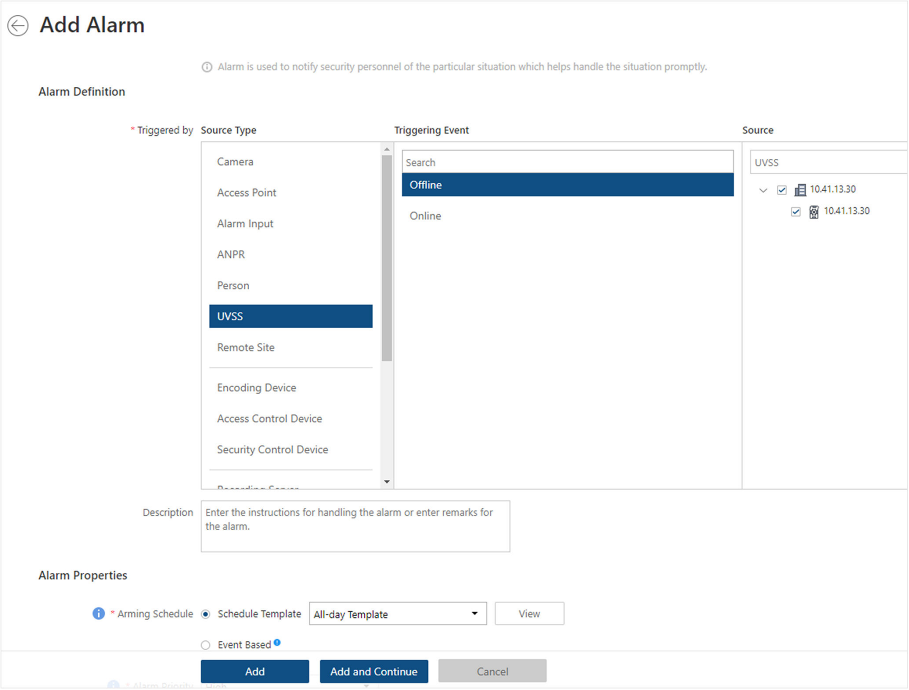
12.4.8 Add Alarm for UVSS

You can set alarms for added UVSSs, including UVSS online and offline, and trigger a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification.

Perform this task when you need to add alarms for the added UVSS.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: UVSS; Triggering Event: Offline; Source: ☑ 10.41.13.30, ☑ 10.41.13.30

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template ○ Event Based

Figure 12-30 Add Alarm for UVSS

2. Set **UVSS** as the source type in the **Triggered by** field.
3. Select a specific triggering event and a specific UVSS as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

Arming Schedule

The UVSS is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

- **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipient

Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- To relate the UVSS's related camera for recording, select **Source Related Camera** and select the storage location for storing the video files.
- To relate other cameras, select **Specified Camera** and Click **Add** to add other cameras as related cameras. Select the storage location for storing the video files.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- For setting the UVSS's related camera, refer to ***Edit Under Vehicle Surveillance System for Current Site***
- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarm.

   After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.

Enable All Alarms Click **Enable All** to enable all the added alarms.

Disable Alarm Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms Click **Disable All** to disable all the added alarms.

Test Alarm Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

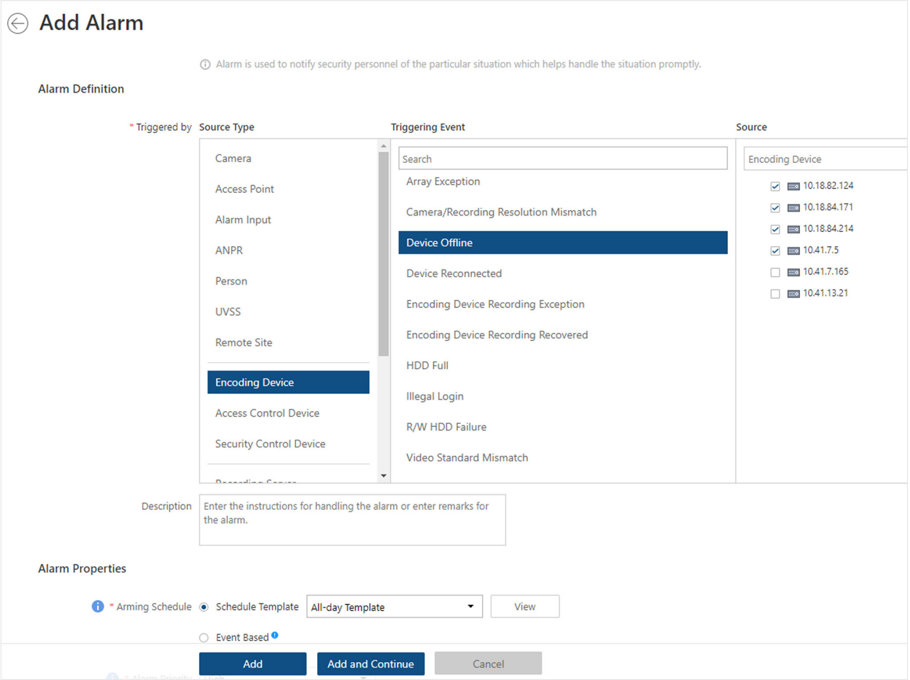
12.4.9 Add Alarm for Encoding Device

You can set alarms for the added encoding devices and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add alarm for the added encoding device.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: Encoding Device; Triggering Event: Device Offline; Source: ☑ 10.18.82.124, ☑ 10.18.84.171, ☑ 10.18.84.214, ☑ 10.41.7.5, □ 10.41.7.165, □ 10.41.13.21

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template ○ Event Based

Figure 12-31 Add Alarm for Encoding Device

2. Set the source type as **Encoding Device**in the **Triggered by** field.
3. Select triggering event and a specific encoding device as the source for triggering the alarm.
4. **Optional:** Configure the alarm definition including alarm name and description.
5. Set the required information.

   Arming Schedule

The device is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

- **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
- **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipient

Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.

- Click **Add** to add the alarm and go back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarms.

The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.

8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm

Click ✎ in the Operation column to edit the alarm.

Copy to Other Alarms

You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm

Click × in the Operation column to delete the alarm.

Delete All Alarms

Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms

Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm

Click ✓ in the Operation column to enable the alarm.

Enable All Alarms

Click **Enable All** to enable all the added alarms.

Disable Alarm

Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms

Click **Disable All** to disable all the added alarms.

Test Alarm

Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

12.4.10 Add Alarm for Access Control Device

You can set alarms for added access control devices, such as device online/offline, tampering alarm, low battery, etc., and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add an alarm for an added access control device.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.

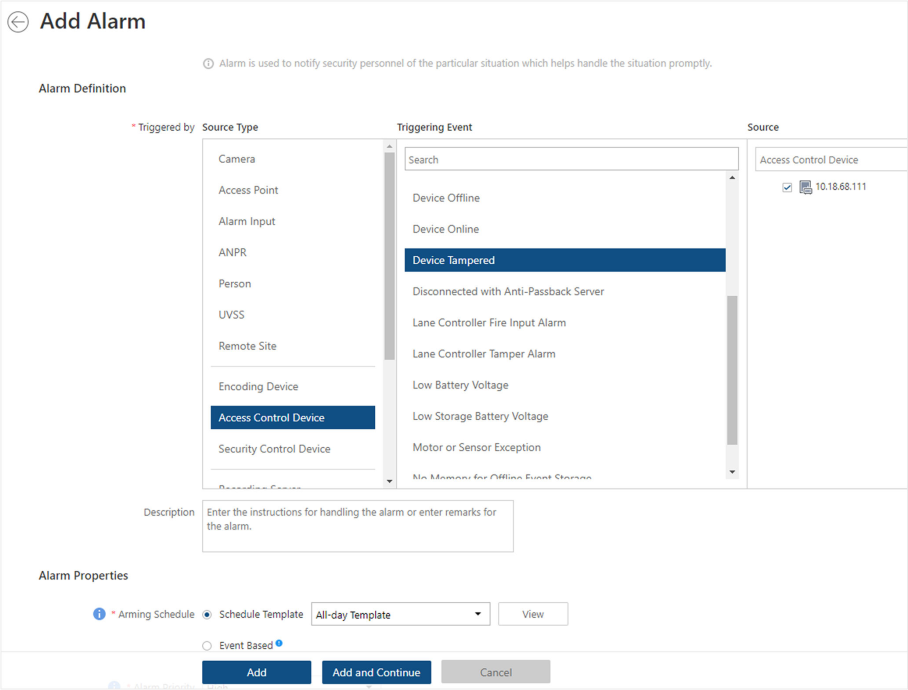


Figure 12-32 Add Alarm for Access Control Device

2. Set **Access Control Device** as the source type in the **Triggered by** field.
3. Select a triggering event and a specific device as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

Arming Schedule

The device is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

Schedule Template

Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .

Event Based

Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

Alarm Priority

Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

Alarm Recipient

Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

Select the camera(s) to record the alarm video when the alarm is triggered.

Post-record

Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.

View Pre-Alarm Video

If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.

Lock Video Files for

Set the days for protecting the video file from being overwritten.

Display Video by Default

Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and recorded video files when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected

public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of the Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarms.

   The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.
Disable All Alarms	Click **Disable All** to disable all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

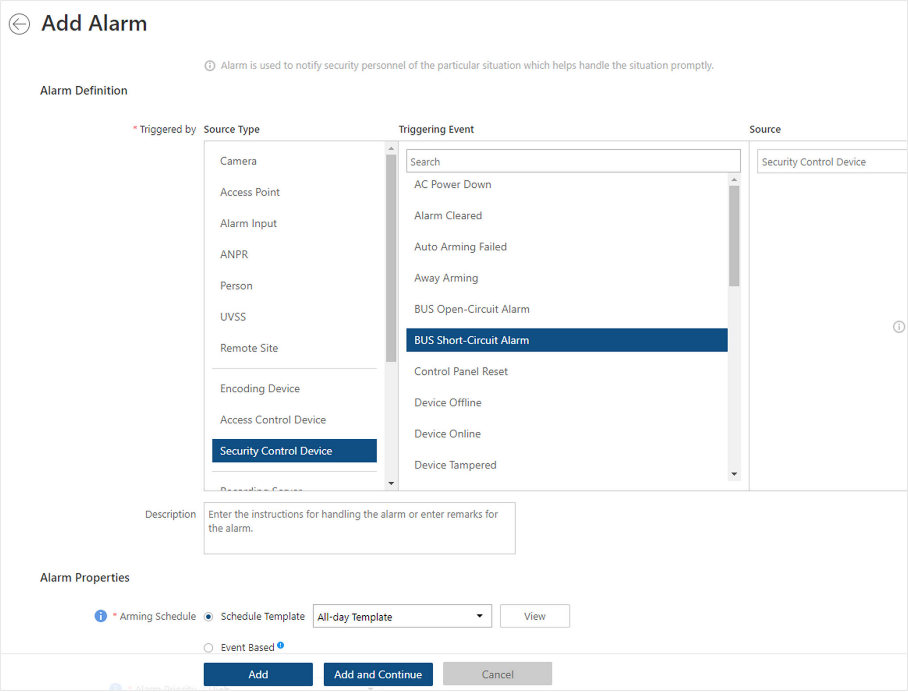
12.4.11 Add Alarm for Security Control Device

You can set alarms for the added security control devices, such as device online/offline, tampering alarm, low battery, etc., and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add an alarm for an added security control device.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.



Add Alarm

ⓘ Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

* Triggered by: Source Type: Security Control Device; Triggering Event: BUS Short-Circuit Alarm; Source: Security Control Device

Description: Enter the instructions for handling the alarm or enter remarks for the alarm.

Alarm Properties

* Arming Schedule: ● Schedule Template: All-day Template

Figure 12-33 Add Alarm for Security Control Device

2. Set **Security Control Device** as the source type in the **Triggered by** field.
3. Select a triggering event and a specific device as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The device is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.
6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and recorded video files when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of the Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarms.

   The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.

8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms	Click **Disable All** to disable all the added alarms.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

12.4.12 Add Alarm for Streaming Server and Recording Server

You can set server exception alarms for added servers (Streaming Server and Recording Server) and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add alarms for the added Streaming Server and Recording Server.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the adding alarm page.
2. Set **Recording Server** or **Streaming Server** as the source type in the **Triggered by** field.
3. Select a specific triggering event and a specific server as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The server is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.

- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.

8. Optional: Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms	Click **Disable All** to disable all the added alarms.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

12.4.13 Add Alarm for X-VMS Server

You can set alarm for the exception (including hardware exception and service exception) of the servers which have been installed with the X-VMS services (such as VSM service, third-party device access gateway, NGINX service, keyboard proxy service, smart wall management service, etc.) and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add a new alarm for the X-VMS server exception.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set **X-VMS Server** as the source type in the **Triggered by** field.
3. Select a specific triggering event and select **X-VMS Server** in the **Source** list as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The server is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For details about setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For details about setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and recorded video files when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For details about configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.

- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

After adding the alarm, it displays on the alarm list, and you can view the alarm name and alarm status.

8. Perform the following operation(s) after adding the alarm.

Edit Alarm

Click ✎ in the Operation column to edit the alarm information.

Copy to Other Alarms

You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm

Click × in the Operation column to delete the alarm.

Delete All Alarms

Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms

Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm

Click ✓ in the Operation column to enable the alarm.

Enable All Alarms

Click **Enable All** to enable all the added alarms.

Disable Alarm

Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms
Click **Disable All** to disable all the added alarms.

Test Alarm
Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly .

12.4.14 Add Alarm for User

You can set alarms for the users, including user login and user logout, and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add a new alarm for the system users.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set **User** as the source type in the **Triggered by** field.
3. Select a specific triggering event and a specific user as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The user is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify other user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select the user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

   You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on the Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.

- Click **Add** to add the alarm and back to the alarm list page.
- Click **Add and Continue** to add the alarm and continue to add other alarm.

The alarm will be displayed in the alarm list, and you can view the alarm name and alarm status.

8. Optional: Perform the following operation(s) after adding the alarm.

Edit Alarm
Click ✎ in the Operation column to edit the alarm information.

Copy to Other Alarms
You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm
Click × in the Operation column to delete the alarm.

Delete All Alarms
Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms
Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm
Click ✓ in the Operation column to enable the alarm.

Enable All Alarms
Click **Enable All** to enable all the added alarms.

Disable Alarm
Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms
Click **Disable All** to disable all the added alarms.

Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

12.4.15 Add Alarm for User-Defined Event

You can set alarms for the added user-defined event and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Before You Start
You should have created at least one user-defined event. For details, refer to ***Configure User-Defined Event*** .

Perform this task when you need to add a new alarm for the user-defined event.

Steps

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set **User-Defined Event** as the source type in the **Triggered by** field.
3. Select a specific user-defined event as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required parameters.

   Arming Schedule

   The event is armed during the arming schedule and the event occurred during the arming schedule will be triggered as alarm and notify the user. It provides two types of arming schedule:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.
6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

   You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details and all the alarm related cameras' live videos and playback when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add another alarm.

   The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.
Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms	Click **Disable All** to disable all the added alarms.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

12.4.16 Add Alarm for Generic Event

You can set alarms for the added generic event and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Before You Start

You should have created at least one generic event. Refer to ***Configure Generic Event*** for details about creating generic event.

Perform this task when you need to add alarm for the added generic event.

Steps

1. Click **Event & Alarm → Alarm → Add** on home page.
2. Select **Generic Event** as the source type in the **Triggered by** field.
3. Select a specific generic event as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required parameters.

   Arming Schedule

   The event is armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For details about setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For details about setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

   Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Trigger Pop-up Window

Select to display the alarm window on the Control Client to show the alarm details when alarm occurs.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.
- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For details about configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarms.

   The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm

Click ✎ in the Operation column to edit the alarm.

Copy to Other Alarms

You can copy the current alarm's specified parameters to other added alarms for batch configuration.

Click ✎ in the Operation column to enter the alarm details page and click **Copy to**.

Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm

Click × in the Operation column to delete the alarm.

Delete All Alarms

Click **Delete All** to delete all the added alarms.

Delete All Invalid Alarms

Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.

Enable Alarm

Click ✓ in the Operation column to enable the alarm.

Enable All Alarms

Click **Enable All** to enable all the added alarms.

Disable Alarm

Click ⊖ in the Operation column to disable the alarm.

Disable All Alarms

Click **Disable All** to disable all the added alarms.

Test Alarm

Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly as you want.

12.4.17 Add Alarm for Remote Site

If the system is Central System with Remote Site Management module (based on the license you purchased), you can set site offline alarm for the added Remote Site and configure a series of linkage actions (e.g., triggering pop-up window on the Control Client) for notification when alarm is triggered.

Perform this task when you need to add the alarm for Remote Site.

Steps

Note

You can set alarms for added Remote Site only when the system has Remote Site Management module.

1. Click **Event & Alarm → Alarm → Add** to enter the Add Alarm page.
2. Set **Remote Site** as the source type in the **Triggered by** field.
3. Select a triggering event and a specific Remote Site as the source for triggering the alarm.
4. **Optional:** Enter instructions for handling the alarm or enter remarks for the alarm.
5. Set the required information.

   Arming Schedule

   The resources on Remote Site are armed during the arming schedule and when an event occurs during the arming schedule, an alarm will be triggered to notify the user. Two types of arming schedule are provided:

   - **Schedule Template:** Select an arming schedule template for the alarm to define when the alarm can be triggered. For setting customized template, refer to ***Configure Arming Schedule Template*** .
   - **Event Based:** Specify a user-defined event or an alarm input as the start or end event of the arming schedule. When the user defined event or alarm input is triggered, the arming schedule will start or end.

   Alarm Priority

   Define the priority for the alarm. Priority can be used for filtering alarms in the Control Client. For setting alarm priority, refer to ***Alarm Settings*** .

   Alarm Recipient

   Select a user to send the alarm information to and the user can receive the alarm information when he/she logs in to X-VMS via the Control Client or Mobile Client.

6. **Optional:** Set the alarm's additional settings such as alarm related cameras and map, and alarm linkage actions

Related Camera

You can view the live video and play back the recorded video files when alarm occurs in the Alarm Center of the Control Client.

- Select the camera(s) to record the alarm video when the alarm is triggered.
- **Post-record:** Record video from periods following detected alarms. Specify the number of seconds which you want to record video for after the alarm stops.
- **View Pre-Alarm Video:** If the camera has recorded video files before the alarm, you can view the video recorded from periods preceding the alarm. Specify the number of seconds which you want to view the recorded video for before the alarm starts. For example, when someone opens a door, you can view the recorded video to see what happens right before the door opened.
- **Lock Video Files for:** Set the days for protecting the video file from being overwritten.
- **Display Video by Default:** Set the default video to be displayed on the Control Client when checking the triggered alarm information.

Note

- Make sure the related camera(s) have been configured with recording schedule.
- Up to 16 cameras can be set as related camera.

Related Map

View the Remote Site's location on GIS map or when you checking alarm details in the Alarm Center and Alarm & Event Search of the Control Client.

Note

You should locate the map on the GIS map first. For details, refer to ***Locate Sites on Map*** .

Trigger Pop-up Window

Display the alarm window on Control Client to show the alarm details.

Display on Smart Wall

Display the alarm video of the alarm's related camera or display the specified public view on the smart wall. You can select the added smart wall and select which window to display the alarm.

- **Alarm's Related Cameras:** Display the video of the alarm's related cameras on the smart wall. You can select to display the video on which smart wall and which window. Select the stream type for the alarm video displayed on smart wall.
- **Public View:** A view enables you to save the window division and the correspondence between cameras and windows as favorites to quickly access the related cameras later. If you select **Public View**, when the alarm is triggered, the system can display the selected

public view on the specified smart wall and users can view the video of the cameras pre-defined in the view.

- **Stop Displaying Alarm:** Define when the system will stop displaying the alarm on the smart wall. The system can stop displaying alarm within specified seconds, or replace the original alarm when other alarm with higher alarm priority is triggered.

Restrict Alarm Handling Time

When the alarm is triggered, you need to handle the alarm on the Control Client. Enable this function to trigger user-defined event(s) or alarm output(s) if the alarm is not handled within the configured alarm handling time.

Note

- Up to 16 user-defined events and alarm outputs can be set as the triggered event when handling alarm timed out.
- For configuring the user-defined event, refer to ***Configure User-Defined Event*** .

Trigger Audible Warning

Set the voice text for playing on the PC when alarm is triggered.

Note

You should set voice engine as the alarm sound on System Settings page of Control Client.

Trigger User-Defined Event

Trigger the user-defined event(s) when alarm is triggered.

Note

- Up to 16 user-defined events can be selected as alarm linkage.
- For setting the user-defined event, refer to ***Configure User-Defined Event*** .

7. Finish adding the alarm.
   - Click **Add** to add the alarm and go back to the alarm list page.
   - Click **Add and Continue** to add the alarm and continue to add other alarms.

   The alarm will be displayed on the alarm list, and you can view the alarm name and alarm status.
8. **Optional:** Perform the following operation(s) after adding the alarm.

Edit Alarm	Click ✎ in the Operation column to edit the alarm.
Copy to Other Alarms	You can copy the current alarm's specified parameters to other added alarms for batch configuration. Click ✎ in the Operation column to enter the alarm details page and click **Copy to**. Specify the settings of the source alarm, select target alarm(s), and click **OK**.

Delete Alarm	Click × in the Operation column to delete the alarm.
Delete All Alarms	Click **Delete All** to delete all the added alarms.
Delete All Invalid Alarms	Click **Delete All Invalid Items** to delete all the invalid alarms in a batch.
Enable Alarm	Click ✓ in the Operation column to enable the alarm.
Enable All Alarms	Click **Enable All** to enable all the added alarms.
Disable Alarm	Click ⊖ in the Operation column to disable the alarm.
Disable All Alarms	Click **Disable All** to disable all the added alarms.
Test Alarm	Click ◎ to trigger this alarm automatically. You can test if the linkage actions work properly.

12.5 Configure Arming Schedule Template

When setting event and alarm, you can select the predefined arming schedule template to define when the event or alarm will be triggered. The system predefines three default arming schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Steps

1. Click **System** on the home page.
2. Click **Schedule → Arming Schedule Template** on the left.
3. Click **Add** to enter the adding arming schedule page.

Note

You can add up to 32 templates.

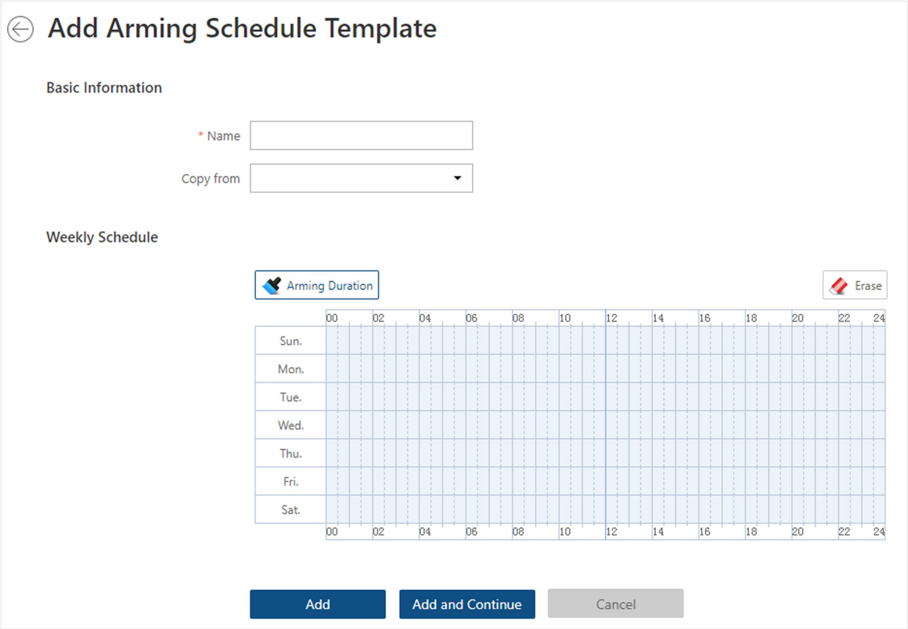


Figure 12-39 Add Arming Schedule Template Page

4. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

5. Click **Arming Duration** and drag on the time bar to set the time periods.

Note

Up to 4 time periods can be set for each day.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
7. Finish adding the arming schedule template.
   - Click **Add** to add the template and go back to the arming schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The arming schedule template will be displayed on the arming schedule template list.
8. **Optional:** Perform the following operations after adding the arming schedule template.

   View Template Details Click the template to view its details.

   Edit Template Click ✎ in the Operation column to edit template details.

   Delete Template Click × in the Operation column to delete the template.

Delete All Templates	Click **Delete All** to delete all the added templates (except the default templates). If the added templates have been used by events or alarms, you will be asked whether or not to replace the schedule.

Chapter 13 Manage Map

Two types of map are available: GIS map and E-map. On the GIS map, you can set and view the current site, Remote Site, and element's geographic location. On the e-map, which is a static map, you can set and view the geographic locations of the installed cameras, alarm inputs, and alarm outputs, etc. After configuring the map via Web Client, you can view the live video and playback of the resources added to the map via Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

With GIS map, you can see the geographic locations of your surveillance system. This type of map uses a geographic information system to accurately show all the hot spots' (resources (e.g., camera, alarm input) placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access cameras at multiple locations around the world in a geographically correct way. If the resources locate in multiple locations (e.g., different cities, different countries), GIS map can give you a single view to show them all and help you quickly go to each location to view video from the cameras. With the hot region, you can link to the e-map to view the detailed monitoring scenario, for example, the monitoring scenario of a building.

E-map is a static image (it does not have to be geographical maps, although they often are. Depending on your organization's needs, photos and other kinds of image files can also be used as e-maps) which gives you a visual overview of the locations and distributions of the hot spots (resources (e.g., camera, alarm input) placed on the map are called hot spots). You can see the physical locations of the cameras, alarm inputs, and alarm outputs, etc., and in what direction the cameras are pointing. With the function of hot region, e-maps can be organized into hierarchies to navigate from large perspectives to detailed perspectives, e.g., from floor level to room level.

After configuring the e-map via Web Client, you can view the live video and playback of the elements via Control Client, and get a notification message from the map via Control Client when an alarm is triggered.

13.1 Set GIS Map and Icons

You can enable the GIS map function and configure the map API URL to display the GIS map on the Web Client and Control Client, showing the geographic location of the resources (such as current site, Remote Site, cameras). You can also customize the icons of hot region and hot spot (such as camera, alarm input, and alarm output).

Perform this task for setting GIS map API URL and customized icons.

Steps

1. Click **System → Normal → Map** to enter the map settings page.
2. Set the GIS Map.
   1) Set the **GIS Map** switch to ON to enable the GIS map function.
   2) Input the GIS map API URL.

Note

- The Google map API is supported currently.
- Google Maps are provided by Google Inc. (Hereinafter referred to as “Google”). We only provides you the URLs to use Google Maps. You shall apply by yourself for the use of Google Maps from Google. You shall comply with Google terms and provide certain information to Google if required.

3. Set the customized icons.
   1) Select hot region or hot spot as the icon type in the **Type** field.
   2) Set the icon size, including width (px) and height (px).
   3) **Optional:** Click the icon to cancel the aspect ratio.

   Note

   By default, the aspect ratio is maintained.

   4) Click **Add** in the Picture field to select a picture file from the local path.

   Note

   The icon picture format can only be PNG, JPG, or JPEG.

   The added pictures display as thumbnail preview in the Picture field.
4. Click **Save**.

Result

You can view the GIS map in the Logical View page and perform the following operations in the map area.

Filter	Click and select the object type you want to show on the map.
Full Screen	Click to show the map in full-screen mode.
Zoom In/Out	Scroll the mouse wheel or click + / − to zoom in or zoom out the map.
Adjust Map Area	Click-and-drag the map to adjust the map area for view.

13.2 Link E-Map to Area

You can add and link e-maps to the area so that the elements assigned to the area can be added to e-map.

Perform the task when you want to link e-map to area.

Steps

1. Click **Logical View**.

2. Three ways are available for adding e-map.

Add E-Map When Adding Area

a. Click + on the area list panel.
b. Set the parameters for adding area.
c. Set the **Related Map** switch to ON.
d. Hover the mouse over the Map field and link a map for the area.
   You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
e. **Optional:** Repeat the previous step to add more e-maps for the area.

Add E-Map When Editing Area

a. Select a map and click ✎ on the area list panel to enter the area editing page.
b. Edit the area settings as desired.
c. Set the **Related Map** switch to ON if it is OFF.
d. Hover the mouse over the empty Map field and link a map for the area.
   You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
e. **Optional:** Repeat the previous step to add more e-maps for the area.

Directly Link Map to Existing Area

Note

You can adopt this way when the GIS map is not enabled.

a. Click 🗺 to show the map area.
b. Click **Relate Map** for adding and linking map.
c. Select the areas for linking e-maps.
d. Hover the mouse over the Map field and link a map for the area.
   You can click **Upload Picture** and select a picture from local PC as the e-map. Or click **Existing Map** and select an existing map for linking to current area.
e. **Optional:** Repeat the previous step to add more e-maps for the area.

3. **Optional:** Hover the mouse over the added e-map area to perform the following operations.

Edit Picture Click and change a picture.

Edit Map Name Click and set a custom name for the map.

Unlink Map Click to remove the map or cancel the linkage between the map and area.

4. Click **Save** to confirm the settings.
5. **Optional:** Perform the following operations after adding map in the map area.

Filter Click 👁 and select the object type you want to show on the map.

Full Screen Click ⛶ to show the map in full-screen mode.

Zoom In/Out Scroll the mouse wheel or click + / − to zoom in or zoom out the map.

Adjust Map Area Drag the map or the red window in the lower part to adjust the map area for view.

13.3 Search Locations

You can search the locations on the GIS map.

Before You Start
You should enable the GIS Map function and set the GIS Map API URL properly. For details, refer to ***Set GIS Map and Icons*** .

Perform this task when you need to search the locations on the GIS map.

Steps

1. Click **Logical View** on home page.
2. Click 🗺 to show the map area.
3. Enter a location name you want to search in the 🔍 field.

   The related locations display in the search field.
4. Click to select the location you want to locate from the related locations.

Result

The location will be located on the map.

13.4 Locate Sites on Map

You can set the current site's and added Remote Site's location to the GIS map.

Before You Start
You should enable the GIS Map function and set the GIS Map API URL properly. For details, refer to ***Set GIS Map and Icons*** .

Perform this task when you need to set the sites' location to the GIS map.

Steps

1. Click **Logical View** on home page.
2. Click 🗺 to show the map area.
3. Select current site or Remote Site from the drop-down list on area list panel.

   Note

   The icon 🌐 indicates that the site is current site, and 🌐 indicates Remote Site.
4. Click **Locate** on the GIS map area.

   Note

   The **Locate** button is only available when the site is not located on GIS map.

5. Operate the GIS map to find the location of the site and click on the map to locate the site on the map.

   Note

   You can use you mouse to drag, zoom in, and zoom out the map.

   After successfully located, the site icon will be displayed at the location you select.

6. **Optional:** Perform the following operations after adding the site to the GIS map.

View Site Details	Click the site icon to view the site details, including site address, location, and remark information
Edit	Click the site icon and click **Edit** to edit the site information.
Delete	Click the site icon and click **Delete** to remove the site from the map.
View Site's Resources	Click the site icon and click **View Site's Resources** to view the resources of the site.

13.5 Add Hot Spot

You can add elements as the hot spot and place the hot spot on the e-map or GIS map.

Before You Start

A map should have been added. Refer to ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Perform this task when you need to get the live view and alarm information of the surveillance scenarios via the hot spot on the map.

Steps

1. Click **Logical View** on the home page.
2. Select current site from the drop-down list on area list panel.

   Note

   The icon 🌐 indicates that the site is current site, you can only add current site's elements as the hot spots.

3. Three ways are available for adding hot spot.

Add Hot Spot When Adding Element to Area	a. Click the tab to enter the corresponding element page. b. Click + in the element area. c. Set the required parameters for adding the element to area. **Note** For details, refer to ***Add Element to Area*** . d. Check **Add to Map** checkbox and the map area displays.

e. In the map area, click to select a map to add the hot spot to.
f. Click **Add** and you can see the adding element result in the pop-up dialog.

Drag Element to Map

Note

You can adopt this way when the element is added to the area but not added to map.

a. Click the tab to enter the corresponding element page.
b. **Optional:** Click to select an area so that the elements of this area display.
c. Click 🗺 to show the map area.
d. In the map area, click to select a map to add the hot spot to.
e. Drag an element with Added to Map as No to the map.

Add Hot Spot When Editing the Element

Note

You can adopt this way when the element is added to the area but not added to map.

a. Click the tab to enter the corresponding element page.
b. **Optional:** Click to select an area so that the elements of this area can be displayed.
c. Click the Name field of the element with Added to Map as No.
d. Set the **Add to Map** switch to ON.
e. In the map area, click to select a map to add the hot spot to.
f. Configure the required settings for the hot spot.
g. Click **Save**.

4. **Optional:** Perform the following operations after adding the hot spot.

Adjust Hot Spot Location
Drag the added hot spot on the map to the desired locations.

Edit Hot Spot
Click the added hot spot icon on the map and click **Edit** to edit the detailed information (such as setting GPS location (only available when parent map is GIS map, and refer to ***Search Locations*** for details), and selecting icon style).

For camera hot spot, you can also edit the detection area, including radius, direction and angle, or drag the displayed sector on the map to directly adjust the detection area.

Delete Hot Spot
Click the hot spot icon on the map and click **Delete** to remove the hot spot from the map.

13.6 Add Hot Region

The hot region function links a map to another map. When you add a map to another map as a hot region, an icon of the link to the added map is shown on the main map. The added map is called child map while the map to which you add the hot region is the parent map.

Before You Start

At least 2 maps should have been added. Refer to ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding maps.

Perform this task when you want to link a map to another map for convenient access.

Steps

1. Click **Logical View** on the home page.
2. Select a current site from the drop-down list on area list panel.

   Note

   The icon 🌐 indicates that the site is current site, you can only add hot region for current site.

3. Click 🗺 to show the map area.
4. Select an added e-map or GIS map as the parent map.
5. Click on the map area and click on the spot where you want to place the hot region.

   A dialog for setting child map appears.
6. Select a child map on the panel to set it as the hot region of the current map.
7. Click **Save** on dialog to add the hot region.

   The added hot region icon will be displayed on the parent map.
8. **Optional:** Perform the following operation(s) after adding the hot region.

   Adjust Hot Region Location Drag the added hot region on the parent map to the desired locations.

   Edit Hot Region Click the added hot region icon on the map to view and edit the detailed information, including GPS location (only available when parent map is GIS map, and refer to ***Search Locations*** for details), hot region name, icon style, name color, and remarks on the appearing dialog.

   Delete Hot Region Click the hot region icon on the map and click **Delete** on the appearing dialog to delete the hot region.

13.7 Add Label

You can add labels with description on the map.

Before You Start

At least one map should have been added. Refer to ***Link E-Map to Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Perform this task when you need to add label on the map.

Steps

1. Click **Logical View** on the home page.
2. Select current site from the drop-down list on area list panel.

   Note

   The icon 🌐 indicates that the site is current site, you can only add label for current site.

3. Click 🗺 to show the map area.
4. Select a map to add label to.
5. Click ⚐ on the map area and click on the map where you want to place the label.
6. Customize a name for the label, and you can input content for the label as desired.
7. Click **Save**.

   The added label icon will be displayed on the map.

8. **Optional:** Perform the following operation(s) after adding the label.

Adjust Label Location	Drag the added label on the map to the desired locations.
Edit Label	Click the added label icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Label	Click the label icon on the map and click **Delete** on the appearing dialog to delete the label.

Chapter 14 Manage Vehicle

You can import the vehicle information according to the pre-defined template and you can add the vehicle information manually. The added vehicle information can be used for ANPR alarm when adding the alarm.

Note

Refer to ***Add Alarm for ANPR Camera*** for detailed information about adding alarm.

14.1 Add Vehicle List

Before adding the vehicle information to the system, you should create the vehicle list.

Perform the following steps to add the vehicle list.

Steps

Note

Up to 100 vehicle lists can be added to the system.

1. Click **Vehicle** to enter the Vehicle Management page.
2. Click + on the left to open the adding vehicle list window.
3. Set a descriptive name for the vehicle list.
4. **Optional:** Click **Download Template** and import vehicle information in a batch, or you can import vehicle information when checking vehicle list details. Refer to ***Add Vehicle Information*** for details.
5. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing one with the new vehicle information if the license plate number for importing already exists in other vehicle list. Otherwise, the original vehicle information will be reserved.
6. Click **Add**.

   The added vehicle list will be displayed on the left of the Vehicle page.
7. **Optional:** Perform the following operations on the vehicle list area.

Edit Vehicle List	Click ✎ on the vehicle list area to edit the vehicle list name.
Delete Vehicle List	Click 🗑 on the vehicle list area to delete the list.

14.2 Add Vehicle Information

After adding the vehicle list, you can check the vehicle information in the vehicle list or you can add the vehicle information to the list.

The added vehicle information can be used for ANPR alarm when adding the alarm.

You can import the vehicle information in batch or you can add the vehicle information manually.

Note

Each vehicle list can contain up to 5,000 vehicles.

14.2.1 Import Vehicle Information in a Batch

You can import multiple vehicle information at one time.

Before You Start

You should add the vehicle list before you can add the vehicle information. Refer to ***Add Vehicle List*** for details.

Perform the following task when you need to import vehicle information in a batch.

Steps

Note

Each vehicle list can contain up to 5,000 vehicles.

1. Click **Vehicle** to enter the Vehicle Management page.
2. Select a vehicle list.
3. Click **Import** to open the Import window.
4. Click **Download Template** on the Import window to save the template file (CSV format) to your PC.
5. Open the downloaded template file.
6. Enter the required vehicle information in the corresponding column.
7. Click … and select the template file.
8. **Optional:** Check **Replace Repeated License Plate Number** to replace the existing one with the new vehicle information if the template contains the license plate number which already exists in the current or other vehicle list. Otherwise, the original vehicle information will be reserved.
9. Click **Import**.
10. **Optional:** Perform the following operations after importing the vehicle information.

Edit Vehicle Information
Click the plate number in License Plate Number column to edit the vehicle information

Edit Effective Period
Select the vehicle(s) and click **Edit Effective Period** to edit the effective period of the selected vehicle(s) in a batch.

If the license plate number is expired, it cannot trigger an event or alarm when license plate number matched if license plate number matched event/alarm is configured.

Delete Vehicle Information
Check the vehicle information and click **Delete** to delete the selected vehicle information

Export Vehicle Information	Click **Export All** to save the vehicle information of the list (CSV file) to your PC, which can be imported to other vehicle list.

14.2.2 Manually Add Vehicle Information

You can add single vehicle information manually.

Before You Start

You should add the vehicle list before you can add the vehicle information. Refer to ***Add Vehicle List*** for details.

Perform this task when you need to add vehicle information manually.

Steps

1. Click **Vehicle** to enter the Vehicle Management page.
2. Select a vehicle list.
3. Click **Add** to enter the adding vehicle page.
4. Enter the license plate number.
5. **Optional:** Set a effective period for this vehicle.

   If the license plate number is expired, it cannot trigger an event or alarm when license plate number matched if license plate number matched event/alarm is configured.
6. **Optional:** Enter the vehicle owner information including name and phone number.
7. **Optional:** Upload an undercarriage picture for this vehicle.
   1) Move the cursor to the image area and click **Upload**.
   2) In the pop-up window, select the undercarriage picture to upload it.

   After uploading an undercarriage picture, you can view both the current vehicle's captured undercarriage picture and this uploaded picture for comparison on the Control Client.
8. Finish adding the vehicle information.
   - Click **Add** to add the vehicle information and back to the vehicle list page.
   - Click **Add and Continue** to save the settings and continue to add other vehicles.

   Note

   If the license plate number already exists (in current vehicle list or other vehicle lists), a prompt box will be displayed and you can select whether to replace the existing vehicle with a new one.
9. **Optional:** Perform the following operations after importing the vehicle information.

Edit Vehicle Information	Click the plate number in License Plate Number column to edit the vehicle information
Edit Effective Period	Select the vehicle(s) and click **Edit Effective Period** to edit the effective period of the selected vehicle(s) in a batch. If the license plate number is expired, it cannot trigger an event or alarm when license plate number matched if license plate number matched event/alarm is configured.

Delete Vehicle Information	Check the vehicle information and click **Delete** to delete the selected vehicle information
Export Vehicle Information	Click **Export All** to save the vehicle information of the list (CSV file) to your PC, which can be imported to other vehicle list.

Chapter 15 Manage Person List

You can add person information to the system for further operations such as access control (adding the person to access group), face comparison (adding the person to face comparison group), time and attendance (adding the person to attendance group), etc. After adding the persons, you can edit and delete the person information if needed.

Note

Up to 10,000 persons can be managed in the system.

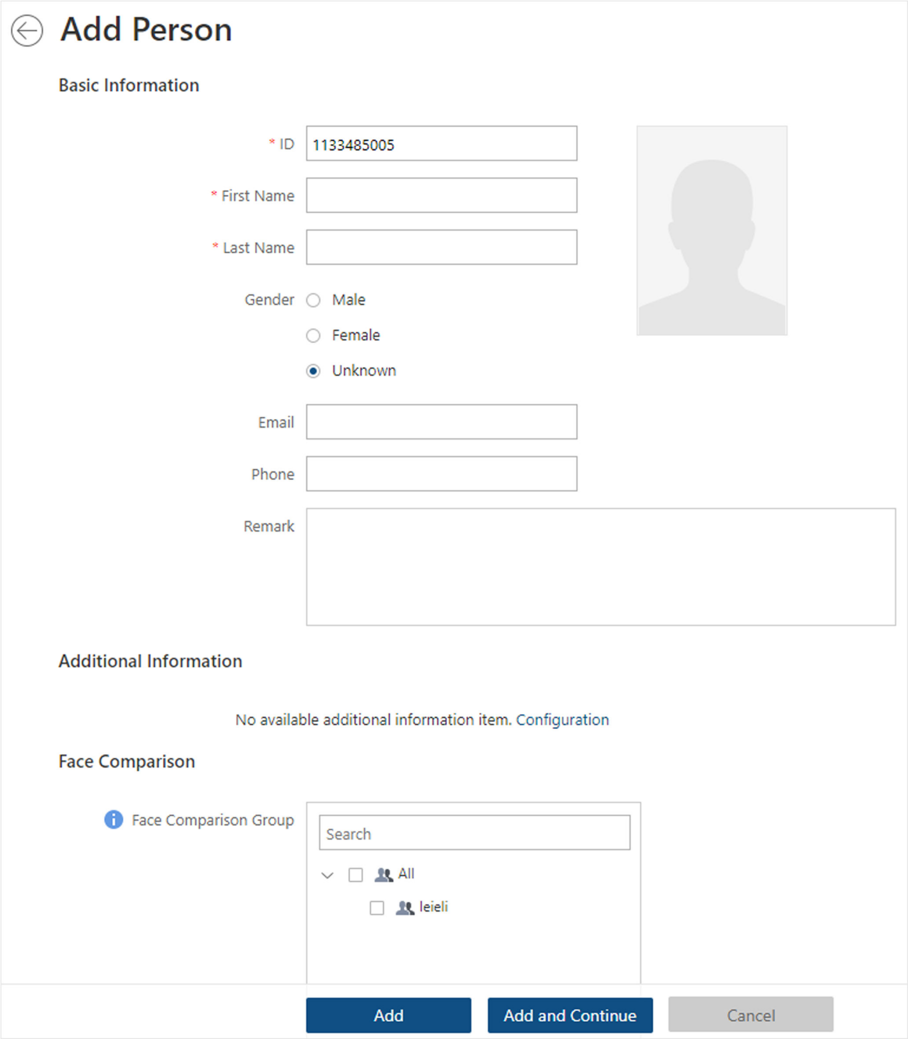
15.1 Add a Person

You can add the person information to the system one by one.

Perform this task if you want to add the person information one by one.

Steps

1. Click **Person → Person List → Add** to enter the adding person page.



Add Person

Basic Information

* ID 1133485005

* First Name

* Last Name

Gender ○ Male ○ Female ● Unknown

Email

Phone

Remark

Additional Information

No available additional information item. Configuration

Face Comparison

Face Comparison Group

Search

□ All

□ leieli

Figure 15-1 Add a Person

2. Set the person basic information.

ID

The default ID is generated by the system. You can edit it if needed.

Note

It should contain 1 to 16 characters and the first character cannot be 0.

Person Picture

Upload a person's face picture. You can click **Take a Picture** to use the PC's webcam to take a picture. Or click **Upload Picture** to select a picture from your PC.

Note

It is recommended that the face in the picture should be in full-face view directly facing the camera, without a hat or head covering.

3. **Optional:** Set the person's additional information.

   Note

   You can customize these items according to actual needs as the person's additional information. For details, refer to ***Custom Additional Information*** .

4. **Optional:** Add the person to the existing face comparison group(s) which will be used for face recognition and comparison.

   Note

   After adding the person to the face comparison group, you should apply the face comparison group to a device to make the settings effective. For details about applying face comparison group to the device, refer to ***Apply Face Comparison Group to Device*** .

5. **Optional:** Set the access control and time & attendance information.

   Effective Period

   Set the effective period for the person in access control application and time & attendance application. For example, if the person is a visitor, his/her effective period may be short and temporary.

   Access Group

   Add the person to the existing access group(s) which can be linked with access level(s). The linkage of access level and access group defines the access permission that which person(s) can access which access point(s) in the authorized period.

   You can click the access group name to view its linked access levels.

   Move the cursor to the access level to view its access point(s) and access schedule.

   Note

   You can click **Add New** to add a new access group. For details, refer to ***Add Access Group*** .

   Super User

   If the person is set as a super user, he/she will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.

   Note

   For details about setting these functions, refer to ***Edit Access Point for Current Site*** .

   Extended Access

   When the person accessing door, grant this person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

You should set the door's extended open duration in Logical View. For details, refer to ***Edit Access Point for Current Site*** .

Attendance Group

Add the person to the existing attendance group if your need to monitor the person's working hours and absenteeism.

Note

You can click **Add New** to add a new attendance group. For details, refer to ***Add Attendance Group*** .

Note

The extended access and super user functions cannot be enabled concurrently.

6. Set the person's credential information, including PIN, face credential, card number, fingerprint, and duress credentials.

Note

Up to 50,000 credentials are allowed in total.

PIN

The PIN must be used after card or fingerprint when accessing. It cannot be used independently.

Note

It should contain 1 to 8 digits.

Set Profile as Face Credential

If you want to use turnstile with face recognition function, you need to set the person's profile picture as her\his face credential so that the person can scan her\his face on the face recognition terminal when he/she wants to access the turnstile. Make sure you have uploaded a picture as the person profile.

Card

Issue a card to the person to assign the card number to the person. You can enter the card number manually, or swipe a card on the card enrollment station or card reader to get the card number, and then issue it to the person.

a. Click **+** in the **Card** field.

b. Place the card that you want to issue to this person on the card enrollment station or on the card reader and the card number will be read automatically. Or you can enter the card number manually

Note

If the card enrollment station is not detected or the issuing configuration is incorrect, you can click **Configuration** to set the issuing mode. For details, refer to ***Set Card Issuing Parameters*** .

c. Set the card's effective period if the card is used for temporary purpose. If the card is set with effective period, other cards linked to this person will be inactive, and the fingerprints and profile linked to these inactive cards will be linked to this card with effective period. After deleting the card with effective period, these inactive cards will recover to active, and their previously linked fingerprints and profile will recover, too.

Note

Up to 5 cards can be issued to one person.

Fingerprint

After connecting the fingerprint recorder to your PC, click **+**, place and lift your fingerprint on the recorder following the prompts and it will collect your fingerprint automatically.

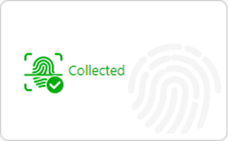


Figure 15-3 Fingerprint Recorded

Note

Up to 10 fingerprints can be added to one person.

Credential under Duress

Set the credentials (card number and fingerprint) so that when you are under duress, you can swipe the card or scan the fingerprint configured here. The door will be unlocked and the Control Client will receive a duress alarm (if configured) to notify the security personnel.

Note

When the person accesses with credentials under duress, he/she cannot be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization. Extended access is not allowed as well.

7. Finish adding the person.

- Click **Add** to add the person and return the person list.
- Click **Add and Continue** to add the person and continue to add other persons.

The person will be displayed in the person list and you can view the details.

8. **Optional:** After adding the person, you can do one or more of the followings:

Edit Person	Click the person name to edit the person details.

Delete Person	Select the person(s) and click **Delete** to delete.
Export Added Person Information	Click **Export All** to export all the added person information and you can save the file in your PC. For data security, you are required to set a password before exporting which is required when decompressing the downloaded ZIP file.

15.2 Batch Add Persons

You can add the information of multiple persons to the system by importing a template with person information.

Perform this task when you need to batch add information of multiple persons.

Steps

1. Click **Person → Person List** to enter the person list page.
2. Click **Import → Import Persons** .
3. Click **Download Template** to download the template file and you can save it in your PC.
4. In the downloaded template, enter the person information following the rules in the template.
5. Click **Import → Import Persons** .
6. Select the template with the person information
7. Click **Import** to start importing.

   Note

   If the exported person's ID is same with the added person in the list, it will replace the added person's information.

   The importing progress shows and you can check the results.
8. **Optional:** After adding the person, you can do one or more of the followings:

Edit Person	Click the person name to edit the person details.
Delete Person	Select the person(s) and click **Delete** to delete the person(s).
Export Added Person Information	Click **Export All** to export all the added person information and you can save the file in your PC. For data security, you are required to set a password before exporting which is required when decompressing the downloaded ZIP file.

15.3 Import Domain Persons

You can import the users in the AD domain in a batch to the system as persons. After importing the person information (including person name and account name) in the AD domain, you can set other information for the persons, such as credentials.

Before You Start

You should configure the active directory settings. See ***Set Active Directory*** for details.

Steps

1. Click **Person → Person List** to enter the Person List Management page.
2. Click **Import → Import Domain Persons** to enter the following page.

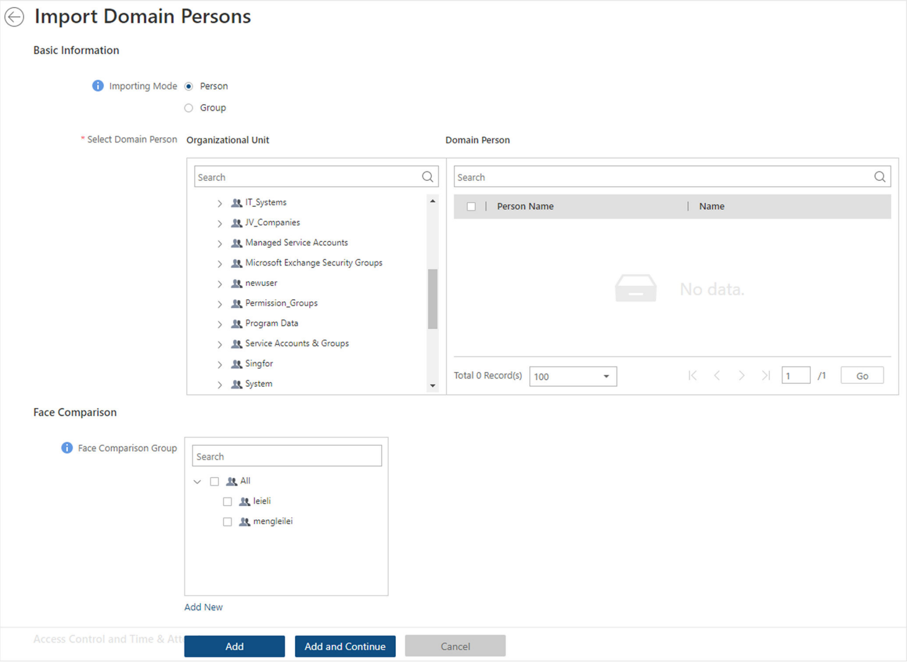


Figure 15-5 Import Domain Persons

3. Select the importing mode.

   Person

   Import the specified persons. Select the organization unit and select the persons under the organization unit which are displayed in the Domain Person list on the right. It will synchronize person information based on each person.

   Group

   Import all the persons in the organization unit. It will synchronize person information based on each group.

4. Add the persons to the existing face comparison group(s) which will be used for face recognition and comparison.

   Note

   After adding the persons to the face comparison group, you should apply the face comparison group to a device to make the settings effective. For details about applying face comparison group to the device, refer to ***Apply Face Comparison Group to Device*** .

5. Set the access control and time & attendance information.

Effective Period

Set the effective period for the person in access control application and time & attendance application. For example, if the person is a visitor, his/her effective period may be short and temporary.

Access Group

Add the persons to the existing access group(s) which can be linked with access level(s). The linkage of access level and access group defines the access permission that which person(s) can access which access point(s) in the authorized period.

You can click the access group name to view its linked access levels.

Move the cursor to the access level to view its access point(s) and access schedule.

Note

You can click **Add New** to add a new access group. For details, refer to ***Add Access Group*** .

Super User

If the persons are set as super users, they will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first card authorization.

Note

For details about setting these functions, refer to ***Edit Access Point for Current Site*** .

Extended Access

When the persons accessing access point, grant these person more time to pass through doors which have been configured with extended open duration. Use this function for the persons with reduced mobility.

Note

You should set the access point's extended open duration in Logical View. For details, refer to ***Edit Access Point for Current Site*** .

Attendance Group

Add the persons to the existing attendance group if your need to monitor the persons' working hours and absenteeism.

Note

You can click **Add New** to add a new attendance group. For details, refer to ***Add Attendance Group*** .

Note

The extended access and super user functions cannot be enabled concurrently.

6. Complete importing the domain persons.
   - Click **Add** to add the persons.

- Click **Add and Continue** to save the settings and continue to add persons.

7. **Optional:** After importing the person information in the domain to the system, if the person information in domain is changed, click **Synchronize Domain Persons** to get the latest information of the persons imported to the system. If the persons are imported by group, it will synchronize the latest person information from the domain group (including added persons, deleted persons, edited persons, etc., in the group).

15.4 Batch Add Profiles

You can add multiple person pictures to the system by importing a ZIP file containing person pictures.

Before You Start
Name the person picture after the person ID and packet the person pictures to a ZIP file.

Note

- Currently it supports pictures in JPG, JPEG, and PNG format.
- Recommendation for each picture: Dimensions: 295×412. Size: 60 KB to 100 KB.
- The ZIP file should be smaller than 100 MB, or the uploading will fail.

Perform this task when you need to batch add person profiles to the system.

Steps

1. Click **Person → Person List** to enter the person list page.
2. Click **Import → Import Profiles** .
3. Select the ZIP file containing the person pictures
4. Click **Import** to start importing.

   The importing progress shows and you can check the results.

15.5 Batch Issue Cards to Persons

The system provides a convenient way to issue card to multiple persons in a batch.

Perform this task when you need to issue the cards to multiple persons in a batch.

Steps

Note

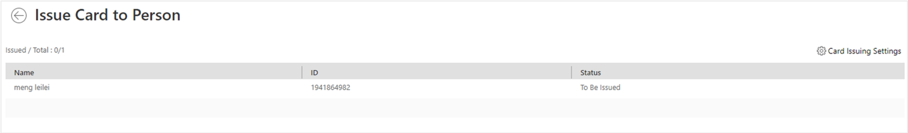
- Up to 5 cards can be issued to one person.
- You cannot issue cards to persons who have cards with effective period.

1. Click **Person → Person List** to enter the person list page.

Note

The selected persons who have less than 5 cards will be displayed.

2. Select the persons to issue the card to.
3. Click **Credential Management → Batch Issue Cards to Persons** to enter the following page.



Issue Card to Person

Issued / Total : 0/1

Name	ID	Status
meng leilei	1941864982	To Be Issued

Figure 15-7 Issue Card to Persons in Batch

4. Click **Card Issuing Settings** to select the issuing mode and set the parameters.

Note

For details about setting the card issuing mode and parameters, refer to ***Set Card Issuing Parameters*** .

5. Place the card on the card enrollment station or swipe the card on the card reader according to the issuing mode you select.

   The card number will be read automatically and the card will be issued to the first person in the list.
6. Repeat the above step to issue the cards to the persons in the list in sequence.
7. Click **Save**.

15.6 Set Card Issuing Parameters

X-VMS provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the Web Client, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

Steps

1. Click **Person** on the home page and enter the **Person List** page.
2. You can enter the card issuing parameters settings page when adding single person or issuing cards to persons in a batch.
   - For entering the card issuing parameters settings page when adding single person, refer to ***Add a Person*** .
   - For entering the card issuing parameters settings page when issuing cards to persons in a batch, refer to ***Batch Issue Cards to Persons*** .
3. Set the issuing mode and set related parameters.

   Card Enrollment Station

Connect a card enrollment station to the PC running the Web Client. You can place the card on the card enrollment station to get the card number.

If you select this mode, you should set the card format and card encryption function.

Card Format

If the card is Wiegand card, select **Wiegand**. Otherwise select **Normal**.

Card Encryption

If you set the card format as ***Normal***, you can enable the card encryption function for security purpose. After enabled, you should enable the card encryption in the access control device's configuration page to take effect.

Card Reader

Select one card reader of one access control device added to the system. You can swipe the card on the card reader to get the card number.

Note

- One card reader can be set to issue card by up to one user at the same time.
- If you set a third-party card reader to read the card number, you should set the device's custom Wiegand protocol to configure the communication rule first.

4. Click **Save**.

15.7 Custom Additional Information

You can customize the additional information items which are not pre-defined in the basic information according to actual needs.

Perform this task if you want to customize the additional information.

Steps

Note

Up to 20 additional information can be customized.

1. Click **Person → Person List → Custom Additional Information** to enter the custom addition information page.
2. Click **Add**.
3. Create a name for this item.

   Note

   Up to 32 characters are allowed in the name.

4. Click **Save**.
5. **Optional:** After adding the additional information, you can do one or more of the followings.

   Edit Name Click ✎ to edit its name.

Delete	Click × to delete the additional information. **Note** The additional information which is linked with person information in domain cannot be deleted.

Chapter 16 Manage Access Control

After adding the persons to the person list, you can assign the access permission to persons to define when they can get access to which door(s). To define the access permission, you should create an access level to group the doors and an access group to group the persons. After assigning the access level to the access group, the persons in the access group will be authorized to access the doors in the access level with their credentials during the authorized time period.

16.1 Add Access Group

Access group is a group of persons who have the same access permission. The persons in the access group can access the same doors (the doors in the linked access level) during the same authorized time period. You need to assign the access level(a) to the access group so that these persons in the access group can access the door(s) in the access level.

Before You Start

Add person to the system, for details, refer to ***Manage Person List*** .

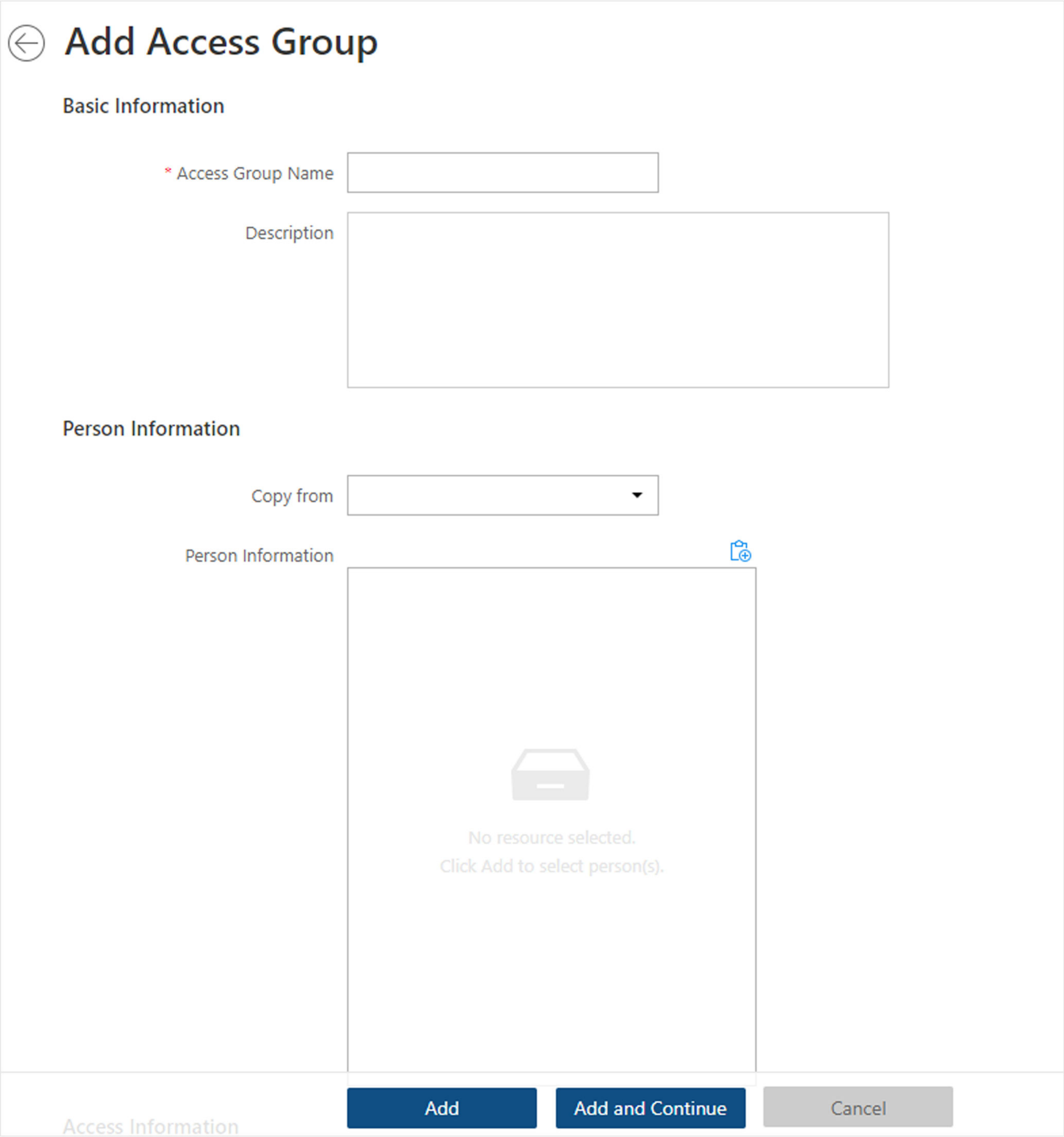
Perform this task to add an access group.

Steps

Note

Up to 64 access groups can be added.

1. Click **Person → Access Group → Add** to enter the adding access group page.



Add Access Group

Basic Information

* Access Group Name

Description

Person Information

Copy from

Person Information

No resource selected.
Click Add to select person(s).

Access Information

Figure 16-1 Add Access Group

2. Set the basic information.

Access Group Name

Create a name for the access group.

3. Optional: Set the person(s) to add to the access group.

1) Click .

   All the persons added to the system display. You can view the person name, picture, person ID, and remark information.
2) Select the person(s) to add to the access group.
3) **Optional:** You can also select the existing access group or attendance group from the **Copy from** drop-down list to copy person information from other group.

   Note

   For setting the attendance group, refer to ***Add Attendance Group*** .

Note

Up to 1,000 persons can be added to one access group.

4. **Optional:** Select the access level(s) to link the access group to the access level(s) so that the person(s) you selected in step 3 can access the doors linked to the access level(s) during the authorized time period.

Note

- Up to 8 access levels can be assigned to one access group.
- You can click **Add New** to add a new access level. For details, refer to ***Add Access Level*** .
- Move the cursor to the access level and you can view its door(s) and access schedule.

5. Finish adding the access group.
   - Click **Add** to add the access group and return to the access group management page.
   - Click **Add and Continue** to add the access group and continue to add other access groups.
6. **Optional:** After adding the access group, you can do one or more of the followings.

Edit Access Group	Click in the Operation column to edit its details.
Delete Access Group	Click × in the Operation column to delete it.
Delete All Access Groups	Click **Delete All** to delete all the added access groups.

16.2 Manage Access Level

In access control, access level is a group of door(s). After assigning the access level to certain access group(s), it defines the access permission that which person(s) can get access to which door(s) during the authorized time period.

16.2.1 Add Access Level

To define the access permission, you need to add an access level first and group the doors.

Perform this task if you need to add an access level.

Steps

Note

Up to 128 access levels can be added to the system.

1. Click **Access Level** on the Home page to enter the access level management page.
2. Click **Add**.

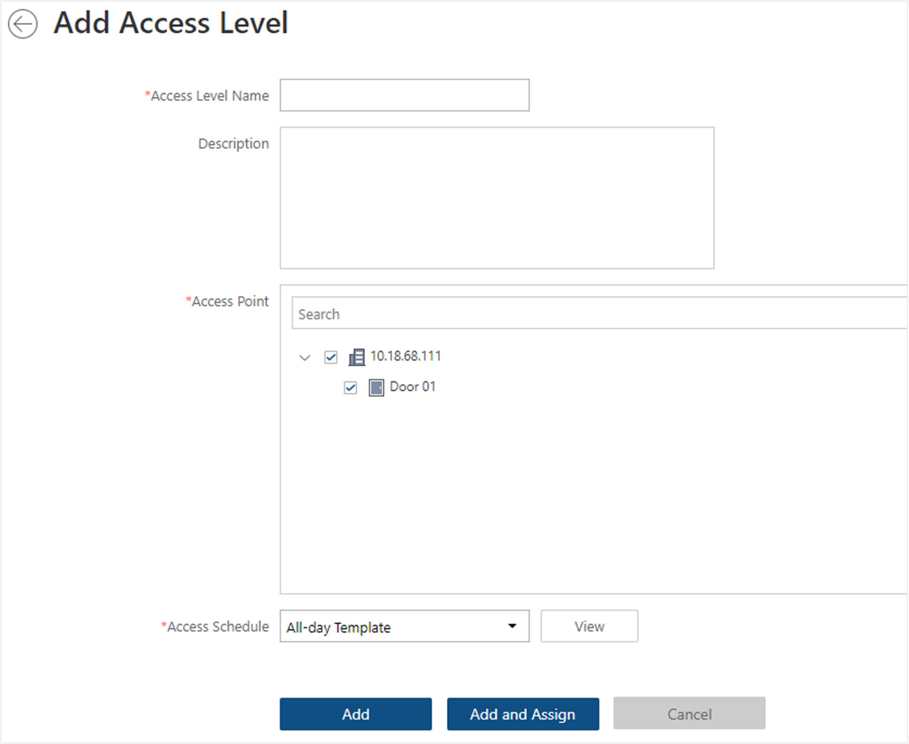


Figure 16-2 Add Access Level

3. Create a name for the access level.
4. **Optional:** Enter the description for the access level.
5. Select the door(s) to add the door(s) to the access level.
6. Select the access schedule to define in which time period, the persons are authorized to access the doors (selected in step 5).

   Note

   The default and customized access schedules are displayed in the drop-down list. You can click **Add New** to customize a new schedule. For details, refer to ***Set Access Control Schedule Template*** .

7. Finish adding the access level.
   - Click **Add** to add the access level and return to the access level management page.
   - Click **Add and Assign** to assign the access level to some access group(s) so that the person(s) in the access group(s) will have the access permission to access the door(s) selected in step 5.

Note

- For details about assigning the access level to the access group, refer to ***Assign Access Level to Access Group*** .
- For setting the access group, refer to .

8. **Optional:** After adding the access level, you can do one or more of the followings.

Edit Access Level
Click ✎ in the Operation column to edit its details. If you want to change the assigned access group(s), or assign it to another access group, click **Configuration**.

Assign to Access Group
Click ✐ in the Operation column to assign the access level to the added access group(s). For details, refer to ***Assign Access Level to Access Group*** .

Delete Access Level
Click ✕ in the Operation column to delete the access level.

Delete All Access Levels
Click **Delete All** to delete all the added access levels.

16.2.2 Assign Access Level to Access Group

After adding the access level, you need to assign it to access group(s). After that, the persons in the access group(s) will have the permission to access the door(s) linked to the access level.

Before You Start
Add the access group(s). For details, refer to .

Perform this task if you need to assign the access level to the access group(s).

Steps

Note

You can also link the access group to access level(s) when adding or editing the access group. The latest configured linkage will take effect. For details, refer to ***Add Access Group*** .

1. Click **Access Level** on the Home page to enter the access level management page.
2. Enter the Assign to Access Group page.
   - After you setting the parameters of access level when adding, click **Add and Assign**.
   - When editing the access level, click **Configuration** in the access level details page.
   - Click ✐ in the Operation column.
3. In the Assign to Access Group field, select the access group(s) you want to assign the access level to.
4. **Optional:** Click **Add New** to add a new access group.
5. Click **Save**.

16.3 Apply Persons' Access Levels to Device

After setting the linkage between access group and access levels, or if the person's access level and access group settings are changed, you need to apply the person's access level settings to the access control device of the access point linked to the access level to take effect. After that, the persons in the access group can access the access points during the authorized time period defined by the related access level.

16.3.1 Manually Apply Persons' Access Levels to Device

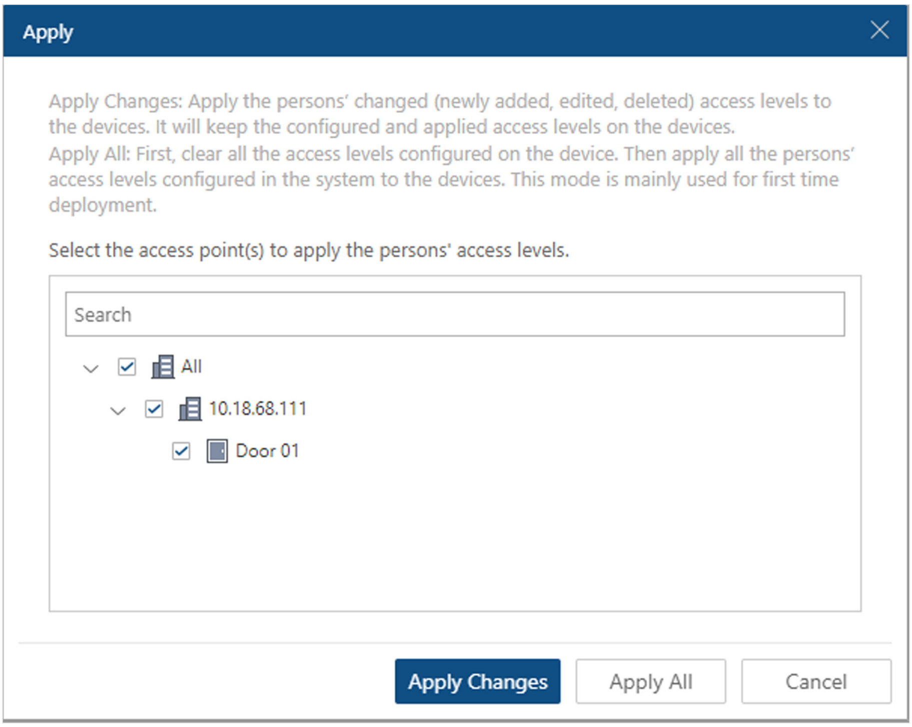
After setting the access levels and assigning access levels to access group, you should apply the relation between persons and access points to the access control device. In other words, after setting or changing the access groups and access levels, you need to apply these settings to the access control device to take effect.

Before You Start

Link the access group with access level to define the access permission. For details, refer to ***Assign Access Level to Access Group*** or ***Add Access Group*** .

Steps

1. Click **Person → Access Group** to enter the access group management page.
2. Click **Apply to Device** to open the Apply window.



Apply Changes: Apply the persons' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices.

Apply All: First, clear all the access levels configured on the device. Then apply all the persons' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

Select the access point(s) to apply the persons' access levels.

Figure 16-3 Apply to Device Manually

3. Select the access point(s) to apply the persons' access levels.

4. Select the applying mode.

   Apply Changes

   Apply the persons' changed (newly added, edited, deleted) access levels to the devices. It will keep the configured and applied access levels on the devices.

   Apply All

   First, clear all the access levels configured on the device. Then, apply all the persons' access levels configured in the system to the devices. This mode is mainly used for first time deployment.

   During this process, the devices will be offline for a while, and persons cannot access via these access points.

5. **Optional:** If the person's access permission settings are changed (such as changes in linked access level, person credentials, etc.), the ⓘ icon will display near the **Apply to Device** icon, indicating that these new access permission settings should be applied to the device. You can hover the cursor to it to view that the access levels of how many persons' should be applied to the device.

16.3.2 Regularly Apply Person's Access Levels to Devices

Besides manually applying to device, you can also set a schedule and the system can apply the access levels assigned to persons configured in the system to the device automatically every day.

Before You Start

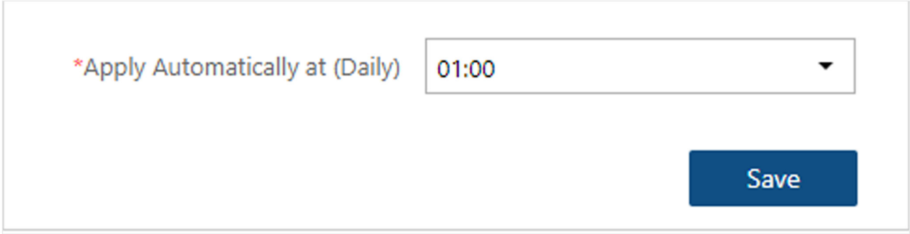
Link the access group with access level to define the access permission. For details, refer to ***Assign Access Level to Access Group*** or ***Add Access Group*** .

Steps

Note

By default, the system will apply the persons' access levels automatically to the device at 01:00 every day.

1. Click **Person → Access Group** to enter the access group management page.
2. Click **Apply to Device (Scheduled)** to open the following window.



*Apply Automatically at (Daily) 01:00

Figure 16-4 Apply to Device Regularly

3. Set a time and the system will apply the changed access levels linked with persons, as well as the applying failed access levels, to device at the configured time automatically.

Note

The time here is the VSM server's time.

4. Click **Save**.

16.4 Set Access Control Schedule Template

The access control schedule defines when the person can open the access point with credentials, or when the access point remains unlocked so that person can open the access point with free access. The system predefines three default access control schedule templates: All-day Template, Weekday Template, and Weekend Template. You can also add a customized template according to actual needs.

Perform this task to set the customized access control schedule.

Steps

1. Click **System** on the home page.
2. Click **Schedule → Access Schedule Template** tab on the left.
3. Click **Add** in the Access Schedule page to enter the adding access schedule template page.

   Note

   You can add up to 32 templates.

4. Set the required information.

   Name

   Set a name for the template.

   Copy from

   Optionally, you can select to copy the settings from other defined templates.

5. Draw a time period on the time bar.

   Note

   Up to 8 time periods can be set for each day.

6. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.
7. **Optional:** Set the holiday schedule. The priority of holiday schedule is higher than the weekly schedule which means the predefined holidays will adopt the holiday schedule rather than the weekly schedule.
   1) Click **Add Holiday**.
   2) Select the predefined holiday(s), or click **Add New** to create a new holiday (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Draw a time period on the time bar.

Note

Up to 8 time periods can be set for each day.

5) **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding drawn time period.

8. Finish adding the access control schedule template.
   - Click **Add** to add the template and back to the access control schedule template list page.
   - Click **Add and Continue** to add the template and continue to add other template.

   The access control schedule template will be displayed on the access control schedule template list.

9. **Optional:** Perform the following operations after adding the template.

View Template Details	Click the template to view its details.
Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click × in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the schedule templates (except the default templates and the template(s) in use).

16.5 Configure Anti-Passback Rules

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which cards must be used in order to grant access. The person should exit via the access point in the anti-passback if he/she enters via the access point in the anti-passback.

Steps

1. Click **Logical View** on the home page.
2. Select one area which contains the access point you want to configure an anti-passback rule for.
3. Click ✎ to enter the editing area page.
4. In the Anti-Passback field, click **Add** to add an anti-passback rule.

   In the Add Anti-Passback page, all the areas with access points display.
5. Select the access point(s) to add to the anti-passback rule.

   Note

   - Up to 16 access points can be added to one anti-passback rule.
   - Select at least one access point in the current area.

6. Click **Add**.

   The anti-passback rule is added in the table and you can view the access points in the rule.

Chapter 17 Manage Time and Attendance

After adding the persons to the person list, if you want to track and monitor when the persons start/stop work and monitor their working hours and late arrivals, early departures, time taken on breaks, and absenteeism, you can add the person to the attendance group and assign a shift schedule (a rule for the attendance defining how the schedule repeats, the shift type, break settings, and the card swiping rule.) to the attendance group to define the attendance parameters for the persons in the attendance group.

17.1 Add Attendance Group

After adding the persons, you can group the persons into different attendance groups. The persons in the same attendance group are assigned with the same shift schedule.

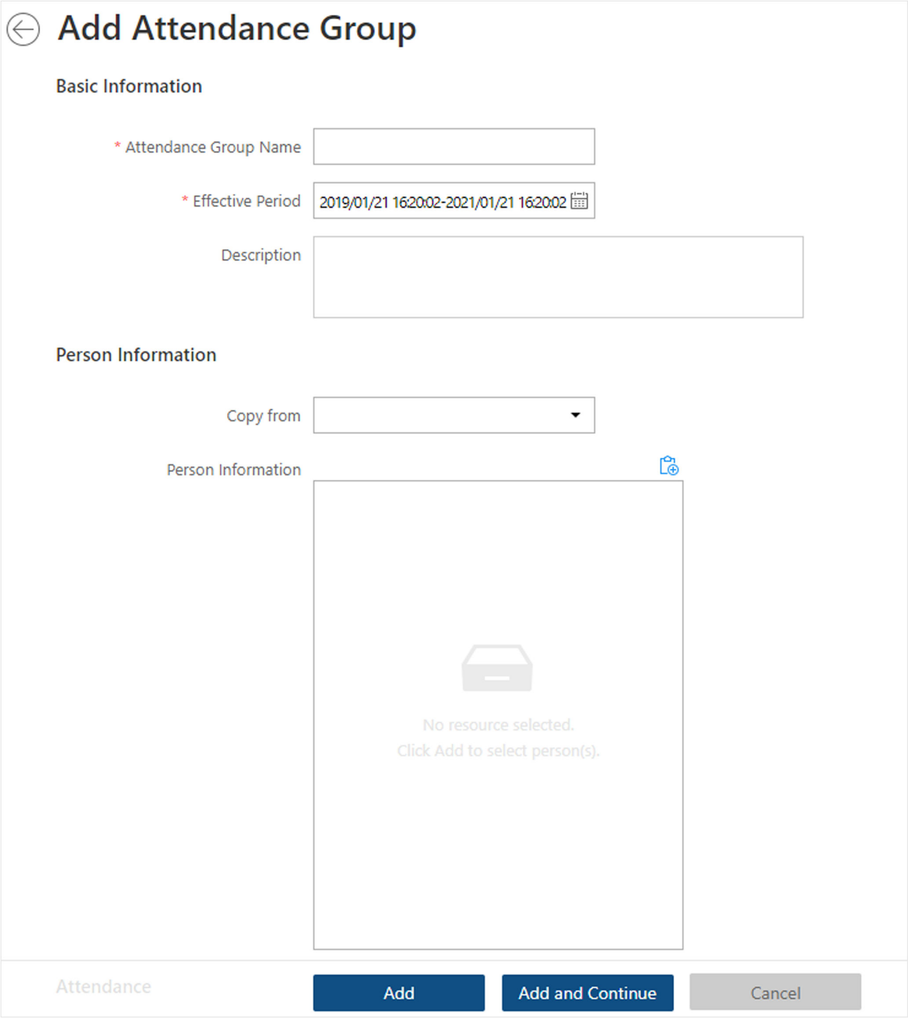
Perform this task if you need to group the persons into different attendance group.

Steps

Note

- Up to 64 attendance groups can be added.
- For each person, he/she can be added to up to one attendance group.

1. Click **Person → Attendance Group → Add** to enter the adding attendance group page.



Add Attendance Group

Basic Information

* Attendance Group Name

* Effective Period: 2019/01/21 16:20:02-2021/01/21 16:20:02

Description

Person Information

Copy from

Person Information

No resource selected.
Click Add to select person(s).

Figure 17-1 Add Attendance Group

2. Set the basic information of the group.

   Attendance Group Name

   Create a name for the attendance group.

   Effective Period

   Set the effective period for the group. Once expired, the attendance records of the persons in the group will not be recorded.

3. Set the person(s) to add to the attendance group.
   1) Click .

      All the persons added to the system display. You can view the person name, picture, and person ID.
   2) Select the person(s) to add to the attendance group.
   3) **Optional:** You can also select the existing access group from the **Copy from** drop-down list to copy the person information from other groups.

Note

For setting the access group, refer to ***Add Access Group*** .

Note

Up to 1,000 persons can be added to one attendance group.

4. **Optional:** Set the shift schedule for the persons in the group so that they need to attend according to this shift schedule.

   Note

   Click **Add New** to add a new shift schedule. For details, refer to ***Add Shift Schedule*** .

5. Finish adding the attendance group.
   - Click **Add** to add the attendance group and return to the attendance group list page.
   - Click **Add and Continue** to add the attendance group and continue to add other groups.
6. After adding the attendance group, you can do one or more of the followings:

Edit Attendance Group	Click ✎ in the Operation column to edit its details.
Delete Attendance Group	Click × in the Operation column to delete it.
Delete All Attendance Groups	Click **Delete All** to delete all the added attendance groups.

17.2 Add Shift Schedule

An shift schedule is an attendance schedule which defines the scheduled work time and how it repeats. You can create an shift schedule to compare the employees' attendance with it so as to identify those who are tardy, leave early, take long break, or are absent, etc.

Perform this task to add a shift schedule.

Steps

Note

Up to 128 shift schedules can be added to the system.

1. Click **Time & Attendance → Shift Schedule → Add** to enter the adding shift schedule page.
2. Set the shift schedule's basic information, including a custom name and the description.
3. **Optional:** Select another shift schedule from the drop-down list of **Copy from** field to copy the schedule information to the current schedule. You can edit the schedule settings on this basis.
4. Set the schedule's repeating mode.

   Week

   The schedule will repeat every 7 days based on the week.

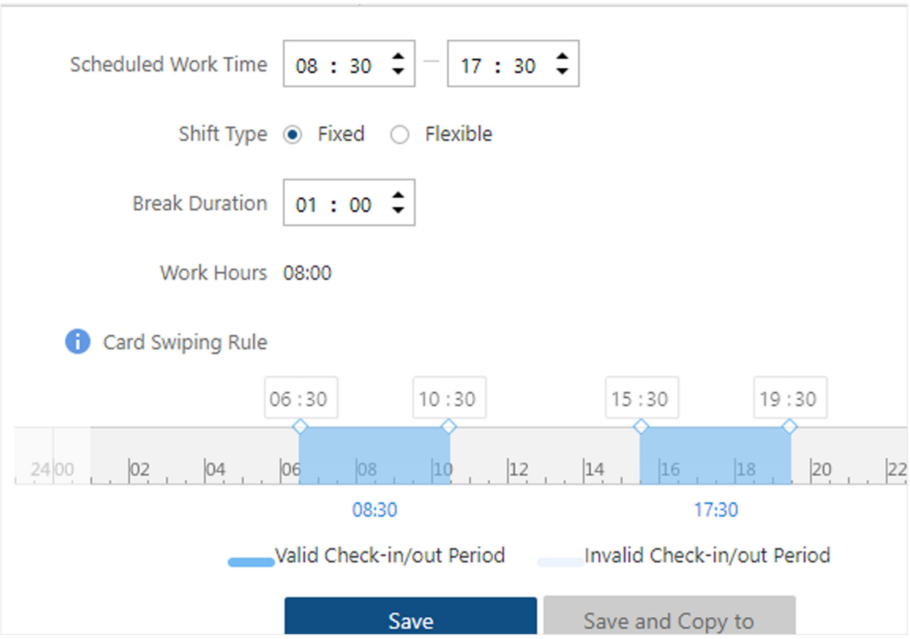
   Day(s)

You can customize the number of days in one period. You should set a start date of one period for reference which can define how the schedule repeats.

5. Draw the scheduled work time on the timeline.

1) Drag on the timeline to set the range of the scheduled work time.

   The detailed schedule rule parameters will be displayed.



Scheduled Work Time 08 : 30 — 17 : 30

Shift Type ● Fixed ○ Flexible

Break Duration 01 : 00

Work Hours 08:00

Figure 17-2 Set Detailed Schedule Rule

2) **Optional:** Edit the required work time to make it more accurate if necessary.
3) Select the shift type.

   Fixed

   The scheduled start-work time and end-work time is fixed. Only when the employee checks-in before the start-work time and checks-out after the end-work time, the attendance status is normal. Or it may be late, early leave, or absent.

   Flexible

   Flexible work schedule is an alternative to the fixed schedule. It allows employees to extend their start-work time and end-work time and you can set the allowable extended duration for both start-work and end-work time.
4) **Optional:** For flexible schedule, set the flexible duration, which defines the extended duration for both start-work and end-work time. During this flexible schedule, the check-in/out will be recorded and the status will be **Normal**.

   Example

   If the required work time is set as 09:00 to 18:00, and the flexible duration is 30 min, if the employee checks-in at 09:15, and checks-out at 18:15, the attendance status on that day will be **Normal**.
5) Set the break duration such as lunch time.

For fixed schedule, the required work hours will be calculated automatically according to the above settings (except flexible duration).

6) **Optional:** For flexible schedule, set the minimum work hours.
7) Set the valid check-in/out period on the timeline. If the employee checks-in/out during the valid check-in/out period, the check-in/out will be recorded and the attendance status will not be absent.
8) Click **Save**. You can click **Save and Copy to** to copy the schedule to other days.

6. Select the holidays on which days the shift schedule will not be effective.

Note

For setting the holiday, refer to ***Set Holiday*** .

7. Finish adding the shift schedule.
- Click **Add** to add the shift schedule and return to the shift schedule management page.
- Click **Add and Assign** to add the shift schedule and assign it to the attendance group. For details, refer to ***Assign Shift Schedule to Attendance Group*** .

17.3 Assign Shift Schedule to Attendance Group

After setting the shift schedule, you need to assign it to the attendance group so that it will calculate the attendance records for persons in the attendance group according to this shift schedule.

Before You Start

- Add a shift schedule and set the rule. For details, refer to ***Add Shift Schedule*** .
- Add an attendance group. For details, refer to ***Add Attendance Group*** .

Perform this task to assign a shift schedule to attendance group(s).

Steps

1. Click **Time & Attendance → Shift Schedule** to enter the shift schedule management page.

2. Enter the Assign to Attendance Group page.
- After you set the parameters of shift schedule when adding, click **Add and Assign**.
- When editing the shift schedule, click **Configuration** in the shift schedule details page.
- Click ⇲ in the Operation column.

3. In the Assign to Attendance Group field, select the attendance group(s) you want to assign the shift schedule to.

Note

Only the attendance groups which haven't been linked to a shift schedule will display.

4. **Optional:** Click **Add New** to add a new attendance group.

5. Click **Save**.

17.4 Add Attendance Check Point

You should set a door as an attendance check point, so that the check-in/out by credentials (such as swiping card on the door's card reader) will be valid and will be recorded.

Perform this task to add a attendance check point.

Steps

1. Click **Time & Attendance → Attendance Check Point** to enter the attendance check point management page.
2. Click **Add**.

   All the doors which haven't been set as attendance check point will be displayed.
3. Select the door(s).
4. Click **Add**.

   The selected door(s) will be displayed in the attendance check point list.
5. To delete the added attendance check point, select the door(s) and click **Delete**.

Note

If the attendance check point is deleted, the attendance records on this attendance check point will be deleted as well, and it will affect the persons' attendance results for the days on which the attendance data haven't been calculated.

17.5 Manage Attendance Record

The persons' attendance records will be recorded and stored in the system. You can search the records by setting the search conditions to view the attendance details and view the person's attendance report. You can also correct check-in/out time for the exceptional records according to actual needs.

17.5.1 Search Attendance Record

You can search the attendance records to view the person's attendance status by setting the search conditions.

Before You Start

Make sure the person's attendance group is not expired. Or the attendance records will not be recorded. For setting the attendance group's effective period, refer to ***Add Attendance Group*** .

Perform this task to search the attendance records.

Steps

1. Click **Time & Attendance → Attendance Record** to enter the attendance record page.
2. In the filter panel, set the search conditions.

Time

Set the time range of the attendance records you want to search. You can search the persons' attendance records recorded within one year.

3. Click **Filter** to filter the attendance records according to the search conditions.

   If you search the attendance records on one day, you can view the persons' attendance status and detailed work time (including scheduled work time and actual work time).

   If you search the attendance records on multiple days, you can view the persons' attendance report including the times of normal, late, early leave, absent status during the time period, and the total work hours.
4. **Optional:** If you search the attendance records on multiple days, hover the cursor on the number of late, early leave, or absent times to view the specific date.
5. **Optional:** Click the person name to view the person's attendance records.

   Note

   Hover the cursor on the date to view the detailed work time, including scheduled work time and actual work time.
6. **Optional:** You can also correct the check-in/out for the exceptional attendance status if necessary. For details, refer to ***Correct Attendance Record for Single Person*** .
7. **Optional:** Click **Export** and select the items to export the filtered attendance records and save in your PC.

   Note

   The exported file is in CSV format.

17.5.2 Correct Attendance Record for Single Person

After searching the person's attendance record, you can correct one person's check-in/out time according to actual needs if the attendance status is not normal.

Perform this task if you need to correct the person's attendance check-in/check-out time.

Steps

1. Click **Time & Attendance → Attendance Record** to enter the attendance record page.
2. Search the attendance records.

   Note

   For details, refer to ***Search Attendance Record*** .
3. **Optional:** If you search the attendance records on one single day, you can perform the following steps to correct the check-in/out time.
   1) Click 📅 in the Operation column.
   2) Set the correct check-in/out time.

3) **Optional:** Enter the reason for correction.
4) Click **OK**.

   The person's attendance status on that day changes according to the correction.

4. **Optional:** If you search the attendance records on multiple days, you can perform the following steps to correct the check-in/out time.
   1) Click the person name to enter the detailed attendance record page.

      The person's attendance statuses are displayed on the calendar.
   2) Hover the cursor to the date which attendance status is not normal and click **Correct Check-in/out**.
   3) Set the correct check-in/out time.
   4) **Optional:** Enterthe reason for correction.
   5) Click **OK**.

      The person's attendance status on that day changes according to the correction and the icon will show, indicating that the status is corrected.

17.5.3 Correct Attendance Records for Multiple Persons

You can correct multiple persons' check-in/out time in a batch according to actual needs if the attendance status is not normal.

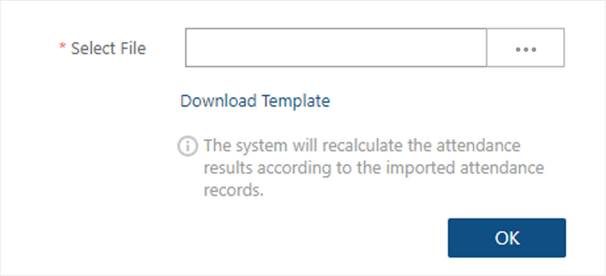
Perform this task if you need to correct multiple persons' check-in/out time.

Steps

Note

Up to 50,000 attendance records can be corrected at a time.

1. Click **Time & Attendance → Attendance Record** to enter the attendance record page.
2. Click **Batch Correct Check-in/out** to open the following window.



The system will recalculate the attendance results according to the imported attendance records.

Figure 17-5 Batch Correct Attendance Records

3. Click **Download Template** to download the template file and you can save it to your PC.
4. In the downloaded template, enter the actual start-work time or/and end-work time following the rules in the template.
5. Click **Batch Correct Check-in/out** and upload the template with the corrected attendance records.
6. Click **OK** and the progress will be displayed.

Note

The system will recalculate the attendance results according to the imported attendance records.

Chapter 18 Manage Face Comparison Group

After adding the persons to the person list, you should create a face comparison group, and then add persons (selected from the person list) to the group before you can perform face comparison. Finally, you need to apply the face comparison group with person information to the face recognition device to take effect. When a person's face is detected and it matches or mismatches the person information in the face comparison group, an event/alarm (if configured) will be triggered to notify the security personnel and you can view the face comparison information during live view on the Control Client.

18.1 Add Face Comparison Group

After adding the person(s), you can add a face comparison group and add person(s) to the group for face comparison.

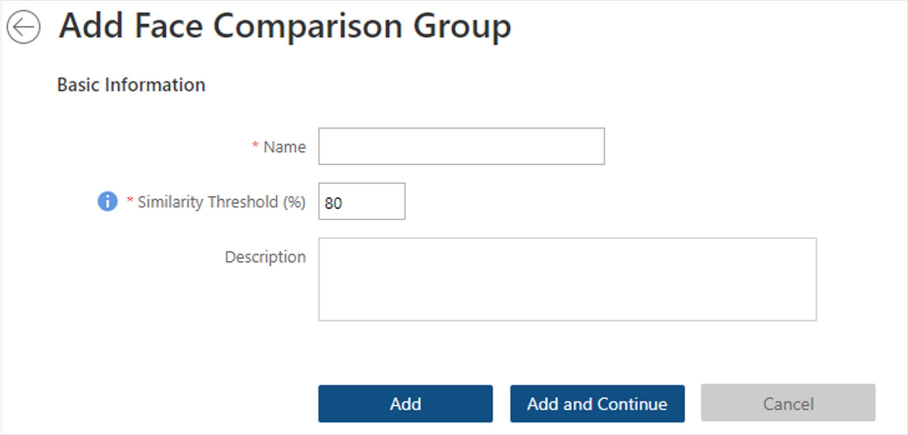
Perform this task if you want to add a face comparison group.

Steps

Note

Up to 64 face comparison groups can be added.

1. Click **Person → Face Comparison Group** to enter the face comparison group management page.



Add Face Comparison Group

Basic Information

* Name

* Similarity Threshold (%) 80

Description

Figure 18-1 Add Face Comparison Group

2. Add a new face comparison group.
   1) Click **Add**.
   2) Create a name for the face comparison group.
   3) Set the face comparison similarity threshold which affects the frequency and accuracy of face picture comparison alarm. When the face comparison similarity is higher than the configured threshold, the camera will regard the person as matched.
   4) **Optional:** Enter the description information if needed.

5) Click **Add** to add the group and go back to the face comparison group list. You can also click **Add and Continue** to add other groups.

3. Add person(s) to the group.

1) In the face comparison group list page, click › to show the persons added to the group.
2) Click **+** to open the following window.

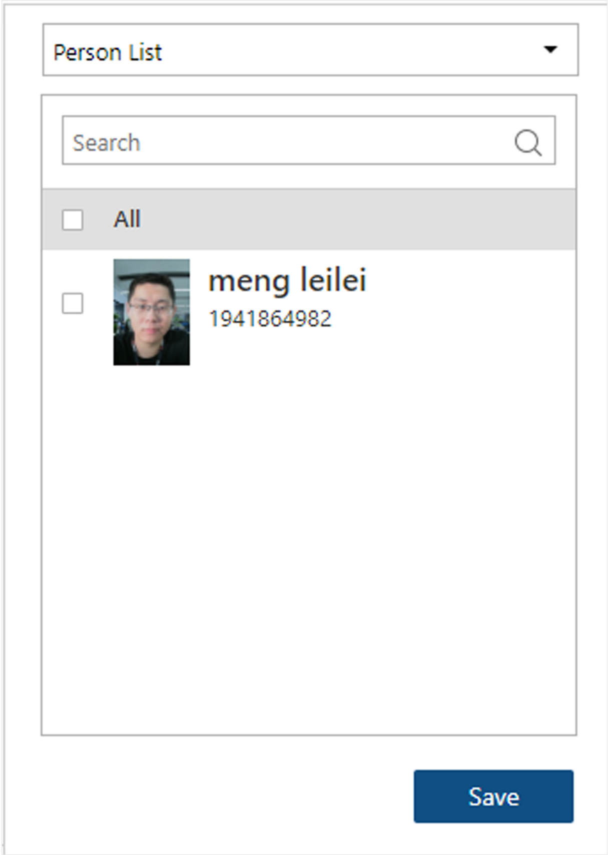


Figure 18-2 Add Person to Face Comparison Group

3) Select the adding mode as **Person List**.

   All the persons in the person list who haven't been added to the current group will be displayed.
4) Select the person(s) to add to the group.
5) Click **Save**.
6) **Optional:** You can also set the adding mode as **Added Face Comparison Group** or **Imported Domain Group** to add the persons in other existing groups to the current group.

Note

The original persons in the current group will not be replaced after adding person from existing group.

Note

Up to 10,000 persons can be added to one face comparison group.

4. **Optional:** After adding the persons to the face comparison group, you can do one or more of the followings.

Remove Person from Face Comparison Group	Hover the cursor to the face picture and click ☒ .
Edit Face Comparison Group	Click ✎ in the Operation column to edit it and view the cameras that it is applied to.
Delete Face Comparison	Click × in the Operation column to delete it.
Delete All Face Comparison Groups	Click **Delete All** to delete all the added face comparison groups.

What to do next

After adding the face comparison group and configuring the persons in the group, apply the group to the camera which supports face picture comparison to take effect. For details, refer to ***Apply Face Comparison Group to Device*** .

18.2 Apply Face Comparison Group to Device

After setting the face comparison group and adding person(s) to the group, you need to apply the group settings to the camera which supports face picture comparison so that the camera can compare the detected faces with the face pictures in the face comparison group and trigger alarms (if configured). After applying the face comparison group to the device, if the data in the group are changed (such as adding a person to the group, removing person from the group, etc.), the system will automatically apply the data in the group to the device to take effect.

Before You Start

Add camera which supports face picture comparison to the system.

Perform this task if you need to apply the person information in the face comparison group to the camera to take effect.

Steps

Note

- Currently it only supports applying to camera which supports face picture comparison.
- The maximum number of groups that can be applied to the camera depends on the camera capability.

1. Click **Person → Face Comparison Group** to enter the face comparison group management page.
2. Click **Apply to Device**.
3. Select the face comparison group(s) to be applied.

4. Select the camera(s) to apply the selected face comparison group(s) to.
5. Click **Apply** to start applying.

   The applying progress will display in the Operation column.
6. **Optional:** If there exists applying failed face comparison group, the ❗ icon will display near the group name. Hover the cursor to the icon to check the prompt.

   Note

   You can click **Retry** to apply this group to the linked camera(s) again. Click **Details** to view the exception details.

Chapter 19 Manage Role and User

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

19.1 Add Role

You can assign the permissions to the roles as required, and the users can be assigned with different roles to obtain different permissions.

Perform this task when you add role.

Steps

1. Click **Security → Roles** to enter the Role Management page.

   Note

   The system pre-defines two default roles: administrator and operator. You can click the role name to view the details and operations. But you cannot edit or delete the two default roles.

   Administrator

   The role that has all the permission of the system.

   Operator

   The role that has all the permission for operating the Control Client and has the permission for operating the Applications (Live View, Playback, and Local Configuration) on the Web Client.

2. Click **Add** to enter the Add Role page.
3. Set the role name, expiry date, and description as desired.

   Expiry Date

   The date that this role becomes invalid.

4. Set the permission for the role.
   - Select the default or pre-defined role from the **Copy form** drop-down list to copy the permission settings of selected role.
   - Assign the permissions to the role.

     Area Display Rule

     Show or hide the specific area(s) for the role. If the area is hidden, the user with the role cannot view and access the area and its resources on any interface.

     Resource Access Permission

Select the functions from the left panel and select resources from right panel to assign the selected resources' permissions to the role.

Note

If you do not check the resources, the resource permission cannot be applied to the role.

User Permission

Assign the resource permissions, configuration permissions on the Web Client, and the control permissions on the Control Client to the role.

5. Complete adding the role.
   - Click **Add** to add the role.
   - Click **Add and Continue** to save the settings and continue to add roles.
6. **Optional:** After adding the role, you can do one or more of the following:

Edit Role	Click the **Name** field to edit the settings of the role.
Refresh Role	Click **Refresh All** to get the latest status of the roles.
Delete Role	Click **Delete** to delete the role.
Filter Role	Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

19.2 Add Normal User

You can add normal users for accessing the system and assign role to the normal user. Normal users refer to all the users except the admin user.

Perform this task when you need to add normal user.

Steps

1. Click **Security → Users** to enter the User Management page.
2. Click **Add** to enter the Add User page.
3. Set the required parameters.

User Name

For user name, only letters(a-z, A-Z), digits(0-9), and - can be contained.

Password

The system provides a default password (Abc123). You can use it or customize a stronger password. However, you must change the initial password for first time login.

Expiry Date

The date when this user account becomes invalid.

Email

The system can notify user by sending an email to the email address. If the normal user forget his/her password, he/she can reset the password via email.

Note

The email address of the admin user can be edited by the user with the role of administrator.

Restrict Concurrent Logins

If necessary, set **Restrict Concurrent Logins** switch to ON and input the maximum number of concurrent logins.

User Status

Two kinds of status are available. If you select freeze, the user account is inactive until you set the user status to active.

4. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example

When user1 and user2 control the PTZ unit at the same time, the user who has the higher PTZ control permission level will take the control of the PTZ movement.

5. Check the existing roles to assign the role(s) for the user.

Note

- If no role has been added, two default roles are selectable: administrator and operator.
  Administrator
  The role that has all permissions of the system.

  Operator
  The role that has all permissions of the system Control Client.
- If you want to add customized roles, you can click **Add New Role** to quickly enter the Add Role page. See ***Add Role*** for details.

6. Complete adding the user.
   - Click **Add** to add the user.
   - Click **Add and Continue** to save the settings and continue to add users.

Note

You will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

7. **Optional:** Perform the following operations after adding the normal user.

Edit User	Click the **Name** field of the user to edit the information
Reset Password	In the Edit User page, click **Reset** to reset password of the user.

Note

- If you reset the password, the user's password will be reset to its initial password Abc123. The user should log in with initial password and then change the password.
- The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. For changing the password, refer to ***Change Password for Reset User*** .

Delete User Click **Delete** to delete the user.

Force Logout You can also select the online user and click **Force Logout** to log out the online user.

Refresh All Click **Refresh All** to get the latest status of the users.

Filter User Click ▽ to expand the filter conditions. Set the conditions and click **Filter** to filter the users according to the set conditions.

Note

The administrator user named admin was pre-defined by default. It cannot be edited ,deleted, or forced to log out.

19.3 Import Domain Users

You can import the users in the AD domain in a batch to the system (including user name, real name, and email) and assign roles to the domain users.

Before You Start

You should configure the active directory settings. See ***Set Active Directory*** for details.

Steps

1. Click **Security → Users** to enter the User Management page.
2. Click **Import Domain Users** to enter the Import Domain Users page.
3. Select the importing mode.

   User

   Import the specified users. Select the organization unit and select the user accounts under the organization unit which are displayed in the Domain User list on the right.

   Group

   Import all the users in the group.

4. **Optional:** Set **Restrict Concurrent Logins** switch to ON and enter the maximum number of concurrent logins.
5. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

Note

The larger the value is, the higher permission level the user has. The user with higher permission level has the priority to control the PTZ unit.

Example

When user1 and user2 control the PTZ unit at the same time, the user who has the higher PTZ control permission level will take the control of the PTZ movement.

6. Check the existing roles to assign the role(s) for the selected domain user.

Note

- If no role has been added, two default roles are selectable: administrator and operator.
  Administrator
  The role that has all permissions of the X-VMS.

  Operator
  The role that has all permissions of the X-VMS Control Client.
- If you want to add customized roles, you can click **Add New Role** to quickly enter the Add Role page. See ***Add Role*** for details.

7. Complete importing the domain user.
   - Click **Add** to add the user.
   - Click **Add and Continue** to save the settings and continue to add users.
8. **Optional:** After importing the user information in the domain to the system, if the user information in domain is changed, click **Synchronize Domain Users** to get the latest information of the users imported to the system. If the users are imported by group, it will synchronize the latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).

Result

After successfully adding the domain users, the users can log in to the X-VMS via the Web Client, Control Client and Mobile Client by their domain account and password.

19.4 Change Password of Current User

When you log in via Web Client, you can change your password as desired.

Perform this task when you need to change the password of the current login user.

Steps

1. Move the cursor on the name of the current user at the top-right corner of the system and .

2. From the drop-down list, select **Change Password** to open the Change Password dialog.
3. Enter the old password, new password, and confirm password.

Caution

The password strength of the device can be checked by the system. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

4. Click **OK** to change the password.

19.5 Reset Password for Admin User

When you forgot the password of admin user, you can reset the password and set a new password for admin user.

Perform this task when you forgot the admin user's password.

Steps

1. In the address bar of the web browser, enter the address of the PC running VSM (Video Surveillance Management Service) and press **Enter**.

   Example

   If the IP address of PC running VSM is 172.6.21.96, you should enter ***http://172.6.21.96*** in the address bar.

   Note

   You should configure the VSM's IP address in **System → WAN Access** before accessing the VSM via WAN. For details, refer to ***Set WAN Access*** .

   A login page will pop up.

2. **Optional:** When you log in via current Internet Explorer browser for the first time, you should install the plug-in before you can access the functions.

   Note

   If a new version of plug-in is detected, you should update it to ensure the proper usage and better user experience.

   1) Click **OK** in the pop-up dialog to install the plug-in. Or click **Download Plug-in** to download it.
   2) Save the plug-in file to your PC and close the web browser.
   3) Find the plug-in that stores on your PC and install the plug-in according to the prompt.

4) Re-open the web browser and log in to the VSM (step 1).

Note

Please allow the browser to run the plug-in in the pop-up prompt.

3. Input ***admin*** in the User Name field.
4. Click **Forgot Password** to open the Reset Password dialog.
5. Enter the required parameters in the pop-up dialog, including activation code, new password, and confirm password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For detailed settings of minimum password strength, refer to ***Manage System Security*** Security.

Caution

The password strength of the device can be checked by the system. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Click **OK** to reset the admin password.

Note

If you forgot the password of other users, contact the administrator user to reset the password and then change the password for login.

19.6 Reset Password for Normal User

If the user forgot the password, he/she can contact the users with administrator role to reset the password.

Perform this task to reset the password for normal user.

Steps

Note

The admin user can reset the passwords of all the other users. Other users with administrator role can reset the passwords of the users without administrator role. See ***Add Normal User*** for details about user's role settings.

1. Click **Security** to enter the Security Management page.
2. Click **Users** on the left.
3. Select one user and click the **Name** field to enter the user details page.
4. Click **Reset** to reset the password of the selected user.

   After resetting the password, the user's password will be reset to its initial password Abc123.

Chapter 20 Maintenance

X-VMS provides backup of the database, so that your data can be well protected and recovered when an exception occurs.

You can also export the system's configuration data and save it to the local PC.

20.1 Set System Data Backup

For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up the data in the system, or configure a schedule to run the backup task regularly. The system data includes data configured in the system, pictures configured in the system, received events and alarms, face comparison data, card swiping data, server logs, etc.

Perform this task when you need to configure the schedule to run the system data backup task regularly or manually back up the data.

Steps

Note

The backups are stored in the VSM server and the default saving path is C:\Program Files (x86)\X-VMS\VSM Servers\VSM\Backup. If you want to edit the default saving path, you should enter Back Up and Restore System Data page via the Web Client running on the VSM server.

1. Click **Back Up and Restore System Data** on the home page.
2. Click **Back Up** in the pop-up dialog to enter the backup page.
3. Select the system data type for backup.

   Configured Data

   The data configured via the Web Client, including physical resources, logical resources, user permissions, etc. It is selected by default.

   Configured Pictures

   The pictures uploaded when setting maps, persons, vehicles, etc.
4. Set the backup schedule to run backup regularly.
   1) Select the frequency to back up the system data.

   Note

   - If you select the data type besides configured data, you cannot set the frequency as **Daily**.
   - If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

   2) Select what time of the day to start backup.
   3) Set the **Max. Number of Backups** to define the maximum number of backup files available on the system.

Note

The value ranges from 1 to 5.

5. **Optional:** Click **Back Up Now** and click **OK** in the pop-up dialog if you need to perform the backup immediately.
6. Click **Save**.

20.2 Restore Database

When an exception occurs, you can restore the database if you have backed up the database.

Before You Start
You should have backed up the database. Refer to ***Set System Data Backup*** for details.

Perform this task when you need to restore the database.

Steps

Note

Database recovery will restore the database to an earlier state. Thus the data added after that state will be lost.

1. Click **Back Up and Restore Database** on the home page.
2. Click **Restore** in the pop-up dialog to enter the database restore page.
3. Select a backup file to restore the database to an earlier state.
4. Click **Restore** to confirm the database recovery.

What to do next
After restoring the database, you must reboot the VSM via Service Manager and log in again via Web Client.

20.3 Export Configuration File

You can export and save configuration data to the local PC, including Remote Site, recording settings and etc.

Perform this task when you need to export configuration data.

Steps

1. Click **Export Configuration Data** on the home page to open the Export Configuration Data dialog.
2. Select the configuration data type to export.
3. Click **Export** to save the data to your local PC.

Note

- You can set the saving path by following the prompt of the browser.
- The configuration data file is in CSV format.

Chapter 21 Manage System Security

System security is crucial for your system and property, you can set the password strength and lock IP address to prevent malicious attacks, and set other security policies to increase the security of the system.

Perform this task to set the minimum password strength, IP address locking, and other security policy settings to prevent malicious attacks.

Steps

1. Click **Security → Security Settings** to open the Security Settings page.
2. Set **Lock IP Address** switch to ON and the number of failed login attempts is limited.
   1) Select the allowable login attempts for accessing X-VMS.

      Note

      Failed login attempt includes failed password attempt and failed verification code attempt.

   2) Set the locking duration for this IP address. During the locking duration, the login attempt from this IP address is not allowed.

   The number of login attempts is limited.
3. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
4. Set the maximum password age.
   1) Set **Enable Maximum Password Age** switch as ON to force user to change the password when password expires.
   2) Set the maximum number of days that the password is valid.

      Note

      After this number of days, you will have to change the password. You can select the pre-defined time length or customize the time length.
5. Configure the settings to automatically lock the Control Client after a time period of inactivity on the Control Client.
   1) Set **Auto Lock Control Client** switch to ON to lock the Control Client after a time period of inactivity on Control Client.
   2) Select time period for user inactivity. You can select the pre-defined time period or customize the time period.
6. Click **Save**.

Chapter 22 System Configuration

You can configure the site name, WAN IP address, NTP settings, active directory, etc. for VSM, and perform other settings for the system.

- For the VSM of Central System, you can enable it to receive the registration from Remote Site.
- For the VSM without Remote Site Management module, you can set to register it to the Central System as a Remote Site.

22.1 Set Site Name

You can set a name for the current system.

Perform this task when you need to set a site name for the current VSM.

Steps

1. Click **System → Normal → Site Name** on home page.
2. Edit the site name for the current VSM.
3. Click **Save**.

22.2 Set Warning Threshold for Server Usage

You can enable the system to trigger an alarm if the VSM server's CPU usage and RAM usage reaches a pre-defined warning threshold and lasts for a pre-defined time. The related threshold value can be checked via the Control Client.

Perform the following steps for setting the warning threshold of CPU and RAM usage

Steps

1. Click **System → Normal → Server Usage Thresholds** on the home page.
2. Drag the ⌂ to adjust the CPU and RAM threshold value.
3. Define the duration in the **Notify if Value Exceeds for (s)** field for CPU Usage and RAM Usage.

Example

- If you set warning threshold as 60%, and set 20 in the **Notify if Value Exceeds for (s)** field of CPU Usage, you can view the CPU status changes to Waring in Health Monitoring in Control Client when the CPU usage reaches the warning threshold and lasts for 20 seconds.
- If you set 60% as the warning threshold, and set 20 in the **Notify if Value Exceeds for (s)** field of CPU Usage, and set an alarm for CPU Warning (see ***Add Alarm for X-VMS Server***), the alarm will be triggered when the CPU usage reaches the warning threshold and lasts for 20 seconds.

22.3 Set NTP

You can set the NTP server for syncing the time between the VSM and the NTP server.

Perform the following task when you need to set NTP server.

Steps

1. Click **System → Network → NTP Settings** .
2. Set the **Time Synchronization** switch to ON to enable the NTP function.
3. Set the NTP server address and NTP port.
4. Enter the interval for the auto time synchronization.
5. **Optional:** Click **Test** to test the communication between the VSM and NTP server.
6. Click **Save**.

22.4 Set Active Directory

If you have the AD (Active Directory) domain controller which contains the information (e.g., user data, computer information), you can configure the settings to get the related information. In this way, you can add the users that belong to an organization unit (OU) (e.g., a department of your company) to X-VMS conveniently.

Perform this task when you need to set active directory.

Steps

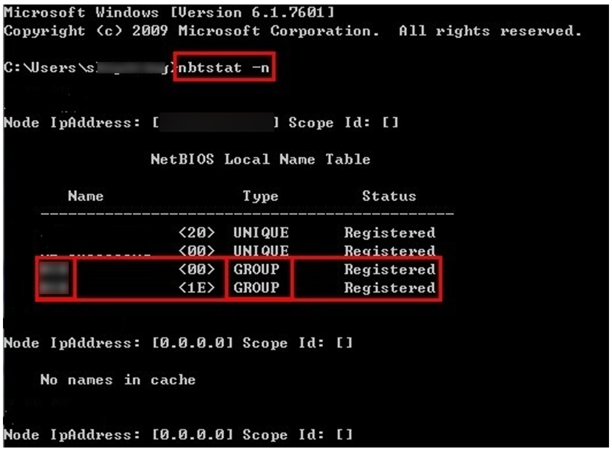
1. Click **System → Network → Active Directory** on the home page.
2. Configure the basic information parameters to connect to the AD domain controller.

   Domain Name

   The domain name of the AD domain controller.

   Note

   - X-VMS only supports the NetBIOS format: e.g TEST\user and not the DNS Domain name format.
   - To get the NetBIOS domain name, open the CMD window and enter ***nbtstat – n***.
     The NetBIOS domain name is the one in **GROUP** type.

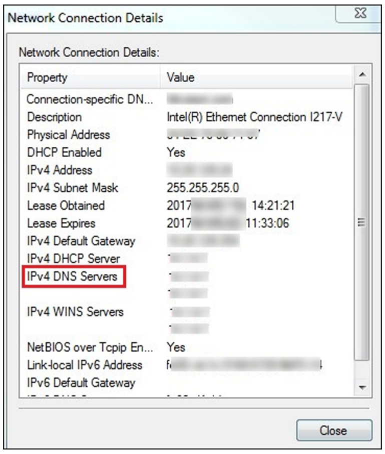


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\s[redacted]>nbtstat -n

Node IpAddress: [[redacted]] Scope Id: []

                NetBIOS Local Name Table

       Name               Type         Status
    ---------------------------------------------
    [redacted]     <20>  UNIQUE      Registered
    [redacted]     <00>  UNIQUE      Registered
    [redacted]     <00>  GROUP       Registered
    [redacted]     <1E>  GROUP       Registered

Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

Node IpAddress: [0.0.0.0] Scope Id: []
```

Figure 22-1 How to Get NetBIOS Domain Name

Host Name

The DNS server's IP address. You can get it in Network Connection Details.



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN...	[redacted]
Description	Intel(R) Ethernet Connection I217-V
Physical Address	[redacted]
DHCP Enabled	Yes
IPv4 Address	[redacted]
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	2017[redacted] 14:21:21
Lease Expires	2017[redacted] 11:33:06
IPv4 Default Gateway	[redacted]
IPv4 DHCP Server	[redacted]
IPv4 DNS Servers	[redacted] [redacted]
IPv4 WINS Servers	[redacted] [redacted]
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	[redacted]
IPv6 Default Gateway	

Figure 22-2 How to Get Host Name

Port No.

The port No. of the AD domain controller. By default, it is 389.

Enable SSL (Optional)

Enable SSL if required by the AD domain controller.

User Name

The user name of the AD domain controller. This needs to be the domain administrator.

Password

The password of the AD domain controller.

Base DN (Distinguished Name)

Enter the filter condition in the text filed if you are familiar with the format. Or you can click **Fetch DN** to get the filter condition entered automatically.

Note

- Only users found within an Organizational Unit (OU) in the domain can be imported. Click **Fetch DN** to have the filter condition entered automatically.
- If you enter the Base DN manually, you need to define the root node as desired. If you click **Fetch DN**, then the entire structure stored on the AD domain controller will be obtained.

3. **Optional:** Link the person information you concerned stored in the domain to the person information in the system.
   1) Set the **Link Person Information** switch to ON.

      The email and custom additional information items (see ***Custom Additional Information***) are displayed in the Person Information area by default. You can set the link relationship for those or add new person information items as you desired.
   2) **Optional:** Click **Add New** to add a person information item you concerned.

      Note

      - You needn't add the basic person information items, including ID, First Name, Last Name, Phone, and Remark) manually, which has the default link relationship with the domain.
      - The new person information item is also displayed on Custom Additional Information page, where you can edit or delete the items. Refer to ***Custom Additional Information*** for details.
      - The person information item is case-sensitive.
   3) **Optional:** Click + to show the person information items stored in the domain.
   4) Check the checkbox in the domain to link it to the added person information items when importing the domain persons.
   5) **Optional:** Hover over the linked person information in domain and click × to remove the relationship. You can also change the link relationship among each other by clicking and dragging the one item to anther.
4. Click **Save**.

   After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on User Management page.

   If the Link Person Information function is enabled, the corresponding person information in the system will match the linked person information in the domain and cannot be edited.

22.5 Enable Receiving Generic Event

After creating a generic event to analyze the received TCP and/or UDP data packages from a very wide range of external systems, you can enable the receiving generic event function so that the system can receive the configured generic events.

Perform this task when you need to enable receiving generic event function.

Steps

1. Click **System → Network → Receiving Generic Event** .
2. Check **Receiving Generic Event** to enable this function.
3. Click **Save**.

Note

You can configure the system's port No. for generic event: Open Service Manager (installed on the PC running VSM service), and click **VSM Platform Video Surveillance Management Service** to edit.

22.6 Allow for Remote Site Registration

For the system with Remote Site Management module (as we called Central System), it can receive the registration from other Remote Sites after enabling this function.

Before You Start

If a remote site needs to register to the Central System, it should open the Remote Site's Web Client and enter **Registering to Central System** to configure the Central System's parameters. See ***Register to Central System*** for details.

Perform this task when you need to allow the Central System to accept the registration from Remote Site.

Steps

Note

Allowing for Remote Site registration is only available for the system with Remote Site Management module.

1. Click **System → Network → Receiving Site Registration** .
2. Check **Receiving Site Registration** to enable this function.
3. Click **Save**.

22.7 Register to Central System

For the system without Remote Site Management module (as we called Remote Site), it can register to the Central System after enabling this function and setting the Central System's parameters.

Before You Start

For Central System, it should enable the receiving site registration function so that it can receive the Remote Site registration. See ***Allow for Remote Site Registration*** for details.

Perform this task when you need to register the Remote Site to the Central System.

Steps

Note

Registering to Central System is only available for the system without Remote Site Management module.

1. Click **System → Network → Registering to Central System** .
2. Set the **Registering to Central System** switch to ON to enable this function.
3. Enter the IP address and port No. of Central System.

   Note

   Open Service Manager (installed on the PC running central system's VSM service), and click **X-VMS Video Surveillance Management Service** if you need to view or edit the Central System's port.
4. Click **Save**.

22.8 Set WAN Access

In complicated network environments, you need to set a static IP address and ports for X-VMS to enable it to access the VSM server via WAN (Wide Area Network). For example, if the VSM server is in a local area network, and you need to visit the system via the Web Client or Control Client running in WAN, you should enable WAN access and set a static IP address and ports for X-VMS.

Perform this task when you need to set WAN access.

Steps

1. Click **System → Network → WAN Access** .
2. Set the **WAN Access** switch to ON to enable the WAN access function.
3. Enter a static IP address for WAN access.
4. Set the port for X-VMS, including HTTP, HTTPS, RTSP (Real Time Streaming Port), video file streaming port, and WebSocket port.
5. **Optional:** If you adopts generic event to integrate X-VMS with external sources, you need to set the TCP port and UDP port to receiving the TCP and/or UDP data packages.

   Note

   For setting the generic event, refer to ***Configure Generic Event*** .
6. **Optional:** For the VSM of Central System, set the port to receive the registration from a Remote Site.

   Note

   This configuration item is only available for the Central System with a Remote Site Management module based on the License you purchased.

7. Click **Save**.

22.9 Set Network Timeout

Network timeout duration refers to the default waiting time for the configurations on the Web Client. The configuration will be regarded as failure if no response within the configured timeout time.

The minimum default waiting time of the interactions between the configurations and VSM server is 60s, the minimum time between VSM server and devices is 5s, and the minimum time between the configurations and devices is 5s.

Note

This parameter affects all the Web Clients accessing the current VSM server.

22.10 Set Device Access Mode

Set the access mode as automatically judge or proxy mode to define how the system accesses all the added encoding devices and decoding devices.

Perform this task to define how the system accesses all the added encoding devices and decoding devices.

Steps

1. Click **System → Network → Device Access Mode** .
2. Set the device access mode as automatically judge or proxy mode.

   Automatically Judge

   The system will automatically judge the condition of network connection and then set the device access mode accordingly as accessing directly or accessing via Streaming Gateway and Management Service.

   Proxy

   The system will access the device via Streaming Gateway and Management Service. It is less effective and less efficient than accessing directly.
3. Click **Save** to confirm the settings.

   System accesses all the added encoding devices and decoding devices via the selected mode.

22.11 Set Server NIC

You can select the NIC of the current VSM server so that the system can receive the alarm information of the device connected via ONVIF protocol.

Perform this task when you set server NIC.

Steps

1. Click **System → Network → Server NIC** .
2. Select the currently used NIC name of VSM in the drop-down list.

   The NIC information including description, MAC address, and IP address will display.
3. Click **Save**.

22.12 Set Data Retention Period

You can set the data retention period for the events, logs, and some records in VSM server, such as recording tags, face comparison data, and so on.

Perform the following task to set data retention period.

Steps

1. Click **System → Storage → Data Recorded in System** .
2. Set the data recorded period from the drop-down list for the required data types.

   Note

   The card swiping records are saved as the configured period. The user with the permission can search the persons' swiping records and view related information during this period, even if the searched persons have been deleted from the VSM server.
3. Click **Save**.

22.13 Set Holiday

You can add the holiday to define the special days that can adopt different shift schedule or access control schedule.

Perform this task to add some special days as holiday.

Steps

1. Click **System → Schedule → Holiday Settings** .
2. Click **Add** to open the adding holiday dialog.

   Note

   You can add up to 16 holidays.
3. Set a customized name.
4. Click the Time field and define the start date and end date for the holiday period.
5. Click **Add** to save the holiday.
6. **Optional:** Perform the following operations after adding the holiday.

Edit Holiday	Click ✎ in the Operation column to edit holiday (including the holiday(s) in use).

Delete Holiday	Click × in the Operation column to delete the holiday.
Delete All Holidays	Click **Delete All** to delete all the holidays (except the holiday(s) in use).

22.14 Set Email Template

You should set the email template properly before sending the event message to the designate email account(s) as email linkage.

22.14.1 Configure Email Account

You should configure the parameters of sender's email account before the system can send the message to the designate email account(s) as email linkage.

Perform this task when you need to configure the sender's email account.

Steps

1. Click **System → Email** to enter the email page.
2. Click **Email Settings** to enter the Email Settings page.
3. Configure the parameters according to actual needs.

   Server Authentication (Optional)

   If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

   Cryptographic Protocol

   Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

   SMTP Server Address

   The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

   SMTP Server Port

   The default TCP/IP port used for SMTP is 25.
4. Click **Email Test**to test whether the email settings work or not.

   The corresponding attention message box will pop up.
5. Click **Save**.

22.14.2 Add Email Template

You can set email templates including specifying the recipient, email subject, and content, so that the system can send the information to the designate recipient according to the pre-defined email template.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Perform this task when you need to add a new email template.

Steps

1. Enter **System → Email** to enter the email page.
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

   Name

   Create a name for the template.

   Recipients

   Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

   Click **Add Email** and enter the recipient(s) email address to send the email to.

   Note

   You can enter multiple recipients and separate them by ";".

   Subject

   Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

   Content

   Define the event information to be sent. You can also click the button in the lower part of the window to add the related information to the content.

   Note

   If you select to add the event time to the email subject or content, and the email application (such as Outlook) and the system are in different time zones, the displayed evnet time may have some deviations.

4. **Optional:** Check **Attach Image** to send email with image attachment.
5. Finish adding the email template.
   - Click **Add** to add the template and go back to the email template list page.
   - Click **Add and Continue** to add the template and continue to add other templates.

   The email template will be displayed on the email template list.
6. Perform the following operation(s) after adding the email template:

Edit Template	Click ✎ in the Operation column to edit template details.
Delete Template	Click × in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

22.15 Send Report Regularly

Reports are essential documents in order to submitting performance to users to make business run smoothly and effectively. Users can use reports as basis in creating decisions, addressing problems, checking tendency and comparison, etc. X-VMS provides report functions that the system can send reports automatically and regularly to target users by emails, showing the occurred events and alarms, number of passing vehicles, people counting, queue management, and temperature status during specified time period.

22.15.1 Send Event Report Regularly

You can set a regular report rule for specified system-monitored events, and the system can send an email with a report attached to the target recipients daily or weekly, showing the details of specified system-monitored events triggered in the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 event records in total.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Event**.
3. Create a name for the report.
4. Set the system-monitored event(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the added system-monitored events are displayed.
   2) (Optional) Filter the events by event source type and triggering event.
   3) Select the event(s).

      Note

      Up to 32 events can be added in one report rule.
   4) Click **Add**.
5. Set the report type as **Daily** or **Weekly** and set the sending time.

   Daily Report

Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains information of the events triggered on the day (24 hours) before the current day.

For example, if you set the sending time as 20:00, the system will send a report at 20:00. every day, containing details of all the events triggered between 00:00. and 24:00. before the current day.

Weekly Report

As compared to daily report, weekly report can be less time-consuming, since it is not to be submitted every day. The system will send one report at the sending time every week, which contains information of the events triggered on the last 7 days before the sending date.

For example, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing details of all the events triggered between last Monday and Sunday.

6. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

7. Select Excel or PDF as the report format.
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.15.2 Send Alarm Report Regularly

You can set a regular report rule for specified alarms, and the system can send an email with a report attached to the target recipients daily or weekly, showing the details of specified alarms triggered in the day or the week.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

One report can contain up to 10,000 alarm records in total.

1. Click **System** on the home page and enter **Report** page.

2. Select the report category as **Alarm**.
3. Create a name for the report.
4. Set the alarm(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the added alarms are displayed.
   2) (Optional) Filter the alarms by alarm source type, triggering event, and alarm priority.
   3) Select the alarm(s).

      Note

      Up to 32 alarms can be added in one report rule.
   4) Click **Add**.
5. Set the report type as **Daily** or **Weekly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains information of the alarms triggered on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing details of all the alarms triggered between 00:00 and 24:00 before the current day.

   Weekly Report

   As compared to daily report, weekly report can be less time-consuming, since it is not to be submitted every day. The system will send one report at the sending time every week, which contains information of the alarms triggered on the last 7 days before the sending date.

   For example, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing details of all the alarms triggered between last Monday and Sunday.
6. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .
7. Select Excel or PDF as the report format.
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.15.3 Send Passing Vehicle Report Regularly

You can set a regular report rule for specified ANPR cameras, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of passing vehicles detected by these ANPR cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Vehicle**.
3. Create a name for the report.
4. Set the ANPR camera(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the ANPR camera(s) added to the current site are displayed.
   2) Select the ANPR camera(s).
   3) Click **Add**.
5. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the number of passing vehicles detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the number of passing vehicles detected on the last 7 days or last month before the sending date.

   For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing number of passing vehicles detected between last Monday and Sunday.

6. After setting the report time, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of passing vehicles detected in each hour or each minute for one camera.
7. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .
8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.15.4 Send People Counting Report Regularly

You can set a regular report rule for specified people counting cameras, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of people entered or exited, detected by these people counting cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **People Counting**.
3. Create a name for the report.
4. Set the people counting camera(s) contained in the report.
   1) In the Report Target field, click **Add**.

      All the people counting camera(s) added to the current site are displayed.

2) Select the people counting camera(s).
3) Click **Add**.

5. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the number of people entered and exited detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the number of people entered and exited detected on the last 7 days or last month before the sending date.

   For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing number of people entered and exited detected between last Monday and Sunday.

6. After setting the report time, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each camera respectively in the report, showing the number of people entered and exited detected in each hour or each minute for one camera.

7. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

8. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.15.5 Send Queue Analysis Report Regularly

You can set a regular report rule for specified cameras which support queue management, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing queue exceptions, number of persons in the queue, and queue status, detected by these people counting cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Queue**.
3. Create a name for the report.
4. Set the camera(s) which support queue management contained in the report.
   1) In the Report Target field, click **Add**.

      All the camera(s) which support queue management added to the current site are displayed.
   2) Select the camera(s).
   3) Click **Add**.

   The report will show the data of all the queues configured on the cameras.

   Note

   For configuring the queue, refer to the user manual of the camera.
5. Set the report type as **Daily**, **Weekly**, or **Monthly**.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing queue data detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the queue data detected on the last 7 days or last month before the sending date.

   For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing queue data detected between last Monday and Sunday.
6. Set the content in the report.

Queue Exception

The number of exceptions (people amount exceeding and waiting timeout) of each queue.

People Amount Exceeding

The number of persons in the queue exceeds the configured threshold.

Waiting Timeout

The waiting duration for the persons in the queue exceeds the configured threshold.

Person Amount in Queue

The number of persons in each queue.

Queue Status

The status of each queue, including persons' waiting duration and number of persons in the queue.

If you select **Queue Status**, you should select the **Analysis Type** as waiting duration or queue length, and set the range.

Waiting Duration

The report will show the number of persons in each queue who have waited for specified duration.

For example, if you set the report range as ***Range 1 < 300 ≤ Range 2 ≤ 600 < Range 3***, the report will show that in each queue, how many persons have waited for less than 300s, how many persons have waited for 300 to 600s, and how many persons have waited for more than 300s.

Queue Length

The report will show how many seconds each queue status (number of persons in different ranges) lasts.

For example, if you set the report range as ***Range 1 < 5 ≤ Range 2 ≤ 10 < Range 3***, the report will show that in each queue, how many seconds the status lasts when there are less then 5 persons, how many seconds the status lasts when there are 5 to 10 persons, and how many seconds the status lasts when there are more than 10 persons.

7. Set the sending time according to the report type.
8. Select the email template from the drop-down list to define the recipient information and email format.

Note

You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

9. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.15.6 Send Temperature Report Regularly

You can set a regular report rule for specified thermal cameras, and the system can send an email with a report attached to the target recipients daily, weekly, or monthly, showing temperature exceptions or min./max. temperature, detected by these thermal cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Set the email settings such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. Click **System** on the home page and enter **Report** page.
2. Select the report category as **Temperature**.
3. Create a name for the report.
4. Set the thermal camera(s) and presets contained in the report.
   1) In the Report Target field, click **Add**.

      All the thermal camera(s) added to the current site are displayed.
   2) Select the thermal camera(s) and preset.
   3) Click **Add**.

   The report will show the temperature exceptions (including temperature too high or too low) or maximum and minimum temperature of different thermometry points on these presets.
5. Set the report type as **Daily**, **Weekly**, or **Monthly** and set the sending time.

   Daily Report

   Daily report shows data on a daily basis. The system will send one report at the sending time every day, which contains data detected on the day (24 hours) before the current day.

   For example, if you set the sending time as 20:00, the system will send a report at 20:00 every day, containing the temperature exceptions or min./max. temperature detected between 00:00 and 24:00 before the current day.

   Weekly Report and Monthly Report

   As compared to daily report, weekly report and monthly report can be less time-consuming, since they are not to be submitted every day. The system will send one report at the sending time every week or every month, which contains the temperature exceptions or min./max. temperature detected on the last 7 days or last month before the sending date.

For example, for weekly report, if you set the sending time as 6:00 on Monday, the system will send a report at 6:00 in the morning on every Monday, containing temperature exceptions or min./max. temperature detected between last Monday and Sunday.

6. After setting the report time, set how the report will present the data detected in the specified time period.

   Example

   For example, if you select the report type as **Daily**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each thermometry point respectively in the report, showing the temperature exceptions or min./max. temperature detected in each hour or each minute.

7. Set the content in the report.

   Temperature Exception

   The number of exceptions on temperature (temperature too high or too low) of each thermometry point.

   Temperature Status

   The maximum temperature and minimum temperature of each thermometry point.

8. Select the email template from the drop-down list to define the recipient information and email format.

   Note

   You can click **Add New** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

9. Finish adding the report.
   - Click **Add** to add the report and go back to the report list page.
   - Click **Add and Continue** to add the report and continue adding other reports.

22.16 Set Transfer Protocol

You can set the VSM server's transfer protocol to define the access mode for the VSM (via Web Client, Control Client, or Mobile Client) as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Perform this task when you need to set the VSM server's transfer protocol.

Steps

Note

Setting transfer protocol is only available when accessing the Web Client on the VSM server locally.

1. Click **System → Advanced → Transfer Protocol** .
2. Select **HTTP** or **HTTPS** as the transfer protocol.

3. If you select **HTTPS**, you are required to set the certificate. You can use the system provided certificate, or select **New Certificate** and click ··· to select a new certificate file.

Note

- The new certificate should be in PEM format.
- The public key and private key should be in the same certificate file.

4. Click **Save**.
   - The VSM server will reboot automatically after changing the transfer protocol or the certificate.
   - The users of the Control Clients and Mobile Clients connecting to this VSM server will be forced logout, and are not allowed to login until rebooting completed.

Result

You can access the VSM via Web Client, Control Client, or Mobile Client by the selected transfer protocol.

22.17 Set Camera ID

When displaying live view on smart wall, you may use a keyboard for convenience operations such as starting live view on smart wall, PTZ control, etc. If you want to display certain camera's live view on smart wall, you should press the camera's identifier number on the keyboard, which is called **Camera ID**. As a result, X-VMS provides this module for you to set a unique ID for each camera.

Click **System → Advanced → Camera ID** to enter the camera ID settings page.

You can filter the cameras by setting the site and area, or entering keywords of camera name or camera ID.

The system provides a default ID for each camera. You can edit the default value for the cameras if needed.

Note

The camera ID should be unique in the system.

22.18 Set Working Mode

In access control, if you adopt DS-K5600 face recognition series (such as DS-K5603-Z) in actual application, you need to set the working mode for these devices after adding them to the system according to actual needs.

If the DS-K5600 series device is applied with our turnstile, select **Face Recognition Terminal** mode to form a turnstile with face recognition function. The persons can access the turnstile by scanning their faces with the DS-K5600 series device after setting the face credentials and access levels.

If the DS-K5600 series device is applied with other third-party turnstile, select **Access Control Terminal** mode and you can set access levels in the system to define the access permissions.

22.19 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the system, you should export the service component certificate stored in the VSM server and import it to the Streaming Server or Cloud Storage Server you want to add so that the certificates of the Streaming Server or Cloud Storage Server and VSM are the same.

Perform this task when you need to export service component certificate.

Steps

Note

Exporting VSM server's service component certificate is only available when you access the Web Client on the VSM server locally.

1. Click **System → Advanced → Service Component Certificate** .
2. Click **Export** to export the service component certificate and save it in the local PC.

What to do next

Import the exported certificate file to the Cloud Storage Server and Streaming Server you want to add. For the following operations, see ***Add Cloud Storage Server*** and ***Add Streaming Server*** for details.

22.20 Configure System Hot Spare

If you build the hot spare system when installing the VSM service, you can enable the hot spare function and configure the hot spare property of the current VSM server as host server or spare server. When the host server fails, the spare server switches into operation, thus ensuring the stability of the system.

Before You Start

You should build the hot spare system when installing the VSM service. See ***Install Module*** for details.

Perform this task when you need to set system hot spare.

Steps

1. Click **System → Advanced → Hot Spare** .
2. Set the **Hot Spare Configuration** switch to ON to enable the hot spare function.

   The current VSM server's server name and available IP address will be displayed.
3. Set the server as host server or spare server in Hot Spare Property.
4. Click **Save**.

22.21 Reset Device Network Information

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment. Otherwise the device live view, playback and other functions will be affected.

Perform this task when you need to reset the network information of the added device.

Steps

1. Click **System → Advanced → Reset Network Information** .
2. Click **Reset** to one-touch reset the device network information.

Chapter 23 Applications

The X-VMS also provides functionalities of live view, playback, and local configuration through web browser.

Note

- If the VSM's transfer protocol is HTTPS, the Applications module (including Live View, Playback, and Local Configuration) is available only when accessing the Web Client via Internet Explorer.
- If the VSM's transfer protocol is HTTP, the Live View and Playback modules are available for Internet Explorer, Google Chrome, and Firefox. But Local Configuration module is available for Internet Explorer only.

23.1 Live View

In the Live View module of Web Client, you can view the live video of the added cameras and do some basic operations, including picture capturing, recording, PTZ control, and so on.

23.1.1 Start Live View

After adding the cameras into areas, you can start live view to view the camera's live video, and perform some basic operations via the Web Client.

Before You Start

An area with cameras assigned to is required to be defined for live view.

Perform this task when you need to view the live video of the camera via Web Client.

Steps

1. Click **Live View** on home page to enter the Live View page.
2. Select a site from the drop-down list.

   The area and cameras of the selected site is displayed.
3. **Optional:** Enter a keyword of camera name or area name in the search field and click **Search in All Sites** or **Search in Current Site** to search the cameras or areas.

   All the search results display.

   Note

   You can move the cursor to the camera name to view the image thumbnail.
4. **Optional:** Click ⊞ on the live view toolbar, and select a window division mode.

Note

Up to16-window mode is available when you access the Web Client via the Google Chrome, Firefox or Internet Explorer.

5. Drag the camera to the display window, or double-click the camera name after selecting the display window to start the live view. The selected window is outlined in red.

Note

- If the system is Central System with Remote Site Management module, you can also view the live video of the cameras imported from remote site. For managing remote site's cameras in areas, refer to ***Add Camera to Area for Remote Site*** .
- You can also double-click the area name to start the live view of cameras in the area. The display windows adapt to the number of cameras in the area.

6. **Optional:** Move the mouse over the display window during live view, and you can perform some operations, such as digital zoom, instant playback, two-way audio, and so on.

23.1.2 PTZ Control

Cameras with the pan/tilt/zoom functionality can be controlled through the web browser. You can also set the preset, patrol, and pattern for the cameras.

Configure Preset

A preset is a predefined image position which contains configuration parameters for pan, tilt, zoom, focus and other parameters. You can also set a virtual preset after enabling digital zoom.

Perform this task when you need to add a preset for the camera.

Steps

1. Click **Live View** on the home page to enter the live view page.
2. Start live view of camera.

Note

See ***Start Live View*** for details about how to start live view.

3. Click on the live view toolbar to open the PTZ control panel.
4. Click ⚑ to enter the PTZ preset configuration panel.
5. Click the direction buttons to move the camera to the desired view or zoom in/out the view.

Note

You can also scroll the mouse wheel to zoom in or zoom out the view.

6. Select a PTZ preset number from the preset list and click ✎ .

7. Create a name for the preset.
8. Click **OK** to save the settings.

Note

Up to 256 presets can be added.

9. **Optional:** After setting the preset, you can do one or more of the followings:

Call Preset Double-click the configured preset in the list, or select the preset and click ▶ to call the preset.

Edit Preset Select the configured preset from the list and click ✎ to edit it.

Delete Preset Select the configured preset from the list and click × to delete it.

Configure Patrol

A patrol is a scanning track specified by a group of user-defined presets (including virtual presets), with the scanning speed between two presets and the dwell time of the preset separately programmable.

Before You Start

Two or more presets for one PTZ camera need to be added.

Note

See ***Configure Preset*** for details.

Perform this task when you need to add a patrol for the camera.

Steps

1. Click **Live View** on the home page.
2. Start live view of camera.

Note

See ***Start Live View*** for details about how to start live view.

3. Click 👤 on the live view toolbar to open the PTZ control panel.
4. Click ⟳ to enter the patrol configuration panel.
5. Select a patrol and click ✎ .
6. Click + to add a configured preset, and set the dwell time and the patrol speed.

Note

- The preset dwell time ranges from 15 to 30s.
- The patrol speed ranges from 1 to 40.

7. Repeat the above step to add other presets to the patrol.
8. **Optional:** Perform the following operations after adding the preset.

Remove Preset from Patrol Select the added preset and click × to remove the preset from the patrol.

Adjust Preset Sequence Select the added preset and click ↑ ↓ to adjust the preset sequence.

9. Click **OK** to save the patrol settings.

> **Note**
>
> Up to eight patrols can be configured.

10. **Optional:** Perform the following operations after setting the patrol.

Call Patrol Click ⏵ to start the patrol.

Stop Calling Patrol Click ⏹ to stop the patrol.

Configure Pattern

You can set patterns to record the movement of the PTZ.

Perform this task when you need to add a pattern for the camera.

Steps

1. Click **Live View** on the home page to enter the Live View page.
2. Start live view of the camera.

> **Note**
>
> See ***Start Live View*** for details about how to start live view.

3. Click ▣ on the live view toolbar to open the PTZ control panel.
4. Click ↗ to enter the PTZ pattern configuration panel.
5. Click ⏵ to start recording movement pattern path.
6. Click the direction buttons and other buttons to control the PTZ movement.
7. Click ⏹ to stop and save the pattern recording.

> **Note**
>
> Only one pattern can be configured each time, and the newly-defined pattern will overwrite the previous pattern.

8. **Optional:** Perform the following operations after setting the pattern.

Call Pattern Click ⏵ to call the pattern.

Stop Calling Pattern Click ⏹ to stop calling the pattern.

Delete Pattern Click × to delete the pattern.

23.2 Playback

The video files stored on the local storage devices such as HDDs, Net HDDs and SD/SDHC cards or the Recording Server can be searched and played back remotely through the web browser.

23.2.1 Search Video File

You can search the video files of cameras and filter the searched video files by video type or by storage location.

Perform this task when you need to search the specific video files.

Steps

1. Click **Playback** on home page to open the Playback page.
2. **Optional:** Enter a keyword of camera name or area name in the search field and click **Search in All Sites** or **Search in Current Site** to search the cameras or areas.

   All the search results display.

   Note

   You can move the cursor to the camera name to view the image thumbnail.
3. Drag the camera to the display window, or double-click the camera to start the playback.

   Note

   If the system is central system with Remote Site Management module, you can also play back the recorded video of the cameras imported from remote site. For managing remote site's cameras in areas, refer to ***Manage Area*** .
4. **Optional:** Click the date and time on the toolbar to select the date and time to search the video files.

   Note

   - In the calendar panel, the date with video files will be marked with a triangle.
   - The calendar is not supported by cameras on remote site.
5. **Optional:** Click ▽ on the playback toolbar to select the video file type for playback.
6. **Optional:** Select the storage location and the stream type of the video files for playback.

For camera configured with auxiliary storage:	Select the storage location of the video files for playback.
For camera configured with dual-stream recording:	Select the stream type of the video files for playback.

Note

For setting the storage location of recording, refer to ***Configure Recording*** .

23.2.2 Play Video File

After searching the video files, the playback starts. You can control the video playback via timeline. The timeline indicates the time duration for the video file.

Perform this task when you need to control the playback.

Steps

1. Click **Playback** on home page to open the Playback page.
2. Search the video file of cameras for playback. For details, refer to ***Search Video File*** .

   The playback starts.
3. Click the icons on the toolbar to control the playback.
4. Click on the timeline or drag the timeline to play back the video of the specific time.
5. **Optional:** Click ⊞ or ⊟ or use the mouse wheel to scale up or scale down the timeline bar.
6. **Optional:** Move the cursor to the display window in playback to access further functions, including capture, clipping, and other functions.

Open Digital Zoom

Click 🔍 to enable the digital zoom function and draw a rectangle on the video. Click again to disable the function.

Note

When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function.

Camera Status

Click 📈 to show the camera's recording status, signal status, connection number, etc.

Stream Switch

Click , , or (if supported) to switch the live view stream to main stream, sub-stream, or smooth stream (if supported).

Note

The smooth stream will show if the device supports smoothing function. You can switch to smooth stream if in low bandwidth situation to make live view more fluent.

Audio Control

Click 🔊 or 🔇 to turn off/on the sound.

Note

You can adjust the volume when moving the cursor on 🔊 .

23.3 Local Configuration

X-VMS provides live view and playback functions via the Web Client. You can set the related network transmission parameters (such as hardware decoding, stream type, etc.) for the performance of live view and playback via the current Web Client. You can also view the saving path of video files and captured pictures on your current PC.

Steps

Note

The parameters in Local Configuration only affect the current Web Client.

1. Click **Local Configuration** on home page to enter the Local Configuration page.
2. Click **Network Transmission** tab on the left.
3. Set the following parameters as desired.

   GPU Hardware Decoding

   Enable the GPU decoding for live view and playback to save CPU resources.

   Note

   - Your PC must support GPU hardware decoding.
   - After enabling GPU hardware decoding, restart live view and playback to take effect.
   - If the client shows a blurred screen after enabling GPU hardware decoding, disable it.

   Global Stream

   The default stream type for global usage in the current Web Client.

   If the device doesn't support smooth stream, it will use sub-stream. If the device doesn't support sub-stream, it will use main stream.

   If the network is in good condition, select main stream or sub-stream. If the network is in poor condition, select smooth stream.

   Threshold for Main/Sub-Stream

   If a window's proportion of the displaying area is larger than the configured threshold, the stream type will be main stream. If the proportion is smaller than the threshold, it will be switched to sub-stream.

   For example, if you set the threshold as ¼, when the window division turns to 5-window, the camera's stream type will be switched from main-stream to sub-stream.

   Note

   This parameter is only available when the **Global Stream** is set as **Main Stream**.

   Network Timeout

   The default waiting time for the operations in Applications on the current Web Client. The operations will be regarded as failure if no response within the configured time.

The minimum default waiting time of the interactions between the Applications and VSM server is 60s, the minimum time between VSM server and devices is 5s, and the minimum time between the Applications and devices is 5s.

Video Caching

Video caching should be determined based on network performance, computer performance, and bit rate. You can set is as **Small (1 Frame)**, **Medium (6 Frames)**, or **Large (15 Frame)**. Larger frame caching will result in better video performance.

Picture Format

Set the file format for the captured pictures during live view or playback. Currently it supports **BMP** and **JPEG** formats.

Device Access Mode

Restore Default

Restore the device access mode as configured in the **System → Device Access Mode** on Web Client.

Automatically Judge

Judge the device access mode according to the current network.

Directly Access

Access the device directly, not via X-VMS Streaming Service.

Proxy

Access the device via X-VMS Streaming Gateway and X-VMS Management Service.

Note

By default, the system will judge the device access mode according to the current network. If you change to other mode, it only affects the client you logged in currently.

4. **Optional:** Click **Default Value** to restore the defaults of the settings.
5. Click **Save**.
6. **Optional:** Click **Saving Path** on the left to view the saving path of the recorded or clipped video files and captured pictures during live view or playback in your local PC.

Chapter 24 Important Ports

X-VMS uses particular ports when communicating with other servers, devices, and so on.

Make sure that the following ports are not occupied for data traffic on your network and you should forward these ports on router for WAN access or open these ports in the firewall in case you may need to access the system via other networks.

Port No.	Description
NGINX Port	
80 (TCP)	Used for web browser access in HTTP protocol.
443 (TCP)	Used for web browser access in HTTPS protocol.
VSM Port	
14200 (TCP)	Used for Remote Site registration to central system.
15300 (TCP and UDP)	Used for receiving generic event.
Streaming Gateway Port	
554 (TCP)	Used for getting stream (real time streaming port).
559 (TCP)	Used for getting stream for Google Chrome or Firefox (WebSocket port).
10000 (TCP)	Used for getting stream for playback (video file streaming port).
Keyboard Proxy Service Port	
8910 (TCP)	Used for network keyboard to access the Keyboard Proxy Service.
NTP Service Port	
123 (UDP)	NTP port used for time synchronization.
Streaming Service Port	
554 (TCP)	Used for Streaming Service to get stream (real time streaming port).
559 (TCP)	Used for getting stream for Google Chrome or Firefox (WebSocket port).
10000 (TCP)	Used for Streaming Service to get stream for playback (video file streaming port).
6001 (UDP)	Network management port.

UD13408C